Research Article

Secure Optical Encryption Technique for Real Time Security Related Applications - A Review

Anusree. L[1], Abdul Rahiman. M[2]

[1]Assistant Professor, Department of ECE, LBSITW, Kerala, India.
[2]Director of LBS Centre for Science and Technology, Kerala, India.

Article History: Received: 10 November 2020; Revised: 12 January 2021; Accepted: 27 January 2021; Published online: 05 April 2021

Abstract: Recent development in the digital system shows that data security is most important and that optical encryption can be used not only to keep signals confidential but also to authenticate information. By integrating sparsity constraint with optical encryption, the reconstructed decoder image is not always visually recognizable, but can be authenticated using optical correlation means methods. Traditional optical encryption methods can add an extra layer of security to this design as it authenticates without leaking primary signal information. This paper discusses advances in optical authentication and includes theoretical principles and implementation examples to demonstrate the workings of typical authentication systems. Benchmarking and upcoming possibilities are discussed and it is hoped that this review work useful in advancing the field of optical safety.

Keywords: Optical Encryption, Sparsity Constraint, Contrastive Analyses, Digital Systems, Data Security

1. Introduction

The goal of preserving or transmitting information safely sparked the rise of information technology and prompted a multitude of scholarly work on the examination of encryption schemes [1]. Due to the rapid development in optical information processing, new approaches and data protection strategies have been developed using optical methods [2]. Optical encryption methods have been of considerable importance as they enable speed efficiency is parallel processing of image information to be concealed in various parameters, like phase, wavelength, frequency of spatial, and polarization of light [3]. Classical double random phase coding (DRPE) premised on the 4F optical scheme must have developed a great deal of interest among scientists in optical information security research [4]. Several algorithms have been developed, including abbreviation of phase, selection of phase, and positioning of phase [5].

DRPE is an encryption technology a pattern recognition scheme because the Fourier considering changing domain multiplication refers to matching filtering. Once properly designed, the random phase scheme can be applied to authentication systems with invalid biometric information. The encrypted image obtained using the DRPE system is a complex matrix that includes amplitude and phase information, and the encrypted data must be registered for holographic [6]. This means that the DRPE system requires precise optical position, that is tough to achieve in practice. To comfort this limitation, a joint transform correlator (JTC) was introduced into the DRPE framework. In a JTC-based cryptosystem, the plaintext input associated with RPM is placed next to the encryption key on the plane and the power distribution of the joint power spectrum (JPS), because the encrypted information can be written with a mutual power-law sensor, like charge-coupled device (CCD) [7].

The DRPE-based fingerprint key encryption scheme has been reported to survive a known-plain-text attack (KPA). Subsequently, a modern scheme for generating biometric keys based on digital holographic technologies includes the use of optical encryption to secure information [8]. In another instance, Ghost Imaging (GI), also identified as correlated imaging, is dynamic. The optical approach that allows substances to be viewed in difficult. The GI system has two optical beams. The bucket detector detects a spatial resolution bypassing a beam object called a signal beam. Another beam named the reference beam sensed a spatial resolution detecter. Currently, much attention is paid to optical encryption, and the search for and applying optical images based on beam propagation [9]. The input image has been proven to convert stationary white to noise and has some unique features such as optical encryption, parallel processing, and multi-dimensional performance. Optical imaging of imaging systems based on beam propagation. The multi-image optical encryption technique was created on modulation and computer hologram. A computer hologram was introduced for the recording of encrypted complex images, which could solve the difficulties of recording and transmitting encrypted results [10].

This paper is ordered as section II deals with the methodologies of optical encryption. Section III explained previous works based on optical encryption. In section IV discuss with performance analysis of optical encryption and section V concludes the work.

2. Methodologies

Fig. 1. Shows the methodologies of converting plaintext image into ciphertext in optical encryption.

