ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 8, Issue, 6, pp. 17414-17420, June, 2017

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

AN ENHANCEMENT ON HYBRID OPTICAL-DIGITAL INFORMATION ENCRYPTION AND COMPRESSION FOR MULTIPLE IMAGE ENCRYPTIONS

***Sivamalar, R[1] and Swati Sharma[2]**

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

[2]Department of Electrical Engineering, Jodhpur National University, Jodhpur, Rajasthan, India

DOI: http://dx.doi.org/10.24327/ijrsr.2017.0806.0349

ARTICLE INFO

Article History:

Received 17th March, 2017
Received in revised form 21th April, 2017
Accepted 28th May, 2017
Published online 28th June, 2017

Key Words:

Optical image encryption and compression, Compressive sensing, Multiplexing, CKRMDRPE-DADWTC-LCSLM-CS, Enhanced Non-negative Matrix Factorization.

ABSTRACT

Due to the rapid growth of data security applications, optical image with digital information encryption and compression techniques have been developed for improving the data security during transmission. In previous researches, hybrid optical image encryption with digital information named CKRMDRPE-DADWTC-LCSLM-CS was proposed based on the Compressive Sensing (CS) approach and Liquid Crystal Light Modulators (LCSLM). This approach improves the security and quality of the reconstructed and decrypted image at the end of the process. However, this approach was not used for simultaneous encryption and compression using multiple images. Hence in this paper, CKRMDRPE-DADWTC-LCSLM-CS approach is improved in order to utilize the multiple images for encryption and compression. A joint multiple-image multiplexing method is proposed with the simultaneous encryption and compression in which an Enhanced Non-negative Matrix Factorization (ENMF) is applied 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. Finally, the experimental results show that the proposed approach provides high-level of security by performing multiple-image encryption and compression successfully.

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. The inherent diversity of optical signals and the high precision requirement in optical devices significantly enhance the system security levels (Javidi *et al,* 2016). In addition, different computer algorithms have been developed for different types of optical systems for enabling the encryption, and compression on the high-dimensional signals ((Sivamalar and Sharma, 2016). Hence, the modern optical systems have better security for image communication.

In CKRMDRPE-DADWTC-LCSLM-CS, both optical image and digital information are utilized for encryption based on the dynamic encryption key by using two LCSLM. In addition, two-step-only quadrature phase-shifting digital holography based CS algorithm is introduced for enhancing the quality of the reconstructed and decrypted image after the transmission. This approach improves the parallel process simultaneously by reducing the computational power and holograms data volume effectively. However, this approach uses only one image at the time of transmission and not developed for using multiple image transmission with encryption and compression. The transmission of the multiple images is the most concern with the encryption and compression techniques which are performed based on the multiplexing scheme.

In this research, a joint multiple-image multiplexing technique is introduced in order to enhance the CKRMDRPE-DADWTC-LCSLM-CS approach. In the proposed approach, both Non-negative Matrix Factorization (NMF) and digital holography are applied for multiplexing technique. Initially, a number of images are converted into the noise-like digital holograms. These are then decomposed into the defined number of basis images and corresponding weighting matrix by using NMF

Corresponding author:* **Sivamalar, R
Department of Computer Science and Information System Engineering, Jazan University, Ministry of Higher Education, Jazan, Kingdom of Saudi Arabia

method. The determined basis images are stored as the encrypted data and served as a lock in an encryption system based on CKRMDRPE-DADWTC-LCSLM-CS. Alternatively, the column vectors in the weighting matrix are served as the keys for the corresponding addresses of the multiplexed images. However, the computation complexity of the NMF method is high due to its iteration process and PSNR degradation is also negligible in the reconstructed images. Hence, NMF is further enhanced by using k-means clustering algorithm for initializing the NMF factors randomly. Therefore, this approach reduces the computation complexity and improves the PSNR value significantly.

The rest of the article is organized as follows: In Section 2, description of different optical encryption, compression and multiplexing schemes are given. In Section 3, detailed information of the proposed hybrid encryption and compression with multiplexing scheme 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.

Related Work

Liu, W., *et al.* proposed the simultaneous optical image compression and encryption by utilizing the error-reduction phase retrieval algorithm. In this proposed approach, the actual secret images were compressed and encrypted simultaneously into the real-valued ciphertext by two phases of phase retrieval approach. During this processes, two individual random phase keys were generated and the size of the ciphertext keys were minimized for providing simple storage and transmission. The secret images which are being processed were multiplexed as the input intensities of a cascaded diffractive optical system. Finally, a compressed complex-valued data with fewer measurements were attained. However, the computation complexity of the approach was depending on the number of iterations.

