AN EVALUATION OF SECURITY LEVEL OF HYBRID OPTICAL-DIGITAL INFORMATION ENCRYPTION AND COMPRESSION OF OPTICAL IMAGES

R. Sivamalar[1], Dr. Swati Sharma[2]

[1](Lecturer, Dept of Computer Science and Information System Engg, Jazan University, Ministry of Higher Education, Jazan, Kingdom of Saudi Arabia, sivamalarphd@gmail.com)

[2](Associate Professor, Department of Electrical Engineering, Jodhpur National University, Jodhpur, Rajasthan, India, er.swathi.sharma15@gmail.com)

Abstract— *Due to the rapid growth of optical encryption and compression techniques, authentication of encoded information has the most significant process for providing high levels of optical security. The present optical encryption and compression methods can provide the secure access to the information and such techniques are improving day by day. In previous researches, hybrid optical encryption and compression was proposed with multiplexing scheme for encrypting and compressing the multiple images simultaneously. However, the classification of the encoded images using SVM and K-NN was simple and easily to distinguish for identifying the images which are obtained from fake samples and genuine samples. Hence in this paper, an Extreme Learning Machine (ELM) based classification is proposed for classifying the images which are encoded using the different approaches in order to evaluate the encoded performance. The main aim of this paper is to develop an optical system which has the highest-level of optical security with high identification complexity for identifying the encoded images. Finally, the experimental results show that improved security level by reducing the classification accuracy of encoded image identification.*

Keywords— Optical encryption and compression; Multiplexing; Encoding; Optical security; Classification; Extreme learning machine

1. INTRODUCTION

In modern years, optics and photonics technologies have been highly developed for security and encryption. Among different optical data security and encryption algorithms, the most used optical encryption method is Double Random Phase Encoding (DRPE) and Fourier domain [1]. Such optical techniques may provide large bandwidth, many degrees of freedom, small wavelengths, and multidimensional keys for security applications. However, the limitations of such methods are overcome by CKRMDRPE-DADWTC-LCSLM-CS-ENMF approach which performs different processes such as multiplexing, and simultaneous encryption and compression by using multiple optical images [2, 3].

In CKRMDRPE-DADWTC-LCSLM-CS-ENMF approach, both Enhanced Non-Negative Matrix Factorization (ENMF) and digital holography are introduced for multiplexing process. A number of images are transformed into the noise-like digital holograms. Then, the obtained digital holograms are decomposed into the defined number of basis images and corresponding weighting matrix by using ENMF. The ENMF is proposed based on the conventional NMF algorithm which is further improved by using k-means clustering algorithm in order to initialize the NMF factors randomly [4, 5]. Then, the basis images are encrypted based on the simultaneous optical image encryption and compression with digital information using liquid-crystal light modulators and compressive sensing scheme (CKRMDRPE-DADWTC-LCSLM-CS). This approach improves the PSNR value and reduces the computation complexity significantly. However, the classification of the encoded images for identifying the images which are obtained from fake samples and genuine samples was simple and easily to distinguish.

Therefore in this paper, an Extreme Learning Machine (ELM) based classification is proposed for classifying the images which are encoded using the different approaches with the aim of developing an optical system which has the highest-level of optical security high identification complexity for identifying the encoded images. The polarized light is used for illuminating the proposed system and the double random phase mask is used for encoding the optical image effectively. Then, the evaluation of encoded mechanisms is achieved based on the Extreme Learning Machine (ELM) classifier with the help of training dataset. Thus, the proposed system improves the multiple security levels of the optical image transmission efficiently.

The rest of the article is organized as follows: In Section 2, description of different optical encryption, compression, multiplexing, and security schemes are given. In Section 3, detailed information of the proposed optical image security authentication based hybrid encryption and compression is described. In Section 4, results of experimental results are presented. In Section 5, conclusion of the research work and its future scope are given.

2. RELATED WORK

Liu, S., & Sheridan, J. T. [6] proposed the optical encryption based on the different image scrambling methods

in fractional Fourier domains. In this proposed approach, data or information hiding was achieved in the two-dimensional images by utilizing the proposed approach. At first, the image was randomly shifted according to the jigsaw transform algorithm. Then, the pixel scrambling method was applied based on the Arnold Transform (ART). These scrambled images were encrypted in a randomly selected fractional Fourier domain. But, the quality of decrypted image depends on the ART time period and iteration number.