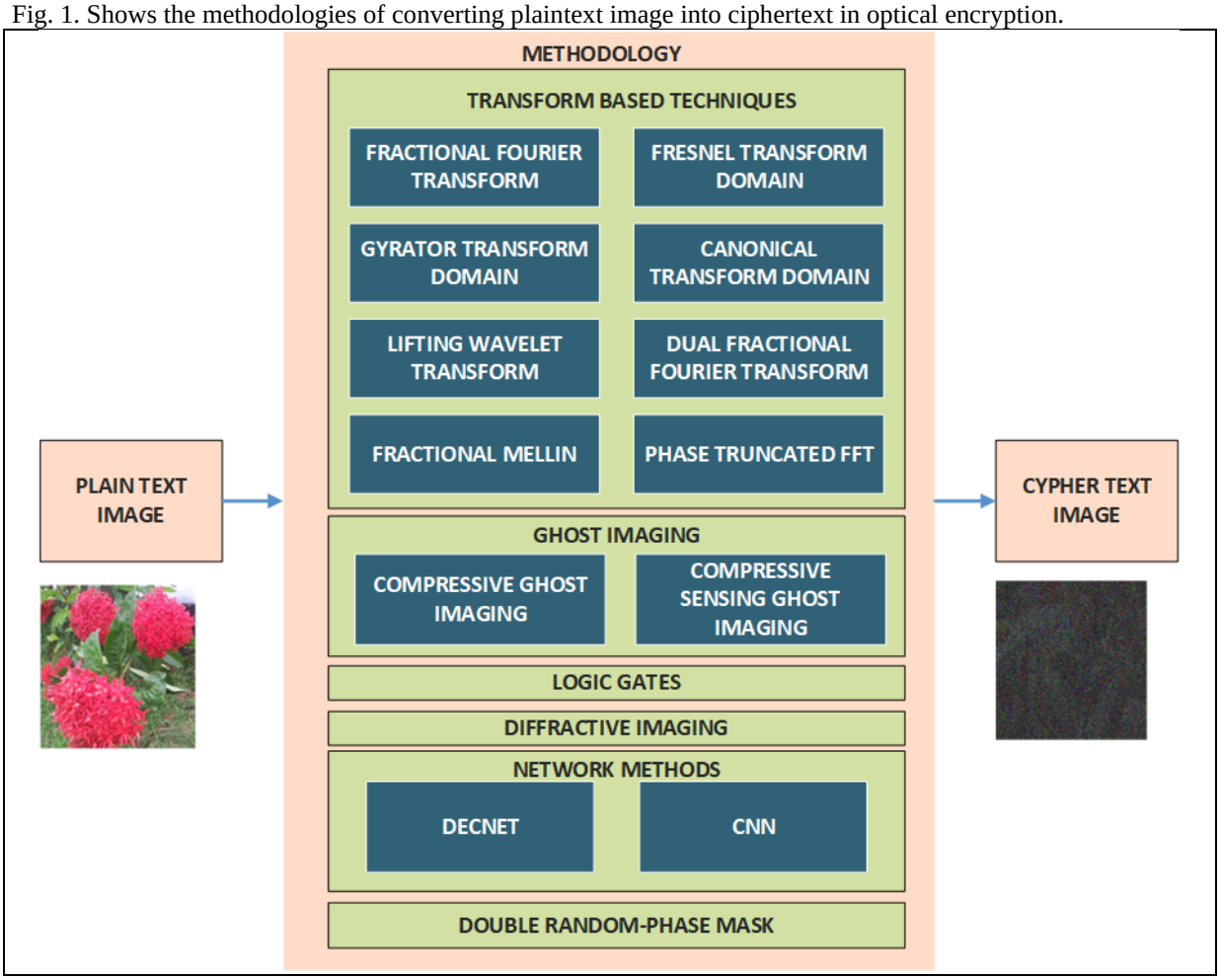

Figure 1. Methodologies for converting plaintext into ciphertext

The Fractional Fourier Transform (FRT) is the generalization of the ordinary transformation of Fourier. The properties and applications of the ordinary transformation of Fourier are unique to those of the FRT. In any area whereby, Fourier transforms and using the rules of the frequency domain, there is space for generalization and growth by the use of fractional transformation. The Fresnel Transform (FST) paired with an FFT of approximately ordered by a sufficient magnification and an extra quadratic step multiplication. It's used to offer additional degrees of freedom.

