A Survey on Various Optical Image Encryption Techniques

R.Sivamalar [1], Mitesh Sharma [2]

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

Department of Computer Science, JIET, Jodhpur, Rajasthan, India.Designation

sivamalar.jazan@gmail.com mail2miteshsharma@gmail.com

Abstract—

Objective: To analysis different techniques for optical image encryption and decryption to improve the security level of system.

Findings: Nowadays optical techniques play an important role in various fields pay TV, medical or biometric, confidential video conferencing over optical fiber, military applications, police identification procedures, online banking systems, governmental services, identity (ID) cards, etc used optical images. So it is more important to provide security for transmission and storage of images. During transmission of images encryption is a well suited method for providing security for images. There are various techniques were proposed for optical image encryption. This paper provides detailed information about various optical image encryption techniques.

Results: In this paper various optical image encryption techniques are compared through parameters to prove Double Random Phase Encoding (DRPE) and chaotic Baker map is better than other techniques.

Application/Improvements: The findings of this work prove that the Double Random Phase Encoding (DRPE) and chaotic Baker map provides better result than other approaches.

Keywords: Double Random Phase Encoding, optical image encryption, chaotic Baker map, optical image decryption.

I. Introduction

OPTICAL image processing techniques are widely used for information security. The optical image encryption technique is used in optical information processing field. The images are protected into two different ways. One is watermarking technology another one is encryption technology [1]. The encrypted image is in the form of non- identifiable by the hackers. Most of all techniques based optical architectural implementations for image encryption have been proposed for its high parallelism, high speed, and multi-parameter selection [2] in different applications.

Many techniques such as key rotation multiplexing method, lensless multiple image optical encryption, optical asymmetric crypotosystem, structured-illumination-based lensless diffractive imaging, modified Gerchberg–Saxton algorithm were extensively benefits from optical image encryption. In this paper various optical image encryption techniques were analyzed through the parameters like correlation coefficient, Mean square error and peak signal to noise ratio.

Survey:

Yong-Liang, X., et al [3] presented a technique in Fresnel domain for the encryption of multiple image called key rotation multiplexing method into double random phase encoding system. In this technique each and every plaintext was encoded by the similar phase mask situated in an input plane that produced stationary white-noise cipher text. Thus the phase mask was allowed to revolve a key in a particular angle. From the rotation of key cipher text was created for each plaintext and finally all cipher text were added to get a final cipher text that act as single source for decryption. However, the rotation multiplexing is limited to binary images for encryption.

Huang, J., et al [4] proposed a technique called lensless multiple image optical encryption for optical multiple image encryption. This technique is based on image encryption based on the modified Gerchberg–Saxton algorithm. This proposed technique cross talk between the decrypted images was completely discarded by a traditional architecture called two phase adjacent phase only functions (POF) in the domain of Fresnel transform. The images are encrypted individually in POF through the MGSA then the images are decrypted with the help of multiple position parameters in Fresnel transform domain, wavelength and the created POFs. Thus the system security was improved and it also achieved unlimited capacity. However this technique is not a straight forward method.

Pan, W., & Qiao, J., [5] introduced a technique for optical image encryption and decryption. In this technique the input image is divided into two equal parts of image. One part of the encryption key is used to encrypt another part of the image. One part of the divided image is encrypted using double random phase optical encryption system and it produced a cipher text that is transformed as a key by two phase masks. It can be done by double random phase optical iterative encryption and non linear transformation technique. Thus this technique prevents the phase retrieval attack.

Chen, W., & Chen, X., [6] introduced an optical asymmetric crypotosystem for the purpose of optical color image encryption. It can be achieved through the phase-truncated strategy in the Fresnel domain. Based on phase-truncated strategy indexed image methods and multiple wave length were extended. This technique is more efficient and more effective for color image encryption.

Chen, W., & Chen, X., [7] introduced a method structured-illumination-based lensless diffractive imaging for optical image encryption. The proposed method utilized grating pitches of images and charge-coupled device is utilized to store the sequentially varied phase grating image.

Moreover a high quality images in the stored images were extracted by phase retrieval algorithm through the rapid convergence rate. Thus the proposed method recovered the object information in stored grating images (diffraction patterns). It is used in the Fresnel domain for optical image encryption. However, the proposed method provides huge key space for optical image encryption.

Hwang, H., [8] proposed a technique to encode a color image that is based on modified Gerchberg–Saxton algorithm (MGSA) in the Fresnel-transform (FrT) domain. In this proposed technique a color image is encode and it created three phase functions. It was created for three various channels like red, green and blue. Thus the encoded three channels discarded the cross talk. The decryption process is carried over with the help of three POFs in the encryption process and adding the decrypted red, green and blue images. These images are decrypted one after the other. Thus the security of the system is enhanced by creation of key using system parameters and three POFs.

Zhang, Y., & Xiao, D., [9] created we design a novel discrete fractional random transform based on 2D chaotic logistic maps and two chaotic random masks. Two chaotic random masks was created from Chirikov standard map. Then the double optimal images are encrypted using chaos-based discrete fractional random transform and the discrete Chirikov standard map. The proposed discrete Chirikov standard map was utilized to mess up pixels of two optical images because of the images property of area preserving. Thus the two messed images are considered as phase and amplitude of the input signal and the discrete Chirikov standard map and chaos-based discrete fractional random transform is used for complete encryption. The keys of the proposed optical image encryption technique is depends on the initial values of chaotic maps.

Liu, J., et al [10] proposed computer generated hologram (CGH) and chaotic theory for the purpose of optical color image encryption and decryption. The input color image is modified into three different components are red, green and blue. Then the modified images were modulated using various random phase arrays were developed by an efficient sequence called chaotic sequence. Then Brunch's coding method is utilized to fabricate CGH as the encryption image and the reconstruction of original is continued until get an correct system parameters and initial value of chaotic function.

Zhou, N., et al [11] proposed an optimal image encryption technique that is based on fractional Mellin transform. This proposed approach encrypts the image as a non linear system. The original image with center and geometric center are converted to fractional Mellin transform with various orders. Then the complex valued images are encrypted using fractional Mellin transform that converts the complex valued images into single cipher text. This technique provides more security to the system.

Singh, N., & Sinha, A., [12] introduced approach based on improper Hartley transform and chaos theory for optical image encryption. The encryption of an image is created using Hartley transform and chaos theory in this technique. Hartley transform is evaluated by fractional multiple of $\pi/2$ of Fourier transform and it is act as key in the process of encryption and decryption. Chaos theory used the tent map, Ikeda map, logistic map and Ikeda map for the creation of random intensity maks.

Li, X., & Zhao, D., [13] proposed a method based on 2 dimensional fractional Hartley transform for optical color image encryption. In this method a input image is divided as three monochromatic color images are red, green and blue and the divided image is encrypted independently based on various wavelengths. Then the images are encrypted and decrypted based on random phase mask and fractional Hartley transform are used as keys.

Lin, C., et al [14] introduced reference waves with various random amplitude masks and incident angles into Fourier transform hologram configuration for the purpose of multiple image encryption. To encrypt an optical image the random amplitude masks were located in the reference arm at vertical position. Thus the security of optical image is increased such as that the original image decrypted only after knowing the reference wave along with the incident angle used in encryption.

Liu, X., et al [15] proposed a method based on compressed sensing and Arnold transformation for the purpose of optical image encryption. The input digital image was encrypted and compressed based on the features of compressed sensing, dimension reduction and random projection. Then the encrypted image was mess up by Arnold transformation and then the encrypted image was encrypted one more time with the help of double random phase encoding optical encryption technique. Finally the keys were created by two random phase masks with the sequence of irrational number and it is integrated and transmitted.

