WULFENIA JOURNAL KLAGENFURT, AUSTRIA ISSN:1561-882X

Vol 24, No. 6;Jun 2017

Hybrid Optical-Digital Information Encryption and Compression with Compressive Sensing

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

[1]*Lecturer, Department of Computer Science and Information System Engineering, Jazan University, Ministry of Higher Education, Jazan, Kingdom of Saudi Arabia.*

[2]*Associate Professor, Department of Electrical Engineering, Jodhpur National University, Jodhpur, Rajasthan, India.*

E-mail: [1]sivamalarphd@gmail.com, [2]er.swathi.sharma15@gmail.com

ABSTRACT

Mostly, optical images have been subjected to the different types of attacks during transmission. In previous optical encryption and compression researches both Chaotic Kicked Rotator Map- Double Random Phase Encoding (CKRMDRPE) and Direction-Adaptive Discrete Wavelet Transform Compression (DADWTC) techniques were simultaneously used for reducing the bandwidth during optical image transmission. However, this approach is mainly concerned with the optical image encryption and compression schemes not related to the digital image encryption. Hence in this paper, a simultaneous encryption and compression scheme is enhanced by using the hybrid optical image and digital information. In this approach, CKRMDRPE-DADWTC technique is further improved by introducing optical image encryption with digital information input and dynamic encryption key based on two Liquid Crystal (LC) light modulators (SLM). Therefore, the computation power for parallel optical processing is reduced by considering the significant amount of data during transmission. However, the efficiency of reconstructing the optical images from encrypted images is not improved. Hence, the proposed CKRMDRPE-DADWTC-LCSLM is further enhanced by applying Compressive Sensing (CS) scheme. Therefore, the reconstruction of encrypted optical images is improved by reducing the holograms data volume. Finally, the experimental results illustrate that the effectiveness of the proposed approach compared with the other techniques.

Keywords: Optical image encryption and compression, Chaotic Kicked Rotator Map with Double Random Phase Encoding, Direction-Adaptive Discrete Wavelet Transform Compression, Liquid crystal light modulators, Compressive sensing.

I. INTRODUCTION

Due to the rapid growth of modern communication techniques, both information security and intellectual property protection are considered as the great concern. This

has provided to extensive study of the data encryption, digital signature, authentication and watermarking techniques. The most attracted significant interest is optical encryption techniques since they recommend the possibility of high-speed parallel transmission of 2D image data and hiding information in multiple dimensions for preventing the optical images from attackers during transmission (Liu et al, 2014). Therefore, optical encryption techniques are used for providing better and safer image communication. The most common and fundamental optical encryption scheme in which multiplication of the image is done by random phase masks both in the space and Fourier domains. If two random phases are statistically independent white noises, then the encrypted image will be shown to be a stationary white noise (Thomas et al, 2014).

In addition, DRPE is proposed with Chaotic Baker Map (CBM) which is implemented in two layers for enhancing the security level of the conventional DRPE (Elshamy et al, 2013). The first layer is a pre-processing layer which is performed with the CBM on the original image. The conventional DRPE is utilized in the second layer. But, the CBM has low speed problem and number representation problems since the utilization of floating point values over the other number representations. To overcome these problems, Chaotic Kicked Rotator Map (CKRM) is applied instead of CBM for reducing the computation complexities and the speed problems by using the bit-wise representation of the numbers (Sivamalar et al, 2016a). Moreover, the encrypted optical images require high bandwidth for proper transmission. This issue is overcome by performing the compression of optical images with encryption simultaneously. Hence, the simultaneous encryption and compression of optical images is achieved by employing Direction-Adaptive Discrete Wavelet Transform Compression (DADWTC) with CKRMDRPE based encryption. This approach is called as CKRMDRPE-DADWTC which reduces the bandwidth and transmission rate (Sivamalar et al, 2016b). However, these approaches are mainly related to only optical image encryption and compression schemes not related to the digital image encryption and compression. In addition, these factors such as light intensity distribution and its phase distribution and speckle noise provide very poor decryption quality during optical implementations.

Hence in this article, optical image encryption with digital information scheme and dynamic encryption key is proposed based on two Liquid Crystal (LC) light modulators (SLM). This approach improves the decryption quality and also reduces the computation power for parallel optical processing by considering the significant number of data while transmission. However due to compression, good visual quality of decrypted images is corrupted by interference fringes which are amplified by decryption process. This degrades the reconstruction of the original optical images. Therefore, efficiency of reconstructing the optical images is improved by introducing the Compressive Sensing (CS) scheme. This approach is applied for improving the decrypted image quality by highly decreasing holograms data volume for optical

image encryption process. Thus, the optical image encryption and compression with digital information improves the security of the optical images during transmission.

The rest of the article is organized as follows: In Section 2, description of different optical encryption and compression schemes are given. In Section 3, detailed information of the proposed optical image encryption and compression with digital information based on LCSLM and CS schemes 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.

II. RELATED WORK

A novel image encryption algorithm (Lai et al, 2010) was proposed 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.

Optical encryption (Liu et al, 2013) was proposed based on the combination of image scrambling techniques in fractional Fourier domains. In this paper, information hiding was done in two-dimensional images using proposed algorithm. Initially, the image was randomly shifted by using the jigsaw transform algorithm. Then, a pixel scrambling technique was applied based on the Arnold Transform (ART). The scrambled image was then encrypted in a randomly selected fractional Fourier domain. After that, these processes were iteratively repeated. However, the decrypted image quality depends on the time period of ART and the iterative number.

Simultaneous optical image compression and encryption (Liu et al, 2015) was proposed by using error-reduction phase retrieval algorithm. In this paper, the original secret images were simultaneously compressed and encrypted into the real-valued ciphertext by two stages of phase retrieval processes. Two individual random phase keys were generated during the similar processes. The sizes of the ciphertext and keys were reduced which makes easier storage and transmission. The secret images to be processed were multiplexed as the input intensities of a cascaded diffractive optical system. At last, a compressed complex-valued data along with fewer measurements were obtained. However, the computation complexity depends on the number of iterations.

Photon-counting imaging based double random phase encryption (Perez-Cabre et al, 2011) was proposed 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.

Image compression and encryption scheme (Zhou et al, 2016) was proposed based on hyper-chaotic system and 2D compressive sensing. In this paper, initially the original image was measured based on the matrix measurements in two directions for achieving the compression and encryption simultaneously. Hyper-chaotic systems were used for generating chaotic sequences for image scrambling according to its randomness characteristic. Then, the resulting image was re-encrypted by the cycle shift operation controlled by the hyper-chaotic system. The cycle shift operation may modify the values of the pixels effectively. Thus, the proposed algorithm was used for reducing the costs for storage with acceptable security.

The multiple-image encryption technique (Kong et al, 2014) was proposed based on the Optical Wavelet Transform (OWT) and Multichannel Fractional Fourier Transform (MFrFT). In this method, the images may be decomposed into sub-images of different frequencies due to the properties of WY multi-resolution decomposition and the WT may focus the image's energy on the low-frequency parts. Hence, the low-frequency parts obtained by WT may be reassembled into an image. MFrFT was implemented through corresponding channels in the fractional domain encoding for different low-frequency parts. Finally, the encryption process was completed by using the random phase masks. Based on the reverse process, encrypted images were obtained.

The optical color-image encryption (Qin et al, 2016) was proposed based on the diffractive-imaging scheme. In this paper, the color image was separated into three channels such as red, green and blue for encryption. Then, these components were appended by the redundant data before being transmitted to the encryption process. The carefully designed optical setup which is comprised of three 4f optical architectures and a diffractive-imaging based optical scheme can encode the three plaintexts into the single noise-like intensity pattern. An iterative phase retrieval algorithm with a filter operation was applied for extracting the primary color images from the diffraction intensity map during decryption process.

Optical asymmetric image encryption (Mehra et al, 2015) was proposed by using Gyrator Wavelet Transform (GWT). In this paper, a gyrator wavelet transform was proposed for securing the phase image by using amplitude and phase-truncation approach. GWT has four basic parameters such as gyrator transform order, type and level of mother wavelet, and position of different frequency bands. The random phase

codes with the above parameters were acted as encryption keys. Thus, the GWT tool was used for simultaneous encryption and compression of an image.

The optical multi-image encryption (Liu et al, 2011) was proposed based on the frequency shift. In this paper, a novel multi-image encryption and decryption algorithm was proposed based on Fourier transform and fractional Fourier transform. Lower frequency parts of the original images were selected and the selected frequency was shifted. Then, double phase encoding in fractional Fourier domains were used for encrypting these shifted frequencies. Then, a single image was obtained by encrypting the combined multiple images. The proposed scheme has the features of enhancement in decryption accuracy and high optical efficiency.

The new spectral image compression method (Alfalou et al, 2010) was proposed based on the optimal phase coding and RMS duration principle. In this paper, the proposed new spectral lossy compression technique reduces the required memories and adaptively retrieve the original images by using only spectral phase information and increases the Peak-to-Correlation Energy (PCE) at the output of the correlator. The compression ratio of the proposed method was increased by introducing an optimal phase coding based on the fading grid. A variable number of quantization bits were used for quantizing phase information which is depending on the significance of the spectral phases. Moreover, the phase information can be classified based on the principle of RMS duration.

The numerical implementation of an optimized multiple image optical encryption and compression technique (Ouerhani et al, 2015) was presented. Initially, the double optimization process was introduced for spectrally multiplexing the multiple images. The new proposed method was a combination of spectral fusion based on the properties of Fourier Transform (FT), a specific spectral filtering and a quantization of the remaining encoded frequencies by using an optimal number of bits. The spectral plane was decomposed in different independent areas which are assigned based on the specific way. Moreover, each spectrum was shifted for minimizing the overlap. In addition, the second level of encryption was performed based on the real key image which is used for reinforcing the encryption.

A novel 1D hybrid chaotic map-based image compression and encryption (Zhang et al, 2016) was proposed using Compressed Sensing (CS) and Fibonacci-Lucas Transform (FLT). In this approach, the entire encryption process may be involved based on the different processes such as compression by CS, scrambling with FLT and diffusion after linear scaling. Bernoulli measurement matrix was generated due to better uniform distribution of the proposed scheme. The chaotic sequences were generated by varying the transform kernel of FLT in each permutation round which ensures the security and complexity.

III. PROPOSED METHODOLOGY

In this section, the proposed hybrid optical image encryption with digital information and compressive sensing scheme is explained in detail. The basic experimental setup of hybrid optical image encryption with digital information and dynamic encryption key based on two LCSLM is shown in figure 1.