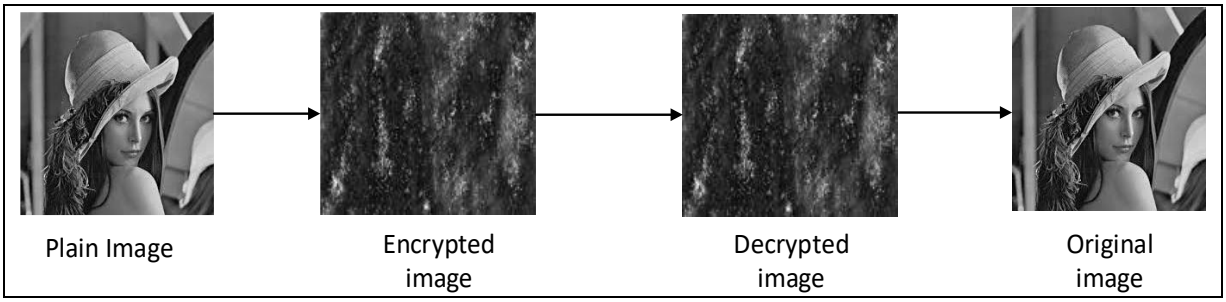

Figure 2. Optical Encryption method

The Gyrator Transform (GT) is commonly used for optical, the digital, holographic and transformational imaging. The GT angle α transforms the 2D image. Canonical transform structures are vulnerable to attacks or their free form. As stability is reported to be violated by adding the amplitude mask on the Fourier plane, the DPRE scheme is capable of nullifying the high-level known-plaintext attack, but the weakness is noticed against such a basic impulse function attack. For transform-based gyrator image encryption, random operations, such as random step encoding, are used in transform-domain image gyrator domains to encrypt a hidden image. In

addition to random operations, the rotation angles used in the transformation of the gyrator are often used as secret keys. Compressive ghost imaging system to encode an intermediate multi-image synthesizer using coordinate sampling.

Dec Net is designed to train ciphertext images (training data) and corresponding plain text images (training label). Dec Net uses the Deep Residual Convolutional Network (Res Net) architecture, where each layer links to each other within the block in a feed-forward manner. Compared to traditional co evolutionary networks, Res Nets provides more clear ties across layers, strengthens the propagation of features, promotes the re-use of features and greatly decreases the number of parameters. Thus, Res Nets is fitted with a greater generalization capability. Neural network methods for extracting unidentified plaintexts from specified ciphertexts without the use of separate optical encryption keys. Simulations and optical experiments at the same time indicate that deep-learning algorithm attacks are feasible and efficient, and a promising strategy for cryptoanalysis of various interference-based optical encryption techniques is anticipated.

Diffractive-based encryption solution as an alternative to the DRPE system. It is approached by multiplexing wavelength and multiplexing distance. Diffractive-based encryption has significantly simplified the encryption architecture, as only intensity patterns are used for decryption and stage information can be discarded addition, the device has relatively high protection as the linearity of the DRPE encryption schemes is violated. It should be stressed that the above stated Diffractive-based encryption methods need at least three strength patterns to be fully retrieved. In Fig.2. shows the structure of the standard optical encryption method. The plain image encrypted with the above any one of the technique or combined with two or more technique and then decrypt that image. Finally, get the original plain image from the decrypted image by performing the decoding process.

3. Previous Works

Han Hai et al proposed optical cryptosystems based on random phase encoding (RPE) are under attack by chosen-plaintext attack (CPA) using in the neural network. A Deep Neural Network (DNN) architecture trained to learn the workings of optical cryptosystems to obtain specific optimized DNA that performs as a decryption system. Dec Net deep learning technique used for this optical encryption technique. As the DRPE improved as triple RPE (TRPE) security. It takes a lot of plain text-ciphertext pairs to operate out the association between any ciphertext and the plain text associated with it. This does not rely on the method of physical decryption or encryption using Ghost imaging in deep learning (GIDL) [11]. Meng Liu et al. proposed traditional GI and associated ground-truth equivalents to using a set of images. An in-depth neural network can be equipped to learn the detecting model and then improve the efficiency of images reproduction. Also, comprehensive comparisons are made between the restored images with in-depth learning and compression. In machine learning techniques used to learn to scatter in optical imaging architecture support for vector degression [12].

Xiaogang Wang et al proposed Flexible optical encryption system that relies on disparate lighting and asymmetric encryption. The input image is encrypted using two random phase masks (RPMs) on the input. Compared to peers using planar lighting and symmetric keys, the significant distinction is that the location of the optical components used for encryption can be constantly changed, leading from encryption keys to various decryption keys, encrypted/decrypted images. Detailed statistical definition and estimation results using various bandwidth of the device. This method can essentially extend the area of the dual random face coding application for optical safety testing [13].

Wen Chen approach a method of 3D space with optical encryption of multiple images. The input image is separated into a sequence of particle-like points that are spread over 3D space and all points, such as the generated particle, are encrypted simultaneously into a phase mask. The three input images are encoded, and every input image is separated into a set of particle-like points which are divided into three-dimensional spaces. Both particle-like points must follow a digital approach to encoding into a phase mask and learn a step-by-step reconstruction algorithm to remove the phase mask. The horizontal regions of the plaintext planes and the three input images are used as plaintext during encryption [14].