Gong, Q., et al. [7] proposed the multiple-image encryption and authentication including with the sparse representation by using space multiplexing. In this proposed approach, the redundant spaces in the sparse representation strategy were optimized. The sparse data of multiple encrypted images were extracted by using the Random Binary Amplitude Masks (RBAM). Then, the extracted images were combined into the synthesized ciphertext by using space multiplexing approach. Finally, the authentication was performed which requires both the random phase masks and the RBAM. Furthermore, the robustness of the system against noise and distortion was demonstrated.

Rajput, S. K., et al. [8] proposed an optical image security method based on the polarized light encoding and photon counting method. Initially, an input image was encoded by using the polarized light principle which is parameterized using Stokes-Mueller formalism. The encoded image was further encrypted by applying the photon counting imaging method for obtaining the photon limited image. The photon limited decrypted image was then obtained by using the polarized light decoding method with the help of appropriate keys. The obtained photon counted decrypted image was verified based on the correlation filters. In addition, this approach was also used for hologram watermarking.

Lai, J., et al. [9] proposed a novel image encryption algorithm based on the Fractional Fourier Transform (FRFT) and Chaotic system. In this approach, the image encryption process was performed by using two processes. Initially, the image was encrypted by employing Fractional Fourier domain double random phase. Then, the confusion image was encrypted by using confusion matrix which is generated by chaotic system. Finally, the cipher image was obtained securely. However, the security of the algorithm depends on the sensitivity to the randomness of phase mask, the order of fractional Fourier transform and the initial conditions of chaotic system.

Chang, H. T., et al. [10] proposed the wavelength multiplexing multiple-image encryption by using cascaded phase-only masks in the Fresnel transform domain. In this paper, wavelength multiplexing was proposed based on the Modified Gerchberg-Saxton Algorithm (MGSA) and cascaded phase modulation method in the Fresnel transform domain for reducing the interference in the multiple-image-encryption method [11]. Initially, each plain image was encoded to the complex function by using MGSA. Then, the phase components of the generated complex functions were multiplexed with different wavelength parameters and then these parameters were modulated before multiplexing as a phase-only function which is recorded in the first Phase-Only Mask (POM). Finally, the second POM was generated by applying the MGSA again on the amplitude derived from the summation of the total generated complex functions.

Nishchal, N. K., & Naughton, T. J. [12] proposed the flexible optical encryption with multiple users and multiple security levels. In this paper, a basic optimal encryption framework was presented which utilizes various cryptography applications according to the multiplexing scheme. Here, users may decrypt the different private images from the similar encrypted images and a superuser may have a key that decrypts all encrypted images. In addition, the multiplexed images were also encrypted along with the different levels of security. Moreover, a real-world three-dimensional scene was used which is captured with digital holography and encrypted by using fractional Fourier transform.

Perez-Cabre, E., et al. [13] proposed photon-counting imaging based double random phase encryption for information security and verification. In this paper, a deeper analysis of the photon-counting imaging based DRPE method was presented. In this approach, the sparse encrypted distribution was generated and the decoded image cannot be recognized by direct visual inspection. By utilizing the reduced number of photons in the encryption process, verification of the decrypted information by nonlinear correlation was demonstrated and its discrimination from very similar images was also achieved. Thus, the vulnerability of the DRPE technique was overcome by this approach.

3. Proposed Methodology

In this section, the proposed secure authentication of optical images using polarization and classification of encoded image using ELM are explained.

A. Polarization Technique for Hybrid Optical-Digital Information Encryption and Compression

During polarization in hybrid encryption and compression method, a quasi-monochromatic transverse electromagnetic field is propagating in the z-axis direction and is defined as $E = \big(E_x(r,t), E_y(r,t), 0\big)$. The state of polarization of the wave-front is described by Stokes vector $S = (S_0, S_1, S_2, S_3)$ and the Stokes parameters are defined as follows:

$$S_0 = \langle E_x^* E_x \rangle + \langle E_y^* E_y \rangle$$

$$S_1 = \langle E_x^* E_x \rangle - \langle E_y^* E_y \rangle$$

$$S_2 = \langle E_x^* E_y \rangle + \langle E_y^* E_x \rangle$$

$$S_3 = i\big[\langle E_y^* E_x \rangle - \langle E_x^* E_y \rangle\big] \quad (1)$$

In equation (1), $\langle \cdot \rangle$ refers the temporal average over time interval T and

$$\langle E_i^* E_j \rangle = \frac{1}{T} \int_T E_i^* E_j \, dt \quad (2)$$

Here, S_0 refers the measure of the irradiance of the beam, S_1 compares the irradiance of the wave in the x and y-directions, and S_2 is similar to S_1 but the comparison is performed along two perpendicular directions rotated $\pm 45^\circ$ with respect to the x-axis [14]. In addition, S_3 provides the information of the circular content of the wave. Such as, for a linearly polarized beam with the polarization angle ψ with respect to the x-axis, the Stokes vector represents as $S =$

$S_0(1, \cos 2\psi, \sin 2\psi, 0)$. Elliptically polarized light is defined as Stokes vector:

$$S = S_0(1, \cos 2\psi \cos 2\epsilon, \sin 2\psi \, cos \, 2\epsilon, \sin 2\epsilon) \quad (3)$$

In equation (3), ϵ refers the eccentricity angle. The degree of polarization is described as follows:

$$P = \frac{1}{S_0}\sqrt{S_1^2 + S_2^2 + S_3^2}, P \leq 1 \quad (4)$$

The Stokes parameters are easily measured with help of a polarizer. Whereas the light is characterized by these Stokes parameters, the samples and optical devices which are interacted with the light are described by the components of Mueller matrix. When the light beam interacts with matter, the resulting state-of-polarization is obtained by multiplying the Muller matrix by the Stokes vector. If the beam passes through the different optical devices, the overall Mueller matrix is obtained by combining the Muller matrices of each element. The Muller matrices for a linear polarizer with polarization axes in the $0^\circ, 45^\circ, 90^\circ, and -45^\circ$ directions are given in below.

$$M_{0^\circ} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; \; M_{\pm 45^\circ} = \frac{1}{2}\begin{pmatrix} 1 & 0 & \pm 1 & 0 \\ 0 & 0 & 0 & 0 \\ \pm 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix};$$

$$M_{90^\circ} = \frac{1}{2}\begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix};$$

$$M_{QWP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \quad (5)$$

These values are obtained based on the Fresnel coefficients. Moreover, the Muller matrix for a different direction of polarization θ is obtained by using rotation matrix $R(\theta)$ as,

$$R(\theta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\theta & \sin\theta & 0 \\ 0 & -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (6)$$

$$M_\theta = R(-\theta) M_{0^\circ} R(\theta) \quad (7)$$

By using this polarization approach, the polarized laser beam is passed through the lenses. Then, the encryption and compression operations are performed simultaneously. After that, the encoded optical images are classified in order to identify the fake and genuine samples which provide high complexity for identification and prove the effectiveness of the encoding.

B. Extreme Learning Machine (ELM) Classification

Consider a training dataset X for M_θ arbitrary samples and I^x represents a x dimensional feature of m^{th} sample and J^y represents the target vector. The arbitrary samples are represented as (x_m, v_m) and $x_m = [x_{m1,} x_{m2} \ldots . x_{mx,}]^T \epsilon I^x$ and $v_m = [v_{m1,} v_{m2} \ldots . v_{my,}]^T \epsilon J^y$. The single hidden layer feed forward neural network is represented in mathematical form which is given as follows:

$$\sum_{m=1}^{\tilde{x}} \beta_m h_m(x_p) = \sum_{m=1}^{\tilde{x}} \beta_m h(w_m x_p + bias_m) = y_k, k = 1,2, \ldots M \quad (8)$$

Where w is the input weight matrix that connects the input and hidden nodes and $\beta_m$is the output weight matrix that connects the output and hidden nodes and $w_m x_p$ is the inner product of w_m and x_p and y is the output vector with the activation function of $h(x)$. In the extreme learning machine the hidden nodes are randomly it degrade the performance of classification [15]. The matrix form of ELM is given as follows:

$$H\beta = Y \quad (9)$$

Where H is the hidden matrix, β is the output weight, and Y is the output vector. These are given as follows:

$$H(w, b, x) = \begin{bmatrix} g(w_1 \cdot x_1 + b_1) & \cdots & g(w_m \cdot x_1 + b_m) \\ \vdots & \ddots & \vdots \\ g(w_1 \cdot x_p + b_1) & \cdots & g(w_m \cdot x_p + b_m) \end{bmatrix}_{p \times m} \quad (10)$$

$$\beta = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_m \end{bmatrix}_{m \times k} \; and \; Y = \begin{bmatrix} y_1 \\ \vdots \\ y_k \end{bmatrix}_{m \times k} \quad (11)$$

Thus, the classification of encoded image is achieved by using the output vector and output weight values using ELM classifier. This increases the complexity of identification of the original image from encoded images in order to identify the samples which are obtained from fake and genuine samples.

Algorithm: ELM Classification

Input: Training Set X, activation function h(x), M number of hidden node;

Output: Output weight β, input bias $bias_m$, input weight w_m;

- Assign input weight and bias randomly
- Compute the hidden layer output matrix H
- Compute the output weight $\beta = H^T Y$

4. EXPERIMENTAL RESULTS

In this section, the performance of the proposed approach is analyzed with the other techniques. For evaluating the performance, two optical images such as A and B are taken as input image for encryption and compression. The comparison is made between CKRMDRPE-DADWTC, CKRMDRPE-DADWTC-LCSLM, CKRMDRPE-DADWTC-LCSLM-CS, and CKRMDRPE-DADWTC-LCSLM-CS-ENMF in terms of precision, recall, and classification accuracy using SVM, K-NN and ELM classifiers.

The optical encrypted images using CKRMDRPE-DADWTC, CKRMDRPE-DADWTC-LCSLM, CKRMDRPE-DADWTC-LCSLM-CS, and CKRMDRPE-DADWTC-LCSLM-CS-ENMF are shown in figure 1.

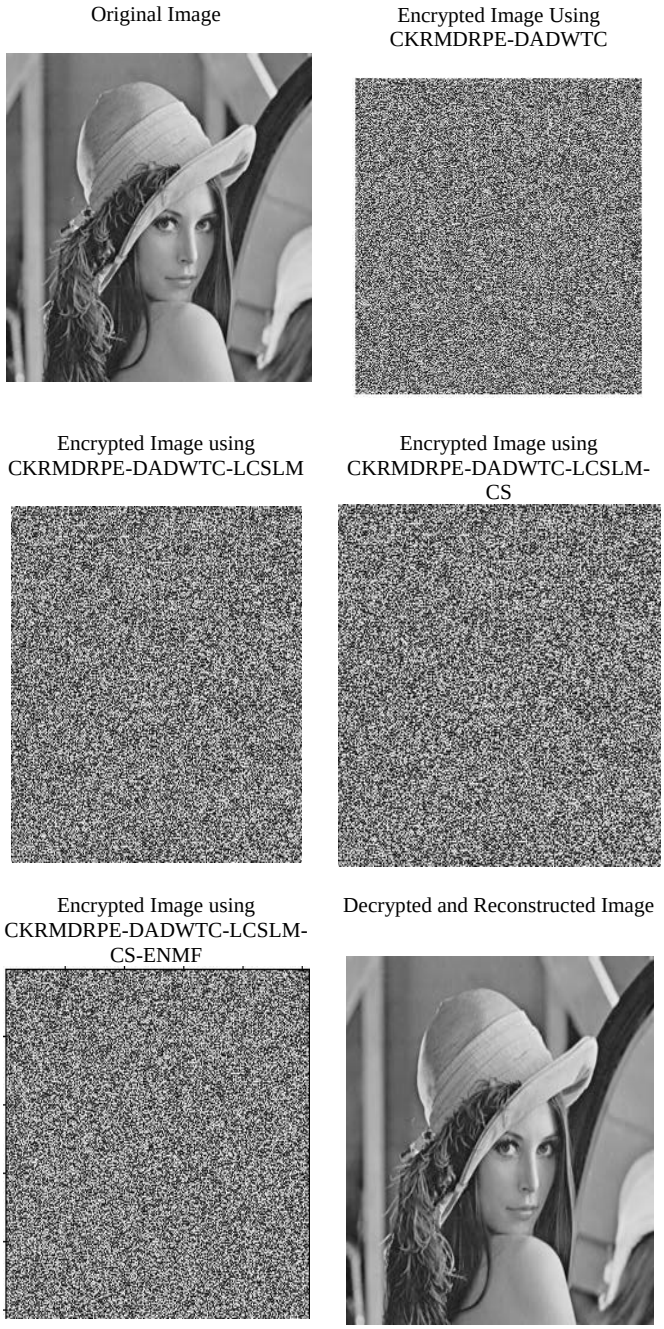

Fig 1. Original Image, Encrypted Images and Decrypted Image

A. *Precision*

Precision is defined as the ratio of the true positives or measured based on the user prediction at true positive and false positive values. It is measured by using the following formula:

$$Precision = \frac{True\ Positive\ value\ (TP)}{True\ Positive\ value\ (TP) + False\ Positive\ value\ (FP)}$$

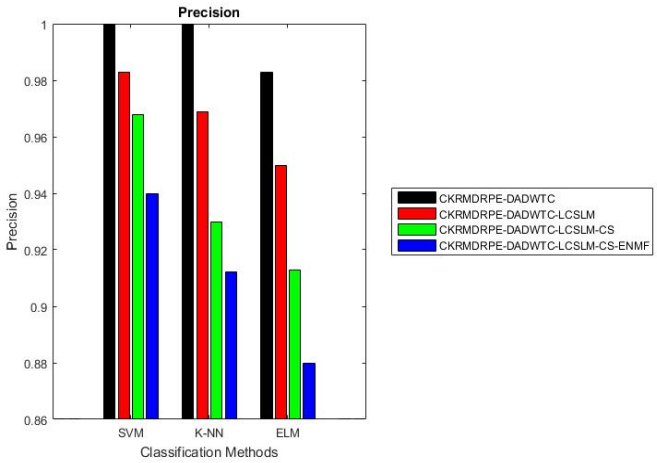

Fig 2. Comparison of Precision

Figure 2 shows that the comparison of different optical image encryption and compression schemes with different classifiers in terms of precision. From the graph, it is observed that CKRMDRPE-DADWTC-LCSLM-CS-ENMF has precision value of 0.88 whereas the other classifiers have high precision values. Thus, it proves that the ELM provides the complex identification of encoded image by reducing the precision value.

B. *Recall*

Recall is defined based on the successful prediction at true positive rate and false negative rate. It is evaluated by using the following formula:

$$Recall = \frac{True\ Positive\ value\ (TP)}{True\ Positive\ value\ (TP) + False\ Negative\ value\ (FN)}$$

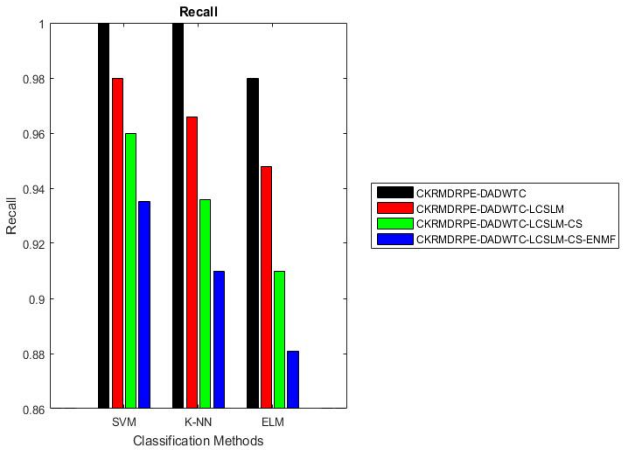

Fig 3. Comparison of Recall

Figure 3 shows that the comparison of different optical image encryption and compression schemes with different classifiers in terms of recall. From the graph, it is observed that CKRMDRPE-DADWTC-LCSLM-CS-ENMF has recall value of 0.882 whereas the other classifiers have high recall values. Thus, it proves that the ELM provides the complex identification of encoded image by reducing the recall value.

C. Classification Accuracy

Accuracy means the proportion of true positives and true negatives among the total number of features examined and it is given by,

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

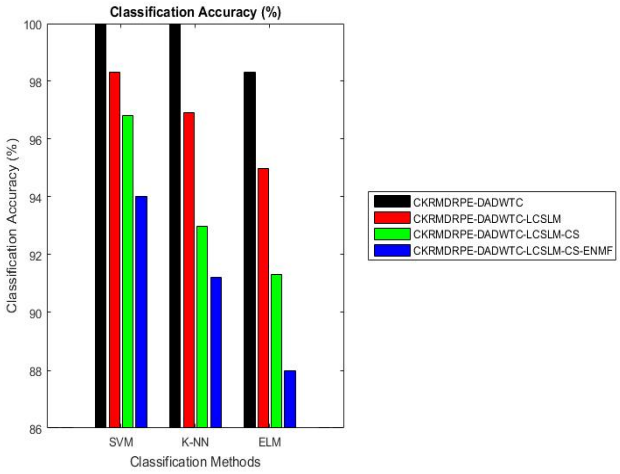

Fig 4. Comparison of Classification Accuracy (%)

Figure 4 shows that the comparison of different optical image encryption and compression schemes with different classifiers in terms of classification accuracy (%). From the graph, it is observed that CKRMDRPE-DADWTC-LCSLM-CS-ENMF has classification accuracy value of 88% whereas the other classifiers have high accuracy values. Thus, it proves that the ELM provides the complex identification of encoded image by reducing the classification accuracy value.

5. Conclusion

In this paper, the secure authentication of an optical image is enhanced by improving the polarization approach and ELM classification method. The main aim of the proposed method is designing an optical system which has the highest-level of optical security with high identification complexity for identifying the encoded images. The polarized light beam is used for illuminating the proposed system and double random phase mask is used for encoding the optical images. The polarization patterns of the optical images are described by using Muller matrix which uses the Stokes parameters. Then, the ELM is applied for classifying the encoded images in order to evaluate the effectiveness of the encoding mechanism. The experimental results show that the proposed ELM classifier has high level of security during transmission of optical images than the other classification techniques.

References

[1] W. Chen, B. Javidi, and X. Chen, “Advances in optical security systems”, Advances in Optics and Photonics, vol. 6, no. 2, pp. 120-155, 2014.

[2] R. Sivamalar, and S. Sharma, “An optical image encryption using chaotic kicked rotator map with double random phase encoding”, International Journal of Applied Research in Science and Engineering, pp. 118-123, 2016.

[3] R. Sivamalar, and S. Sharma, “Simultaneous encryption and compression using chaotic kicked rotator map–DRPE with direction adaptive discrete wavelet transform”, International Journal for Technological Research in Engineering, pp. 170-174, 2016.

[4] H. T. Chang, J. W. Shui, and K. P. Lin, “Image multiplexing and encryption using the nonnegative matrix factorization method adopting digital holography”, Applied Optics, vol. 56, no. 4, pp. 958-966, 2017.

[5] L. Gong, and A. K. Nandi, “An enhanced initialization method for non-negative matrix factorization”, IEEE International Workshop on Machine Learning for Signal Processing, pp. 1-6, 2013.

[6] S. Liu, and J. T. Sheridan, “Optical encryption by combining image scrambling techniques in fractional Fourier domains”, Optics Communications, vol. 287, pp. 73-80, 2013.

[7] Q. Gong, X. Liu, G. Li, and Y. Qin, “Multiple-image encryption and authentication with sparse representation by space multiplexing”, Applied optics, vol. 52, no. 31, pp. 7486-7493, 2013.

[8] S. K. Rajput, D. Kumar, and N. K. Nishchal, “Photon counting imaging and polarized light encoding for secure image verification and hologram watermarking”, Journal of Optics, vol. 16, no. 12, 125406, 2014.

[9] J. Lai, S. Liang, and D. Cui, “A novel image encryption algorithm based on fractional Fourier transform and chaotic system”, International Conference on Multimedia Communications, pp. 24-27, 2010.

[10] H. T. Chang, H. E. Hwang, and C. L. Lee, “Position multiplexing multiple-image encryption using cascaded phase-only masks in Fresnel transform domain”, Optics Communications, vol. 284, no. 18, pp. 4146-4151, 2011.

[11] H. T. Chang, H. E. Hwang, C. L. Lee, and M. T. Lee, “Wavelength multiplexing multiple-image encryption using cascaded phase-only masks in the Fresnel transform domain”, Applied optics, vol. 50, no. 5, pp. 710-716, 2011.

[12] N. K. Nishchal, and T. J. Naughton, “Flexible optical encryption with multiple users and multiple security levels”, Optics Communications, vol. 284, no. 3, pp. 735-739, 2011.

[13] E. Pérez-Cabré, M. Cho, and B. Javidi, “Information authentication using photon-counting double-random-phase encrypted images”, Optics letters, vol. 36, no. 1, pp. 22-24, 2011.

[14] A. Carnicer, and B. Javidi, “Optical security and authentication using nanoscale and thin-film structures”, Advances in Optics and Photonics, vol. 9, no. 2, pp. 218-256, 2017.

[15] H. Zhang, S. Zhang, and Y. Yin, “An improved ELM algorithm based on EM-ELM and ridge regression”, International Conference on Intelligent Science and Big Data Engineering, pp. 756-763, 2013.