Liu, Z., *et al.* proposed the optical multi-image encryption according to the frequency shift. In this proposed method, a novel multi-image encryption and decryption algorithm was introduced by using Fourier transform and fractional Fourier transform. Lower frequency parts of the actual images were chosen and then shift operation was performed for the selected frequencies. After that, these shifted frequencies were encrypted based on the double phase encoding in fractional Fourier domains. Here, multiple images were encrypted together as a single image. Thus, this approach achieves decryption accuracy and high optical efficiency.

Chang, H. T., *et al.* proposed the position and 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. 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.

Hwang, H. E., *et al.* proposed the lensless optical data embedding system by using concealogram and cascaded digital Fresnel hologram. In this paper, a robust lensless optical data embedding was proposed based on the both computer-generated concealogram and the Digital Fresnel Hologram (DFH). The concealogram and DFH were cascaded as the input and filter planes respectively. The hidden data was extracted at the output plane without using any lenses while the concealogram was illuminated by the plane wave. The longitudinal positions of the filter and the output planes along with the wavelength were used as the secret keys for enhancing the system security. Moreover, the robustness of the proposed system was also illustrated against noise and distortion.

Liu, S., & Sheridan, J. T. proposed the optical encryption according to the combination of image scrambling techniques in fractional Fourier domains. In this paper, information hiding was performed in the two-dimensional images by using the proposed algorithm. Initially, the image was shifted randomly based on the jigsaw transform algorithm. After that, a pixel scrambling technique was introduced according to the Arnold Transform (ART). Then, the scrambled image was encrypted in a randomly chosen fractional Fourier domain. These processes were repeated iteratively for achieving better solution. However, the quality of the decrypted image was depending on the time duration of ART and the number of iteration steps.

Deepan, B., *et al.* proposed a novel multiple-image encryption and decryption technique. In this paper, a space multiplexing was proposed based on the Compressive Sensing (CS) with the Double Random Phase Encryption (DRPE). The space multiplexing approach was employed for integrating the multiple-image data. Initially, the images were compressed to a smaller signal in the sparse domain and the sampled signals of all images were integrated into the single encrypted signal. The integrated cipher text was further encrypted by using DRPE method. The CS technique and space multiplexing techniques were used for providing the additional key space in the proposed method. The binary masks were used in the decryption process for separating each image data after DRPE decryption which is followed by CS reconstruction for obtaining the original image information.

Gong, Q., *et al.* proposed the multiple-image encryption and authentication with the sparse representation by space multiplexing. In this approach, the redundant spaces in the sparse representation strategy were optimized. The sparse data of multiple encrypted images were extracted with the help of the Random Binary Amplitude Masks (RBAM) and then integrated into the synthesized ciphertext with space multiplexing. Here, both the random phase masks and the RBAM were required for authentication. Moreover, the robustness of the proposed system was also illustrated against noise and distortion.

MATERIALS AND METHODS

In this section, the proposed Enhanced Non-negative Matrix Factorization (ENMF) is explained in which the digital holography is adopted on the plain images and the noise-like hologram images are obtained as the training images in the

ENMF method. The determined basis images are also noise-like and thus any information of the original images cannot be identified from the silhouettes in the basis images. After that, the weighting factors in each row of the determined weighting matrix W may serve as the secret key for the corresponding image. All r weighting factors related to this specific image are required for accurately recovering one of the n plain images. Otherwise, the reconstructed and decrypted image will be distorted. The detailed ENMF based multiplexing is described as follows.

Consider a plain image $g_p(x,y)$ using CKRMDRPE-DADWTC-LCSLM-CS technique for encryption and compression. In the encryption phase, each plain image is embedded into a larger size of black background image for successfully retrieving the plain images from the digital hologram (Chang *et al.* 2017, Takeda *et al.* 2015). Digital hologram is used for converting the plain images into the digital holograms which is shown in figure 1.

For a given non-negative matrix V with n rows and m columns, the ENMF is used for finding the non-negative factors such as W and H such that,

$$V_{n\times m} = W_{n\times r}H_{r\times m},\ r < (nm)/(n+m) \quad (4)$$

The values of W and H are obtained based on the multiplication update rule by minimizing an objective function such as root-mean-squared residual D.

$$D = \sqrt{\frac{\sum_{j=1}^{n}\sum_{i=1}^{m}(V_{ij}-(WH)_{ij})^2}{m\times n}} \quad (5)$$

Where $H \leftarrow H\frac{W^TV}{W^TWH}$ and $W \leftarrow W\frac{VH^T}{WHH^T}$

The factor W is initiated by using k-means clustering algorithm [14, 15] and then the initial factor H is calculated using the following initialization method.

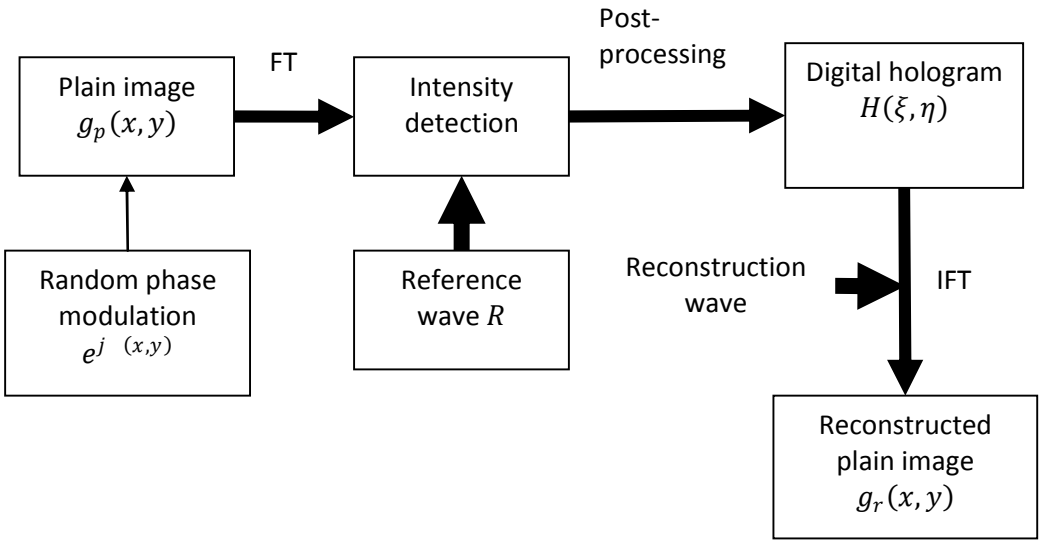

Figure 1 Generation of Digital Hologram $H(\xi,\eta)$

The digital hologram is represented as follows:

$$H(\xi,\eta) = G_p(\xi,\eta)R(\xi,\eta) + G_p(\xi,\eta)R\ (\xi,\eta) \quad (1)$$

In equation (1), $H(\xi,\eta)$ refers the digital hologram which is decomposed by using the ENMF method. Also, $G_p(\xi,\eta)$ refers the Fourier transform of the plain image and $R(\xi,\eta)$ denotes the Fourier transform of the plain image which is interfere with the reference wave R.

$$G_p(\xi,\eta) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} g_p(x,y)exp[j2\pi\ (x,y)]exp[\ j2\pi(\xi x + \eta y)]dxdy \quad (2)$$

$$R(\xi,\eta) = R_0 exp[j2\pi(a\xi + b\eta)] \quad (3)$$

In equation (2) and (3), (x,y) is the random number within the range $[0,1]$, a and b are the parameters used for determining the location of the plain image at the reconstruction plane in which the plain images can be extracted. After that, the extended image is recorded as a digital hologram with the parameters a and b used in the reference wave. Once a plain image is converted into the digital holograms, the training matrix V is obtained which is composed of all digital holograms.

The initial basis matrix W is constructed by using the cluster centroids which are obtained by k-means clustering algorithm. Then the membership degrees of each data point are calculated by using the results from k-means clustering as follows:

$$_{kq} = \frac{1}{\sum_{k'=1}^{k}\left(\frac{d(x_q,c_{k'})}{d(x_q,c_k)}\right)^{\frac{2}{1-m}}} \quad (6)$$

In equation (6), $d(\ )$ is the Euclidean distance between the two points, x_q is q^{th} data point and c_k is k^{th} cluster centroid. Also, m refers the fuzzification parameter which is set to 2. Then, the initial matrix H is obtained by using the membership degrees.

With the iteration process in ENMF method, the corresponding basis images and weighting factor matrices are obtained. The matrices H and W are served as the lock and keys in the security system respectively. The weighting coefficients for each key are uniformly distributed in the ENMF method. Thus, the security level is improved by using the proposed ENMF which is applied onto the digital holograms. Therefore, the overall encryption process is denoted as follows based on CKRMDRPE-DADWTC-LCSLM-CS approach.

$$\psi_B(x,y) = FT^{-1}\left[FT\left(f_B(x,y)\varphi_n(x,y)\right)\ \ \varphi_m(\bar{p},\bar{q})\ \ g_i(x,y)\ \ G_p(\xi,\eta)\right] \quad (7)$$

During decryption phase inverse Fourier transform is applied directly on the hologram and all the coefficients in the weighting matrix and the holographic parameters such as a and b should be correct. Moreover, the overall decryption process is represented as,

$$g_r(x,y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} H(\xi,\eta)exp[j2\pi(\xi x+\eta y)]d\xi d\eta \quad (9)$$

Hence, the proposed approach is used for increasing the uniformity of the coefficients in the weighting matrix and also improving the sensitivity on coefficient variation which enhances the security level.

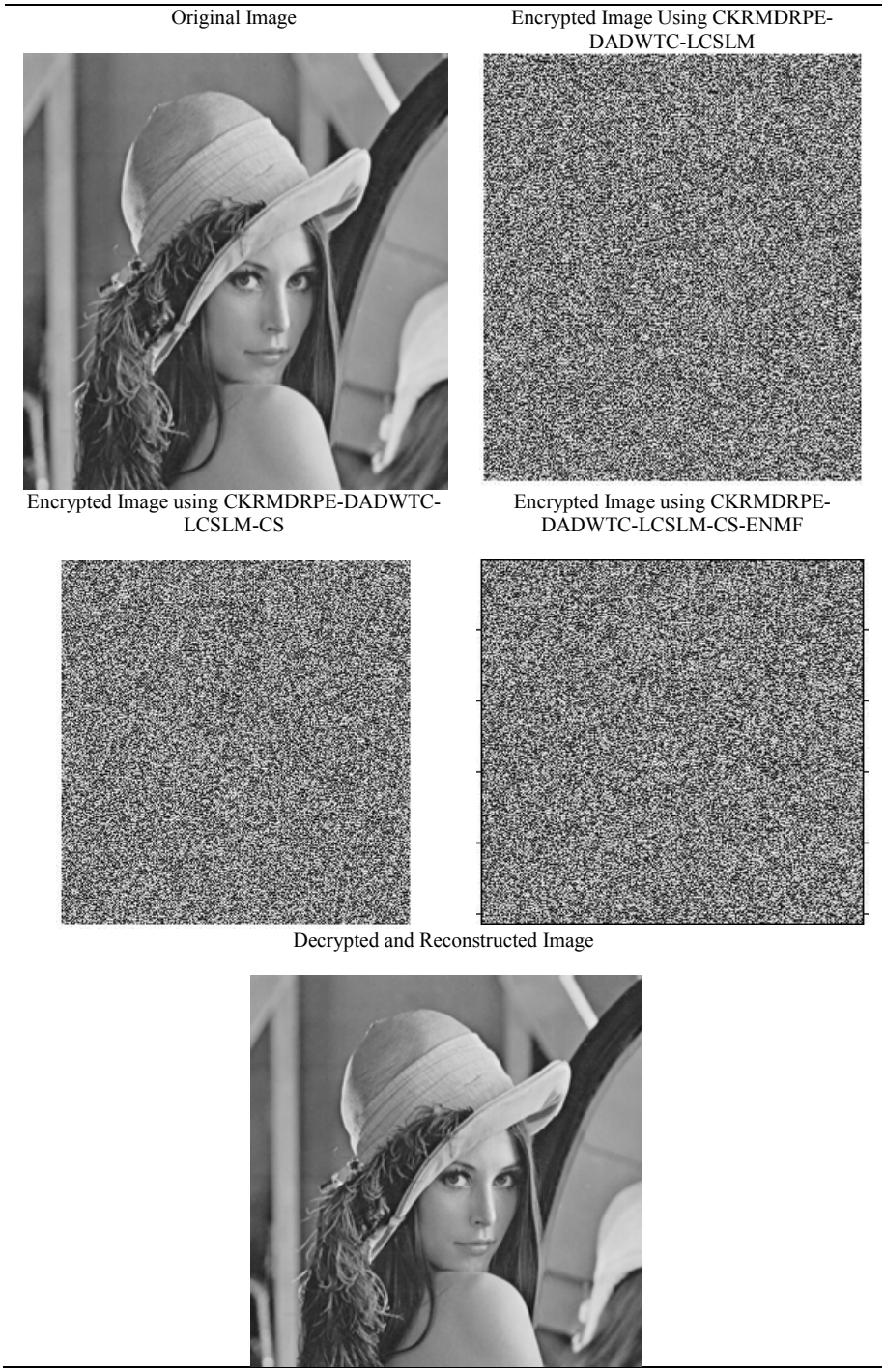

Figure 2 Original Image, Encrypted Images and Decrypted Image

$$FT^{-1}\left[FT\left(\psi_B(x,y)\right)\ \ \varphi_m(\bar{p},\bar{q})\ \ g_i(x,y)\ \ y(x,y)\ \ H(\xi,\eta)\right] = f_B(x,y)\varphi_n(x,y)g_i(x,y)g_r(x,y) \quad (8)$$

In equation (8), $g_r(x,y)$ is the wave disturbance at the reconstruction plane which is given as,

(ENMF)

Input: Non-negative matrix, $V_{n\times m}$
Output: Basis matrix W and Initial matrix H

- For a given non-negative matrix $V_{n\times m}$ and its pseudo-inverse X, do

- Apply k-means clustering on the matrix $V_{n\times m}$
- Generate the cluster centroids $C_i\ (i = 1,2,\dots,k)$ // k refers the reduced dimensionality which may be set to any value
- Construct the basis matrix of NMF W by inversing the cluster centroids as C_i^T
- Obtain the initial matrix H by using membership degrees which is calculated as

$$_{kq} = \frac{1}{\left[\sum_{k'=1}^{k}\left(\frac{d(x_q, c_{k'})}{d(x_q, c_k)}\right)^{\frac{2}{1-m}}\right]}$$

- Repeat the process until obtain the final results

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-CS, and CKRMDRPE-DADWTC-LCSLM-CS-ENMF in terms of Maximum Deviation (MD) value, Correlation Coefficient (CC), Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The optical encrypted images using CKRMDRPE-DADWTC-LCSLM, CKRMDRPE-DADWTC-LCSLM-CS, and CKRMDRPE-DADWTC-LCSLM-CS-ENMF are shown in figure 2.

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.

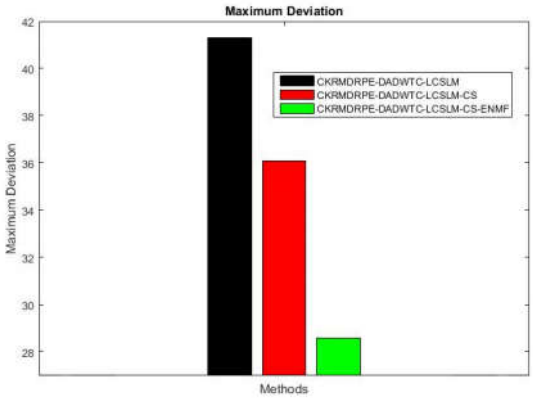

Figure 3 Maximum Deviation Analysis

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 3 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 28.6 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.

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:

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

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

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

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

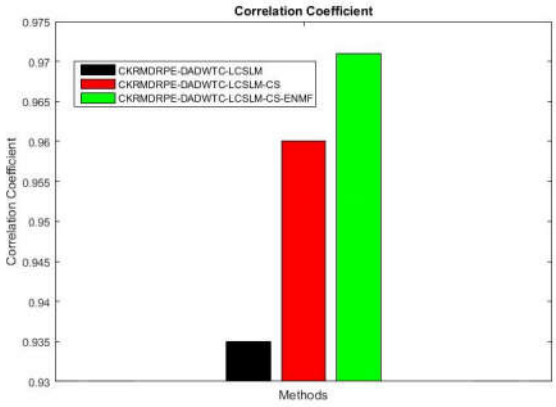

Figure 4 Correlation Coefficient

Figure 4 shows that the comparison of CKRMDRPE-DADWTC-LCSLM-CS-ENMF with the other techniques in terms of CC values. CKRMDRPE-DADWTC-LCSLM-CS has 0.971 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.

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,

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

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

Figure 5 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 0.325 whereas the other techniques have higher MSE values.

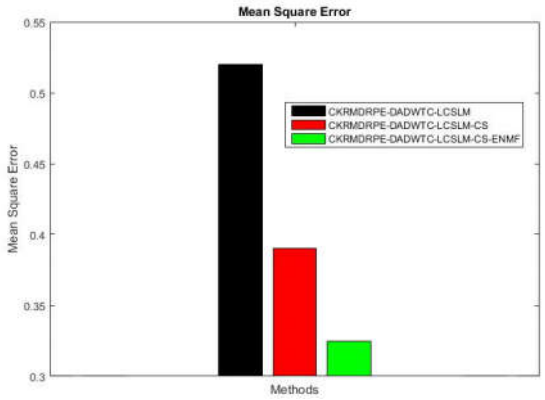

Figure 5 Mean Square Error

Thus, it proves that the CKRMDRPE-DADWTC-LCSLM-CS-ENMF provides better encryption with minimized MSE values.

Peak Signal-to-Noise Ratio (PSNR)

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

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

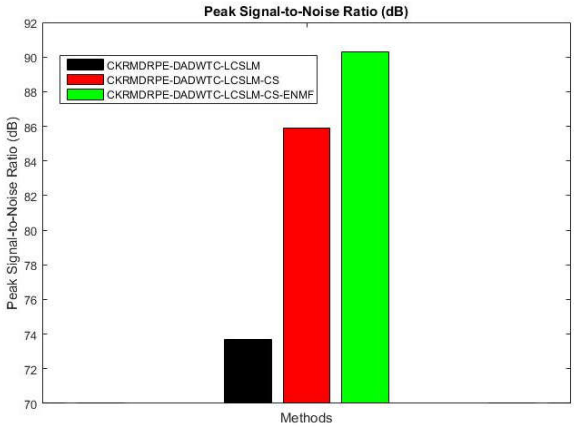

Figure 6 Peak Signal-to-Noise Ratio (dB)

Figure 6 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 90.3dB 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.

CONCLUSION

In this paper, the simultaneous hybrid optical image encryption and compression is proposed with multiplexing scheme in order to use the multiple images. In this approach, a joint multiple-image multiplexing method is introduced with the encryption and compression during multiple optical image transmission. The proposed approach utilizes the ENMF scheme which is applied with the digital holography method. Initially, the plain images are converted into the noise-like digital hologram which is used for obtaining the basis images and corresponding weighting matrix by using ENMF. Then, the obtained basis images are encrypted with high security level. To decrypt and reconstruct the original plain images, the parameters used in digital holography and weighting factors are required for improving the PSNR value and quality of the reconstructed and decrypted images. The experimental results show that the proposed approach has better effectiveness which reduces the computation complexity compared with the other techniques.

References

Javidi, B., Carnicer, A., Yamaguchi, M., Nomura, T., Pérez-Cabré, E., Millán, M. S., & Peng, X. (2016). Roadmap on optical security. *Journal of Optics*, 18(8), 083001.

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.

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.

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 Optic*s, 122(11), 1010-1013.

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.

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.

Hwang, H. E., Chang, H. T., & Lie, W. N. (2011). Lensless optical data embedding system using concealogram and cascaded digital Fresnel hologram. *JOSA* A, 28(7), 1453-1461.

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

Deepan, B., Quan, C., Wang, Y., & Tay, C. J. (2014). Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique. *Applied optics*, 53(20), 4539-4547.

Gong, Q., Liu, X., Li, G., & Qin, Y. (2013). Multiple-image encryption and authentication with sparse representation by space multiplexing. *Applied optics*, 52(31), 7486-7493.

Chang, H. T., Shui, J. W., & Lin, K. P. (2017). Image multiplexing and encryption using the nonnegative matrix factorization method adopting digital holography. *Applied Optics*, 56(4), 958-966.

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.

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.

Wang, W. (2010, April). An improved non-negative matrix factorization algorithm for combining multiple clusterings. In Machine Vision and Human-Machine Interface (MVHI), 2010 International Conference on (pp. 604-607). IEEE.

How to cite this article:

Sivamalar, R and Swati Sharma.2017, An Enhancement on Hybrid Optical-Digital Information Encryption and Compression For Multiple Image Encryptions. *Int J Recent Sci Res.* 8(6), pp. 17414-17420. DOI: http://dx.doi.org/10.24327/ijrsr.2017.0806.0349

****