Kang Yi et al. suggested an approach for optical encryption focused on public-key cryptography with compressive ghost imaging (CSGI). The GI method's phase object has a hidden impact. The public key RSA method is needed to calculate the key distribution problem. Developing safety networks minimized its cost. The use of compression test process certifies the optimal quality of plain text recovery for restoration in the event of lesser ciphertexts. The structure blends the benefits of RSA public key algorithm besides GI technologies to provide safety and reliability for effective data transfer. It takes a strong confrontation to statistical analysis and

repeated assault and is very strong. Optical CSGI-based encryption and public-key cryptography can provide high quality, security, reliability, wide applicability and low cost of encryption [15].

Alejandro Velez Zea et al. proposed a new protocol to achieve a low noise level and thus a high non-static collection in the optical encryption. It is facilitating, the authentication and optimum retrieval for any encrypted gray images and the untried cryptosystem DPRE. The protocol incorporates the new developments that help minimise noise owing to the random chance step mask interaction in the decryption process and uses the reference mask is also take as the reference item to remove noise owing to the complicated design of the mask used in DRPE experimental settings. The experimental Joint Transformation Correlator (JTC) set of noise reduction techniques used in the cryptosystem. The use of a new reference mask to remove noise owing to the imperfection of the phase mask object by this approach [16]. Naveen K. Nishal et al suggested the optical encryption technique that enables cryptographic requests created on multiplexes. Users can encrypt separate remote images from the encrypted the same file, the superuser can provide a key that encrypts all encrypted images, and can encrypt multiplexed images at different security levels. The method is viewed in the sense of a general architecture for the creation of optical encryption applications. It can represent an entire encrypted 3D scene using a fractional Fourier transformation captured using optical holography [17].

David Maluenda et al. proposed polarimetric optical encoder for the encryption and testing of images. The method for making arbitrarily polarised vector keys founded on the Mach-Zehnder arrangement of the translucent liquid crystal displayed in every direction of the interferometer. In the Encrypted signal, the polarisation information is obtained using the information given by the parameters of the stokes. Besides, the encryption method uses a photon-integrating model that provides data sparseness and non-linear conversions to boost reliability. Registered users with access to optical design variables and polarisation keys can retrieve and verify plain text counting photons. The findings of the optical experiments reveal the potential to use the encryption process [18].

Guangyu Luan et al. proposed the scheme of asymmetric optical image encryption and interference silhouette exclusion with equal modulus resolution (EMD). Plain text is divided into two masks of complex value that use EMD in the FST domain of the same module. The encoded two masks act as four-phase only masks (POMs), these two are ciphertext and the supplementary two are plaintext-dependent private keys with varying diffraction distances and noise-based encryption using inverse Fresnel transformation. Information on the plain text, with its silhouette, can't be accessed with one to four POMs. This removes the drawbacks of the same module in EMD and eliminates the possibility of recurrence of amplitude-phase attacks and extended-amplitude-phase attacks. Numerical models have been used to assess validity and safety [19].

Lina Zhou et al. proposed optical encryption created on the diffraction image is subject to learning attack. With a machine learning attack, an opponent can extract anonymous plaintext from a ciphertext. This method uses end-to-end learning to extract the best display relationships between ciphertext and plaintext. Without specifically extracting or checking the optical encryption keys, an authorized user may extract anonymous plain text from the ciphertext created by the trained learning models. The qualified learning model can extract anonymous plain text from a given ciphertext without directly extracting or checking the various optical encryption keys [20].

4. Performance Analysis

Correlation Coefficient

The correlation coefficient (CC) or the number of iterations is expressed as [21-22]

$$CC\ (F,f) = \frac{E\{[F - E(F)][f - E(f)]\}}{\sqrt{E}\{[F - E(F)]^2\}\, E\{[f - E(f)]^2\}}$$

here F and f represent the plain image and decrypted image

Mean Square Errors

Mean Square Errors (MSEs) between the original image and the decrypted image. Mathematically it can be expressed as

$$MSE = \frac{1}{Px * Px}\sum_{i=1}^{Px}\sum_{j=1}^{Px} |\ \hat{I}(i,j) - I(i,j)|^2$$

where $Px * Px$ represents the number of image pixels, $\hat{I}(i,j)$, $I(i,j)$ signify the original image values and decrypted image values and at the (i,j) pixel.

Peak Signal to Noise Ratio

Peak signal-to-noise ratio (PSNR) is a technical term for the ratio of the highest potential power of the signal to the power of the completely corrupted noise that influences the accuracy of its representation.

$$PSNR = 20.\log_{10} MAX_{PX} - 10.\log_{10} MSE$$

Where MAX_{PX} represents a maximum image pixel value.

