COMPARISON OF VARIOUS PROPOSED OPTICAL ENCRYPTION AND COMPRESSION TECHNIQUES

R.Sivamalar[1], Dr.Swati Sharma[2]
[1]Lecturer, Department of Computer Science and Information System, Jazan University, Ministry of Higher Education, Jazan, Kingdom of Saudi Arabia
[2]HOD, Associate Professor, Department of Electrical Engineering, Jodhpur National University, Jodhpur

Abstract: Optical encryption and compression techniques have considered as the most significant processes due to their high-speed parallel transmission capability by utilizing the data hiding methods which prevents the optical images from malicious attacks during transmission. Hence in the previous researches, various efficient optical image compression and encryption techniques are proposed for secured transmission in optical network. In this paper, the performance of the various proposed technique in the previous researches is analyzed. The comparison of CBRMDRPE, CKRMDRPE, CKRMDRPE-DADWTC, CKRMDRPE-DADWTC-LCSLM,CKRMDRPE-DADWTC-LCSLM-CS, and CKRMDRPE-DADWTC-LCSLM-CS-ENMF is evaluated based on performance metrics such as Maximum deviation, Correlation coefficient, Mean square error and Peak signal-to-noise ratio.

Keywords: Optical image Encryption and Compression, Chaotic Baker Map (CBM), Chaotic Kicked Rotator Map with Double Random Phase Encoding (CKRMDRPE), Direction-Adaptive Discrete Wavelet Transform compression (DADWTC), Liquid Crystal Spatial Light Modulator (LCSLM), Compressive Sensing (CS), Enhanced Non-Negative Matrix Factorization (ENMF).

I. INTRODUCTION

NOWADAYS, both information security and intellectual property protection are the great intentions due to the fast development of digital communication systems. Among the different data security and encryption algorithms, the optics-based devices have shown high security levels for resisting the possible intrusions from the data transmission through the various kinds of networks.

Optical information hiding techniques have received significant attention recently, because of their considerable potential advantages, such as their inherent capabilities for parallel ultra-fast processing, and the possibility of their applications in biometrics [1], optical security [2] and product authenticity verification [3]. Using these techniques, information can be hidden or secured in a large number of different kinds of dimensions offering many degrees of freedom. In 1995 Refregier and Javidi [2] proposed the double random phase encoding (DRPE) method to encode an amplitude image into a stationary white noise pattern. This includes multiplication of the image by random phase screens both in the input (space) and Fourier (spatial frequencies) planes. Fully phase-based encryption (PE) provides much better performance than linear amplitude-based (AE) encryption because of the secure properties of non linear PE [4]. Several other algorithms, for instance, digital optical stream cipher [5], optical XOR image encryption [6], and information encryption with phase-shifting interferometry [7], have yielded theoretical and experimental results that indicate a high level of security can be achieved by applying optically inspired hiding techniques.

Among different optical encryption schemes, Chaotic Baker Map with Double Random Phase Encoding (CBMDRPE) [8] is the mostly utilized for providing the optical security by using the double random phase masks in both space and Fourier domains. However, this approach has high computation complexity, low speed, and number representation issues due to the CBM method. Hence in the previous researches, an efficient optical image compression and encryption techniques are proposed for secured transmission in optical network.

Initially, Chaotic Kicked Rotator Map with Double Random Phase Encoding (CKRMDRPE) [9] technique is proposed for reducing the computation complexity and improving the performance speed by providing the bit-wise number representations. Then, the simultaneous compression and encryption approach such as Direction-Adaptive Discrete Wavelet Transform Compression with CKRMDRPE (CKRMDRPE-DADWTC) [10] is proposed for reducing the required bandwidth for transmitting the encrypted optical image. Moreover, the hybrid optical image encryption and compression with digital information is proposed based on the Liquid-Crystal light Modulators (CKRMDRPE-DADWTC-LCSLM) and Compressive Sensing method (CKRMDRPE-DADWTC-LCSLM-CS) for improving the reconstructed and decrypted image quality and reducing the computation power in terms of reducing the holograms data volume. In addition, a joint multiple-image multiplexing technique which utilizes an Enhanced Non-negative Matrix Factorization(CKRMDRPE-DADWTC-LCSLM-CS-ENMF) [11] is introduced for compressing and encrypting the multiple images simultaneously with high security. Furthermore, encoded optical images are classified by using Extreme Learning Machine (ELM) classifier for evaluating the effectiveness of the encoded mechanism. Also, ELM based classifier achieves less classification accuracy which proves that the proposed CKRMDRPE-DADWTC-LCSLM-CS-ENMF [12] has high level of security during optical image transmission. In this paper, the performance of the various proposed technique in the previous researches is