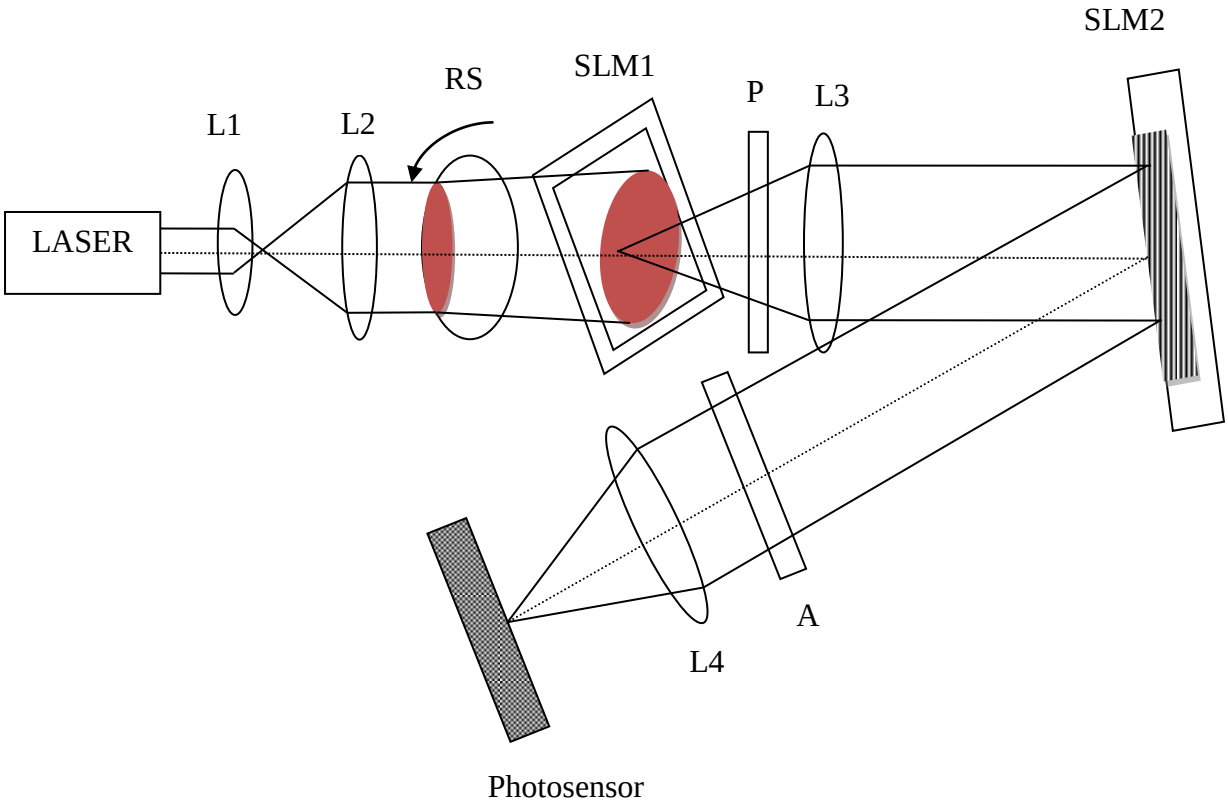


Figure.1. Process of Optical Image Encryption with Digital Information and Dynamic Encryption key based on Two LCSLM

In figure 1, linearly polarized laser radiation is expanded and collimated by two lenses such as L1 and L2. The spatial coherence is removed by rotating the scatter RS. Spatially incoherent monochromatic radiation illuminates SLM1 which is used for information input. The polarizer P selects the polarization for correct operation of SLM2. SLM1 and SLM2 are positioned in focal planes of lens L3. SLM2 is used for synthesized encryption Diffractive Optical Element (DOE) imaging. Reflected from SLM2 light passes through analyzer A. Lens L4 positioned so that when SLM2 is turned off and acts as a mirror, it forms of SLM1 on camera's photosensor. If DOE is imaged on SLM2 then optical convolution of SLM1 image and DOE Point Spread

Function (PSF) is formed in photosensor plane. This optical convolution is encrypted image. Two LCSLM are used for implementing dynamic digital information input and dynamic encryption key change.

Optical encryption in spatially incoherent light considers the additive noise which is given as follows:

$$g_i(x,y) = f(x,y) \otimes h(x,y) + n(x,y) \qquad (1)$$

In equation 1, g_i refers the registered light intensity distribution corresponding to encrypted image, f refers the light intensity distribution corresponding to the image to be encrypted, h denotes the DOE PSF, n is the additive noise and x, y are indexes' corresponding to the image pixels coordinates (Bondareva et al, 2015). This registered light intensity distribution is included with the CKRMDRPE method. Therefore, the encryption process can be represented as follows:

$$\psi_B(x,y) = FT^{-1}\left[FT\left(f_B(x,y)\varphi_n(x,y)\right) \cdot \varphi_m(\bar{p},\bar{q}) \cdot g_i(x,y)\right] \qquad (2)$$

For decryption process, it can be rewritten as,

$$FT^{-1}\left[FT\left(\psi_B(x,y)\right) \cdot \varphi_m^*(\bar{p},\bar{q}) \cdot g_i^*(x,y) \cdot y(x,y)\right] = f_B(x,y)\varphi_n(x,y)g_i(x,y) \qquad (3)$$

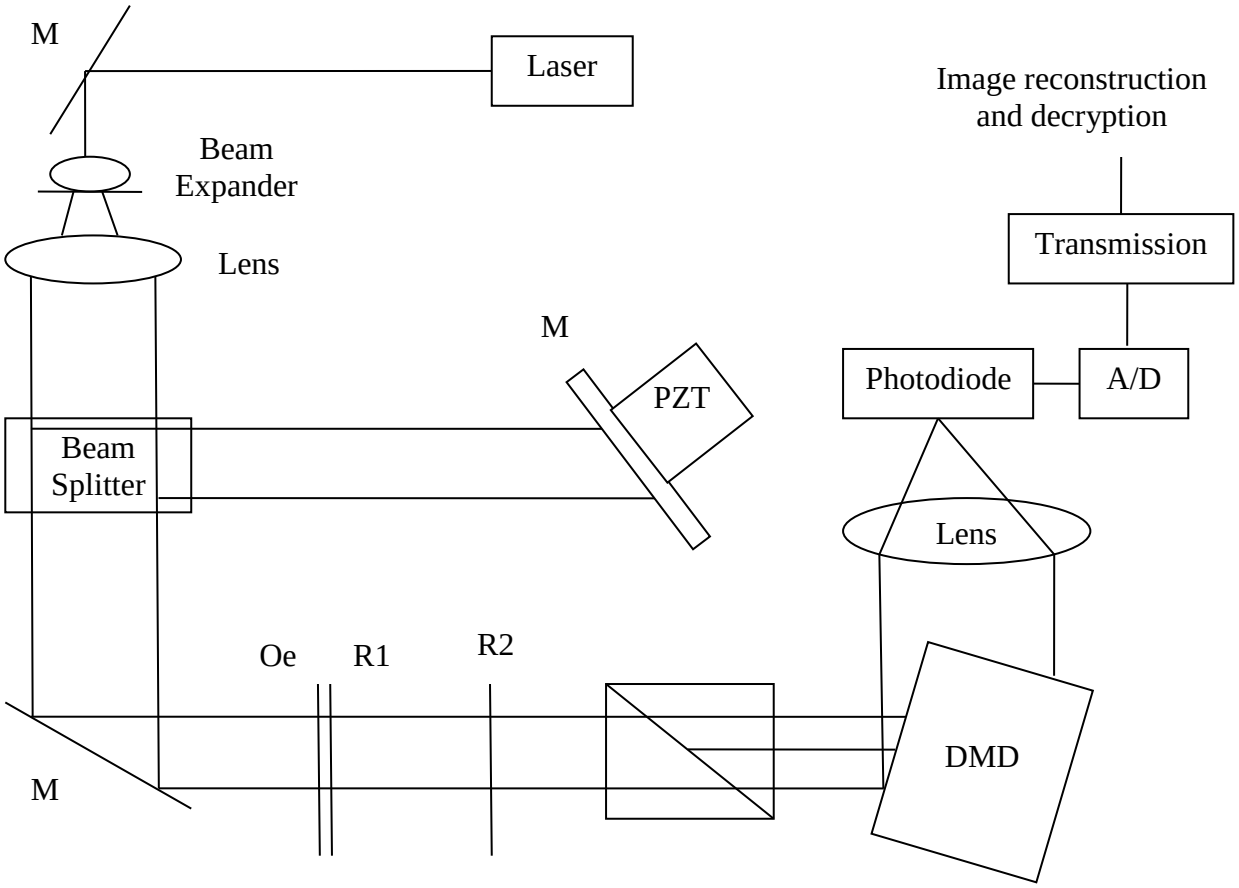
In equation 3, $y(x,y) = \frac{1}{H(x,y)}$ is called as the inverse decryption filter. Moreover, the decryption error values are evaluated as Normalized Root Mean Square (NRMS) between decrypted image and original image based on the threshold ε. The NRMS is equal to or less than the threshold value and is calculated as follows:

$$NRMS = \sqrt{\frac{\sum_{i=1}^{n}\sum_{j=1}^{n}|I_d(i,j)-I(i,j)|^2}{\sum_{i=1}^{n}\sum_{j=1}^{n}|I(i,j)|^2}} \qquad (4)$$

Where, $I_d(i,j)$ and $I(i,j)$ are the matrices with intensity values of the decrypted and original images respectively and i, j are discrete coordinates and $n = M \times N$ which refers the quantity of pixels of images. Simultaneously, DADWTC is performed for image compression based on the 2D DWT which consists of two processes. Initially, the 1D DWT is applied to the image followed by the vertical sub-sampling for obtaining the low-pass sub-band L and the high-pass sub-band H. Then, the other 1D DWT is applied to L and H, followed by horizontal sub-sampling for obtaining the LL, LH, HL and HH sub-band respectively. For image compression, the filtering directions in DADWTC must be selected for reducing the distortion of the reconstructed image.

Hence, the decryption of image is enhanced by introducing the two-step-only quadrature phase-shifting digital holography with compressive sensing approach.

Initially, an image is illuminated by the object beam, which is used for encryption. Then, it is passes through two random phase masks R_1 and R_2 for encrypting an image using DRPE method (Philippe et al, 1995). Alternatively, the phase of the reference wave is controlled by a Piezoelectric Transducer mirror (PZT). Then, the two waves overlap for generating an interference pattern in the plane of a Digital Micro-mirror Device (DMD). The random linear measurements of the interferograms I_H and the measurement matrix ψ are computed by using DMD. Then, the compressed data is obtained by using a photodiode. Finally, the compressed hologram images are acquired by the communication channel and reconstructed based on the CS algorithm. The original object is decrypted by using inverse-Fresnel-transformed with only two reconstructed holograms and the correct keys. The optical setup for an image encryption technique combined two-step-only quadrature phase-shifting digital holography with CS is shown in figure 2.



M: Mirror

Oe: Object Image

R: Random Phase Plate

DMD: Digital Micro-mirror Device

PZT: Piezoelectric Transducer mirror

A/D: Analog-to-Digital Converter

Figure.2. Optical Setup for an Image Encryption Method Combined Two-Step-Only Quadrature Phase-Shifting Digital Holography with CS

The reference wave is denoted as $R \cdot exp(j \cdot 0)$. The complex object filed $U(x, y)$ on the DMD plane which is expressed as follows,

$$U(x,y) = FR_{Z2}\{FR_{Z1}\{U(x_0,y_0)exp[i2\pi \cdot p(x_0,y_0)]\} \times exp[i2\pi \cdot q(x_1,y_1)]\} \quad (5)$$

In equation (5), $U(x_0, y_0)$ is the complex object field in the plane R_1 and FR_Z is the Fresnel transform of distance z. The complex amplitude transmittances of R_1 and R_2

are $exp[i2\pi \cdot p(x_0, y_0)]$ and $exp[i2\pi \cdot q(x_1, y_1)]$ respectively in which $p(x_0, y_0)$ and $q(x_1, y_1)$ are two independent white noises uniformly distributed in $[0,1]$. The distance between planes R_1 and R_2 is z_1 and the distance between R_2 and DMD is z_2. The two on-axis quadrature-phase holograms on the DMD plane are sampled sequentially by setting the phases of the reference wave in the first and second exposure to 0 and $\frac{\pi}{2}$.

$$I_{H1} = |R + U(x,y)|^2 = I_0(x,y) + 2Re[U(x,y)] \cdot R \quad (6)$$

$$I_{H2} = \left|R \cdot exp\left(i \cdot \frac{\pi}{2}\right) + U(x,y)\right|^2 = |jR + U(x,y)|^2$$

$$= I_0(x,y) + 2lm[U(x,y)] \cdot R \quad (7)$$

$$\text{Zero-order light, } I_0(x,y) = R^2 + |U(x,y)|^2 \quad (8)$$

The light reflected by the mirrors in direction towards lens is summed at the photodiode for computing the measurement as its output voltage (Li et al, 2015).

$$Y(m) = \{y_{1m}, y_{2m}\} = \Phi_m[I_{H1}, I_{H2}] \quad (9)$$

In equation (9), Φ_m refers m^{th} pseudo-random matrix on the DMD plane where $m = \{1,2, \dots, M\}$. The pseudo-random number is selected 0 or 1 randomly along with the user-defined numbers radial lines in the Fourier domain for producing the measurement matrix uploaded into the DMD device. The output value is given as,

$$Y = [y_1, y_2] = \psi[I_{H1}, I_{H2}] \quad (10)$$

$$[I_{H1}, I_{H2}] = \begin{bmatrix} I_{H11} & I_{H21} \\ I_{H12} & I_{H22} \\ \vdots & \vdots \\ I_{H1M} & I_{H2M} \end{bmatrix} \quad (11)$$

In above equations, I_{H1M} denotes the hologram I_{H1} in M^{th} measurement, $\psi \in R^{M \times \sqrt{N} \times \sqrt{N}}$ refers the measurement matrixes uploaded into the DMD device, $Y \in R^{M \times 2}$ refers the measurement data on the photodiode and $y_k \in R^{M \times 1}, I_{HK} \in R^{\sqrt{N} \times \sqrt{N} \times 1}, k = 1,2$. Therefore, the overall encryption process is expressed as follows:

$$\psi_B(x,y) = FT^{-1}\left[FT\left(f_B(x,y)\varphi_n(x,y)\right) \cdot \varphi_m(\bar{p}, \bar{q}) \cdot g_i(x,y) \cdot U(x,y)\right] \quad (12)$$

The optical signal is converted into the electrical signal by using a floating point type photodiode and the electrical signal is discretized to the digital signal through an Analog-to-Digital (AD) converter based on its quantization bits. Finally, these digital signals are transmitted through the communication channel to the computer in which the original image is reconstructed and decrypted.

3.1 Image reconstruction and decryption process: Initially, Two-step Iterative Shrinkage (TwIST) algorithm is applied for reconstructing the interference patterns $\hat{I}_{HK}$ on the DMD plane by solving the following optimization problem:

$$\min_{\hat{I}_{HK}} \frac{\mu}{2} \left\| Y_k - \psi \hat{I}_{HK} \right\|_2^2 + TV\left(\hat{I}_{HK}\right) \text{ Subjected to } Y_k = \psi I_{HK} \qquad (13)$$

In equation (13), $\left\| Y_k - \psi \hat{I}_{HK} \right\|_2^2$ refers the l_2 norm of $Y_k - \psi \hat{I}_{HK}$ and μ is a constant. The first penalty is a least-squares term which is small when $\hat{I}_{HK}$ is consistent with the correlation vector Y_k. The second penalty $TV\left(\hat{I}_{HK}\right)$ refers the signal's total variation which is given as,

$$TV\left(\hat{I}_{HK}\right) = \sum_{i,j} \sqrt{\left(\hat{I}_{HK(i+1)j} - \hat{I}_{HKi,j}\right)^2 + \left(\hat{I}_{HKi,j+1} - \hat{I}_{HKi,j}\right)^2} \qquad (14)$$

Where, indices i, j run over all pairs of adjacent pixels in $\hat{I}_{HK}$. An approximated TV is computed due to the non-differentiability of the Euclidean norm at the origin which is given as,

$$TV\left(\hat{I}_{HK}\right) = \sum_{i,j} \sqrt{\left(\hat{I}_{HK(i+1)j} - \hat{I}_{HKi,j}\right)^2 + \left(\hat{I}_{HKi,j+1} - \hat{I}_{HKi,j}\right)^2 + \xi^2} \qquad (15)$$

Here, ξ refers a small positive parameter. The intensity patterns $\hat{I}_{H1}$ and $\hat{I}_{H2}$ are obtained. Then, a parameter called 2D Correlation Coefficient (CC) is constructed as $CC = abs(E_T) \otimes abs(E)$, where $abs(.)$ denotes the amplitude of $(.)$, E_T refers the image decrypted by single hologram $\hat{I}_{H1}$ and the correct keys, E is the decrypted image at different amplitude values R_C of the reference light with two holograms $\hat{I}_{H1}$ and $\hat{I}_{H2}$ and the correct keys and $\otimes$ refers 2D correlation operation.

Then, the criterion is set such that the minimum point of the CC curve locates the actual amplitude value of the reference light. Therefore, the original image is reconstructed by using this obtained amplitude value of the reference wave as follows:

$$I_0 = \frac{2R_C^2 + \hat{I}_{H1} + \hat{I}_{H2}}{2} - \frac{\sqrt{\left(2R_C^2 + \hat{I}_{H1} + \hat{I}_{H2}\right) - 2\left(\hat{I}_{H1}^2 + \hat{I}_{H2}^2 + 4R_C^2\right)}}{2} \qquad (16)$$

In addition, the complex amplitude on the DMD plane is calculated as,

$$U(x, y) = \frac{(\hat{I}_{H1} - I_0) + (\hat{I}_{H2} - I_0)}{2R_C} \qquad (17)$$

After the complex amplitude $U(x,y)$ with the random phase masks R_1 and R_2, z_1, z_2 and λ are known, an original object image is digitally or optically reconstructed from the encrypted image as,

$$FT^{-1}\left[FT\left(\psi_B(x,y)\right)\cdot\varphi_m^*(\bar{p},\bar{q})\cdot g_i^*(x,y)\cdot y(x,y)\cdot O'(x,y)\right]= f_B(x,y)\varphi_n(x,y)g_i(x,y)U(x,y) \quad (18)$$

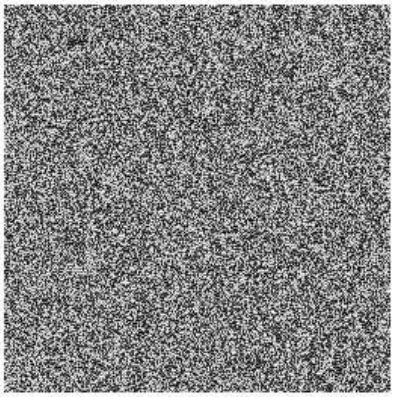
$$O'(x,y)=IFR_{Z1}\{IFR_{Z2}\{U(x,y)\}\times exp[-i2\pi\cdot q(x_1,y_1)]\times exp[-i2\pi\cdot p(x_0,y_0)]\} \quad (19)$$

In equation (19), IFR_Z refers the inverse Fresnel transformation of distance z. Thus, the original image is reconstructed and decrypted accurately.

IV. 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, LCSLM, CKRMDRPE-DADWTC-LCSLM, and CKRMDRPE-DADWTC-LCSLM-CS in terms of Maximum Deviation (MD) value, Correlation Coefficient (CC), Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR).

The optical image encrypted using CKRMDRPE-DADWTC, LCSLM, CKRMDRPE-DADWTC-LCSLM, and CKRMDRPE-DADWTC-LCSLM-CS are shown in figure 3.

Original Image	Encrypted Image Using
	

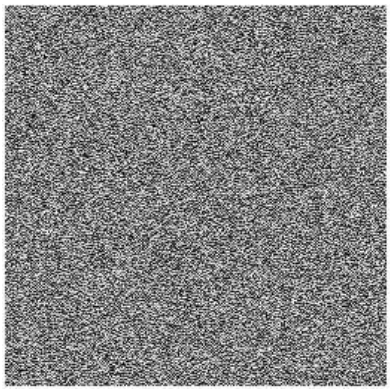
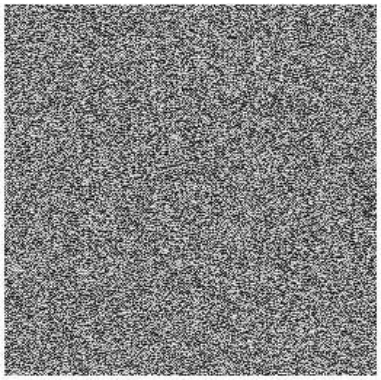
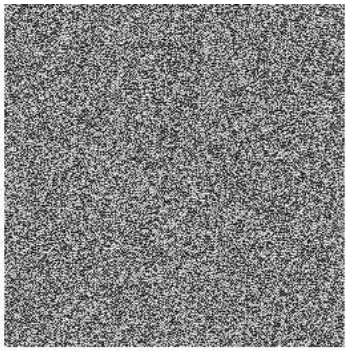
Encrypted Image Using LCSLM 	Encrypted Image Using 
Encrypted Image using CKRMDRPE- 	Reconstructed and Decrypted Image 

Figure.3. Original Image, Encrypted Images and Decrypted Image

4.1 Maximum Deviation (MD) value: The maximum deviation is used for measuring the quality of encryption in terms of how it maximizes the deviation between the original and encrypted images. The value of MD is computed as following steps:

1. Count the number of pixels for each gray-scale value in the range of 0 to 255 and present the results graphically for both original and encrypted images.
2. Determine the absolute difference or deviation between the two curves and represent it graphically.

3. Compute the area under the absolute difference curve which is the sum of deviation values.

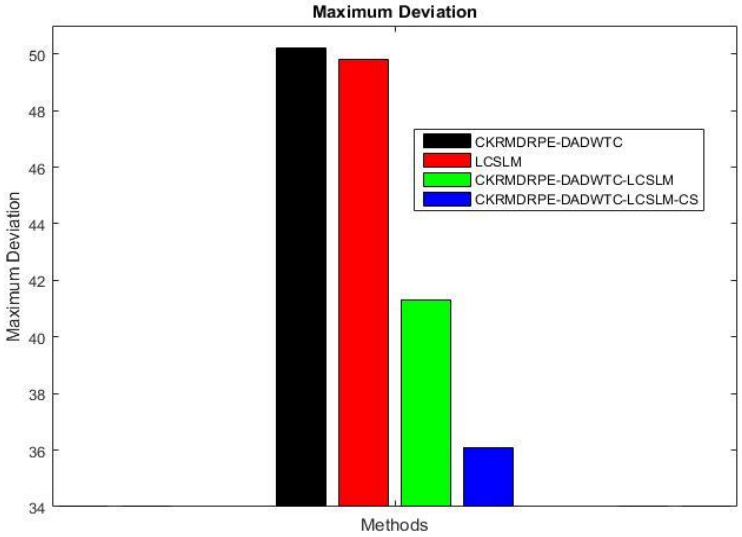


Figure.4. Maximum Deviation Analysis

Figure 4 shows that the comparison of CKRMDRPE-DADWTC-LCSLM-CS with the other techniques in terms of MD values. CKRMDRPE-DADWTC-LCSLM-CS has 36.1 whereas the other techniques have higher deviation values. Thus, it proves that the CKRMDRPE-DADWTC-LCSLM-CS provides better encryption with reduced deviation value.

4.2 Correlation Coefficient (CC): The CC between the original and encrypted images is used as a tool for evaluating the encryption quality. The CC is computed as follows:

$$r = \frac{cov(f,\psi)}{\sqrt{D(f)}\sqrt{D(\psi)}}$$

$$D(f) = 1/L \sum_{l=1}^{L} (f_l - E(f))^2$$

$$cov(f,\psi) = 1/L \sum_{l=1}^{L} (f_l - E(f)(\psi_t - E(\psi))$$

$$E(f) = 1/L \sum_{l=1}^{L} f_l$$

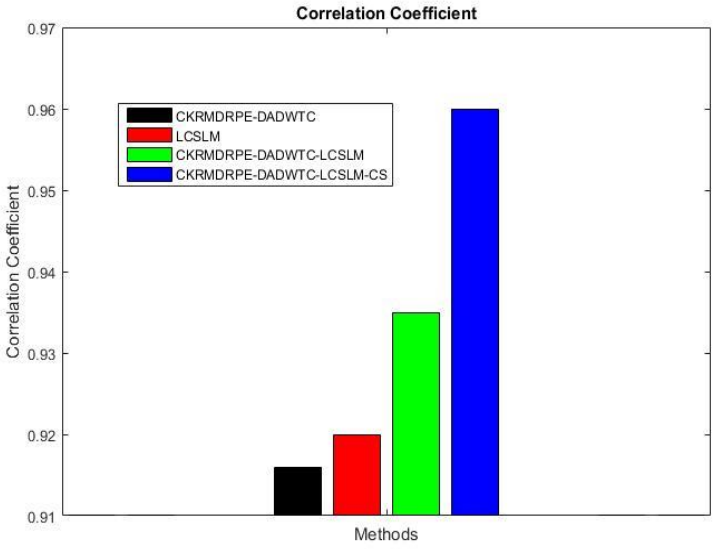


Figure.5. Correlation Coefficient

Figure 5 shows that the comparison of CKRMDRPE-DADWTC-LCSLM-CS with the other techniques in terms of CC values. CKRMDRPE-DADWTC-LCSLM-CS has 0.96 while the other techniques have less CC values. Thus, it proves that the CKRMDRPE-DADWTC-LCSLM-CS provides better encryption with increased correlation coefficient value.

4.3 Mean Square Error (MSE): Mean Square Error (MSE) is defined as the average of the squared error values between the actual and decrypted image values. MSE between the original and decrypted images is computed as,

$$MSE = \frac{1}{XY}\sum_{x=1}^{X}\sum_{y=1}^{Y}|f(x,y) - \hat{\mathrm{f}}(\mathrm{x},\mathrm{y})|^2$$

Here, X and Y are the image dimensions, $f(x,y)$ and $\hat{\mathrm{f}}(\mathrm{x},\mathrm{y})$ refers the original and decrypted images respectively.

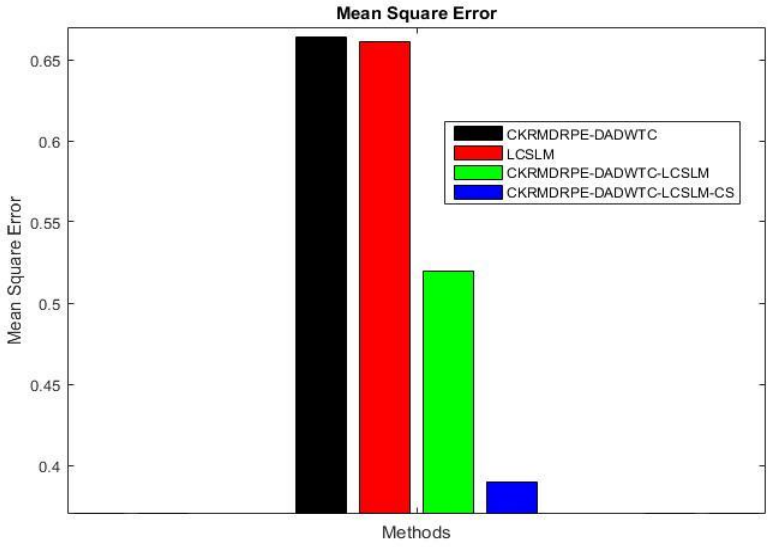


Figure.6. Mean Square Error

Figure 6 shows that the comparison of CKRMDRPE-DADWTC-LCSLM-CS with the other techniques in terms of MSE values. CKRMDRPE-DADWTC-LCSLM-CS has 0.39 whereas the other techniques have higher MSE values. Thus, it proves that the CKRMDRPE-DADWTC-LCSLM-CS provides better encryption with minimized MSE values.

4.4 Peak Signal-to-Noise Ratio (PSNR): Peak Signal-to-Noise Ratio (PSNR) is computed by using MSE value as follows:

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right)$$

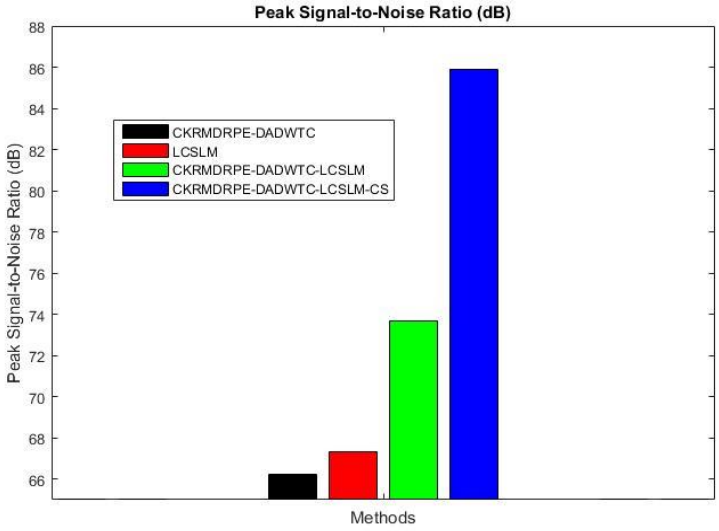


Figure.7. Peak Signal-to-Noise Ratio (dB)

Figure 7 shows that the comparison of CKRMDRPE-DADWTC-LCSLM-CS with the other techniques in terms of PSNR values. CKRMDRPE-DADWTC-LCSLM-CS has 85.91dB whereas the other techniques have less PSNR values. Thus, it proves that the CKRMDRPE-DADWTC-LCSLM-CS provides better encryption with maximized PSNR values.

V. CONCLUSION

In this paper, the simultaneous optical image encryption and compression technique for data security applications is enhanced with the digital information. A hybrid optical image encryption with digital information and compression technique is proposed by improving the CKRMDRPE-DADWTC technique. The proposed approach utilizes optical image with digital information for encryption by using the dynamic encryption key based on two LCSLM. This approach reduces the computation power for parallel process such as both encryption and compression simultaneously achieved by considering the reduced amount of data for transmission. Moreover, two-step-only quadrature phase-shifting digital holography based CS algorithm is applied for improving the quality of the reconstructed and decrypted image at the output end. This scheme reduces the holograms data volume for obtaining the reconstructed and decrypted original image accurately. The experimental results show that the proposed CKRMDRPE-DADWTC-LCSLM-CS has better effectiveness than the other encryption and compression schemes.

REFERENCES

Liu, S., Guo, C., & Sheridan, J. T. (2014). A review of optical image encryption techniques. *Optics & Laser Technology*, *57*, 327-342.

Thomas, D., & Prabu, T. (2014, April). Optical Image Encryption and Data Hiding using Double Random Phase Encoding and Advanced Encryption Standard on Chaotic Baker Mapped Image. *International Journal of Engineering Research and Technology*, *3*(4), 512-516.

Elshamy, A. M., Rashed, A. N., Mohamed, A. E. N. A., Faragalla, O. S., Mu, Y., Alshebeili, S. A., & El-Samie, F. A. (2013). Optical image encryption based on chaotic baker map and double random phase encoding. *Journal of Lightwave Technology*, *31*(15), 2533-2539.

Sivamalar, R., & Sharma, S. (2016). An optical image encryption using chaotic kicked rotator map with double random phase encoding. *International Journal of Applied Research in Science and Engineering*, 118-123.

Sivamalar, R., & Sharma, S. (2016). Simultaneous encryption and compression using chaotic kicked rotator map–drpe with direction adaptive discrete wavelet transform. *International Journal for Technological Research in Engineering*, 170-174.

Lai, J., Liang, S., & Cui, D. (2010, August). A novel image encryption algorithm based on fractional Fourier transform and chaotic system. In *Multimedia Communications (Mediacom), 2010 International Conference on (pp. 24-27).* IEEE.

Liu, S., & Sheridan, J. T. (2013). Optical encryption by combining image scrambling techniques in fractional Fourier domains. *Optics Communications*, *287*, 73-80.

Liu, W., Liu, Z., & Liu, S. (2015). Simultaneous optical image compression and encryption using error-reduction phase retrieval algorithm. *Journal of Optics*, *17*(12), 125701.

Pérez-Cabré, E., Abril, H. C., Millán, M. S., & Javidi, B. (2011, June). Photon-counting imaging based double-random-phase encryption for information security and verification. In *Information Optics (WIO), 2011 10th Euro-American Workshop on* (pp. 1-3). IEEE.

Zhou, N., Pan, S., Cheng, S., & Zhou, Z. (2016). Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing. *Optics & Laser Technology*, *82*, 121-133.

Kong, D., & Shen, X. (2014). Multiple-image encryption based on optical wavelet transform and multichannel fractional Fourier transform. *Optics & Laser Technology*, *57*, 343-349.

Qin, Y., Wang, Z., Pan, Q., & Gong, Q. (2016). Optical color-image encryption in the diffractive-imaging scheme. *Optics and Lasers in Engineering*, *77*, 191-202.

Mehra, I., & Nishchal, N. K. (2015). Optical asymmetric image encryption using gyrator wavelet transform. *Optics Communications*, *354*, 344-352.

Liu, Z., Zhang, Y., Zhao, H., Ahmad, M. A., & Liu, S. (2011). Optical multi-image encryption based on frequency shift. *Optik-International Journal for Light and Electron Optics*, *122*(11), 1010-1013.

Alfalou, A., Elbouz, M., Mansour, A., & Keryer, G. (2010). New spectral image compression method based on an optimal phase coding and the RMS duration principle. *Journal of Optics*, *12*(11), 115403.

Ouerhani, Y., Aldossari, M., Alfalou, A., & Brosseau, C. (2015, April). Numerical implementation of the multiple image optical compression and encryption technique. In *SPIE Defense+ Security* (pp. 94770M-94770M). International Society for Optics and Photonics.

Zhang, T., Li, S., Ge, R., Yuan, M., & Ma, Y. (2016). A Novel 1D Hybrid Chaotic Map-Based Image Compression and Encryption Using Compressed Sensing and Fibonacci-Lucas Transform. *Mathematical Problems in Engineering*, *2016*.

Bondareva, A. P., Cheremkhin, P. A., Evtikhiev, N. N., Krasnov, V. V., & Starikov, S. N. (2015). Scheme of Optical Image Encryption with Digital Information Input and Dynamic Encryption Key based on Two LC SLMs. *Physics Procedia*, *73*, 320-327.

Philippe, R., & Bahram, J. (1995). Optical image encryption using input plane and Fourier plane random encoding. In *Proceeding of SPIE* (Vol. 2565, pp. 767-769).

Li, J., Li, H., Li, J., Pan, Y., & Li, R. (2015). Compressive optical image encryption with two-step-only quadrature phase-shifting digital holography. *Optics Communications*, *344*, 166-171.