Barrera, J. F., & Torroba, R., [16] proposed free propogation scheme for optical image encryption. In this approach multiplexing encryption operation is performed to avoid any sequential objects positioning procedure. This encryption doesn't need any step up alterations and the decoded images are recovered in their original images. The security is increased by replacing random phase masks technique to free propagation technique.

Elshamy, A. M., et al [17] proposed a optical image encryption technique based on chaotic Baker map and Double Random Phase Encoding (DRPE). To achieve a high level of security DRPE with chaoticmap pre-processing is processed at two layers. The preprocessing is carried over in first layer that is processed along with the chaotic Baker map. Then in the second layer DRPE is used to improve the security level. Thus this technique achieves high performance and it provides good diffusion and permutation mechanisms.

Table 1. Comparison of optical image encryption techniques

Ref. No	Title	Parameters Used
3	Key rotation multiplexing for multiple-image optical encryption in the Fresnel domain	Correlation coefficient(-0.5 degree rotation) For 128 level key = 0.4 32 level key = 0.4 4 level key = 0.38 2 level key = 0.35
4	Optical multiple-image encryption based on phase encoding algorithm in the Fresnel transform domain	Correlation coefficient At -2 target image = 0.2 For 100 gray images = 0.9999
5	An Iterative Optical Image Encryption Based on Double Random Phase	Correlation coefficient Violence attack = 0.00037 known-plaintext attack = 0.00188 chosen-plaintext attack = 0.00453
6	Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain	Correlation coefficient Red channel = 0.3450 Green channel = 0.3723 Blue channel = 0.4253
7	Structured-illumination-based lensless diffractive imaging and its application to optical image encryption	Correlation coefficient In 2 iterations = 0.962 In 10 iterations = 0.986
8	Optical color image encryption based on the wavelength multiplexing using cascaded phase-only masks in Fresnel transform domain	Correlation coefficient (distance) Red =0.1 m Green = 0.128 Blue = 0.161m
9	Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform	Self correlation coefficient Horizontal peppers = 0.9506 Lena = 0.9807 Encrypted image = 0.0117
10	Optical color image encryption based on computer generated hologram and chaotic theory	Mean Square Error 50% occlusion R(%) = 14.85, B(%) = 16.24 G(%) = 13.39 Additive noise R(%) = 12.71, B(%) = 14.19 G(%) = 11.48
11	Novel optical image encryption scheme based on fractional Mellin transform	Correlation coefficient Original image Horizontal = 0.9613 Encrypted image Horizontal = 0.1089
12	Optical image encryption using improper Hartley transforms and chaos	Mean Square Error Logistic map = 0.8471 Tent map = 1.0021 Kaplan–Yorke map = 1.4338 Ikeda map = 1.2349
13	Optical color image encryption with redefined fractional Hartley transform	Mean Square error Recovered image red = 5.9878, green = 8.0285 blue = 5.0408
14	Multiple images encryption based on Fourier transform hologram	Correlation coefficient Lena = 0.0024 Baboon = 0.00082 Peppers = 0.00023 Cameraman = 0.0013
15	Optical image encryption technique based on compressed sensing and Arnold transformation	Peak Signal to Noise Ratio At 120 radius of filter = 8
16	One step multiplexing optical encryption	Normalized Mean Square Error At 40 percentage of occlusion = 0.4 At 50 percentage of occlusion = 0.5 At 60 percentage of occlusion = 0.6
17	Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding	Correlation coefficient Lena = -0.0011, Girl = 0.0019, plane = -0.0011 Peak Signal to Noise Ratio Lena = 10.2918, Girl = 10.8824, plane = 10.6846

From the above table, it is proved that the chaotic baker map & DRPM is better than the all existing optical image encryption techniques in terms of Correlation coefficient and PSNR for all images represented in the table. The disadvantages of Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding in terms of security is analyzed and propose new algorithm is the main motivation of this survey.

Conclusion:

There various techniques were developed for optical image encryption. Among them Chaotic Baker Map and Double Random Phase Encoding technique process at two layer as preprocessing layer and in another layer DRPE is used to improve the security level of DRPE and it also provide better immunity to noise.

References

1. Li, J., Li, J. S., Pan, Y. Y., & Li, R. (2015). Compressive optical image encryption. *Scientific reports*, *5*.
2. Zhou, N., & Dong, T. (2009, May). Optical image encryption scheme based on multiple-parameter random fractional Fourier transform. In *Electronic Commerce and Security, 2009. ISECS'09. Second International Symposium on* (Vol. 2, pp. 48-51). IEEE.
3. Yong-Liang, X., Su, X., Li, S., Liu, X., & Zeng, S. (2011). Key rotation multiplexing for multiple-image optical encryption in the Fresnel domain.*Optics & Laser Technology*, *43*(4), 889-894.
4. Huang, J. J., Hwang, H. E., Chen, C. Y., & Chen, C. M. (2012). Optical multiple-image encryption based on phase encoding algorithm in the Fresnel transform domain. *Optics & Laser Technology*, *44*(7), 2238-2244.
5. Pan, W., & Qiao, J. (2010, October). An iterative optical image encryption based on double random phase. In *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)* (Vol. 14, pp. V14-80). IEEE.
6. Chen, W., & Chen, X. (2011). Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain. *Optics Communications*,*284*(16), 3913-3917.
7. Chen, W., & Chen, X. (2012). Structured-illumination-based lensless diffractive imaging and its application to optical image encryption. *Optics Communications*, *285*(8), 2044-2047.
8. Hwang, H. E. (2012). Optical color image encryption based on the wavelength multiplexing using cascaded phase-only masks in Fresnel transform domain. *Optics Communications*, *285*(5), 567-573.
9. Zhang, Y., & Xiao, D. (2013). Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform. *Optics and Lasers in Engineering*, *51*(4), 472-480.
10. Liu, J., Jin, H., Ma, L., Li, Y., & Jin, W. (2013). Optical color image encryption based on computer generated hologram and chaotic theory.*Optics Communications*, *307*, 76-79.
11. Zhou, N., Wang, Y., & Gong, L. (2011). Novel optical image encryption scheme based on fractional Mellin transform. *Optics communications*,*284*(13), 3234-3242.
12. Singh, N., & Sinha, A. (2010). Optical image encryption using improper Hartley transforms and chaos. *Optik-International Journal for Light and Electron Optics*, *121*(10), 918-925.
13. Li, X., & Zhao, D. (2010). Optical color image encryption with redefined fractional Hartley transform. *Optik-International Journal for Light and Electron Optics*, *121*(7), 673-677.
14. Lin, C., Shen, X., Tang, R., & Zou, X. (2012). Multiple images encryption based on Fourier transform hologram. *Optics Communications*, *285*(6), 1023-1028.
15. Liu, X., Cao, Y., Lu, P., Lu, X., & Li, Y. (2013). Optical image encryption technique based on compressed sensing and Arnold transformation. *Optik-International Journal for Light and Electron Optics*, *124*(24), 6590-6593.
16. Barrera, J. F., & Torroba, R. (2010). One step multiplexing optical encryption.*Optics Communications*, *283*(7), 1268-1272.
17. 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..

R.Siva Malar received the MCA, M.Phil and M.Sc degrees from Bharathiar University, India in 2006, 2008 and 2009 respectively. She also received her M.E degree from Anna University, India in 2012. Since 2012 she has been working as lecturer in Computer Science department, Jazan University, Kingdom of Saudi Arabia. She is currently doing her Ph.D in Computer Science and Engineering at Jodhpur National University, India. Her research interests are in the areas of resource management and scheduling in the area of Cloud Computing and Image Processing.