Structural Similarity Index Measure

The Structural Similarity Index Calculation (SSIM) is a means of estimating the perceived consistency of digital television and film images, and other types of digital images and videos. SSIM is used to calculate the resemblance between the two images.

$$SSIM_{(I,J)} = \frac{(2\mu_I\mu_J + d_1)(2\sigma_{IJ} + d_2)}{(\mu_I^2 + \mu_J^2 + d_1)(\sigma_I^2 + \sigma_J^2 + d_2)}$$

Where μ_I represents the average of I, μ_J represents an average of J, σ_I^2 represents the variance of I, σ_J^2 represents the variance of J, σ_{IJ} represents the covariance of I and J, d_1 and d_2 represents stabilize the division with weak denominator variables.

Mean Absolute Error

Mean Absolute Error (MAE) is a calculation of the average degree of error in the collection of predictions, without considering their path. This is the average over the test sample of the absolute deviations between the prediction and the real observation that all the deviations are of equal weight.

$$MAE = \frac{\sum_{t=1}^{n} |y_t - x_t|}{n}$$

Where y_t represents the prediction value and x_t represents the true value. Table.1 shows the performance of previous works.

Table1. Performance of previous works

Method	CC	PSNR	SSIM	MSE	MAE
[1]	0.72	7.24	0.28	23.41	5.09
[13]	0.68	5.38	0.11	36.89	11.32
[10]	0.03	6.29	0.26	11.25	9.76
[22]	0.05	4.22	0.41	45.81	8.42
[14]	0.69	6.48	0.83	72.35	5.65

5. Conclusion

In this work, a review is performed for optical cryptography for digital images. Various methodologies and their advantages and disadvantages are explained in this paper. The detailed discussion of numerical algorithm, implementation of the DRPE-based method, and exploration of stable features based on key sensitivity. Besides, an approximate comparison of the process was given under similar operating conditions. To validate the performance various performance measures such as PSNR, CC, SSIM, MSE and MAE are considered.

References

1. Zhao, Shengmei, Le Wang, Wenqiang Liang, Weiwen Cheng, and Longyan Gong. "High performance optical encryption based on computational ghost imaging with QR code and compressive sensing technique." Optics Communications 353 (2015): 90-95.
2. Ibrahim, Sameh, Mohamed G. Egila, H. Shawky, Mohamed KH Elsaid, Walid El-Shafai, and Fathi E. Abd El-Samie. "Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption." Multimedia Tools and Applications (2020): 1-26.
3. Chen, Wen, Guohai Situ, and Xudong Chen. "High-flexibility optical encryption via aperture movement." Optics express 21, no. 21 (2013): 24680-24691.
4. Liu, Shi, Changliang Guo, and John T. Sheridan. "A review of optical image encryption techniques." Optics & Laser Technology 57 (2014): 327-342.
5. Javidi, Bahram, Artur Carnicer, Masahiro Yamaguchi, Takanori Nomura, Elisabet Pérez-Cabré, María S. Millán, Naveen K. Nishchal et al. "Roadmap on optical security." Journal of Optics 18, no. 8 (2016): 083001.
6. Lyu, Meng, Wei Wang, Hao Wang, Haichao Wang, Guowei Li, Ni Chen, and Guohai Situ. "Deep-learning-based ghost imaging." Scientific reports 7, no. 1 (2017): 1-6.
7. Xiong, Y., Du, J. and Quan, C., 2020. Optical encryption and authentication scheme based on phase-shifting interferometry in a joint transform correlator. Optics & Laser Technology, 126, p.106108.
8. Zea, Alejandro Vélez, John Fredy Barrera, and Roberto Torroba. "Innovative speckle noise reduction procedure in optical encryption." Journal of Optics 19, no. 5 (2017): 055704.
9. Verma, Gaurav, Meihua Liao, Dajiang Lu, Wenqi He, Xiang Peng, and Aloka Sinha. "An optical asymmetric encryption scheme with biometric keys." Optics and Lasers in Engineering 116 (2019): 32-40.
10. Xi, Sixing, Nana Yu, Xiaolei Wang, Mei Ying, Zhao Dong, Qiaofen Zhu, Wei Wang, and Huaying Wang. "Optical encryption method of multiple-image based on θ modulation and computer generated hologram." Optics Communications 445 (2019): 19-23.
11. Hai, Han, Shuixin Pan, Meihua Liao, Dajiang Lu, