Kingdom of Saudi Arabia
Ministry of Education
Jazan University

JAZAN UNIVERSITY

JOURNAL OF
JAZAN UNIVERSITY
For
Applied Sciences

A Refereed Scientific Periodical

ISSN:1658-6913

Supplement To Vol. 11 No 1 September 2023(Rabi` al-Awwal)

Publication Rules

The University of Jazan provides an opportunity for scholars to publish their scholarly work on research. The editorial board will consider manuscripts from all fields of knowledge. Manuscripts submitted in either Arabic or English, and if the due accepted for publication, may not be published elsewhere, without permission of the Editor-in-Chief. The journal issues one volume per year. The types of manuscript classification used by the Editorial Board run as follows:

1. **Article:**
   An author's original work contributing new knowledge to the field in which research was conducted.
2. **Review Article:**
   A critical synthesis of the current literature in a particular filed, or a synthesis of the literature in a particular field during an explicit period of time.
3. **Brief Article:**
   A short article (note) with the characteristics of an article.
4. Book Reviews
5. **Forum:**
   Letters to the editor, comments, responses, preliminary results or findings, and miscellany

General Instructions

1. Submission of manuscripts:

Original manuscripts should be typewritten (one side only), using an A4 size paper, double spaced along with 3 copies. All pages are to be numbered consecutively, including tables and graphs. Tables, other illustrations, and references should be presented on separate sheets with their proper text position indicated.

2. Abstracts:

Manuscripts for articles, review articles, and brief articles require both Arabic and English abstracts, using no more than 200 words, in single column (13cm wide), for each version.

3. Tables and other illustrations:

Tables, charts, figures, and plates should fit the journal's page size (12.5 com x 18cm). All inner drawings must be presented on high quality. Tracing paper is necessary, using black Indian ink as well. Photographs may be submitted, but on glossy print paper in either black or color.

4. Abbreviations and Units:

A4 sizes and quantities should be expressed according to international standards. Standardized abbreviation should only be used. The names of periodicals should be abbreviated in accordance with the words of scientific periodicals.

5. Title Page:

Should contain the title, name of the authors, name and address of the institution, where the work was carried out. The title should be brief and use strong keywords. Scientific names of organism should be clearly stated and should be typed italic.

6. Text:

The organization of the manuscript should be as follows: Introduction, materials, results, discussion, and references. Results and discussions can be combined in one section. Acknowledgement (if needed) should be brief and added before the reference sections.

1. References:

Citation of the references (within the text) should be indicated by author. Date, style, and references should be listed in an alphabetical order and conform to the following examples: Periodical citations in the text are to be enclosed in one line brackets, e.g.(6).

Periodical references are to be presented in the following

form:

References number in line brackets ( ), author's name followed by a given name and/or initials, the title of an article or periodical (italicized), volume number, year of publication (in parentheses) and pages e.g.

Basahy, A.Y. (1992). Protein and Amino Acid contents in seeds of some soybean cultivate (Glycin Max 1) Arab Gulf J. Sci. Res. 11(2), 221-228.

Book Citation:

Book references should include the following:

Reference number ( ), author's surname followed by a given name and/or title of the book (italicized), place of publication, publisher, and year of publication.

Example:

Lehman. H.C. (1953). Age and Achievement. Princeton: Princeton University Press.

2. Content Notes:

Content notes are to be presented on separate sheets. They will be printed below a solid line separating the content notes from the text.

9. The manuscripts and forum items submitted to the journal for publication contain the author's conclusions and opinions, and if published they do no bear a conclusion or opinion of the Editorial Board.

10. Authors will be provided with 20 reprints free of charge, along with two issues of the journal. Additional copies could be purchased, if ordered when the proofs are returned. Price will be shown on the order form.

11. It is the responsibility of the researcher to make sure that the manuscript is free of linguistic, grammatical and typo errors.

12. The editors' board has the right to set priorities of publishing the research.

13. The journal is not obligated to repeat the research it reaches, whether it was approved for publication or not.

14. All the received research is subject to primary examination by the editorial board in order to determine their eligibility for arbitration. The editorial board is entitled to excusing itself from accepting the research without giving reasons.

15. The journal is published twice a year.

Kingdom of Saudi Arabia
Ministry of Education
Jazan University

JOURNAL OF
JAZAN UNIVERSITY
For
Applied Sciences

A Refereed Scientific Periodical

Supplement To Vol. 11 No 1 September 2023(Rabi` al-Awwal)

ISSN:1658-6913

Journal Jazan University

for applied sciences

Correspondence

All correspondence should be directed to:
Editor-in-chief of Jazan University Journal of Applied Sciences, Jazan - University City
Administrative Tower - PO Box 114 - Zip Code 4514, Kingdom of Saudi Arabia
jas@jazanu.edu.sa

فهرس المحتويات

الموضوع **صفحة**

Left Ventricular Thrombus: Insight into Pathophysiology, Risk Factors, Diagnosis, Complications, and Management- A Review Article

Ahmed Sayed
Assistance professor, Internal Medicine Department, College of Medicine, Jazan University, Saudi Arabia

Abstract

Left ventricular thrombus (LVT) is a serious complication of acute and chronic cardiovascular disease particularly when it is associated with compromised left ventricular systolic function. LVT is a major risk factor for systemic embolization which can lead to devastating health consequences. The pathophysiology of LVT is complex and involves the triad of Virchow's triad: blood stasis, tissue injury, and prothrombotic state. LVT detection has improved over the past few years due to advances in cardiac imaging technology. The main step of management is anticoagulation (heparin, vit K antagonist), which decreases the risk of systemic embolization. Use of new oral anticoagulation (NOAC) has limited evidence in these types of patients. This article reviews left ventricular thrombus with emphasis on evidence-based management and the most recent guidelines.

Keywords: cardiovascular disease; left ventricular thrombus; anticoagulation; new oral anticoagulation.

Introduction and background:

According to the World Health Organization's most recent report, published on June 11th, 2021: Cardiovascular disorders (CVDs) are one of the leading causes of death worldwide. Furthermore, 17.9 million people have died as a result of CVDs, accounting for 32% of all global deaths, the majority of which were caused by coronary artery disease or strokes (1). Even with early reperfusion therapy used in cases of acute myocardial infarction, left ventricular thrombus (LVT) continues to be a deadly cardiovascular disease complication. According to recent researches, the prevalence of LVT in acute myocardial infarction is 15-25% (2) and up to 36% in dilated cardiomyopathy (3). Despite adequate anticoagulation therapy, LVT remains a serious complication associated with a high risk of cerebral and peripheral arterial embolism and death (4, 5). According to American and European guidelines (6, 7), taking a vitamin K antagonist (VKA) for at least 3 to 6 months is recommended. Therefore, in this review, we aim to introduce LVT pathophysiology, relevant risk factors, diagnosis, complications, and management

Review

1.1 Definition of Left Ventricular Thrombosis:

One of the problems of the cardiovascular diseases (CVDs) is the development of thrombus or which is known as thrombosis. Thrombosis is considered one of the most severe complications that is linked to groups of CVDs such as myocardial infraction (MI), acute ischemic stroke and venous thromboembolism. Thrombosis occurs when a thrombus formed in the blood vessels and starts to stick to the wall of the blood vessels interrupting movement of the blood in the cardiovascular system. (8). Thrombus may be formed in several parts in the cardiovascular system, especially in the ventricle which is known as Left Ventricular Thrombosis (LVT). LVT is considered one of the most important complications of acute myocardial infraction in which the heart muscle cells starts to die because they do not get enough blood **(2)**. Also it can be a complication of dilated cardiac myopathy **(9)**. Despite Primary Percutaneous coronary interventions (PCI) that have been improved in the care of the patient **(10)**, the complications that occur after myocardial infraction such as LVT remain one of the causes of morbidity and mortality. In a study that has been published in 2010, it reveals that LVT is responsible for about 15% of incidence of morbidity and mortality which requires from the primary care providers to find more strategies for diagnosis, prevention and treatment of LVT **(11, 12)** Left ventricular thrombosis can result in serious complications that lead to the death. One of these complications is embolism that block other capillaries in the body such as brain leading to stroke **(13)**.

2. Pathophysiology of Left ventricular thrombosis:

Knowledge of the pathophysiology of LVT is important because it provides the main points to determine the best timing for providing diagnostic evaluation and therapeutic interventions (13) .

2.1 Relation between LVT and MI:

It has been determined that LVT is considered as a complication to acute myocardial infraction (AMI), especially acute ST-segment elevation myocardial infraction (STEMI) **(14).** According to research that has been published in 2019, the incidence of LVT is 12.3% detected by cardiac magnetic resonance (CMR) for patients who have survived from acute myocardial infraction. Also, the incidence of LVT is 6.2% detected by two-dimensional echocardiography for patients who have survived from acute myocardial infraction **(14)**. In another study that was made on 8000 patients with STEMI in 1998, LV thrombus was detected in 427 patients (5.1%) **(15)**.

Acute myocardial infraction (AMI) is a condition which is characterized by shortage of blood flow to the heart muscle leading to necrosis in the heart tissue with low blood flow **(16)**. AMI has several types, one of these types is acute ST-segment myocardial infraction (STEMI) which is characterized by ST-segment elevation due to occlusion of coronary artery with a thrombus **(17)**.

It has been demonstrated that the relation between Acute myocardial infraction (AMI) and LVT occurs due to several factors including blood stasis which occurs after regional and global dysfunction **(18)**. In fact, LVT occurs as a complication to acute anterior transmural MI, especially which occurs in the apex **(19)**. In case of apical stasis, it is associated with abnormal blood flow which is considered a predictive factor during formation of thrombus **(20)**. Different studies and clinical trials involving echocardiographic methods have determined that LVT occurs mainly in the first week after the occurrence of MI, particularly when such factors as endothelial injury and hypercoagulation are the most intense **(21)**. In the later course of infraction, LVT occurs mainly due to adverse remodeling which includes dilation in the left ventricle, reduced global function and formation of aneurysm **(21)**.

2.2 Relation between LVT and Virchow's triad:

The factors of Virchow's triad which include reduced ventricular motion, local myocardial injury and stasis of blood flow contribute mainly to the occurrence of the thrombus in the left ventricle **(22)**.

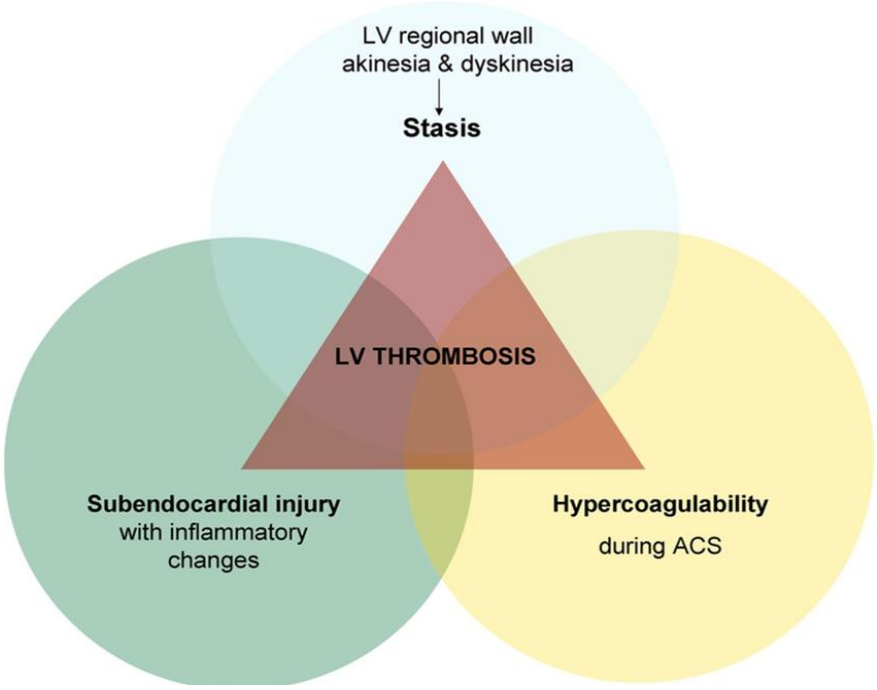


Figure١ The three components of Virchow's triad in the development of LVT **(11)**

2.2.1 Relation between LVT and reduced ventricular motion:

when the blood starts to move slowly in a weak, non-contractile segment, it is considered a risk factor in the development of thrombus in the left ventricle **(22)**. In some studies, it has been shown that reduced ejection fraction is considered a cause for the development of LVT **(23)**. Also, in another paper which shows that patient with reduced ejection fraction have a higher risk for developing thrombi in the left ventricle more than patients with normal ejection fraction at the time of

discharge from the hospital **(24, 25)**. Additionally, another factor which contributes mainly to reduced ventricular motion is increased LV internal diastolic dimension, which in turn results in development of thrombus **(26)**.

2.2.2 Relation between LVT and local myocardial injury:

It is known that injury in cardiac muscle is associated with increased in some biomarkers such as troponin and CK-MB. In a study which focuses on these biomarkers, the results noted increased levels of troponin and CK-MB in case of thrombus formation **(27)**. In another retrospective study, all patients with LVT noted to have apical akinesis although there is no relation between LVT and the principle of location of MI **(23)**.

2.2.3 Relation between LVT and hypercoagulability:

It has been noted that patients who develop LVT after acute MI can display hematological abnormalities which can indicate if there is pro-inflammatory state or coagulation abnormalities **(22)**.

2.2.3.1 In case of pro-inflammatory state:

It has been reported that levels of C-reactive protein (CRP) are higher in patients who develop LVT more than patients who do not have thrombus (48 versus 8.4 mg/L). In this case, CRP levels can be used as a predictor biomarker for LVT which occurs as a complication to STEMI **(28)**.

2.2.3.2 In case of coagulation abnormalities:

In a study which reveals the relation between MI and LVT, it has been noted that mean platelet volume and white blood count (are more higher in patients who develop LVT after MI **(27)**. It has been determined that fibrinogen levels can be considered as predictor biomarker for LVT as a complication to STEMI **(28)**.

3. Risk factors for development of LVT:

A lot of risk factors have been investigated in several research. According to a retrospective study that has been published in 2022, smoking, drug abuse, pregnancy induced hypertension, diabetes with complications, valvular heart disease, connective tissue disorders, coagulopathy, anemia and depression are considered as major risk factors for the development of LVT **(29)**. Additionally, low ejection fraction is one of the most important factors that contribute mainly to the occurrence of LVT **(30)**. According to prospective study that has been published in 2020, cardiac patients who have low ejection fraction can develop left ventricular thrombosis (31).

4. Complications of Left Ventricular Thrombosis:

The main complication which occurs after LVT is the development of embolism. Embolism is a condition when a part from the thrombus in the left ventricle detaches from the main thrombus and travels in the main blood stream until blocking of another blood vessel in another part from the body. It has been determined that embolism complications are reported to occur with 10% of cases with LVT **(32)**. Different researches have determined that left ventricular thrombus which is protruding in the ventricle cavity has a high capability for independent mobility which is associated with embolization more than thrombus without these features **(33)** (**Figure٢**). Several retrospective studies have demonstrated the direct relationship between the morphology of the protruding left ventricular thrombus and the development of embolism due to movement of the thrombus to another location **(32).**

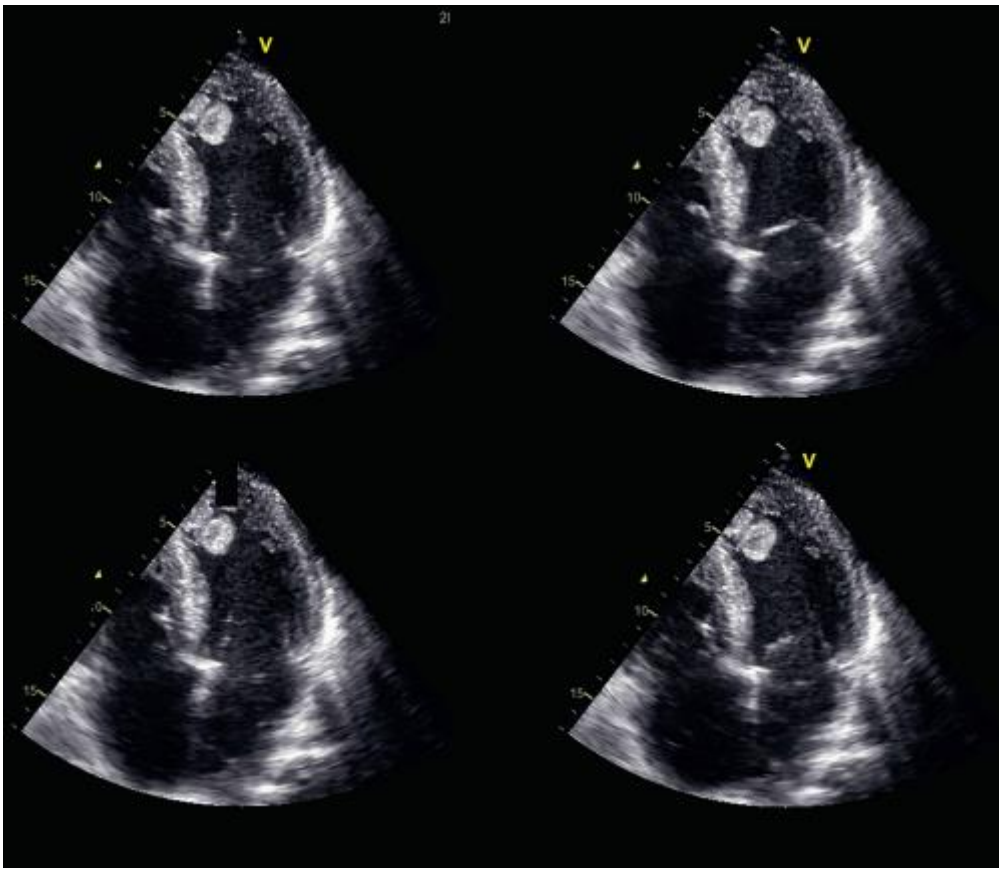


Figure٢ Transthoracic echocardiography appearance of mobile, left ventricular thrombus.
J Vleugels and Rianne H A de Bruin, Department of Cardiology, Academic Medical Center, Amsterdam, the Netherlands (11) .

5. Management of Left Ventricular Thrombosis:

The interventions of the medical therapy to reduce the main LVT after the occurrence of acute MI is less understood. However, several studies have recommended the use of ACE inhibitors and beta-blockers to reduce the incidence of myocardial injury and the mortality rate. But until now, there is no systemic study that has evaluated the effect of these medications on the reduction of LVT **(22)**.

LVT is still considered as a complication of STEMI. However, the main problem associated with LVT is the development of systemic embolization. Although surgical removal of thrombus is one of the interventions present, the main line to prevent embolization associated with LVT is using the antithrombotic therapy **(34)**.

5.1 Heparin:

The results collected from the patients who receieved heparin therapy in the first 2 weeks for the management of LVT were conflicting to some extent. This leads for some systemic reviews to make a belief that heparin is effective in the management of LVT on a short term **(34)**. In a randomized controlled trial that has been published in 1989, the patients who survived from AMI were divided into two groups: the first group received high-dose of heparin (12500 units subcutanously every 12 hours), while the second group received low-dose of heparin (5000 units subcutanously every 12 hours) and the two groups had the heparin therapy for 10-day period, the results had determinded that patients who received high dose heparin had more decrease in the rate of LV thrombus formation **(35)**. In other studies, they have provided that although high dose heparin could decrease the size of the thrombus, it did not prevent the fomation of LV thrombus **(36)**. And most of the researches has detected no embloic events during the treatment with heparin therapy.

5.2 Vitamin K antagonist:

European and United states guidelines have recommended the usage of Vitamin K antagonists such as warfairn for the management of LVT and prevention of embloism even for a long period ranging from 3 to 6 months **(6)**. However, due to the safety profile of warfarin and the risk of bleeding especially at the long term, it is needed to focus on another line of anti-coagulant therapy.

5.3 Non-Vitamin K antagonist oral drugs (NOACs):

The guidelines of cardiology and cardiovascular diseases recommend the usage of anticoagulant therapy in the management of LVT, specifically vitamin K antagonsits such as warfarin is considered the first drug. But because of different reasons, warfarin may be not the best anticoagulant therapy for some patients, mainly because of the safety profile. This allows for many researches to investigate for new anticoagulation therapies. NOACs are considered a suitable alternative to vitamin K antagonists such as dapigatran, rivaroxaban, apixaban, and edoxaban.

Vitamin K antganosists depend in their mechanism of action on inhibiting Vitamin K epoxide reductase, this allows for decreasing the levels of several clotting factors in the coagulation pathway including factor II, VII, IX and X. But because of this mechanism of action, the onset and offset of the action of warfarin is delayed and in some cases, it may reach to several days, a condition which requries rapid-acting parentral warfarin to be used which may result in occurrence of some complications during the medical therpay. On the other hand, NOACs act specifically in which dabigatran inhibits thrombin, while rivaroxaban, apixaban, and edoxaban inhibit factor Xa. This allows for providing a rapid onset of action especially after 1-4 hours following the oral adminsteration with half-life 12 hours. Also NOACs have rapid offset of action (37).

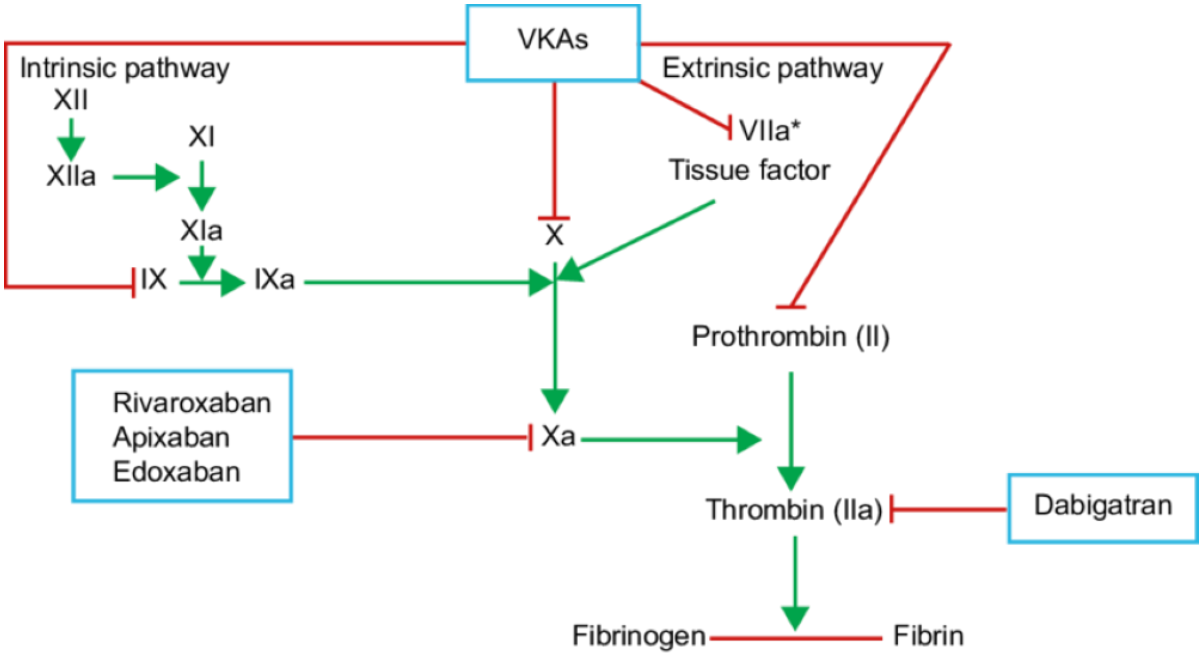


Figure 3 Mechanism of action of Warfarin and NOACs (38)

Warfarin usually exerts its effect within a theraputic range and needs monitoring during usage of this anticoagulant therapy. While NOACs do not need coagulation monitoring during usage. All NOACs are considered as active drugs, except dabigatran is considered a prodrug and hydrolyzed by carboxylesterase to the active form **(38, 39)**. All NOACs share similar characteristics, 2-4 hours are needed to reach to peak plasma levels with half-life is about 8-12 hours. According to the bioavailability, it has a minimal effect on NOACs except rivaroxaban which requires food for complete gastrointestinal absorption. Accoriding to the metabolism, factor Xa inhibitors such as rivaroxaban, apixaban, and edoxaban are metabolized mainly through CYP3A4 enzyme. However, all NOACs are known to be substrates to p-glycoprotein **(40)**. According to the elimination, The NOACs are partially eliminated through the kidney, dabigatran and edoxaban are mainly eliminated through the kidney, while apixaban and rivaroxaban are partially eliminated. This explains the risk of increased drug exposure in case of renal function impairment, especially in case of dabigatran **(41)**.

The approval of NOACs for the treatment of pulmonary embolism (PE) and deep vein thrombosis (DVT) as well as the secondary prevention of VTE represents one of the largest changes in the management of thromboemboism over the past ten years (42). The European Society of Cardiology's (ESC) most recent 2019 guidelines suggest treating all eligible patients with a non-vitamin K antagonist oral anticoagulant (NOAC) rather than a vitamin K antagonist (VKA) (43).

Moreover, the effect of NOACs in cases of LVT is compared to the effect of warfarin in many researches. In an observational study that has been published in 2021, more and earlier resolution of LV thrombus was observed in patients who received NOACs compared to patients who received vitamin K antagonist such as warfarin. Additonally to the theraputic effect of NOACs, the major bleeding events which is considered the most important side effect of anticogaulation therapy was lower with NOACs compared to warfarin therapy with no effects on the thromboembolism rates **(44).** In another retrospective study that has been published in 2020, the results show that rate of occurrence of stroke and bleeding was not highly different between the NOACs therapy and Vitamin K antagonist therapy, even after one year of treatment **(45)**. From several reviews and studies that compares the management of LVT with VKA or NOACs, it has been concluded that the NOACs have comparble efficacy with warfarin and lower side effects than warfarin. However, it requires much more studies to confirm the results.

Conclusions:

Left ventricular thrombosis is not an uncommon problem that can complicate many cardiovascular diseases, particularly when there is LV systolic dysfunction. Prompt diagnosis and early management can minimize its devastating complications. Anticoagulation therapy is the main step of management which is received by patients during hospital stay and after discharge to treat or prevent thromboembolic disease. The effectiveness of NOACs in treating thromboembolism has been demonstrated by substantial clinical data, especially in cases of pulmonary embolism and deep vein thrombosis. However, while it is widely used in thromboembolic patients, the role of NOACs in LVT is not clearly established. Further studies are needed to assess the usefulness of these drugs in these high-risk patients.

References:

1. organization wh. Cardiovascular diseases (CVDs) 2021 [Mar 14, 2023]. Available from: https://www.who.int/news-room/fact-sheets/detail/cardiovascular-diseases-(cvds).

2. McCarthy CP, Vaduganathan M, McCarthy KJ, Januzzi JL, Jr, Bhatt DL, McEvoy JW. Left Ventricular Thrombus After Acute Myocardial Infarction: Screening, Prevention, and Treatment. JAMA Cardiology. 2018;3(7):642-9. doi: 10.1001/jamacardio.2018.1086.

3. Cruz Rodriguez JB, Okajima K, Greenberg BH. Management of left ventricular thrombus: a narrative review. Ann Transl Med. 2021;9(6):520. Epub 2021/04/15. doi: 10.21037/atm-20-7839. PubMed PMID: 33850917; PubMed Central PMCID: PMCPMC8039643.

4. Maniwa N, Fujino M, Nakai M, Nishimura K, Miyamoto Y, Kataoka Y, et al. Anticoagulation combined with antiplatelet therapy in patients with left ventricular thrombus after first acute myocardial infarction. Eur Heart J. 2018;39(3):201-8. Epub 2017/10/14. doi: 10.1093/eurheartj/ehx551. PubMed PMID: 29029233.

5. McCarthy CP, Murphy S, Venkateswaran RV, Singh A, Chang LL, Joice MG, et al. Left Ventricular Thrombus: Contemporary Etiologies, Treatment Strategies, and Outcomes. J Am Coll Cardiol. 2019;73(15):2007-9. Epub 2019/03/09. doi: 10.1016/j.jacc.2019.01.031. PubMed PMID: 30846340.

6. Ibanez B, James S, Agewall S, Antunes MJ, Bucciarelli-Ducci C, Bueno H, et al. 2017 ESC Guidelines for the management of acute myocardial infarction in patients presenting with ST-segment elevation: The Task Force for the management of acute myocardial infarction in patients presenting with ST-segment elevation of the European Society of Cardiology (ESC). Eur Heart J. 2018;39(2):119-77. Epub 2017/09/10. doi: 10.1093/eurheartj/ehx393. PubMed PMID: 28886621.

7. O'Gara PT, Kushner FG, Ascheim DD, Casey DE, Jr., Chung MK, de Lemos JA, et al. 2013 ACCF/AHA guideline for the management of ST-elevation myocardial infarction: executive summary: a report of the American College of Cardiology Foundation/American Heart Association Task Force on Practice Guidelines: developed in collaboration with the American College of Emergency Physicians and Society for Cardiovascular Angiography and Interventions. Catheter Cardiovasc Interv. 2013;82(1):E1-27. Epub 2013/01/10. doi: 10.1002/ccd.24776. PubMed PMID: 23299937.

8. Alkarithi G, Duval C, Shi Y, Macrae FL, Ariëns RAS. Thrombus Structural Composition in Cardiovascular Disease. Arteriosclerosis, Thrombosis, and Vascular Biology. 2021;41(9):2370-83. doi: doi:10.1161/ATVBAHA.120.31575.

9. Roberts WC, Siegel RJ, McManus BM. Idiopathic dilated cardiomyopathy: analysis of 152 necropsy patients. Am J Cardiol. 1987;60(16):1340-55. Epub 1987/12/01. doi: 10.1016/0002-9149(87)90618-7. PubMed PMID: 3687784.

10. Sanchis-Gomar F, Perez-Quilis C, Leischik R, Lucia A. Epidemiology of coronary heart disease and acute coronary syndrome. Ann Transl Med. 2016;4(13):256. Epub 2016/08/09. doi: 10.21037/atm.2016.06.33. PubMed PMID: 27500157; PubMed Central PMCID: PMCPMC4958723.

11. Delewi R, Nijveldt R, Hirsch A, Marcu CB, Robbers L, Hassell ME, et al. Left ventricular thrombus formation after acute myocardial infarction as assessed by cardiovascular magnetic resonance imaging. Eur J Radiol. 2012;81(12):3900-4. Epub 2012/09/22. doi: 10.1016/j.ejrad.2012.06.029. PubMed PMID: 22995173.

12. Solheim S, Seljeflot I, Lunde K, Bjørnerheim R, Aakhus S, Forfang K, et al. Frequency of left ventricular thrombus in patients with anterior wall acute myocardial infarction treated with percutaneous coronary intervention and dual antiplatelet therapy. Am J Cardiol. 2010;106(9):1197-200. Epub 2010/10/30.doi: 10.1016/j.amjcard.2010.06.043. PubMed PMID: 21029812.

13. Stokman PJ, Nandra CS, Asinger RW. Left Ventricular Thrombus. Curr Treat Options Cardiovasc Med. 2001;3(6):515-21. Epub 2001/11/07. doi: 10.1007/s11936-001-0025-6. PubMed PMID: 11696271.

14. Phan J, Nguyen T, French J, Moses D, Schlaphoff G, Lo S, et al. Incidence and predictors of left ventricular thrombus formation following acute ST-segment elevation myocardial infarction: A serial cardiac MRI study. Int J Cardiol Heart Vasc. 2019;24:100395. Epub 2019/07/20. doi: 10.1016/j.ijcha.2019.100395. PubMed PMID: 31321288; PubMed Central PMCID: PMCPMC6612928.

15. Chiarella F, Santoro E, Domenicucci S, Maggioni A, Vecchio C. Predischarge two-dimensional echocardiographic evaluation of left ventricular thrombosis after acute myocardial infarction in the GISSI-3 study. Am J Cardiol. 1998;81(7):822-7. Epub 1998/04/29. doi: 10.1016/s0002-9149(98)00003-4. PubMed PMID: 9555769.

16. Saleh M, Ambrose JA. Understanding myocardial infarction. F1000Res. 2018;7. Epub 2018/09/20. doi: 10.12688/f1000research.15096.1. PubMed PMID: 30228871; PubMed Central PMCID: PMCPMC6124376.

17. Akbar H, Foth C, Kahloon RA, Mountfort S. Acute ST Elevation Myocardial Infarction. StatPearls. Treasure Island (FL): StatPearls Publishing Copyright © 2022, StatPearls Publishing LLC.; 2022.

18. van Dantzig JM, Delemarre BJ, Bot H, Visser CA. Left ventricular thrombus in acute myocardial infarction. European Heart Journal. 1996;17(11):1640-5. doi:10.1093/oxfordjournals.eurheartj.a014746.

19. Vaitkus PT, Barnathan ES. Embolic potential, prevention and management of mural thrombus complicating anterior myocardial infarction: a meta-analysis. J Am Coll Cardiol. 1993;22(4):1004-9. Epub 1993/10/01. doi: 10.1016/0735-1097(93)90409-t. PubMed PMID: 8409034.

20. Delemarre BJ, Visser CA, Bot H, Dunning AJ. Prediction of apical thrombus formation in acute myocardial infarction based on left ventricular spatial flow pattern. J Am Coll Cardiol. 1990;15(2):355-60. Epub 1990/02/01. doi: 10.1016/s0735-1097(10)80062-2. PubMed PMID: 2299076.

21. Keren A, Goldberg S, Gottlieb S, Klein J, Schuger C, Medina A, et al. Natural history of left ventricular thrombi: Their appearance and resolution in the posthospitalization period of acute myocardial infarction. Journal of the American College of Cardiology. 1990;15(4):790-800.doi: https://doi.org/10.1016/0735-1097(90)90275-T.

22. Habash F, Vallurupalli S. Challenges in management of left ventricular thrombus. Ther Adv Cardiovasc Dis. 2017;11(8):203-13. Epub 2017/06/08.doi:10.1177/1753944717711139. PubMed PMID: 28589748; PubMed Central PMCID: PMCPMC5933579.

23. Gianstefani S, Douiri A, Delithanasis I, Rogers T, Sen A, Kalra S, et al. Incidence and predictors of early left ventricular thrombus after ST-elevation myocardial infarction in the contemporary era of primary percutaneous coronary intervention. Am J Cardiol. 2014;113(7):1111-6. Epub 2014/02/04. doi: 10.1016/j.amjcard.2013.12.015. PubMed PMID: 24485697.

24. Shacham Y, Leshem-Rubinow E, Ben Assa E, Rogowski O, Topilsky Y, Roth A, et al. Frequency and correlates of early left ventricular thrombus formation following anterior wall acute myocardial

infarction treated with primary percutaneous coronary intervention. Am J Cardiol. 2013;111(5):667-70. Epub 2012/12/25.doi:10.1016/j.amjcard.2012.11.016. PubMed PMID: 23261006.

25. Shacham Y, Birati EY, Rogovski O, Cogan Y, Keren G, Roth A. Left ventricular thrombus formation and bleeding complications during continuous in-hospital anticoagulation for acute anterior myocardial infarction. Isr Med Assoc J. 2012;14(12):742-6. Epub 2013/02/12. PubMed PMID: 23393712.

26. Nunes MC, Kreuser LJ, Ribeiro AL, Sousa GR, Costa HS, Botoni FA, et al. Prevalence and risk factors of embolic cerebrovascular events associated with Chagas heart disease. Glob Heart. 2015;10(3):151-7. Epub 2015/09/27. doi: 10.1016/j.gheart.2015.07.006. PubMed PMID: 26407510.

27. Acar Z, Ziyrek M, Korkmaz L, Kiris A, Sahin S, Celik S. Mean platelet volume at admission is a determinant of left ventricular thrombus formation after primary percutaneous coronary intervention for first anterior wall myocardial infarction. Acta Cardiol. 2014;69(6):603-9. Epub 2015/02/04. doi: 10.2143/ac.69.6.1000002. PubMed PMID: 25643430.

28. Shacham Y, Leshem-Rubinow E, Ben Assa E, Rogowski O, Topilsky Y, Roth A, et al. Comparison of C-reactive protein and fibrinogen levels in patients having anterior wall ST-Segment elevation myocardial infarction with versus without left ventricular thrombus (from a primary percutaneous coronary intervention cohort). Am J Cardiol. 2013;112(1):57-60. Epub2013/04/09.doi:10.1016/j.amjcard.2013.02.052. PubMed PMID: 23562384.

29. Luthra K, Avula SR, Raju M, Gangu K, Waqar Z, Doddamani R, et al. Risk factors and outcomes associated with Left Ventricular Thrombus in patients with Peripartum Cardiomyopathy: An insight from National Inpatient Sample Database. American Journal of Preventive Cardiology. 2022;9:100313. doi: https://doi.org/10.1016/j.ajpc.2021.100313

30. Okuyan E, Okcun B, Dinçkal MH, Mutlu H. Risk factors for development of left ventricular thrombus after first acute anterior myocardial infarction-association with anticardiolipin antibodies. Thrombosis Journal. 2010;8(1):15. doi: 10.1186/1477-9560-8-15.

31. Aljaber NN, Mattash ZA, Alshoabi SA, Alhazmi FH. The prevalence of left ventricular thrombus among patients with low ejection fraction by trans-thoracic echocardiography: Left ventricular thrombus in low ejection fraction. Pakistan Journal of Medical Sciences. 2020;36(4). doi: 10.12669/pjms.36.4.1972.

32. Meltzer RS, Visser CA, Fuster V. Intracardiac thrombi and systemic

embolization. Ann Intern Med. 1986;104(5):689-98. Epub 1986/05/01. doi:10.7326/0003-4819-104-5-689. PubMed PMID: 3516044.

33. Johannessen KA, Nordrehaug JE, von der Lippe G, Vollset SE. Risk factors for embolisation in patients with left ventricular thrombi and acute myocardial infarction. Br Heart J. 1988;60(2):104-10. Epub1988/08/01.doi:10.1136/hrt.60.2.104. PubMed PMID: 3415869; PubMed Central PMCID: PMCPMC1216530.

34. Delewi R, Zijlstra F, Piek JJ. Left ventricular thrombus formation after acute myocardial infarction. Heart. 2012;98(23):1743-9. doi: 10.1136/heartjnl-2012-301962.

35. Turpie AG, Robinson JG, Doyle DJ, Mulji AS, Mishkel GJ, Sealey BJ, et al. Comparison of high-dose with low-dose subcutaneous heparin to prevent left ventricular mural thrombosis in patients with acute transmural anterior myocardial infarction.N Engl J Med. 1989;320(6):352-7.Epub1989/02/09.doi:10.1056/nejm198902093200604. PubMed PMID: 2643772.

36. Vecchio C, Chiarella F, Lupi G, Bellotti P, Domenicucci S. Left ventricular thrombus in anterior acute myocardial infarction after thrombolysis. A GISSI-2 connected study. Circulation. 1991;84(2):512-9. Epub 1991/08/01. doi: 10.1161/01.cir.84.2.512. PubMed PMID: 1860196.

37. Yeh CH, Hogg K, Weitz JI. Overview of the new oral anticoagulants: opportunities and challenges. Arterioscler Thromb Vasc Biol. 2015;35(5):1056-65. Epub2015/03/21.doi:10.1161/atvbaha.115.303397. PubMed PMID: 25792448.

38. Ingrasciotta Y, Crisafulli S, Pizzimenti V, Marcianò I, Mancuso A, Andò G, et al. Pharmacokinetics of new oral anticoagulants: implications for use in routine care. Expert Opin Drug Metab Toxicol. 2018;14(10):1057-69. Epub 2018/10/03.doi:10.1080/17425255.2018.1530213. PubMed PMID: 30277082.

39. Mekaj YH, Mekaj AY, Duci SB, Miftari EI. New oral anticoagulants: their advantages and disadvantages compared with vitamin K antagonists in the prevention and treatment of patients with thromboembolic events. Ther Clin Risk Manag. 2015;11:967-77. Epub 2015/07/08. doi: 10.2147/TCRM.S84210. PubMed PMID: 26150723; PubMed Central PMCID: PMCPMC4485791.

40.Steffel J, Verhamme P, Potpara TS, Albaladejo P, Antz M, Desteghe L, et al. The 2018 European Heart Rhythm Association Practical Guide on the use of non-vitamin K antagonist oral anticoagulants in patients with atrial fibrillation. Eur Heart J. 2018;39(16):1330-93. Epub 2018/03/22. doi: 10.1093/eurheartj/ehy136. PubMed PMID: 29562325.

41. Turpie AGG, Purdham D, Ciaccia A. Nonvitamin K antagonist oral anticoagulant use in patients with renal impairment. Ther Adv Cardiovasc Dis. 2017;11(9):243-56. Epub 2017/06/28. doi: 10.1177/1753944717714921. PubMed PMID: 28651452; PubMed Central PMCID: PMCPMC5562140.

42. Howard LS. Non-vitamin K antagonist oral anticoagulants for pulmonary embolism: who, where and for how long? Expert Rev Respir Med. 2018;12(5):387-402. Epub 2018/03/16. doi: 10.1080/17476348.2018.1452614. PubMed PMID: 29542359.

43. Konstantinides SV, Meyer G, Becattini C, Bueno H, Geersing GJ, Harjola VP, et al. 2019 ESC Guidelines for the diagnosis and management of acute pulmonary embolism developed in collaboration with the European Respiratory Society (ERS). Eur Heart J. 2020;41(4):543-603. Epub 2019/09/11. doi: 10.1093/eurheartj/ehz405. PubMed PMID: 31504429.

44. Jones DA, Wright P, Alizadeh MA, Fhadil S, Rathod KS, Guttmann O, et al. The use of novel oral anticoagulants compared to vitamin K antagonists (warfarin) in patients with left ventricular thrombus after acute myocardial infarction. Eur Heart J Cardiovasc Pharmacother. 2021;7(5):398-404. Epub 2020/07/31. doi: 10.1093/ehjcvp/pvaa096. PubMed PMID: 32730627.

45. Guddeti R, Anwar M, Walters R, Apala D, Pajjuru V, Kousa O, et al. Treatment of Left Ventricular Thrombus With Direct Oral Anticoagulants: A Retrospective Observational Study. The American Journal of Medicine. 2020;133. doi: 10.1016/j.amjmed.2020.05.025.

خثرة البطين الأيسر: نظرة في الفيزيولوجيا المرضية وعوامل الخطر والتشخيص والمضاعفات والعلاج - مقالة مراجعة

أحمد إبراهيم سيد
قسم الباطنية، كلية الطب، جامعة جازان. المملكة العربية السعودية

ملخص

تخثر البطين الأيسر أحد المضاعفات الخطيرة لأمراض القلب والأوعية الدموية الحادة والمزمنة خاصة عندما يرتبط بضعف الوظيفة الانقباضية للبطين الأيسر. ان تخثر البطين الايسر عامل خطر يؤدي الى انتشار التخثرات في الجهاز الوعائي الدموي والذي يسبب مضاعفات خطيرة على صحة الانسان. الفسيولوجية المرضية لهذا التخثر ناتجة عن عملية معقدة تتضمن ثالوث فيركود: الذي يشمل ركود الدم، إصابة الانسجة و قابلية الدم للتخثر. عملية الكشف عن خثرات القلب تحسنت في الأعوام الأخيرة بسبب التقدم العلمي والتقني في تشخيص التصويري لأمراض القلب. الخطوة الأولى و الأساسية في العلاج لهذا التشخيص هو عن طريق مميعات الدم مثل الهيبارين و الورفاريين، التي تقلل احتمالية انتشار هذي الخثرات في الجسم. الا ان استخدام مميعات الدم الجديدة التي تؤخذ عن طريق الفم لها دور محدود مثبت علميا في مثل هذي الحالات. تستعرض هذه المقالة الخثرة في البطين الايسر مع التركيز على التقدم في العلاجات القائمة على أحدث الأدلة والمبادئ التوجيهية.

الكلمات المفتاحية: أمراض القلب والأوعية الدموية، خثرة البطين الأيسر منع تخثر الدم، مميعات الدم ، منع تخثر الدم الجديد عن طريق الفم،

UNSTEADY SHOCK WAVE DIFFRACTION OVER 180^{O} CURVED SPLITTERS

Ahmed M. Bagabir

Faculty of Engineering, Jazan University, Saudi Arabia

Abstract

The study of shock wave diffraction contributes to a new understanding of many flow phenomena that have applications for high-speed vehicles, noise control, propulsion, and aerodynamics. Computational fluid dynamics have been used to simulate unsteady compressible flows with complex wave interactions. However, flows with adverse pressure gradients such as shock wave diffraction over the curved surface are difficult to simulate due to the separation of the boundary layer and multiple shock interactions. The present paper simulates shock diffraction over 180^{o} curved splitters for shock Mach numbers of M=1.31 and 1.59. The numerical experiments investigate two cases of a confined shock-tube experiment and free-space domain without the interference of shocks reflected from the upper wall. The computational methodology is based on an explicit second-order upwind scheme for the Reynolds average Navier-Stokes equations combined with the *SST* turbulence model. The mesh has been adaptively refined up to fivefold in regions where density gradients exceed 5%, revealing a mesh size of a maximum of half a million cells. To reduce the computation time without reducing the accuracy of the numerical solution, the grid is coarsened so that the density gradient is less than 2% minimum in places where important flow features are faded away. It is found that the primary results fully correspond to the experimental shadowgraph and schlieren images. The present computations have been extended over a long temporal scale. The computational schlieren demonstrates subtle details of flow evolution not previously reported in shock-tube and numerical experiments.

Keywords: Compressible flow, curved surface, Navier-Stokes equations, shock interaction, turbulent, vortex.

1. Introduction

Shock diffraction is a complex process that has been extensively investigated but not yet fully decoded. Computational fluid dynamics is an effective research tool that provides an analysis of the physical phenomena of fluids, especially in cases where the use of practical experiments is not possible or difficult. Moreover, It is difficult to keep track of the rapidly changing unsteady flow to capture all details (Law *et al.*, 2014). The numerical simulation revealed an excellent qualitative and quantitative agreement with the corresponding shock-tube experiments (Bagabir, 2016; 2017; Bagabir and Abutaleb, 2021; Brahmia *et al.*, 2020; Seshadri and Dea, 2020; Toro, 1999).

On the other hand, shock wave diffraction over curved geometries produces a different flow field than the sharp corners (Bagabir and Abutaleb, 2021; Gnani *et al.*, 2014; Law *et al.*, 2014; Quinn, 2013). Flow features depend on the intensity of the incident Mach number and the bending. The 180°bending structure promotes a higher adverse pressure gradient which makes numerical computation more challenging (Law *et al.*, 2014). The shear layer separation is due to the adverse pressure gradient formation on the curved structure, which is not self-similar in time because it contains a length scale (Law *et al.*, 2014). Most of the published papers have been done on the interaction of curved surfaces with shock waves of Mach number less than 2.0. For research examining the effect of shock intensity, the flow fields were compared with Mach numbers 1.31 and 1.59 as well as 1.28 and 1.55 in the experimental studies of Gnani *et al.* (2014) and Queen (2013), respectively. It has been reported that flow with a Mach number above 1.6 will not add any new features (Bazarov *et al*., 1991; Skews, 2005).

As mentioned previously, the experimental results have not revealed precise details of shock and vortex interactions (Quinn, 2013; Law *et al.*, 2014). The current research is conducting numerical experiments for diffracted shock waves over a 180^o curved splitter. The objective of the present paper is to analyze the generated flow field behind weak (M=1.31) and strong (M=1.59) shock waves. The numerical computations also investigate two cases of confined and free domains. The latter allows the formation of vortices without the interference and interaction of the shock reflected from the upper wall.

The next section is dedicated to problem definition. The third section presents the research methodology. The CFD results are presented and analyzed in the fourth section. Finally, the conclusion is drawn.

2. Problem Definition

Shock wave diffractions over splitters occur in engineering applications of high-speed vehicles and airplanes. As shown in Fig. 1, an incident normal shock wave enters from the left side into still air (1atm and 300K) and diffracts over a 180^o curved splitter of diameter, h. The total computational domain length is 44h. The domain height shown in Fig. 1 is 23h and is for the free space case, which is performed without interacting with the upper wall reflected shock. The confined-space case, which is similar to the shock-tube experiments of Gnani *et al.* (2014) and Quinn (2013), represents the evolution of the flow that involves the interaction with the shock reflected from the upper wall. For the confined space, the height of the upper boundary is 4.4h above the splitter which is a quarter of the height of the free-space case. An ideal gas, which has specific a heat ratio of 1.4 and a gas constant of 287J/kgK, is simulated. The properties behind the shock are estimated by Rankine-Hugoniot conditions (Toro, 1999). The effect of supersonic shock wave strength is taken into account by examining a weak shock (M=1.31) and relatively a strong shock (M=1.59) similar to the experiments of Gnani *et al.* (2014). The non-reflecting conditions are set for the outlet and lower boundaries. The upper boundary is either non-reflecting or wall condition for the free and confined computations, respectively.

3. Computational Fluid Dynamics

The computational investigation has been performed using ANSYS FLUENT. The two-dimensional Reynolds average Navier-Stokes equations are employed with *SST* turbulence model. The density-based solver is applied. However, turbulent solution verification is performed using inviscid (Euler) and laminar solvents. The flow domain is discretized using unstructured quadrilateral mesh. The computational domain is initially divided into a cell of $1mm^2$ while the cell is refined to 0.01 mm^2 around the circular surface and vortex region. An adaptive grid technique based on intensity gradients is used. It reveals a cell size of up to 9.75×10^{-4} mm^2. Preliminary simulations are performed to confirm a strong grid independency, although, the accuracy of the results is limited by the available computing facility which is Intel Core i7 with 12.0 GB RAM.

4. Results and Discussion

Schlieren images of the shock wave diffraction evolution over the 180^o curved splitter are presented in Fig. 2. The computational solutions of the inviscid, laminar and turbulent solvers at a Mach number of 1.31 are compared with the experimental results of Quinn (2013). As shown in the upper set of frames of Fig. 2, the laminar and turbulent solvers simulate the separation of the boundary layer developed on the round wall. It has been found that the inviscid solver does not accurately simulate flow. However, similar to the experiment shadowgraphs, the laminar solver develops a small secondary vortex on the upper wall of the splitter close to the end of the curvature due to boundary layer separation, see second-row frames of Fig. 2. This can be attributed to the extra viscosity associated with the laminar solver. Therefore, the 180^o curved structure required the addition of laminar viscosity (Bagabir and Abutaleb, 2021, Toro, 1999). The turbulent solver reproduces the flow features while the laminar solver creates an unstable shear layer (Bagabir and Abutaleb, 2021). It can be concluded that the turbulent solver predicts finer details of the flow field features compared to the shock tube shadowgraphs of Quinn (2013), Fig. 2.

The schlieren images shown in Fig. 3 illustrate the characteristics of the developed flow near the splitter body. The same flow characteristics were reported in the previously published studies (Gnani *et al.*, 2014; Quinn, 2013; Law *et al.*, 2014; Skews, 2005). However, there are additional flow features that are not shown in Fig. 3 and will be introduced later in the discussion because they occurred later or because the existing frames were zoomed in. Figures 3(a) and 3(b) correspond to the real time t=100μs of a shock wave of the M=1.31 case, while Fig. 3(c) shows the results of the M=1.59 case at time t=43μs. The diffractions reveal a complex system of unsteady shock waves associated with the boundary layer separation. It is found that both shock intensities reveal almost similar flow evolution, however, the features of the flow structure become more obvious with the increase of the shock strength, see Fig. 5. shock wave and structure interactions develop three vortex structures within each other due to boundary layer separation. The main vortex (*V*) is caused by the diffraction of the incident shock. The second (*V2*) and third (*V3*) vortices are due to induced flow generated by the main and second vortices, respectively (see Fig. 3). Figure 3 will help explain the complex unsteady flow physics that will be discussed later.

Figures 4 and 5 of the numerical schlieren images of M=1.31 and 1.59, respectively, demonstrate

the onset of vortices formation due to diffraction of shock over the round splitter. In the beginning, the planar incident shock, *IS*, generates diffracted shock, *DS*, which propagates upwards, (see the first row of Figs. 4 and 5). After the diffracted shock passes the curved surface, the boundary layer, *BL*, separates at the location, *SP*. The advanced shear layer, *SL*, grows over time. The shear layer has high local vorticity (Bagabir, 2016), therefore, begins to roll up into a large spiral vortex, *V*, which is very close to the splitter curvature (see also Fig. 3). As shown in Fig.

3, the vortex size of the case M=1.31 is about 50% larger than that of the case M=1.59. It is found that the vortex pulls the fluid toward its center resulting in an induced airflow that moves downward along the radius of curvature. There is an interesting focus event, a secondary shock, *SS*, begins to form at the point of separation due to the expansion of the flow. It is found that this first *SS* should be an oblique shock because the backflow is locally supersonic (Law *et al.*, 2014). The schlieren images exhibit the creation of a lambda-shaped shock, *LS*, consisting of the first two secondary shocks along the downstream edge of the main shear layer, and a shock (*LS tail*) extends downward from the point of intersection of the two adjacent secondary shocks (Gnani *et al.*, 2014; Law *et al.*, 2014; Quinn, 2013), see Figs. 3-5. A similar lambda-shaped shock structure has been also reported for separated flow behind shock waves diffracting over a sharp corner (Bagabir, 2016). As time progresses, a series of secondary shocks develop, *SS*, along the shear layer. However, because the flow field is non-uniform, the intensity of the newly generated secondary shocks gradually decreases and is not strong enough to form a lambda-shaped shock. The secondary shocks of the higher Mach number case (M=1.59) are strong enough to penetrate the shear layer embedded in the primary vortex (see Fig. 3c) causing what is known as embedded shocks, *ES* (Law *et al.*, 2014; Quinn, 2013). The secondary shear layer, *SSL*, is more pronounced in the higher Mach number case (see second-row frames of Fig. 5).

The separation in high-intensity shock occurs at a higher point than in lower-intense shock, which results in the formation of a smaller vortex structure at M=1.59 (Fig. 3). However, as shown in Fig. 6, the separation point is not fixed and is moving as time progresses (Bagabir and Abutaleb, 2021; Law *et al.*, 2014). The separation angle is bounded between two lines passing through the center of the curved splitter, one perpendicular and the other passing through the separation point. For both shock intensities, the initial separation point travels gradually toward the curvature apex. Over time, the strong drift of air along the separator surface leads to the detachment of the developed boundary layer leading to the formation of a second vortex structure (*V2*), see Fig. 3. Its evolution, elements, and structure resemble the main vortex that was previously explained but in an inverted position (see the frames at 80-105μs of Fig. 4 and the frames at 35-45μs of Fig. 5). It believes that the drifting air forces the separation point to retract. For the lower shock intensity, the separation occurs at a position even lower than its initial location, Fig. 6. However, the separation point of both Mach numbers rises again to the second peak angle (see Fig.6). That is due to the creation of the second shear layer, which protects the separation point from the effect of air drift by the main vortex (see last row frames of Figs. 4 and 5). For higher Mach number case, a compression wave, *CW*, which also was reported in the experimental results of Quinn (2013) and Gnani *et al.* (2014), is developed within the lambda-shaped shock, *LS*, and propagates with the flow (see Fig. 5 at t=50μs). Later on, it bifurcates at the main shear layer (see Fig. 5 at t=60μs).

Likewise, just as the second vortex forms after the main vortex, the tiny third vortex (*V3*) forms after the second vortex but in an inverted position (see Fig. 3b). As shown in Fig. 3(b), the third vortex creates only one secondary shock (*SS3*) at the separation point (*SP3*) which of course is not sufficient to form a triangle-shaped lambda shock. It is noteworthy that the formation of the third vortex (*V3*) takes a very short time (about 10μs and 3μs for M=1.31 and 1.59, respectively), which is approximately one-third of the time required for the formation of the second vortex (*V2*). Being so small and occurring in a very short time, the capture of the third vortex was not reported in the previous studies neither in the shock tube nor in numerical experiments. Over time, the main vortex structure is ejected from the splitter body as it interacts and swallows up some of the second vortex structure (see last two frames of Figs. 4 and 5). Moreover, the lambda-shock segments move farther apart

while keeping the oblique secondary shock fixed at the point of separation. As can be seen from Fig. 6, after the separation point rises to the angle of the second peak, it begins to descend again due to the stretching of the shear layer relative to the departure of the main vortex from the surface. There is a similar trend of the separation points in the two cases shown. However, the separation point for the lower shock intensity moves a longer distance than the higher Mach number case, Fig 6.

The late flow field development sequence for diffraction of shock waves of M=1.31 and M=1.59 are shown in the first-row schlieren images of Figs 7 and 8, respectively. It is worth mentioning that the M=1.59 cases have been plotted on a smaller scale to show all the interesting features of the flow. The late progress of the spiral vortex of the free-space case extends without restrictions. However, the multiple interactions excite the flow field further resulting in chaotic flow as time goes on. The main distorted vortex structure can be observed moving away from the splitter, while only the shear layer can be seen from the second vortex (see first row frames of Figs 7 and 8). The secondary and lambda-shaped shocks continue to expand and interact with each other. Shocks are still embedded in the main vortex, and some shock waves are transmitted within the main vortex. The higher Mach number case (M=1.59) emphasizes the developed embedded shocks depicted within the vortex structure.

The schlieren images of Figs 7 and 8 also illustrate a direct comparison of the flow evolution over a splitter for the free and confined spaces. Due to several shock-shock and shock-vortex interactions, the sophisticated flow structure of shock wave diffraction in the confined space (last row of Figs. 7 and 8) is more complex than in the free-space case (top row of Figs 7 and 8). The first frame corresponds to the moment in time when the shock wave reflected, *RS*, from the upper wall first comes into contact with the vortex structure (see the frame of the last row of Figs 7 and 8). The reflected shock propagates through different flow backgrounds, therefore, it is deformed from the normal concave shape to the one shown in the frame of the last row of Figs. 7 and 8. The upstream segment of the reflected shock wave moves faster in a lighter fluid with a higher velocity of sound than in a denser fluid on the downstream side (see the first frame of the last row of Figs. 7 and 8). The central segment of the reflected shock travels through the vortex structure and then disappears inside it as seen in the frames of the last row of Figs. 7 and 8. The second frame of the last row of Figs. 7 and 8 show that the upstream segment of the reflected shock wave hits the top surface of the splitter and reflects towards the top wall, while the downstream segment still moves slowly downwards. In the M=1.59 case, the downstream segment of the reflected shock wave is almost standing still. The reflected shock rotates 90° parallel to the direction of flow in the case of M= 1.31 as indicated by the time (t=240μs) of the third frame of the last row of Fig. 7. In the stronger shock wave case (M=1.59), the reflected shock that is still moving downwards merges with the shocks embedded within the main vortex (see last row frames of Fig. 8). As the flow evolves, the structures of the main and second vortices are subjected to many interactions that affect the shape and direction of motion continuously through the evolution of the flow. The instantaneous locations of the main vortex core of the weak and strong shock wave diffraction on free and confined spaces are demonstrated in Fig. 9. The location trace of the shock wave of M=1.31 is compared with the confined experimental results of Quinn (2013). It shows that the free-vortex structure propagates along a diagonal axis, while the confined-vortex structure is suppressed by the reflected shock. Figure 9 clearly illustrates that the core of the vortex of the M=1.31 case propagates along a diagonal axis forming an angle of 50^o with the horizontal line. While the bath of the core of the vortex of the M=1.59 moves along a diagonal axis 57^o with the horizontal line until time t=145μs and then decreases by four degrees.

5. Conclusions

The employed turbulent solver successfully simulates the flow field behind diffracting shocks around 180^o curved splitters. The adaptively-refined solver even reproduced the finer details of the complex flow. It is found that the diffraction of the shock waves over the 180^o curved splitters produces three vortex structures one inside the other. The development of the three vortices is due to the rolls of the shear layers resulting from the separation of the accelerated flows. Each vortex is in an inverted position of the vortex that precedes it and also rotates in a direction opposite to the direction of the vortex that precedes it. The third vortex was not observed in previous studies because it is very small and its onset time is very short, which is about 3-10μs depending on the incident shock intensity

References

Bagabir A. and Abutaleb A. Numerical experiments and analysis of shock wave diffraction around structures. Yanbu Journal of Engineering and Science 8(1), 48-56 (2021).

Bagabir A. Numerical experiments on shock wave diffraction around ramp splitter using small and large shock tubes. Yanbu Journal of Engineering and Science, 15, 61-72 (2017).

Bagabir A. Comparison of compression and blast waves diffraction over 90° sharp corner. Aljouf University Science and Engineering Journal, 3(2), 10-20 (2016).

Bazarov, S., Gvozdeva, L., Kryukov, B., Lagutov, Y., Landin, A., Zharkov, A. Study of shock wave diffraction in gases at sharp and curved corners. In: Takayama K (ed.) Shock Waves, 18th International Symposium on ShockWaves, pp. 1155–1160. Springer (1991).

Brahmia, N., Hadjadja, A., Sonia, V., Chaudhurib, A. Analysis of shock-wave diffraction over double concave cylindrical wedges. Part I: Shock dynamics. Acta Astronautica, 172, 134-139 (2020).

Gnani, F., Lo, K.H., Zare-Behtash, H., Kontis, K. Experimental investigation on shock wave diffraction over sharp and curved splitters. Acta Astronautica, 99, 143–152 (2014).

Hillier, R. Computation of shock wave diffraction at a ninety degrees convex edge. Shock Waves, 1 (2), 89-98 (1991).

Law, C., Muritala, A. , Skews, B. Unsteady flow with separation behind a shock wave diffracting over curved walls. Shock Waves, 24 (3), 283-294 (2014).

Quinn, M. Shock diffraction phenomena and their measurement, Ph.D. thesis, University of Manchester (2013).

Seshadri, P., and Dea, A. Investigation of shock wave interactions involving stationary and moving wedges. Physics of Fluids, 32 (2020).

Skews, B. Shock wave diffraction on multi-faceted and curved walls. Shock Waves. 14(3), 137–146 (2005).

Sun, M., Takayama, K. A note on numerical simulation of vortical structures in shock diffraction. Shock Waves, 13, 25–32 (2003).

Toro, E. Riemann solvers and numerical methods for fluid dynamics, Springer (1999).

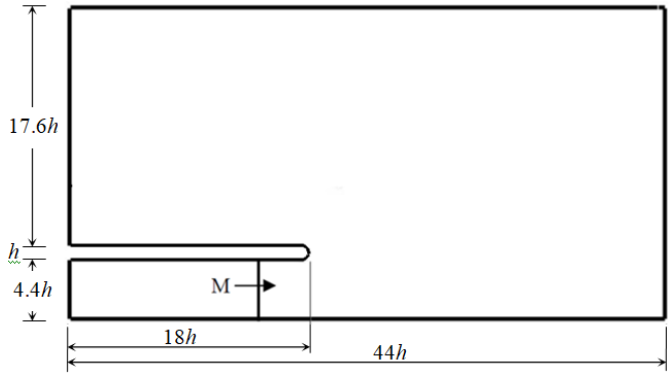


Fig. 1: Geometry for shock wave diffraction around curved splitter.

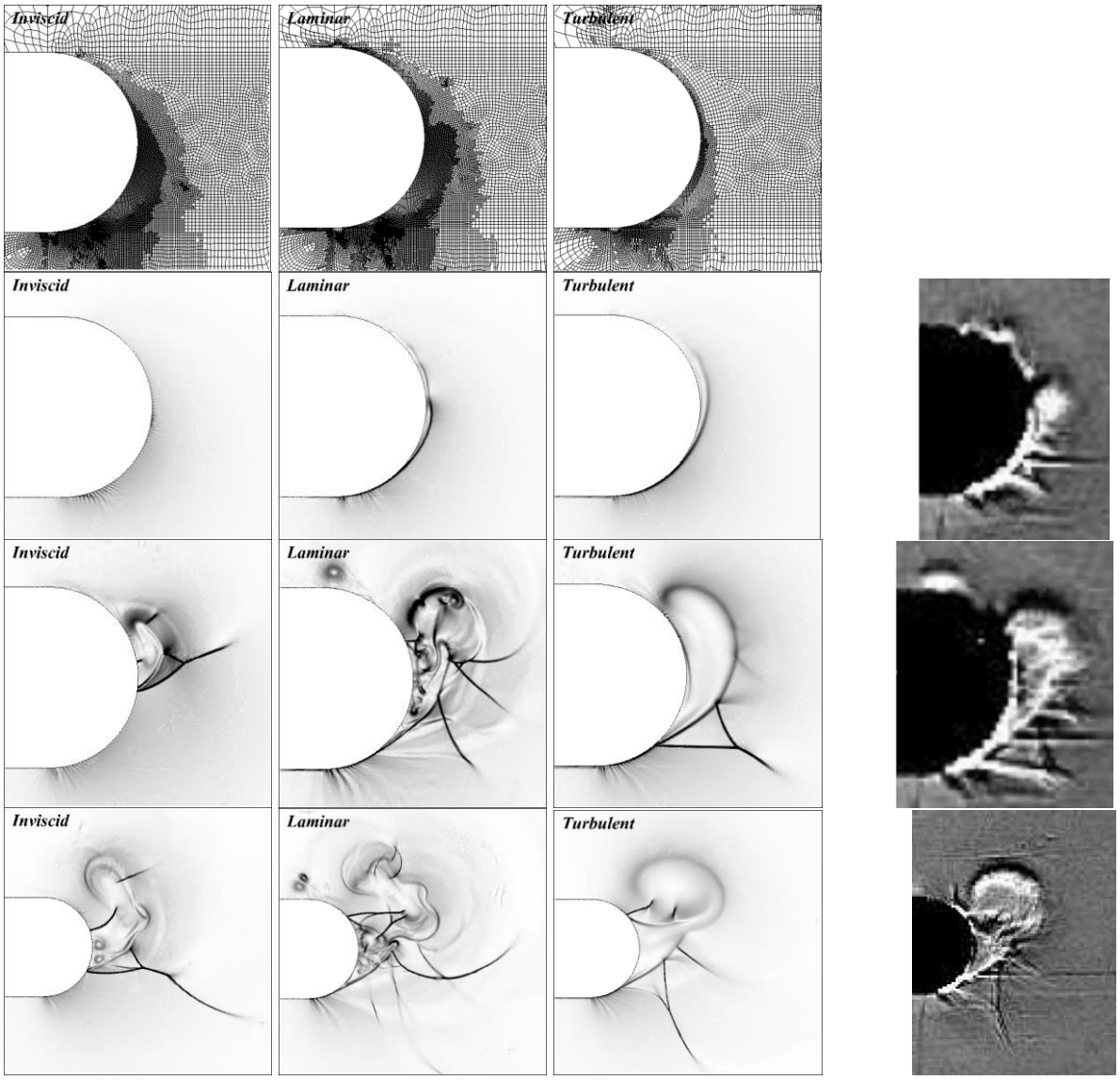
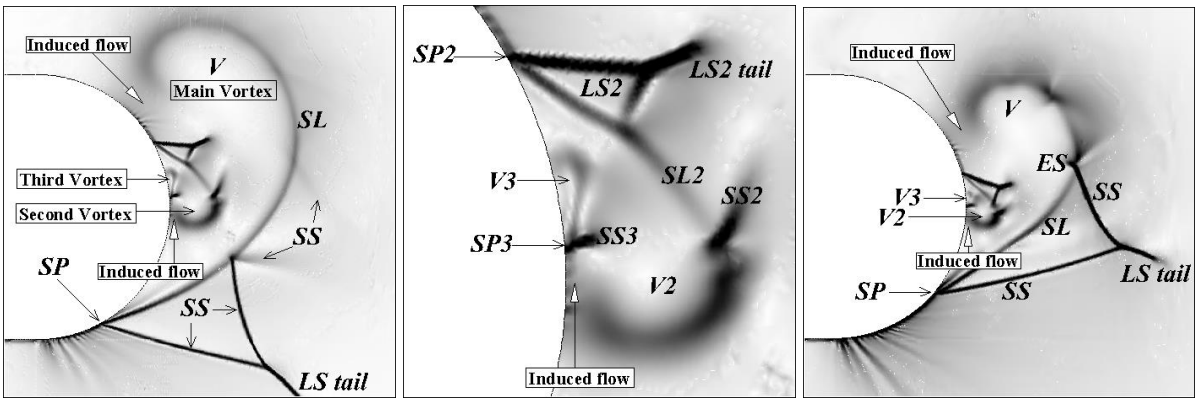


Fig. 2: Numerical schlieren sequence (t=40, 80 and 120μs) of M =1.31 shock wave diffraction for different solvers compared with the experimental shadowgraphs of Quinn (2013). The top row shows mesh around the splitter.



(a) (b) (c)

Fig. 3: Schlieren images show the three developed vortex configurations.
(a) M=1.31 (t=100μs), (b) M=1.31 (t=100μs) magnified, and (c) M=1.59 (t=43μs). *SP*: separation point, *SL*: shear layer, *SS*: secondary shock, *LS*: lambda shocks, *ES*: embedded shock, *V*: vortex.

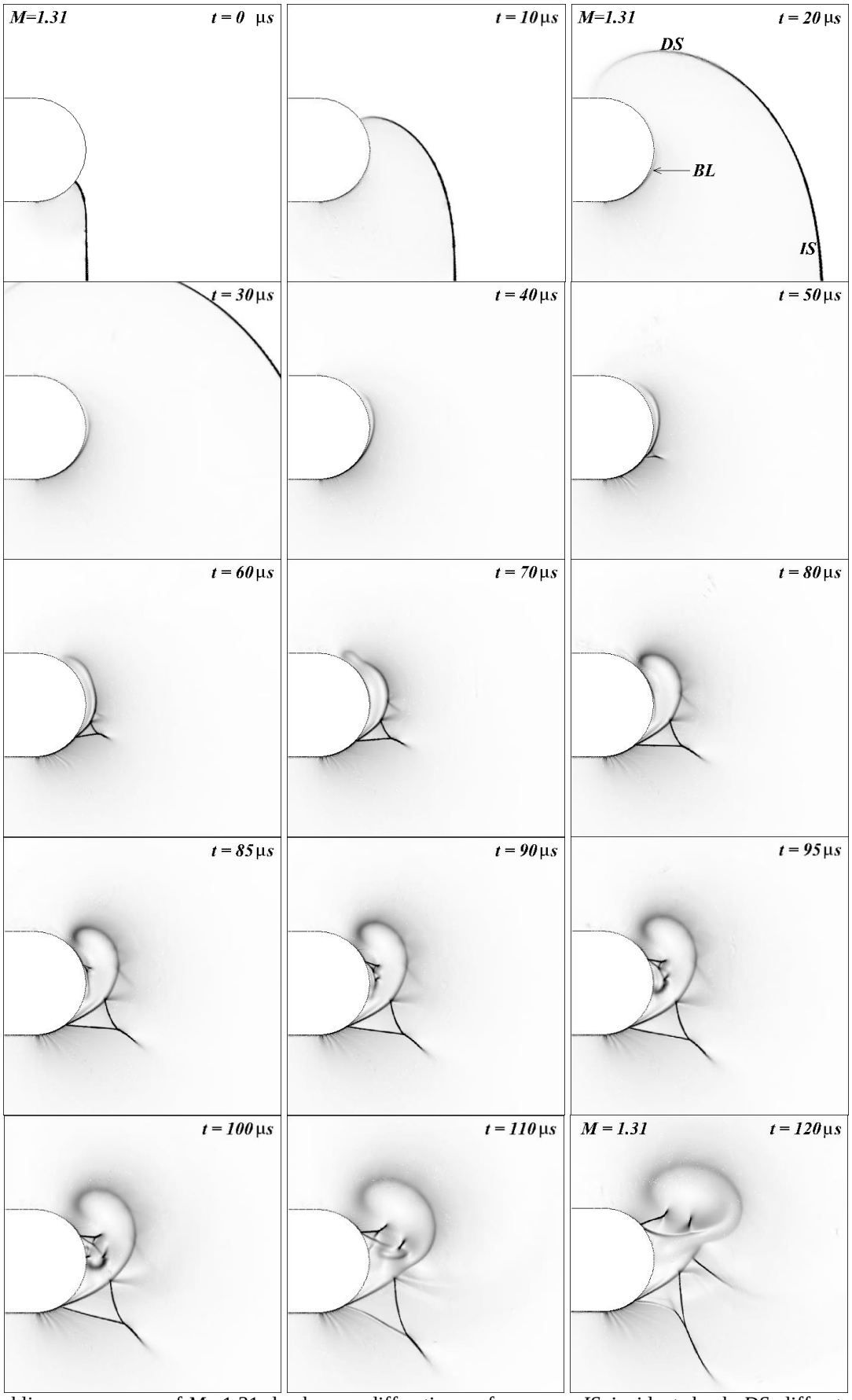


Fig. 4: Schlieren sequences of M =1.31 shock wave diffraction on free space. *IS*: incident shock, *DS*: diffracted shock, *BL*: boundary layer.

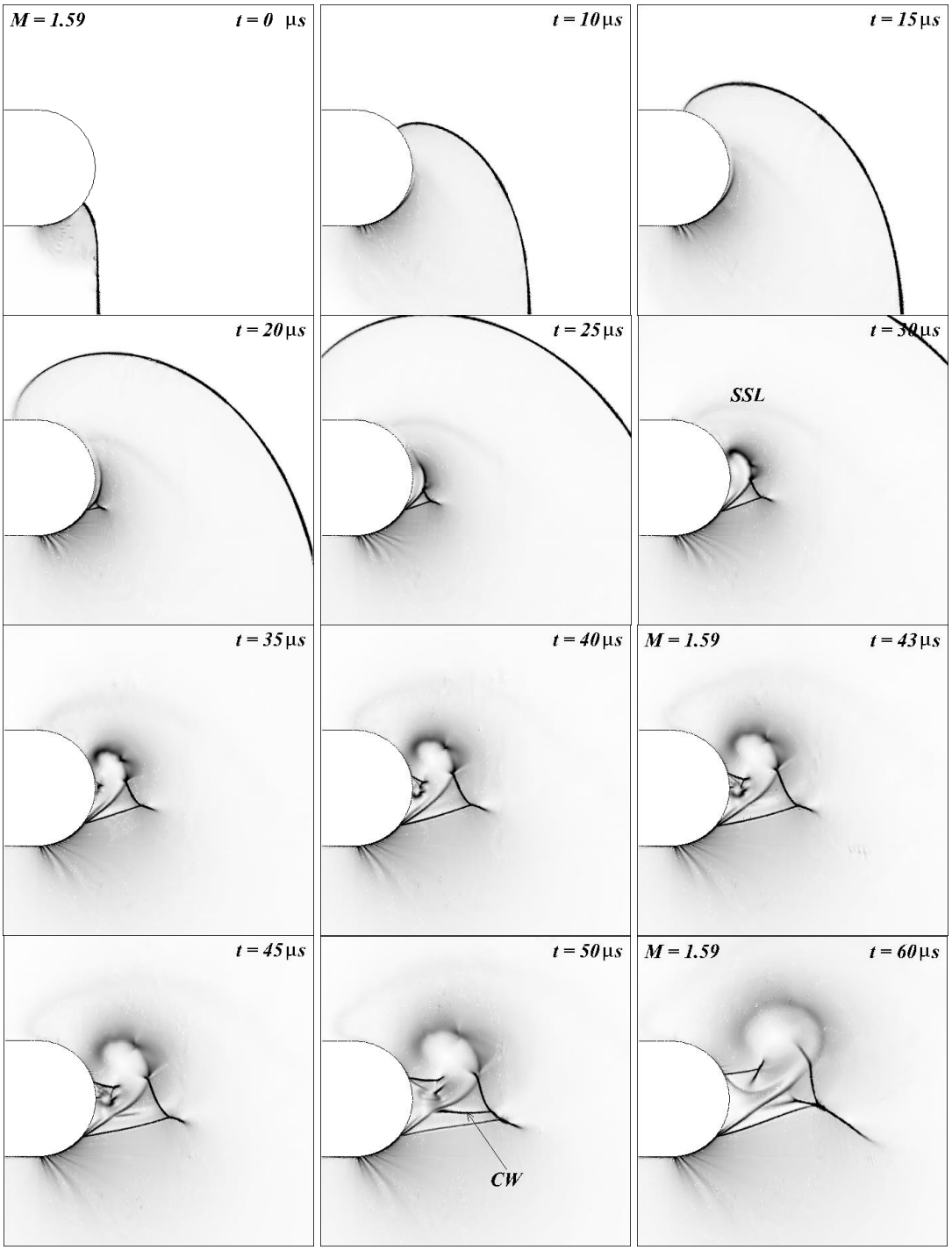


Fig. 5: Schlieren sequences of M =1.59 shock wave diffraction on free space (SSL: secondary shear layer, CW: compression wave).

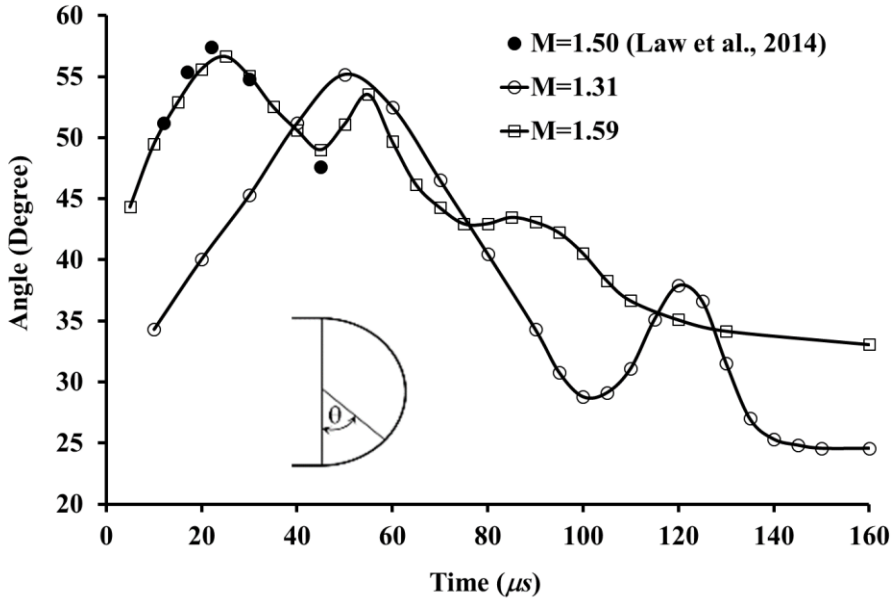


Fig. 6: Location of vortex core of the two shock waves diffraction on free and confined spaces; compared with confined experimental results (Quinn, 2013).

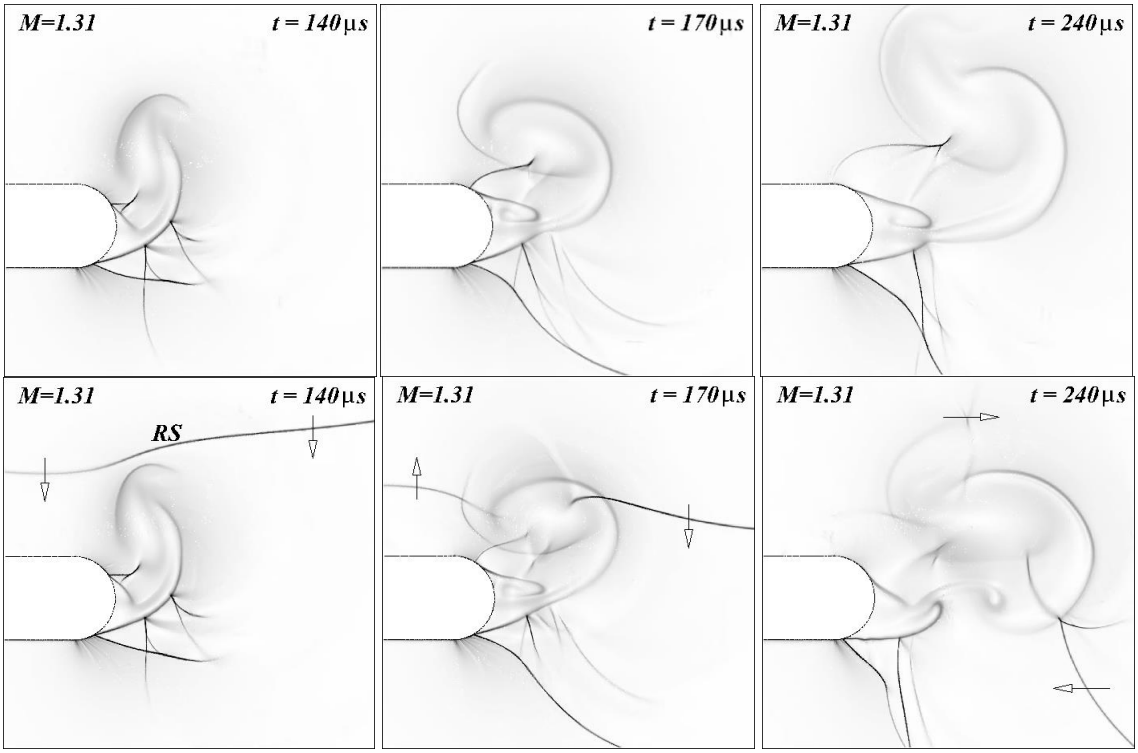


Fig. 7: Comparison of schlieren images of *M* =1.31 shock wave diffraction on free (top) and confined (bottom) spaces. *RS*: reflected shock

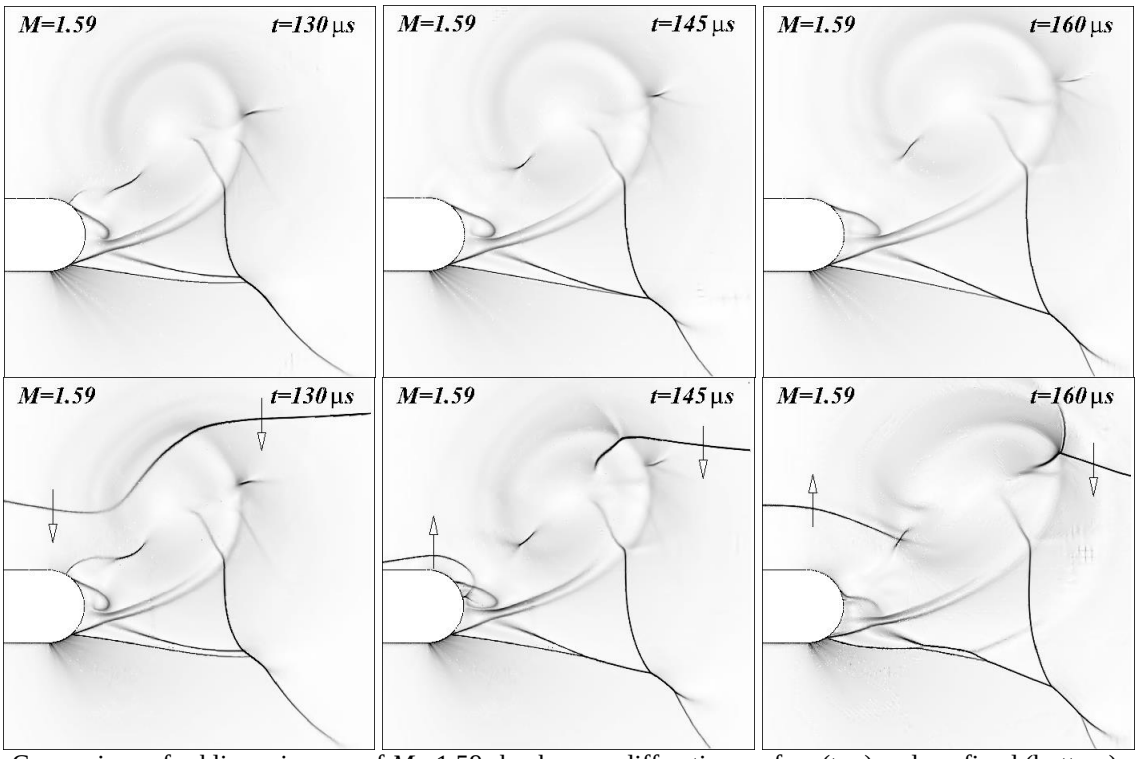


Fig. 8: Comparison of schlieren images of M =1.59 shock wave diffraction on free (top) and confined (bottom) spaces.

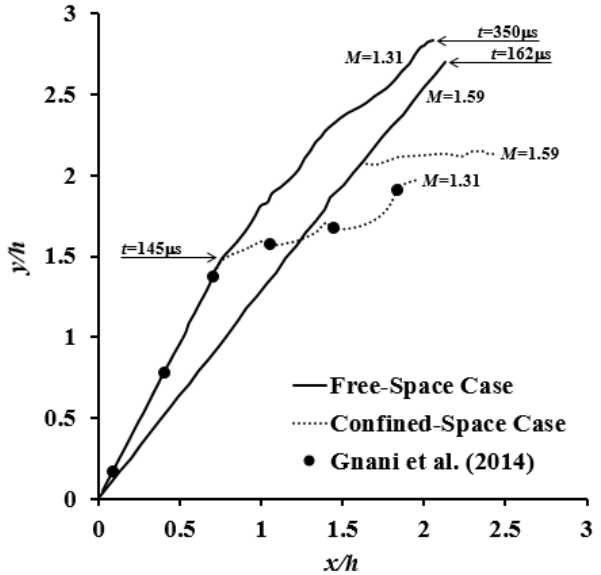


Fig. 9: Location of vortex core of the two shock waves diffraction on free and confined spaces; compared with confined experimental results (Quinn, 2013).

انحراف موجة صدمة غير مستقرة حول فواصل ذات ١٨٠ درجة انحناء

أحمد محمد باجابر

كلية الهندسة – جامعة جازان– المملكة العربية السعودية

الملخص

تساهم دراسة حيود موجة الصدمة في فهم جديد للعديد من ظواهر التدفق التي لها تطبيقات للمركبات عالية السرعة، والتحكم في الضوضاء، والديناميكا الهوائية. تم استخدام قوانين الموائع الحسابية لمحاكاة التدفقات غير المستقرة القابلة للانضغاط مع تفاعلات الموجة المعقدة. التدفقات ذات تدرجات الضغط المعاكس مثل حيود موجة الصدمة على السطح المنحني هي أكثر صعوبة لمحاكاة العددي بسبب فصل الطبقة الحدودية وتفاعلات الصدمات المتعددة. تحاكي الورقة الحالية حيود الصدمات على فواصل منحنية ١٨٠ درجة لأرقام ماخ 1.31 و١,٥٩. تحقق التجارب العددية في حالتين لتجربة أنبوب الصدمة المحصورة ومجال الفضاء الحر بدون تدخل الصدمات المنعكسة من الجدار العلوي. تعتمد المنهجية الحسابية على حلول من الدرجة الثانية لمعادلات نافيير-ستوكس جنبًا إلى جنب مع نموذج اضطراب. تم زيادة دقة شبكة الحل بشكل تكيفي يصل إلى خمسة أضعاف في المناطق التي تتجاوز فيها تدرجات الكثافة ٥٪، مما يكشف عن حجم شبكة بحد أقصى نصف مليون خلية. لقد وجد أن النتائج الأولية تتوافق تمامًا مع الصور المعملي. تم تمديد الحسابات الحالية على نطاق زمني طويل. توضح النتائج تفاصيل دقيقة لتطور التدفق لم يتم الإبلاغ عنها مسبقًا في أنابيب الصدمات والتجارب العددية.

كلمات مفتاحية: تدفق انضغاطي، جسم منحني، معادلات نافيير-ستوكس، موجة الصدمة، مائع اضطراب.

Study of atmospheric pollution of particulate matter in the urban environment in Jazan

Entesar H. EL-Araby and Sabina P. Dhawale

Physics Department, Faculty of Science, Jazan University, Saudi Arabia

Abstract

The concentration of aerosols in the atmosphere has attracted great interest from many researchers in the past decade. Research has shown that aerosols are responsible for harmful chemical reactions that lead to the physical deterioration of stratospheric ozone. Moreover, aerosols increase the risk of cancer in humans when inhaled in significant proportions. This paper seeks to estimate the concentration of all heavy metals in the air of Jazan city, through the application of neutron activation analysis (NAA). The analysis revealed that the maximum concentration of (PM10) and (TSP) aerosols in Jazan city occur during the spring season. The highest concentration of Ba, Br, Th, Zn, and Rb was recorded at the airport while the highest concentration of Ca, Ce, Co, Cr, Eu, La, Sb, and Sc is recorded in the industrial area and the mountain district. In addition, it was concluded that Jazan city aerosol (PM10) and (TSP) were rich in Ca, Br, Zn, and Fe which resulted from human activities. Therefore, attention should be paid to green belts around cities and the rationalization of the use of transportation and construction machinery to reduce the concentration of aerosols and reduce pollution.

Keywords: the total suspended particles TSP and particulate matter PM10 - Enrichment factors (EF) - Heavy metals - Jazan city– the neutron activation analysis NAA.

1- Introduction

Increasing aerosol concentration in the atmosphere has attracted great interest from many researchers in the past decade [Entesar et al., (2011); Entesar et al., (2021)]. It has been found that aerosols pose several environmental hazards because they interact with Earth's radiation either directly or indirectly. For example, aerosols may scatter sunlight, thus interfering with the Earth's energy budget. In addition, it was found that aerosols are responsible for the occurrence of the physical deterioration of the stratospheric ozone layer. Aerosols fall into two main categories, namely total suspended particulate matter (TSP) and particulate matter of 10 µm in diameter (PM10) [Chao et al., (2014)].

Basically, (TSP) refers to all particulate matter in the atmosphere. Elevated (TSP) levels may reduce atmospheric visibility and affect human health by causing irritation of the eyes [Dragana et al., (2004)]. In addition, it has been found that both (TSP) and (PM10) aerosols contain an appreciable amount of non-degradable heavy metals that may cause serious damage to various body organs, especially the nervous system [Kakoli et al., (2006); Celine et al., (2007)]. The elevated level of aerosols is common in an urban environment, especially in developing countries [Salaam et al., (2003)].

(PM10) consists of fine particles measuring less than 10 µm in diameter. As a result, (PM10) particles can easily be inhaled by humans, thus causing health impacts. Some of the main sources of (PM10) aerosols include windblown dust, emissions from paints, and automobile emissions [Entesar et al., (2011); Entesar et al., (2021)]. Anthropogenic emissions are responsible for the elevated concentration of heavy metals in the atmosphere [Le Petit et al., (2002)].

Earth’s crusts consist of varying proportions of heavy metals. There are minerals that are useful to humans such as Zn, Fe, Cu, and Co, but there are many heavy metals that have a very harmful effect on the health of living organisms [Entesar et al., (2011); Entesar et al., (2021); de Oliveira et al., (2018); Giordani et al., (2017)]. The presence of heavy metals in aerosols is a very important warning because of their high impact on the degree of toxicity as they are inhaled directly and cause lung cancer. Also, many heavy metals are deposited in plants [de Oliveira et al., (2018); Giordani et al.,

(2017)]. Several studies in Europe, America, and China have shown high percentages of heavy metals in the samples that were studied [de Oliveira et al., (2018); Giordani et al., (2017); Li et al., (2018); Liu et al., (2013); Harris et al., (2011)]. The danger also lies in the deposition of many harmful minerals in medicinal plants, which doubles the risk of being affected by them [Wu & Xue, (2013)]. Therefore, heavy recyclers in aerosols and medicinal plants must be analyzed and evaluated to maintain public health.

Based on the requirements of the World Health Organization (WHO), the annual atmospheric TSP concentration should be less than 90×10^3 ng/m^3. However, the acceptable range of concentration according to the WHO is (60-90) $\times10^3$ ng/m^3 per year. The challenge is greater in developing countries, and as a result, the WHO accepts a range of 120×10^3-150 $\times10^3$ ng/m^3. On the other hand, the safe concentration of PM10 is taken as 50×10^3 ng/m^3, according to the guidelines of the World Health Organization [WHO, (1997); WHO, (2003)].

This work is dedicated to estimating the concentrations of heavy metals in air samples of the city of Jazan using the neutron activation analysis (NAA) technique due to its good sensitivity and stability.

2- Measurement and Methods

2.1Siting Samples:

We selected for sampling from four different locations in the city of Jazan: the industrial area, the airport, the mountain district, and Cady Mall. However, the industrial area has several workshops for car repair, paint, blacksmithing, carpentry, and upholstery. The airport area is a residential area next to the airport with the constant activity of people and aircraft. The mountainous

Figure 1 shows the four sites and their surroundings.

district is an old Jazan region amid its mountains, the Jazan market, and the gold markets with a high population activity. Cady Mall is a large market next to several restaurants and is located on the sea due to the high activity of vehicles and population movement.

*2.2*The sample preparation

Total particle suspended matter was sampled with TSP using a large volume of General Metal Works, model GMWL-2000. The sampler provided a relatively high flow rate of 67.8 m^3/h using an air blower through Whitman 41 cellulose filters of diameter 10 cm. The particulate matter (PM10), with a diameter of 10 μm, was sampled by a properly positioned filter on top of a wire mesh. Four samples are collected at each site every month. They are mixed well, and a homogeneous sample is taken and analyzed to give an integrated picture of the site. Samples were collected over 10 months [Entesar et al., (2011); Entesar et al., (2021)].

2.2.1 Neutron Activation Analysis (NAA)

(TSP and PM10) samples were collected from study sites and stored in clean aluminum cups. The samples were irradiated using thermal neutron activation analysis to determine the nuclide values in the samples using the Egyptian ETRR-2 reactor providing a relatively high heat flux of 3.31 x 10^{12} N/cm^2 [Sitaram et al., (2007), Entesar et al., (2011)]. After 2 hours of irradiation, the samples were refilled, and the filters were analyzed by metering for four Approximately minutes after refrigeration for a maximum of four days. The second measurement took 90 minutes followed after the samples had cooled for 20 days. Radiant filters are counted using a 2.5 Kev resolution single-crystal HPGe spectrometer for the ^{60}Co 1332.5 Kev line, with an efficiency of about 40% relative to a 3x3' NaI detector for the same line. The gamma spectra were analyzed, and the concentrations of the various detected elements were estimated.

2.2.2 determination of the Enrichment factor (EF)

The enrichment factor is used to determine the origin of the heavy metals in the samples and the degree of impact of the anthropogenic emission. To determine the enrichment factor, the following equation is used:

$$EF = \frac{\left(\frac{X}{E_{ref}}\right) sample}{\left(\frac{X}{E_{ref}}\right) crust}$$

Where X is the concentration of the element, and E_{ref} is the reference element for normalization.

In this paper, the reference element $E_{ref}$was scandium. The element was selected due to its relatively low volatility and the high reliability of its analysis and results [Entesar et al., (2011); Le Petit et al., (2002)]. Since the analysis was performed in relation to the natural abundance of the specimen in the earth's crust, a value of EF close to unity represents a sample whose predominant source is the earth's crust, while that having an EF value greater than 10 is mainly because of anthropogenic sources [Entesar et al., (2011); Entesar et al., (2022); Boubel et al., (1985); Entesar et al., (2021); Gonzalo et al., (2012)].

3- Results and Discussion

3.1 Aerosols particulate matter (PM10 & TSP)

Jazan city is one of the regions with varied climatic conditions throughout the year, which affect the level of aerosol concentration in the air. Table 1 summarizes the average concentration of (PM10 and TSP) in Jazan city during ten months with the values of wind, relative humidity, temperature, and atmospheric pressure. The results showed that the average concentrations of TSP ranged from 313.41×10^3 to 733.38×10^3 ng/m^3, while the average concentrations of PM10 ranged between 205.53×10^3 and 261.57×10^3 ng/m^3 in all samples of Jazan city. Figure 2a&b show that the PM10 aerosol concentration ranged from 163.83×10^3 to 320.07×10^3 ng/m^3 in the airport area with an average value of 228.61×10^3 ng/m^3, while the values in Cady Mall ranged from 134.38 to 296.32×10^3 ng/m^3 with an average value of 235.13×10^3 ng/m^3. TSP concentrations ranged from 315.95×10^3 to 800.24×10^3 ng/m^3 in the mountain district, while the change of values in the industrial zone was from 310.88×10^3 to 707.01×10^3 ng/m^3. It was found that the average concentration of TSP in the mountain district and industrial zone is 447.02×10^3 ng/m^3 and 368.55×10^3 ng/m^3 respectively. The results reveal a significant level of variance in the PM10 and TSP samples. This can be

attributed to the diverse influences of climatic conditions within the studied regions. The TSP values in Jazan city were mostly higher than the values set by the World Health Organization [WHO, (2004)], which reported a concentration of 90×10^3 ng/m^3 per year. The Environmental Affairs Agency [EEAA, (2008)] reported that TSP concentration values in the air should not exceed 137×10^3 ng/m^3.

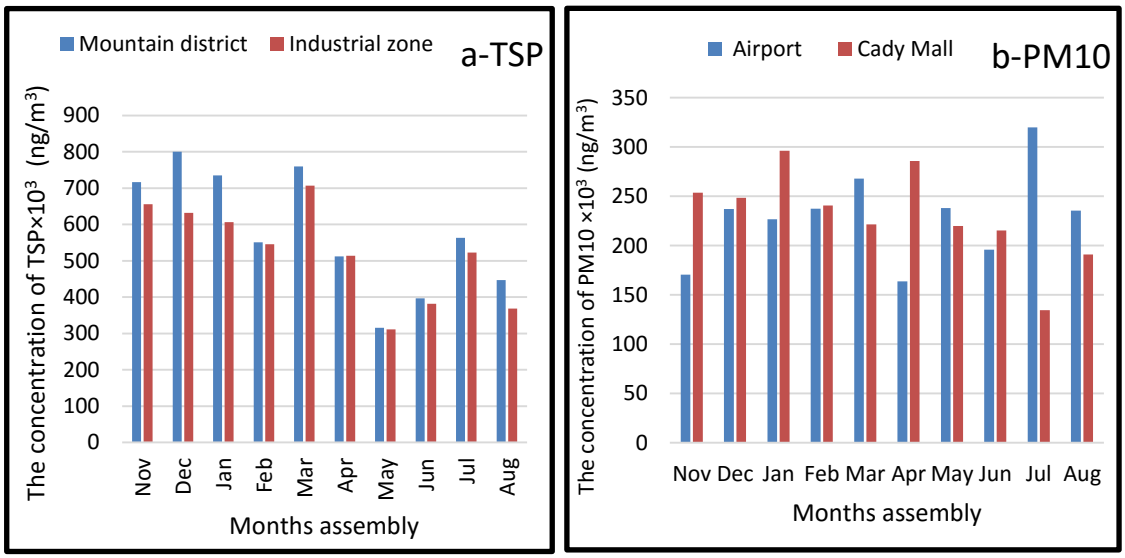


Figure (2): PM10 and TSP aerosols particulate matter (ng/m^3)

Table(2): Average of different parameters and aerosol particulate matter (ng/m^3) of PM10 and TSP over 10 months.

Months Assembly	Pressure (mbar)	T (ºC)	RH (%)	Wind Speed (m/S)	PM10 (ngm^{-3}×10^3)	TSP (ngm^{-3}×10^3)
Nov	1010.00	29.20	67	4	212.08	686.23
Dec	1011.20	28.00	70	5	242.82	715.99
Jan	1012.90	٢٣.50	69	5	261.57	670.58
Feb	1010.40	٢٥.50	71	5	239.06	548.39
Mar	1010.30	٢٧.90	66	5	244.78	733.38
Apr	1006.90	٢٩.90	63	5	224.88	512.80
May	1004.40	٣٣.40	64	5	228.90	313.41
Jun	1002.10	33.80	63	6	205.53	389.01
Jul	1001.60	35.60	65	7	227.22	542.89
Aug	1001.60	33.90	64	6	213.80	407.80
Average	1007.14	30.74	66.2	5.3	230.06	552.05

The measured values were also higher than those measured by [Heal et al., (2005)], which were 120×10^3-150×10^3 ng/m^3. Also, the measured PM10 values were above the annual limit allowed by EEAA, which is 70×10^3 ng/m^3. Also, the maximum daily value of particulate matter (PM10) accepted in many countries [Kaisa Salminen et al., (2003): Gobbi et al., (2007)] is 50 µg/m^3. The results also showed that the spring season (March) showed maximum concentration levels. Again, this can be attributed to the presence of sandstorms during the spring. Similarly, the higher concentrations seen between November and January may be the result of increased local pollution. Other factors that may have contributed to the increased concentrations include increased traffic density during the fall, fuel burning, construction activities, and demolition of structures. These factors contribute directly to the raising of dust into the atmosphere and the release of emissions.

3.2 Concentrations of Heavy Elements.

Table 3 summarizes the heavy metal concentration values in the airport

district and Cady Mall in PM10 samples. Table 4 also displays the heavy metal concentration values in the mountain district and the industrial area for the TSP samples.

3.2.1 Elements of High Concentrations (Ba, Ca, Fe, and Zn):

By adopting the level of the concentration of elements in the atmosphere as a criterion for the order, it was found that the elements Ba, Ca, Fe, and Zn are the most prevalent elements in the study area. It was found that the average concentration of Ba was 12558.58± 5240.62, 18612.07± 2997.26, and 27087.13± 678.24 ng/m^3 in the regions of the Mountain district and Industrial zone in TSP and Airport in PM10, respectively. The Cady Mall area has not recorded the presence of Ba, because it is a market and restaurant area, and there are no painting activities or car paints, which are the main source of Ba [Entesar et al., (2021); Entesar et al., (2011)]. Table 5 shows the comparison between the values of the elements measured in the current work and the values measured in Egypt and Jordan, which are countries on the Red Sea and have similar conditions. The average value of Ba 18612.07±2997.21 ng/m^3 corresponds to the value measured in Egypt in 2011, which recorded a value of Br (11410±450 ng/m^3), but it is less than the value measured in Jordan in 2013, which was (470×10^6 ng/Kg) [Entesar et al., (2011); Hussain et al., (2013)].

The results showed that the highest concentrations of Ca were in the mountain district and the industrial area with a value of 66998.36± 32095.11, and 61580.60± 41376.71 ng/m^3, respectively. The increase in the concentration of Ca is due to the presence of demolition and renovation works, and dirt roads contribute to an increase in the concentration of Ca in the air. Traces of calcium may also be caused by paint pigments or emissions from oil-fired power plants [Entesar et al., (2021); Finlayson-pitts et al., (1997)].

The results showed that with Fe metal concentration ranged between ٧٠٠٣.85±1867.26 and 27798.71±11375.11 ng/m^3 in the Airport and Cady Mall, respectively, with an average value of 17084.13±8497.44 ng/m^3. The main sources of increased Fe concentration in samples can be dust from construction plants, soil particles, and oil-fired power plants [Entesar et al., (2011); Liu et al., (2013)]. Table 5 shows that there is a correlation between the value of Fe in

the aerosol measured in Jizan and its value measured in Egypt, while it is less than the value measured in Jordan.

The highest concentration of Zn was recorded in the Airport area with a value of 41069.65±14408.41 ng/m^3 and the lowest concentration was recorded in the Industrial area with a value of 12955.05±5587.78 ng/m^3. The increase in Zn in Jazan city can be attributed to tire wear, brake pad wear, and exhaust emissions [Entesar et al., (2011); Kennedy &Gadd (2003)]. Table 5 shows that the value of iron in the aerosols in Jazan is lower than the values measured in both Egypt and Jordan.

3.2.2 Elements of Low Concentrations

The results showed that the elements found to be the least common based on the concentrations are Br, Cr, and Rb.

It was found that the concentration of Br in the samples ranged between 97.53±38.71 ng/m^3 in the TSP samples in the industrial area and 663.21±240.48 ng/m^3 in the PM10 samples from the airport area. The effects of Br in the samples can be attributed to automobile emissions. In fact, the contribution of cars to bromine emissions cannot be greater than five percent [Gonzalo et al., (2012)].

Table 3: the concentration of heavy elements (ng/m^3) for PM10 Samples

Elements	The concentration of element (ng/m^3) for PM10 in Airport						The concentration of element (ng/m^3) for PM10 in Cady Mall					
	Average	SD	Min	Median	Max	EF	Average	SD	Min	Median	Max	EF
Ba	27087.13	6782.24	18185.13	20191.14	41956.83	425.26	---	---	---	---	---	---
Br	663.21	240.48	357.41	633.82	937.89	236.50	328.58	196.78	134.42	389.56	576.67	7.24
Ca	46770.98	10961.03	2718.67	68521.96	92352.96	87915.37	26058.82	10485.88	16574.23	19978.34	40236.51	68720.50
Ce	32.68	14.24	19.53	22.36	49.61	1.34	22.355	6.75	15.89	18.02	30.72	1.28
Co	6.89	3.08	3.29	5.64	10.36	1.93	7.93	3.49	4.09	5.93	11.49	3.12
Cr	70.40	19.04	48.34	62.61	92.2	2.93	61.14	28.54	31.22	64.86	98.65	3.57
Eu	0.76	0.23	0.52	0.61	1.01	1.88	0.64	0.26	0.41	0.5	1.01	2.24
Fe	7003.85	1867.26	5101.59	7760.67	9251.77	0.68	27798.71	11375.11	17956.71	19598.87	42356.91	3.79
Hf	10.93	4.32	6.86	10.98	16.89	5.35	7.31	2.86	3.89	6.01	9.78	5.02
La	16.31	4.93	10.98	14.93	21.86	1.45	10.135	3.88	7.01	9.78	15.69	1.27
Rb	90.36	47.41	37.63	67.72	145.53	4.42	18.29	3.61	15.87	17.89	23.51	1.26
Sb	18.21	2.98	15.95	17.97	22.49	26.73	1.64	0.50	0.98	1.52	2.09	3.38
Sc	3.33	1.61	1.92	4.02	5.27	1.00	2.37	0.95	1.49	2.02	3.72	1.00
Th	6.69	3.82	11.63	5.88	2.38	2.05	3.59	1.47	1.65	3.61	5.21	1.55
Zn	41069.65	14408.41	21946.16	32955.94	61991.88	985.77	22704.82	7385.29	15463.86	17869.51	31472.21	764.57

Table 4: the concentration of heavy elements (ng/m^3) for TSP Samples												
Elements	The concentration of element (ng/m^3) for TSP in an industrial zone						The concentration of element (ng/m^3) for TSP in mountain					
	Average	SD	Min	Median	Max	EF	Average	SD	Min	Median	Max	EF
Ba	18612.07	2997.21	14872.45	17891.14	21959.73	171.05	12558.45	5240.62	6873.56	9873.89	18723.56	98.66
Br	97.525	38.71	68.36	87.79	154.34	20.36	182.52	56.55	144.42	161.35	266.64	32.57
Ca	61580.6	41376.71	2819.69	62528.76	92852.97	67760.34	66998.36	32095.11	25573.67	59872.69	99786.43	63015.76
Ce	37.295	17.20	17.53	28.36	53.32	0.89	43.655	23.10	18.76	30.98	70.01	0.89
Co	9.77	3.37	6.29	9.64	14.36	1.60	12.055	4.03	6.98	10.88	16.21	1.69
Cr	80.725	35.42	41.34	62.61	120.23	1.97	91.85	37.50	65.76	81.1	147.31	1.91
Eu	1.325	0.49	0.92	1.02	2.01	1.94	1.355	0.62	0.82	0.99	2.2	1.69
Fe	16721.15	5485.02	9786.51	14967.71	21887.18	0.95	16812.82	5769.27	10221.43	13898.76	22735.7	0.82
Hf	14.225	5.27	7.86	11.98	19.17	4.08	12.715	6.16	5.26	10.98	19.86	3.11
La	21.565	7.12	13.98	17.93	30.21	1.13	22.665	8.78	12.78	17.87	31.23	1.01
Rb	108.31	37.15	70.73	89.82	156.53	3.10	120.96	61.06	49.89	103.78	196.28	2.96
Sb	9.095	4.03	6.14	8.79	14.89	7.82	10.225	3.85	6.87	9.23	15.78	7.51
Sc	5.68	2.56	3.01	4.02	8.27	1.00	6.645	3.10	2.87	5.69	10.11	1.00
Th	3.645	1.54	1.63	3.88	5.38	0.65	4.715	2.44	1.65	3.99	7.21	0.72
Zn	12955.05	5587.78	7320.98	9789.45	19922.86	182.03	18977.7	2936.89	15321.78	18243.67	22253.31	227.93

Table 5: Comparison between heavy metal concentrations (ng/m^3)in the current study and similar studies in other countries.

Elements	The present study In jazan (KSA)	Entesar et al., 2011 In Egypt	Hussain et al., 2013 In Jordan
Ba	18612.07±2997.21	11410±450	470×10^6
Ca	61580.6±41376.71	--	--
Fe	16721.15 ±5485.02	22230±1800	574×10^6
Zn	12955.05±5587.78	146930±6200	181×10^6
Br	97.53± 38.71	180± 40	--
Cr	80.73± 35.42	500± 40	248×10^6
Rb	108.31± 37.15	150± 30	--
Ce	37.39± 17.20	93.18±10	--
Eu	1.33± 0.4	7.80±2	--
La	21.57± 7.12	67.43±2	--
Sc	5.68± 2.56	14.83±1	--
Th	3.65± 1.54	32.22±2	--
Hf	14.22± 5.27	57.08±3	--
Sb	9.09± 4.03	--	--
Co	9.77± 3.37	12.35±4	5.8×10^6

The results recorded the highest concentration of Cr in TSP samples from the Mountain district with a value of 91.85±37.50 ng/m^3. The concentration may be harmful based on the results of the Environmental Protection Agency EPA, which showed that continuous inhalation of about 0.8 ng/m^3 of Cr increases the risk of infection Cancer at a rate of 1.0 x 10^{-6} percent [EPA, (2010); EPA, (2019); Giordani et al., (2017)]. Finally, it was found that the highest concentration of Rb in the Mountain district was 120.96±61.06 ng/m^3. The concentration values of (Br, Cr, and Rb) were lower than the values measured in other countries as Table 5.

3.2.3 The

3.2.4 trace elements and Rare earth

The ground elements mainly include Ce, Eu, and La, while the trace elements include Sc, Th, Hf, Sb, and Co. The maximum concentration of Sc and Co was observed in the mountain district samples, while higher concentrations of Th and Sb were found in the airport area. The maximum concentration of Hf was observed in the industrial zone samples, while the highest concentration of La, Ce, and Eu was observed in the mountain district samples. When comparing the values of rare earth elements and trace elements that were recorded in the present work with other countries. It was found that the values of the elements in the aerosols of Jazan city are lower than those recorded in Egypt in 2011. While Jordan did not record any of them except (Cr and Co), which were higher than those measured in Jazan city. This indicates that the aerosols of Jazan city have acceptable levels in all values of rare earth and trace elements, except for cobalt. Cobalt is higher than the internationally permitted value recommended by the Environmental Protection Agency (EPA), which specified a value not exceeding 5 ng/m³ [EPA, 2010; EPA, 2019].

The EF enrichment factors for the different elements are summarized in Tables 3 and 4. The results showed that the elements Co, Hf, Cr, and Rb showed the least enrichment factors, most of which were less than 20. The results also showed that the enrichment factor values for the predominant elements such as Ce, Eu, La, Th, and Fe were close to unity, which means that the possible sources were related to human activities such as Road dust and soil dust.

4. Conclusions:

PM10 and TSP samples were collected from Jazan city and analyzed using neutron activation analysis. The results showed that the aerosols of Jazan city contain fifteen elements of heavy metals. The heavy metal concentration values were dependent on the difference in climate from one month to another, as well as on the difference in environmental activities practiced in the region. It is clear from the results that the spring season increases the aerosols of particles in the atmosphere in Jazan city. A high concentration of Fe, Zn, Ba, and Ca was detected in the different samples of PM10 and TSP aerosols because of the presence of haze pollution in the area, which is mostly due to the sandstorms that blow in the area. The radionuclides and trace elements concentrations were lower than the values measured in other countries. The value of Co concentration was higher than the internationally permitted limit, according to the report of the Environmental Protection Agency (EPA). we recommend creating green belts around of Jazan city and reducing construction and demolition operations. Rationalizing the use of transport machines that increase the concentration of spray in the air. It is suggested to conduct a comprehensive assessment before implementing any industrial project to ensure its pollution level as well as its compatibility with a sustainable environment framework.

References:

Boubel, R. W., Fox, D. L., Turner, D. B., Stern. A. C. (1985) “Fundamentals of Air Pollution. Academic Press Inc., San Diego”, Science of the Total Environment. **44**, 303.

Celine, S.L.Lee, Xiang-Dong, Li, Gan, Zhang, Jun, Li, Ai-Jun, Ding, Tao,

Wang. (2007), "Heavy metals and Pb isotopic composition of aerosols in urban and suburban areas of Hong Kong and Guangzhou, South China-Evidence of the long-range transport of air contaminants", Atmospheric Environment. **41**, 432–447.

Chao, J.H., Liu, C.C., Cho, I.C., Niu, H. (2014) "Monitoring of 7Be in surface air of varying PM10 concentrations", Applied Radiation and Isotopes. **89**, 95–101.

de Oliveira, L. M., Das, S., da Silva, E. B., Gao, P., Gress, J., Liu, Y., & Ma, L. Q. (2018) "Metal concentrations in traditional and herbal teas and their potential risks to human health", Science of the Total Environment, **633**, 649–657.

Dragana, Dordevic, Zorka, Vukmirovic, Ivana, Tosic, Miroslava, Unkasevic, (2004), "Continuation of dust transport and resuspension to particulate matter levels in the Mediterranean atmosphere" Atmospheric Environment. **38**, 3637–3645.

Entesar H. E., Doaa H. Shabaan, (2022) "Investigation of the radioactive rates of radon gas and its progeny in new buildings", Journal of Radioanalytical and Nuclear Chemistry, **331**, 2779–2784.

Entesar H. E., Doaa S. H. and Zainab Y., (2021) "Evaluation of radioactive exposure in soil", International Journal of Radiation Research, **19,** 719-727.

Entesar H. E., Abd El-wahab M. M., EL-Desouky T. M., Diab H. M., Mohseen M. M. (2011) " Assessment of atmospheric heavy metal deposition in Egypt by Using Neutron Activation Analysis " Applied Radiation and Isotopes **69**, 1506–1511.

Entesar H. E., Khaled A. S., Fawzia M., (2021) "Human Risk Due to Radon and Heavy Metals in Soil", Iran J Public Health, **50**, 1624-1634.

Environmental Affairs. Agency EEAA, (2008) reports on environmental profile of Egyption Governorates, in Arbic. Available online at https://www.eeaa.gov.eg/portals/0/eeaaReports/SoE2009en/Egypt%20State%20of%20Environment%20Report.pdf

EPA. (2010) "Integrated Risk Information System (IRIS)", United States Environmental Protection Agency. https://cfpub.epa.gov/ncea/iris.

Finlayson-Pitts, B.J., Pitts Jr., J.N. (1997) "The chemical basis of air quality. Kinetics and mechanisms of photochemical air pollution and application to control strategies", Adv Environ Sci Technol. **7**, 76–162.

Giordani, P., Minganti, V., Brignole, D., Malaspina, P., Cornara, L., & Drava, G. (2017)"Is there a risk of trace element contamination in herbal preparations? A test study on the lichen Cetraria islandica" Chemosphere, **181**, 778–785.

Gobbi G. P., Barnaba F., Ammannato L., (2007) " Estimating the impact of Saharan dust on the year 2001 PM10 record of Rome, Italy". Atmospheric Environment, 41, 261-275.

Gonzalo, Bermudez, M.A., Raquel Jasan, Rita Pla, Maria L. Pignata. (2012) "Heavy metals and trace elements in atmospheric fall-out: Their relationship with topsoil and wheat element composition", Journal of Hazardous Materials. **213**, 447– 456.

Harris, E. S., Cao, S., Littlefield, B. A., Craycroft, J. A., Scholten, R., Kaptchuk, T., Isenbergg, D. M. (2011) "Heavy metal and pesticide content in commonly prescribed individual raw Chinese herbal medicines" Science of the Total Environment, **409**(20), 4297–4305.

Heal M. R., Hibbs L. R., Agius R. M., Beverland I. j. (2005) " interpretation of variations in fine, coarse and black smoke particulate matter concentrations in a northern European city",

Atmospheric Environment, 39, 3711-3718.

Hussain A.M. T., Ashraf E.M. K., Farouq I. H., (2013) "Heavy elements concentrations, physiochemical characteristics and natural radionuclides levels along the Saudi coastline of the Gulf of Aqaba" Arabian Journal of Chemistry , 6, 183–189.

Kaisa Salminen, Vuokko, Karlsson. (2003) "Comparability of low-volume PM10 sampler with β-attenuation monitor in background air" Atmospheric Environment, 37, 3707-3712.

Kakoli, Karar, Gupta, A.K., Animesh, ArunKanti, Biswas (2006) "Seasonal variations of PM10 and TSP in residential and industrial sites in an urban area of Kolkata, India", Environmental Monitoring and Assessment. **118**, 369–381.

Kennedy, P., Gadd, J. (2003) "Preliminary Examination of Trace Elements in Tyres, Brake Pads and Road Butimen in New Zealand", Prepared for Ministry of Transport, New Zealand by Kingett Mitchell Limited, November, 2000, revised October.

Le Petit, G., Deschamps, J. P., Nouchpramools, S. (2002) "Trace Elements in Total Atmospheric Suspended Particles in a Suburban Area of Paris: A Study Carried Out by INAA. In: Environmental Changes and Radioactive Tracers". IRD Editions, Paris. 299-321.

Li, J., Wang, Y., Yang, H., Yu, P., & Tang, Y. (2018) "Five heavy metals accumulation and health risk in a traditional Chinese medicine Cortex moutan collected from different sites in China" Human and Ecological Risk Assessment: An International Journal, **24**(8), 2288–2298.

Liu, Y., Wu, J., Wei, W., & Xu, R. (2013) "Simultaneous determination of heavy metal pollution in commercial traditional Chinese medicines in China" Journal of Natural Medicines, **67**(4), 887–893.

Salaam, A., Bauer, H., Kassin, K., Ullah, S. M., Puxbaum, H. (2003) "Aerosol Chemical Characteristics of a Mega-city in Southeast Asia (Dhaka–Bangladesh)", Atmospheric Environment. **37**, 2517-2528.

Sitaram, Garimella., Ravin, N. Deo. (2007) "Neutron Activation Analysis of Atmo- spheric Aerosols from a Small Pacific Island Country. A Case of Suva, Fiji Islands", Aerosol and Air Quality Research. **7** (4), 500–517.

U.S. EPA (2019) "Guidelines for human exposure assessment". Washington, DC: U.S. Environmental Protection Agency. https://www.epa.gov/risk/guidelineshuman-exposure-assessment

WHO. (1997) "Guidelines for Air Quality", Fact Sheet No. 187, World 47, Elsevier, Amsterdam, 1991 Health Organization, Geneva, p. 123.

WHO. (2003) "Health aspects of air pollution with particulate matter, ozone and nitrogen dioxide". Report on a WHO working group, 13–15 January 2003, Bonn, Germany.

Wu, X., & Xue, J. (2013) "Heavy metals contamination status and analyses of Traditional Chinese Medicine" Asian Journal of Chemistry, **25**(1), 19–22.

دراسة تلوث الغلاف الجوي للمواد الجسيمية في البيئة الحضرية بمنطقة جازان

انتصار حنفي العربي وسابينا باولي

قسم الفيزياء ، كلية العلوم ، جامعة جازان ، المملكة العربية السعودية

الملخص

جذب تركيز الجسيمات العالقة في الغلاف الجوي اهتمامًا كبيرًا للعديد من الباحثين في العقد الماضي. حيث أظهرت الأبحاث أن الجسيمات العالقة مسؤول عن حدوث تفاعلات كيميائية ضارة تؤدي إلى التدهور الفيزيائي لطبقة الأوزون في الستراتوسفير. علاوة على ذلك ، يزيد الهباء الجوي من خطر الإصابة بالسرطان لدى البشر عند استنشاقه بنسب كبيرة. تسعى هذه الورقة إلى تقدير تركيز جميع المعادن الثقيلة في هواء مدينة جازان ، من خلال تطبيق تحليل التنشيط النيوتروني (NAA) . كشف التحليل أن أقصى تركيز لهباء PM10 و TSP في مدينة جازان يحدث خلال فصل الربيع. تم تسجيل أعلى تركيز لـ Ba و Br و Th و Zn و Rb في المطار بينما تم تسجيل أعلى تركيز لـ Ca و Ce و Co و Cr و Eu و La و Sb و Sc في المنطقة الصناعية وحي الجبل. بالإضافة إلى ذلك، تم التوصل إلى أن الهباء الجوي لمدينة جازان PM10 و TSP غني بالكالسيوم والباريوم والزنك والحديد، وكلها نتيجة للأنشطة البشرية. لذلك يجب الاهتمام بالأحزمة الخضراء حول المدن وترشيد استخدام آلات النقل والبناء لتقليل تركيز الهباء الجوي وتقليل التلوث.

الكلمات المفتاحية: إجمالي الجزيئات العالقة TSP و PM10 - عوامل الإثراء (EF) - المعادن الثقيلة - جازان - تحليل التنشيط النيوتروني NAA.

Ganoderma lucidum: Production of biomass as a source of nutritionally active compounds through a submerged fermentation process

Abdulrahman A. Alsayegh
Clinical Nutrition Doctor of Philosophy Jazan University

Abstract

Ganoderma lucidum (*G. lucidum*) is a versatile mushroom with chief bioactive compounds triterpenoids and polysaccharides. *G. lucidum* had been applied as traditional remedy and for food in antique times and is now used as a nutraceutical and functional food. The mushroom also contains secondary metabolites with numerous medicinal benefits that make it a potential substitute treatment that could be functional as an anticancer, immunomodulator, anti-oxidant, antimicrobial, anti-diabetic, and anti-inflammatory medicine. The miraculous attributes of these bioactive compounds fascinate the researchers because of their development and production. In this study used Plackett–Burman experimental design and selected nine nutritional parameters. The biomass obtained after the submerged fermentation process, in each of the 12 experimental trials was 22.30 gL^{-1}, 26.42 gL^{-1}, 22.40 gL^{-1}, 22.80 gL^{-1}, 21.40 gL^{-1}, 26.20 gL^{-1}, 26.40 gL^{-1}, 26.82 gL^{-1}, 20.40 gL^{-1}, 23.60 gL^{-1}, 25.46 gL^{-1}, and 19.60 gL^{-1} in complex media (peptone 5 gL^{-1}, yeast extract 5 gL^{-1}, potassium dihydrogen phosphate 1 gL^{-1}, magnesium sulfate 0.5 gL^{-1}, vitamin B_1 0.05 gL^{-1}, and distilled water 1 L, adjusted to pH 5.8) as per the experimental design. It was concluded that the maximum production was obtained from experimental trial 8 (26.8 gmL^{-1}), whereas the minimum production was from experimental trial 12 (19.6 gmL^{-1}). Finally, it was concluded that different variables effects the production of biomass and among the nine nutritional components used in this study, maltose, glucose, NaCl, biotin, and elicitor contributed largely to biomass production.

Keywords: *Ganoderma lucidum*، Submerged fermentation, Biomass, Plackett–Burman experimental design, Bioactive compound.

Introduction

Ganoderma lucidum (*G. lucidum*) is a mushroom (also called reishi) that has been employed as a traditional medication in Asian countries (Wu et al., 2022). For many years, this mushroom has been eaten and cherished for its aroma, as well as their economic and ecological values in traditional medicine and their nutraceutical value (Khoo et al., 2022). Various active constituents are found in these mushrooms that have great therapeutic as well as prophylactic potential (Zhang et al., 2022). The most important pharmacological active *G. lucidum* constituents are reported to be polysaccharides and ganoderic acids. In addition, the *G. lucidum* mushroom contains a variety of other constituents, such as dietary fiber, organic germanium, nucleosides, nucleotides and RNAs, vitamins, alkaloids, essential fatty acids, and minerals, that have a key role against various diseases (Core et al., 2018; Ahmad, 2019). It has been used as a traditional medicine due to its miscellaneous applications and various biological activities in the prevention and management of numerous disorders. The diverse applications of the reishi mushroom have pulled people's attention towards its precious effects, such as its antioxidant (Karimi et al., 2022), anti-cancer (Ahmad et al., 2020), hypoglycemic (Zhang et al., 2022), anti-inflammatory (Wen et al., 2022), and immunomodulatory effects (Liu et al., 2022), its anti-hypertensive action (Ahmad, 2018), and its applications in liver disease **(**Zhang et al., 2022), insomnia/anxiety **(**Chu et al. 2007; Yakju et al. 2004.), and rheumatoid arthritis (Heo et al., 2023).

The fermentation process was carried out with a distinct objective. The aim was to yield biomass without concern for its composition, which gives a brief idea about the probability of production by using various pharmacological active constituents. The use of a submerged culture ensures high productivity, a shorter time duration, low cost, convenience, control, and an easy downstream in the mycelial biomass production and obtaining the various triterpenoids (Park et al., 2001; Wagner et al., 2004). Submerged fermentation has advantages greater than traditional basidiocarp cultivation. During this fermentation process, reasonable amounts of biomass can be achieved in a few weeks (Tang & Zhong, 2002; Hu et al., 2017). The optimization of medium composition regarding the parameters such as aeration, fungal morphology, agitation speed, inoculum density, pH, and temperature was extensively studied in present time (Chang et al., 2006). This research aimed to enhance the biomass production from *G. lucidum* mycelium through a submerged fermentation process rather than compostion or bioactive properties and to understand how different variables affect their production.

Materials

G. lucidum fungal cultures were collected from the National Research Centre for Mushroom, India. Cultures were preserved consistently on a potato dextrose agar medium and subcultured every 30 days. Complex media prepared with peptone 5 gL^{-1}, yeast extract 5 gL^{-1}, potassium dihydrogen phosphate 1 gL^{-1}, magnesium sulfate 0.5 gL^{-1}, vitamin B_1 0.05 gL^{-1}, and distilled water 1 L, adjusted to pH 5.8 as per the experimental design. Microorganism *Penicillium citrinum* was used for the development of the elicitor. It was preserved on slants of potato dextrose agar medium at 4°C.

Methods

Preparation of seed culture and fermentation

A seed culture of potato dextrose broth (PDB) medium was used to prepare the inoculums of *G. lucidum* at a temperature of 27°C in a 250 ml Erlenmeyer flask; it was then shaken for 7 days at 150 rpm in a shaker incubator. Every experiment was performed in Erlenmeyer flask (250 ml) containing 50 ml of complex media (peptone 5 gL^{-1}, yeast extract 5 gL^{-1}, potassium dihydrogen phosphate 1 gL^{-1}, magnesium sulfate 0.5 gL^{-1}, vitamin B_1 0.05 gL^{-1}, and distilled water 1 L, adjusted to pH 5.8) according to the experimental plan. With a 10% seed culture, these flasks were inoculated and incubated for 12 days at 27°C (4 days shaken at 120 rpm and 8 days in a static condition).

Preparation of elicitor

Fungal elicitors are a group of chemicals that are able to encourage the secondary metabolite production in plants and microbial cells. Several parameters, like the nature of the elicitor, concentrations, and time of elicitor exposure, are significant factors to encourage the highest level of bioactive compounds. Microorganism *Penicillium citrinum* was used for the development of the elicitor. It was preserved on slants of Potato Dextrose Agar (PDA) medium at 4°C and the subculture was made from actively growing slants of PDA medium. The seed culture was made in the PDB medium and incubated at 27°C for 5 days in an Erlenmeyer flask of 250 ml and shaken in a shaker incubator at 150 rpm. Thereafter, the cultures were autoclaved for 15 minutes, and the produced fungal culture was sonicated for up to 5 minutes. Finally, the culture was sterilized and used as the elicitor.

Optimization of fermentation nutritional components

Nine medium constituents, i.e., glucose, maltose, corn flour, $MnSO_4.H_2O$, urea, soya flour, biotin, NaCl, and the fungal elicitor, were chosen for the study to evaluate the various nutrients needed for the production of biomass. Altogether there were eleven variables used: each of nine experiments was assigned one of the medium constituents (nutritional components, which were the independent variables) and two experiments were assigned dummy variables as per the Plackett–Burman experimental (PBE) design (Plackett and Burman, 1946). For every nutrient variable, two different concentrations, high (+) and low (-), were evaluated (Table 1). The concentrations of the variables at diverse levels can be seen in Table 2.

Table 1: The PBE design of 12 trials with 11 variables (Each row signifies an experiment and each column signifies a different variable).

Trial	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}
1	+	+	-	+	+	+	-	-	-	+	-
2	-	+	+	-	+	+	+	-	-	-	+
3	+	-	+	+	-	+	+	+	-	-	-
4	-	+	-	+	+	-	+	+	+	-	-
5	-	-	+	-	+	+	-	+	+	+	-
6	-	-	-	+	-	+	+	-	+	+	+
7	+	-	-	-	+	-	+	+	-	+	+
8	+	+	-	-	-	+	-	+	+	-	+
9	+	+	+	-	-	-	+	-	+	+	-
10	-	+	+	+	-	-	-	+	-	+	+
11	+	-	+	+	+	-	-	-	+	-	+
12	-	-	-	-	-	-	-	-	-	-	-

Results and discussion

Through the use of fermentation processes, currenttly interest in producing naturally active compounds has grown. Submerged fermentation produces the desire product in shorter period of time while conventional basidiocarp cultivation takes longer time. The development of basidiocarp using the traditional method takes approximately three to five months, and also do not confirm a quality product due to substrate compositions that affect the basidiocarp formulations and variations from batch to batch (Yang et al., 2021). Owing to this reason, the production of biologically active compounds of *G. lucidum* using fermentation technology through submerged culture is a potential alternate. The collection of biomass is the one of the most important factors to measure growth and finding bioactive componuds after experiments. Biomass in submerged fermentation process is generally recovered by filtration under suction or centrifugation. In the current study, the quantification of biomass was done by filtration through pre-weighed filter paper with a standardized pore size and weight was measured on dry basis.

Table 2: Variables concentration at various levels in the PBE design for the production of biomass using submerged culture.

S. No.	**Designation**	**Variable**	**Low level (-) (gL^{-1})**	**High level (+) (gL^{-1})**
1	X_1	Maltose	20	30
2	X_2	Glucose	20	30
3	X_3	Corn flour	20	30
4	X_4	$MnSO_4.H_2O$	0.1	0.3
5	X_5	Urea	1	3
6	X_6	Dummy 1	-	-
7	X_7	Soya flour	1	3
8	X_8	NaCl	2	6
9	X_9	Biotin	0	0.1
10	X_{10}	Dummy 2	-	-
11	X_{11}	Elicitor	0	0.12

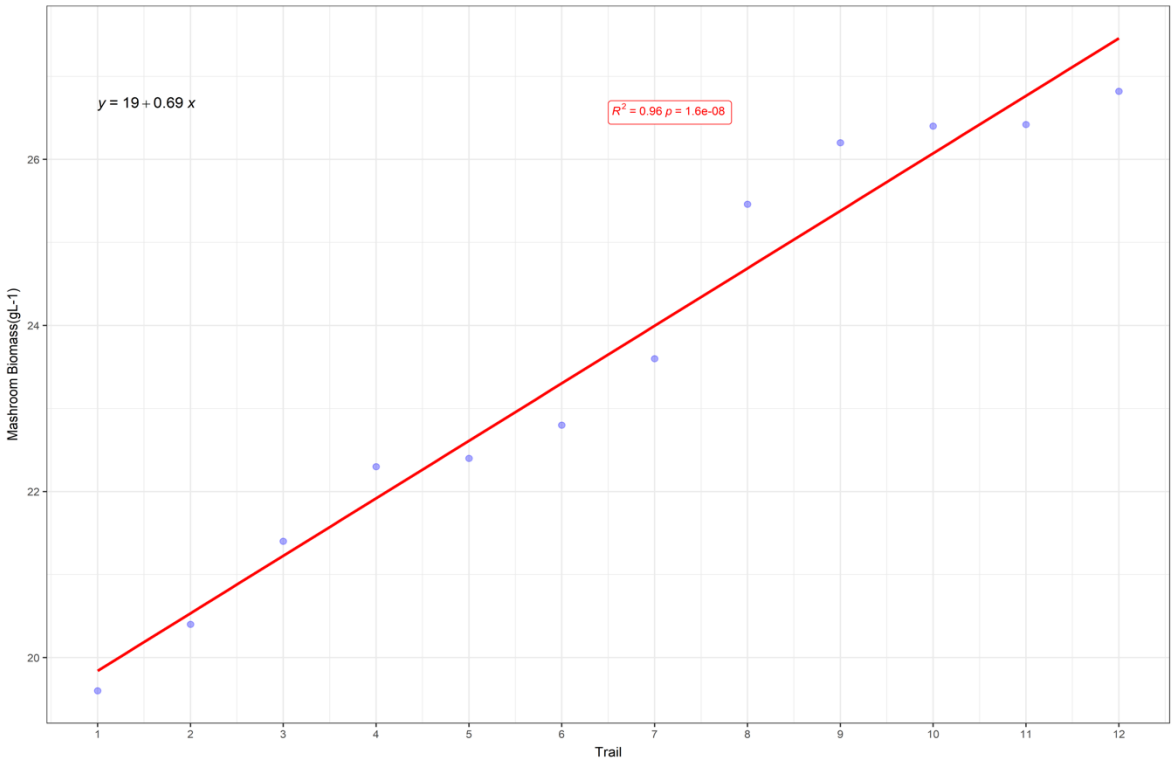
It was observed that different variables produced different weights of biomass. The weights of biomass produced in each trial were 22.30 gL^{-1}, 26.42 gL^{-1}, 22.40 gL^{-1}, 22.80 gL^{-1}, 21.40 gL^{-1}, 26.20 gL^{-1}, 26.40 gL^{-1}, 26.82 gL^{-1}, 20.40 gL^{-1}, 23.60 gL^{-1}, 25.46 gL^{-1}, and 19.60 gL^{-1} (Table 3). Maximum production of biomass was observed in experimental trial 8 (26.8 gmL^{-1}), highly significance ($P<0.01$) difference was observed between the 12 trails biomass weight(gl-1). 8th trial combination (glucose+, maltose+, corn flour, $MnSO_4.H_2O$, urea, soya flour, biotin+, NaCl+, and the fungal elicitor+) of variable were given the significantly higher weight than the others trial combination of variables. Whereas minimum production was observed in experimental trial 12 (19.6 gL^{-1}). Among the nine nutritional components used in this study, maltose, glucose, NaCl, biotin, and fungal elicitor contributed largely to biomass production. The production of biomass is not a concern to its composition. Weight growth rate was determined by fitting the regression line can be seen in figure. 1.

Table 3: The PBE design of 12 trials with 11 variables (9 nutrients + 2 dummy variables) with observed biomass production in fermented broth (Each row signifies an experiment and each column signifies a different variable).

Trial	**X1**	**X2**	**X3**	**X4**	**X5**	**X6**	**X7**	**X8**	**X9**	**X10**	**X11**	**Production of biomass (gL^{-1})**	**[§]P-Value**
1	+	+	-	+	+	+	-	-	-	+	-	22.30	0.0004
2	-	+	+	-	+	+	+	-	-	-	+	26.42	
3	+	-	+	+	-	+	+	+	-	-	-	22.40	
4	-	+	-	+	+	-	+	+	+	-	-	22.80	
5	-	-	+	-	+	+	-	+	+	+	-	21.40	
6	-	-	-	+	-	+	+	-	+	+	+	26.20	
7	+	-	-	-	+	-	+	+	-	+	+	26.40	
8	+	+	-	-	-	+	-	+	+	-	+	26.82	
9	+	+	+	-	-	-	+	-	+	+	-	20.40	
10	-	+	+	+	-	-	-	+	-	+	+	23.60	
11	+	-	+	+	+	-	-	-	+	-	+	25.46	
12	-	-	-	-	-	-	-	-	-	-	-	19.60	

[§]t-test for single mean test statistic is 4.969797 and $P<0.01$ highly significant.

Figure-1: Growth curve of weight change by shake flask



Arranging the biomass weight in ascending order and weight growth rate was determined by fitting the regression line using the equation Y=19+0.69X where the parameters X and Y are the trail number and mushroom biomass weight (gL^{-1}). The average growth rate of the function was 0.69 and it was highly significant ($p<0.01$) between the trails.

Conclusion

The versatility of triterpenoids (ganoderic acid) inspired the researchers to effectively produce secondary metabolites in a short span of time with a superior outcome compared to traditional approaches. The fermentation method produced the desired product with high efficiency, low cost, and convenient control with rapid extraction. The production of biomass is an important factor in obtaining secondary metabolites, particularly triterpenoids and polysaccharides. During fermentation, to improve biomass production, various parameters were regulated and observed, such as temperature, pH, nutrition, media, biochemical signals, and nutritional components (sucrose and glucose). Maximum production of biomass was achieved in experimental trial 8 (26.8 gmL^{-1}), highly significance ($P<0.01$) difference was observed between the 12 trials biomass weight (gL-1), where maltose, glucose, NaCl, biotin, and elicitor contributed well to obtain maximum production.

References

Ahmad, M. F. (2018). Ganoderma lucidum: Persuasive biologically active constituents and their health endorsement. *Biomedicine & Pharmacotherapy*, *107*, 507-519.

Ahmad, M. F. (2019). Ganoderma lucidum: A macro fungus with phytochemicals and their pharmacological properties. *Plant and Human Health*, *2*(), 491–515.

Ahmad, M. F. (2020). Ganoderma lucidum: A rational pharmacological approach to surmount cancer. *Journal of Ethnopharmacology*, 260, 113047.

Chang, M. Y., Tsai, G. J., & Houng, J. Y. (2006). Optimization of the medium composition for the submerged culture of Ganoderma lucidum by Taguchi array design and steepest ascent method. *Enzyme and Microbial Technology*, *38*(3–4), 407–414.

Chu, Q. P., Wang, L. E., Cui, X. Y., Fu, H. Z., Lin, Z. B., Lin, S. Q., & Zhang, Y. H. (2007). Extract of Ganoderma lucidum potentiates pentobarbital-induced sleep via a GABAergic mechanism. *Pharmacology Biochemistry and Behavior*, *86*(4), 693–698.

Cör, D., Knez, Z., & Knez Hrnčič, M. (2018). Antitumour, antimicrobial, antioxidant and antiacetylcholinesterase effect of Ganoderma lucidum terpenoids and polysaccharides: A review. *Molecules*, *23*(3), 649.

Heo, Y., Kim, M., Suminda, G. G. D., Min, Y., Zhao, Y., Ghosh, M., & Son, Y. O. (2023). Inhibitory effects of Ganoderma lucidum spore oil on rheumatoid arthritis in a collagen-induced arthritis mouse model. *Biomedicine & Pharmacotherapy*, 157, 114067.

Hu, Y., Ahmed, S., Li, J., Luo, B., Gao, Z., Zhang, Q., Li, X., & Hu, X. (2017). Improved ganoderic acids production in Ganoderma lucidum by wood decaying components. *Sci. Rep*. 7, 46623.

Karimi, M., Raofie, F., & Karimi, M. (2022). Production Ganoderma lucidum extract nanoparticles by expansion of supercritical fluid solution and evaluation of the antioxidant ability. *Scientific Reports*, *12*(1), 1–12.

Khoo, S. C., Ma, N. L., Peng, W. X., Ng, K. K., Goh, M. S., Chen, H. L., ... & Sonne, C. (2022). Valorisation of biomass and diaper waste into a sustainable production of the medical mushroom Lingzhi

Ganoderma lucidum. *Chemosphere*, 286, 131477.

Kim, J. H., Lee, D. H., Lee, S. H., Choi, S. Y., & Lee, J. S. (2004). Effect of Ganoderma lucidum on the quality and functionality of Korean traditional rice wine, yakju. *Journal of Bioscience and Bioengineering*, *97*(1), 24–28.

Liu, L., Feng, J., Gao, K., Zhou, S., Yan, M., Tang, C., ... & Zhang, J. (2022). Influence of carbon and nitrogen sources on structural features and immunomodulatory activity of exopolysaccharides from Ganoderma lucidum. *Process Biochemistry*, *119*, 96-105.

Park, J. P., Kim, S. W., Hwang, H. J., & Yun, J. W. (2001). Optimization of submerged culture conditions for the mycelial growth and exo-biopolymer production by Cordyceps militaris. *Lett Drug Des Discov*, *33*, 76–81.

Plackett, R. L., & Burman, J. P. (1946). The design of optimum multifactorial experiments. Biometrika, 33(4), 305-325.

Tang, Y. J., & Zhong, J. J. (2002). Fed-batch fermentation of Ganoderma lucidum for hyperproduction of polysaccharide and ganoderic acid. *Enzyme and Microbial Technology*, *31*(1–2), 20–28.

Wagner, R., Mitchell, D. A., Sassaki, G. L., & de Almeida Amazonas, M. A. L. (2004). Links between morphology and physiology of Ganoderma lucidum in submerged culture for the production of exopolysaccharide. *Journal of Biotechnology*, *114*(1–2), 153–164.

Wen, L., Sheng, Z., Wang, J., Jiang, Y., & Yang, B. (2022). Structure of water-soluble polysaccharides in spore of Ganoderma lucidum and their anti-inflammatory activity. *Food Chemistry*, 373, 131374.

Wu, T., Cai, M., Hu, H., Jiao, C., Zhang, Z., Liu, Y., & Xie, Y. (2022). Whole-genome sequencing and transcriptome analysis of Ganoderma lucidum strain Yw-1-5 provides new insights into the enhanced effect of Tween80 on exopolysaccharide production. *Journal of Fungi*, *8*(10), 1081.

Yang, X., Yang, Y., Zhang, Y., He, J., & Xie, Y. (2021). Enhanced exopolysaccharide production in submerged fermentation of Ganoderma lucidum by Tween 80 supplementation. *Bioprocess and Biosystems Engineering*, *44*(1), 47–56.

Zhang, L., Qiao, H. Y., Liu, H. X., Jiang, G. C., Wang, L. Y., & Liu, X. J. (2022). Antioxidant, hypoglycemic and protection of acute liver injury activities of Ganoderma lucidum spore water extract. *Journal of Functional Foods*, 97, 105254.

غانوديرما لوسيدوم (الفطر الريشي): إنتاج الكتلة الحيوية كمصدر للمركبات النشطة من الناحية التغذوية من خلال عملية التخمير المغمورة

عبدالرحمن الصايغ
قسم التغذية الاكلينيكية-كلية العلوم الطبية التطبيقية-جامعة جازان- المملكة العربية السعودية

الملخص

غانوديرما لوسيدوم (G. lucidum) هو فطر متعدد الاستخدامات يحتوي على مركبات رئيسية نشطة بيولوجيا triterpenoids و polysaccharides. تم استخدام هذا الفطر في الطب التقليدي والطعام في العصور القديمة ويستخدم الآن كغذاء وظيفي. يحتوي الفطر على مستقلبات ثانوية مع العديد من الفوائد الطبية التي تجعله علاجًا بديلاً محتملاً يمكن أن يكون فعالاً كمضاد للسرطان، ومعدّل للمناعة، ومضاد للأكسدة، ومضاد للميكروبات، ومضاد للسكري، ومضاد للالتهابات. إن السمات المعجزة لهذه المركبات النشطة بيولوجيًا تبهر الباحثين بسبب تطورها وإنتاجها. يهدف هذا البحث إلى تعظيم إنتاج الكتلة الحيوية من G. lucidum mycelium عن طريق عملية التخمير المغمورة. باستخدام التصميم التجريبي لـ Plackett-Burman، تم اختيار تسعة متغيرات غذائية. بعد عملية التخمير، كانت الكتلة الحيوية التي تم الحصول عليها في كل من التجارب الـ ١٢ التجريبية ٢٢,٣٠ جم/لتر$^{-1}$، ٢٦,٤٢ جم/لتر $^{-1}$، ٢٢,٤٠ جم/لتر $^{-1}$، ٢٢,٨٠ جم/لتر $^{-1}$، ٢١,٤٠ جم/لتر $^{-1}$، ٢٦,٢٠ جم/لتر $^{-1}$، ٢٦,٤٠ جم/لتر $^{-1}$، ٢٦,٨٢ جم/لتر $^{-1}$، ٢٠,٤٠ جم/لتر $^{-1}$، ٢٣,٦٠ جم/لتر $^{-1}$، ٢٥,٤٦ جم/لتر $^{-1}$، و ١٩,٦٠ جم/لتر $^{-1}$ في الوسائط المعقدة (ببتون ٥ جم لتر $^{-1}$، مستخلص الخميرة ٥ جم/لتر $^{-1}$، فوسفات هيدروجين البوتاسيوم ١ جم/لتر $^{-1}$، كبريتات المغنيسيوم ٠,٥ جم/لتر $^{-1}$، فيتامين ب ١ ٠,٠٥ جم/لتر $^{-1}$، والماء المقطر ١ لتر، معدّل إلى الرقم الهيدروجيني ٥,٨) حسب التصميم التجريبي. تم التوصل إلى أن أقصى إنتاج تم الحصول عليه ٨ (٢٦,٨ جم/لتر $^{-1}$) بينما كان الحد الأدنى للإنتاج ١٢ (19.6 جم/لتر $^{-1}$). أخيرًا ، تم استنتاج أن المتغيرات المختلفة تؤثر على إنتاج الكتلة الحيوية. ومن بين المكونات الغذائية التسعة المستخدمة في هذه الدراسة: المالتوز، الجلوكوز، كلوريد الصوديوم، البيوتين، والإليسيتور ساهموا بشكل كبير في إنتاج الكتلة الحيوية.

الكلمات المفتاحية: غانوديرما لوسيدوم (الفطر الريشي)، تخمير مغمور، كتلة حيوية، الاختبار التجريبي لبلاكيت-بورمان، مركب نشط بيولوجيًا.

A Review of potential Cyber Security Issues in the Internet of Things and the Blockchain-based Solution

Abdoh Jabbari[1]

[1]College of Computer Science and Information Technology, Jazan University, Kingdom of Saudi

Abstract

Blockchains have been more popular since Satoshi Nakamoto's Bitcoin white paper appeared in 2008; since then, they have become one of the most often discussed ways for preserving data storage and transmission via decentralized, trustless, peer-to-peer networks. A thorough evaluation of both the advantages and disadvantages of the most frequently used blockchain security applications is provided in this research. In addition, peer-reviewed research on the use of blockchain technology for cyber security is highlighted. Based on the outcome of review, the Internet of Things (IoT) seems to be an excellent platform for developing innovative blockchain applications, particularly for industrial applications. These technologies include network and machine visualization, public-key cryptography, online applications, certification systems, and safe storage of personal information. In addition, the present research provides a window into future study directions. The main goal of this review is to bring the various security challenges & issues on different layers of IoT architecture and their possible solutions. This paper surveyed recent security advances to overcome IoT limitations using blockchain. In this article, the blockchain attempts to overcome IoT limitations that are related to cyber security.

Keywords: Internet of Things (IoT), Cybersecurity, Blockchain.

1 Introduction

The word IoT refers to the network that enables different devices to connect to the internet and allows users control ability through the internet[1]. With the rise in IoT demand, it becomes essential to comprehend some of the significant things concerned with the internet of things. Thus, understanding the architectural world associated with IoT, the layered approach used and based on the approach, the three layers, perception, network, and application layers becomes very critical in safeguarding IoT using blockchain technology[2]. IoT systems currently in use are designed using a centralized server/client architecture, necessitating the connection and server-based authentication of all devices. This model would not be able to meet future IoT system expansion requirements. Therefore, shifting the IoT system to a decentralized path might be the best course of action. Blockchain is a well-known decentralization platform. Blockchain, being similar to relational database, is a public electronic ledger that can be shared openly by different users and has the ability to create an interchangeable record of the user's transactions, with each record time-stamped and linked to the previous transaction [3]. Within the user community established, each user has to keep information copy while all members must collectively validate any updates. The primary purpose of IoT is to collect sensing data from smart terminals dispersed throughout various environments, such as forests, mountains, volcanoes, and other inaccessible locations, where it is challenging to recharge the devices. Energy-saving mechanisms in the Internet of Things are therefore a popular area for research given the state of energy technology. IoT is expanding, and with it, the amount of sensitive and private data being transmitted. It becomes urgent in this circumstance to effectively protect these data. Some intrusion detection systems can spot information that has been altered or misrepresented, as well as some routing threats[4][5]. The advantages of combining blockchain and IoT are numerous. The blockchains decentralized model will be able to process trillions of transactions between IoT devices, which will significantly cut down on the costs of setting up and maintaining massive centralized data centers and spread out the demands for computation and storage across the trillions of IoT devices. Additionally, employing blockchain technology will remove the centralized IoT architecture's single point of failure.

1.1 Background

According to Vega (2020), the International Data Corporation's 2017 projection on IoT, global IoT expenditure will top one trillion dollars by 2020, with 2021 predicted to expand by another 100 million dollars, with more than 55 percent spent on services and software [4]. Three sectors, namely transportation, logistics, and manufacturing, will account for half of all IoT expenditure in 2020, and it is worth noting that when looking at end-point IoT market size, three segments control half of the industry [4]. From the 5.81 billion IoT end-point units, about 3.16 billion are in use, with utility sectors utilizing 1.37 billion units, government using 0.7 billion units, and physical security using 1/09 billion units.

Based on Sajjad and Arshad (2019), at the perception layer, IoT is responsible in collecting every information essential for processing and care has to be taken to ensure only authentic information comes from sensors. With devices connecting to the network, the attacker can damage the sensors or replace the tampering node to access confidential information such as

cryptographic keys. The other security threat associated with the perception layer is that the attacker can inject malicious codes in to the node gaining access to the entire network [6]. This mainly takes place when software upgrade is taking place. At the network layer, Mario and Pasquale (2018) show that different attacks are possible in the form of routine attack, storage attack, DoS attack, man in the middle attack, and data transit attack. Routine attack takes place when malicious intermediate nodes affects the entire network through network manipulation. DoS attacks are associated with unnecessary requests that make the entire system halt while man in the middle attacks take place when every IoT network node for communication is attacked resulting in unsecure sending or receiving of data[7]. Network injection is an attack where the original sender is changed, by the hacker, and starts sending data like the hacker is part of the IoT network. At the application/cloud layer, security threats interfere with data privacy resulting in altered data integrity, authenticity, and confidentiality. These threats takes place in various forms like data leakage, DoS attacks, sniffing attacks, malicious codes, intermediate attacks, booting susceptibility, and reverse engineering model among others[8].

With its ability to reduce IoT security vulnerabilities by maintaining an immutable historical record, blockchain technology has emerged as a preferred component in IoT systems. Blockchain technology, which maintains immutable historical records, enables autonomous operation of many devices without the need for a centralized authority. As a result, blockchain opens the door to safe and trustless communications between IoT and devices, where each message is processed in a way similar to bitcoin network transactions, allowing the exchange of messages to be leveraged in smart contracts, which mimic agreements between two parties[9] .

1.2 **Architecture of IoT**

A four-layer architecture has independent functions and scalability for each layer. Through effective heterogeneous networking components, cloud servers store the sensing data gathered from a variety of sensors. Numerous different network architectures make up the heterogeneous networking units. IoT has been implemented in both industry and daily life as a result of advancements in the hardware design of sensors and network topology optimization. The remaining paragraphs of this section describe the four layers of the architecture. Figure 1 depicts a four-layer future Internet of Things architecture developed by Qiu et al. [2018], which contains an applications layer, a cloud computing layer, a network and sensing layer, and a sensing layer[10].

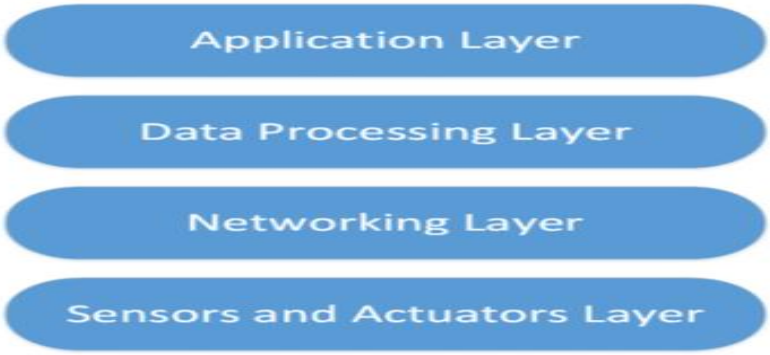


Figure 1. IoT architecture

Four Layers of the Architecture are:

1. Application Layer: All IoT-related applications are defined at the application layer. It serves as the network's interface with the end IoT devices. IoT applications for smart cities, smart homes, and smart health. It has the power to give the applications services.
2. Data Processing Layer: The data were sent directly to the network layer in a multiple architecture. The likelihood of suffering damages rises as a result of sending data directly. In a four-layer architecture, information from a perception layer is sent to this layer. Data Processing Layer has two responsibilities: it verifies that data is transmitted by legitimate users and protects against threats.
3. Network Layer: A transmission layer is another name for this layer. It serves as a bridge that transports and transmits data collected from real world objects by sensors. Either a wireless or wired medium may be used. Additionally, it links networks and network devices together. As a result, it is very susceptible to attacks from the attackers. It has substantial security problems with the authenticity and integrity of the data being transmitted to the network.
4. Sensor Layer: The task of object recognition and data collection falls to the sensor layer. There are many different kinds of sensors attached to the objects that collect data, including RFID, sensors, and 2-D barcodes. The sensors are chosen based on the demands of the applications. These sensors can gather information about location, changes in the atmosphere, the environment, etc. Attackers want to use them to replace the sensor with their own, but that is their prime objective.

1.3 **Blockchain Technology**

Blockchain technology is a decentralized, distributed digital ledger that makes data recording and sharing safe, transparent, and impenetrable. It runs on a network of computers that collaborate to validate and verify transactions and keep the data's integrity. The architecture of the system is built on a chain of blocks, each of which has a distinct digital signature, or hash, that connects it to the block before it. As a result, a record of transactions is created that is immutable and cannot be changed or deleted without network consensus.

Although most commonly linked to cryptocurrencies like Bitcoin, Blockchain technology has the potential to transform various industries beyond finance. It can provide a secure and transparent way to record and share data, making it useful for applications such as supply chain management, healthcare, and real estate, among others. The decentralization of blockchain technology, which does away with the need for middlemen or centralized authorities, is one of its main benefits. This lowers transaction costs and boosts efficiency. Advanced cryptography is used to protect privacy and security, making it nearly impossible to hack or alter the data[11].

Blockchain technology is still a relatively new and developing technology, despite its potential advantages. Its use is still hampered by difficulties and restrictions, such as scalability and legal concerns. Nevertheless, continuing research and development are assisting in resolving these issues and realizing the full potential of this potent technology[12]. Fig 2 shows benefits of integrating with IoT.

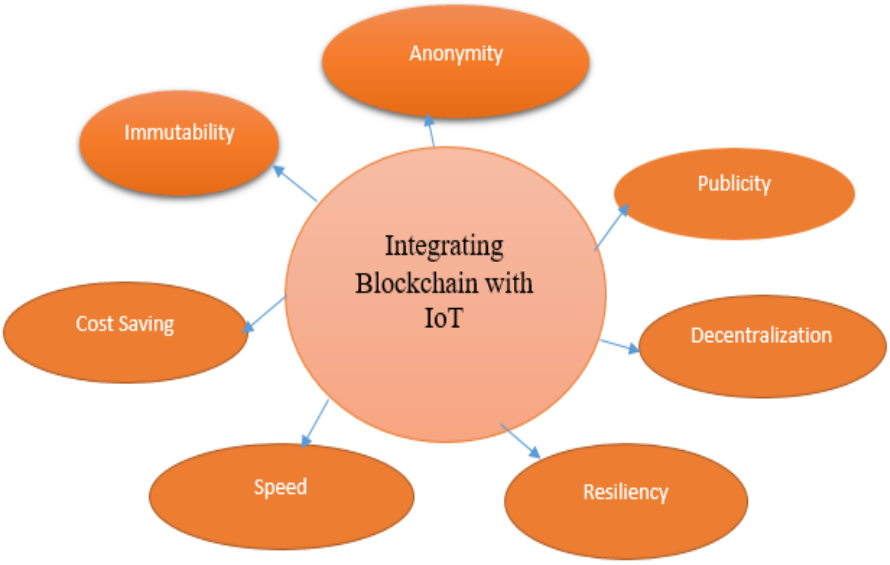


Figure 2: Benefits of Blockchain

In general, blockchain technology can offer a transparent and secure framework for fending off cyberattacks. Organizations can create robust systems that are better protected against cyberattacks by utilizing the special characteristics of blockchain. While blockchain technology has several advantages for securing IoT devices, there are some drawbacks to the most commonly used blockchain security applications[13].

Fig.3 shows limitations of blockchain and IoT. Here are some of the drawbacks:

1. As the number of users and transactions increases, the current blockchain technology faces scalability challenges, resulting in network congestion and slower transaction processing. This can be a problem for Internet of Things systems that require real-time processing and low latency.
2. Applying blockchain-based security solutions can be difficult, requiring specialized technical expertise and significant resources. For organizations lacking the necessary technical expertise and resources, this can be a significant challenge.
3. The legal and regulatory landscape for blockchain technology is still evolving, and there is a lack of clear guidance in many jurisdictions. This can create uncertainty and risk for organizations considering implementing blockchain-based security solutions.

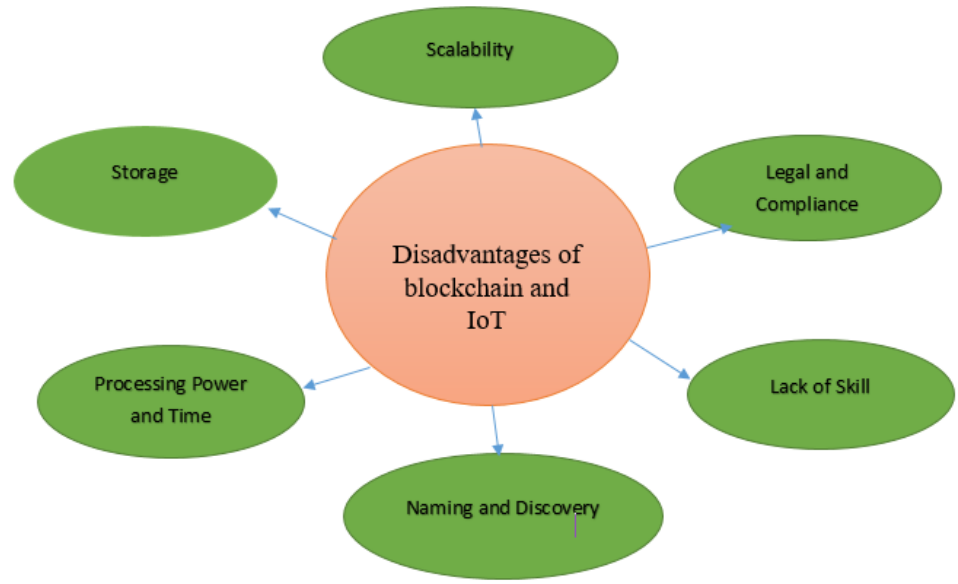


Figure 3: Limitations of Blockchain and IoT

1.4 **Related Work**

In a few papers, the incorporation of blockchain with IoT has been studied. In order to create a distributed network of devices, the IBM Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT) project uses the blockchain. Regarding the ADEPT project, numerous other strategies are working to create a plan that will enable the fusion of all the various applications based on blockchain technology [14] .

Dorri et al.[15] Have put forth a new, blockchain-based, secure, private, and lightweight IoT architecture that removes the overhead while retaining the majority of the technology's security and privacy advantages was examined on a smart home application as a case study that is representative of more general IoT applications. With smart homes, an overlay network, and cloud storages coordinating data transactions with blockchain to provide privacy and security, the proposed architecture was hierarchical.

As according to Jesus et al. (2018), blockchain technology enables for access and anonymity control in the Internet of Things since it is not controlled by a single point of failure or by a single entity. This enables the construction of decentralized services as well as the creation of new application types[16]. A feature of blockchain technology is its ability to divorce names records and characteristics from the availability of data, hence distinguishing control from data. In order to do this, it is constructed of two layers and one block that are conceptually isolated from the control plane, which is in charge of data storage. Name registration and link creation are governed by protocols defined by the control plane, which is comprised of a layer and a block that are conceptually isolated from the control plane, which is in charge of storage. Every piece of data stored as a consequence is signed with the name owner key, making it more difficult to hack as a result.

Further, Älvebrink and Maria Jansson (2018) show that blockchain can be integrated into IoT by using cloud infrastructure to allow blockchain to track items [17]. Blockchain technology is used in the strengthening of IoT security and is useful in storing information concerned with credentials and identity. With every transaction taking place in the open, interested parties are able to identify patterns, when analyzing data, and in so doing, it becomes possible to establish connections between addresses same time acquiring information based on their true identities. When used in securing IoT, blockchain technology utilizes its strong protection against tampering of data [18]. The strong protection locks access associated with internet of things devices and allows the shutting down of compromised devices within an IoT network[19].

Kshetri N et al. (2019) stated about the Blockchain implementation that is related to the decentralized approach for all of the networks. All of these networks can assist it in several ways. The proper security can be ensured by it in order to measure protection and privacy of data[20].

Taylor et al. (2020) provided framework for protection and solution can be provided by the block chain and it also offer privacy protection. This paper examines the major role of block chain for strengthening cyber security[21].

Abdulkader et al. (2019) particularly highlights that how block chain-based solutions can be possible by considering the various privacy and security issue [22].

Kshetri N et al. (2017) explains about the role of block chain for enhancing the cyber security solutions. It also explains the distributed solution for automotive privacy and security[23].

Neisse et al. (2019) study also explores the views about block chain based cyber security solution and it explains its implementations as well[24].

Khan Salah (2017) focuses on the blockchain based cybersecurity solution in IoT and provides effective solutions. The

insecure neighbor discovery issue is identified which is resolved by authentication using the Elliptic Curve Cryptography based signatures. In IoT devices, some privacy violations are also determined caused by Transport level end to end security which is resolved by applying DTLS and other protocols based on the security and authorization[25].

2 Issues and Vulnerabilities On different levels of IoT

Many layers of the Internet of Things (IoT)'s devices, systems, and networks are susceptible to various problems and security risks. The following are some of the problems and weaknesses that affect IoT at various levels:

- Internet of Things hardware is susceptible to physical assaults like theft, tampering, or devastation. Additionally, they may be vulnerable to software attacks like viruses, malware, or illegal access.
- IoT connectivity between devices can be intercepted, tampered with, or spoofed, which could result in data theft, unauthorized access, or other unlawful actions.
- DDoS attacks, which overload the network and make it crash or become inaccessible, can be used to compromise Internet of Things (IoT) networks.
- Applications for the Internet of Things (IoT) may be vulnerable to a range of security risks, such as unauthorized access, data breaches, and data tampering

There are various security issues in IoT which majorly include data privacy and Integration. Authentication and Authorization of data, service availability, energy consumption and single point of failure. These all issues are summarised in below table 1.Table 1 below shows Different issues on different layers of IoT and the significance of these issues on IoT layers with categorization of issue levels as low, Intermediate and high. There are three levels of IoT security concerns: low level, intermediate level, and high level[26].

Low-level: Physical layer and data link layer threats are categorized as low-level problems. These include physical interface security issues, spoofing attacks, jamming attacks, unsecure device initialization, and sleep deprivation attacks.

Intermediate Level: At the network and transport layers, issues with communication and routing are regarded as being of an intermediate level. Attacks using fragmentation-based duplication, identification of vulnerable neighbours, Attacks on cloud-based networks include attacks on location and identity, denial of service, buffer reservation, low power and lossy networks, sinkhole and wormhole attacks, device authentication, and secure communication.

High Level: These problems are caused by the IoT devices' applications. These include attacks on web, mobile, and cloud interfaces, issues with data privacy, attacks on insecure software and firmware, and issues with middleware security.

Table1. Issues on different layers of IoT and the significance of these issues on IoT layers

Author	Issue level	Issues	Significance	Layer of IoT
[27]–[29]	Low Level	The Jamming Adversaries.	Disruption and DoS	Physical
[30], [31]		The Low level Sybil and the spoofing attacks.	Network disruption, DoS	Physical
[32], [33]		Insecure Initialization.	Privacy violation and DoS	Physical
[34]		Insecure physical interfaces.	Privacy violation, DoS	Hardware
[35]		Sleep deprivation attacks	Energy consumption	Link
[36], [37]	Intermediate Level	Replay attacks due to disintegration.	Disruption and Dos	Network
[38]		Insecure neighbour discovery.	Ip Spoofing	Network
[37]		Buffer reservation attacks.	Blocking of reassembly buffer	Network
[39], [40]		RPL routing attack.	Eavesdropping and man-in-the-middle attacks	Network
[41]–[43]		Sinkhole and the wormhole attacks.	Dos	Network
[40], [44]		Sybil attacks.	Privacy violation, spamming, Byzantine faults, unreliable	Network
[45]		Authentication and the secure communication.	Privacy-violation	Transport layer, Network
[46], [47]		Transport level security.	Privacy-violation	Transport layer, Network
[48]–[50]		Session establishment and recommencement.	DoS	Transport layer, Network
[51]–[53]	High Level	CoAP security with internet.	Network bottleneck, DoS	Application layer, and network
[54]		Insecure interfaces	Privacy-violation, DoS, network disruptions	Application layer, and network
[34]		Insecure software or firmware	Privacy-violation, DoS, network disruptions	Application layer, and network
[55]–[57]		Middleware security issues	Privacy-violation, DoS, network disruptions	Application layer, and network

3. Cybersecurity Attacks at different levels of IoT

Today, the IoT is practically ubiquitous. As a result, in order to safeguard both the devices themselves and the data being gathered, businesses need to be aware of the various IoT cyber security threats. Table 2 shows cybersecurity attacks at different layers of issues and the details of attacks and its effect on each layer is given.

Types of Cybersecurity Attacks are:

1. Physical attacks: When anyone can physically access IoT devices, physical attacks happen. It's crucial that your IoT devices are in a protected area, which is frequently not an option, as the majority of cybersecurity attacks originate from within a company.
2. Encryption Attacks: Unencrypted IoT devices allow an intrusive party to sniff the data and capture it for use later. Furthermore, "cyber-assailants can install their own algorithms and take control of your system once encryption keys are unlocked." Because of these factors, encryption is essential for your IoT environment cyber security efforts.
3. Denial of Service (Dos): When a service, like a website, is rendered unavailable, a DoS attack happens. Through the use of a botnet, numerous systems attack a single target, causing a large number of devices to simultaneously request services. Attackers in this instance aren't typically looking to steal data, but if services are disrupted, they could have a significant negative impact on a company.
4. Firmware Hijacking: You run the risk of a cyber-security attack if you don't regularly update your IoT firmware. Verify that your updates are coming from the expected source; otherwise, a hacker could take over your device and install malicious software.
5. Man-in-the-middle attacks: When a hacker intercepts communications between two different systems, it is known as a man-in-the-middle attack. This kind of attack deceives the recipient into believing they are receiving a genuine message by covertly intercepting communications between two parties.
6. Ransomware: Malware known as ransomware encrypts files and restricts access to them. The attackers then offer to sell you the decryption key so that you can access your files once more. Naturally, this kind of attack can interfere with regular operations, and obtaining the encryption key is frequently very expensive. Imagine if hackers gained access to a power grid and held onto the keys for several days.
7. Eavesdropping: A hacker uses a weakened connection between an IoT device and a server in this type of attack to intercept network traffic and steal sensitive data. In order to eavesdrop, one usually listens to digital or analog voice communication or intercepts sniffed data. Once more, in this instance, the attacker makes off with sensitive, corporate information.

Table2. Cybersecurity issues at different layers of IoT

Cybersecurity Attacks in IoT at Sensing layer
Node Capturing: It is possible for the aggressors to try to capture or usurp a node in the Internet of Things system by using a pernicious or hazardous node. The new node will seem as a component of the framework; but, the cyber-aggressor has placed restrictions on it. This may lead to a trade-off between the overall security of the IoT system and other considerations.
Malicious Code Injection Attack: With the use of these programs, cybercriminals may persuade nodes to engage in certain undesired behaviours or even seek to get access to the whole Internet of Things network..
False Data Injection Attack: When a node is captured, the aggressor may utilize it to inject fake information into the IoT environment, which can be used to his advantage. This will result in erroneous results and may even result in the collapse of an IoT initiative.
Side-Channel Attacks (SCA): Side-channel assaults have the ability to trigger the disclosure of sensitive information. In addition to power consumption, laser-based attacks and electromagnetic assaults are all potential side-channel attack vectors that may be used.
Eavesdropping: Nodes in the Internet of Things are vulnerable to cyber-attacks. When data is being sent or validated, cyber-aggressors may eavesdrop and seize information. They can also interfere with the data transmission or validation. **Sleep Deprivation Attacks:** In the course of these attacks, the cyber-attackers make an effort to drain the batteries of the low-powered Internet of Things devices. A denial of service is triggered on the IoT System nodes as a result of a dead battery on one of the nodes. **Booting Attacks:** Edge devices are very susceptible to a wide range of assaults when they are in the process of starting up. It is possible that cyber-attackers will take advantage of this vulnerability and seek to enter the devices once they have been reset.
Cybersecurity Attacks in IoT at Network Layer
Phishing Site Attack: A client's identity and authentication are compromised, and as a result, the whole Internet of Things network that the firm relies on is now susceptible to attack. Phishing attacks may be launched with relative ease from the networking layer on up.
Access Attack: Advanced persistent threat is the term used to describe this kind of assault. This is a kind of attack in which the Internet of Things infrastructure is breached by someone who has not been granted permission to do so.
DDoS/DoS Attack: Attackers use this method to try to overwhelm a target database, which they do by sending a large number of unnecessary requests for operation to the database in question.
Data Transit Attacks: The Internet of Things (IoT) technologies are capable of storing and sharing a large amount of data. The need for constant access to data is critical, and as a consequence, cyber-attackers spend the bulk of their time and resources to it.
Routing Attacks: Malicious nodes are deployed over an IoT network via the transmission of information as part of such attacks in an attempt to block routing patterns.
Cybersecurity Attacks in IoT at Middleware Layer
Man-in-the-Middle Attack: With the MQTT protocol, subscribers and users communicate via a publish-and-subscribe model. In addition, the MQTT broker acts as an appropriate intermediary between the two sides. Furthermore, this assistance may be supplied without the recipient being aware of the decoupling of the publishing and subscribing entities from one another, and it may be provided without the recipient having any prior knowledge of the decoupling of the publishing and subscribing companies.
SQL Injection Attack: Attackers may use malicious SQL proclamations to infect software in order to take vengeance in this manner. As a result of this attack, the cyber-assailants will get access to each customer's personal information and will modify the information about the company that is contained in the database.
Signature Wrapping Attack: The cyber-attacker is able to conduct operations or edit eavesdropped messages by exploiting weaknesses in the basic Object Access Protocol while retaining the integrity of the signature code that was utilized in the signature wrapping cyber-attack, which is a kind of phishing attack.
Cloud Malware Injection: In certain cases, the attacker may seize control of the program, inject malicious code into the program, or inject a virtual machine into the software, depending on how the situation is handled. The attacker may inspect the target's service requests and collect sensitive information that can be updated by the case manager if

the attacker employs this technique of attack.
Flooding Attack in Cloud: There is a significant effect on the quality of service due to this assault, which functions in a way that is almost comparable to the cloud DoS attack in terms of operation. When cloud services are entirely drained, the aggressors submit a constant stream of support requests, which are answered repeatedly.
Replay attack: Data packets are intercepted and sent to their intended destinations without being altered in any manner by attackers in order to disturb the consistency of two interacting entities.
Impersonation Attack: It is possible to commit an intrusion by impersonator, which is a kind of attack in which an attacker tries to assume the identities of authorized entities in a scheme or protocol by adopting their physical appearance.
Cybersecurity Attacks in IoT at Application Layer
Data Thefts: The Internet of Things (IoT) services must be able to deal with a huge volume of sensitive data on a regular basis. However, despite the fact that vast volumes of information are being transferred through IoT services, information sent while traveling is far more vulnerable to cyber-attacks than information sent when at home
Access Control Attacks: It is a kind of permission software that limits access to information or accounts to only legitimate customers or processes. It is also known as access control software. When it comes to Internet of Things systems, attacking the Access Management system is a key assault because once security is penetrated, the whole IoT infrastructure becomes vulnerable to cyberattacks.
Service Interruption Attacks: They are also fairly similar to unlawful invasions and distributed denial of service (DDoS) assaults, which are also forms of cybercrime. Attacks against Internet of Things systems have been carried out in a number of cases in which they are comparable.
Malicious Code Injection Attacks: Cyber-assailants are always on the hunt for the fastest and most basic method of infiltrating a network or software program. If the code tests are inadequate and the system is exposed to malicious material, a cyber-assailant will use this area as the principal entry point into the system.
Sniffing Attacks: Scanning devices, often known as sniffers, are instruments used by cyber-assailants to monitor the network traffic of the Internet of Things architecture. Attackers will be able to get personal customer information if there are inadequate defensive measures in place to prevent it.
Reprogram Attacks: If the software design of IoT devices is not adequately safeguarded, attackers may attempt to remotely reprogram the devices.

The Internet of Things (IoT) is a system that includes interconnected physical objects, such as cars, buildings, and other physical objects, that can collect and exchange data. These objects are embedded with electronics, software, sensors, and network connectivity. IoT security vulnerabilities can happen at various layers of the IoT architecture. Here are some examples:

1. Sensing Layer: Attackers can take control of IoT devices directly at this layer. They can, for instance, take or copy IoT devices, extract data or credentials from them, or tamper with the hardware to change how the devices behave.
   Attackers have the ability to eavesdrop on communication between IoT devices and gateways at this layer. They are capable of conducting man-in-the-middle attacks, listening in on data transmissions, and inserting malicious packets into data streams.
2. Network Layer: Attackers can take advantage of limitations in the network infrastructure connecting IoT devices at this layer. For instance, they could penetrate the network perimeter, start denial-of-service attacks, or gain unauthorized access to network resources. Attackers have the ability to eavesdrop on communication between IoT devices and gateways at this layer. They are capable of conducting man-in-the-middle attacks, listening in on data

transmissions, and inserting malicious packets into data streams.

3. Middleware Layer: Attackers can take advantage of issues in the protocols used to transfer data between IoT devices and servers at this layer. For instance, they can use session hijacking strategies to access IoT data or launch attacks on the transport layer security (TLS) protocol.
4. Application Layer: Attackers can take advantage of shortcomings in the software applications that are installed on servers or IoT devices at this layer. For instance, they can use social engineering strategies to manipulate users into disclosing sensitive information, launch SQL injection attacks, or exploit buffer overflow problems.

Effective safety precautions must be put in place at every layer of the IoT architecture in order to reduce the risk of cyberattacks on IoT.

4 Categorization of Issues/Attacks.

Devices that are part of the IoT (Internet of Things) usually consist of up of several layers, each with a distinct function and purpose. IoT security can be increased by categorizing problems and attacks across different IoT layers to help find possible vulnerabilities. Here are a few instances of problems and assaults that may happen in various IoT layers:

Sensing Layer:

- Unauthorized access to the physical device or sensor
- Physical tampering with the device or sensor
- Eavesdropping on the wireless communication between devices

Network Layer:

- Denial-of-service (DoS) attacks, where an attacker floods the network with traffic to make it unavailable.
- Routing attacks, where an attacker manipulates the routing of data to redirect it to a malicious destination.
- Network sniffing attacks, where an attacker monitors the network traffic to capture sensitive information.
- Spoofing attacks, where an attacker pretends to be a legitimate device to gain access to the network.
- Jamming attacks, where an attacker floods the network with noise to disrupt communication.
- Man-in-the-middle attacks, where an attacker intercepts and modifies data exchanged between devices.

Middleware Layer:

- TCP/IP attacks, where an attacker exploits vulnerabilities in the TCP/IP protocol stack to gain unauthorized access to the device or network.
- SSL/TLS attacks, where an attacker exploits weaknesses in SSL/TLS encryption to intercept and modify data in transit.
- DDoS attacks, where multiple devices are used to flood a target with traffic to make it unavailable.

Application Layer:

- SQL injection attacks, where an attacker injects malicious SQL code into a web application to gain access to the underlying database
- Cross-site scripting (XSS) attacks, where an attacker injects malicious scripts into a web page viewed by other users.
- Remote code execution attacks, where an attacker gains unauthorized access to a device or network by executing malicious code through a vulnerability in an application.

Figuring out possible risks and weaknesses connected to each layer of IoT devices is crucial, as is putting the right security measures in place to reduce these risks.Table3 below, we have categorised Issues with description and under which category of layers they fall. Based on the description of issue and category it falls we will try to find possible blockchain solution.

Table 3. Categorization of issues and related layer in IoT

Issue	Description	Category
• Jamming adversaries • Insecure initialization Configuration • Sleep deprivation attack • Side channel Attack • Node capture and Timing Attacks	Confidentiality	Sensing
• Low level Sybil and spoofing attacks • Disruption and denial-of-service • IP-Spoofing • Blocking of reassembly buffer • Eavesdropping, man-in-the-middle attacks Sybil attacks	Confidentiality, privacy and compatibility	Network
• Authentication and secure communication • Transport level end-to-end security • Session establishment and resumption • Malicious Insider • Man in the middle attack • Virtualization Threat Third party relationship	Authenticity, integrity , Availability and Confidentiality	Middleware
• Insecure interfaces • Insecure software/firmware • Middleware security • Malicious Scripts Unauthorized Access	Data privacy and identity authentication	Application

5 Blockchain based methods to countermeasure Cybersecurity attacks.

IoT device management and security will be greatly aided by blockchain, which is regarded as an emerging technology. Table 4 below shows possible blockchain based methods used to counter measure different attacks at different layers of IoT. IoT security issues can be resolved using blockchain technology. The following list includes a few blockchain features important for IoT security.

- Blockchain technology can be used to register and identify IoT network devices.

IoT devices have properties, connections, capabilities, and features. Devices can interact with one another, with people, and with services. Blockchain technology provides a solution to these problems.

- Security features based on cryptographic algorithms are inherent benefits of using Blockchain technology to connect IoT devices. When the sender and user identities are verified and authenticated by the Blockchain network, the integrity and authentication of transmitted data is ensured. On the common database known as ledger, all communications and data transactions would be documented and tracked.
- The functionality of decentralized authentication rules and logic for IoT device authentication is provided by blockchain networks for smart contracts. Smart contracts provide simpler authentication rules than conventional authorization protocols.
- Based on smart contracts by managing and controlling user rights, such as the ability to upgrade software, apply software patches, and manage IoT device software or hardware-related operations, blockchain networks maintain data privacy.
- The security of IoT communication protocols is not intended. To make IoT device communication secure, additional steps must be taken, adding to the computational burden. Blockchain networks simplify security protocols, making them better suited for Internet of Things (IoT) devices with constrained memory and processing power[58].

Table4. Possible blockchain based methods used to counter measure different attacks in IoT layers

Reference	Focus	Framework/system	Tool	Strength	Access	Method
[59]	According to this study, blockchain technology should be used to give nodes a way to check the legitimacy and integrity of firmware before downloading it, while also making sure that the firmware is easy to find.	System	Ethereum	A system for safe software update was developed, in which the IPFS and Ethereum were utilized to store the software file, ensuring that the program is highly available and that its integrity is maintained.	-	Smart contract
[60]	People are working on a project called "data-preserving AI." They want to build an AI system that can keep learning data safe for future use by using a blockchain-based learning data environment model to check the integrity of the learning data.	Framework	-	According to expectations, it will aid in the prevention of dangers such as cyberattacks and data degradation.	-	Smart contract
[24]	As a response to the recent Defence Cooperation Act, we've come up with a blockchain-based platform that would make cybersecurity certification information more transparent and traceable while also cutting down on the costs of doing so.	Framework	Hyperledger blockchain	Expected to increase users' trust in the digital era.	private	Smart contract
[2]	In this article, we'll show you how to build an Internet of Things architecture that doesn't use a lot of resources but still has a lot of the security and privacy advantages of traditional Blockchain.	Framework	Simulator NS3	The design's security and privacy are examined, with the results demonstrating the new architecture's resistance to a variety of threats.	Public	Distributed trust method
[61]	Data created by personal IoT devices will be safely kept in an open, distributed system whose architecture ensures anonymity, enabling individuals, the true data owners, to select who they want to share their data with and when.	Architecture	Blockchain Bitcoin	Security and privacy	-	Public key cryptography
[62]	It is our intention to conduct a full security analysis of our planned BC-based smart home system in order to demonstrate its safety in terms of core security objectives such as confidentiality, integrity and availability.	Architecture	Simulator NS3	Confidentiality,Intergity,availability, user control and authentication	-	Symmetric encryption and hashing
[63][64]	We've developed a blockchain-based, quick-to-implement system for controlling access to the Internet of Things.	Framework	Bitcoin and smart contract	Access control, security , privacy	Public	Proof of concept
[65][66]	A distributed IoT network design based on blockchain technology should be implemented at several levels of security,	Model	Smart contract	Privacy , authentication	Private	Proof of existence

	according to the conclusions of this study.					
[67][68]	Ethereum is built on the Ethereum blockchain, and we created and implemented an integrity-first communication protocol for the Internet of Things that is distributed and scalable on Ethereum.	protocol	Ethereum	Address the problems with communication integrity for IoT devices.	public	proof of work consensus algorithm
[69][64]	For this purpose, we have developed and prototyped an edge-IoT framework dubbed "EdgeChain," which is built on blockchain technology and smart contracts.	Framework	Ethereum	security , privacy	Private	Smart contract
[70][71]	EdgeChain, an edge-IoT framework based on blockchain technology and smart contracts, is being developed and prototyped to address the issues stated above[71].	Framework	NS2 simulator	security , privacy	public	Smart contract

As a whole, blockchain technology has the potential to improve cybersecurity by offering a secure and decentralized method of data transmission, verification, and storage.

6 Conclusion

The security limitations of IoT technology have recently been improved by using blockchain technology. The decentralized aspects of blockchain technology, the distributed nature of the network, the shared resources, and the immutable data transfer are just a few of the characteristics that could increase the security of IoT devices with limited resources. The solutions examined in this review paper use blockchain technology to improve data privacy and anonymity, authentication and identity management, data integrity, availability, and confidentiality. As a result of this inquiry, current research on how blockchain technology may aid in the resolution of cyber security challenges has been identified, and as a result of the discoveries, this research has been made publically available for viewing. The scope of this inquiry has been reduced to just cover cyber security as a part of its examination. The usage of blockchain technology is undeniably practical. However, the technologies decentralized, trustless nature does not allow it to effectively solve all of the difficulties that may emerge in the field of information security, and here is where it falls short of the mark. The growing popularity of blockchain applications has increased support for existing measures to strengthen security and prevent hostile actors from participating in cyber security activities, which is encouraging. As a consequence of the findings of this study, it is possible that future research in the field of cyber security will be conducted in areas that are not directly connected to the Internet of Things. In order for the World Wide Web to continue to evolve toward widespread use of https encryption, and as end users become more reliant on some form of encryption for their regular interactions, it is becoming increasingly important to manage the cryptography and certification systems that surround them in a secure manner.

7 Future work

There is an ongoing need for research and development into cybersecurity problems and solutions as the Internet of Things (IoT) expands and blockchain technology spreads. Overall, research in this area is crucial for ensuring the security and integrity of IoT systems in the future. Blockchain-based cybersecurity solutions for IoT devices are currently being developed and improved. In relation to the subject of cybersecurity issues in IoT and blockchain-based solutions, the following are some potential future research areas:

- Creation of more reliable blockchain-based security solutions: Although blockchain technology can offer an IoT device security framework, there is still room for advancement. Research in the future may concentrate on creating more reliable blockchain-based security solutions that can better defend against new threats to cybersecurity.
- Lack of standardization in IoT device cybersecurity protocols: Currently, IoT device cybersecurity protocols are not standardized. Future research can concentrate on creating uniform cybersecurity protocols that can be applied to various IoT platforms and devices.

- Integration of machine learning (ML) and artificial intelligence (AI) into cybersecurity: ML and AI can be used to identify and address cybersecurity threats instantly. In order to improve the effectiveness of blockchain-based cybersecurity solutions, future research can concentrate on integrating AI and ML into them.
- The impact of blockchain-based cybersecurity solutions is evaluated: Despite the potential of blockchain-based cybersecurity solutions, ongoing testing is necessary to determine how well they perform in practical situations.
- Establishment of approachable cybersecurity solutions based on blockchain: The implementation and understanding of blockchain-based cybersecurity solutions can be challenging for non-technical users. Future research can concentrate on creating straightforward cybersecurity solutions based on blockchain that is simple to use and implement for a wider range of members.

- **References**

[1] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.2022.

[2] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," *Proc. - 2017 IEEE/ACM 2nd Int. Conf. Internet-of-Things Des. Implementation, IoTDI 2017 (part CPS Week)*, no. April, pp. 173–178, 2017, doi: 10.1145/3054977.3055003.

[3] J. Hayat Mosakheil, "Security Threats Classification in Blockchains," 2018.

[4] T. R. Vance and A. Vance, "Cybersecurity in the Blockchain Era," pp. 107–112, 2019.

[5] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustain. Cities Soc.*, vol. 50, no. August 2018, p. 101660, 2019,doi: 10.1016/j.scs.2019.101660.

[6] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, 2018, doi: 10.1109/JIOT.2017.2767291.

[7] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electr. Power Syst. Res.*, vol. 215, no. July 2022, 2023,doi:10.1016/j.epsr.2022.108975.

[8] Taherdoost, H. Security and Internet of Things: Benefits, Challenges, and Future Perspectives. *Electronics* 2023, *12*, 1901. https://doi.org/10.3390/electronics12081901.

[9] G. Janani Alias Pandeeswari and D. M. D. Preethi, "Investigation of Security Concerns and Solutions for the Internet of Things," *Proc. 3rd Int. Conf. Artif. Intell. Smart Energy, ICAIS 2023*, no. Icais, pp. 158–163, 2023, doi: 10.1109/ICAIS56108.2023.1007366.

[10] S. N. G. Aryavalli and H. Kumar, "Top 12 layer-wise security challenges and a secure architectural solution for Internet of Things,"

Comput. Electr. Eng., vol. 105, no. November 2022, p. 108487, 2023, doi:10.1016/j.compeleceng.2022.108487.

[11] T. Alam, "Blockchain-Based Internet of Things: Review, Current Trends, Applications, and Future Challenges," *Computers*, vol. 12, no. 1, 2023, doi: 10.3390/computers12010006.

[12] M. Al-Shabi and A. Al-Qarafi, "Improving blockchain security for the internet of things: challenges and solutions," *Int. J. Electr. Comput. Eng.*, vol. 12, no. 5, pp. 5619–5629, 2022,doi:10.11591/ijece.v12i5.pp5619-5629.

[13] M. S. Mahmood and N. B. Al Dabagh, "Blockchain technology and internet of things: review, challenge and security concern," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 1, pp. 718–735,2023,doi:10.11591/ijece.v13i1.pp718-735.

[14] M. Samaniego and R. Deters, "Blockchain as a Service for IoT," *Proc. - 2016 IEEE Int. Conf. Internet Things; IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016*, no. January 2020, pp. 433–436, 2017,doi:10.1109/iThings GreenCom-CPSCom-SmartData.2016.102.

[15] E. F. Jesus, V. R. L. Chicarino, C. V. N. De Albuquerque, and A. A. D. A. Rocha, "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack," *Secur. Commun. Networks*, vol. 2018, 2018, doi: 10.1155/2018/9675050.

[16] S. Katsikeas, P. Johnson, M. Ekstedt, and R. Lagerström, "Research communities in cyber security: A comprehensive literature review," *Comput. Sci. Rev.*, vol. 42, p. 100551, 2021, doi: 10.1016/j.cosrev.2021.100431.

[17] J. Älvebrink and M. Jansson, "Investigation of blockchain applicability to Internet of Things within supply chains Masterprogram i industriell ledning och innovation Master Programme in Industrial Management and Innovation," 2018.

[18] K. Košt'ál, P. Helebrandt, M. Belluš, M. Ries, and I. Kotuliak, "Management and monitoring of IoT devices using blockchain," *Sensors (Switzerland)*, vol. 19, no. 4, Feb. 2019, doi: 10.3390/s19040856.

[19] M. Hosseini Shirvani and M. Masdari, "A survey study on trust-based security in Internet of Things: Challenges and issues," *Internet of Things (Netherlands)*, vol. 21, no. November 2022, p. 100640, 2023, doi: 10.1016/j.iot.2022.100640.

[20] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," *IT Prof.*,vol.19,no.4, pp. 68–72, 2017,doi:10.1109/MITP.2017.3051335.

[21] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, "A systematic literature review of blockchain cyber security," *Digital Communications and Networks*, vol. 6, no. 2. Chongqing University of Posts and Telecommunications, pp. 147–156, 01-May-2020,doi: 10.1016/j.dcan.2019.01.005.

[22] O. Abdulkader, A. M. Bamhdi, V. Thayananthan, F. Elbouraey, and B. Al-Ghamdi, "A Lightweight Blockchain Based Cybersecurity for IoT environments," in *Proceedings - 6th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2019 and 5th IEEE International Conference on Edge Computing and Scalable Cloud,*

EdgeCom 2019, 2019, pp. 139–144, doi:10.1109/CSCloud/EdgeCom.2019.000-5.

[23] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecomm. Policy*, vol. 41, no. 10, pp. 1027–1038,Nov.2017,doi:10.1016/j.telpol.2017.09.003.

[24] R. Neisse, J. L. Hernández-Ramos, S. N. Matheu, G. Baldini, and A. Skarmeta, "Toward a Blockchain-based Platform to Manage Cybersecurity Certification of IoT devices," 2019.

[25] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions,and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.2022.

[26] M. N. Al Dalaien, S. A. Hoshang, A. Bensefia, and A. R. A. Bathaqili, "Internet of Things (IoT) security and privacy," *Powering Internet Things With 5G Networks*, no. April, pp. 247–267, 2017, doi: 10.4018/978-1-5225-2799-2.ch010.

[27] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2005, pp. 46–57, doi: 10.1145/1062689.1062697.

[28] G. Noubir and G. Lin, "Low-power DoS attacks in data wireless LANs and countermeasures," *ACM SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 7, no. 3, pp. 29–30, Jul. 2003, doi: 10.1145/961268.961277.

[29] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats," in *Proceedings of the 2004 ACM workshop on Wireless security - WiSe '04*, 2004, p. 80, doi: 10.1145/1023646.1023661.

[30] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," in *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON*, 2007, pp. 193–202, doi: 10.1109/SAHCN.2007.4292831.

[31] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of sybil attacks in wireless networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 3, pp. 492–503, Sep. 2009, doi: 10.1109/TIFS.2009.2026454.

[32] Y. W. P. Hong, P. C. Lan, and C. C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, 2013, doi: 10.1109/MSP.2013.2256953.

[33] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 10, pp. 1617–1628, Oct.2014,doi:10.1109/TIFS.2014.2341453.

[34] "OWASP Internet of Things," 2018. [Online].Available: https://owasp.org/www-project-internet-of-things/. [Accessed: 23-Oct-2020].

[35] T. Bhattasali and R. Chaki, "A survey of recent intrusion detection systems for wireless sensor network," in *Communications in Computer and Information Science*, 2013, vol. 196 CCIS, pp. 268–280, doi: 10.1007/978-3-642-22540-6_27.

[36] H. G. Kim, "Protection against packet fragmentation attacks at 6LoWPAN adaptation layer," in *Proceedings - 2008 International Conference on Convergence and Hybrid Information Technology, ICHIT 2008*, 2008, pp. 796–801, doi: 10.1109/ICHIT.2008.261.

[37] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, "6LoWPAN fragmentation attacks and mitigation mechanisms," in *WiSec 2013 - Proceedings of the 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2013, pp. 55–66, doi: 10.1145/2462096.2462107.

[38] R. Riaz, K. H. Kim, and H. F. Ahmed, "Security analysis survey and framework design for IP connected LoWPANs," in *Proceedings - 2009 International Symposium on Autonomous Decentralized Systems, ISADS 2009*, 2009, pp. 29–34, doi: 10.1109/ISADS.2009.5207373.

[39] A. Dvir, T. Holczer, and L. Buttyan, "VeRA - Version number and rank authentication in RPL," in *Proceedings - 8th IEEE International Conference on Mobile Ad-hoc and Sensor Systems, MASS 2011*, 2011, pp. 709–714, doi: 10.1109/MASS.2011.76.

[40] Xiao wang, "Social Turing Tests: Crowdsourcing Sybil Detection – NDSS Symposium," 2013. [Online]. Available: https://www.ndss-symposium.org/ndss2013/ndss-2013-programme/social-turing-tests-crowdsourcing-sybil-detection/. [Accessed: 23-Oct-2020].

[41] K. Weekly and K. Pister, "Evaluating sinkhole defense techniques in RPL networks," in *Proceedings - International Conference on Network Protocols, ICNP*, 2012, doi: 10.1109/ICNP.2012.6459948.

[42] F. Ahmed and Y.-B. Ko, "Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks," *Secur. Commun. Networks*, vol. 9, no. 18, pp. 5143–5154, Dec. 2016, doi: 10.1002/sec.1684.

[43] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, "The impact of rank attack on network topology of routing protocol for low-power and lossy networks," *IEEE Sens. J.*, vol. 13, no. 10, pp. 3685–3692, 2013, doi: 10.1109/JSEN.2013.2266399.

[44] W. Wang, J. Kong, B. Bhargava, and M. Gerla, "Visualisation of wormholes in underwater sensor networks: A distributed approach," *Int. J. Secur. Networks*, vol. 3, no. 1, pp. 10–23, 2008, doi: 10.1504/IJSN.2008.016198.

[45] J. Granjal, E. Monteiro, and J. S. Silva, "Network-layer security for the Internet of Things using TinyOS and BLIP," *Int. J. Commun. Syst.*, vol. 27, no. 10, pp. 1938–1963, Oct. 2014, doi: 10.1002/dac.2444.

[46] Martina Brachmann, "(13) (PDF) Security for Practical CoAP Applications: Issues and Solution Approaches," 2103. [Online]. Available: https://www.researchgate.net/publication/265973615_Security_for_Practical_CoAP_Applications_Issues_and_Solution_Approaches. [Accessed: 23-Oct-2020].

[47] Ajit A.Chavan, "Secure CoAP Using Enhanced DTLS for Internet of Things | Open Access Journals," 2014. [Online]. Available: https://www.rroij.com/open-access/secure-coap-using-enhanced-dtls-forinternet-of-things-.php?aid=47629. [Accessed: 23-Oct-

2020].

[48] N. Park and N. Kang, "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle," *Sensors*, vol. 16, no. 1, p. 20, Dec. 2015, doi: 10.3390/s16010020.

[49] M. Hamada Ibrahim, "Octopus: An Edge-Fog Mutual Authentication Scheme," 2016.

[50] R. Hummen, H. Wirtz, J. H. Ziegeldorf, J. Hiller, and K. Wehrle, "Tailoring end-to-end IP security protocols to the internet of things," in *Proceedings - International Conference on Network Protocols, ICNP*, 2013, doi: 10.1109/ICNP.2013.6733571.

[51] M. Brachmann, O. Garcia-Morchon, S.-L. Keoh, and S. S. Kumar, "Security Considerations around End-to-End Security in the IP-based Internet of Things," 2012.

[52] J. Granjal, E. Monteiro, and J. S. Silva, "Application-layer security for the WoT: Extending CoAP to support end-to-end message security for internet-integrated sensing applications," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2013, vol. 7889 LNCS, pp. 140–153, doi: 10.1007/978-3-642-38401-1_11.

[53] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar, "End-to-end transport security in the IP-based internet of things," in *2012 21st International Conference on Computer Communications and Networks,ICCCN2012Proceedings*,2012,doi:10.1109/ICCCN.2012.6289292.

[54] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," in *Proceedings - IEEE 7th International Conference on Service-Oriented Computing and Applications, SOCA 2014*, 2014, pp. 230–234, doi: 10.1109/SOCA.2014.58.

[55] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, and M. A. Spirito, "The VIRTUS middleware: An XMPP based architecture for secure IoT communications," in *2012 21st International Conference on Computer Communications and Networks, ICCCN 2012 - Proceedings*, 2012, doi: 10.1109/ICCCN.2012.6289309.

[56] A. Gómez-Goiri, P. Orduña, J. Diego, and D. López-De-Ipiña, "Otsopack: Lightweight semantic framework for interoperable ambient intelligence applications," *Comput. Human Behav.*, vol. 30, pp. 460–467, Jan. 2014, doi: 10.1016/j.chb.2013.06.022.

[57] H. G. C. Ferreira, R. T. De Sousa, F. E. G. De Deus, and E. D. Canedo, "Proposal of a secure, deployable and transparent middleware for Internet of Things," in *Iberian Conference on Information Systems and Technologies, CISTI*, 2014, doi: 10.1109/CISTI.2014.6877069.

[58] Y. Lu and L. Da Xu, "Internet of things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, 2019, doi: 10.1109/JIOT.2018.2869847.

[59] N. Mtetwa, P. Tarwireyi, and M. Adigun, "Secure the Internet of Things Software Updates with Ethereum Blockchain," *Proc. - 2019 Int. Multidiscip. Inf. Technol. Eng. Conf. IMITEC 2019*, 2019, doi: 10.1109/IMITEC45504.2019.901585.

[60] J. Kim and N. Park, "Blockchain-based data-preserving AI learning environment model for AI cybersecurity systems in IoT service environments," *Appl. Sci.*, vol. 10, no. 14, 2020, doi: 10.3390/app10144718.

[61] M. Conoscenti, A. Vetro, and J. C. De Martin, "Peer to peer for privacy and decentralization in the internet of things," *Proc. - 2017 IEEE/ACM 39th Int. Conf. Softw. Eng. Companion, ICSE-C 2017*, pp. 288–290, 2017, doi: 10.1109/ICSE-C.2017.60.

[62] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2017*, no. March, pp. 618–623, 2017, doi: 10.1109/PERCOMW.2017.7917634.

[63] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: a new Blockchain-based access control framework for the Internet of Things," *Secur. Commun. Networks*, vol. 9, no. 18, pp. 5943–5964, 2016, doi: 10.1002/sec.1748.

[64] F. A. Reegu, S. M. Daud, S. Alam, and M. Shuaib, "Blockchain-based Electronic Health Record System for efficient Covid-19 Pandemic Management," 2021, doi: 10.20944/preprints202104.0771.v1.

[65] C. Li and L. J. Zhang, "A blockchain based new secure multi-layer network model for internet of things," *Proc. - 2017 IEEE 2nd Int. Congr. Internet Things, ICIOT 2017*, pp. 33–41, 2017, doi: 10.1109/IEEE.ICIOT.2017.34.

[66] F. A. Reegu, M. O. Al-Khateeb, W. A. Zogaan, M. R. Al-Mousa, S. Alam, and I. Al-Shourbaji, "Blockchain-Based Framework for Interoperable Electronic Health Record," *Ann. Rom. Soc. Cell Biol.*, pp. 6486–6495, 2021.

[67] E. Reilly, M. Maloney, M. Siegel, and G. Falco, "An iot integrity-first communication protocol via an ethereum blockchain light client," *Proc. - 2019 IEEE/ACM 1st Int. Work. Softw. Eng. Res. Pract. Internet Things, SERP4IoT 2019*, pp. 53–56, 2019,doi:10.1109/SERP4IoT.2019.00016.

[68] shadab alam faheem reegu, salwani daud, zaid hakami, Kaiser kareem reegu, "Towards Trustworthiness of Electronic Health Record system using Blockchain," *Ann. RSCB*, vol. 25, no. 6, 2021.

[69] G. Sargsyan, N. Castellon, R. Binnendijk, and P. Cozijnsen, "Blockchain security by design framework for trust and adoption in IoT environment," *Proc. - 2019 IEEE World Congr. Serv. Serv. 2019*, pp. 15–20, 2019, doi: 10.1109/SERVICES.2019.00018.

[70] G. Rathee, A. Sharma, R. Kumar, and R. Iqbal, "A Secure Communicating Things Network Framework for Industrial IoT using Blockchain Technology," *Ad Hoc Networks*, vol. 94, p. 101933, 2019, doi: 10.1016/j.adhoc.2019.101933.

[71] F. Reegu, W. Khan, … S. D.-… C. on R., and undefined 2020, "A Reliable Public Safety Framework for Industrial Internet of Things (IIoT)," *ieeexplore.ieee.org*.

مراجعة لقضايا الأمن السيبراني المحتملة في إنترنت الأشياء والحل القائم على البلوكشين Blockchain

عبده محمد جباري

كلية علوم الحاسب وتقنية المعلومات، جامعة جازان، المملكة العربية السعودية

الملخص

كانت البلوكشين (Blockchain) أكثر شهرة منذ ظهور الورقة البيضاء لساتوشي ناكاموتو في عام ٢٠٠٨؛ منذ ذلك الحين ، أصبحت واحدة من أكثر الطرق التي تمت مناقشتها في كثير من الأحيان للحفاظ على تخزين البيانات ونقلها عبر شبكات لا مركزية وغير موثوقة من نظير إلى نظير. يتم توفير تقييم شامل لكل من مزايا وعيوب تطبيقات أمان blockchain الأكثر استخدامًا في هذا البحث. بالإضافة إلى ذلك ، تم تسليط الضوء على الأبحاث التي تمت مراجعتها من قبل الأقران حول استخدام تقنية blockchain للأمن السيبراني. استنادًا إلى نتيجة المراجعة ، يبدو أن إنترنت الأشياء ((IoTمنصة ممتازة لتطوير تطبيقات blockchain المبتكرة ، خاصة للتطبيقات الصناعية. تتضمن هذه التقنيات تصور الشبكة والآلة ، وتشفير المفتاح العام ، والتطبيقات عبر الإنترنت ، وأنظمة الشهادات ، والتخزين الآمن للمعلومات الشخصية. بالإضافة إلى ذلك ، يوفر البحث الحالي نافذة على اتجاهات الدراسة المستقبلية. الهدف الرئيسي من هذه المراجعة هو عرض تحديات وقضايا الأمان المختلفة على طبقات مختلفة من هندسة إنترنت الأشياء والحلول الممكنة لها. استعرضت هذه الورقة التطورات الأمنية الأخيرة للتغلب على قيود إنترنت الأشياء باستخدام .blockchainفي هذه المقالة ، تحاول blockchain التغلب على قيود إنترنت الأشياء المتعلقة بالأمن السيبراني.

الكلمات المفتاحية: *انترنت الأشياء، الامن السيبراني، البلوكشين (*Blockchain*)*

Comparative Study of Machine Learning and Deep Learning models to Detect Breast Cancer

Faisal Alshanketi *

Department of Computer Science Jazan, University Jazan, KSA

Abstract

Breast cancer is the most frequent cancer in women and causes the maximum number of cancer deaths. Initially, the primary diagnostic mechanisms for detecting breast cancer were mammography and ultrasound. These images were supposed to be manually investigated by expert medical practitioners to identify the malignant tumour. The primary concern in these manual investigations is the accuracy that depends on the availability of specialist medical practitioners in the domain. Finding such experts will be difficult for the large population when breast cancer is rising sharply. Much progress in medical imaging and healthcare technology has taken place, and much research has been done in this domain. Machine learning and deep learning techniques have been successfully applied to predict whether a tumour is malignant or benign in the initial stage to save women's lives. However, there is still a great chance to improve the prediction accuracy to reduce the required time and data to train the model. In this study, we show that by using machine learning and deep learning models to predict whether a tumour is malignant or benign in the initial stage to save women's lives. We compare nine traditional machine learning classifiers against deep learning models that lead to achieving higher accuracy performance for predicting breast cancer. We study splitting data into (80% and 20%) sets and 10-fold cross-validation techniques. Experimental evaluation is based on the public breast cancer dataset. The best performance overall was achieved using the deep learning (Sequential Neal Network) algorithm, with an accuracy of 99.12%.

Keywords: Wisconsin Diagnostic Breast Cancer (WDBC), Breast cancer, Machine Learning and Deep Learning, Detect Breast Cancer.

1. Introduction

Breast cancer (BC) early identification has a substantial impact on lowering the disease's mortality rate. Globally, BC has a severe effect on women, leading to death as a second causing of death, and early detection is critical for reducing this high mortality rate. Unfortunately, BC has no recognized reason, and many cause women get the disease without exhibiting symptoms. Early detection, enabled by routine breast screening, allows earlier treatment, particularly for those with a high or average risk of developing BC. According to [1], women in America were projected to have 268,600 new positive BC cases and 62,930 new BC instances that are not invasive. BC accounts for 23% of all cancer cases in developing nations, and women are projected to be diagnosed with the disease every year [1–3]. In 2016, roughly 29% of female fatalities were attributed to BC. In 2016, 595,690 Americans died from cancer, or 1,600 every day [4]. Since 2001, the number of breast cancer diagnoses among Saudi women has more than tripled, from 545 instances to 2463 in 2017. This is a 351.9% increase [5].

Because of regular progress in early tumor diagnosis, the death rate from BC has been progressively reducing at a pace of around 1% each year. Since 2010, almost 7 million women have been diagnosed with BC, and it is expected that 23% of all women will be diagnosed with BC in 2022 [6]. Unfortunately, the etiology of BC is unknown, and many women have the condition without realizing it. Regular screenings may help find problems before they become serious, and if BC is caught early, the five-year survival rate is about 100% [7]. So that a patient with a benign tumor does not endure unneeded therapy, it is important to determine whether or not a tumor is malignant if one is found. In order to better diagnose BC, we are interested in analyzing dataset that has been processed by machine learning (ML) approaches, which may aid doctors in determining if a tumor is benign or malignant. We begin with the Wisconsin Diagnostic Breast Cancer (WDBC) dataset that includes information that may be diagnostic of BC.

Several variables contribute to the development of BC. These include genetic predisposi- tions, obesity, hormones, radiation treatment, and reproductive aspects. The World Health Agency estimates that one million women are newly diagnosed with BC yearly, with half of them dying due to the illness being detected late [8] according to a study by the organiza- tion. When a mistake or mutation occurs in one cell, the system may either shut down the cell or induce a rash of cell proliferation. This process generates BC. Masses may grow from cells that have incorrect instructions if the issue is not resolved after many months.

In contrast to malignant tumors, which may spread to nearby cells and other body sections, benign masses cannot spread to other tissues, and their growth is thus restricted to the soft group [9, 10]. Detecting BC in the early stage seems to be difficult because of the lack of symptoms at the onset of the illness. However, following a series of clinical testing, a correct diagnosis should be able to distinguish between benign and malignant tumors, allowing for earlier treatment. An efficient detection system has a miner error rate, including false positives and false negatives [11].

Accurate diagnosis and treatment of the disease may reduce mortality and enable rapid treatment. BC is diagnosed and

discovered via imaging, physical examination, and biopsy [12]. Mammography and ultrasound are used to identify BC. This procedure uses X-rays to make breast pictures. Mammograms are these images—radiologists who interpret mammograms to detect BC. Radiologists can explain the screening technique's effective-

ness [13]. Patients with palpable BC may have regular mammography sonograms and mammography with delicate or nonspecific appearance [14]. It is an invasive surgical procedure with psychological and physical effects on patients.

Moreover, depending on the breast density, radiologists may miss up to 30% of BC [15]. Masses and micro calcifications are important indications used to analyze mammography in BC. A mammogram's mass identification is more complex than micro-calcification detection because masses generally have low image contrast [16]. Radiologists interpret mammograms based on subjective factors and experience. Even skilled specialists might have inter-observer variances of 65-75 percent [17].

Researchers have already built Computer-aided diagnosis (CAD) systems that enable radiologists to discover anomalies quickly. To interpret mammograms, CAD may assist radiologists in learning and categorizing masses. According to research, 65-90 percent of suspected cancer biopsies are benign, making it critical to develop tools that discriminate between dangerous and benign tumors. ML methods used with CAD would dramatically enhance detection accuracy. Without CAD, detection accuracy was below 80% and with CAD around 90% [2]. In the long run, early detection of BC could make a big difference in how long people live with the disease, so it is essential to enhance BC prediction performance. Many papers have used deep learning (DL) and ML when it comes to the BC detection.

However, there is still a great chance to improve the prediction accuracy to reduce the required time and data to train the model. In this study, we show that by using machine learning and deep learning models to predict whether a tumour is malignant or benign in the initial stage to save women's lives. We want to select the model that has the best performance in terms of accuracy. Therefore, we are motivated to explore a dataset that includes the different factors of BC. The WDBC dataset is obtained from UCI Repository and is widely used. With the help of this dataset, we will train our models in this study.

Following is the structure of this paper: Section 2 provides a summary of relevant research on the Wisconsin dataset for BC detection. Section 3 describes extracted features and our approach to BC. Section 4 explains the experimental assessment of the suggested approach to problem-solving. In Section 5, we conclude with closing comments and a summary of future work.

2. RELATED WORK

Several studies on medical analysis for ordinary computer systems have been published in the literature. Two different approaches have been discovered, the traditional ML models and DL models, as follows:

2.1. Traditional machine learning

The BC dataset was observed by M. Rana et al. [18] using Naive Bayes (NB), Logistics Regression (LR), K Nearest Neighbor (KNN), and Support Vector Machine (SVM) classi- fiers. The KNN approach was constructed using Manhattan and Euclidean distances. The

NB technique employed normal and kernel distributions. All strategies were analyzed us- ing data from UCI's WPBC and WDBC repositories. They utilized a ML tool (MATLAB tool) to categorize data accurately. The WPBC dataset had 34 features used to predict BC, whereas the WDBC dataset contained 32 attributes used to diagnose BC. The performances of 93%, 95.68%, 90%, and 92% were obtained for SVM, KNN, LR, and NB, respectively.

Chaurasia et al. [19] compared several ML models. In the study, a Wisconsin dataset containing 268 rows for BC and ten attributes. They used Radial Basis Function (RBF) Networks, decision tree (C4.5), and Simple Logistics (SL) to enhance outcomes. For BC, they extracted nine features which are patient age, Menopause, Tumor size, Invnodes, Node caps Degree of malignancy, Breast, Breast quadrant, Irradiation, and Class to create patient templates. By applying C4.5, RBF Network, and SL, the performance of 71.32%, 73.77%, and 74.47% were obtained, respectively.

Dubey et al. [20] presented a technique for the BCWD dataset where in addition to the (standard features), the impact of the clustering of the data was investigated. The overall positive system performance was 92% by applying the K-means algorithm to the individual variable parameters.

D. Lavanya and K. U. Rani [21] conducted another study using the BCWD dataset. They applied two techniques, a hybrid approaches, and a CART classifier. Three methods have been compared: CART, CART With Feature Selection, and the hybrid to enhance classification accuracy. The best performance was obtained of 97.85 % using the hybrid approach to predict BC.

Wang and Gotoh [22] applied four distinct classifiers in the analysis, a Decision Tree (J48) classifier, an NB classifier, an SVM classifier, and a KNN classifier. The experiment was conducted on the publicly available dataset that contains 78 samples and 24481 genes. They achieved the highest average accuracy of 85.9% using the KNN classifier.

With the BCWD dataset, Vikas Chaurasia and colleagues [9] constructed a prediction model that was evaluated on the dataset, and they utilized 10- cross-validation procedures to compare the result of three ML algorithms (NB, J48, and RBF Network). According to their findings, the NB algorithm is the most accurate classifier, with an accuracy of 97.36%, 96.77% for RBF Network, and 93.41% for J48.

The model proposed by Mohammed H. et al., based on data collected from their lab, aims to assist physicians in determining the degree to which a person is at risk of developing BC while also providing opportunities for medical students to gain hands-on experience. They applied SVM, Artificial Neural Network (ANN), and KNN to recognize the severity of the BC. After evaluating and testing their approaches on BC datasets, the researchers discovered that they had an accuracy of 77.63%, 75.34%, and 76.80% respectively.

For BC diagnosis, two algorithms were compared: ANN and SVM. The SVM classifier was used to recognize patterns in the BCWD dataset based on the patient's age and tumor size. SVM was utilized to determine if the tumors were benign or malignant, while ANN was employed to simulate nonlinear functions. Both methods were validated using the K Fold approach. The authors [23] evaluated the validation method based on its correctness. SVM was proven to be more accurate than ANN. SVM had a 96.9% accuracy rate, whereas ANN had a 95.4% accuracy rate.

On the WDBC dataset, Omondiagbe et al. [24] employed the SVM, the ANN, and the NB approaches for feature selection and extraction procedures. Based on the findings, a technique was developed making use of dimensional reduction by the application of linear discriminant analysis (LDA) to the data, followed by SVM. The accuracy of the model was found to be 98.82%, the sensitivity of the model was found to be 98.41%, the specificity of the model was found to be 99.07%, and the area under the curve for the model was found to be 0.9994.

These classic ML methods benefit from modest design complexity, but they cannot deal with complex data. In this paper, we consider applying models integrating these earlier described methods on the WDBC dataset and comparing the results.

2.2. Deep learning models

Several studies have been published in the literature on WDBC datasets in DL mod- els. However, only a limited number of studies have concentrated on feature selection and optimization strategies.

For comparison, P. Mekha and N. Teeyasuksaet [25] employed ML approaches such as RF, J48, SVM, and NB to recognize BC cells. The Wisconsin dataset comprised 457 benign and 241 malignant cancers. The authors discovered that the exponential Rectifier Linear Unit (ELU) activation function method has the most remarkable accuracy rate of 96.99%.

Puja Gupta et al. [26] examined six different classifiers (Logistic Regression (LG), J48, RF, SVM, and DL) on the WDBC dataset, using their hyperparameters to determine which was the best algorithm for the WDBD dataset. Their findings suggest that, among the six algorithms tested, DL to utilizefrom Adam Gradient Descent (AGD) Learning performed the best accuracy in detecting the return of the BC illness (98.24 percent accuracy).

P Mekha, N Teeyasuksaet [25] compared BC categorization methods based on the tumor cell. They applied a DL algorithm to identify BC utilizing Tanh, Rectifier, Maxout, and Exprectifier as activation functions. RF, NB, DT, SVM, and AdaBoost are compared. The data was taken from the BCWD dataset and processed with the Rapidminer tool. A 10-cross validation technique was used for training and testing, where they achieved an accuracy of 96.99% using a DL model.

Review study [27] from 2018 states that ANN models are widely utilized for BC detection. The goal of this study is to compare the efficacy of ANN with that of other ML techniques in predicting whether a BC would be benign or malignant. They leverage characteristics gathered from tumor pictures via image preprocessing, segmentation, and feature extraction to create these kinds of predictions. They began by taking a look at some of the methods that have already been implemented.

In order to provide an ANN model, ANN-WDBC, Alshayejia et al. [7] investigated the dataset . Using a single suggested hidden layer, the ANN-WDBC model is able to provide predictions about the likelihood of a BC diagnosis. With five-fold cross-validation and no feature optimization or selection processes, we used 80% of the dataset for training and 20% for testing. In this concept, a hidden layer of several neurons is responsible for relaying information from the inputs to the outputs. There are thirty feature vectors in the model’s

input layer. With a ReLU activation function that scales with the number of neurons, the hidden layer can support a maximum of 100. A single neuron with a sigmoid activation function in the output layer decides whether the input is cancerous or benign.

Five classifiers, including KNN, NB, Sequential Neural Network (SNN), Multi Layer Perceptron (MLP), and decision tree, were evaluated by Salama et al. [28] on three separate BC datasets. The WDBC, Wisconsin Breast Cancer (WBC), and Wisconsin Breast Cancer Prognosis (WBP) are the three sets of information used in this study. For WBC, the greatest results were achieved by SNN, with an accuracy of 96.99%. This was followed by NB (95.27%), MLP (95.13%), Decision Tree (95.13%), and KNN (94.56%).

Shimomura A et al. [29] employed a highly sensitive microarray analysis to assess serum miRNA expression patterns in many large cohorts in order to uncover new miRNA that may be used to diagnose early-stage BC. The researchers utilized serum samples from BC patients held in the National Cancer Center Biobank. They applied linear discriminant analysis to detect early BC with a sensitivity of 97.3%, specificity of 82.9%, and accuracy of 89.7% by combining five microRNA (miR1246, miR13073p, miR4634, miR68615p, and miR68755p) through using formula (0.25 miR1246) + (0.49 miR13073p) (1.06 miR4634) + (1.89 miR6875).

3. Methodology

Complex and high-dimensional data may be modeled using DL methods. However, be- cause of the increased computational difficulty and potential training time, In this research, we'll create a neural network and compare its results to those of more conventional models using WDBC dataset.

For the WDBC dataset, we compared the performance of ANN models to that of other ML techniques. For the ANN models, feed-forward containing the data of various BC features from inputs to outputs via models that contain both one and two hidden layers with a variable number of neurons has been taken. The best result received from these ANN models has been further compared with other ML techniques. The models' input layers contain the number of neurons corresponding to the number of features in WDBC dataset. We vary the number of neurons in the hidden layer(s) with ReLU activation functions proportional to their numbers in both layers. Finally, the output layers have a single neuron with a sigmoid activation function that classifies the input as malignant or benign. Figure 1 demonstrates one example of the ANN model that has two hidden layers with 20 neurons each.

We evaluate ANN models against other ML techniques on WDBC dataset. Different BC feature data is fed forward from inputs to outputs in ANN models with either one or two hidden layers and a varying number of neurons. The dataset includes a different number of features, and the number of neurons in the models' input layers is proportional to that number; for example, the WDBC dataset has 30. We use ReLU activation functions proportionate to the number of neurons in both layers and change the number of neurons in the hidden layer(s). Finally, a single neuron with a sigmoid activation function is located

in the output layers, and it determines if the input is cancerous or benign. One such ANN model, seen in Figure 1, has two hidden layers of 20 neurons each.

Our work contribution includes :

- Comparing Artificial Neural Network (ANN) models to several classifiers such as LG, KNN, Random Forest, Decision Tree, Gradient Boosting, Stochastic Gradient Descent (SGD), SVM, XGBoost, and Adaboost.
- Creating suitable models to categorize and predict BC diagnostic outcomes with high accuracy for small and medium datasets.
- Identifying significant attributes or features that lead to classifying or categorizing BC correctly.
- Tweaking hyperparameters and assessing performance based on accuracy, specificity, sensitivity, precision, and F1 score.
- Evaluating the performance of ML algorithms on the WDBC dataset.

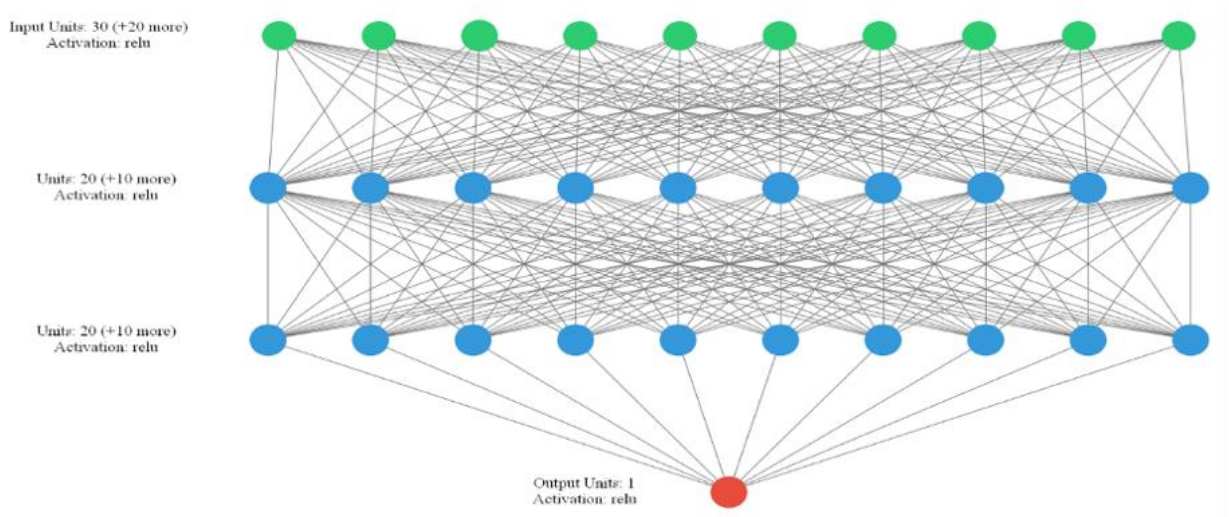


Figure 1: Proposed Artificial Neural Network Model

This paper has investigated the traditional ML and DL models. We compared these models to predict the BC survival rate data collected in this research. We applied these classification algorithms to determine which one best indicates mortality rates.

By Using k-fold cross-validation, we compare MLP and Sequential ANN models against a number of ML methodologies in order to predict the diagnosis. These ML techniques are outlined below.

A. MLP: the input is modified non-linearly [30].

B. Logistic Regression: The logistic sigmoid function is used to convert the output into a probability value. The probability value is then associated with two or more variables. [31]

C. Decision Tree: constructs a model with a tree-like structure, using the if-then rule of mathematics to produce subcategories that fit inside bigger categories and allow for exact, organic classification [32].

D. Random Forest: during the training phase, it constructs a large number of decision trees and then outputs the class depending on the mode of the individual trees [33].

E. Gradient Boosting: utilized in regression and classification applications to generate a prediction model that is often an ensemble of weak prediction models (decision tree). A gradient-boosted tree is a weak learner [34].

F. SGD: an approach that is not only easy to use but also highly effective for fitting linear classifiers and regressors to convex loss functions such as (linear) SVM and LR. Despite its extensive history, SGD has only lately attracted widespread attention in the context of large-scale learning [35]

G. SVM: data is categorised, and models are trained using SVM within super finite polarity degrees, resulting in a three-dimensional classification [36].

H. K-Nearest Neighbors: a pattern recognition method that saves and learns from train- ing data points by analyzing how the data points correlate in an n-dimensional space. It also attempts to discover the k closest connected data points in a previously unknown batch of data [37].

I. XGBoost: implements gradient boosted decision trees with a focus on speed and performance, and has lately dominated the area of applied ML and Kaggle contests with structured or tabular data [38].

J. Adaboost: utilized for both classification and regression issues by providing more weight to cases that were difficult to categorize and less weight to instances that were already adequately handled. Adaboost also combines many classifiers (both strong and weak) to increase accuracy. AdaBoost's less capable learners are known as decision stumps, which are decision trees with only one branch [39].

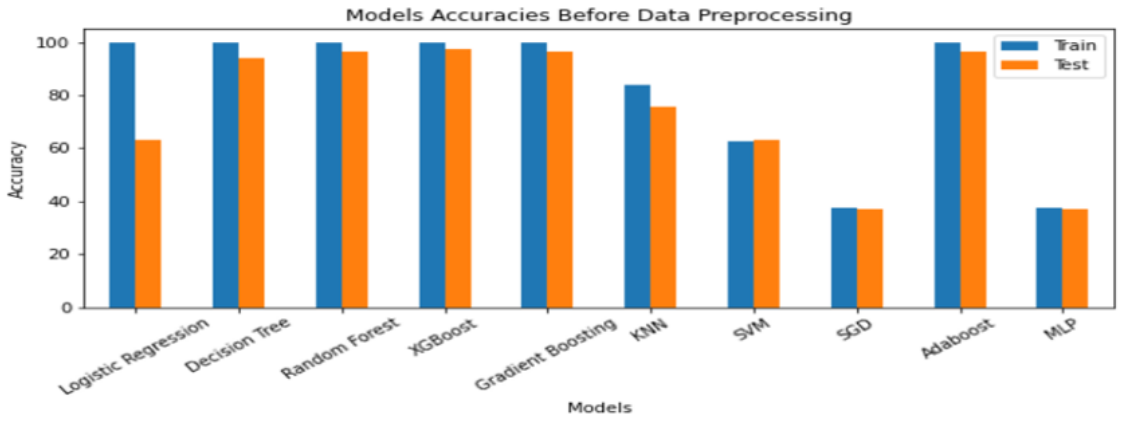


Figure 2: Models Performance Before Data Preprocessing

As mentioned previously, we will compare ANN with multiple prediction models using various ML algorithms and analyze how well each model does in terms of its accuracy, then choose the model that performs the best overall. The accuracy, sensitivity, and specificity

of the model, in addition to its F1 score, will be utilized to evaluate its overall performance. Moreover, we will use a confusion matrix to report TP: number of true positives, FP: number of false positives, FN: number of false negatives, and TN: number of true negatives. Later, we will use transfer learning to apply the same models to another dataset with the same target variable (malignant or benign).

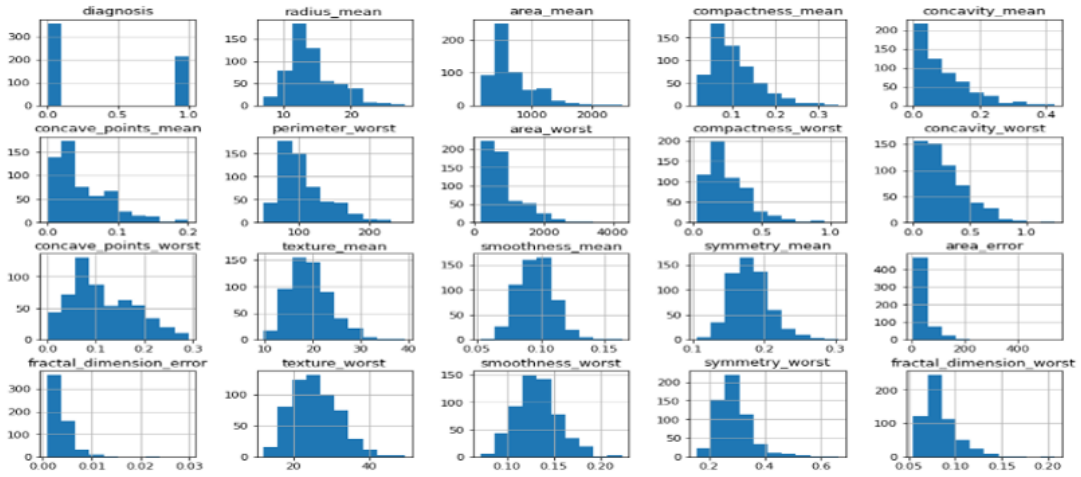


Figure 3: Histogram of WDBC Features

Before applying data preprocessing, we start by investigating the ML methods that were described earlier. Figure 2 provides an illustration of this concept by illustrating the degrees of accuracy achieved by each approach on the WDBC dataset's training and testing datasets respectively. Clearly, some classifiers obtain accuracies that are more than 96% due to the fact that the dataset is clean; yet, some classifiers have overfitting (as in LG), while others have underfitting (such as in SVM).

The distributions of the characteristics for the WDBC dataset are shown in Figure 3. In order to locate the characteristics that are the most beneficial, we use the GridSearchCV technique to feature selection. GridSearchCV is a library function that can be found in the "sklearn.model selection package." Its purpose is to assist in the process of looping over specified hyperparameters and fitting an estimator (model) on a training set [11]. In order to identify the characteristics that are skewed, we first compute the correlation between the goal (diagnosis) and each feature. We next assess if the correlation has a positive or negative skewness by looking at its absolute value (which must be more than 0.5). Figure 4 displays the 19 most optimally skewed characteristics for the WDBC.

4. Experiments and Data Analysis

4.1. Data

The dataset used in our experiment provides 32 attributes and 569 instances. We ex- tracted from the data only standard features (ID number, Diagnosis, radius, texture, perime- ter, smoothness, area, compactness, concavity, concave points, symmetry, and fractal dimen- sion). The dataset was collected by Dr. William, W. Nick, and Olvi L from the University

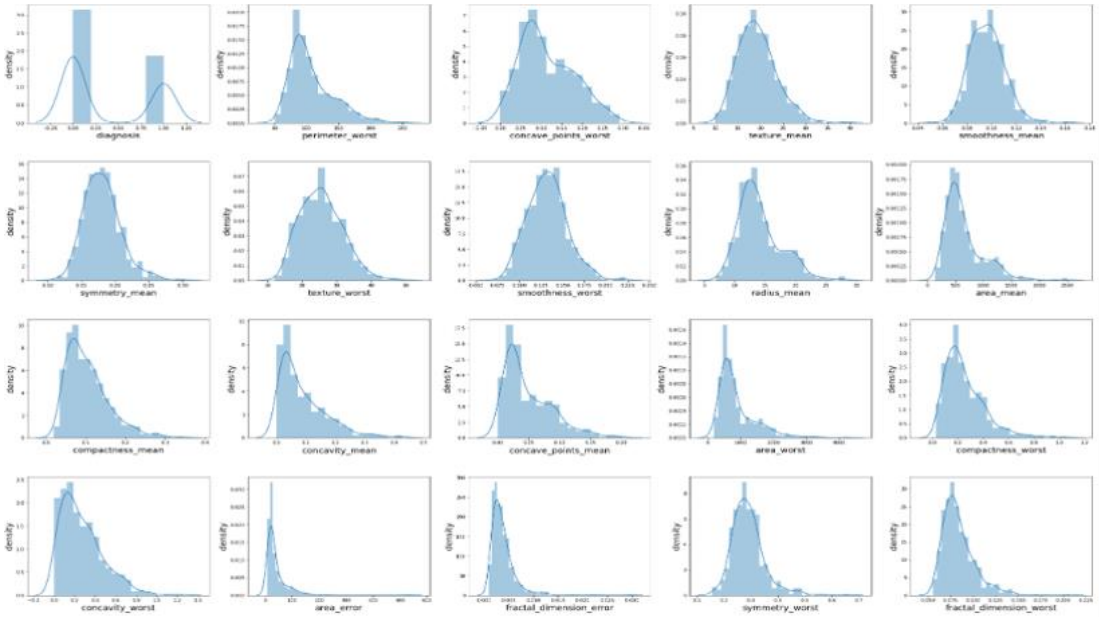


Figure 4: : Best Skewed Features

of Wisconsin, Clinical Sciences Center, and made available online at UCI Repository[1] . The dataset was collected from different patients who provided 357 benign samples and 212 malignant samples.

	id	diagnosis	radius_mean	texture_mean	perimeter_mean	area_mean	smoothness_mean	compactness_mean	concavity_mean
0	842302	M	17.99	10.38	122.80	1001.0	0.11840	0.27760	0.30010
1	842517	M	20.57	17.77	132.90	1326.0	0.08474	0.07864	0.08690
2	84300903	M	19.69	21.25	130.00	1203.0	0.10960	0.15990	0.19740
3	84348301	M	11.42	20.38	77.58	386.1	0.14250	0.28390	0.24140
4	84358402	M	20.29	14.34	135.10	1297.0	0.10030	0.13280	0.19800

Figure 5: WDBC dataset

Figure 5 shows the total number of cases as benign or malignant in the WDBC dataset. Note that more of the instances are benign (357) than malignant (212) as shown in Figure 6
. The dataset has no missing values.

4.2. Experimental Analysis

We applied traditional ML and DL algorithms to classify malignant patients and identify benign ones in our experiment. A profile is constructed for each patient using a training set comprised of positive or malignant samples from the patient and negative or benign samples from other patients.

[1]https://archive.ics.uci.edu/ml/datasets/breast+cancer+wisconsin+(diagnostic)

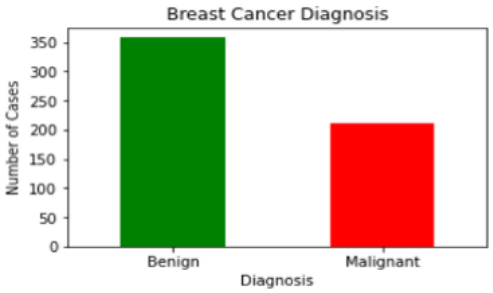


Figure 6: Number of samples of WDBC dataset

The 10-fold cross-validation method, in which 90% of the dataset is used for training and 10% is used for testing, was the one that we applied. We compute the Precision for each patient in each test round by comparing the (10%) actual test samples (i.e., from the patient) against the patient's profile. Similarly, the Recall is determined for each patient by comparing the (10%) test samples from other patients to the patient's profile. The test round Precision/Recall is calculated by averaging the individual Precision/Recall. In addition, the overall Precision/Recall is derived by averaging the values acquired throughout the ten rounds of cross-validation [40].

The performance of the BC system can be evaluated after training our model by using the training samples and the testing data. An assessment of the model's performance is presented in the next section. Furthermore, the results of the two alternative techniques are provided.

4.3. Experimental Metrics

Accuracy and F1 scores were the primary BC performance evaluation metrics. The ratio of accurately categorized samples to the total number of classified samples, with a range of 0-1, is a commonly used measure in system performance assessment. F1 score typically varies from 0 to 1, and is derived from the weighted average of accuracy and recall. Consequently, both false positive and false negative evaluation findings are included.

$$Accuracy = \frac{Number\ of\ correctly\ predicted\ breast\ cancer}{Total\ Number\ of\ predictions} \quad (1)$$

$$F\ 1\ score = \frac{2 \times (Reacall \times Precision)}{Reacall + Precision} \quad (2)$$

A Receiver Operating Characteristic Curve (ROC) is often used to simulate such fluctu- ations in operating parameters. The ROC curve plots the erroneous acceptance rate on the x-axis versus the equivalent false rejection rate on the y-axis in general. The F1-score, defined as a single measure that incorporates both precision and recall into its operation.

4.4. Experimental Result and Discussion

As we proposed, we applied two techniques to report the accuracy and overall perfor- mance of the two artificial neural networks models (multilayers perceptron and sequen- tial) and the nine traditional ML models to select the best performance.In the first tech- nique, we evaluated nine classifiers using 10-fold cross-validation. While in the second tech- nique, we split the data into a training set (80%) and a testing set (20%) with 42 random states. During the evaluation process, we took a step to optimize the models' hyperparam- eters by applying the GridSearchCV technique. GridSearchCV is a library function in the "sklearn.model_selection package" that helps to loop through predefined hyperparameters and fit estimator (model) on the training set. In the end, it shows the best parameters to choose from. Moreover, we tested the performance through additional cross-validation, testing, and confusion matrices measures and ROC curves of the testing phase [41].

Data preprocessing is a necessary process to improve the performance of ML algorithms. Therefore, we checked the missing values and found that the WDBC dataset has no missing values. Many scikit-learn ML estimators require dataset normalization to perform well. Thus, we applied the StandardScaler() method to bring all features to the same scale. Moreover, StandardScaler() method helps to improve the models' performance.

Since some models achieved accuracy above 96% without data preprocessing, the feature selection technique was applied, and the accuracy improved. We selected skewed features based on the correlation score. We considered the absolute value of the correlation (cor- relation > 0.5). The most correlated features include eight mean features, two standard error features, and nine worst features. The heatmap illustrating the correlation between the skewed features can be seen in Figure 8 . However, we were not satisfied with the perfor- mance; therefore, the standardization method was employed. As a result, models performed well and achieved high accuracies. We have considered two parameters for evaluation which are Accuracy and F1 score. Figure 7 illustrates the performance of the aforementioned models according to training and testing accuracies as well as the F1 score.

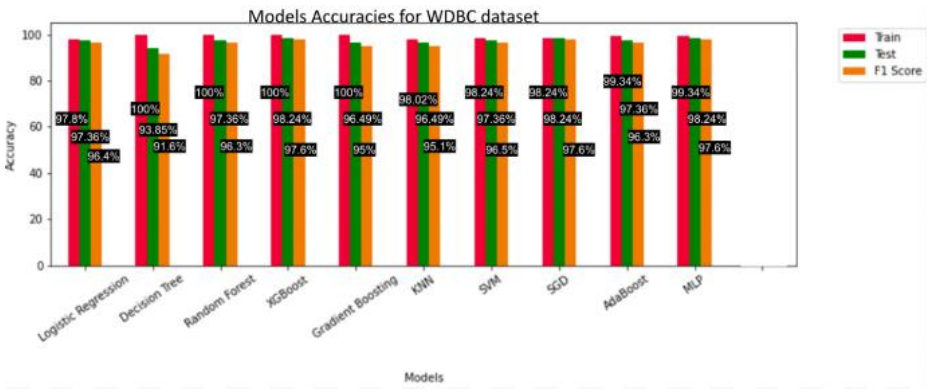


Figure 7: Models Performance After Data Preprocessing forWDBC

In preparation for predicting BC as benign or malignant, we proposed ANN model. After

multiple experiments, we found that the proposed ANN with two hidden layers and 20

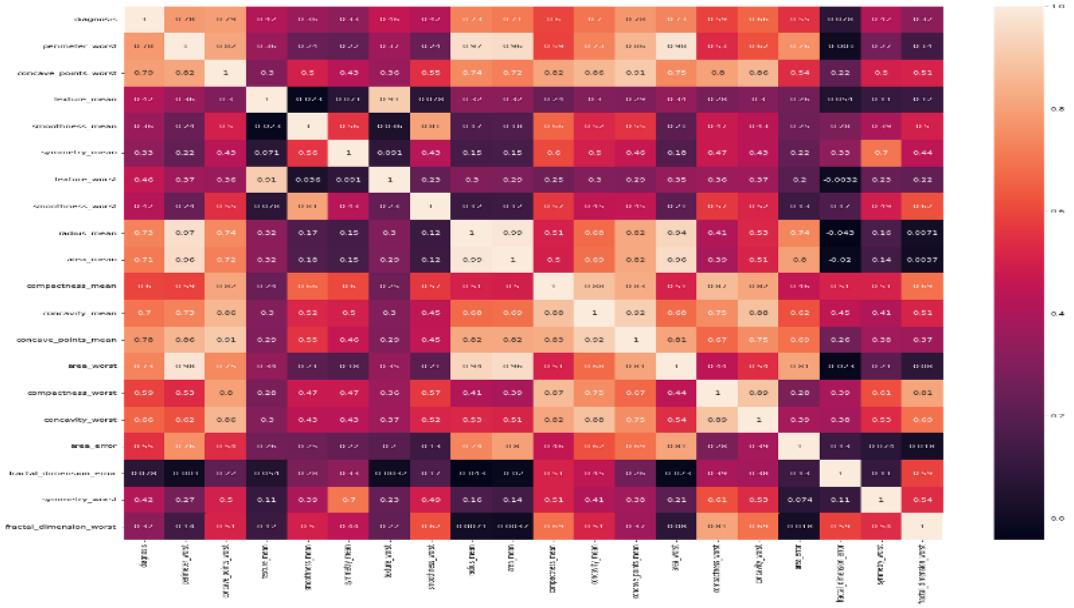


Figure 8: Correlation score heatmap of skewed features forWDBC dataset

neurons yielded the best performance according to tries and errors. Therefore, we examined multiple ANN models and reported the F1-Score through two experiments. In the first experiment, we designed 30 models consisting of a single hidden layer with different numbers of neurons from (1 – 30) with a ReLU activation function proportional to their number. The output layer has a single neuron with a sigmoid activation function. The best performance of this experiment was achieved when using 18 neurons with F1- Score 98.97, as shown in Figure 9.

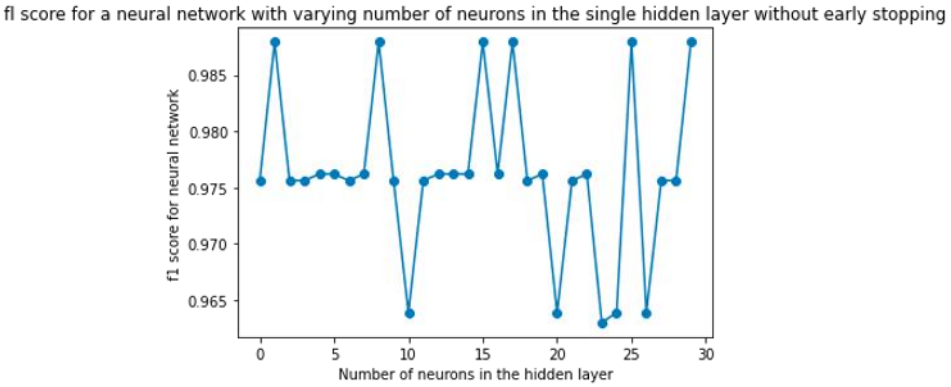


Figure 9: F1 score for neural networks with 1 hidden layer containing between 1 and 30 epochs

In the second experiment, we designed 30 models consisting of two hidden layers with

different numbers of neurons from (1 – 30) with a ReLU activation function proportional to their number in both layers. The output layer has a single neuron with a sigmoid activation function. This experiment yielded the best performance when using 3 neurons with F1- Score 99.12, as shown in Figure 10 .

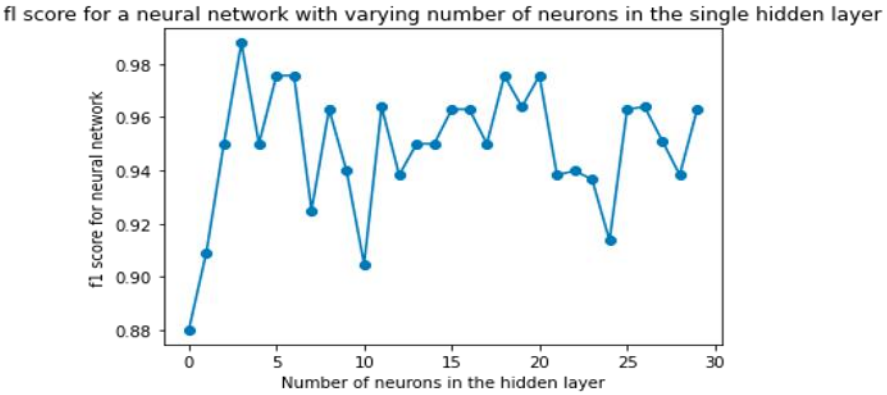


Figure 10: F1 score for neural networks with 2 hidden layers where the first contains between 1 and 30 neurons and the second has exactly 3 epochs

Table 2 shows the performance evaluation of ten classifiers. This experiment applied the K-fold cross-validation method to train on multiple train-test splits using 10 cross- validations. We observed that MLP yields the best prediction and the highest accuracy score of 98%, followed by MLP with an accuracy score of 97.54 %. The Decision Tree classifier had the lowest accuracy of the classifiers, with 93.32%, whereas all of the other classifiers had accuracy of 96% or higher.

Table 1 demonstrates the achievement of the second experiment. In this experiment, we used the train-test split technique. As mentioned previously, the dataset is split into a training set (80%) and a testing set (20%). The best result was obtained with SNN when setting the hidden layers to two, number of epochs to 30 corresponding to performance=
99.12 %. On the other hand, using SVM the performance of 99.03% was achieved.

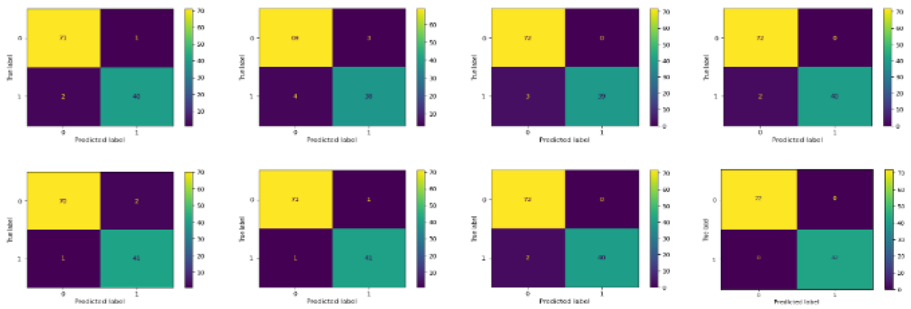


Figure 11: Confusion matrices of the testing phase usingtrain-test split

Also, we evaluated the models' performance by calculating the residual Histogram, as shown in Figure 11 . It has appeared that the prediction is closed to the actual label.

Table 1: Models performance after train-test split

	Classifier	Hyperparameters	Average Accuracy
1	Logistic Regression	Default	97.36
2	Decision Tree	Default	93.85
3	Random Forest	estimators=100, criterion = 'Gini', features='sqrt'	97.36
4	XGBoosting	max_depth=7, n_estimators=350, subsample=0.8, eval_metric='auc'	98.24
5	Gradient Boosting	Default	96.49
6	K Nearest Neighbors	leaf_size= 20, metric= 'minkowski', n_neighbors= 3, p= 2, weights= 'uniform'	96.49
7	SVM	SVM_CLS = svm.SVC(C= 4.5, kernel= 'linear', gamma= 1)	99.03
8	SGD	alpha= 0.001, epsilon= 0.1	98.24
9	AdaBoost	n_estimators=100, learning_rate= 0.1	97.36
10	Multilayer Perceptron	solver='adam', alpha=0.001, hidden_layer_sizes=(20, 20), random_state=1	98.24
11	SNN	Two hidden layers, 30 epochs	99.12

Moreover, we evaluated the performance of the models by generating a confusion matrix, as shown in Figure 12 from left to right (LG, DT, RF, XGBoost, SVM, SGD, MLP, SNN). The confusion matrix shows that SNN achieved an excellent performance to predict BS as (benign and malignant).

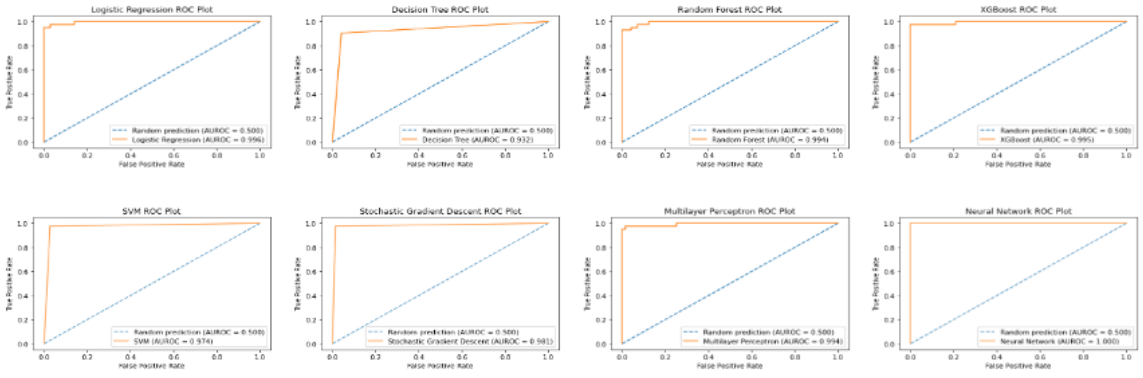


Figure 12: ROC of the testing phase using train-test split

Table 2: Models evaluation using 10-Fold cross-validation

	Classifier	Hyperparameters	Average Accuracy
1	Logistic Regression	Default	97.54
2	Decision Tree	Default	93.32
3	Random Forest	estimators=100, criterion = 'Gini', features='sqrt'	97.01
4	XGBoosting	max_depth=7, n_estimators=350, subsample=0.8, eval_metric='auc'	97.71
5	Gradient Boosting	Default	96
6	KNN	leaf_size= 20, metric= 'minkowski', n_neighbors= 3, p= 2, weights= 'uniform'	96.65
7	SVM	SVM_CLS = svm.SVC(C= 4.5, kernel= 'linear', gamma= 1)	96.3
8	SGD	alpha= 0.001, epsilon= 0.1	97.18
9	AdaBoost	n_estimators=100, learning_rate= 0.1	96.3
10	MLP	solver='adam', alpha=0.001, hidden_layer_sizes=(20, 20), random_state=1	98

4.5. Discussion

The F1 score was the primary factor considered in our analyses of the outcomes of our investigations. Largely unbalanced class distributions were seen in the dataset, just as they were in the classification difficulties that occurred in the actual world.

Cost-sensitive learning is the process of putting various amounts of weight on the training samples that indicate varying levels of misclassification costs. To be more specific, positive samples (also known as malignant samples) are given more weight than negative samples (also known as benign samples).

When doing research, it is necessary to either under-sample the majority class (also known as benign) or over-sample the minority class (malignant). When doing training, under- sampling involves picking a smaller portion of the population that belongs to the majority class, whereas over-sampling involves employing a larger portion of the population that belongs to the minority class. The superset may be produced by either repeatedly using the same samples or by producing new samples in a laboratory. Both of these methods can also produce fake samples. Both cost-sensitive learning and over-sampling were implemented in the trials that we utilized for the assessment of this study.

Table 3 provides a summary of the performances acquired for previous research on BC detection for women patients, and compares these results with our own study. The perfor- mance of our proposed method is quite satisfactory when compared to the previous work.

When taken into consideration with the diverse algorithms that were employed, this is en- couraging. We compare the prediction models and outputs that we have presented with those that were used in the earlier work, as well as the models and methodologies that were used in those earlier studies. The items that are bolded are the outcomes that exceeded those of earlier works. SNN, the suggested model, achieved an accuracy of 99.12%, while the accuracy of LR with RFE was the closest achievable 99.03% [42].

Table 3: COMPARISON OF OUR WORK WITH PREVIOUS RESEARCH WORKS

Author Name	Reference	Year	Model/Method	Best Observed Accuracy
M. Rana. et al.	[18]	2015	KNN	95.68%
V Chaurasia	[19]	2014	SL	74.47%
D. Lavanya & K. U. Rani	[21]	2012	CART	97.85%
Wang	[27]	2010	KNN	85.9%
Yue et al.				
Vikas Chaurasiet al.	[43]	2018	NB	97.36%
Mohammed H. Tafish & El-Halees	[3]	2018	SVM	77.63%
E. A. Bayrak et al.	[23]	2019	SVM	96.9%
Omondiagbe et al.	[24]	2019	SVM with LDA	98.82%
P. Mekha and N. Teeyasuk-saet	[25]	2019	DL utilizing RLU	96.99%
Dubey et al.	[20]	2020	DL utilizing AGD	98.24%
G. I. Salama et al.	[28]	2012	SNN	96.99%
Maglogiannis & E Zafiropoulos	[44]	2009	SVM Gaussian RBF	97.54%
Mert et al.	[45]	2015	KNN	92.56%
Hazra et al.	[46]	2016	SVM (using 19 features)	94.423%
Osman A. H	[47]	2017	SVM	95.23%
Wang et al.	[27]	2018	SVM based en-semble learning	96.67%

Continued on next page

Table 3 continued

Abdar et al.	[48]	2018	Nested Ensemble 2-MetaClassifier (K = 5)	97.01%
Mushtaq et al.	[49]	2020	KNN with multiple distances (Correlation K = 2)	91.00%
H. Rajaguru	[50]	2019	KNN Euclidean distance	95.61%
Durgalakshmi & Vijayakumar	[51]	2020	SVM	73%
F. Khan et al.	[52]	2020	SVM	97.06%
Al-Azzam & Shatnawi	[53]	2021	LR with area under curve	96%
Abdur Rasool	[42]	2021	Polynomial SVM	99.03%
This paper			Polynomial SVM	99.03%
			LR with RFE	**98.06%**
			MLP	98.24%
			SNN, Two hidden layers, 30 epochs	**99.12%**

5. Conclusion

In this paper, we applied ML and DL algorithms to improve the accuracy performance of BC. We also compared 11 different classifiers results on the publicly available dataset to show that the proposed approach yields much improved performance results.

When compared to other ML algorithms for identifying BC, we discovered that ANN performed particularly well for small to medium-sized datasets. Finding a huge BC dataset or extracting additional characteristics from the BC picture collection might be future work that needs to be done. Because we looked at an unbalanced dataset and found that it led to high accuracies and F1 scores, we could also utilize balancing approaches to assess the performance of the models in a balanced dataset. This is because we investigated the imbalanced dataset.

References

[1] A. Jemal, F. Bray, J. Ferlay, Global Cancer Statistics, CA Cancer J Clin49(2)(1999)33–64

[2] K. Doi, D. Ph, K. Rossmann, Computer- Aided Diagnosis : Potential Usefulness in : Diagnostic Radiology and Telemedicine, Research, Practice, and Opportunities, Proceedings of the National Forum (1996) 9–13.

[3] Tafish, Mohammed H., and Alaa M. El-Halees. "Breast cancer severity degree predication using data mining

techniques in the gaza strip." *2018 International Conference on Promising Electronic Technologies (ICPET)*. IEEE, 2018.

[4] K. D. Miller, R. L. Siegel, C. C. Lin, A. B. Mariotto, J. L. Kramer, J. H. Rowland, K. D. Stein, R. Alteri, A. Jemal, Cancer treatment and survivorship statistics, 2016, CA: a cancer journal for clinicians 66 (4) (2016) 271–289.

[5] A. M. Basudan, Breast Cancer Incidence Patterns in the Saudi Female Population: A 17-Year Retro- spective Analysis, Medicina 58 (11) (2022) 1617.

[6] Breast Cancer Statistics. Breastcancer.org (2022).

[7] M. H. Alshayeji, H. Ellethy, S. Abed, R. Gupta, Computer-aided detection of breast cancer on the wisconsin dataset: An Artificial Neural Networks approach, Biomedical Signal Processing and Control 71 (2022) 103141–103141.

[8] M. H. Forouzanfar, K. J. Foreman, A. M. Delossantos, R. Lozano, A. D. Lopez, C. J. Murray, M. Naghavi, Breast and cervical cancer in 187 countries between 1980 and 2010: a systematic analysis, The lancet 378 (9801) (2011) 1461–1484.

[9] L. A. Altonen, R. Saalovra, P. Kristo, F. Canzian, A. Hemminki, P. Peltomaki, R. Chadwik, A. D. L. Chapelle, Incidence of hereditary nonpolyposis colorectal cancer and the feasibility of molecular screen- ing for the disease, N Engl J Med 337 (1998) 1481–1487.

[10] S. Chakraborty, Bayesian kernel probit model for microarray based cancer classification, Computational Statistics and Data Analysis 12 (2009) 4198–4209.

[11] I. Guyon, J. Weston, S. Barnhill, V. Vapnik, Gene selection for cancer classification using support vector machines, Machine Learning 46 (2002) 389–422.

[12] A. A. Ardakani, A. Gharbali, A. Mohammadi, Classification of breast tumors using sonographic texture analysis, J. Ultrasound Med 34 (2) (2015) 225–231.

[13] Sprague, Brian L., et al. "Variation in mammographic breast density assessments among radiologists in clinical practice: a multicenter observational study." *Annals of internal medicine*165.7 (2016): 457-464.

[14] P. E. Freer, Mammographic breast density: impact on breast cancer risk and implications for screening 35 (2015) 302–317.

[15] T. M. Kolb, J. Lichy, J. H. Newhouse, Comparison of the Performance of Screening Mammography, Physical Examination, and Breast US and Evaluation of Factors that Influence Them: An Analysis of 27,825 Patient Evaluations, Radiology 225 (1) (2002) 165–175.

[16] H. D. Cheng, X. J. Shi, R. Min, L. M. Hu, X. P. Cai, H. N. Du, Approaches for automated detection and classification of masses in mammograms, Pattern Recognit 39 (4) (2006) 646–668.

[17] P. Skaane, K, Analysis of sonographic features in the differentiation of fibroadenoma and invasive ductal carcinoma, Am. J. Roentgenol 170 (1) (1998) 109–114.

[18] M. Rana, P. Chandorkar, A. Dsouza, N. Kazi, Breast cancer diagnosis and recurrence prediction using machine learning techniques, IJRET: International Journal of Research in Engineering and Technology eISSN (2015) 2319–1163.

[19] V. Chaurasia, S, Data mining techniques: to predict and resolve breast cancer survivability, International Journal of Computer Science and Mobile Computing IJCSMC 3 (1) (2014) 10–22.
[20] A. K. Dubey, U. Gupta, S. Jain, Analysis of k-means clustering approach on the breast cancer Wisconsin dataset, International journal of computer-assisted radiology and surgery 11 (11) (2016) 2033–2047.
[21] D. Lavanya, K. U. Rani, Ensemble decision tree classifier for breast cancer data, International Journal of Information Technology Convergence and Services 2 (1) (2012) 17–17.
[22] X. Wang, O. Gotoh, A robust gene selection method for microarray-based cancer classification, Cancer informatics 9 (2010) 3794–3794.
[23] E. A. Bayrak, P. Kirci, T. Ensari, Comparison of machine learning methods for breast cancer diagnosis, Scientific Meeting on Electrical-Electronics (2019) 1–3.
[24] Omondiagbe, David A., Shanmugam Veeramani, and Amandeep S. Sidhu. "Machine learning classification techniques for breast cancer diagnosis." *IOP Conference Series: Materials Science and Engineering*. Vol. 495. No. 1. IOP Publishing, 2019.
[25] P. Mekha, N. Teeyasuksaet, Deep learning algorithms for predicting breast cancer based on tumor cells, Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer, and Telecommunications Engineering (2019) 343–346.
[26] P. Gupta, S. Garg, Breast Cancer Prediction using varying Parameters of Machine Learning Models, Procedia Computer Science 171 (2020) 593–601.
[27] W. Yue, Z. Wang, H. Chen, A. Payne, X. Liu, Machine Learning with Applications in Breast Cancer Diagnosis and Prognosis 2 (2018).
[28] G. I. Salama, M. Abdelhalim, M. A. E. Zeid, Breast cancer diagnosis on three different datasets using multi-classifiers, Breast Cancer (WDBC) 32 (569) (2012) 2–2.
[29] A. Shimomura, S. Shiino, J. Kawauchi, S. Takizawa, H. Sakamoto, J. Matsuzaki, M. Ono, F. Takeshita, S. Niida, C. Shimizu, Novel combination of serum microRNA for detecting breast cancer in the early stage, Cancer science 107 (3) (2016) 326–334.
[30] S. Haykin, Neural networks and learning machines, 3/E, Pearson Education India, 2009.
[31] R. E. Wright, Logistic regression. (1995).
[32] W. Du, Z. Zhan, Building decision tree classifier on private data (2002).
[33] L. Breiman, Random forests, Machine learning 45 (1) (2001) 5–32.
[34] A. Natekin, A. Knoll, Gradient boosting machines, a tutorial, Frontiers in neurorobotics 7 (2013) 21.
[35] J. H. Friedman, Stochastic gradient boosting, Computational statistics & data analysis 38 (4) (2002) 367–378.
[36] W. S. Noble, What is a support vector machine?, Nature biotechnology 24 (12) (2006) 1565–1567.
[37] L. E. Peterson, K-nearest neighbor, Scholarpedia 4 (2) (2009) 1883.
[38] T. Chen, C. Guestrin, Xgboost: A scalable tree boosting system, in: Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining, 2016, pp. 785–794.
[39] Schapire, Robert E. "Explaining adaboost." *Empirical inference*.

Springer,Berlin,Heidelberg,2013. 3752.
[40] F. Alshanketi, I. Traore, A. A. Ahmed, Improving performance and usability in mobile keystroke dynamic biometric authentication, 2016 IEEE security and privacy workshops (2016) 66–73.
[41] J. Davis, M. Goadrich, The relationship between Precision-Recall and ROC curves, in: Proceedings of the 23rd international conference on Machine learning, 2006, pp. 233–240.
[42] A. Rasool, Improved machine learning-based predictive models for breast cancer diagnosis, International journal of environmental research and public health 19 (2022) 3211–3211.
[43] V. Chaurasia, S. Pal, B. Tiwari, Prediction of benign and malignant breast cancer using data mining techniques, Journal of Algorithms & Computational Technology 12 (2) (2018) 119–126.
[44] I. Maglogiannis, E. Zafiropoulos, Anagnostopoulos, I. An intelligent system for automated breast cancer diagnosis and prognosis using SVM based classifiers, Appl. Intell 30 (2009) 24–36.
[45] A. Mert, Kılıç, E. Bilgili, A. Akan, Breast cancer detection with reduced feature set, Comput. Math. Methods Med (2015).
[46] A. Hazra, S. K. Mandal, A. Gupta, Study and analysis of breast cancer cell detection using Naïve Bayes, SVM and ensemble algorithms, Int. J. Comput. Appl 145 (2016) 39–45.
[47] A. H. Osman, An enhanced breast cancer diagnosis scheme based on two-step-SVM technique, Int. J. Adv. Comput. Sci. Appl 8 (2017) 158–165.
[48] M. Abdar, N. Y. Yen, J. C. Hung, Improving the diagnosis of liver disease using multilayer perceptron neural network and boosted decision trees, J. Med. Biol. Eng 38 (2018) 953–965.
[49] Z. Mushtaq, A. Yaqub, S. Sani, A. Khalid, Effective K-nearest neighbor classifications for Wisconsin breast cancer data sets, J.Chin. Inst. Eng 43 (2020) 80–92.
[50] H. Rajaguru, Analysis of decision tree and k-nearest neighbor algorithm in the classification of breast cancer. Asian Pac, J. Cancer Prev. APJCP 20 (2019) 3777–3777.
[51] B. Durgalakshmi, V. Vijayakumar, Feature selection and classification using support vector machine and decision tree, Comput.Intell 36 (2020) 1480–1492.
[52] F. Khan, M. A. Khan, S. Abbas, A. Athar, S. Y. Siddiqui, A. H. Khan, M. Hussain, Cloud-based breast cancer prediction empowered with soft computing approaches, J. Healthc. Eng (2020) 8017496–8017496.
[53] N. Al-Azzam, I. Shatnawi, Comparing supervised and semi-supervised Machine Learning Models on Diagnosing Breast Cancer, Ann. Med. Surg 62 (2021) 53–64.

دراسة مقارنة لنماذج التعلم الآلي والتعلم العميق للكشف عن سرطان الثدي

فيصل الشنقيطي

قسم علوم الحاسب، جامعة جازان ، المملكة العربية السعودية

الملخص

سرطان الثدي هو أكثر أنواع السرطانات شيوعا بين النساء ويسبب أكبر عدد من وفيات السرطان. في البداية، كانت آليات التشخيص الأولية للكشف عن سرطان الثدي هي التصوير الشعاعي للثدي والموجات فوق الصوتية. كان من المفترض أن يتم فحص هذه الصور يدويًا بواسطة ممارسين طبيين خبراء لتحديد الورم الخبيث. الشاغل الأساسي في هذه التحقيقات اليدوية هو الدقة التي تعتمد على توافر الممارسين الطبيين المتخصصين في المجال. سيكون العثور على مثل هؤلاء الخبراء أمرًا صعبًا بالنسبة لعدد كبير من السكان عندما يرتفع سرطان الثدي بشكل حاد. تم إحراز تقدم كبير في التصوير الطبي وتكنولوجيا الرعاية الصحية ، وتم إجراء الكثير من الأبحاث في هذا المجال. تم تطبيق تقنيات التعلم الآلي والتعلم العميق بنجاح للتنبؤ بما إذا كان الورم خبيثًا أم حميدًا في المرحلة الأولية لإنقاذ حياة النساء. ومع ذلك ، لا تزال هناك فرصة كبيرة لتحسين دقة التنبؤ لتقليل الوقت والبيانات المطلوبة لتدريب النموذج. في هذه الدراسة ، أوضحنا أنه باستخدام التعلم الآلي ونماذج التعلم العميق للتنبؤ بما إذا كان الورم خبيثًا أو حميدًا في المرحلة الأولية لإنقاذ حياة النساء. نقارن تسعة مصنّفات تقليدية للتعلم الآلي بنماذج التعلم العميق التي تؤدي إلى تحقيق أداء أعلى دقة للتنبؤ بسرطان الثدي. ندرس تقسيم البيانات إلى مجموعات (٨٠٪ و ٢٠٪) و ١٠ أضعاف تقنيات التحقق من الصحة. يعتمد التقييم التجريبي على مجموعة بيانات عامة عن سرطان الثدي. تم تحقيق أفضل أداء بشكل عام باستخدام خوارزمية التعلم العميق (شبكة نيل التسلسلية) ، بدقة ٩٩,١٢٪.

الكلمات المفتاحية: سرطان الثدي التشخيصي في ولاية ويسكونسن (WDBC) ، سرطان الثدي ، التعلم الآلي والتعلم العميق ، اكتشاف سرطان الثدي.

The External and Internal Precision Concept in Horizontal Geodetic Networks

Hisham Mohammed Abouhalima
Associate Professor, Civil Engineering Department, Faculty of Engineering, Jazan University, Kingdom of Saudi Arabia

ABSTRACT

Free geodetic networks have become more frequently used in various engineering developments during the past few years. It was evident that when the results from fixed and free geodetic networks with identical configurations and measurement techniques were compared, the results from the free geodetic networks produced unexpectedly lower numerical values for traditional precision criteria.

This research intends to investigate the causes of this phenomenon by analyzing and clarifying the diversity in the geometrical significations for precision measures of both free and fixed geodetic networks. The internal precision in fixed networks may now be described using new criteria. As a result, a fair comparison between free and fixed network is possible. Using a schematic geodetic network as an example, various factors have been employed in adjustment technique to establish the importance of the study.

Keywords: Precision criteria; external precision; internal precision; positional errors; geometrical meaning; network centroid; computational base.

1- INTRODUCTRION

Today, wide ranges of engineering control survey applications frequently use engineering geodetic networks as local horizontal control networks. This can be used to detect the deformation of large structures like dams and bridges as well as horizontal crustal movements. Measures for sensitivity, economy, precision, and reliability can be used to determine the level of quality of these engineering control networks. In this essay, the only criterion that will be considered is precision. The precision of a geodetic network may be a good indicator of the extent of random error propagation inside the network. All the information about the precision of the adjusted parameter is contained in the variance-covariance matrix. The precision of the network is expressed by the size elements of the variance-covariance matrix. It should be noted that the desired measure of precision should meet the requirements listed below [**1, 3**]:

a- Invariant with regard to the selection of the computational base.
b- Invariant with regard to the datum transformation.
c- Not depend on the choice of least squares adjustment techniques.
d- Describe the positional precision of the network points.
e- Suitable to primary as well as secondary geodetic networks.

The main objective of this paper is to investigate and analyze the precision concept for the fixed and free geodetic networks. Also, an important objective is to find a measure to describe the internal precision for fixed geodetic networks. In this work, the adjustment for the schematic geodetic network is performed by a least squares method using the parametric technique.

2- GAUSS-MARKOV MODEL OF GEODETIC NETWORKS

In the classical Gauss-Markov model, the unknown parameters x of a linearized least squares model for a parametric adjustment are determined based on the following functional and stochastic models [**1, 2**],

$$\left.\begin{aligned} \mathbf{v} &= \mathbf{A}\,\mathbf{x} - \mathrm{l} \\ \mathbf{P} &= Q_l^{-1} = \sigma_o^2\, C_l^{-1} \end{aligned}\right\} \qquad (1)$$

where **v** is the n by 1 vector of residuals ; **A** is the n by u configuration matrix ; **P** is the n by n weight matrix of observations ; Q_ℓ is the cofactor matrix of observations; σ_0^2 is the a priori variance factor ; and C_ℓ is the covariance matrix of observations. The covariance matrix of the estimated parameters (coordinates) can be estimated using the relation,

$$C_{\hat{x}} = \hat{\sigma}_o^2\, Q_{\hat{x}} = \hat{\sigma}_o^2\, (\mathbf{A}^{\mathbf{T}}\,\mathbf{P}\,\mathbf{A})^{-1} \qquad (2)$$

where $\hat{\sigma}_o^2$ is the a posteriori variance factor and $Q_{\hat{x}}$ is the u by u cofactor matrix or the weight coefficient matrix of the estimated coordinates $\hat{x}$[**7, 8**]. In the design phase, the variance-covariance matrix of the estimated coordinates can be expressed as

$$C_{\hat{x}} = \hat{\sigma}_o^2 \, (\mathbf{A}^T \mathbf{P} \mathbf{A})_{rs}^{-} \tag{3}$$

with $(\mathbf{A}^T \mathbf{P}\mathbf{A})_{rs}^{-}$ representing the reflexive generalized inverse of a matrix. Assume the network is complete, i.e., without configuration a defect, then the number of rank defects of A is equal to the number of datum defects **d** of the network. After a definition of the datum of the network has been given by

$$\mathbf{G}^T \mathbf{x} = \mathbf{0} \tag{4}$$

with the rank of matrix **G** being equal to the number of rank defects of **A** , then the variance-covariance matrix of the estimated coordinates is given by [**7**]

$$C_{\hat{x}} = \hat{\sigma}_o^2 \, (\mathbf{A}^T \mathbf{P} \mathbf{A} + \mathbf{G}\,\mathbf{G}^T)^{-1} - \mathbf{H}\,(\mathbf{H}^T \mathbf{G}\,\mathbf{G}^T \mathbf{H})^{-1}\,\mathbf{H}^T \tag{5}$$

where the matrix **H** spans the null space of matrix **A**, satisfying the relation

$$\mathbf{A}\,\mathbf{H} = \mathbf{0} \tag{6}$$

and for a two dimensional trilateration network with m geodetic points, matrix **H** is expressed as [**1, 9**]:

$$\mathbf{H}^T = \begin{bmatrix} 1 & 0 & \ldots\ldots & 1 & 0 \\ 0 & 1 & \ldots\ldots & 0 & 1 \\ -x_1^o & y_1^o & \ldots\ldots & -x_m^o & y_m^o \end{bmatrix} \tag{7}$$

with (x_1^o , y_1^o) (i = 1, ..., m) being the approximate coordinates of net-points. If matrices **G** and **H** are equal then the so-called inner constraints are used in the adjustment procedure.

3- ANALYSIS OF THE PRECISION CRITERIA

3.1 The Common Precision Criteria

In geodetic network, the variance-covariance matrix of the adjusted coordinates contains all information that contributes to determine the precision criteria. Two types of precision criteria are used, the local and the global measures of precision. These precision criteria can be summarized as follows [**4, 6**]:

1- The standard deviations of the net-point coordinate can be given as follows:

$$\sigma_x = \hat{\sigma}o \sqrt{Q_{xx}} \qquad \sigma_y = \hat{\sigma}o \sqrt{Q_{yy}} \tag{8}$$

2- The positional error (standard point error) of the net-point

$$\sigma_P = \pm \sqrt{\sigma_x^2 + \sigma_y^2} = \hat{\sigma}o \sqrt{Q_{xx} + Q_{yy}} \quad (9)$$

3- The absolute error ellipse which is a graphical representation of the precision of the estimated net-point coordinates. The three parameters of the standard absolute error ellipse for any point can be computed as follows:

$$\left.\begin{aligned} A &= \hat{\sigma}o \cdot \sqrt{(Q_{xx} + Q_{yy} + Q)/2} \\ B &= \hat{\sigma}o \cdot \sqrt{(Q_{xx} + Q_{yy} - Q)/2} \\ 2\theta &= \arctan\left(\frac{2Q_{xy}}{Q_{xx} - Q_{yy}}\right) \end{aligned}\right\} \quad (10)$$

in which

$$Q = \sqrt{(Q_{xx} - Q_{yy})^2 + 4Q_{xy}^2}$$

where A and B are the semi-major and semi-minor axis of the error ellipse,
θ is the angle between the semi-major axis of the ellipse and the x-axis,
Qxx, Qyy and Qxy are the elements of the cofactor matrix of the adjusted coordinates [**8**].

4- The mean standard errors of the coordinates of all network points are defined as a global measure of precision, and given by

$$\sigma_C = \sqrt{\frac{trace(C_{\hat{x}})}{2m}} \quad (11)$$

5- Another global measure of precision is the mean positional error, which is known in German literature as the mean network error and given by

$$\sigma_N = \sigma_C \cdot \sqrt{2} = \sqrt{\frac{trace(C_{\hat{x}})}{m}} \quad (12)$$

6- The generalized network error (σ_W) or the geometric mean of the eigenvalues is also defined as a global measure of precision, and given by [**6**]:

$$\sigma_W = \sqrt[m]{\det(C_{\hat{x}})} \quad (13)$$

which is dependent on the determinant of the estimated variance-covariance matrix of the adjusted coordinates.

7- The largest eigenvalue of the covariance matrix of the adjusted coordinates (λ_{max}) is also global measure of precision

$$\lambda_{max}(C_{\hat{x}}) = \lambda_1 \quad (14)$$

which can be regarded as an indication of the least precise position in the network. Both the difference between the largest and smallest eigenvalues (λ_{max}- λ_{min}) and the ratio of (λ_{max} / λ_{min}) are also used to judge the homogeneity of the network **[4]**.

3.2 The Precision Concept in Fixed Geodetic Network

In fixed geodetic network, the positional error of the new net-point (σ_{P_i}) can be computed from the estimated Coordinates difference between an arbitrary fixed point $P_F(x_F, y_F)$ and the new point $P_i(\hat{x}_i, \hat{y}_i)$ as follows:

$$\Delta x_{Fi} = \hat{x}_i - x_F \quad , \quad \Delta y_{Fi} = \hat{y}_i - y_F$$

Applying the variance - covariance propagation law, it gives the standard errors of the coordinates differences [**7**]

$$\sigma_{\Delta x_{Fi}} = \sigma_{x_i} \quad , \quad \sigma_{\Delta y_{Fi}} = \sigma_{y_i}$$

And then

$$\pm \sqrt{\sigma^2_{\Delta x_{Fi}} + \sigma^2_{\Delta y_{Fi}}} = \pm \sqrt{\sigma^2_{x_i} + \sigma^2_{y_i}} = \sigma_{P_i} \qquad (15)$$

The above positional error can also be computed from both the estimated distance ($\hat{S}_{Fi}$) and the estimated direction ($\hat{t}_{Fi}$) between an arbitrary fixed point (P_F) and the new point (P_i) using the following relations:

$$\hat{S}_{Fi} = \sqrt{(\hat{x}_i - x_F)^2 + (\hat{y}_i - y_F)^2} \quad \text{and} \quad \hat{t}_{Fi} = \arctan\left(\frac{\hat{y}_i - y_F}{\hat{x}_i - x_F}\right)$$

By applying the law of variance-covariance propagation [**7, 8**], it was found that

$$\sigma^2_{\hat{S}_{Fi}} = \cos^2 \hat{t}_{Fi} \,.\, \sigma^2_{x_i} + \sin^2 \hat{t}_{Fi} .\, \sigma^2_{y_i} + 2 \sin \hat{t}_{Fi} .\, \cos \hat{t}_{Fi} .\, \sigma_{x_i y_i} \qquad (16)$$

and

$$\sigma^2_{\hat{t}_{Fi}} = \frac{\rho''}{\hat{S}^2_{Fi}} [\sin^2 \hat{t}_{Fi} .\, \sigma^2_{x_i} + \cos^2 \hat{t}_{Fi} .\, \sigma^2_{y_i} - 2 \sin \hat{t}_{Fi} .\, \cos \hat{t}_{Fi} .\, \sigma_{x_i y_i}] \qquad (17)$$

From the standard error of the estimated direction $\sigma_{\hat{t}_{Fi}}$, the standard cross error ($\sigma_{q_{Fi}}$) can be estimated as

$$\sigma_{q_{Fi}} = \hat{S}_{Fi} \,.\, \sigma_{\hat{t}_{Fi}} / \rho'' \qquad (18)$$

Based on the above two equations (16) and (18), one obtained

$$\pm \sqrt{\sigma^2_{S_{Fi}} + \sigma^2_{q_{Fi}}} = \pm \sqrt{\sigma^2_{x_i} + \sigma^2_{y_i}} = \sigma_{P_i} \qquad (19)$$

From these results, it can be concluded that, in fixed geodetic network the positional error of any new net-point is identical with the standard error of the Coordinates difference between the new point and an arbitrary fixed point. Furthermore, it is also identical with the geometric addition for the standard error of the estimated distance between the new net-point and an arbitrary fixed net-point and the standard cross error, which can be obtained from the standard error of the estimated direction between the new net-point and an arbitrary fixed net-point.

3.3 The Precision Concept in Free Geodetic Network

It is well known that, the free geodetic network has none fixed points. Consequently, all the net-point coordinates are allowed to receive corrections after performing of the adjustment process. The positional error (σ_{P_i}) in free network can be obtained from the Coordinates difference between a net-point $P_i(\hat{x}_i, \hat{y}_i)$ and the network centroid $P_S(x_S, y_S)$ as follows:

$$\Delta x_i = \hat{x}_i - x_S \quad , \quad \Delta y_i = \hat{y}_i - y_S$$

By putting i = 1, and applying the law of covariance propagation [**7**], it was found that

$$\begin{aligned} Q_{\Delta x_1 \Delta x_1} = Q_{x_1x_1} + \frac{1-2m}{m^2}(Q_{x_1x_1} + Q_{x_1x_2} + ... + Q_{x_1x_m}) \\ + \frac{1}{m^2}\ (Q_{x_1x_2} + Q_{x_2x_2} + ... + Q_{x_2x_m}) \\ . . . . . \\ + \frac{1}{m^2}\ (Q_{x_1x_m} + Q_{x_2x_m} + ... + Q_{x_mx_m}) \end{aligned}$$

In the free network, the sum of the elements in brackets for the above equation is equal zero [**5, 9**], then

Similarly,

$$\left.\begin{aligned} Q_{\Delta x_1 \Delta x_1} = Q_{x_1x_1} \quad \text{or} \quad \sigma_{\Delta x_1} = \sigma_{x_1} \\ Q_{\Delta y_1 \Delta y_1} = Q_{y_1y_1} \quad \text{or} \quad \sigma_{\Delta y_1} = \sigma_{y_1} \end{aligned}\right\} \qquad (20)$$

Based on the results obtained from equation (20) the following can be obtained

$$\pm\sqrt{\sigma^2_{\Delta x_i} + \sigma^2_{\Delta y_i}} = \pm\sqrt{\sigma^2_{x_i} + \sigma^2_{y_i}} = \sigma_{P_i} \qquad (21)$$

The above positional error (σ_{P_i}) in free network can also be calculated from both the estimated distance ($\hat{S}_i$) and the estimated direction ($\hat{t}_i$) between a net-point $P_i(\hat{x}_i, \hat{y}_i)$ and the network centroid $P_S(x_S, y_S)$ as follows:

$$\hat{S}_i = \sqrt{(\hat{x}_i - x_S)^2 + (\hat{y}_i - y_S)^2} \qquad \text{and} \qquad \hat{t}_i = \text{arc tan}\left(\frac{\hat{y}_i - y_S}{\hat{x}_i - x_S}\right)$$

By putting (i= 1) and applying the law of variance-covariance propagation, it was found that:

$$\begin{aligned}
Q_{\hat{S}_1\hat{S}_1} = {} & \cos^2 \hat{t}_1 \,.Q_{x_1x_1} + 2\sin\hat{t}_1 \,.\cos t_1 .Q_{x_1y_1} + \sin^2 \hat{t}_1 .\, Q_{y_1y_1} \\
& + \frac{1-2m}{m^2}[\cos^2 \hat{t}_1 \,(Q_{x_1x_1} + Q_{x_1x_2} + ...+ Q_{x_1x_m}) \\
& \qquad + \sin\hat{t}_1 .\cos\hat{t}_1 (Q_{x_1y_1} + Q_{x_1y_2} + ...+ Q_{x_1y_m})] \\
& + \frac{1}{m^2}[\cos^2 \hat{t}_1 (Q_{x_1x_2} + Q_{x_2x_2} + ...+ Q_{x_2x_m}) \\
& \qquad + \sin\hat{t}_1 .\cos\hat{t}_1 (Q_{x_2y_1} + Q_{x_2y_2} + ...+ Q_{x_2y_m})] \\
& \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
& + \frac{1}{m^2}[\cos^2 \hat{t}_1 (Q_{x_1x_m} + Q_{x_2x_m} + ...+ Q_{x_mx_m}) \\
& \qquad + \sin\hat{t}_1 .\cos\hat{t}_1 (Q_{x_my_1} + Q_{x_my_2} + ...+ Q_{x_my_m})] \\
& + \frac{1-2m}{m^2}[\sin\hat{t}_1 \,.\cos\hat{t}_1 (Q_{x_1y_1} + Q_{x_2y_1} + ...+ Q_{x_my_1}) \\
& \qquad + \sin^2 \hat{t}_1 (Q_{y_1y_1} + Q_{y_1y_2} + ...+ Q_{y_1y_m})] \\
& + \frac{1}{m^2}[\sin\hat{t}_1 \,.\cos\hat{t}_1 (Q_{x_1y_2} + Q_{x_2y_2} + ...+ Q_{x_my_2}) \\
& \qquad + \sin^2 \hat{t}_1 (Q_{y_1y_2} + Q_{y_2y_2} + ...+ Q_{y_2y_m})] \\
& \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
& + \frac{1}{m^2}[\sin\hat{t}_1 \,.\cos\hat{t}_1 (Q_{x_1y_m} + Q_{x_2y_m} + ...+ Q_{x_my_m}) \\
& \qquad + \sin^2 \hat{t}_1 \,(Q_{y_1y_m} + Q_{y_2y_m} + ...+ Q_{y_my_m})]
\end{aligned}$$

As mentioned before, the sum of the elements in brackets for the above equation is equal zero [**5, 9**]. The standard error of the estimated distance between a net-point P_i and the network centroid P_S can be obtained in general form as

$$\sigma_{\hat{S}_i} = \hat{\sigma}_o \sqrt{\cos^2\hat{t}_i Q_{x_ix_i} + 2\sin\hat{t}_i \cos\hat{t}_i Q_{x_iy_i} + \sin^2\hat{t}_i Q_{y_iy_i}} \qquad (22)$$

For the direction:

$$
\begin{aligned}
S_1^2\, Q_{\hat{t}_1\hat{t}_1} = {} & \sin \hat{t}_1\, Q_{x_1x_1} - 2 \sin \hat{t}_1 . \cos \hat{t}_1\, Q_{x_1y_1} + \cos^2 \hat{t}_1\, Q_{y_1y_1} \\
& + \frac{1-2m}{m^2}[\sin^2 \hat{t}_1 (Q_{x_1x_1} + Q_{x_1x_2} + \dots\dots + Q_{x_1x_m}) \\
& \qquad - \sin \hat{t}_1 . \cos \hat{t}_1 (Q_{x_1y_1} + Q_{x_1y_2} + \dots\dots + Q_{x_1y_m})] \\
& + \frac{1}{m^2}[\sin^2 \hat{t}_1 (Q_{x_2x_1} + Q_{x_2x_2} + \dots\dots + Q_{x_2x_m}) \\
& \qquad - \sin \hat{t}_1 . \cos \hat{t}_1 (Q_{x_2y_1} + Q_{x_2y_2} + \dots\dots + Q_{x_2y_m})] \\
& \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
& + \frac{1}{m^2}[\sin^2 \hat{t}_1 (Q_{x_1x_m} + Q_{x_2x_m} + \dots\dots + Q_{x_mx_m}) \\
& \qquad - \sin \hat{t}_1 . \cos \hat{t}_1 (Q_{x_my_1} + Q_{x_my_2} + \dots\dots + Q_{x_my_m})] \\
& + \frac{1-2m}{m^2}[-\sin \hat{t}_1 . \cos \hat{t}_1 (Q_{x_1y_1} + Q_{x_2y_1} + \dots\dots + Q_{x_my_1}) \\
& \qquad + \cos^2 \hat{t}_1 (Q_{y_1y_1} + Q_{y_1y_2} + \dots\dots + Q_{y_1y_m})] \\
& + \frac{1}{m^2}[-\sin \hat{t}_1 . \cos \hat{t}_1 (Q_{x_1y_2} + Q_{x_2y_2} + \dots\dots + Q_{x_my_2}) \\
& \qquad + \cos^2 \hat{t}_1 (Q_{y_1y_2} + Q_{y_2y_2} + \dots\dots + Q_{y_2y_m})] \\
& \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
& + \frac{1}{m^2}[-\sin \hat{t}_1 .\cos \hat{t}_1 (Q_{x_1y_m} + Q_{x_2y_m} + \dots\dots + Q_{x_my_m}) \\
& \qquad + \cos^2 \hat{t}_1 (Q_{y_1y_m} + Q_{y_2y_m} + \dots\dots + Q_{y_my_m})]
\end{aligned}
$$

Because of the sum of the elements in brackets is equal zero [**9**]. The standard error of the estimated direction $\hat{t}_i$ between a net-point P_i and the network centroid P_S can be written in general form as;

$$\sigma = \frac{\rho \cdot \hat{\sigma}_o}{\hat{S}_i} \sqrt{(\sin^2 \hat{t}_i Q_{x_ix_i} - 2\sin \hat{t}_i \cos \hat{t}_i Q_{x_iy_i} + \cos^2 \hat{t}_i Q_{y_iy_i})} \tag{23}$$

The standard cross error $\sigma_{q_{t_i}}$ can be calculated as

$$\sigma_{q_{t_i}} = \hat{\sigma}_o \sqrt{(\sin^2 \hat{t}_i Q_{x_ix_i} - 2\sin \hat{t}_i \cos \hat{t}_i Q_{x_iy_i} + \cos^2 \hat{t}_i Q_{y_iy_i})} \tag{24}$$

Based on the results obtained from Eq. (22) and Eq. (24), the following can be obtained

$$\pm \sqrt{\sigma_{S_i}^2 + \sigma_{q_{t_i}}^2} = \hat{\sigma}_o \sqrt{Q_{x_ix_i} + Q_{y_iy_i}} = \sigma_{P_i} \tag{25}$$

From these results, it can be concluded that, in free geodetic network the positional error of any net-point σ_{P_i} is identical with the standard error of the Coordinates difference between the net-point and the network centroid. Furthermore, it is also identical with the geometric addition for the standard error of the estimated distance between the net-point and the network centroid and the standard cross error, which can be obtained from the standard error of the estimated direction between the net-point and the network centroid.

3.4 The External and Internal Precision Concept

According to the analysis of the previous two sections, it was found that:

1- The positional error (σ_{P_i}) in fixed geodetic networks has different geometrical meaning than those of the free networks.

2- In fixed geodetic networks, σ_{P_i} describes the positional precision of any new point related to the fixed point and can be therefore named as the external positional error.

3- In free geodetic networks, (σ_{P_i}) describes the positional precision of any net-point related to the network centroid and can be therefore named as the internal positional error.

4- Similarly, (σ_N) for both fixed and free geodetic networks can be also named as the external and internal mean network error respectively.

5- Consequently, the comparison between free and fixed geodetic network using the common positional error (σ_{P_i}) is invalid.

The expressions external and internal precision were first introduced by MEISSL [**5**] and it is still being used up-to now in many literatures **[1,3,4,9].**

3.5 The Internal Precision Concept in Fixed Geodetic Network

It was necessary to find a measure to describe the internal precision in fixed geodetic network. This measure can be named as internal positional error. As in the free geodetic network, this measure can be obtained from the geometric addition of the standard errors of the estimated distance and the estimated direction between any new net-point and the network centroid (average of the all coordinates of only the new net-points).
The distance computed from the estimated coordinates of the new net-point (P_i) and the network centroid (P_S) can be represented as

$$\hat{S}_i = \sqrt{\left(\hat{x}_i - \frac{[x]}{m}\right)^2 + \left(\hat{y}_i - \frac{[y]}{m}\right)^2} \qquad (26)$$

Applying the law of variance-covariance propagation [**7, 8**] gives,

$$Q_{\hat{S}_i\hat{S}_i} = a_i^T . Q_{\hat{x}} . a_i \qquad (27)$$

Where (Q_x) is the weight coefficient (cofactor) matrix of the estimated coordinates and the vector (a_i) can be computed from the partial derivatives of the estimated distance with respect to the estimated coordinates of the new net-points,

$$a_i^T = \left[\frac{\partial \hat{S}_i}{\partial x_1} \ldots\ldots \frac{\partial \hat{S}_i}{\partial x_m} \frac{\partial \hat{S}_i}{\partial y_1} \ldots\ldots \frac{\partial \hat{S}_i}{\partial y_m} \right] \tag{28}$$

Where

$$\frac{\partial \hat{S}_i}{\partial x_i} = \frac{m-1}{m} \cos \hat{t}_i \quad , \quad \frac{\partial \hat{S}_i}{\partial x_k} = -\frac{1}{m} \cos \hat{t}_i$$

$$\frac{\partial \hat{S}_i}{\partial y_i} = \frac{m-1}{m} \sin \hat{t}_i \quad , \quad \frac{\partial \hat{S}_i}{\partial y_k} = -\frac{1}{m} \sin \hat{t}_i$$

$i = 1, \ldots\ldots, m$, $k = 1, \ldots\ldots, m$ and $k \neq i$

It should be taken into account that before the computation of the weight coefficients for the estimated directions ($\hat{t}_i$), from the adjusted new points to the network centroid, an optimal orientation angle (z) should be subtracted. This angle can be obtained from the obvious condition that the sum of the squares of the cross errors, which calculated from the directions from the new points to the network centroid, should be a minimum. The optimal orientation angle can be obtained in the general case as follows:

$$z = \frac{\sum S^2 t}{\sum S^2} \tag{29}$$

The orientation direction (r_i) can be computed from the estimated direction ($\hat{t}_i$) and the optimal orientation angle (z) as follows,

$$\left.\begin{aligned} r_i &= \hat{t}_i - z = \hat{t}_i - \frac{S_1^2 \hat{t}_1 + S_2^2 \hat{t}_1 + \ldots\ldots + S_m^2 \hat{t}_m}{[S^2]} \\ \hat{t}_i &= \arctan \frac{\hat{y}_i - y_S}{\hat{x}_i - x_S} \end{aligned}\right\} \tag{30}$$

Applying the law of variance-covariance propagation [**7, 8**] gives,

$$Q_{r_i r_i} = b_i^T . Q_{\hat{x}} . b_i \tag{31}$$

The vector (b_i) can be computed from the partial derivatives of the orientation direction with respect to the estimated coordinates of the new net-points

$$b_i^T = \left[\frac{\partial r_i}{\partial x_1} \ldots\ldots \frac{\partial r_i}{\partial x_m} \frac{\partial r_i}{\partial y_1} \ldots\ldots \frac{\partial r_i}{\partial y_m} \right] \tag{32}$$

where

$$\frac{\partial r_i}{\partial x_i} = -\frac{1}{m\left[S^2\right]} \left[\left(\left[S^2\right] - S_i^2\right)(m-1)\frac{\sin t_i}{S_i} + \sum S_k \sin t_k \right],$$

$$\frac{\partial r_i}{\partial y_i} = +\frac{1}{m\left[S^2\right]} \left[\left(\left[S^2\right] - S_i^2\right)(m-1)\frac{\cos t_i}{S_i} + \sum S_k \cos t_k \right],$$

$$\frac{\partial r_i}{\partial x_k} = +\frac{1}{m\left[S^2\right]} \left[\left(\left[S^2\right] - S_i^2\right)\frac{\sin t_i}{S_i} + (m-1) S_k \sin t_k - \sum S_j \sin t_j \right],$$

$$\frac{\partial r_i}{\partial y_k} = -\frac{1}{m\left[S^2\right]} \left[\left(\left[S^2\right] - S_i^2\right)\frac{\cos t_i}{S_i} + (m-1) S_k \cos t_k - \sum S_j \cos t_j \right].$$

$i = 1, \ldots\ldots, m$, $k = 1, \ldots\ldots, m$ but $k \neq i$
and $j = 1, \ldots\ldots, m$ but $j \neq i \neq k$

In order to avoid the interference with the external precision, the measure of the internal precision for the fixed network should be denoted by the subscript (in), then the internal positional error of the new net-point can be calculated from the following equation:

$$\left(\sigma_{P_i}\right)_{in} = \pm \sqrt{\sigma_{S_i}^2 + \sigma_{q_{r_i}}^2} = \hat{\sigma}_o \sqrt{Q_{\hat{S}_i \hat{S}_i} + Q_{q_{r_i} q_{r_i}}} \tag{33}$$

in which

$$Q_{\hat{S}_i \hat{S}_i} + Q_{q_{r_i} q_{r_i}} = Q_{\hat{S}_i \hat{S}_i} + S_i^2 Q_{r_i r_i} = \left(Q_{P_i P_i}\right)_{in} \tag{34}$$

and the internal mean network error is given as follows :

$$\left(\sigma_N\right)_{in} = \sqrt{\frac{1}{m}\left[\sigma_{P_{in}}^2\right]} = \hat{\sigma}_o \sqrt{\frac{1}{m}\left[\left(Q_{pp}\right)_{in}\right]} \tag{35}$$

4- NUMERICAL EXAMPLE

The above derived results are illustrated using a schematic two-dimensional trilateration network. Eight new points with unknown coordinates (P1, P2....., P8) make up this local network. As shown in Figure (1), the network points (P1, P2, P7, and P8) are connected to eight reference points (A, B, C, D, E, F, G, and H). Table (1) shows the approximate coordinates of the new network points according to the chosen local horizontal coordinate system. By the least squares method, the network was adjusted using the parametric technique [7].

Table (1): The approximate coordinates of the network points.

Points	x (m)	y (m)
P_1	800.000	400.000
P_2	400.000	400.000
P_3	400.000	800.000
P_4	800.000	800.000
P_5	400.000	1200.000
P_6	800.000	1200.000
P_7	400.000	1600.000
P_8	800.000	1600.000

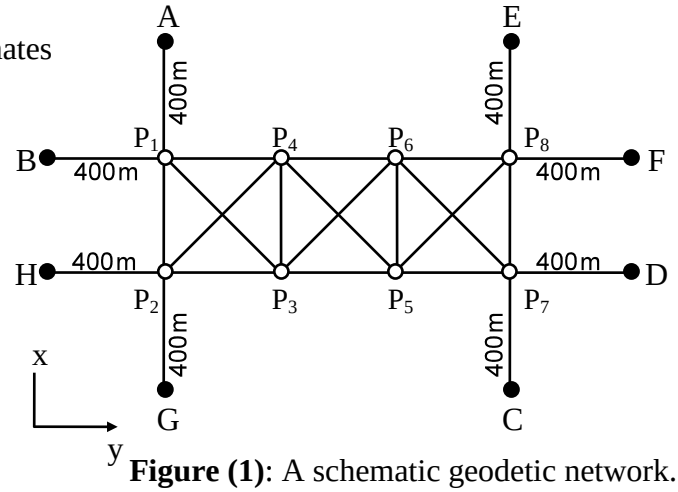


Figure (1): A schematic geodetic network.

For the clarity of this study, the local trilateration network illustrated in Figure (1) should be adjusted in four variants. In the first, second and third variants, the network were adjusted as a fixed network using the over-constrained adjustment approach with eight, six and four fixed points respectively. For the fourth variant, all the fixed points were eliminated and the network was adjusted as a free network using the inner restricted method.

All the computations were performed on a PC computer. The computer program used to adjust the geodetic network using the above mentioned approaches and to estimate the external and internal precision criteria for fixed and free geodetic networks was developed by the author.

5- RESULTS AND DISCUSSION

I- Table (2) contains the common local precision criteria (σ_{P_i}, A_i & B_i) of all estimated net-points for the four variants of the trilateration network. From the obtained results, it was found that:

1- As the number of fixed net-points decrease, values of the external local precision criteria (σ_{P_i}, A_i and B_i) increase (see variants 1, 2 & 3).

2- The external local precision criteria gave the biggest numerical values of the farthest point from fixed network points (see variants 2 & 3).

3- Comparing the external local precision criteria in the variants (1, 2 & 3) numerically show that they are different from each other. This illustrates that the variance-covariance matrix and all the common precision criteria depend upon the choice of the computational base. Consequently, they are not invariant with respect to datum transformation.

Table (2): The common local precision criteria

		Variant (1)	Variant (2)	Variant (3)	Variant (4)
		8-Fixed points A,B,C,D,E,F,G,H	6- Fixed points A,B,C,D,E, & F	4- Fixed points A,B,C & D	Free Network
n		24	22	20	16
u		16	16	16	16
d		-	-	-	3
r		8	6	4	3
σ_{P_i} (cm)	P_1	1.14	1.29	1.32	1.20
	P_2	1.14	1.94	2.10	1.20
	P_3	1.50	1.74	1.99	1.01
	P_4	1.50	1.69	1.88	1.01
	P_5	1.50	1.57	1.88	1.01
	P_6	1.50	1.60	1.99	1.01
	P_7	1.14	1.15	1.32	1.20
	P_8	1.14	1.17	2.10	1.20
A_i (cm)	P_1	0.84	0.99	1.00	1.02
	P_2	0.84	1.52	1.64	1.02
	P_3	1.23	1.38	1.66	0.84
	P_4	1.23	1.41	1.56	0.84
	P_5	1.23	1.28	1.56	0.84
	P_6	1.23	1.33	1.66	0.84
	P_7	0.84	0.85	1.00	1.02
	P_8	0.84	0.85	1.64	1.02
B_i (cm)	P_1	0.77	0.83	0.86	0.65
	P_2	0.77	1.20	1.32	0.65
	P_3	0.85	1.05	1.11	0.56
	P_4	0.85	0.94	1.04	0.56
	P_5	0.85	0.92	1.04	0.56
	P_6	0.85	0.90	1.11	0.56
	P_7	0.77	0.77	0.86	0.65
	P_8	0.77	0.80	1.32	0.65

4- Free network adjustment using the inner constrained approach (variant 4) gave the smallest numerical values of all common local precision criteria (σ_{P_i}, A_i & B_i). This means that, this technique has an important characteristic of having minimum norm and minimum trace. The results obtained from this adjustment gave the internal precision criteria of the free networks (variants 1, 2, 3 & 4) and Figure (2).

5- In free geodetic networks, internal precision decreases as we move towards external boundaries of the network, while internal precision is a maximum around the network centroid.

II- Table (3) gives the common global precision criteria for the four variants of the network. From these results, it can be noted that:

Table (3): The common global precision criteria

	Variant (1)	Variant (2)	Variant (3)	Variant (4)
	8-Fixed points A,B,C,D,E,F,G,H	6- Fixed points A,B,C,D,E, & F	4- Fixed points A,B,C & D	Free Network
trace ($Q_{\hat{x}}$)*	14.16	19.05	27.31	9.91
σ_C (cm)	0.94	1.09	1.31	0.79
σ_N (cm)	1.33	1.53	1.85	1.11
det ($Q_{\hat{x}}$)*	0.12	2.79	30.98	0.01
σ_W (cm^4)	0.77	1.14	1.54	0.56
λ_{max} (cm^2)	1.51	2.31	2.76	1.04
λ_{min} (cm^2)	0.59	0.59	0.74	0.31
$\lambda_{max} - \lambda_{min}$ (cm^2)	0.92	1.72	2.02	0.73
$\lambda_{max} / \lambda_{min}$*	2.56	3.92	3.73	3.35

* unitless

1- As the number of the fixed points in the network decrease, the numerical values of trace ($Q_{\hat{x}}$), det ($Q_{\hat{x}}$) and the all external global precision criteria increase (see variants 1, 2, & 3).

2- The trace and the determinant of the weight coefficient matrix and the all external global precision criteria depend upon the choice of least squares adjustment techniques and the computational base.

3- Free network adjustment using inner constrained approach (variants 4) gave also the smallest numerical values of all global precision criteria. This means that, the numerical values of internal global precision criteria in free networks were less than the values of external global precision criteria in fixed networks.

III- Table (4) shows the internal weight coefficients which are used to compute the internal positional errors of the estimated net-points, while table (5) shows the external and internal positional errors of the estimated net-points as well as the external and internal mean network errors for the four network variants. Comparison of the numerical values for both external and internal precision criteria showed that:

1- In fixed geodetic network, the internal positional errors are always smaller than external positional errors of the estimated net-points.

2- In free geodetic network, $\sigma_{P_i} = (\sigma_{P_i})_{in}$. This means that, the common positional error (σ_{P_i}) describe the internal precision of the estimated net-points and it can be calculated directly from the variance-covariance matrix ($C_{\hat{x}}$) using equation (9). Therefore, *it is not necessary to calculate the internal weight coefficients* ($Q_{S_iS_i}$), ($Q_{q_{ri}q_{ri}}$) and ($Q_{P_iP_i}$)$_{in}$.

3- The external positional errors of the estimated net-points (σ_{P_i}) as well as the external mean network error (σ_N) were dependent on choice of the reference datum.

4- As the number of fixed points for geodetic networks decrease, the numerical values of both external and internal positional errors of the estimated net-points and also external and internal mean network errors increase (see variants 1, 2 & 3).

5- Internal positional errors of the estimated net-points and internal mean network error in free geodetic networks gave the biggest numerical values than those obtained for fixed networks (see variants 1, 2, 3 & 4) and Figure (3).

Table (4): The internal weight coefficients of the estimated net-points

		Variant (1)	Variant (2)	Variant (3)	Variant (4)
		8-Fixed points A,B,C,D,E,F,G,H	6- Fixed points A,B,C,D,E, & F	4- Fixed points A,B,C & D	Free Network
$Q_{S_iS_i}$ (unitless)	P_1	0.365	0.385	0.495	0.696
	P_2	0.365	0.685	0.689	0.696
	P_3	0.501	0.569	0.622	0.623
	P_4	0.501	0.544	0.615	0.623
	P_5	0.501	0.527	0.615	0.623
	P_6	0.501	0.512	0.622	0.623
	P_7	0.365	0.428	0.495	0.696
	P_8	0.365	0.402	0.689	0.696
$Q_{q_{ri}q_{ri}}$ (unitless)	P_1	0.458	0.540	0.742	0.752
	P_2	0.458	0.665	0.748	0.752
	P_3	0.366	0.367	0.383	0.405
	P_4	0.366	0.399	0.400	0.405
	P_5	0.366	0.369	0.400	0.405
	P_6	0.366	0.379	0.383	0.405
	P_7	0.458	0.558	0.742	0.752
	P_8	0.458	0.478	0.748	0.752
$(Q_{P_iP_i})_{in}$ (unitless)	P_1	0.823	0.925	1.237	1.448
	P_2	0.823	1.350	1.437	1.448
	P_3	0.867	0.936	1.005	1.028
	P_4	0.867	0.943	1.015	1.028
	P_5	0.867	0.896	1.015	1.028
	P_6	0.867	0.891	1.005	1.028
	P_7	0.823	0.986	1.237	1.448
	P_8	0.823	0.880	1.437	1.448
$[Q_{PP}]_{in}$		6.760	7.807	9.388	9.904

Table (5): The external and internal positional errors of the estimated net-points (cm)

		Variant (1) 8-Fixed points A,B,C,D,E,F,G,H	Variant (2) 6- Fixed points A,B,C,D,E, & F	Variant (3) 4- Fixed points A,B,C & D	Variant (4) Free Network
External Precision	σ_{P1}	1.14	1.29	1.32	1.20
	σ_{P2}	1.14	1.94	2.10	1.20
	σ_{P3}	1.50	1.74	1.99	1.01
	σ_{P4}	1.50	1.69	1.88	1.01
	σ_{P5}	1.50	1.57	1.88	1.01
	σ_{P6}	1.50	1.60	1.99	1.01
	σ_{P7}	1.14	1.15	1.32	1.20
	σ_{P8}	1.14	1.17	2.10	1.20
	σ_{N}	1.33	1.53	1.85	1.11
Internal Precision	$(\sigma_{P1})_{in}$	0.91	0.96	1.11	1.20
	$(\sigma_{P2})_{in}$	0.91	1.16	1.20	1.20
	$(\sigma_{P3})_{in}$	0.93	0.97	1.00	1.01
	$(\sigma_{P4})_{in}$	0.93	0.97	1.00	1.01
	$(\sigma_{P5})_{in}$	0.93	0.95	1.00	1.01
	$(\sigma_{P6})_{in}$	0.93	0.94	1.00	1.01
	$(\sigma_{P7})_{in}$	0.91	0.99	1.11	1.20
	$(\sigma_{P8})_{in}$	0.91	0.94	1.20	1.20
	$(\sigma_{N})_{in}$	0.92	0.99	1.08	1.11

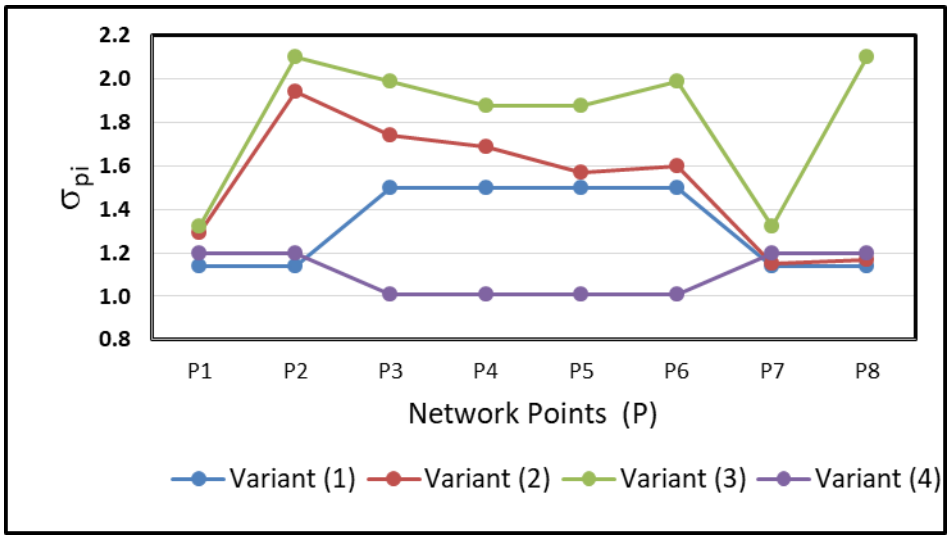


Figure (2): The external positional errors of the estimated net-points (cm)

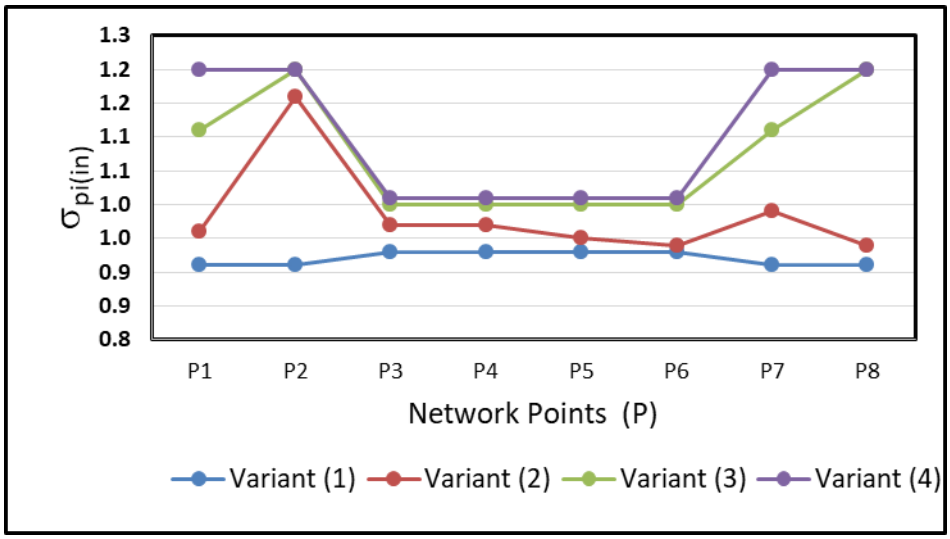


Figure (3): The internal positional errors of the estimated net-points (cm)

6- CONCLUSIONS

The following conclusions can be obtained from the previous discussions:

1- In fixed geodetic networks, positional errors of the estimated net-points have different geometrical meaning than those for the free networks. They describe the external precision for fixed networks and would be defined as external positional errors of the net-points, while they describe internal precision for free networks and would be defined as internal positional errors of the net-points.

2- In free geodetic networks, both internal positional errors of the net-points and internal mean network error would be calculated directly from the variance-covariance matrix of estimated net-points coordinates. In addition, the internal precision decreases at the external boundaries of the network and internal precision is a maximum around the network centroid.

3- In fixed geodetic networks, both internal positional errors of the estimated net-points and internal mean network error would be calculated by applying Eq. (33) and Eq. (35).

4- By calculating the internal precision criteria in fixed geodetic networks, comparison between both fixed and free geodetic networks is valid.

5- Both internal positional errors of the estimated net-points and internal mean network error in fixed geodetic networks are always smaller than both external positional errors of the estimated net-points and external mean network error.

6- In fixed geodetic networks, the net-points farthest away from the fixed points will obviously have the largest error ellipses and the biggest values of both internal and external precision criteria.

7- As the number of fixed net-points or outer constraints increase the internal precision of the geodetic network increase as well.

REFERENCES

1- Caspary, W., (2013). "Fehlertolerante Auswertung von Messdaten: Daten- und Modellanalyse, robuste Schätzung". OldenbourgWissenschaftsverlag.

2- Ghilani, C. D. (2018). "Adjustment Computations: Spatial Data Analysis". Sixth Edition. John Wiley & Sons, Inc., Hoboken, New Jersey.

3- Illner, I. (1995). "Datumsfestlegung in freien Netzen". *DGK*, Reihe C, Nr. 309.

4- Kahler, D. (1997). "Ein Beitrag zur Theorie der inneren Genauigkeit vontrans-formierten Punktkoordinaten", Zeitschrift für vermessungswesen, Stuttgart 112: 153-157.

5- Meissl, P. (1969). "Zusammenfassung und Ausbau der inneren Fehlertheorie eines Punkthaufen", Deutsche geodaetische Kommission, Reihe A, Heft Nr. 61, München: 8-21.

6- Niemeier, W. (1985). "Netzqualitaet und Optimierung", In Pelzer Hrsg. geodaetische Netze in Landes und Ingenieurvermessung II, Stuttgart, Konrad Wittwer Verlag, 153-224.

7- Niemeier, W. (2008). Ausgleichungsrechnung - Statistische Auswertemethoden " (2.überarbeitete und erweiterte Auflage): Walter de Gruyter.

8- Ogundare, J. (2019). "Understanding Least Squares Estimation and Geomatics Data Analysis." 1st Edition, Hoboken, NJ: John Wiley & Sons.

9- Wolf, H. (1981). "Innere Genauigkeit und Gausscher Algorithmus." Zeitschrift für Vermessungswesen, Stuttgart 106: 217-223.

مفهوم الدقة الخارجية والداخلية في الشبكات الجيوديسية الأفقية

هشام محمد شحاتة أبو حليمة
قسم الهندسة المدنية - كلية الهندسة - جامعة جازان- المملكة العربية السعودية

الملخص

لقد زاد فى السنوات الأخيرة إستخدام الشبكات الجيوديسية الأفقية الحرة فى الأعمال الهندسية المختلفة. وقد ظهر جلياً أنه عند مقارنة نتائج الشبكة الحرة بعد إجراء عمليات الضبط الخاصة بها بنتائج شبكة مربوطة أو ثابتة لها نفس الشكل ونفس خطة الأرصاد ومقاسة تحت نفس الظروف الطبيعية وجد أن الشبكات الحرة تعطى قيما عددية لمعايير الدقة المعروفة أقل من القيم العددية لمعايير الدقة للشبكات المربوطة خلافاً للمتوقع وعليه فإن هذا البحث يهدف إلى دراسة وتحليل هذه الظاهرة لمعرفة أسبابها عن طريق تفسير إختلاف المفهوم الهندسى لمعايير الدقة فى كل من الشبكات الجيوديسية الحرة والشبكات المربوطة بهدف الوصول إلى معايير جديدة مناسبة لوصف الدقة الداخلية للشبكات المربوطة والتي يمكن عن طريقها إجراء المقارنة الصحيحة بين دقة الشبكات الحرة والشبكات المربوطة. وقد تم الإستعانة بشبكة جيوديسية أفقية محلية كمثال تطبيقى حيث تم ضبطها عدة مرات بمتغيرات مختلفة لتلائم هذه الدراسة.

الكلمات المفتاحية: معايير الدقة ، الدقة الخارجية ، الدقة الداخلية ، أخطاء التموضع ، المفهوم الهندسي للدقة - مركز (النقطة الوسطي) للشبكة ، القاعدة الحسابية.

Applications of feature selection-based approach to detect web application vulnerabilities

Waleed Abdu Zogaan
Department of Computer Science, Faculty of Computer Science and Information Technology, Jazan University, Saudi Arabia

Abstract:
Today, web applications are widely used by millions of companies and other organizations to facilitate and offer their services on the internet. However, building a secure environment for these websites is expensive and challenging. Feature Selection (FS) methods are effectively employed to detect such vulnerable components in web applications. These techniques can bring accurate results by specifying the most informative features, enabling developers and managers to monitor and control their websites better. Therefore, this paper uses Dwarf Mongoose Optimization Algorithm (DMOA) as a metaheuristic FS-based approach to select the optimal informative feature subset. The DMOA is validated on an open-source dataset for web application vulnerability. Overall experimental results show that DMOA achieves better performance outcomes with a faster convergence speed compared to Particle Swarm Optimization (PSO), Aquila Optimizer (AO), Reptile Search Algorithm (RSA), and Snake Optimizer (SO) FS methods.

Keywords: Web security, detection, metaheuristic algorithms, Feature selection, machine learning.

1. Introduction

Web applications represent the most cost-effective manner for providing facilities to millions of businesses and organizations to offer their services on the internet. The flexible accessibility provided by these services made an individual's life more accessible and conformable, shaped the world, and turned the universe into a global

village [1]. On the other side, this flexibility makes them vulnerable to many different categories of attacks from malicious users because attackers use sophisticated attackers to circumvent these services. For instance, an XSS attack ranked as the second type due to the available tools to launch this attack with minimum knowledge to attack web applications [2].

Information exploitation and web vulnerability threaten web applications, confirming the additional requirements for security measures. Since testing is typically performed manually and with high precision, it is very demanding. It is hard to defend against developer carelessness, and therefore, could lead to several types of vulnerabilities in the code, which on the other hand, could be later exploited [3]. Static, dynamic, and hybrid analysis methodologies all have drawbacks. The disadvantage of static analysis is that not all programming languages are supported, and the findings produced by static analysis tools frequently contain false positives. Dynamic analysis tools cover not all the execution paths, generating high false positives and negatives. [4], while the hybrid analysis method uses both types of analysis to detect such attacks. However, this analysis approach takes a long time in the analysis process and is time-consuming [5 -7]. In order to resolve the problems mentioned above, hybrid analysis and Machine Learning (ML) are required.

Recently, ML and Meta-Heuristic (MH) methods have shown great potential in web security applications. In [8], the authors used MH along with a nonlinear regression algorithm as an effective manner for website phishing. In [9], multiple FS methods are employed to choose the most critical features, and then the selected ones are used as inputs to the Support Vector Machine (SVM) for Intrusion Detection (ID). In [10], a method for detecting XSS attacks is presented using three ML models, including naive Bayes, SVM, and decision trees, to detect XSS. In this method, the authors used a manual feature extraction technique to specify the most informative features to train ML models. In [11], ML approaches are used to classify user inputs using blank separation and tokenizing to detect malicious web code. In [12], the authors employed Genetic Algorithm (GA) to detect cross-site-scripting from source code before deploying an application. In another work [13], the authors combined GA and Reinforcement Learning (RL) to tackle the problem of XSS attack. In [14], two MH methods are incorporated for a better feature selection: Moth flame optimization and hill climbing for ID.

MH methods are popular in FS research because of their strong self-learning capabilities, which can maintain a relatively high detection accuracy of such vulnerabilities in web applications. The main contributions of this paper can be summarized as follows:

- Applications of feature selection-based approach using the DMOA method to detect web application vulnerabilities is presented
- The effectiveness of the DMOA approach is investigated using several quantitative evaluation measures, including accuracy, fitness values, and the number of seceded features on a publically available dataset for web vulnerabilities
- The performance of DMOA is also compared with some other MH: PSO [15], AO [16], RSA [17], and SO [18].

The remaining parts of this paper are structured as follows: In section 2, a brief overview of the DMOA is described. Section 3 presents experimental results, datasets description, evaluation metrics, and discussion. The concludes of this work with future research directions are provided in Section 4,

2. Dwarf Mongoose Optimization Algorithm (DMOA)

DMOA is an MH method [19] introduced in 2022 to simulate the behavior of prey size limitation, social organization, partial traveling life, and others of the dwarf mongoose. The DMOA begins with initializing a set of random candidate populations of mongooses between the Upper Boundary (UB) and Lower Boundary (LB) of the given problem. The

optimization process is represented in the following phases:

Alpha group

After population initialization, the probability value for the suitability of each population can be computed as follows:

$$\alpha = \frac{fit_i}{\sum_{i=1}^{n} fit_i} \quad (1)$$

The number of mongooses in the α group is represented by $\alpha - bs$, where bs is the number of babysitters and $peep$ s the vocalization made by the alpha female to guide the family along a path. Every mongoose sleeps in the first sleeping mound. The DMOA employs the following in order to generate a candidate food position:

$$X_{i+1} = x_i + phi + peep \quad (2)$$

where phi is a random number in the range of [0, 1]
After every iteration, the sleeping mound sm can be given as:

$$sm_i = \frac{fit_{i+1} - fit_i}{max[fit_{i+1}, fit_i]} \quad (3)$$

Table 1. Dataset description

Dataset	Year	No. of features	No. of samples
ICML-09	2009	29,09,162	23,96,000

While the Average (Avg) value of the sm can be represented as :

$$\text{Avgsm} = \frac{\sum_{i=1}^{n} sm_i}{n} \quad (4)$$

In the next (scouting) phase, DMOA fulfills the babysitter exchange condition, followed by an assessment of a new food source.

1. Scout group

Mongooses never return to the previous sleeping mound, and hence, this phase seeks the next sm. This movement, influenced by the overall mongooses' performance, guarantees exploration as the family eats sufficiently. The scout mongoose can be presented as in Eq (5). X_i is a vector that controls how the mongoose moves to the new sm, CF a parameter that controls the collective-volition movement, and it is reduced linearly at the same time as iterations, $rand$ is a random number in the range of [0, 1] and $\vec{M}$ is a mongoose's motion vector to the new sm.

2. The babysitters

Babysitters stay with the youngsters and are toured periodically to facilitate the female alpha (i.e. the mother) to lead. She comes back at noon and in the evening to nurse and serve the little ones. The population affects DMOA as it decides the number of caretakers.

3. Experimental results

This section briefly describes the collection of vulnerable and regular URLs, the selection of parameters of different search optimization algorithms, and evaluation measures. Finally, experimental results are discussed and the hypothesis is tested using a statistical test.

3.1.Experimental setup

In this section, a dataset regarding web vulnerabilities used for evaluation and experimental parameter settings for DMOA and four competing optimization algorithms is discussed. This dataset was published in 2009 and comprises two URL feeds collecting a total of 20,000 URLs per day except for zeros-day, which has 16,000 URLs [20]. The average ratio of benign to malicious URLs is 2:1. The experiment was conducted for 120 days, resulting in a total of 23, 96,000 URLs, and each of them is represented using 29, 09,162 features. The dataset is summarized in Table 1.

The common parameters in this study, such as population size and the maximum number of iterations, are empirically set as 20 and 100, and each method is independently run 20 times to avoid random behavior and achieve reliable

$$X_{i+1} = \begin{cases} X_i - CF * phi * rand[X_i - \overrightarrow{M}] \\ X_i - CF * phi * rand[X_i - \overrightarrow{M}] \end{cases} if \ \text{Avgsm}_{i+1} > \text{Avgsm}_i \quad (5)$$

where,

$$CF = \left(1 - \frac{iter}{max_{iter}}\right)^{2\frac{iter}{max_{iter}}} \quad \text{and} \quad \vec{M} = \sum_{i=1}^{n} \frac{X_i * sm_i}{X_i}$$

statistical evaluation. All the methods are executed as per their implementations in their original work. The parameter settings used for this method are given in Table 2. All the experiments are conducted on a computer with a 3.13 GHz PC with 32 GB RAM and Ubuntu 22.04.1 LTS operating system and implemented using Python Scikit-learn.

3.2. Evaluation measures

In this section, the most commonly used evaluation measures to evaluate detection systems are discussed to compare the DOMA and the other four competing algorithms. Considering the hypothesis for detecting vulnerable URLs (positive cases), various measures can be used to evaluate DMOA efficiency, and they are calculated as follows:

$$AC = \frac{TP + TN}{TP + TN + FN + FP} \quad (6)$$

$$\text{Precision} = \frac{TP}{TP + FP} \quad (7)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (8)$$

$$\text{F1-score} = \frac{2\,P\,R}{P + R} \quad (9)$$

where, True Positive (TP) and True Negative (TN) denote the examples of URLs correctly detected as vulnerable or regular. False Positive (FP) represents regular URLs misclassified as vulnerable. On the other hand, False Negative (FN) denotes the vulnerable URL incorrectly predicted as regular. If several regular URLs are predicted as vulnerable, then FP increases, which results in decreased precision. Similarly, if many vulnerable URLs are not detected, then FN increases and recall decreases. It must be noted that for most real-world vulnerability detection systems decrease in the recall is more critical than precision.

3.3.Experimental results and discussion

In this section, the efficiency of the DMOA is examined and discussed using the real-world dataset provided in Table 1. Table 3 gives the fitness value and Standard Deviation (STD) of the DMOA

Table 3. Comparative performance analysis of the fitness values from different MH methods

Metric	PSO	RSA	SO	AO	DMOA
Best	0.0369	0.0406	0.0340	0.0310	**0.0306**
Worst	0.0714	0.0713	0.0653	0.0643	**0.0631**
Avg.	0.0413	0.0432	0.0375	0.0372	**0.0348**
STD.	0.0082	0.0047	0.0053	0.0057	**0.0052**

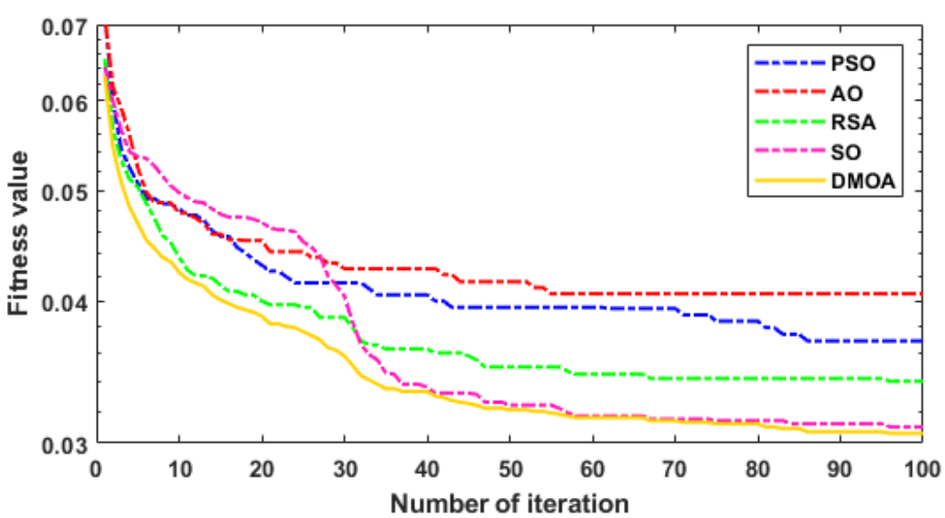


Figure. 1. Convergence behavior of PSO, AO, RSA, SO, and DMOA using ICML-09 dataset for malicious URL detection.

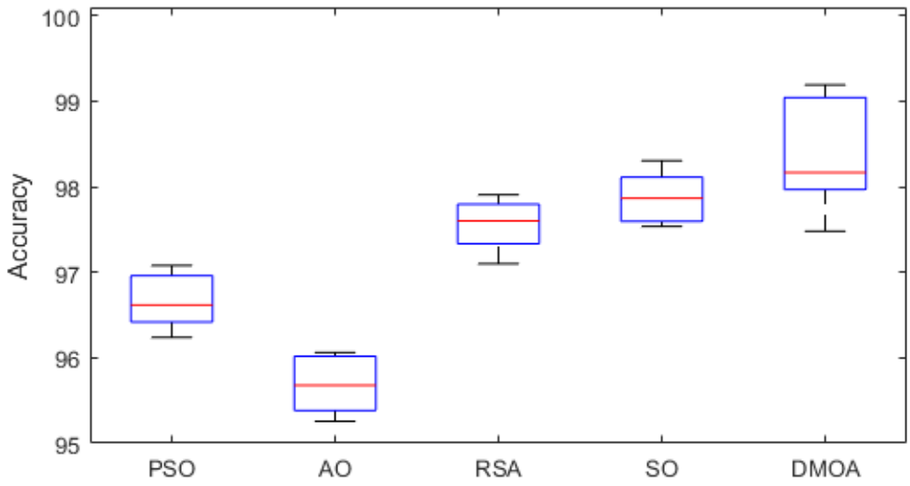
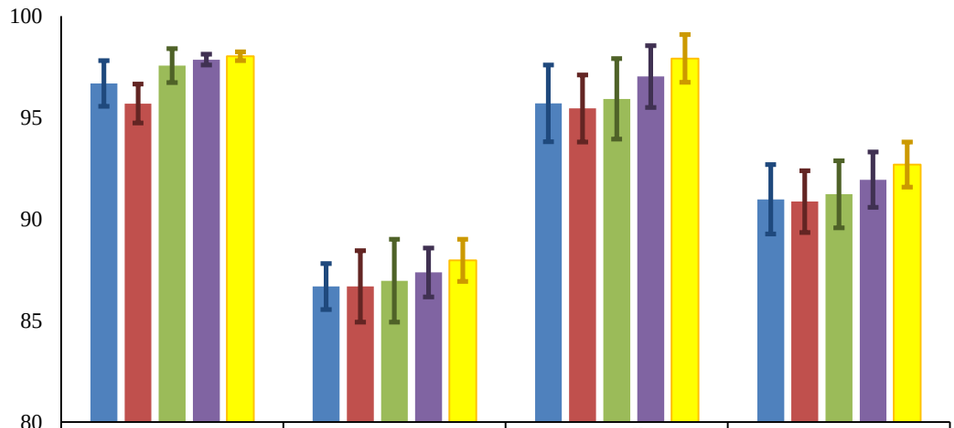


Figure 2. Box plot of the accuracy of MH methods using ICML-09 dataset malicious URL detection.



	Accuracy	Precision	Recall	F1-score
PSO	96.68	86.68	95.7	90.97
AO	95.69	86.69	95.45	90.86
RSA	97.56	86.96	95.92	91.22
SO	97.85	87.37	97.02	91.94
DMOA	98.02	87.97	97.91	92.68

Figure 3. Quantitative comparison of MH methods using ICML-09 dataset malicious URL detection

and other methods. As per the results in table 3, the DMOA got the best and the smallest results in terms of fitness and STD, which reflects its stability as an FS method compared to PSO, MVO, SSA and. AOA methods.

Figure 1 shows the convergence behavior of all the methods. From this figure, it can be seen that the DMOA has a faster rate of convergence speed than that of the other competitors over the defined number of iterations, while SO ranked second, followed by RSA, PSO, and AO.

The box plot is also used to check out the distribution of accuracy obtained by each method, as given in Figure 2. It shows that DMOA achieved the best results compared to trot PSO, AO, RSA, and AO methods.

The results in terms of the evaluation measurements are illustrated in Figure 3. This figure shows that DMOA has the best outcomes in terms of all the used measures. Overall the results confirm that DMOA can be used as an FS method for detecting malicious websites.

3.4.Statistical test

Five MH algorithms with 20 independent runs are subjected to the Friedman test, a popular non-parametric two-way analysis of variances by ranks [47], to determine the relevance of the performance evaluation metrics. The test assumes that the comparison methods perform equally under the null hypothesis (H_0), while the alternative hypothesis (H_1) assumes that the performance of the comparative MH

algorithms differs. The algorithm with the highest accuracy ranking is the best because it prefers greater values. On the other side, because smaller values are chosen, the lowest rank is best for OFS and fitness as provided in Table 4.

In Table 4, the average ranks for five FS algorithms with significance level α=0.05. The highest p-value calculated using Friedman's test for all five datasets was 0.0012, which is less than desired α, indicating that the results are statistically significant. The DMOA gained the best accuracy, OFS, and fitness value. Statistically, AO has best feature selection has it is shown in improved rank for fitness even when accuracy is worst out of all five of them. Similar improvement in fitness rank is shown by PSO compared to RSA.

4. Conclusion and future works

In this paper, DMOA based FS approach is presented, and an open-source web vulnerability dataset is used to test the efficacy of the DMOA. Results show that the DMOA method gained better results than PSO, AO, RSA, and SO in terms of accuracy, fitness values, and the number of selected features, and its convergence speed is faster than the other comparative methods. In the future, DMOA can be used in different applications such as intrusion detection, signal processing, and big data. Another possible avenue is to work on other MH methods to be applied as an FS in the application of web security because these optimization algorithms have shown great potential in other domains.

Table 4: Friedman ranking results for the five MH algorithms across all metrics.

Metric	PSO	AO	RSA	SO	DMOA
ACC	2.85	2.75	2.90	3.10	**3.40**
OFS	3.55	2.85	3.21	3.05	**2.40**
Fitness	3.20	2.55	3.45	2.95	**2.35**

References

[1] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 7(1), 1-29.

[2] Almuhaideb, A. M., & Alynanbaawi, D. Y. (2022). Applications of artificial intelligence to detect android botnets: A Survey. IEEE Access, 10, 71737-71748. Medeiros, I., Neves, N., & Correia, M. (2015). Detecting and removing web application vulnerabilities with static analysis and data mining. IEEE Transactions on Reliability, 65(1), 54-69.

[3] Huang, H. C., Zhang, Z. K., Cheng, H. W., & Shieh, S. W. (2017). Web application security: threats, countermeasures, and pitfalls. Computer, 50(6), 81-85.

[4] Seh, A. H., Al-Amri, J. F., Subahi, A. F., Ansari, M. T. J., Kumar, R., Bokhari, M. U., & Khan, R. A. (2022). Hybrid computational modeling for web application security assessment. CMC-Comput., Mater. Continua, 70(1), 469-489.

[5] Abunadi, I., & Alenezi, M. (2016). An empirical investigation of security vulnerabilities within web applications. J. Univers. Comput. Sci., 22(4), 537-551.

[6] Gupta, S., & Gupta, B. B. (2017). Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. International Journal of System Assurance Engineering and Management, 8(1), 512-530.

[7] Shahid, W. B., Aslam, B., Abbas, H., Khalid, S. B., & Afzal, H. (2022). An enhanced deep learning based framework for web attacks detection, mitigation and attacker profiling. Journal of Network and Computer Applications, 198, 103270.

[8] Babagoli, M., Aghababa, M. P., & Solouk, V. (2019). Heuristic nonlinear regression strategy for detecting phishing websites. Soft Computing, 23(12), 4315-4327.

[9] Vishnu, B. A., & Jevitha, K. P. (2014, October). Prediction of cross-site scripting attack using machine learning algorithms. In Proceedings of the 2014 International Conference on Interdisciplinary Advances in Applied Computing (pp. 1-5).

[10] Komiya, R., Paik, I., & Hisada, M. (2011, September). Classification of malicious web code by machine learning. In 2011 3rd International Conference on Awareness Science and Technology (iCAST) (pp. 406-411). IEEE.

[11] Hydara, I., Sultan, A. B. M., Zulzalil, H., & Admodisastro, N. (2014, October). An approach for cross-site scripting detection and removal based on genetic algorithms. In The Ninth International Conference on Software Engineering Advances ICSEA.

[12] Tariq, I., Sindhu, M. A., Abbasi, R. A., Khattak, A. S., Maqbool, O., & Siddiqui, G. F. (2021). Resolving cross-site scripting attacks through genetic algorithm and reinforcement learning. Expert Systems with Applications, 168, 114386.

[13] Kumar, B. V. (2021). Hybrid metaheuristic optimization based feature subset selection with classification model for intrusion detection in big data environment. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(12), 2297-2308.

[14] Bhagwat, S., & Gupta, G. P. (2022). Android Malware Detection Using Hybrid Meta-heuristic Feature Selection and Ensemble Learning Techniques. In International Conference on Advances in Computing and Data Sciences (pp. 145-156). Springer, Cham

[15] Abualigah, L., Yousri, D., Abd Elaziz, M., Ewees, A. A., Al-Qaness, M. A., & Gandomi, A. H. (2021). Aquila optimizer: a novel meta-heuristic optimization algorithm. Computers & Industrial Engineering, 157, 107250.

[16] Abualigah, L., Abd Elaziz, M., Sumari, P., Geem, Z. W., & Gandomi, A. H. (2022). Reptile Search Algorithm (RSA): A nature-inspired meta-heuristic optimizer. Expert Systems with Applications, 191, 116158.

[17] Hashim, F. A., & Hussien, A. G. (2022). Snake Optimizer: A novel meta-heuristic optimization algorithm. Knowledge-Based Systems, 242, 108320.

[18] S. Mirjalili, A. H. Gandomi, S. Z. Mirjalili, S. Saremi, H. Faris et al., "Salp swarm algorithm: A bio-inspired optimizer for engineering design problems," Advances Engineering Software, vol. 114, pp. 163–191, 2017.

[19] Abualigah, L., Diabat, A., Mirjalili, S., Abd Elaziz, M., & Gandomi, A. H. (2021). The arithmetic optimization algorithm. Computer methods in applied mechanics and engineering, 376, 113609.

[20] Agushaka, J. O., Ezugwu, A. E., & Abualigah, L. (2022). Dwarf mongoose optimization algorithm. Computer methods in applied mechanics and engineering, 391, 114570.

[20] Betarte, G., Pardo, Á., & Martínez, R. (2018, December). Web application attacks detection using machine learning techniques. In 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA) (pp. 1065-1072). IEEE.

منهجية معتمدة على اختيار الخصائص لرصد ثغرات تطبيقات الويب

وليد عبده زعقان

قسم علوم الحاسب الآلي، كلية علوم الحاسب وتقنية المعلومات، جامعة جازان، المملكة العربية السعودية

الملخص

في هذه الأيام، تطبيقات الويب يتم استخدامها من قبل ملايين الشركات والمنظمات لإتاحة وإدارة خدماتها المقدمة عبر الأنترنت. رغم ذلك فإن بناء بيئة آمنه لهذه المواقع هو شي مكلف وفيه الكثير من التحديات. التقنيات المبنية على اختيار الخصائص تم توظيفها بشكل فعال لرصد الثغرات الأمنية في هذه التطبيقات. هذه التقنيات قادرة على تحقيق نتائج دقيقة عن طريق تحديد الخصائص الأكثر دلالة مما يمكن مطوري ومدراء الأنظمة من مراقبة مواقعهم الإلكترونية والتحكم بها بشكل أفضل. لذلك يهدف هذا البحث لاستخدام خوارزمية DMOA ضمن منهجية مبنية على اختيار الخصائص وذلك لاختيار مجموعة الخصائص الأمثل والأكثر دلالة لرصد الثغرات في تطبيقات الويب. تم تطبيق منهجية DMOA على مجموعة بيانات مفتوحة المصدر لثغرات في تطبيقات الويب. بشكل عام أظهرت نتائج الاختبارات ان المنهجية المقترحة في هذا البحث والمبنية على خوارزمية DMOA حققت أداء وسرعة أفضل من بالمقارنة مع مجموعة من الخوارزميات الأخرى.

الكلمات المفتاحية: آمن الويب، رصد الثغرات، خوارزميات Metaheuristic، اختيار الخصائص، تعلم الآلة.

PREDICTION OF SCOUR AT BRIDGE ABUTMENT USING ARTIFICIAL NEURAL NETWORKS

Yasser, A.M. Moussa

Civil engineering Department. College of Engineering. Jazan University

ABSTRACT

For effective foundation design, it is crucial to estimate the local scour depth for bridge abutments provided with scour countermeasures such collars. To forecast the maximum local scour depth at bridge abutments with various collar designs, artificial neural networks (ANNs) utilized a variety of experimental findings that were gathered from the literature. Levenberg-Marquardt algorithm is used to train a multilayer back-propagation method with one hidden layer, which produces the most accurate and general neural network. The outcomes of the ANN model are contrasted with those of the MLR model and numerical simulation. The proposed model for predicting local scour depth using ANNs was shown to have good results (R^2= 98.3%, standard error= 0.03) as compared to numerical simulation (R^2= 97.4, standard error= 0.04). In addition, the MLR model is less effective than ANNs and numerical models for predicting local scour at bridge abutments (R^2 = 80% and standard error = 0.11). These results share to have safe foundation for constructed bridges in valleys and streams.

Keywords: ANN; Hydraulic structure; Bridge abutments; Local Scour; MLR

1. INTRODUCTION

Scour around foundation of hydraulic structures is responsible for nearly 60% of bridge failure as reported by manual of bridge maintenance (Richardson and Davis, 2001). U.S. Federal Highway Administration carried out studies about the failure of 383 bridge. It was found, pier and abutment involved in 25% and 72% for bridge failure, respectively (Richardson and Abed, 1993). Nemours of studies about bridge failure were investigated (Johnson and Dock, 1998; Melville, 1999). The scour types that affects bridge safety are, local scour, contraction scour and degradation scour (Parker et al. (1997)). Scour countermeasures is divided into, armoring and flow altering countermeasures. Armoring countermeasures include adding an extra layer of mobile grains to resist shear stress and therefore protecting the erodible material underneath. Flow altering countermeasures aim to modify the harmful effect of flow characteristics by using spur dikes, guide banks, parallel walls, collars, etc., and therefore minimizing scour at bridge foundations, (Deng and Cai, 2010). Different types of scour countermeasures are investigated (Lagasse et al. (2007); Barkdoll et al. (2007)). The local scour depth at abutments was investigated (Richardson and Davis, 2001; Sturm, 2006; Kose and Yanmaz, 2010). Numerical studies deal with simulation of scour around abutments were carried out (Pu and Lim, 2013;Teruzzi and Ballio, 2016). Experimental and numerical investigation of scour around abutment provided with different arrangements of collar were studied (Abdel-Aal et al. 2010; Mohamed et al., 2016a, b; Nasr-Allah et al. 2016). The artificial intelligence using artificial neural networks was used in different fields of engineering (Li et al. 2005; Xie et al. 2006). Azmathullah, (2006) studied the local scour depth downstream spillways using feed forward network of ANN. Sung-Uk and Sanghwa, (2006) estimated local scour around bridge piers using ANN. Muzzammil, (2008) studied the scour formed at bridge abutment using ANNs. Analysis of experimental data sets were performed for local scour depth around bridge abutments using artificial neural networks (Şarlak and Tiğrek, 2011). ANN is used to predict the local scour depth versus time around bridge abutment by Mohammaddpour et al. (2013). In which, the artificial neural networks (ANN) is considered as a computational model, simulates the human nervous system to recognize the sub symbolic pattern of data processing (Kasabov and Nikola, 1998). The

processing elements of ANN are arranged in layers that connected by weights. The process element, which is the decision maker of the neural network system, implies two functions; the first one is a sum function (input function) while the second function is the firing function (out function). The neural network system is trained (adjusting the weights values) by training algorithm, which can be considered as a mapping between the domain and the solution space of the problem. Many researchers stated that the feed-forward multilayer neural networks which has at least one hidden layer and its processing elements has an input function (summation) and activate function (sigmoid functions) can simulate approximately any measurable function (Kurt Hornik et al. 1989; Cybenkot, 1989). Supervised learning (learning with a teacher) is the most popular and simple training algorithm to map set of noisy training sample of input (excitation) and output (responses) for the evaluated function (Cornelius and Leondes, 1998). Supervised learning is an algorithm in which the input vector and its output answer is presented to the network and the network's weight are corrected (training network) according to the difference between the actual and simulated results. several algorithms are used to train multilayer neural networks. Back-propagation learning algorithm has been the most fully considered and used supervised learning algorithms for neural networks (Ra´ul Rojas, 1996). Back-propagation algorithm is an ineffective algorithm because of it slow converge and local minimum error. Levenberg–Marquardt algorithm make the convergence of the neural network training operation is stable and fast (Bogdan et al. 2011).

1.1 OBJECTIVE OF PRESENT RESEARCH

In the present work, the ANN was applied to simulate the local scour around different shapes of bridge abutments provided with different arrangements of collar. The Levenberg–Marquardt back propagation algorithm is used to train a multi-layer neural network to mapping the relationship between the scour around bridge abutment with respect to the measured values; tail Froude ($v/(gy_t)$^0.5; v: is flow velocity, g; gravitational acceleration, and y_t: tailwater depth) number, expansion ratio(e= B/(B-2b); B: channel width, and b: abutment width) , entrance angle and shape of abutment, and collar dimensions, see Fig.1 and Table1

2. EXPERIMENTAL WORK

The Artificial neural networks through the present study used experimental data (Mohamed et al., 2016a, 2016b; Nasr-Allah

et al. 2016) to correlate the local scour depth with other independent parameters. Table 1 and Fig. 1 present the details of experimental conditions and different arrangements of bridge abutment and collar around it. Details of experimental procedures were clarified (Mohamed et al., 2016a, 2016b; Nasr-Allah et al. 2016).

Table 1. Details of experimental conditions (Mohamed et al., 2016a, 2016b; Nasr-Allah et al. 2016)

Discharge (l/s)	3.5
Median sand size (mm)	1.77
Flow depth (cm)	3 to 7
Froude Number	0.20 to 0.55
Abutment width (b) cm	3.75, 5.0, and 7.5
Entrance angle of abutment (θ) (Degree)	10, 15, 30, 45, 60, and 90^0
Collar width (L_1) cm	4.5 , 6 and 7.5
Radii arrangement of abutment (cm)	0, 1.5, 3, 4.5, 6, 7.5, 10.5, 18.5, 30.5, and 100
Collar Length (L_c) cm	12, 13.5, 15, 20.5, 29, 37.5, 46 and 52

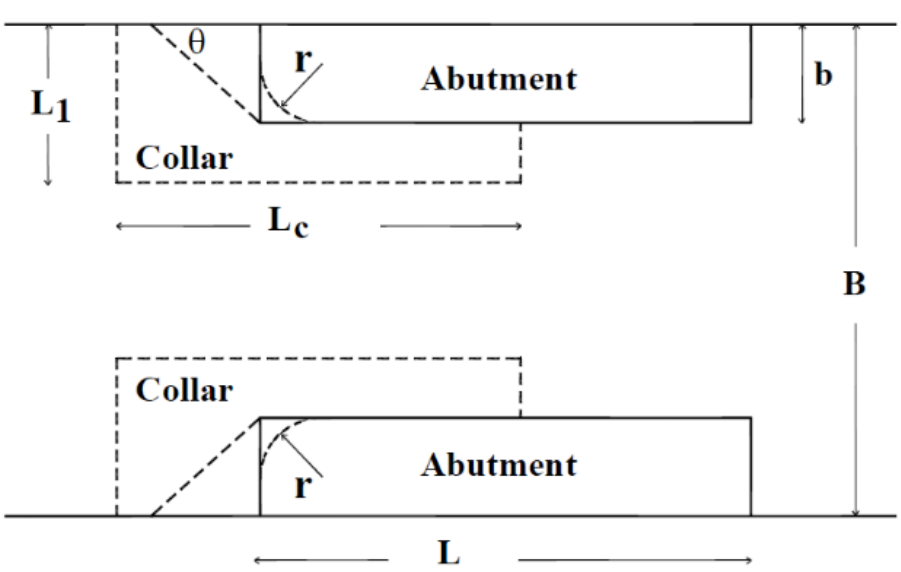


Fig.1 General view of experimental model

3. NEURAL NETWORK TRAINING

The data collected (Mohamed et al., 2016a, 2016b; Nasr-Allah et al. 2016) are set up in a form of matrix, each row (pattern) contains a sample input and its corresponding outputs. These patterns are divided randomly into three subsets; training, evaluation and test sets with ratios 40%, 20%, and 20% respectively (Ivan, 2017). The training set is used to adjust the weights and biases of the net. While the evaluation set is used to early stop the training operation if the network performance of this set remains the same or has not improved for the defined numbers of iterations. Thee last set is used to ensure the generalization of the net only. There are many factors affecting the training of the neural network to obtain the required performance; such as, net structure and the initial weight. The used neural network structure, Fig.2, consists of input layer, with 7 excitatory inputs, output layer, with one node, and only one hidden layer. The number of nodes in the used hidden layer are changed, to obtain the more accurate and generalize neural network. The common structure of the used nodes (neurons) is shown in fig.2. The connection weights are generated randomly between -1 and 1(Kasabov and Nikola 1998). Different sets of weights are used for each net structure, to obtain the more accurate and generalize neural network.

After preparing the previous sets and for each neural network (structure and set weights) the training process is made according the flowing steps;

1- Generate a random set of weights and biases, their values are between 1 and -1 (Kasabov and Nikola 1998).
2- Calculate the output of the net with the generating weights, and estimate the sum of square error (SSE) of the net, Eq. 1.

$$E(x,w) = \frac{1}{2}\sum_{p=1}^{P}\sum_{m=1}^{M} e_{p,m}^2 \qquad \text{Eq.1}$$

Where; E is the error vector

x is the input vector

w is the weight and bias vector

p is the pattern number

m is the output number.

$e_{p,m}$ is the difference between desired output and at output m when applying pattern p.

3- Update the weights according to equation Eq.2.

$$w_{k+1} = w_k - (J_k^T J_k + \mu I)^{-1} J_k e_k \qquad \text{Eq. 2}$$

Where; k is the index of iterations

J is Jacobian matrix

I is the identity matrix

μ is combination coefficient, positive large number

4- Estimate the SSE with the new weights set.

5- Compare resulting SSE of step 2 and 4;

a. If $SSE_{step2} < SSE_{step4}$
   1- reset the weight vector to the precious value
   2- Increase μ by a factor of
   3- Go to step 3.

b. If $SSE_{step2} > SSE_{step4}$
   1. Keep the new weight vector.
   2. Decrease μ by a factor of
   3. Go to step 3.

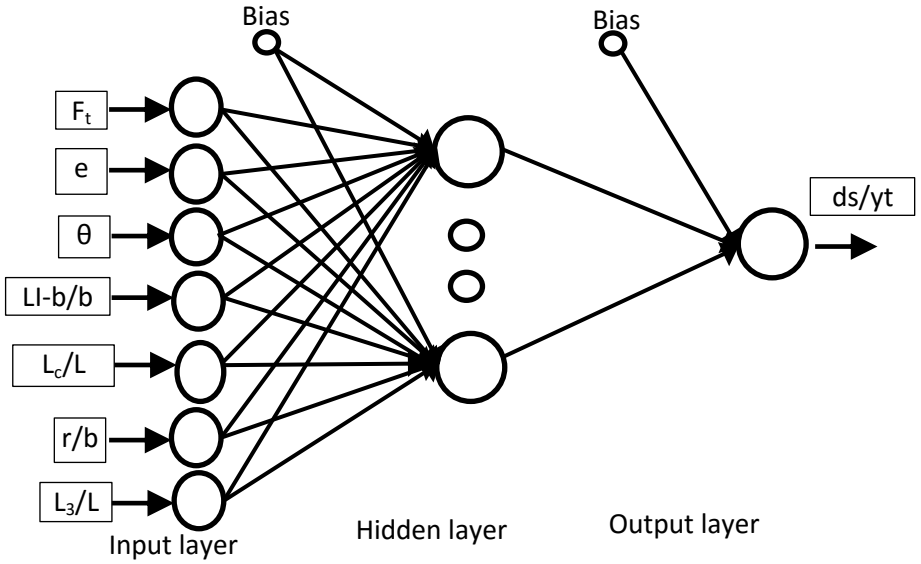


Fig. 2 The Multi-layer neural networks structure.

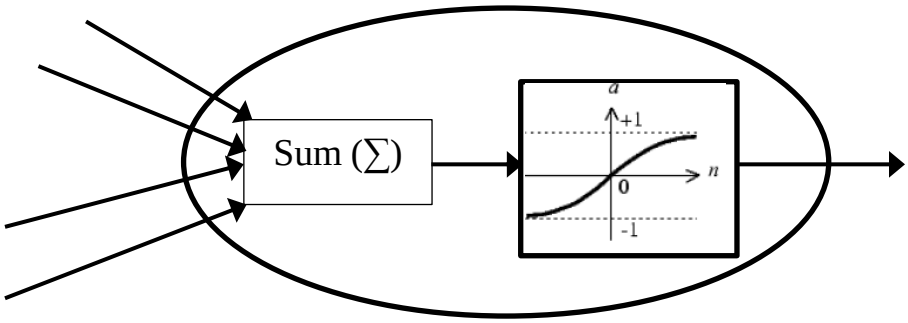


Fig. 3 The process elements structure.

These steps are applied to different structures of ANN. In which, different numbers of nodes in the hidden layer are examined. The number of nodes, in the hidden layer, are 7, 10 and 25. Each structure of artificial neural networks are trained many times with different initial weight sets (about 15 trails for each).

4. PREDICTED MODEL USING MLR

Multiple linear regressions were applied for all experimental data (Mohamed et al., 2016a, b; Nasr-Allah et al. 2016) to model the scour around bridge abutment that provided with collar. The proposed statistical model correlated the relative local scour depth with other independent parameters. Many trails were carried out to have the best equation for predicting local scour depth. The proposed equation has the following form;

$$\frac{d_s}{y_t} = -0.35 + 1.38\,F_t - 0.026e + 0.0034\theta + 0.03\frac{L_c}{L} + 0.003\frac{r}{b} + +0.33\frac{L_3}{L} \qquad \text{Eq.3}$$

The correlation coefficients and standard errors of Eq. 3 are 79%, and 0.11 respectively.

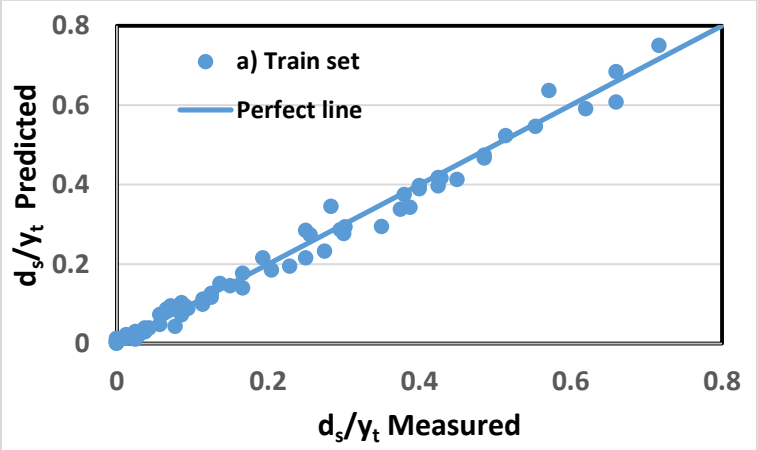
5. RESULTS AND DISCUSSION

As mentioned in the previous section several trails of multilayer back-propagation with one hidden layer are trained with Levenberg–Marquardt algorithm to obtain the most accurate and generalize neural network. The obtained neural network mapping the relation between the scour around bridge support with tail Froude number (F_t), expansion ratio (e), entrance angle (θ),Collar width and length ratios (L_c/L, and L_1/L), curvature ratio of abutment (r/b), and collar length ratio beyond abutment L_3/L. In the present study, different models of artificial neural networks (ANNs) were generated to predict the local scour depth around bridge abutment provided with collar around it. In the predicted models, different structures of artificial neural networks (ANNs) using different initial weights were generated. The best four developed models using ANN have the following structures; two neural networks of 7-7-1 and the other models have a structure of 7-10-1. The initial weights vary for each pair of neural networks. The coefficients of determination for the first pair (7-7-1), are 99.04% and 98.84%, while they are 99.12% and 98.82% for the second pair (7-10-1) of ANN. The simulation results using ANNs, showed that, the efficiently of artificial neural networks to model the local scour at bridge abutment provided with different arrangements of collar around it. The best structure of ANN, from all tested models, was (7-10-1). The proposed neural network, could be used for predicting local scour depth around bridge abutment provided with collar with high efficiency. Table 2 presents coefficients of determination and standard error for the simulated models based on; i) overall data set (145 patterns), ii) training data set (87 pattern), iii) evaluation data set (29 pattern), and iv) test data set (29 pattern). Table 3 presents the average absolute error between numerical and ANN models. The numerical model has average absolute error, for predicting relative scour depth, greater than ANN for data sets, (Overall pattern, training set, evaluation set and test set). The average absolute error for numerical simulation is twice or more compared with average absolute error for ANN models. Fig. 4a,b,c presents the actual versus simulated data for ds/yt for train, validation, and test data sets. The scour

depth at bridge abutment provided with different arrangements of collar was studied theoretically and experimentally (Mohamed et al., 2016a, 2016b; Nasr-Allah et al. 2016). The numerical models were created by applying SSIIM (sediment simulation in water intakes with multiblock option) program. This 3D CFD model was based on the finite volume method to solve the Navier-Stokes equations. The overall correlation coefficient (R^2) and standard error for the numerical results are 97.4%, and 0.04, respectively. Comparison between results of neural network and numerical model (Mohamed et al., 2016a, 2016b; Nasr-Allah et al. 2016) were clarified in Fig. 5. In addition, the actual and predicted results of relative scour depth by MLR were shown in Fig.6. Figures 5 and 6 clarified that, the simulated models of artificial neural networks, for predicting scour around abutment, is better than the numerical simulation and regression models (Eq.3).

Table 2. Standard error and coefficient of determination for the neural network 7-10-1.

Type of pattern	Standard error	Coefficient of determination R^2
Over all pattern	0.032	0.98255
Training set	0.021	0.993255
Evaluation set	0.036	0.978292
Test set	0.050	0.944133



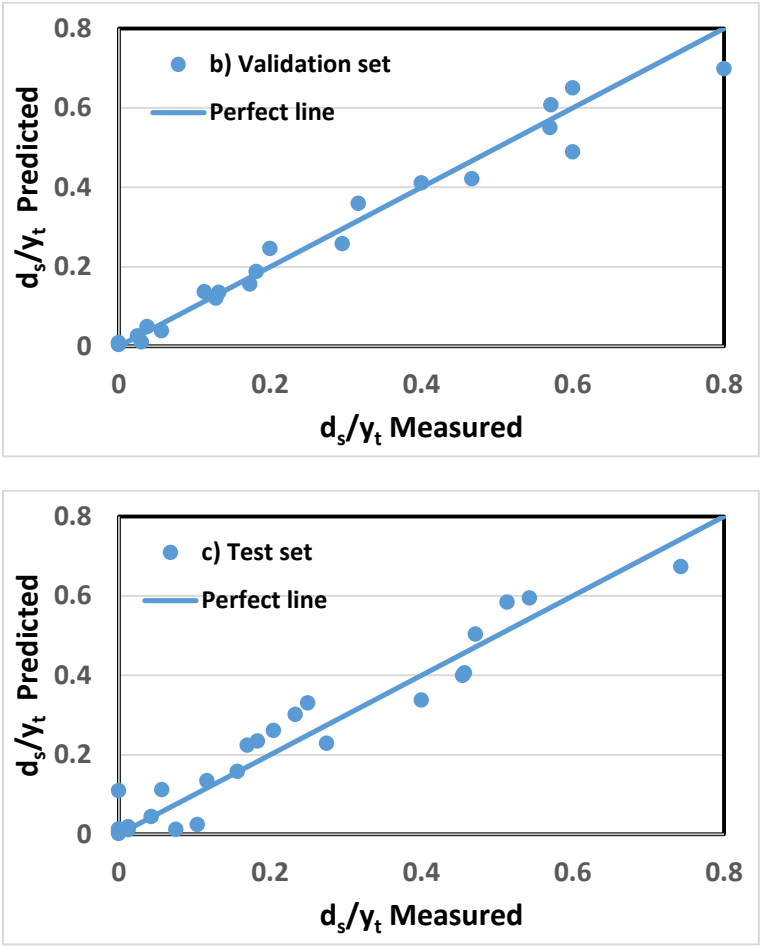


Fig. 4 Actual data of d_s/y_t versus Simulated data using ANN has structure of 7-10-1 for a) Train data set, b) Validation data set, and c) Test Data set.

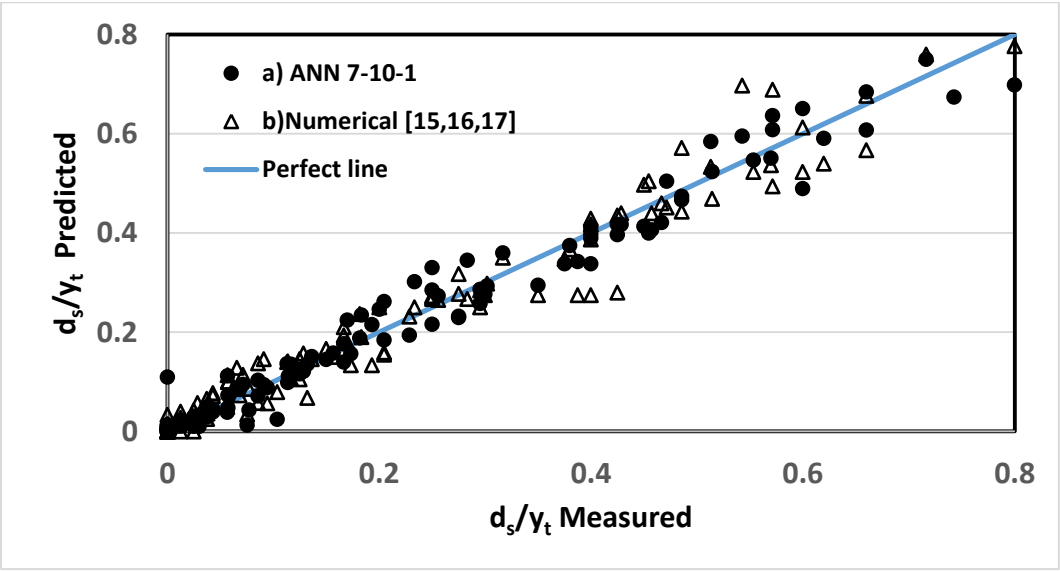


Fig. 5 The comparison between the actual value and the obtained one for both numerical solution and ANN of structure 7-10-1.

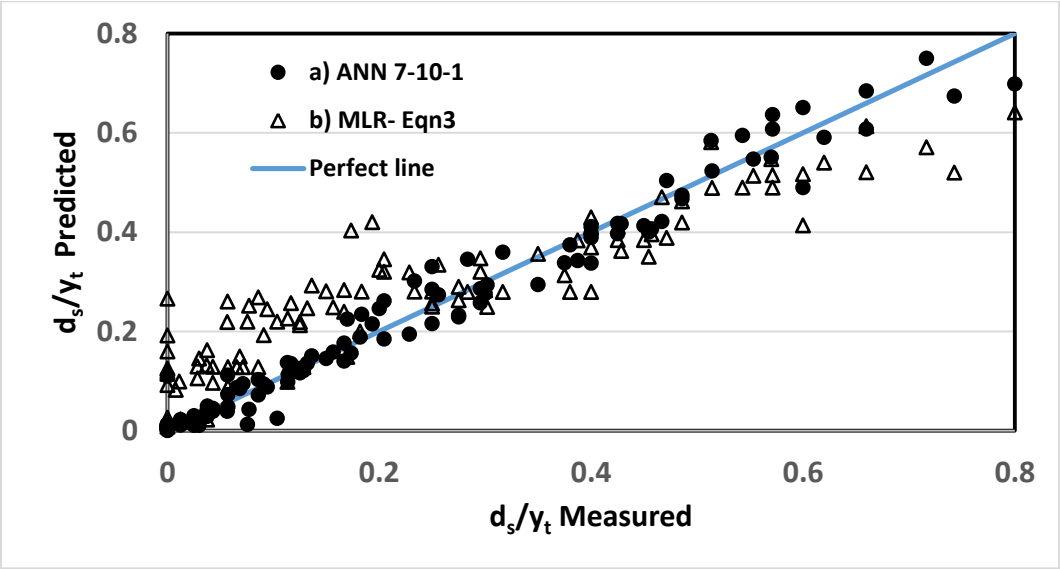


Fig. 6 The comparison between the actual value and the obtained one for both Eq.3 and ANN of structure 7-10-1.

Table 3. The average absolute ratio errors between numerical and ANN results.

Type of pattern	Overall pattern	Training set	Evaluation set	Test set
Average (Abs (Numerical error/ ANN error)) %	329.6	424.6	221.1	153.0

6. CONCLUSION

The present paper investigates the application of artificial intelligence using ANNs to simulate local scour depth at bridge abutment. Scour at bridge foundation could influence the safety of hydraulic structure and thus may cause loss of life. The artificial neural network is generated using experimental data from literature. In the experimental model, the dimension of bridge abutment and entrance angle are changed. In addition, different arrangements of collars around bridge abutment is used. The results of ANN are compared to both of numerical and MLR models. It was found that, the ANN results (R^2=98.3%) agree well with both measured and numerical model (R^2= 97.4%), and better than MLR model (R^2= 79%).

REFERENCES

1- Abdel-Aal, G.M., Mohamed, Y.A., 2010. The effect of collar size and shape on scour depth around bridge piers. *Scientific Bulletin, Faculty of Engineering*, Ain Shames University, Faculty of Engineering, Cairo, Egypt.

2- Azmathullah, H.M.D, Deo M.C, Deolalikar, P.B., 2006. Estimation of scour below spillways using neural Networks. Journal of Hydraulic Research, 44(1), 61–69.

3- Barkdoll, B.D, Ettema, R., Melville, B.W., 2007. Countermeasures to protect bridge abutments from scour. National cooperative highway research program (NCHRP) Rep. No. 587. Washington, D.C.: Transportation Research Board.

4- Bogdan, M., Wilamowski, J., David Irwin, 2011. The industrial electronics handbook, 2nd Edition, Intelligent systems. Taylor and Francis Group, LLC.

5- Cornelius T, Leondes, 1998. Neural network systems techniques and applications. Academic Press Limited; London; UK.

6- Cybenkot, G., 1989. Approximation by superpositions of a sigmoidal function. Math. Control Signals Systems, 2, 303-314.

7- Deng, L., Cai, C.S., 2010. Bridge scour: prediction, modeling, monitoring and countermeasures, review Practice Periodical Struct Des Construct, 15 (2).

8- Ivan Nunes da Silva, 2017. Artificial neural networks a practical course. Springer International Publishing AG, Switzerland.

9- Johnson, P.A., Dock, D.A., 1998. Probabilistic bridge scour estimates. *J. Hydraul. Eng.*, ASCE, 124 (7), 750-754.

10- Kasabov, Nikola K., 1998. Foundations of neural networks, fuzzy systems, and knowledge engineering. A Bradford Book The MIT Press Cambridge, Massachusetts, London, England,.

11- Kose, O., Yanmaz, M.A., 2010. Scouring reliability of bridge abutments. Aksaray University, Aksaray, Turkey. Middle East Technical University, Ankara, Turkey, Published in Teknik Dergi, 21(1), 4919-4934.

12- Kurt Hornik, Maxwell Stinchcombe, Halbert White, 1989. Multilayer feed forward networks are universal approximators. Neural Networks, 2, 359-366.

13- Lagasse, P.F., Clopper, P.E., Zevenbergen, L.W., 2007. Girard LG. Countermeasures to protect bridge piers from scour. National cooperative highway research program (NCHRP) Rep. No. 593. Washington, D.C3: Transportation Research Board.

14- Li, H., Kuhnle, R., Barkdoll, B., 2005. Spur Dikes as an Abutment Scour Countermeasure. Impacts of Global Climate Change, 1-12.

15- Melville, B.W., Coleman, S.E., 1999. Bridge scour. *Water Resources Publications*.

16- Mohamed, Y.A, Abdel-Aal, G.M., Nasr-Allah, T.H., Awad, A.S., 2016a. Experimental and theoretical investigations of scour at bridge abutment" Journal of King Saud University, Engineering Sciences, 28, 32-40.

17- Mohamed, Y.A, Nasr-Allah, T.H., Abdel-Aal, G.M. Awad, A.S., 2016b. Investigating the effect of curved shape of bridge abutment provided with collar on local scour, experimentally and numerically. Ain Shams Engineering Journal, 6 (2), 403-411.

18- Mohamed, Y.A, 2020. prediction of reference evapotranspiration using ANNs. Ain Shams Engineering Journal.

19- Muzzammil, M., 2008. Application of neural networks to scour depth prediction at the bridge abutments. Engineering Applications of Computational Fluid Mechanics, 2(1),30-40 ·
20- Nasr-Allah, T.H., Mohamed, Y.A, Abdel-Aal, G.M. Awad, A.S., 2016. Experimental and numerical simulation of scour at bridge abutment provided with different arrangements of collars. AEJ,55,1455-1463. http://dx.doi.org/10.1016/j.aej.2016.01.021.
21- Parker, G.W., Bratton L., Armstrong, D.S., 1997. Stream stability and scour assessments at bridges in Massachusetts. U.S. Geological survey open file Report No. 97-588 (CD-ROM). Marlborough, Mass.: Massachusetts Highway Dept. Bridge Section.
22- Pu, J.H., Lim, S.Y., 2013. Efficient numerical computation and experimental study of temporally long equilibrium scour development around abutment, Environmental Fluid Mechanics.
23- R., Mohammadpour, A., Ghanib, H.M., Azamathullac, 2013. Estimation of dimension and time variation of local scour at short abutment Int J River Basin Manage, 11(1),121 –135.
24- Ra´ul Rojas, 1996. Neural networks a systematic introduction. Springer-Verlag, Berlin.
25- Richardson E.V, Abed L., 1993. Top width of pier scour holes in free and pressure flow. Proceeding of international conference of hydraulic engineering, Part 1, 25–30.
26- Richardson, E.V., Davis, S.R., 2001. Evaluating scour at bridges. Hydraulic Engineering Circular no. 18, 4th Ed., Federal Highway Administration (FHWA); Arlington, VA.-11.
27- Şarlak, N., Tiğrek, Ş., 2011. Analysis of experimental data sets for local scour depth around bridge abutments using artificial neural networks. Water SA, 37(4).
28- Sturm، T.W., 2006. Scour around bankline and setback abutments in compound channels .J Hydraul Eng, 132 (1), 21–32
29- Sung-Uk Choi, Sanghwa Cheong, 2020. Prediction of local scour around bridge piers using artificial neural networks", Journal of the American Water Resources Association, 487-494.
30- Teruzzi, A., Ballio, F. 2021. Numerical investigation of the turbulent flow around a bridge abutment. River Flow, Ferreira, Alves, Leal & Cardoso.
31- Xie, J.X, Cheng, C.T, Chau, K.W, Pei Y.Z., 2006. A hybrid adaptive time–delay neural network model for multi-step-ahead prediction of sunspot activity. International journal of Environment and Pollution, 28(3), 364–381.

List of Symbols

b	Abutment width in lateral direction
B	channel width
d	Sediment particle diameter
d_s	Maximum local scour depth
E	Error vector
$e_{p,m}$	Difference between desired output and at output m when applying pattern p.
F_t	Tail Froude number
I	Identity matrix
J	Jacobian matrix
k	Index of iterations
L	Length of bridge abutment
L_1	Collar width,
L_c	Length of collar in longitudinal direction, and
m	Output number.
p	Pattern number
r	radius of abutment entrance
w	Weight and bias vector
x	Input vector
yt	Tail water depth
μ	Combination coefficient, positive large number
θ	Entrance angle of abutment

التنبؤ بالنحر عند اكتاف الكباري باستخدام الشبكات العصبية الاصطناعية

ياسر عبد الله محمد موسي

أستاذ الهيدروليكا- قسم الهندسة المدنية- كلية الهندسة – جامعة جازان

المخلص

للتصميم الفعال لأساسات الجسور يتطلب ذلك تقدير دقيقا لعمق النحر المتولد حول اكتاف تلك الجسور والمزودة بألواح حماية مثبته عند قاع المجري المائي. وللتنبؤ بأقصى عمق نحر حول دعامات واكتاف الجسر المذود بأطواق الحماية عند قاع المجري استخدمت انظمه متنوعة من الشبكات العصبية الاصطناعية (ANNs) وتم مقارنتها بالعديد من النتائج التجريبية التي تم جمعها من الدراسات السابقة. استخدمت خوارزمية Levenberg-Marquardt لتدريب طريقة الانتشار الخلفي متعددة الطبقات بطبقة واحدة مخفية، والتي من شأنها ان تبني الشبكة العصبية الأكثر دقة. وقد وجد ان نتائج نموذج الشبكات العصبية الاصطناعية ANN يعطي نتائج أكثر دقة مقارنة بالنماذج الإحصائية وكذا نماذج المحاكاة العددية. أظهر النموذج المقترح للتنبؤ بعمق المسح المحلي باستخدام الشبكات العصبية الاصطناعية نتائج جيدة (R^2 = 98.3٪ ، خطأ معياري = ٠,٠٣) مقارنة بالمحاكاة العددية (R^2 = 97.4 ، خطأ معياري = ٠,٠٤). بالإضافة إلى ذلك ، فإن النموذج الاحصائي للانحدار الخطي المتعدد MLR أقل فعالية من الشبكات العصبية الاصطناعية والنماذج العددية للتنبؤ بالنحر المتكون عند دعامات الجسر (R^2 = 80٪ والخطأ المعياري = ٠,١١). وهذه النتائج تساهم في ان تكون اساسات الجسور اكثر امانا في الاودية المعرضة للفيضانات والمجاري المائية.

الكلمات المفتاحية: الشبكات العصبية- المنشآت الهيدروليكية- اكتاف الكباري- النحر الموضعي- الانحدار الخطي المتعدد.

Code Obfuscation Detection using Deep Merging Image-Based Similarity

Abdullah Sheneamer

Computer Science, Jazan University, Jazan, Saudi Arabia

Abstract

IoT devices are being used in various domains and their numbers are increasing drastically. IoT devices are becoming part of our daily life and they are infiltrating our day-to-day work. Although the applications of these IoT sensing devices are providing a lot of valuable solutions but their security is still a big concern due to the limited hardware resources. Blockchain technology is being proposed in various domains for providing security and immutability to the system and data and it is also being applied in case of providing security to IoT devices. There are many variations and applications of blockchain technology. Non-fungible tokens (NFTs) are one of the prominent and rising applications. Non-fungible tokens (NFTs) are cryptographically unique tokens that are linked to digital (and sometimes physical) content, providing proof of ownership. In this paper, we will investigate the applications of NFTs for providing security to IoT infrastructure and propose a solution.

Keywords: Code obfuscation, Obfuscated code, Deep learning, Image-based similarity, Malware obfuscated code

I. INTRODUCTION

A code obfuscation, transformations are applied to the code, which changes its structure while preserving the meaning. By using obfuscation methods, an attacker would find it difficult to reverse engineer, analyze code, and retrieve sensitive information.

Security threats in the IT industry cost businesses billions of dollars every year to avert. Examples of these threats include tampering and hostile reverse engineering. Here we investigate a unique method for identifying obfuscated code by examining its visual representations. Obfuscated code detection methods in study primarily involve metamorphism and polymorphism transformations of a code block [1].

Following rational thinking, we employ a visual comparison of the original photos to identify possible obfuscation. The pair block picture is composed of pixels (i.e. dots) representing color, grey-scale, or RGB values and is presented by combining two images of source code blocks. When code is metamorphosed, it becomes unintelligible because dead code is inserted, code is replaced, and code is switched.

However, polymorphism uses switching to hide code iterations. In its current form, malware detection software essentially views malicious code as a meaningless string of bytes. They use code signature extraction and signature database comparison to determine classification. Unfortunately, signature-based malware detectors often miss disguised code since they rely on syntactic or structural signatures, which are inadequate in detecting such code. The challenge of ever-expanding families of known malware necessitates the development of anti-malware software that makes use of the semantic structure of a program's code. [2]. Code Obfuscation is a source code method block that is obfuscated version of another method block if they exhibit similar functionality although the structurally they are different from each other. It is similar to semantic clone [2]. The source code files contains either original code or obfuscated code.

Deep learning is represented by the architecture spectrum, which can construct solutions for a wide range of problem areas.

These solutions can be recurrent networks and feedforward focused, allowing previous inputs and their consideration. Computer vision, natural language processing (NLP), speech recognition, bioinformatics, and machine translation are just some of the areas where deep learning architectures including convolutional neural networks, recurrent neural networks, deep reinforcement learning, and deep belief networks have been used. Deep learning can be considered a new step in the evolution of artificial intelligence and applied to a code obfuscation detection system. The latter were first content to react in accordance with a set of predefined rules based on a cognitivist model. Afterwards, a programmer's touch was still required for any further system refinement or the addition of new features or regulations. [3].

Similar to how statistical machine learning gives AI the ability to learn and apply new rules on its own, deep learning gives AI autonomy [4]. As computational power and related applications continue to advance at an exponential rate, deep learning is able to produce increasingly complex and dense layers of neurons. In most cases, an artificial neural network can be employed in picture recognition to spot code obfuscation after being first trained on examples [5, 6]. The purpose of each network tier is to locate a specific feature of the code obfuscation being studied.

The paper is organized as follows: Section 2 discusses related work. In Section 3, we propose a new deep learning framework for the detection of obfuscated code. We evaluate and compare our proposed method and report findings in Section 4. Finally, we conclude our work in Section 5.

II. Related Work

This study discusses code obfuscation detection using deep learning and images. The study also examines how it would be useful if convert obfuscated code into images by employing deep learning approaches to detect them.

A. Code obfuscation

This means to make something difficult to comprehend. The programming code is obfuscated and is to protect the trade or property secrets which also stops the attacker from reverse engineering and a proprietary software program. On the other hand, encrypting all the program code is one of the obfuscation methods [7]. Park et al. [23] proposed a framework to detect Android apps obfuscation in a class-level. Their approach vectorizes each decompiled codes of classes using a paragraph vector and machine learning. We selected plagiarism detectors include Jplag, Sherlock, Sim, and Plaggie.

B. Converting obfuscated code into images using deep learning.

Since the greyscale image is known as a value between 0 to 255, it is feasible to know that it would translate a file into the picture by having bytes of the file become the new image and its pixel [8]. The virtualization in converting obfuscated code into the images by using deep learning also generates a process level virtual environment as well as constructs the interpreter in the form of a switch statement with the instruction set uniquely [9]. For instance, when the program is used, such as Windows binary, the sections of the program seem to be distinct from each other [10].

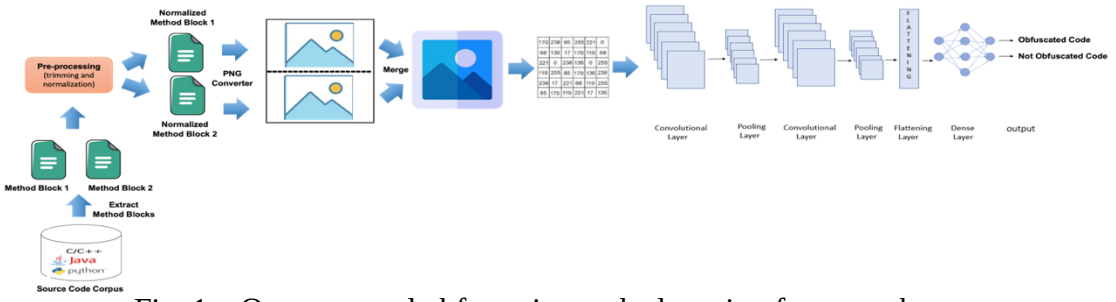


Fig. 1. Our proposed obfuscation code detection framework.

C. Code obfuscation and Malware obfuscated code

According to Gibert et al. [11], obfuscation is the commonly used technique that conceals the code in the original, which is also written by the programmer. This may also render the code, which seems like it is difficult to read and hard to comprehend. This means that it is quite difficult to maintain the functionality of the code written [12]. Every piece of the malware employs obfuscation in some way or other. Kim and Cho [13] determined that malware obfuscation is a procedure that makes binary and textual information quite difficult to comprehend. The techniques related to the obfuscation are employed by attackers, which makes it difficult for the antivirus to detect the malware without a filter. On the other hand, it is noted that malware evolves the body into the new generations through which obfuscation techniques evade the antivirus. Menéndez and Suárez-Tangil [24] proposed a technique is call obfSec (Obfuscation Security) to test and measure the security of obfuscation from a testing perspective. Software flaws are initially discovered by ObfSec, which then reveals how obfuscation might modify the nature of those errors. It focuses in particular on transformations that turn software bugs into an exploitable vulnerable program. Kumar and Vaishakh [25] suggested a system for analyzing Java malware to find lexical and string obfuscation. In order to train a machine learning classifier to distinguish between malware that is obfuscated and malware that is not, we identify a collection of eleven attributes that define obfuscated code. A static analyzer that looks at the bytecode extracts the features.

D. Similarity Tools and Techniques

Plagarism detectors

We selected some plagiarism detectors such as Jplag [28], Sherlock [40], Sim [27] and Plaggie [36]. Jplag and Sim are token-based techniques. These tools has versions for text such as jplag-text and simtext and Java such as jplag-java and simjava. Sherlock depends on digital signatures and Plaggie technique has the same functionalities as Jplag.

Clone detectors

The selected clone detectors including text-based such as Simian [41], NICAD [35] which depend on text lines comparisons, token-based such as CCFinderX (ccfx) [26], iClones [34] which use tokens when comparing between two source codes or texts, tree-based such as Deckard [33] which converts two source codes

into an abstract syntax tree (AST) and computes the similarity.

Compression tools

Normalised compression distance (NCD) is a distance metric between two contents based on compression [42]. We selected CompLearn suite [30] technique that uses the built-in bzlib and zlib compressors. We also chose 7Zip [31] has various techniques versions such as BZip2, Deflate, Deflate64, PPMd, LZMA, and LZMA2. The gzip, bzip2, and xz compressors for Linux are also available in different versions. We also selected additional methods for measuring similarity, including: Text sequences are compared using Gestalt pattern matching by difflib [29], fuzzy string matching by fuzzywuzzy [37], approximation and phonetic string matching by jellyfish [38], and cosine similarity from scikit-learn [32], a machine learning tool.

III. PROPOSED WORK

We use similarity images to automatically identify obfuscated code. The following are the stages of the suggested procedure. Our method's workflow is shown in Figure 1.

- ***Step 1. Preprocessing (Trimming and Normalization) and conduct a lexical analysis.*** We modify and normalize all source files into specified token sequences that allow us to detect identical and similar obfuscated applications.
- ***Step 2. Extract method blocks.*** In order to find every block in the provided source files, lexical analysis and syntactic analysis are needed at this stage.
- ***Step 3. Create files in pairs.*** To determine if the two method blocks are still discernable after being transformed into photos, we compare each pair of blocks.
- ***Step 4. Convert the pairwise file into images.*** This step pairs and merges files into one image. We identify each image that contains a pair of files either as obfuscated codes or not using deep learning algorithms.
- ***Step5. Convert each image into pixels.*** This step con- verts each image into an array of pixels. Each array of pixels feeds into deep learning algorithms.

Generating Images

Each file is transformed into a PNG image (Portable Network Graphics). Then, each pair of obfuscated files is concatenated into a single image. Each image from a pair of files is loaded into memory as a 2-dimensional matrix of size m x n, with each cell's value ranging from 0 to 255 to represent an 8-bit grey-scale version of the original image. We then feed pixels of processed images of the pair of files to a deep learning model. We do an image of each file pair to locate obfuscated code in a software system.

Deep learning model

Deep learning models are used in high-level abstract features. While these features are extracted, these models also provide improved performance over the traditional models, which enhance interpretability and comprehension as well as process the biological information. According to Marastoni et al. [14], the deep learning model is a part of the wider family of machine learning methods. These models are based on artificial neural networks, which also represent learning. It can be unsupervised, supervised or semi-supervised. Deep learning is an AI method derived from the concept of

machine learning. This so-called deep learning method is based more specifically on the concept of an artificial neural network. With a nonlinear structure, an artificial neural network takes the form of a network of sets of information execution units (representing neurons) superimposed in layers and linked together via connectors (synapses). From there, it processes the information through propagation models of activations of these units, activating beyond a certain threshold [15].

The computer model learns to carry out the tasks with its classification from image, sound or text. The models detect the images step by step so that those models can accomplish state-of-the-art accuracy and exceed human-level performance. On the other hand, the recognition of the image is the task in which deep neural networks excel. The computing systems are intended to identify some of the patterns [16].

The architecture is inspired by the structure of the human brain. They also comprise the three kinds of layers, which involve input, hidden and output layers. Deep learning can be used in many contexts and use cases, for example, image recognition, voice recognition, language processing, robotics, cybersecurity and bioinformatics. The technologies are dedicated to assisted driving and diagnostic aids in the medical sector. Deep learning is a mode of machine learning. Both approaches are based on the principle of machine learning. There are, however, notable differences. For machine learning, values and variables are usually selected in advance, unlike deep learning, which also includes computer vision systems [17].

The encoder takes the obfuscated code image as an input and runs it through block and layers series, which also makes them learn about statistical features related to the labelling of the objects. In this approach, the malware can be identified by detection of the images, which results in a lower false-positive rate. The signatures on the images can be changed to evade the detection of scanners in the malware. The modelling of the results is also subject to variation. It is a statistical model for machine learning and numerical optimization for deep learning [18].

Originally, these systems were called artificial neural networks. (ANN, Artificial Neural Networks) to differentiate them from biological systems. They generally consist of a certain number of input and output data (input/output layer), a narrow network of neurons and several intermediate strata (hidden layers). These intermediate layers make it possible to deal with complex problems; without them, the system only solves simple calculations. The number of layers is, therefore, a decisive factor for the complexity of the system and learning; data associated from one layer to another, the results of a first layer serving as input to the next, and so on to arrive at complex decision-making.

This operation in layers gives all its depth to the network and learning. The adjective “deep” is understood here in all senses of the term. In the learning phase, neurons modify their weighting behavior and refine the output results based on the input variables. So there must be feedback on the overall result that influences each neuron.

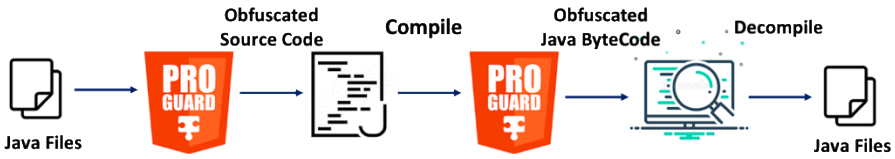


Fig. 2. Java obfuscated dataset generation steps [2].

Therefore, we can say that the input and output variables of a neural network are known but that the values of the neurons, especially in the hidden layers, remain unknown [18]. Taken in isolation, a neural network that has not been trained does not know anything and provides random, even chaotic, results for the user. Only a trained system will provide the desired result. If the problem posed is simple, a simple program, easier to debug, can solve it. For a more complex problem, we will use a neural network, which we will train using large data sets. Each neuron can provide complex output variables and react linearly or non-linearly to input variables. This is a rather subtle point because the neurons must be able to react to all the possibilities to provide an adequate result. This implies two things: either the neural network programmer knows all the possible connections internal to the network.

IV. Evaluation

Datasets

Our major aim is to improve obfuscation detection accuracy for obfuscated clones by employing deep learning techniques that can hold their own against the cutting edge. We utilize Java obfuscated datasets as our target, as detailed below.

Using open-source obfuscation tools, Sheneamer et al. [2] created obfuscated code samples. A total of five Java classes (InfixConverter, SqrtAlgorithm, Hanoi, EightQueens, and MagicSquare) are used to construct the obfuscated code, which they collectively refer to as ObsCode. Every one of the classes has less than 200 lines of code. An Eclipse plugin for source-level obfuscation is called Artifice [19]. The tool changes five different aspects of Java source code: 1) variables, fields, and methods are renamed; 2) assignment, increment, and decrement operations are changed to normal form; 3) additional assignment, increment, and decrement operations are inserted when possible; 4) while is changed to for and vice versa; and 5) if is changed to its short form. To hide the Java classes, some creative writing [19] is used. After that, the unmodified and modified files are both compiled to bytecode. To further improve obfuscation, ProGuard is applied to both bytecode files. The next step is to use Krakatau [21] or Procyon[22] to decompile all four bytecode files, which will result in eight additional masked source code files [20]. They created nine significantly modified versions of each original source code, yielding 50 files for the dataset [20]. As our second subject system [19], they chose the PacMan game 3, which has 21 files and 2400 lines of code. Renaming, contraction, expansion, and loop transformations are used to further alter the classes, according to [19]. In addition, they used Algorithms 1, a set of

supplementary source programs comprising 149 Java source files that were included in the textbook and were responsible for creating the obfuscated code. To create obfuscation files from the aforementioned source file content, they used the method depicted in Figure 2. Each Java class is encrypted using ProGuard. Next, both the original and the obfuscated files are compiled to bytecode. Both files' bytecodes have been encrypted using ProGuard again. An obfuscated source code file is obtained by decompiling the bytecode files with a Java decompiler. Seven hundred eighty-five Java bytecode files were collected for the dataset. The dataset summaries are presented in Table 1.

Table1. Java code obfuscation datasets.

Dataset	Paired Codes	Original Code	Obfuscated Code
ObsCode	2,500	500	2,000
PacMan	8,464	7,968	496
Algorithms	2,230	2,000	230

Experimental setup

Generally accepted criteria from prior studies have been applied in our assessments. It discusses the F1-score and the accuracy of predictions under different input parameters. Classification accuracy is the primary metric used to evaluate deep learning models. Models of the classifiers are produced and tested using train/validate/test split using python where we ensure that the ratio between obfuscate and non-obfuscate classes is the same as in the overall dataset. As an additional tool, we have employed confusion matrices to evaluate the success and failure of various prediction methods.

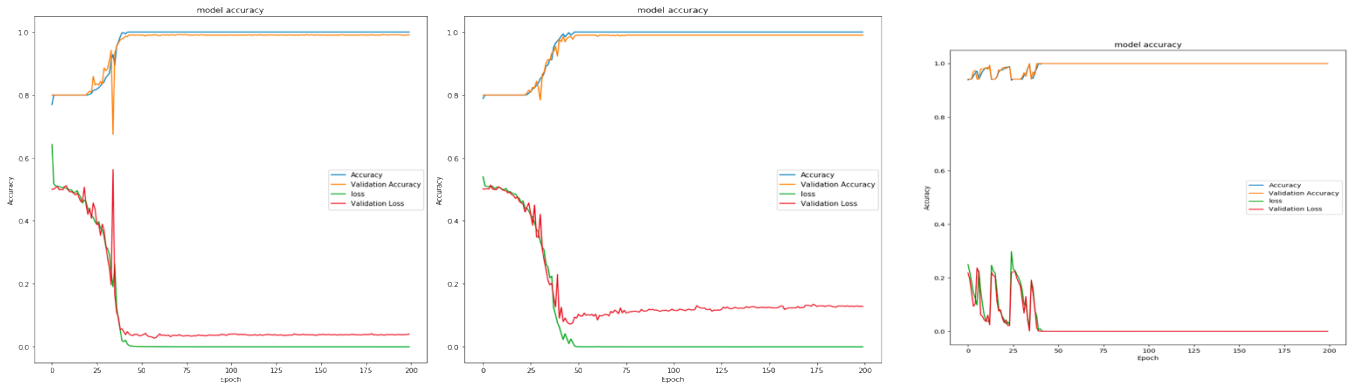
$$Precision(P) = \frac{TP}{TP + FP} \quad (1)$$

$$Recall(R) = \frac{TP}{TP + FN} \quad (2)$$

$$F1 - score = \frac{2 * Precision * Recall}{Precision + Recall} \quad (3)$$

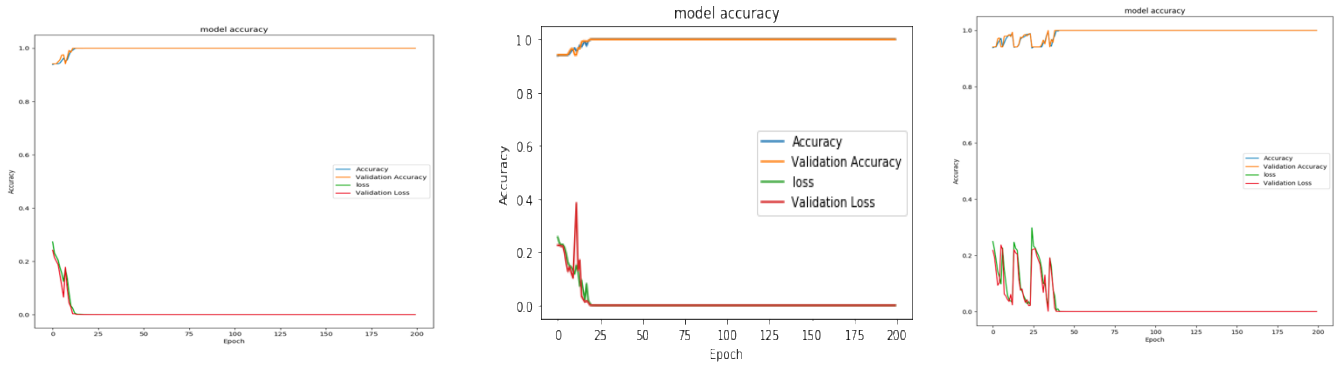
$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad (4)$$

True positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) are indicated by the symbols TP, TN, FP, FN, and FP, respectively, in the aforementioned equations. All of the classifier models utilized in our experiments are evaluated using the F1-score as the key performance measure. A single metric known as the F1-score measures the proportion of accurate predictions to all input samples. Precision, often called true positive rate (TPR), is defined as the ratio of actual positive results to classifier-predicted positive results. You can define this as follows: A measure of accuracy, precision can be written as TP/ (TP + FP), where TP is the correct prediction of a positive sample and FP is the wrong forecast. Nonetheless, recall is a second parameter that is used with precision. Recall can be written as TP/ (TP + FN), where TP is the number of true positive outcomes and FN is the number of false negatives. We also used a confusion matrix table to measure the classifiers' accuracy. The confusion matrix is a four-by-two table including the numbers of correct predictions, incorrect predictions, correct negative predictions, and correct positive predictions. This makes it possible to analyze prediction accuracy in greater depth than just the proportion of correctly classified objects.



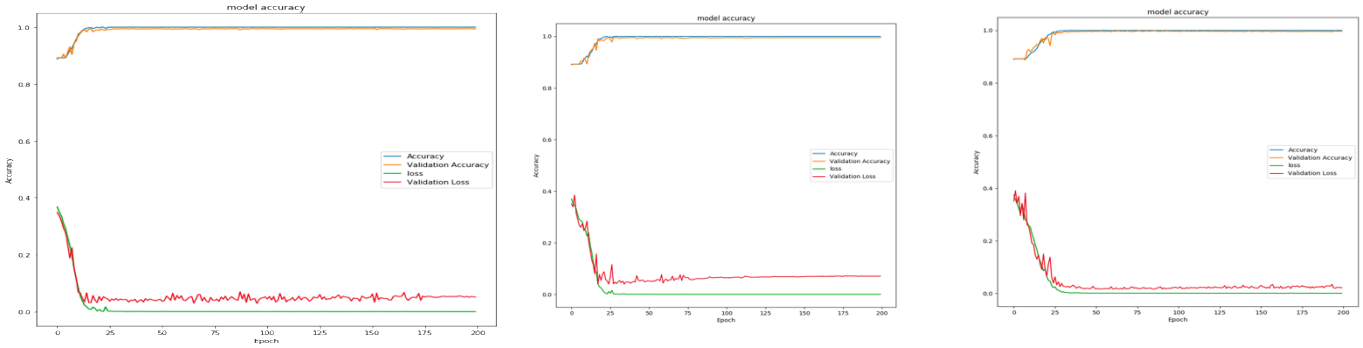
(a) AlexNet model (b) VGG16 model (c) VGG19 mode

Fig. 3. Performance models on ObsCode dataset.



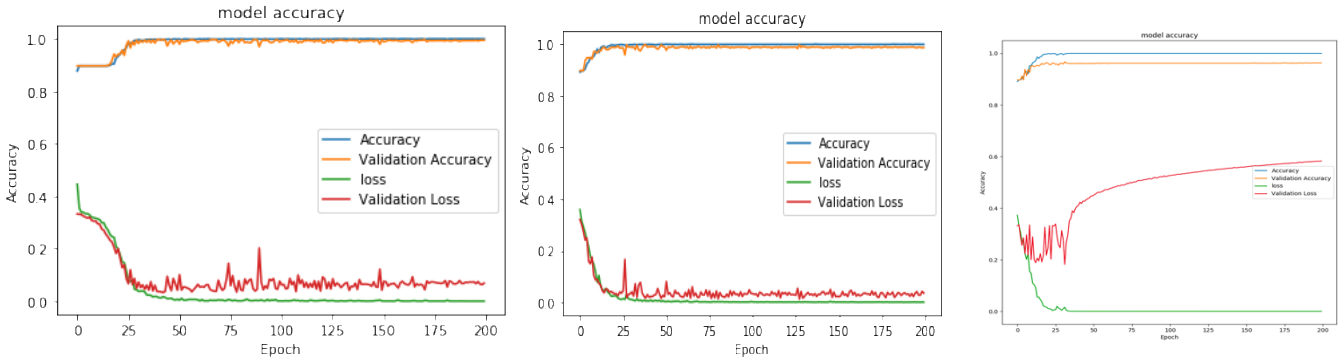
(a) AlexNet model (b) VGG16 model (c) VGG19 mode

Fig. 4. Performance CNN models on PacMan dataset.



(a) AlexNet model (b) VGG16 model (c) VGG19 mode

Fig. 5. Performance CNN models on Algorithm dataset.



(a) AlexNet model (b) VGG16 model (c) VGG19 mode

Fig. 6. Performance CNN models on all datasets.

Experiments Results

Our suggested approach for identifying obfuscated code is extensively tested, and the findings are extensively generated. To show that our method can attain a high detection accuracy, we conduct experiments using a variety of deep learning architectures. 4.3.1 Performance deep learning models

Performance deep learning models

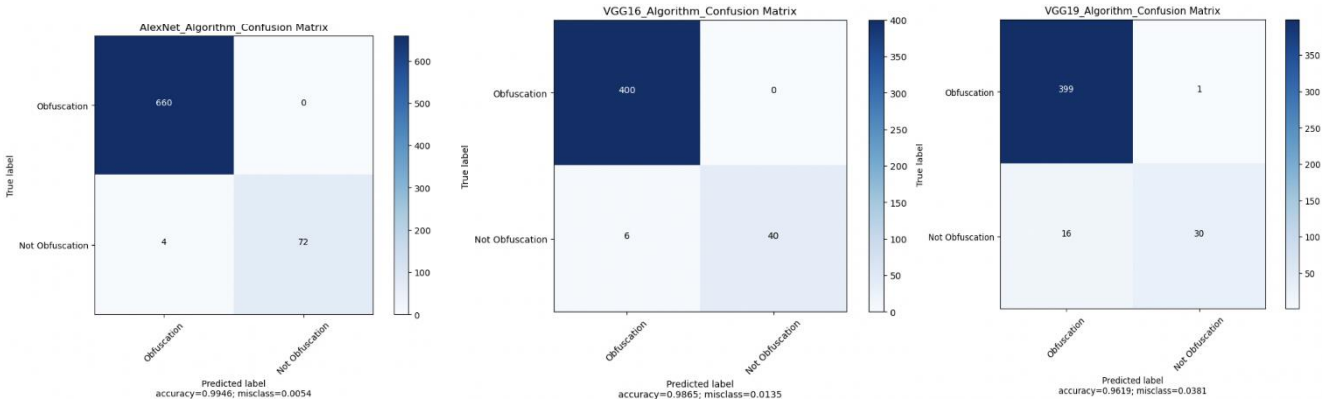
- ObsCode Dataset: In the case of the ObsCode dataset, Figures 3(a),9(a), 3(c) and 9(c) show that Alex and VGG16 architectures achieve 99% accuracy. However, Figure 4(b) shows that VGG19 achieves 100% accuracy.
- PacMan Dataset: In the case of the PacMan dataset, Figures 4 and 8 show that all AlexNet and VGG16, VGG19 architectures achieve 100% accuracy.
- Algorithm Dataset: In the case of the Algorithm dataset, Figures 5(a) and 7(a) show that AlexNet architecture achieves 99.46% accuracy, while Figures 5(b) and 7(b) show that VGG16 architecture achieves 98.65% accuracy, and Figures 5(c) and 7(c) show that VGG19 architecture achieves 96.19% accuracy.

Performance deep learning architectures on cross datasets

In order to spot obfuscated code, we combine samples from various training and testing sets. We combine and evaluate the three datasets. In Figure 6, we can see the outcomes of using many datasets together. Figures 6(a) and 10(a) show that AlexNet architecture achieves 99.47% accuracy, while Figures 6(b) and 10(b) show that VGG16 architecture achieves 99.51% accuracy, and Figures 6(c) and 10(c) show that VGG19 architecture achieves 99.69% accuracy. Even when the model is constructed using one dataset and evaluated on another, our obfuscation code detection model achieves superior results.

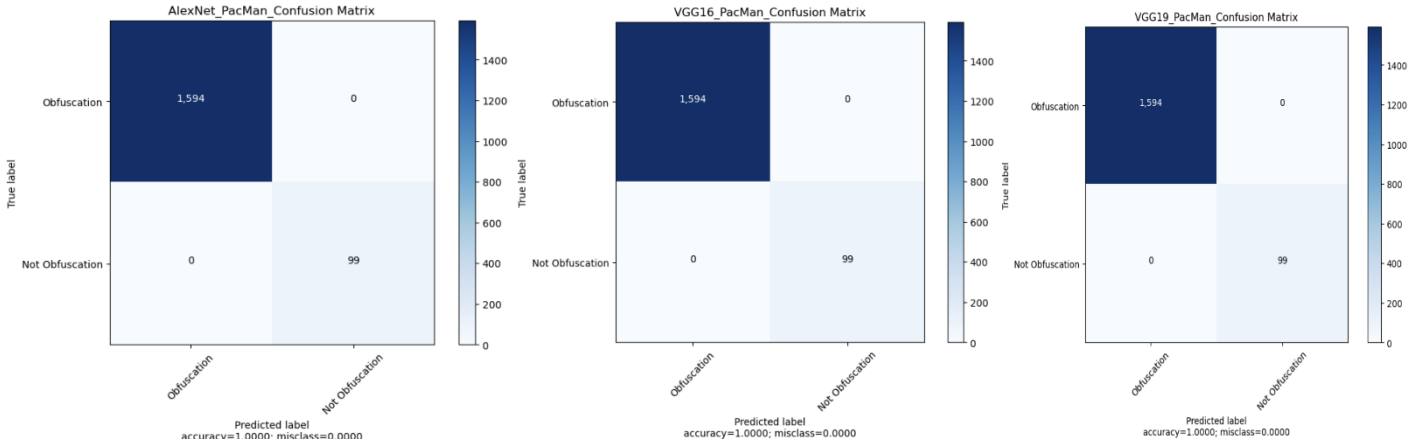
Performance obfuscated detectors comparisons

We evaluate our approach against the most cutting-edge obfuscated code detection techniques available. To evaluate how well different obfuscated code detectors perform, we look at their reported Precision, Recall, and F1-score values [20]. In Table 2 and Figure 11, we compare our findings with those of other obfuscated code detectors on the ObsCode dataset in terms of Recall, Precision, and F1-Score. As can be



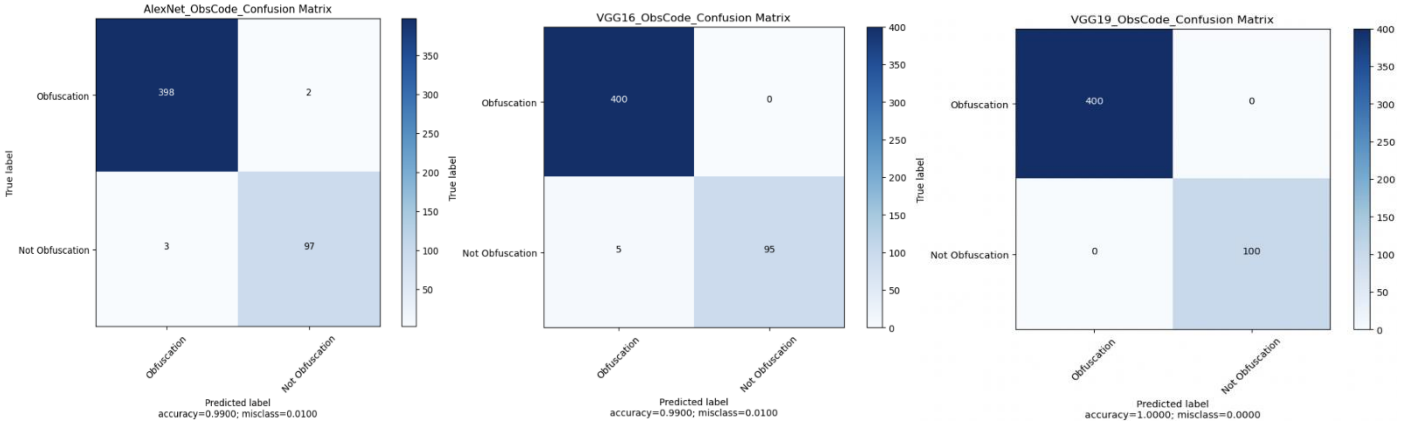
(a)AlexNet model (b) VGG16 model (c) VGG19 mode

Fig. 7. Confusion matrix of CNN models on Algorithm dataset.



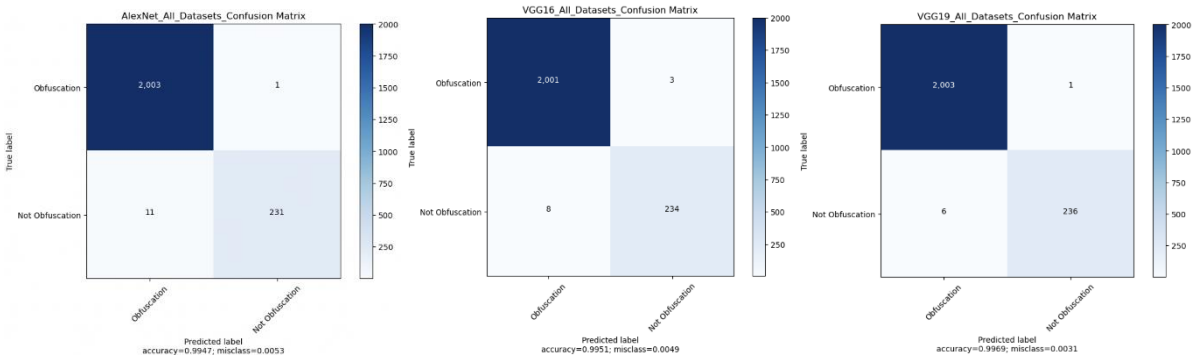
(a) AlexNet model (b) VGG16 mode (c) VGG19 mode

Fig. 8. Confusion matrix of CNN models on PacMan dataset.



(a) AlexNet model (b) VGG16 model (c) VGG19 mode

Fig. 9. Confusion matrix of CNN models on ObsCode dataset.



(a) AlexNet model (b) VGG16 model (c) VGG19 mode

Fig. 10. Confusion matrix of CNN models on All dataset.

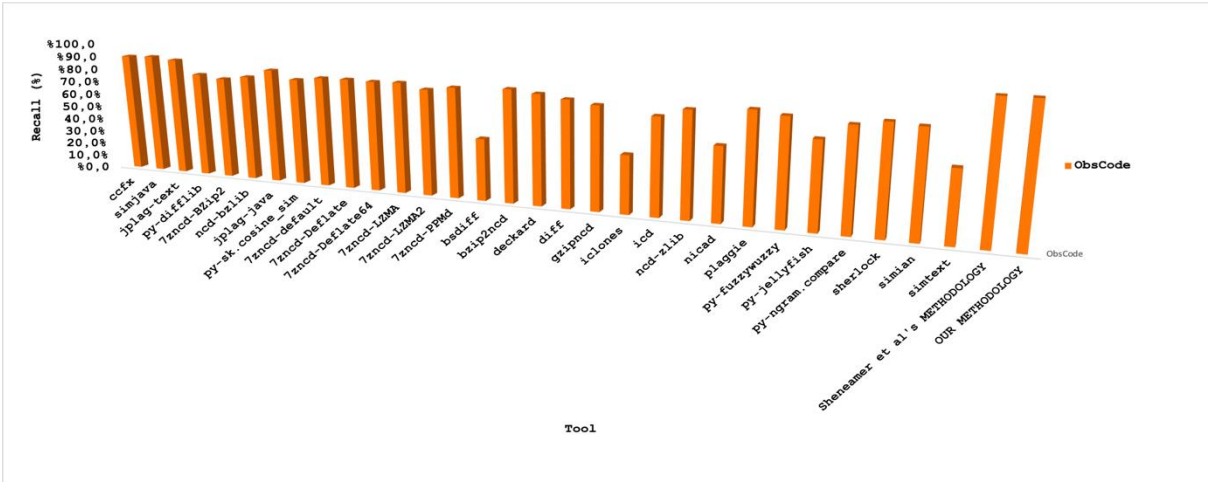
shown, our method outperforms all others in detecting obfuscated code, with the exception of Sheneamer's approach, which achieves identical results. However, when comparing methods for detecting obfuscated codes on the ObsCode dataset, which was constructed using ProGuard and Decompilers, our approach continues to stand head and shoulders above the others with the highest F1- Score (100%) possible in every scenario.

IV CONCLUSION AND FUTUR WORK

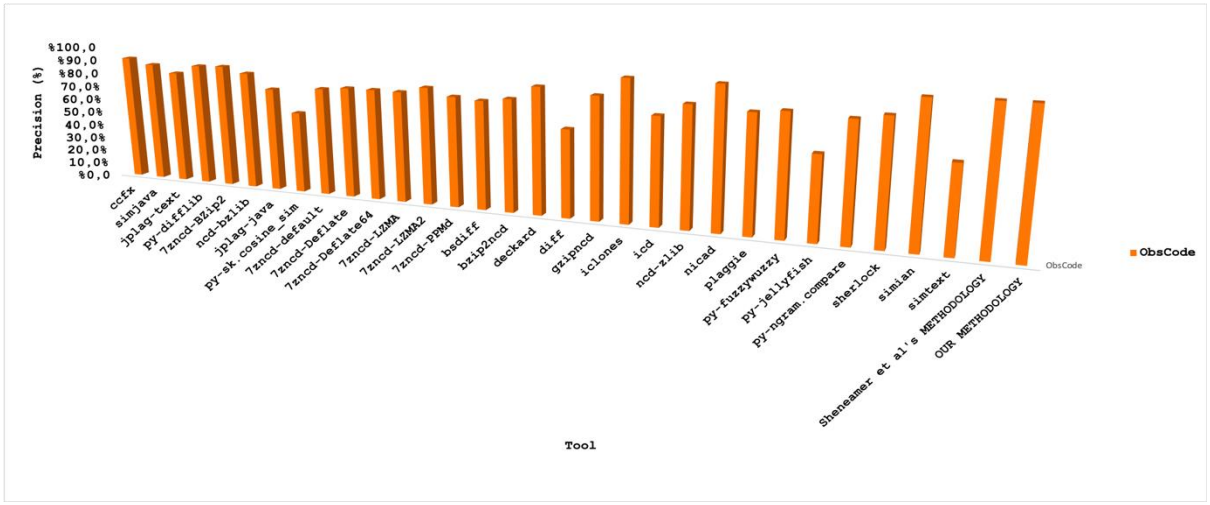
In this paper, we introduce a method for detecting code obfuscation using images. The method merges images using state-of-the-art convolutional neural network architectures. Syntax highlighting and image conversion are applied to the raw source code language, which captures the human visual impression of the code and allows for the merging of two codes into a single image. To enhance obfuscation detection models, we discovered that applying a deep learning architecture to source code images significantly improved precision, recall, F1- score, and accuracy.

Table 2. Results of several techniques for detecting obfuscated code on the ObsCode dataset [20]

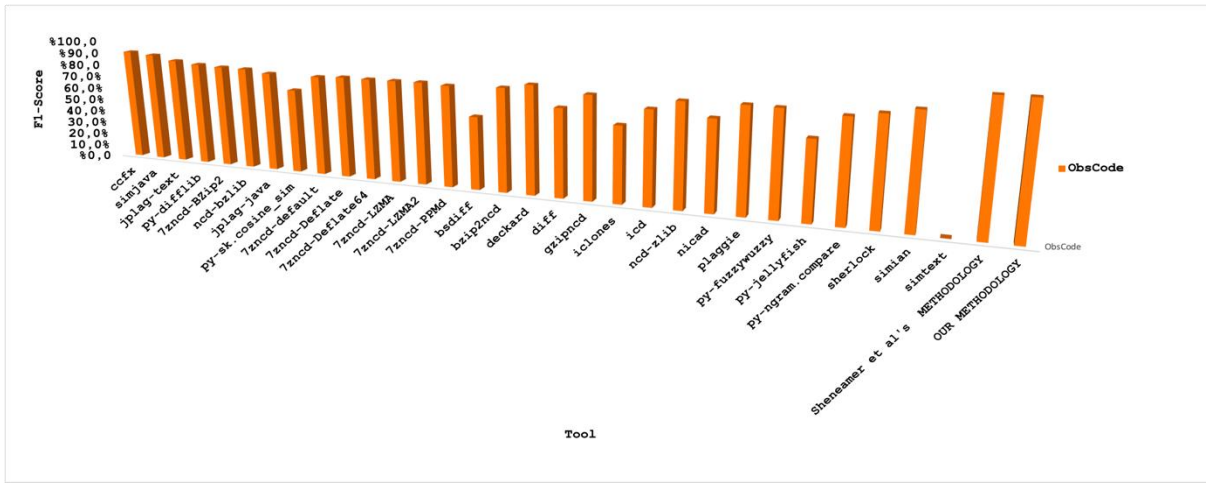
Tool	Precision	Recall	F1-score
ccfx [26]	91.5%	90.4%	90.9%
simjava [27]	87.7%	91.2%	89.4%
jplag-text [28]	82.4%	89.6%	85.8%
py-difflib [29]	89.0%	79.4%	83.9%
7zncd-BZip2 [30]	89.8%	77.2%	83.0%
ncd-bzlib [31]	85.8%	80.0%	82.8%
jplag-java [28]	75.3%	86.4%	80.4%
py-sk.cosine_sim [32]	58.9%	80.4%	68.0%
7zncd-default [31]	78.2%	83.0%	80.5%
7zncd-Deflate [31]	80.0%	83.2%	81.6%
7zncd-Deflate64 [31]	80.1%	82.8%	81.4%
7zncd-LZMA [31]	79.9%	83.4%	81.6%
7zncd-LZMA2 [31]	84.3%	79.6%	81.9%
7zncd-PPMd [31]	79.2%	82.4%	80.8%
bsdiff [20]	77.8%	46.2%	58.0%
bzip2ncd [31]	80.5%	84.0%	82.2%
deckard [33]	90.3%	82.0%	86.0%
diff [20]	62.5%	79.4%	70.0%
Gzipncd [31]	86.9%	76.8%	81.5%
iclones [34]	100.0%	43.2%	60.3%
Icd [20]	76.3%	72.0%	74.1%
ncd-zlib [31]	85.4%	78.2%	81.6%
nicad [35]	100.0%	54.8%	70.8%
plaggie [36]	83.0%	81.2%	82.1%
py-fuzzywuzzy [37]	85.2%	78.4%	81.7%
py-jellyfish [38]	59.2%	64.4%	61.7%
py-ngram.compare [39]	83.3%	75.6%	79.2%
sherlock [40]	86.8%	79.2%	82.8%
simian [41]	99.5%	77.6%	87.2%
simtext [27]	60.6%	52.4%	56.20%
Sheneamer et al's METHODOLOGY [2]	**100.0%**	**100.0%**	**100.0%**
OUR METHODOLOGY	**100.0%**	**100.0%**	**100.0%**



(a) Recall



(b) Precision



(c) F1-measure

Fig. 11. Performance of several techniques for detecting obfuscated code on the ObsCode dataset.

Our method performed comparably to previous obfuscation code detection methods on a dataset of code obfuscation. We propose to turn the source code into an RGB image using a similarity and hashing method, and we use multiple publicly accessible obfuscated code datasets to verify the efficacy of our system.

ACKNOWLEDGMENT:
I would like to express my gratitude to the Jazan University in providing a platform to publish my research work. Also, I

would like to express my appreciation to all the colleagues of my department for their constant support.

DATASET AVALIBITY: The data can be obtained from the corresponding author upon request.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

REFERENCES

[1] Christodorescu, M., Jha, S., Seshia, S. A., Song, D., & Bryant, R. E. (2005, May). Semantics-aware malware detection. In 2005 IEEE symposium on security and privacy (S&P'05) (pp. 32-46). IEEE.

[2] Sheneamer, A., Roy, S., & Kalita, J. (2018). A detection framework for semantic code clones and obfuscated code. Expert Systems with Applications, 97, 405-420.

[3] Ni, S., Qian, Q., & Zhang, R. (2018). Malware identification using visualization images and deep learning. Computers & Security, 77, 871-885.

[4] Sheneamer, A. M. (2021). Multiple Similarity-based Features Blending for Detecting Code Clones using Consensus-Driven Classification. Expert Systems with Applications, 183, 115364.

[5] Sheneamer, A. (2018, December). CCDLC detection framework-combining clustering with deep learning classification for semantic clones. In 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA) (pp. 701-706). IEEE.

[6] Sheneamer, A., Roy, S., & Kalita, J. (2021). An Effective Semantic Code Clone Detection Framework Using Pairwise Feature Fusion. IEEE Access, 9, 84828-84844.

[7] Cui, Z., Xue, F., Cai, X., Cao, Y., Wang, G. G., & Chen, J. (2018). Detection of malicious code variants based on deep learning. IEEE Transactions on Industrial Informatics, 14(7), 3187-3196.

[8] El Abdelkhalki, J., Ahmed, M. B., & Abdelhakim, B. A. (2020). Image malware detection using deep learning. International Journal of Communication Networks and Information Security, 12(2), 180-189.

[9] Darus, F. M., Salleh, N. A. A., & Ariffin, A. F. M. (2018, November). Android malware detection using machine learning on image patterns. In 2018 Cyber Resilience Conference (CRC)(pp. 1-2). IEEE.

[10] Ghanei, H., Manavi, F., & Hamzeh, A. (2021). A novel method for malware detection based on hardware events using deep neural networks. Journal of Computer Virology and Hacking Techniques, 17(4), 319-331.

[11] Gibert, D., Mateu, C., Planes, J., & Vicens, R. (2019). Using convolutional neural networks for classification of malware represented as images. Journal of Computer Virology and Hacking Techniques, 15(1), 15-28.

[12] Lu, T., Du, Y., Ouyang, L., Chen, Q., & Wang, X. (2020). Android malware detection based on a hybrid deep learning model. Security and Communication Networks, 2020.

[13] Kim, J. Y., & Cho, S. B. (2022). Obfuscated Malware Detection Using Deep Generative Model based on Global/Local Features. Computers & Security, 112, 102501.

[14] Marastoni, N., Giacobazzi, R., & Dalla Preda, M. (2018, September). A deep learning approach to program similarity. In Proceedings of the 1st International Workshop on Machine Learning and Software Engineering in Symbiosis (pp. 26-35).

[15] Mercaldo, F., & Santone, A. (2020). Deep learning for image-based mobile malware detection. Journal of Computer Virology and Hacking Techniques, 16(2), 157-171.

[16] Parker, C., McDonald, J. T., & Damopoulos, D. (2021). Machine Learning Classification of Obfuscation using Image Visualization. In SECRYPT (pp. 854-859).

[17] Vasan, D., Alazab, M., Wassan, S., Naeem, H., Safaei, B., & Zheng, Q. (2020). IMCFN: Image-based malware classification using fine-tuned convolutional neural network architecture. Computer Networks, 171, 107138.

[18] Venkatraman, S., Alazab, M., & Vinayakumar, R. (2019). A hybrid deep learning image-based analysis for effective malware detection. Journal of Information Security and Applications, 47, 377-389.

[19] Schulze, S., & Meyer, D. (2013, May). On the robustness of clone detection to code obfuscation. In 2013 7th International workshop on software clones (IWSC) (pp. 62-68). IEEE.

[20] Ragkhitwetsagul, C., Krinke, J., & Clark, D. (2016, October). Similarity of source code in the presence of pervasive modifications. In 2016 IEEE 16th international working conference on source code analysis and manipulation (SCAM)(pp. 117-126). IEEE.

[21] Java decompiler, assembler, and disassembler. https://github.com/ Storyyeller/Krakatau, Accessed: 2015-08-27.

[22] Procyon / java decompiler. https://bitbucket.org/mstrobel/procyon/wiki/Java%20Decompiler, Accessed: 2015-08-27.

[23] Park, M., You, G., Cho, S. J., Park, M., & Han, S. (2019). A Framework for Identifying Obfuscation Techniques applied to Android Apps using Machine Learning. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 10(4), 22-30.

[24] Menéndez, H. D., & Suárez-Tangil, G. (2022). ObfSec: Measuring the security of obfuscations from a testing perspective. Expert Systems with Applications, 210, 118298.

[25] Kumar, R., & Vaishakh, A. R. E. (2016). Detection of obfuscation in java malware. Procedia Computer Science, 78, 521-529.

[26] T. Kamiya, S. Kusumoto, and K. Inoue. CCFinder: a multilinguistic token-based code clone detection system for large scale source code. IEEE Transactions on Software Engineering, 28(7):654–670, July 2002.

[27] D. Gitchell and N. Tran. Sim: a utility for detecting similarity in computer programs. In 30th SIGCSE technical symposium on Computer science education – SIGCSE '99, pages 266–270, 1999.

[28] L. Prechelt, G. Malpohl, and M. Philippsen. Finding plagiarisms among a set of programs with JPlag. Journal of Universal Computer Science, 8(11):1016–1038, 2002.

[29] difflib – helpers for computing deltas. http://docs.python.org/2/library/ difflib.html, Accessed: 2015-08-24.
[30] Complearn. http://complearn.org/index.html, Accessed: 2015-08-24
[31] 7-zip. http://www.7-zip.org, Accessed: 2015-08-27.
[32] Machine learning in python. http://scikit-learn.org/stable/, Accessed: 2015-08-24
[33] L. Jiang, G. Misherghi, Z. Su, and S. Glondu. DECKARD: Scalable and accurate tree-based detection of code clones. In ICSE, 2007.
[34] N. Gode and R. Koschke. Incremental clone detection. In ¨ CSMR'09, pages 219–228, 2009.
[35] C. K. Roy and J. R. Cordy. NICAD: Accurate detection of near-miss intentional clones using flexible pretty-printing and code normalization. In ICPC'08, pages 172–181, 2008.
[36] A. Ahtiainen, S. Surakka, and M. Rahikainen. Plaggie: GNU-licensed source code plagiarism detection engine for Java exercises. In 6th Baltic Sea Conference on Computing Education Research, 2006.
[37] Fuzzy string matching like a boss. https://github.com/seatgeek/ fuzzywuzzy, Accessed: 2015-08-24.
[38] A python library for doing approximate and phonetic matching of strings. https://github.com/jamesturk/jellyfish, Accessed: 2015-08-24.
[39] Ngram 3.3. https://pythonhosted.org/ngram/, Accessed: 2015-08-24.
[40] The sherlock plagiarism detector. http://sydney.edu.au/engineering/it/ ~scilect/sherlock/, Accessed: 2015-08-27.
[41] Simian - similarity analyser. http://www.harukizaemon.com/simian/, Accessed: 2015-08-27.
[42] R. Cilibrasi and P. M. B. Vitanyi. Clustering by compression. ´ IEEE Transactions on Information Theory, 51(4):1523–1545, 200

كشف التعتيم على الكود باستخدام تشابه عميق قائم على الصور

عبدالله شنيمر

قسم علوم الحاسب، كلية علوم الحاسب وتقنية المعلومات، جامعة جازان، المملكة العربية السعودية

الملخص

يعد إخفاء الشفرة أداة مهمة في تطوير البرامج الضارة. هنا ، يتم تعديل أجزاء من الكود لتصبح قابلة للتنفيذ بحيث لا تكون الشفرة مفيدة للمتسلل ولكنها تظل تعمل بكامل طاقتها. يتم استخدام صيغة البرنامج من قبل معظم تقنيات الكشف عن الشفرات المبهمة للكشف عن الرموز غير المعروفة. باستخدام الدمج القائم على الصور وبنى الشبكات العصبية التلافيفية المتطورة ، نقدم تقنية اكتشاف جديدة لاكتشاف تشويش الكود. تدمج هذه الطريقة مجموعتين من التعليمات البرمجية في صورة واحدة عن طريق تطبيق تمييز بناء الجملة وتحويل الصورة إلى نص شفرة المصدر الخام ، وبالتالي إعادة إنشاء المعنى المرئي للكود كما يظهر في IDE. نحن نستخدم الميزات التي تم جمعها من زوج من الصور بعد أن تم تحويلها إلى بكسل. علاوة على ذلك ، يتم استخدام عدد كبير من مجموعات بيانات الشفرة المبهمة المتاحة للجمهور لتقييم كفاءة نهجنا ، ويتم استخدام العديد من معايير التقييم لتقييم جودة الاكتشاف لنهجنا المقترح. من المثير للدهشة ، استنادًا إلى الاستدعاء والدقة وقياس F1 ، أننا نحصل على أداء بنسبة ٩٩٪ -١٠٠٪ في اكتشاف الشفرة المشوشة.

الكلمات المفتاحية: التعتيم على الكود. رمز غامض تعلم عميق؛ التشابه القائم على الصورة ، البرمجيات الخبيثة المشفرة.

Pavement Maintenance Management System of Jazan City Roads Using Geographic Information Systems

Mahmud Abdelrahim Abdelgiom[1,*], Ali Yahiya Almalki[2] ,and Gar Al-nabi Ibrahim Mohamed[3]

[1] Assistant Professor, Department of Civil Engineering, College of Engineering, Jazan University, KSA

[2] Assistant Professor, Department of Civil Engineering, College of Engineering, Jazan University, KSA

[3] Associate Professor, Hydrographic Surveying Department, Faculty of Maritime Studies, King Abdulaziz University, KSA

Abstract

Many of the developed countries throughout the world depend on an interconnected infrastructure that is constructed in compliance with international standards. It includes constructed infrastructure such as road network, sewage network, collection and treatment centers, water pipe network, electrical network, communication network, and rainy drain network.

One element of economic development is the construction of roads. In this situation, it is preferable to have a comprehensive database supported by a regular periodic maintenance plan in Jazan city to assist in providing the maintenance teams with comprehensive information on infrastructure services in order to prevent errors that occur in the absence of information and precise coordinates of the locations where the infrastructure services networks intersect.

The purpose of the study was to develop a database (digital model) for the road network using Geographic Information Systems (GIS) in order to manage the different constructed infrastructure. A ground monitoring system (ground photogrammetric) that gathers its data in a control room can be connected to this digital model. In Jazan city's scheme 6, the creation of the digital model for internal roads was put into practice. Cadastral surveying was used to gather data on the locations of road problems, and following processing and validity testing, this data was included to the database model.

The cost was determined based on the asphalt mixture's ton costs and only the quantities of asphalt mixture needed for maintenance work.

Keywords: Geographic Information Systems (GIS), Cost Estimation, Jazan City, Roads Maintenance, Geo-database, construction Management.

1. Introduction

The pavement condition evaluation of Jazan roads is the subject of a study by (Mubaraki 2014) with the working title "Identification of Pavement Distress Types and Pavement Condition Evaluation Based on Network Level Inspection for Jazan City Road Network." Abdelgiom and Mubaraki (2018) conducted a study in which they used geographic information systems to examine the King Faisal Road settlement and look into its root causes. The soil and concrete-asphalt mixture samples are taken straight from the road and evaluated. GIS is then utilized for geodatabase creation, mapping, and hydrologic analysis.

A geographic Information System (GIS) is a system for mapping and analyzing any object on earth. It is a way of gathering, storing, and managing any type of data with spatial components. GIS data are usually stored in more than one layer. It is the fundamental aspect of GIS, and working with layers of geographical information is generally known as data integration. GIS technology integrates powerful database capabilities with unique visual perspective of a good old fashioned-map. This makes GIS unique among various information collection systems.

Basically, this system utilizes hardware, software, user, and effective management to collect, store, analyze and present the related information of a given area on the earth. Even more, it has the capability to overlap maps and provide an information inquiry facility that can indirectly create a completely new set of information. Here, data output can be obtained in the form of tables, maps, graphs or a combination of this three. The other powerful aspect of GIS is its flexibility in modeling spatial objects to suit the particular needs of the user or application. GIS provides a set of tools or computer programs that allow the user to perform a specific operation on the map, assisted by a set of attribute data. This paper is conducted in Jazan City (Scheme 6), with the objective to explore the potential of GIS in capturing, storing, updating, retrieving, displaying, and printing data to facilitate road database management. Road maintenance is monitored effectively within the district by using the application of ArcGIS10.1 software (Zulkifli B, et al.,2010).

Always the success of GIS is mostly dependent on information structure analysis and conceptual data modeling (Demirel, 2002).

1.1 Uses of GIS in Managing Road Maintenance

A geographic information system (GIS) is a tool that can be used to collect, store, process, and display many kinds of geographic data. Since its introduction, GIS technology has aided the road construction sector in improving the effectiveness of its operations.

These systems enable the planning, administration, and upkeep of road infrastructure through the use of dynamic maps that provide a real-time representation of geo-data. All kinds of information can be gathered from many systems and combine them into a single common platform by using an online GIS. This essay will go through the advantages of GIS technology for the road construction sector. (https://ellipsis-drive.com/blog/how-the-roadwork-industry-can-benefit-from-gis-technology).

According to Yunus and Hassan's 2010 study, "Managing Road Maintenance

Using Geographic Information System Application," the study results in a better organization of the management of digital road data. Additionally, GIS tools boost productivity when managing road repair.

1.1.1 Use of GIS Technology to Store Data and Information Accurately

There are several types of reports during roadwork or maintenance projects, which can be a little intimidating. These reports may include state of the roads, bridges, potholes, road markings, and other infrastructure. Making judgments is made easier when having all of this information in one spot. It helps to save many sorts of data and adapt them based on needs using online GIS. With the aid of an interactive map, the data may be tied to specific geo-locations or coordinates to make it easier grasp. GIS systems might actually make it simpler to carry out field operations and enhance tactics. (https://ellipsis-drive.com/blog/how-the-roadwork-industry-can-benefit-from-gis-technology).

1.1.2 Oversee the Roadwork in Real Time

The problem can be located on the map and label it using GIS technology. They can be updated, examined, and shared with the teamwork using the map editor. They are prepared for the situation when they arrive on location.

On their tablets or smart phones, the maintenance may also send back reliable information. To submit forms and maps, there is no need to go back and forth to the office. The data can be quickly customized, and it is immediately available. In addition to providing quick access to data, it can help in foresee potential problems like potholes, cracks in the road, and vegetation hazards. I addition, it helps to save time and money by developing an informed risk management strategy.

By giving employees immediate notice of any potential dangers and alarms (Huang,et al.2010). Virtual reality (VR) and augmented reality (AR) are both essential for delivering interactive education, as are communication and positioning technologies (Syberfeldt, et al,2020). Real-time monitoring made possible by sensing and the Internet of Things (IoT) also offers chances to control construction waste (Sartipi,2020), improving environmental sustainability and lowering environmental footprint.

The analysis of current studies on building project monitoring in real time. The review concentrates on sensor technologies and approaches for scene interpretation, location, and monitoring of construction activities in both indoor and outdoor situations in real-time(Rao,et.al, 2022).

1.1.3 Get Accurate Information

Receiving current information is essential whether the maintenance personnel at the office or out in the field. This information must all be readily available. It is simpler to oversee the day-to-day operations of the numerous teams as a result. Additionally, it improves communication and team efficiency.
To download all the reports, it is only require to exchanging information. The GIS cloud is also completely scalable, making it appropriate for any project size. (https://ellipsis-drive.com/blog/how-the-roadwork-industry-can-benefit-from-gis-technology).

2. Statement of the Problem

The availability of a multipurpose map of the infrastructure works serves as a representation of the issue of road maintenance. The multi-purpose map contains a database of all subsurface utilities, including telephone and telecommunication networks, sewer lines, and electrical and water pipelines.

Therefore, in order to save time and money and safeguard this infrastructure work, a technology-based road maintenance GIS model is crucial. In light of the issue, ArcGIS10.1 has the ability to analyze, gather, store, manipulate, display, and edit vector and raster data. ArcGIS10.1 is a quick and simple way to create appropriate apps in addition to having a wealth of tools. The proposed model will be coded as a geodatabase and road maintenance model and integrated with the GIS platform in order to demonstrate the efficacy and greater usage of ArcGIS10.1.

3. Objectives of the Research

The major goal of this paper is to create a decision-making model that will be applied to the ArcGIS 10.1 platform to create thematic and network maps of roads as well as to organize road repair tasks. This would make it easier to use the money more effectively and plan it in accordance with the fundamental requirements for upkeep.

Establishing a Pavement Maintenance Management System (PMMS) for the road and parking network in Jazan City-Scheme 6 is the goal of this article. The study's goals might be summed up as follows:

a. To provide a thorough and integrated database for scheme 6's road pavement

b. To create map layers using a Geographic Information System (GIS) for the inventory of the road network and engineering attributes like pavement thickness, material qualities, road condition, etc.

c. To assess the study area's discomfort and pavement condition

d. To calculate the cost of maintenance for each stretch of pavement in the research area

4. Methods and Software

4.1 Field of study

The research region chosen for this paper's study of creating and managing maintenance in roads using the technology of the Geographical Information System in the scheme 6 area of Jazan City is depicted in Figure (1).

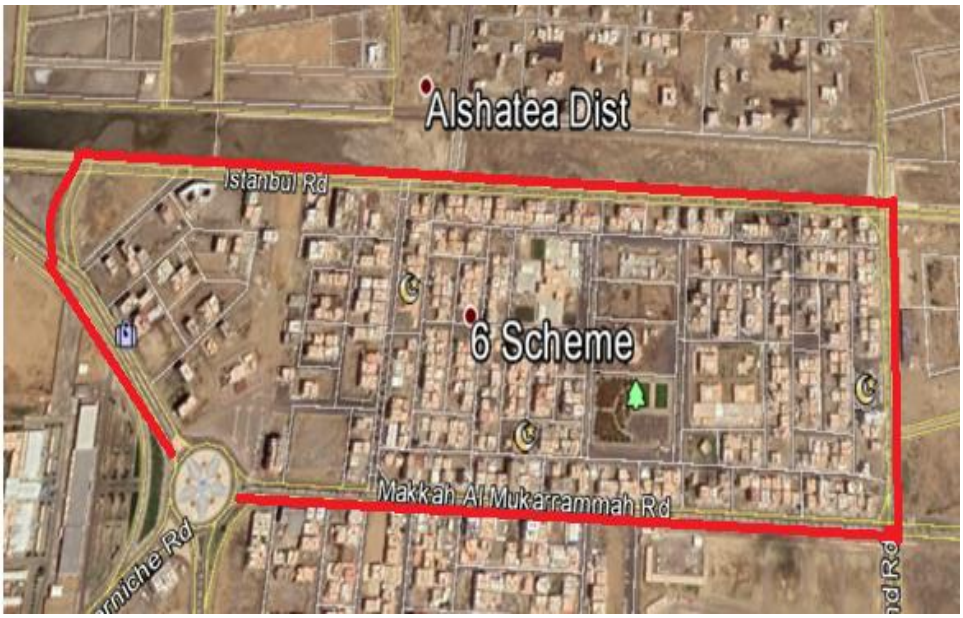


Figure 1. The Studied Area

4.2 Software used

ArcGIS version 10.1 is the program used in the study of road maintenance. The launch of ArcGIS 10.1 heralds a significant change in how GIS professionals and their companies will access and manage geographic information in the years to come. Professionals in GIS now have access to a full GIS thanks to ArcGIS10.1, which better connects desktops, servers, mobile, and web applications. It offers businesses the extra resources and infrastructure they require to expand the use of their current GIS. Additionally, it makes it easier for enterprises to switch to next-generation GIS ideas and platforms without risking their present GIS investments.

4.3 Methodology of Building the Geo-database and Roads Maintenance Management System (RMMS)

The methodology adopted for building the geo-database and road maintenance management system is summarized in the steps below and the flow chart presented in figure 2.

1. Collection of data which includes detailed surveying by Global Positioning System (GPS)of the study area, coordinates of distresses location (See Table 1).A lot of photos are captured and are stored in the GIS maintenance and management system. Figure 3 shows a typical sample of these photos
2. Measurement of the maintenance area in the road and location of the positions of distresses in the road by tapes and asphalt measurement tools
3. Computer programs were used to achieve the objectives of this research, such as Microsoft Excel, and ArcGIS10.1
4. Comparison and discussion of the results of volumes of pavement defect areas in the roads of the study area
5. Estimation of the total cost of the maintenance

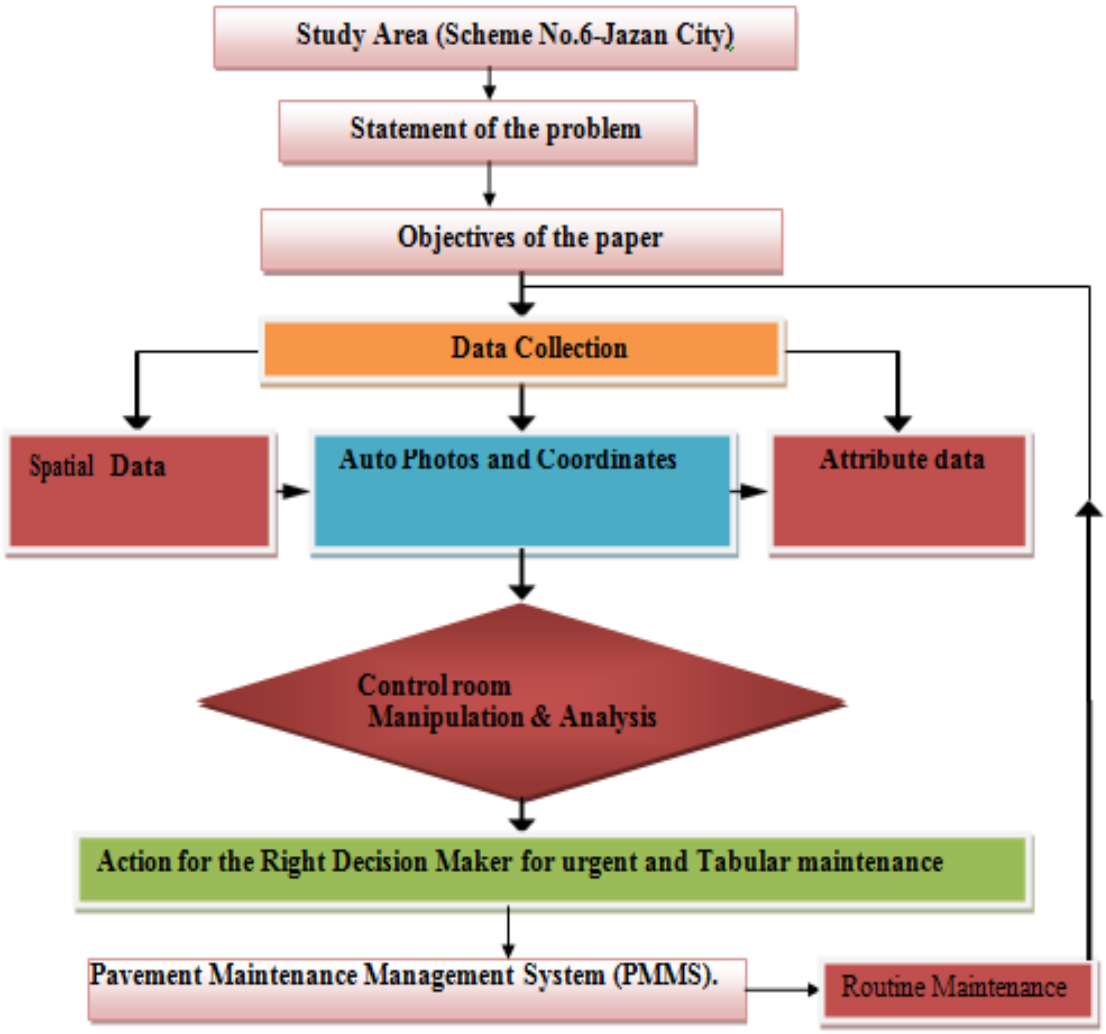


Figure 2. Road Maintenance Flowchart

Figure 3. Samples of Photos Captured from the Field

Table 1. The Coordinates of the Distresses in Roads of Scheme No. 6

Location no	Easting (m)	Northing(m)
1	239623.2	1873424.45
2	239679.33	1873414.53
3	239679.33	1873414.53
4	239744.57	1873422.94
5	239809.96	1873443.66
6	239614.36	1873427.63
7	239866.21	1873442.96
8	239872.81	1873498.24
9	239873.27	1873535.14
10	239814.49	1873569.71
11	239832.94	1873624.84
12	239820.94	1873612.69
13	239821.29	1873640.36
14	239890.33	1873716.4
15	239882.48	1873799.54
16	239832.23	1873806.32
17	239835.5	1873830.88
18	239838.57	1873840.07
19	239793.67	1873800.65
20	239705.29	1873835.58
21	239681.3	1873811.27
22	239698.95	1873801.82
23	239707.48	1873774.04
24	239688.92	1873709.67

5. Data Collection for Paper

The geodatabase model of the road maintenance in the study area was developed by integrating the research different data types, using ArcGIS10.1 geospatial data processing facilities. Both spatial and attribute GIS data have been gathered via a variety of data collection methods, including detailed surveying using a total station or GPS, topographic maps, digital maps with satellite pictures, aerial photographs, interviews, survey questionnaires, and other data (T.cay,et al. 2021).

Photos are integrated in model using ArcGIS10.1 interactive map display facilities, attributes data input and GPS positional data were integrated in the model using ArcGIS10.1 vector data facilities (See Table1). Samples of photos are shown in the Figure 3 and appendixA).

6. SPATIAL ANALYSIS OF DATA USING GIS

The research data was processed and analyzed using ArcGIS10.1 software spatial analysis facilities. These included Selection by Attribute, Selection by location, Buffering commands and Query commands. After establishing a geodatabase model of the road maintenance in the study area a lot of analysis is carried out to support the decision maker for road maintenance.

Road management is becoming more and more dependent on spatial analysis to evaluate the performance of the road infrastructure. As a result, multiple parameters are gathered as explanatory variables, including ground-monitored vehicle observations and remotely sensed climatic and environmental data from satellites(Song, et al.,2018).

Typical examples of these spatial operations are presented in (Appendix B) is listed in figures (B1 to B7).

7. RESULTS AND DISCUSSION

The study of geographic places through the use of mathematical models and statistics is known as spatial analysis. According to https://www.agiratech.com/spatial-analysis-patterns-geography, it uses GIS technologies and methods to depict the real world, including climate predictions, current trends, assessments of crises and pandemics, variations in the data collected, decision-making in complex situations, whether in business or government, site analysis for selecting the ideal locations, etc.

It is a tool where to get all the needed geographic information, which is provided as inputs based on the tasks. Effective analysis requires the use of sophisticated geo-processing techniques. The outcomes are displayed as a map with graphs or statistics. Many different fields use spatial analysis; we have included the main fields and subfields below where they are widely used.

7. 1 Results

The spatial analysis results of the research data are presented in Table 2. Table 2 shows the results of areas, fill volumes, and the total cost of material cost (Asphalt Concrete Mixture) is derived from the road maintenance database. These data are classified in geo-databases according to the roads distresses of the study area.

The following formula of quantity of asphalt in road is used:

1. **The Volume of Asphalt Wearing Course (AWC) by cubic meter = A *(h_1+ h_2+ h_3+,…., h_n)/n *C.F m^3…….Eq.(1)**

Where:

- A: Area of the road maintenance section
- (h_1+ h_2+ h_3+,…., h_n)/n: Average depth
- F.C : Compaction Factor(C.F) the compaction factor(C.F) for AWC (1.28% - 1.3%) in Asphalt 1.3 is used

2. **The Quantity of Asphalt mixture by tone = (Density *volume)/1000*C.F**

Where:

- The Density = 2330 kg/m3
- F.C: Compaction Factor (C.F) the compaction factor (C.F) for AWC (1.28% - 1.3%) in Asphalt
- 1.3 is used
- The total maintenance cost is estimated a according to the price of cubic meter of asphalt (300 S.R Riyadh refinery-2022)

Table 2. Areas, Fill Volumes, and the Total Cost of Asphalt

Location	Area(m^2)	Actual Fill Volume(m^3)	Quantity of Asphalt(Tone)	Description of Distresses	Distresses Cost(S.R)
1	1.7	1.598	4.840342	Pothole	1452.1026
2	0.3685	0.606	1.835574	Pothole	550.6722
3	2.394	2.25	6.81525	Pothole	2044.575
4	13.344	0.47	1.42363	Patching	427.089
5	57.54	3.042	9.214218	Rutting	2764.2654
6	1.441	0.119	0.360451	Pothole	108.1353
7	1.82	0.107	0.324103	Pothole	97.2309
8	14.96	0.738	2.235402	Rutting	670.6206
9	7.5	0.353	1.069237	Rutting	320.7711
10	2.43	0.143	0.433147	Pothole	129.9441
11	0.8	0.0564	0.1708356	Rutting	51.25068
12	25	1.175	3.559075	Patching (electric cables)	1067.7225
13	12.87	0.605	1.832545	Patching (electric cables)	549.7635
14	8.8	0.372	1.126788	Rutting	338.0364
15	6.545	0.154	0.466466	Rutting	139.9398
16	20	1.175	3.559075	Rutting	1067.7225
17	1.1	0.078	0.236262	Rutting	70.8786
18	2.1	0.099	0.299871	Rutting	89.9613
19	4.205	0.208	0.630032	Pothole	189.0096
20	0.5808	0.048	0.145392	Pothole	43.6176
21	2.415	0.131	0.396799	Pothole	119.0397
22	105.19	9.888	29.950752	Rutting	8985.2256
23	17.004	1.159	3.510611	Rutting	1053.1833
24	15.98	1.127	3.413683	Rutting	921.69441
Total	326.0873	25.699	77.8495406	Rutting	23252.45169

7.2 Discussion of the Results

The Total cost of asphalt for reconstructing the Distresses in the study area equal 23252.45 S.R and is classified into the three parts:

1- The total percentage of Rutting equal 70.84%

2- The total percentage of Potholes equal 20.36%

3- The total percentage of Patching equal 8.79 % (See Figure 4).

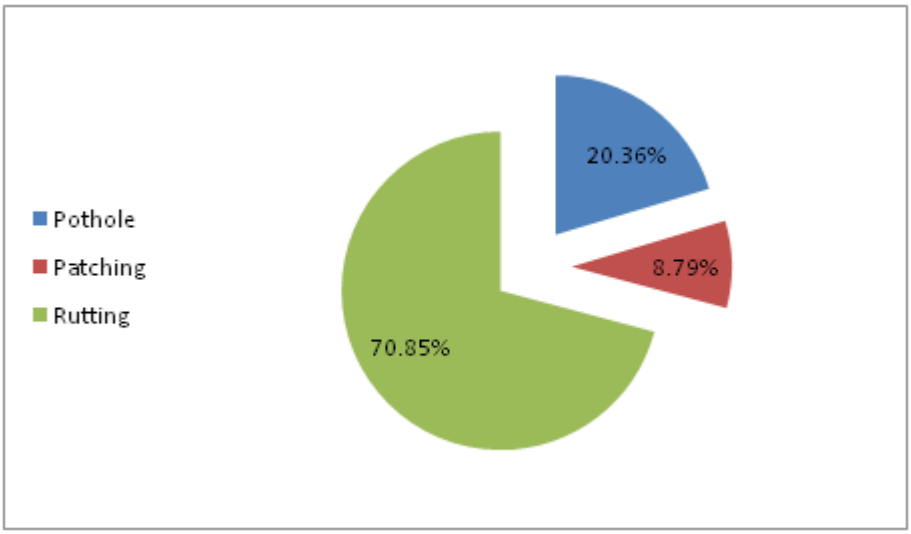


Figure 4. Classification of Distresses

The following charts in figure 5 classified the distresses according to the fill area.

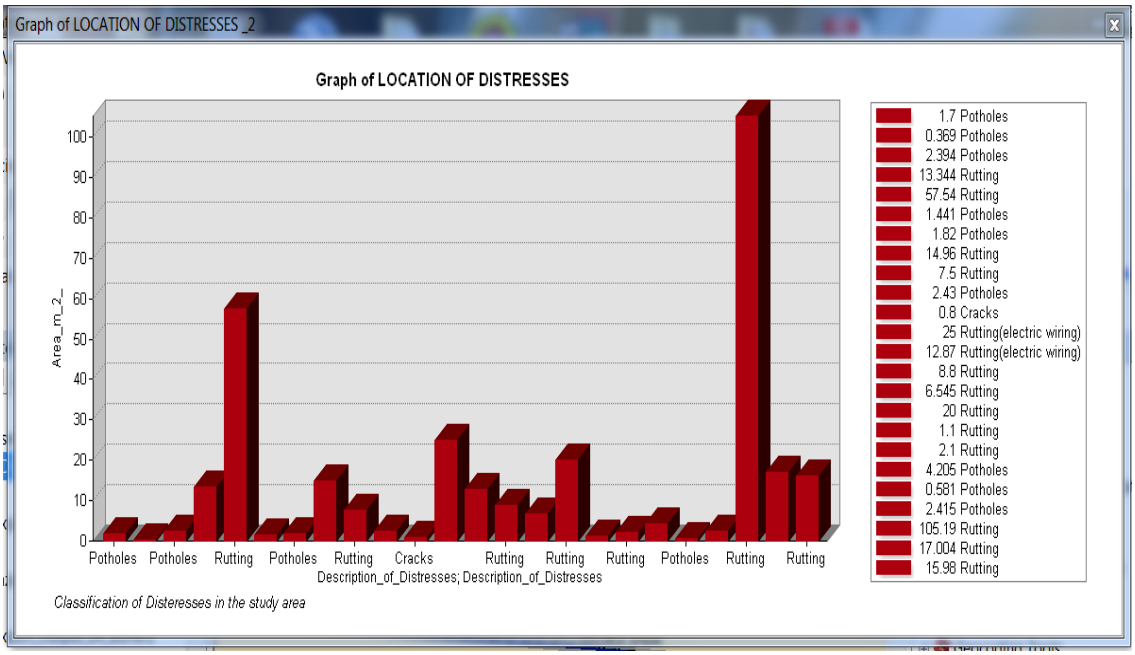


Figure 5. Classification of Distresses in the Studied Area

8. Conclusions

The Ministry pays close attention to road maintenance because it firmly believes that, in order to maintain a level of road efficiency and guarantee the safety of its users, road maintenance and preservation are just as necessary as their implementation. Preventive and routine maintenance is required for more than 60,000 kilometers of paved roads.

A more organized administration of digital data, especially that pertaining to road maintenance data, will result from the deployment of GIS in road maintenance in the research area. The steps of the typical road maintenance job in Jazan City are site visits, surveying projects, assessing the road distresses, estimating the cost of asphalt, and performing the repair. In controlling road maintenance, the GIS system application will also improve job productivity.

The goals set for this study have been fulfilled. Consequently, the following conclusions about the GIS system can be taken from this study:

1. The GIS maintenance model is fairly simple to set up and is appropriate for non-specialist usage of GIS
2. It can quickly recall maintenance data and is comparatively simple to use
3. It reduces unnecessary duplication of work in the gathering of geographical data
4. It can enhance the consistency, correctness, and up-to-dateness of the data that is kept
5. It encourages data sharing and improves teamwork
6. The acquired map data is more organized and safe

Finally, the total maintenance cost is estimated according to the price of a cubic meter of asphalt (cubic meter equal 300 S.R Riyadh refinery-2022).

8.1 Maintenance Suggestions for the future:

The organization and employee skills determine how each nation classifies its road maintenance activities, which are often either routine or periodic. (M. Y. Shaghasy, 2010)

In Jazan City, routine maintenance, periodic maintenance, emergency maintenance, and seasonal maintenance are currently part of the ongoing road maintenance efforts. It is advised that this paper be continued, especially in the design and evaluation of systems for managing the assets on roads.

Additional data, such as black spot areas, roadside development, and other factors connected to road maintenance, should be gathered to aid in planning, reduce costs, and improve decision-making in order to improve the management of road maintenance. The list of advice is represented by what follows:

1. To avoid patching, clotting, and repairing roads, a study of public utility lines should be conducted alongside this one prior to the construction of this road
2. To develop services, cooperation between several Jazan Utility Corporations should be used
3. GIS applications for maintenance management should use all available information, including spatial and non-spatial data, data on climate

4. change, and data on utility services

5. In the real world, using GIS for civil engineering projects has become commonplace. We proposed the creation of a separate GIS lab with a license for ArcGIS in its most recent iteration by the road maintenance unit

6. In the maintenance operation of potholes distress, remove any moist material, clean the area, and then pour asphalt mixture to the potholes pain. Compaction should be permitted for 25% additional volume. Use a straight edge to connect the repair to the existing section of road

7. In the maintenance operation of rutting distress, Pavements are leveled by adding hot, mulled asphalt ingredients. Add a thin asphalt plant-mix overlay or roto-mill overlay after that. By milling, remove the plastic mix and replace it with stable win

8. In the maintenance operation of patching, after the patch area has been cleaned, it is filled with the appropriate asphalt mixture, leaving 25% of the patch's depth open for compaction

References

1. Association of State Highway and Transportation Officials (AASHTO) Standard Specifications for Transportation Materials and Methods of Sampling and Testing AASHTO 245 –Washington DC, 1993.

2. Cay, T., Iscan, F., & Durduran, S. S. (2004, July). The cost analysis of satellite images for using in GIS by the pert. In XX ISPRS Congress, Com. IV (pp. 12-23).

3. Demirel, H. (2002). "An Integrated Approach to the Conceptual Data Modelling of an Entire Highway Agency Geographic Information System".Institute of Geodesy and Geo information Technology Berlin Technical University. PhD. 131 p.

4. F. Sartipi, Influence of 5G and IoT in construction and demolition waste recycling – conceptual smart city design, Journal of Construction Materials 1 (4) (2020) pp. 1–9. doi:10.36756/JCM.v1.4.1.

5. https://www.agiratech.com/spatial-analysis-patterns-geography.

6. (https://ellipsis-drive.com/blog/how-the-roadwork-industry-can-benefit-from-gis- technology).

7. Langunzad, L.V. and Mcpherson, K., GIS Applications for Road Network of The Philippines: A new Technology in Road Management. In journal of the Eastern Asia Society for

Transportation Studies, volume 5, October 2003.pp. 846 -854, 2003.
8. Mahmoud Abdelrahim Abdelgiom, and Muhammad Mubaraki. "Evaluating Settlement on King Faisal Road Using GIS Analysis Techniques." Civil Infrastructures Confronting Severe Weathers and Climate Changes Conference. Springer, Cham, p. 96-109, 2018.
9. McGennis, R. B.; Anderson, R. M.; Kennedy, T. W.; Solaimanian, M. "Background of SUPERPAVE Asphalt Mixture Design and Analysis". U.S Department of Transportation, Federal Highway Administration, Report No. FHWA-SA-95-003, 1995.
10. Mohd Zulkifli B. Mohd Yunus, Hamidah Bt. Hassan, Managing Road Maintenance Using Geographic Information System Application, Journal of Geographic Information System, 2010, 2, 215-219.
11. Mubaraki, M. "Identification of pavement distress types and pavement condition evaluation based on network level inspection for Jazan City road network." The Journal of Engineering Research [TJER] 11.1 (2014): 44-54.
12. M. Y. Shaghasy, Technical Guideline for Road Maintenance of Rural Roads, 1st ed., USOPS Press, 2010, pp. 7-8.
13. Norkhair Ibrahim and Zulkifli Majid, "Prinsip Sistem Maklumat Geografi," Principal of Geographic Infor- mation System, Universiti Teknologi Malaysia, 2002.
14. O. Danielsson, M. Holm, A. Syberfeldt, Augmented reality smart glasses in industrial assembly: Current status and future challenges, Journal of Industrial Information Integration 20 (2020) pp. 100175. doi:10.1016/j.jii.2020.100175.
15. Rao, A. S., Radanovic, M., Liu, Y., Hu, S., Fang, Y., Khoshelham, K., ... & Ngo, T. (2022). Real-time monitoring of construction sites: Sensors, methods, and applications. *Automation in Construction*, *136*, 104099.
16. Ruslan Rainis and Noresah Mohd Shariff, "Sistem Maklumat Geografi," Geographic Information System, Dewan Bahasa Dan Pustaka, Kuala Lumpur, 1998.
17. Roads Maintenance manual, Transport ministry, Saudi Arabia,2019.
18. Song, Y., Wright, G., Wu, P., Thatcher, D., McHugh, T., Li, Q., ... & Wang, X. (2018). Segment-based spatial analysis for assessing road infrastructure performance using monitoring observations and remote sensing data. Remote Sensing, 10(11), 1696.
19. Yunus, Mohd Zulkifli B. Mohd, and Hamidah Bt Hassan. "Managing road maintenance using geographic information system application." Journal of Geographic Information System 2.4 (2010): 215.
20. Z. Zhao, L. Shen, C. Yang, W. Wu, M. Zhang, G. Q. Huang, IoT and digital twin enabled smart tracking for safety management, Computers & Operations Research 128 (2021) pp. 105183. doi:10.1016/j.cor.2020.105183.

نظام إدارة الصيانة لطرق جازان باستخدام نظم المعلومات الجغرافية

محمود عبد الرحيم عبد القيوم ١ * علي يحيى المالكي ٢وجار النبي إبراهيم محمد ٣

قسم الهندسة المدنية ، كلية الهندسة ، جامعة جازان ، ، السعودية ،

قسم الهندسة المدنية ، كلية الهندسة ، جامعة جازان ، السعودية ،

قسم المساحة الجغرافية ، كلية الدراسات البحرية ، جامعة الملك عبد العزيز ، المملكة العربية السعودية

ملخص

تعتمد العديد من البلدان المتقدمة في جميع أنحاء العالم على بنية تحتية مترابطة تم إنشاؤها وفقًا للمعايير الدولية ، وتشمل البنية التحتية المشيدة مثل شبكة الطرق وشبكة الصرف الصحي ومراكز التجميع والمعالجة وشبكة أنابيب المياه والشبكة الكهربائية وشبكة الاتصالات وشبكة تصريف الأمطار.

إن أحد عناصر التنمية الاقتصادية هو بناء الطرق ، لذلك يفضل في هذه الحالة وجود قاعدة بيانات شاملة مدعومة بخطة صيانة دورية منتظمة في مدينة جازان للمساعدة في تزويد فرق الصيانة بمعلومات شاملة عن خدمات البنية التحتية من أجل منع الأخطاء التي تحدث في غياب المعلومات والإحداثيات الدقيقة في المواقع التي تتقاطع فيها شبكات خدمات البنية التحتية.

كان الهدف من هذه الدراسة هو تطوير قاعدة بيانات (نموذج رقمي) لشبكة الطرق باستخدام نظم المعلومات الجغرافية (GIS) من أجل إدارة البنية التحتية المختلفة التي تم إنشاؤها. يمكن توصيل نظام مراقبة الأرض (القياس التصويري الأرضي) الذي يجمع بياناته في غرفة التحكم بهذا النموذج الرقمي. في مخطط رقم ٦ بمدينة جازان ، تم إنشاء النموذج الرقمي للطرق الداخلية موضع التنفيذ. تم استخدام المسح العقاري لجمع البيانات عن مواقع مشاكل الطرق ، وبعد المعالجة واختبار الصلاحية ، تم تضمين هذه البيانات في نموذج قاعدة البيانات. تم تحديد التكلفة بناءً على تكاليف خليط الإسفلت اللازمة لأعمال الصيانة

الكلمات المفتاحية: نظم المعلومات الجغرافية (GIS) ، تقدير التكلفة ، مدينة جازان ، صيانة الطرق ، قاعدة البيانات الجغرافية ، إدارة التشييد.

Appendix A

Figure 6. Pothole (Location No.3)

Figure 7. Patching (Location No.4).

Figure 8. Rutting (Location No.3)

Appendix B

Table

LOCATION OF DISTRESSES

point_no	E__m_	N_m_	L_m__	W_m_	D_m_	Area_m_2_	Volume_m_3	Actual_Vol	Cost_of_material_A	Description_of_Distresse
1	239623.2	1873424.45	1.7	1	0.4	1.7	0.68	1.598	431.46	Potholes
2	239679.33	1873414.53	0.67	0.55	0.7	0.3685	0.25795	0.606183	163.669275	Potholes
3	239679.33	1873414.53	2.1	1.14	0.4	2.394	0.9576	2.25036	607.5972	Potholes
4	239744.57	1873422.94	27.8	0.48	0.015	13.344	0.20016	0.470376	127.00152	Rutting
5	239809.96	1873443.66	13.7	4.2	0.0225	57.54	1.29465	3.042427	821.455425	Rutting
6	239614.36	1873427.63	2.2	0.655	0.035	1.441	0.050435	0.118522	32.001008	Potholes
7	239866.21	1873442.96	1.4	1.3	0.025	1.82	0.0455	0.106925	28.86975	Potholes
8	239872.81	1873498.24	6.8	2.2	0.021	14.96	0.31416	0.738276	199.33452	Rutting
9	239873.27	1873535.14	3	2.5	0.02	7.5	0.15	0.3525	95.175	Rutting
10	239814.49	1873569.71	2.7	0.9	0.025	2.43	0.06075	0.142763	38.545875	Potholes
11	239832.94	1873624.84	1.6	0.5	0.03	0.8	0.024	0.0564	15.228	Cracks
12	239820.94	1873612.69	25	1	0.02	25	0.5	1.175	317.25	Rutting(electric wiring)
13	239821.29	1873640.36	11.7	1.1	0.02	12.87	0.2574	0.60489	163.3203	Rutting(electric wiring)
14	239890.33	1873716.4	4.4	2	0.018	8.8	0.1584	0.37224	100.5048	Rutting
15	239882.48	1873799.54	7.7	0.85	0.01	6.545	0.06545	0.153807	41.528025	Rutting
16	239832.23	1873806.32	4	5	0.025	20	0.5	1.175	317.25	Rutting
17	239835.5	1873830.88	2.2	0.5	0.03	1.1	0.033	0.07755	20.9385	Rutting
18	239838.57	1873840.07	4.2	0.5	0.02	2.1	0.042	0.0987	26.649	Rutting
19	239793.67	1873800.65	2.9	1.45	0.021	4.205	0.088305	0.207517	56.029523	Potholes
20	239705.29	1873835.58	1.32	0.44	0.035	0.5808	0.020328	0.047771	12.898116	Potholes
21	239681.3	1873811.27	1.75	1.38	0.023	2.415	0.055545	0.130531	35.243302	Potholes
22	239698.95	1873801.82	15.7	6.7	0.04	105.19	4.2076	9.88786	2669.7222	Rutting
23	239707.48	1873774.04	65.4	0.26	0.029	17.004	0.493116	1.158823	312.882102	Rutting
24	239688.92	1873709.67	34	0.47	0.03	15.98	0.4794	1.12659	304.1793	Rutting

Figure 9. Attribute Data Input and Calculations

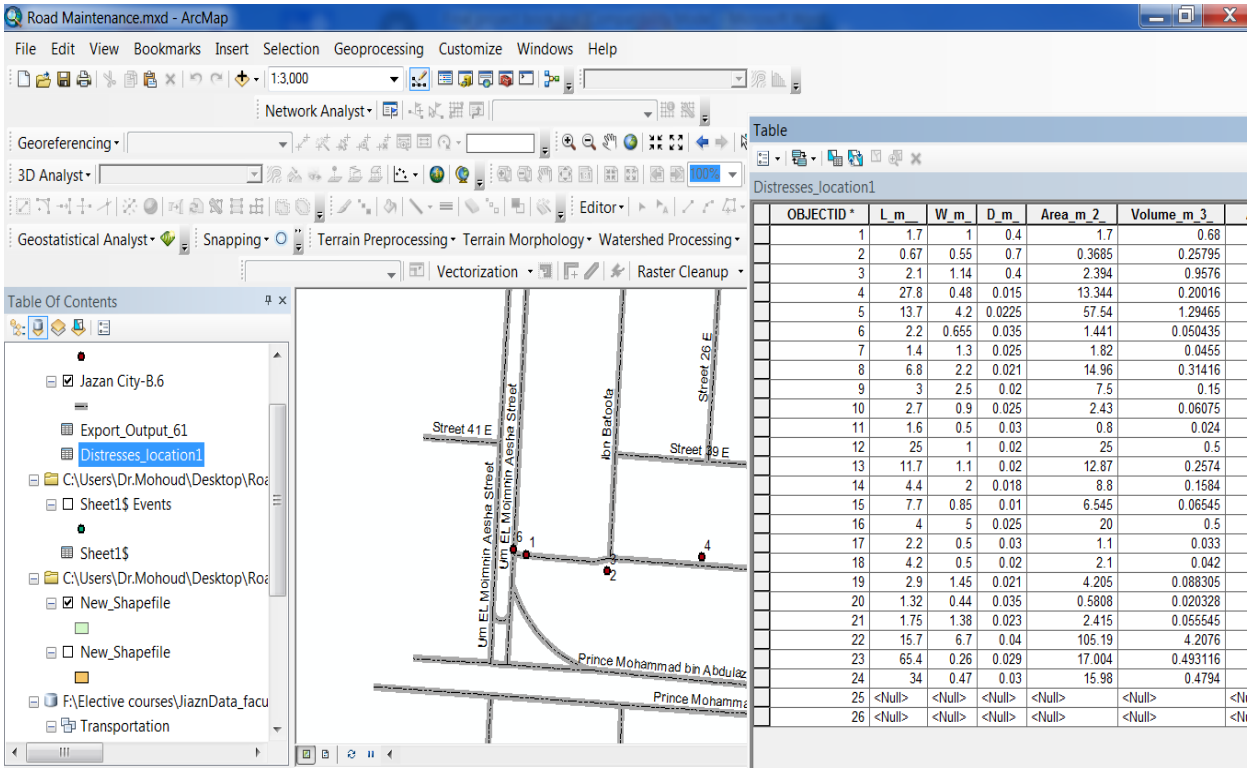


Figure 10. All Theme Legends Displayed in the Form of Table Content

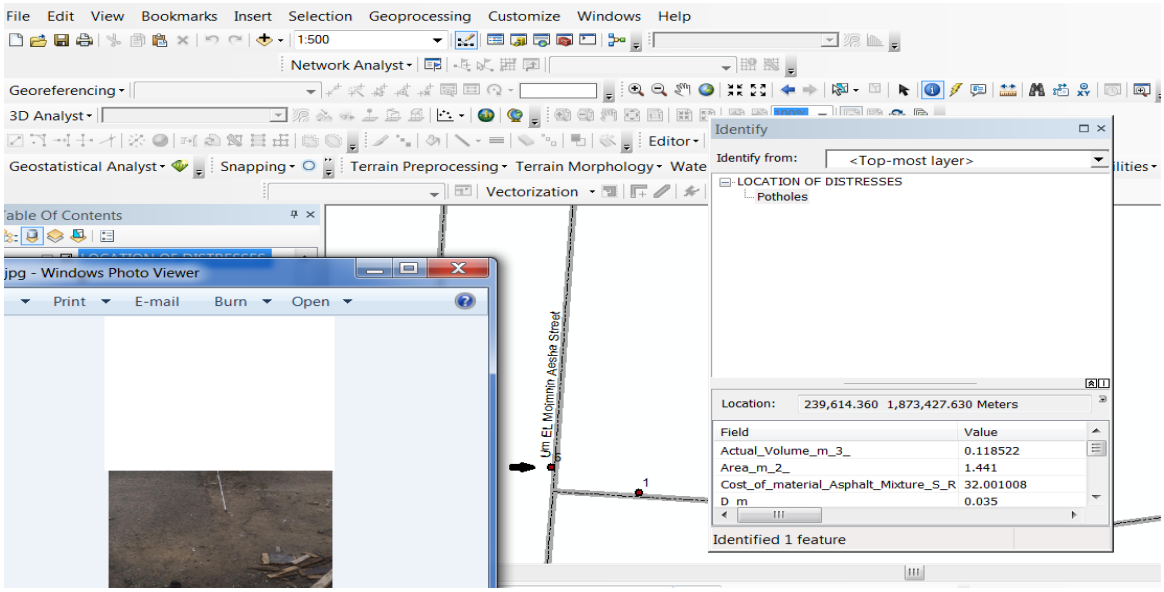


Figure 11. Creating Hyperlink in location 6 in the Um El Momnin Aesha Street

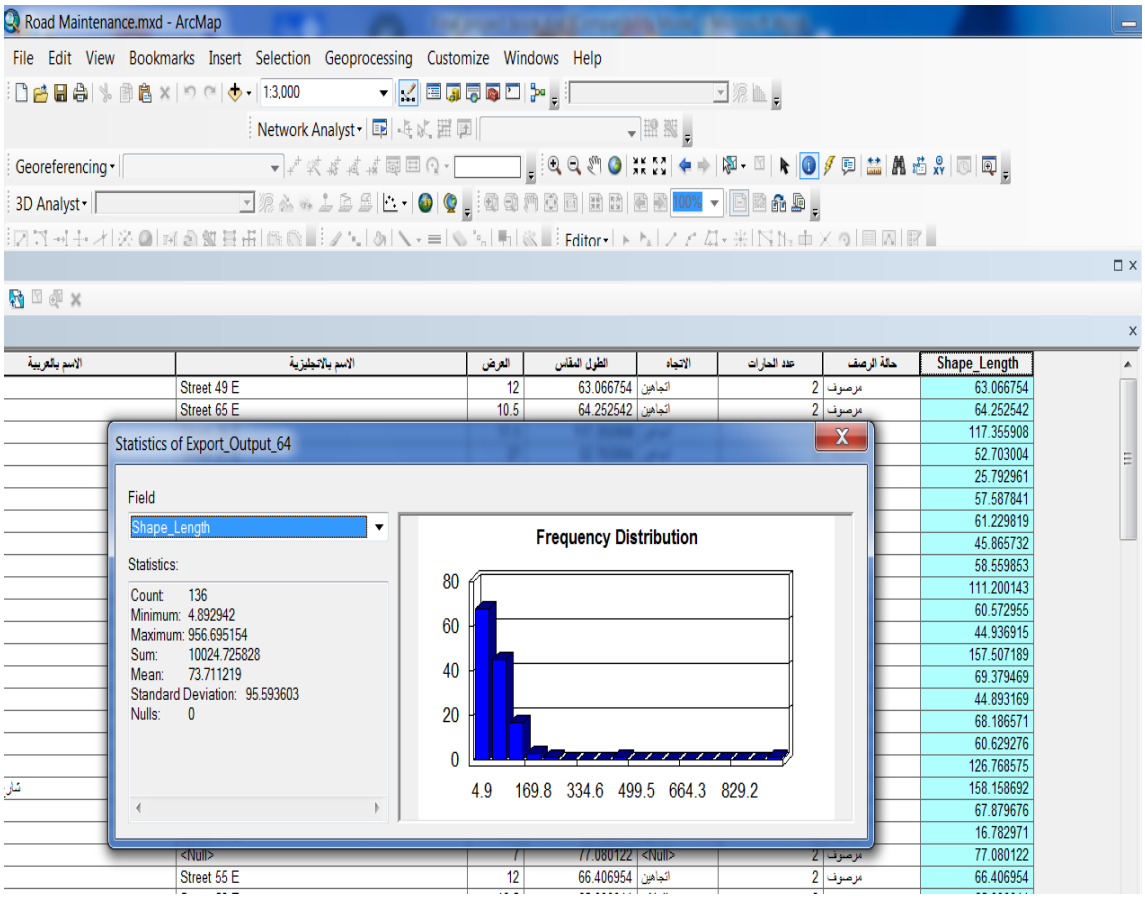


Figure 12. GIS Statistical Analysis of Roads in the Studied Area

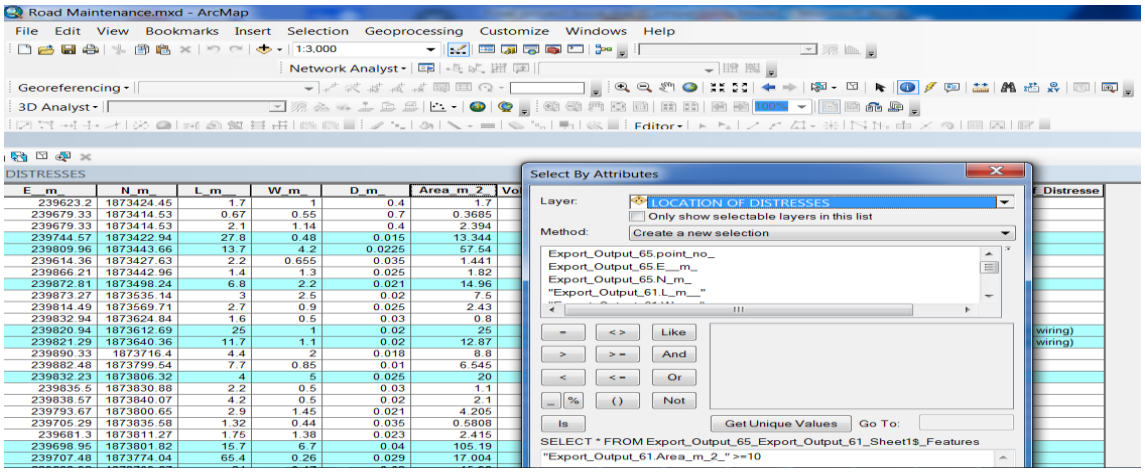


Figure 13. Analysis using selecting by attributes command

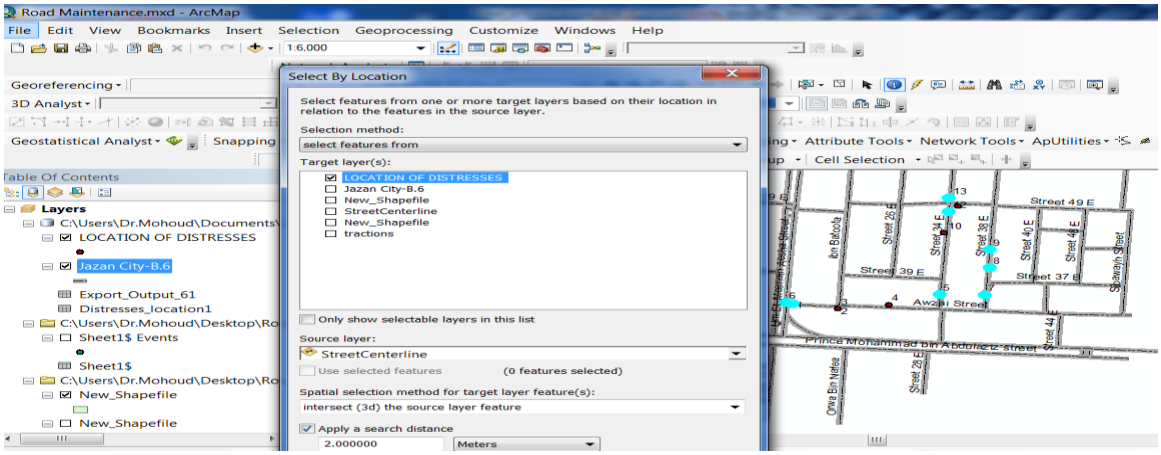


Figure 14. The Distresses within 2 m of the Road's Centerline

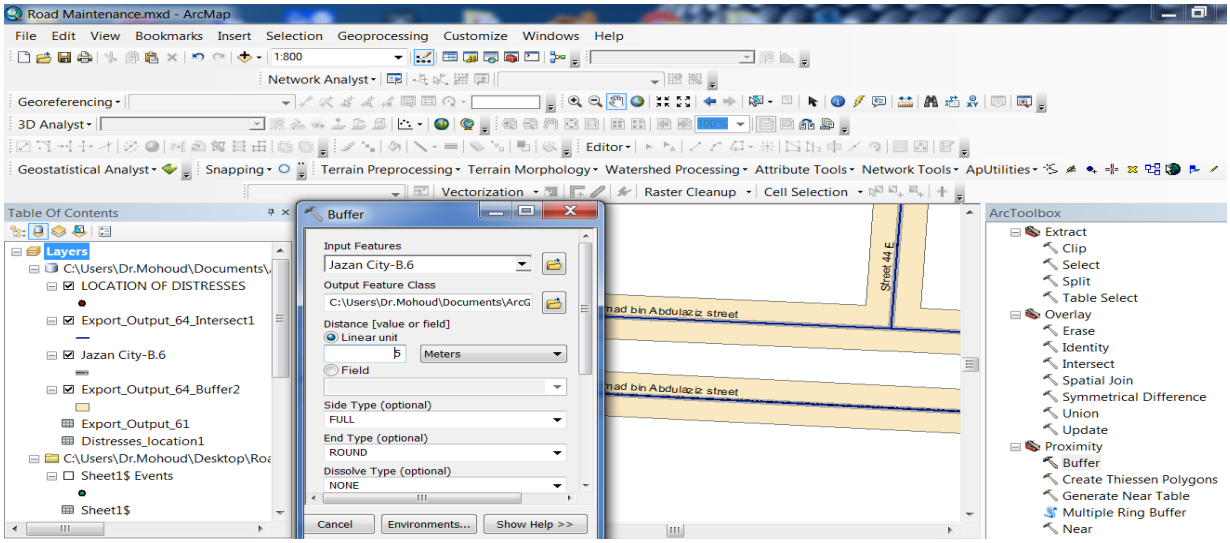


Figure 15. GIS Buffering Command

مجلة جامعة جازان

للعلوم التطبيقية

دورية علمية محكمة

المراسلات

توجه جميع المراسلات إلى:

رئيس هيئة التحرير مجلة جامعة جازان للعلوم التطبيقية جازان –المدينة الجامعية –البرج الإداري – ص ب ١١٤. –الرمز البريدي ٤٥١٤

المملكة العربية السعودية أو على البريد الإلكتروني jas@jazanu.edu.sa

المملكة العربية السعودية

وزارة التعليم

جامعة جازان

مجلة جامعة جازان

للعلوم التطبيقية

دورية علمية محكمة

ملحق المجلد ١١ العدد ١ (ربيع الأول ١٤٤٥هـ - سبتمبر ٢٠٢٣م)

ردمد : ١٦٥٨-٦٩١٣

قواعد النشر في المجلة

مجلة جامعة جازان للعلوم التطبيقية دورية علمية محكمة تنشرها الجامعة، وهي تهدف إلى إتاحة الفرصة للباحثين لنشر إنتاجهم العلمي وتقوم المجلة بنشر المواد الآتية :

١ـ البحث : ويندرج تحت تخصص الباحث ويجب أن يحتوي على إضافة للمعرفة في مجاله .

٢ـ المقالة الاستعراضية التي تتضمن عرضًا نقدياً لبحوث سبق إجراؤها في مجال معين أو أجريت في خلال فترة زمنية محددة.

٣ـ البحث المختصر.

٤ـ نقد الكتب .

٥ـ الخطابات الموجهة إلى المحرر ، والملاحظات والردود ، والنتائج الأولية .

تقوم هيئة التحرير، بالنظر في نشر المواد المعرفية ذات الصلة بذلك الفرع، وتقدم البحوث الأصلية، التي لم يسبق نشرها، وفي حال قبول البحث للنشر تؤول كل حقوق النشر للمجلة و لا يجوز نشره في أي منفذ نشر آخر ورقيا أو إلكترونياً، دون إذن كتابي من رئيس هيئة التحرير .

تعليمات النشر في المجلة

١ـ تقديم المواد : يقدم أصل البحث مخرجا في صورته النهائية متضمنا الإشارة إلى أماكن الجداول والأشكال داخل المتن و مطبوع على هيئة صفحات مرقمة ترقيما متسلسلا، مع ضرورة إرفاق قرص ممغنط مطبوع عليه البحث على برنامج Ms Word باستخدام النظام المتوافق مع IBM ، وسيعتذر عن قبول أي بحث لا يلتزم مؤلفه بهذه التعليمات.

٢ـ الملخصات: يرفق ملخصان بالعربية والإنجليزية للبحوث و المقالات الاستعراضية والبحوث المختصرة على ألا يزيد عدد كلمات كل منهما على ٢٠٠ كلمة، وعلى عمود واحد بعرض كتابة ١٣ سم.

٣ـ لا بد من احتواء كل بحث على كلمات مفتاحية (Key Words) توضع أسفل الملخصين العربي والانجليزي على ألا تزيد عن عشر كلمات.

٤ـ الجداول والمواد التوضيحية: يجب أن تكون الجداول والرسومات واللوحات مناسبة لمساحة الصف في صفحة المجلة ١٦ ٢٤ سم بالحواشي، ويتم إعداد الأشكال الخطية على برامج الحاسب الآلي، ولا تقبل إلا أصول الأشكال. كما يجب أن تكون الخطوط واضحة ومحددة ومنتظمة من حيث كثافة الحبر وتناسب سمكها مع حجم الرسم، ويراعى أن تكون الصور الفوتوغرافية (الضوئية) الملونة وغير الملونة مطبوعة على ورق لماع، أو محملة على برنامج (Adobe Photoshop) مع كتابة عنوان لكل جدول، وتعليق لكل شكل وصورة، والإشارة إلى مصدر المادة إن كانت مقتبسة.

٥ـ الاختصارات: يجب استخدام الاختصارات المقننة دولية مثل : سم، مم، م، كم، سم، مل، مجم، كجم...إلخ.

٦ـ المراجع :يشار إلى المراجع داخل المتن بنظام الاسم والتاريخ، وتوضع المراجع جميعها في قائمة المراجع بنهاية المادة مرقمة ومتبعة نظام ترتيب البيانات الببليوجرافية التالي :

أـ يشار إلى الدوريات في المتن بنظام الاسم والتاريخ بين قوسين على مستوى السطر، أما في قائمة المراجع فيبدأ المرجع بذكر الاسم الأخير للمؤلف، ثم الاسم الأول، ثم الأسماء الأخرى أو اختصاراتها بالخط الأسود، ثم سنة النشر بين قوسين، فعنوان البحث كاملا بين علامتي تنصيص" " ، فاسم الدورية، فرقم المجلد، ثم رقم العدد : ثم أرقام الصفحات تفصل بشرطة .

مثال : هادي، أحمد بن جابر. (٢٠١١م)،" استخدام تقنية النانو لتعريف الشفرات الوراثية "مجلة جامعة جازان، ١، ١ : ٢٠٠ـ٢٢٠.

بـ يشار إلى الكتب في المتن داخل قوسين بالاسم والتاريخ . أما في قائمة المراجع، فيكتب الاسم الأخير للمؤلف، ثم الاسم الأول، ثم الأسماء الأخرى أو اختصارا تها، ثم سنة النشر بين قوسين، فعنوان الكتاب بين علامتي تنصيص، ثم بيان الطبعة، فالناشر، فمدينة النشر :ثم صفحات الكتاب إن وجدت.

مثال :

عبدالهادي، محمد علي، (١٤٣٣هـ)،" مقدمة في التقنية الحيوية"، جامعة جازان، جازان.

ويجب عدم استخدام الاختصارات المرجعية مثل :المرجع نفسه . المرجع السابق...إلخ.

٧ـ أـ الحواشي: تستخدم لتزويد القارئ بمعلومات توضيحية، ويشار إليها في المتن بأرقام مرتفعة عن السطر .وترقيم التعليقات متسلسلة داخل المتن. وفي حال الضرورة؛ يمكن الإشارة إلى مرجع داخل الحاشية عن طريق استخدام كتابة الاسم والتاريخ بين قوسين وبنفس طريقة استخدامها في المتن، وتوضع الحواشي أسفل الصفحة التي تخصها والتي ذكرت بها و تفصل بخط عن المتن وبخط أصغر.

بـ يستخدم في تخريج الأحاديث والآثار الطريقة المنهجية المعتمدة في هذا الفن وهي كالآتي : اسم المؤلف ـ اسم الكتاب ـ رقم الجزء والصفحة والحديث.

٨ـ المواد المنشورة في المجلة تعبر عن وجهة نظر صاحبها، ولا تعبر بالضرورة، عن رأي مجلة جامعة جازان.

٩ـ يتأكد الباحث من صحة اللفظ وسلامة لغة البحث، وخلوه من الأخطاء اللغوية والنحوية.

١٠ـللمجلة الحق في تحديد أولويات نشر البحوث.

١١ـالمجلة غير ملزمة بإعادة البحوث التي تصل إليها سواء أجيزت للنشر أم لم تجز.

١٢ـيتم إخضاع جميع البحوث المستلمة لفحص مبدئي، من قبل هيئة التحرير، لتقرير أهليتها للتحكيم، ويحق لها أن تعتذر عن قبول البحث دون إبداء الأسباب.

١٣ـتصدر المجلة مرتين في العام.

المملكة العربية السعودية

وزارة التعليم

جامعة جازان

مجلة جامعة جازان

للعلوم التطبيقية

دورية علمية محكمة

ردمد: ١٦٥٨-٦٩١٣

ملحق المجلد ١١ العدد ١ (ربيع الأول ١٤٤٥هـ - سبتمبر ٢٠٢٣م)