analyzed. The comparison of CBRMDRPE, CKRMDRPE, CKRMDRPE-DADWTC,CKRMDRPE-DADWTC-LCSLM, CKRMDRPE-DADWTC-LCSLM-CS, and CKRMDRPE-DADWTC-LCSLM-CS-ENMF is evaluated based on performance metrics such as Maximum deviation, Correlation coefficient, Mean square error and Peak signal-to-noise ratio.

II. RELATED WORKS

A novel image encryption algorithm was proposed (Lai, J., et al. 2010) [13] 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.

An optical encryption technique was proposed (Liu, S., & Sheridan, J. T. 2013) [14] 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.

A photon-counting imaging based double random phase encryption was proposed (Perez-Cabre, E., et al. 2011) [15] 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.

The wavelength and position multiplexing multiple-image encryption was proposed (Chang, H. T., et al. 2011) [16] [17] 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. 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.

An optical image security method was proposed (Rajput, S. K., et al. 2014)[18] 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.

III. REVIEW OF OUR PREVIOUS PROPOSED RESEARCH

3.1 An Optical Image Encryption using Chaotic Kicked Rotator Map with Double Random Phase Encoding

In the optical image encryption based on Chaotic Baker Map (CBM) and Double Random Phase Encoding (DRPE), two-layers were implemented for improving the security level of the transmission. The first layer was a pre-processing layer which is performed with the CBM on the actual image. In the second layer, DRPE was used. However, the computational complexity and number representation issues have been addressed due to the usage of floating point values over the other number representations. Hence in this research, these issues are overcome by introducing the Chaotic Kicked Rotator Map (CKRM) based DRPE approach. In the proposed technique, CKRM is replaced instead of the CBM method for reducing the computation complexities and number representation issues by using the bit-wise representation of the numbers. This approach is not affected by the known-plaintext attack which ensures better encryption process. Thus, the proposed CKRMDRPE approach reduces the computation complexity of the optical image encryption process.

3.2 Simultaneous Encryption and Compression using Chaotic Kicked Rotator Map-DRPE with Direction Adaptive Discrete Wavelet Transform

In CKRMDRPE approach, CKRM is used instead of CBM method for optical image encryption in order to reduce the computation complexity and avoid number representation problem. However, the proper transmission of encrypted optical image requires higher bandwidth. Hence in this research, the simultaneous optical image encryption and compression is introduced. In this approach, Direction-

Adaptive Discrete Wavelet Transform Compression (DADWTC) is employed with CKRMDRPE based encryption. This method is called as CKRMDRPE-DADWTC. An optical image is encrypted by using CKRMDRPE whereas simultaneously compressed by DADWTC approach which reduces the bandwidth for achieving the proper transmission. Thus, the proposed CKRMDRPE-DADWTC approach reduces the required bandwidth for transmitting the encrypted optical image using compression technique.

3.3 Hybrid Optical-Digital Information Encryption and Compression with Compressive Sensing

In CKRMDRPE-DADWTC approach, an optical image is simultaneously encrypted and compressed for achieving proper transmission by reducing the required bandwidth. However, this approach is used only the optical images and not related to the digital image encryption and compression. Moreover, the factors such as light intensity distribution and its phase distribution and speckle noise may degrade the decrypted and reconstructed optical image quality. Hence in this paper, hybrid optical image encryption and compression with digital information is proposed. This approach is proposed based on the two Liquid Crystal (LC) light modulators (SLM) (Bondareva, A. P., et al. 2015) [19]. The proposed CKRMDRPE-DADWTC-LCSLM 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 (Li, J., et al. 2015) [20]. This approach is applied for improving the decrypted image quality by highly decreasing holograms data volume for optical image encryption process. Thus, the proposed CKRMDRPE-DADWTC-LCSLM-CS improves the security of the optical images during transmission.

3.4 An Enhancement on Hybrid Optical-Digital Information Encryption and Compression for Multiple Image Encryptions

In CKRMDRPE-DADWTC-LCSLM-CS approach, two Liquid Crystal (LC) light modulators (SLM) and Compressive Sensing (CS) scheme are proposed for improving the security of the optical images and quality of the decrypted and reconstructed the actual optical images. However, this approach was not used for simultaneous encryption and compression using multiple images. Hence in this phase of the research, CKRMDRPE-DADWTC-LCSLM-CS approach is improved in order to utilize the multiple images for encryption and compression. A joint multiple-image multiplexing method (Takeda, M., et al. 2015) [21] is proposed with the simultaneous encryption and compression in which an Enhanced Non-negative Matrix Factorization (ENMF) is applied (Gong, L., & Nandi, A. K. 2013) [22] with the digital holography approach. In this approach, a number of images are transformed into the noise-like digital holograms which are decomposed into the defined number of basis images and the corresponding weighting matrix based on the ENMF method. Then, the encryption and compression are performed for improving the security of the data. Thus, the proposed CKRMDRPE-DADWTC-LCSLM-CS-ENMF approach provides high-level of security by performing multiple-image encryption and compression successfully.

3.5 An Evaluation of Security Level of Hybrid Optical-Digital Information Encryption and Compression of Optical Images

The above proposed approaches are used for improving the security level of optical images during transmission based on the compression, encryption and multiplexing techniques. 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 research, an Extreme Learning Machine (ELM) based classification is proposed for evaluating the encoded performance of the optical images by using the different approaches such as CKRMDRPE-DADWTC, CKRMDRPE-DADWTC-LCSLM, CKRMDRPE-DADWTC-LCSLM-CS, and CKRMDRPE-DADWTC-LCSLM-CS-ENMF. The main aim of this proposed classification technique is to develop an optical system which has the highest-level of optical security with high complexity for identifying the encoded images. Initially, the polarized light is used for illuminating the proposed system and the double random phase mask is used for encoding the optical image effectively (Carnicer, A., &Javidi, B. 2017) [23]. Then, the encoded optical image classification is achieved based on the Extreme Learning Machine (ELM) classifier with the help of training dataset (Zhang, H., et al. 2013) [24]. Thus, the proposed ELM classifier improves the multiple security levels of the optical image transmission efficiently.

IV. EXPERIMENTAL RESULTS

In this section, the performance of the proposed technique is analyzed. In performance evaluation, two optical images such as A and B are taken. The images A and B are given as input to the encryption and image compression algorithms. The comparison of CBRMDRPE, CKRMDRPE, CKRMDRPE-DADWTC,CKRMDRPE-DADWTC-LCSLM, CKRMDRPE-DADWTC-LCSLM-CS, and CKRMDRPE-DADWTC-LCSLM-CS-ENMF is evaluated based on performance metrics such as Maximum deviation, Correlation coefficient, Mean square error and Peak signal-to-noise ratio.

The optical image encrypted using the above mentioned methods are shown below Figure 4.1

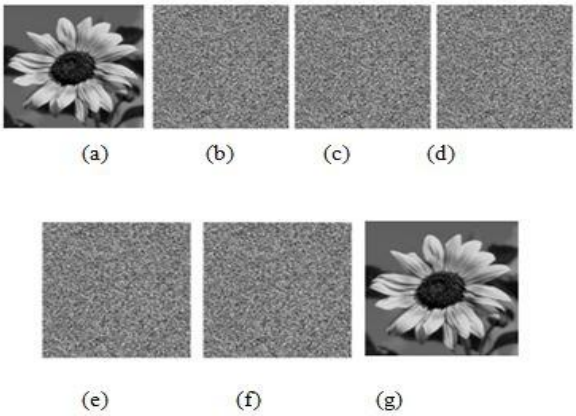

Figure 4.1. Sunflower image (a) Original Image (b) CKRMDRPE Encryped image (c) CKRMDRPE-DADWTC Encrypted image
(d) CKRMDRPE-DADWTC-LCSLM Encrypted image
(e) CKRMDRPE-DADWTC-LCSLM--CS Encrypted image
(f) CKRMDRPE-DADWTC-LCSLM-CS-ENMF Encrypted image (g) Decrypted and Reconstructed Image

4.1 Maximum Deviation Analysis

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:

- 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.
- Determine the absolute difference or deviation between the two curves and represent it graphically.
- Compute the area under the absolute difference curve which is the sum of deviation values.

The comparison of maximum deviation values are given in Table 4.1.

	CBM DRPE	CKRM DRPE	CKRMDRPE-DADWTC	CKRMDRPE-DADWTC-LCSLM	CKRMDRPE-DADWTC-LCSLM-CS	CKRMDRPE-DADWTC-LCSLM-CS-ENMF
Maximum Deviation Value	60	50.2	41.3	36.1	28.6	20.9

Table.4.1. Comparison of Maximum Deviation Analysis

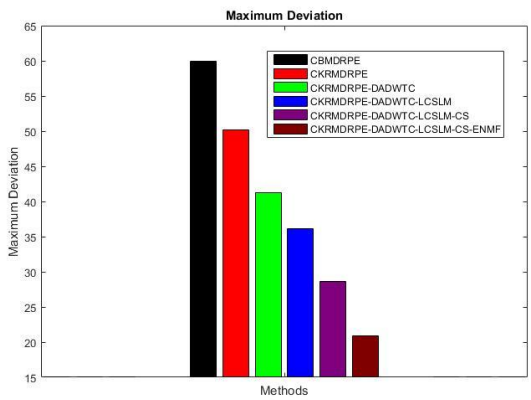

Figure.4.2. Maximum Deviation Analysis

Figure 4.2 shows that the comparison of CKRMDRPE-DADWTC-LCSLM-CS-ENMF with the other techniques in terms of MD values. CKRMDRPE-DADWTC-LCSLM-CS-ENMF has 20.9 whereas the other techniques have higher deviation values. Thus, it proves that the CKRMDRPE-DADWTC-LCSLM-CS-ENMF provides better encryption with reduced deviation value.

4.2 Correlation Coefficient Analysis

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

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

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

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

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

The comparison of correlation coefficient values are given in Table 4.2.

	CBM DRPE	CKRM DRPE	CKRMDRPE-DADWTC	CKRMDRPE-DADWTC-LCSLM	CKRMDRPE-DADWTC-LCSLM-CS	CKRMDRPE-DADWTC-LCSLM-CS-ENMF
Correlation Coefficient Value	0.8	0.92	0.935	0.96	0.971	0.985

Table.4.2. Comparison of Correlation Coefficient

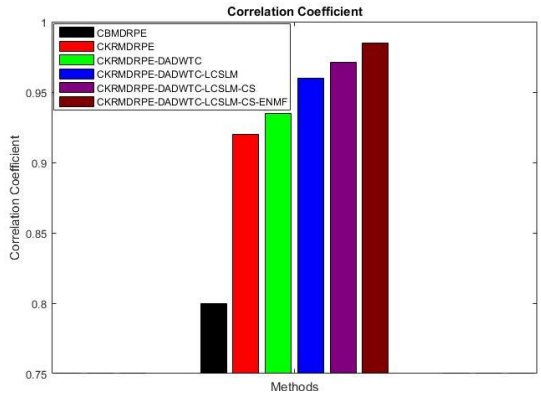

Figure.4.3. Correlation Coefficient Analysis

Figure 4.3 shows that the comparison of CKRMDRPE-DADWTC-LCSLM-CS-ENMF with the other techniques in terms of CC values. CKRMDRPE-DADWTC-LCSLM-CS has 0.985 while the other techniques have less CC values. Thus, it proves that the CKRMDRPE-DADWTC-LCSLM-CS-ENMF provides better encryption with increased correlation coefficient value.

4.3 Mean Square Error Analysis

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,

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

Here, X and Y are the image dimensions, $f(x,y)$ and $\hat{f}(x,y)$ refers the original and decrypted images respectively. The comparison of mean square error values are given in Table 4.3.

	CBM DRPE	CKRM DRPE	CKRMDRPE-DADWTC	CKRMDRPE-DADWTC-LCSLM	CKRMDRPE-DADWTC-LCSLM-CS	CKRMDRPE-DADWTC-LCSLM-CS-ENMF
Mean Square Error Value	0.7	0.664	0.52	0.39	0.352	0.279

Table.4.3. Comparison of Mean Square Error

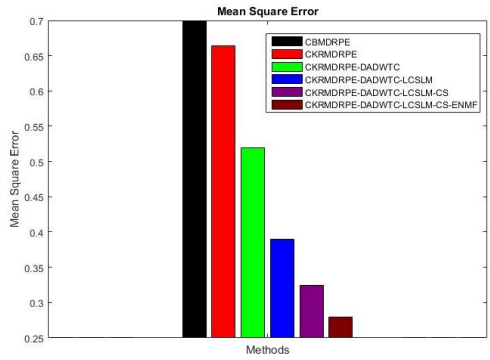

Figure.4.4. Mean Square Error Analysis

Figure 4.4 shows that the comparison of CKRMDRPE-DADWTC-LCSLM-CS-ENMF with the other techniques in terms of MSE values. CKRMDRPE-DADWTC-LCSLM-CS-ENMF has 0.279 whereas the other techniques have higher MSE values. Thus, it proves that the CKRMDRPE-DADWTC-LCSLM-CS-ENMF provides better encryption with minimized MSE values.

4.4 Peak Signal-To-Noise Ratio Analysis

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

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

The comparison of PSNR values are given in Table 4.4.

	CBM DRPE	CKRM DRPE	CKRMDRPE-DADWTC	CKRMDRPE-DADWTC-LCSLM	CKRMDRPE-DADWTC-LCSLM-CS	CKRMDRPE-DADWTC-LCSLM-CS-ENMF
PSNR	59	66.22	73.69	85.91	90.3	96.8

Table.4.4. Comparison of Peak Signal-to-Noise Ratio

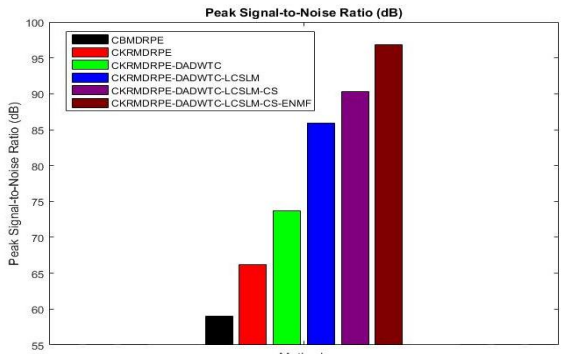

Figure.4.5. Peak Signal-to-Noise Ratio

Figure 4.5 shows that the comparison of CKRMDRPE-DADWTC-LCSLM-CS-ENMF with the other techniques in terms of PSNR values. CKRMDRPE-DADWTC-LCSLM-CS-ENMF has 96.8dB whereas the other techniques have less PSNR values. Thus, it proves that the CKRMDRPE-DADWTC-LCSLM-CS-ENMF provides better encryption with maximized PSNR values.

V. CONCLUSION

In this paper, the performance of the proposed technique is analyzed. The comparison of CBRMDRPE, CKRMDRPE, CKRMDRPE-DADWTC, CKRMDRPE-DADWTC-LCSLM, CKRMDRPE-DADWTC-LCSLM-CS, and CKRMDRPE-DADWTC-LCSLM-CS-ENMF is evaluated based on performance metrics such as Maximum deviation, Correlation coefficient, Mean square error and Peak signal-to-noise ratio. The experimental results show that the proposed CKRMDRPE-DADWTC-LCSLM-CS-ENMF approach has better effectiveness which reduces the computation complexity compared with the other techniques.

REFERENCES

[1] B. Javidi, A. Sergent, Optical Engineering 36 (3) (1997) 935.
[2] P. Refregier, B. Javidi, Optics Letters 20 (7) (1995) 767.
[3] B. Javidi, E. Ahouzi, Applied Optics 37 (26) (1998) 6247.
[4] N. Towghi, B. Javidi, Z. Luo, Journal of the Optical Society of America A 16 (8) (1999) 1915.
[5] M. Madjarova, M. Kakuta, M. Yamaguchi, N. Ohyama, Optics Letters 22 (21) (1997) 1624.
[6] J.W. Han, C.S. Park, D.H. Ryu, E.S. Kim, Optical Engineering 38 (1999) 47.
[7] E. Tajahuerce, O.Matoba, S.C. Verrall, B. Javidi, Applied Optics 39 (14) (2000) 2313.
[8] Ahmed M. Elshamy, Ahmed N. Z. Rashed, Abd El-Naser A. Mohamed, Osama S. Faragalla, Yi Mu, Saleh A. Alshebeili, and F. E. Abd El-Samie, "Optical Image Encryption Based on Chaotic BakerMap and Double Random Phase Encoding", vol 31, August 2013
[9] 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.
[10] 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.
[11] R. Sivamalar& Dr. Swati Sharma (2017) "An Evaluation of Security Level of Hybrid Optical-Digital Information Encryption and Compression of Optical Images" International Journal of Modern

Trends in Engineering and Science"

[12] R. Sivamalar& Dr. Swati Sharma (2017) "An Enhancement on Hybrid Optical-Digital Information Encryption ad Compression for Multiple Image Encryption" International Journal of Recent Scientific Research, 17414-17420

[13] 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.

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

[15] 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.

[16] Chang, H. T., Hwang, H. E., & Lee, C. L. (2011). Position multiplexing multiple-image encryption using cascaded phase-only masks in Fresnel transform domain. Optics Communications, 284(18), 4146-4151.

[17] Chang, H. T., Hwang, H. E., Lee, C. L., & Lee, M. T. (2011). Wavelength multiplexing multiple-image encryption using cascaded phase-only masks in the Fresnel transform domain. Applied optics, 50(5), 710-716.

[18] Rajput, S. K., Kumar, D., &Nishchal, N. K. (2014). Photon counting imaging and polarized light encoding for secure image verification and hologram watermarking. Journal of Optics, 16(12), 125406.

[19] 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.

[20] 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

[21] Takeda, M., Nakano, K., Suzuki, H., & Yamaguchi, M. (2015). Encrypted sensing based on digital holography for fingerprint images. Optics and Photonics Journal, 5(01), 6.

[22] Gong, L., & Nandi, A. K. (2013, September). An enhanced initialization method for non-negative matrix factorization. In Machine Learning for Signal Processing (MLSP), 2013 IEEE International Workshop on (pp. 1-6). IEEE

[23] Carnicer, A., &Javidi, B. (2017). Optical security and authentication using nanoscale and thin-film structures. Advances in Optics and Photonics, 9(2), 218-256.

[24] Zhang, H., Zhang, S., & Yin, Y. (2013, July). An improved ELM algorithm based on EM-ELM and ridge regression. In International Conference on Intelligent Science and Big Data Engineering (pp. 756-763). Springer Berlin Heidelberg.

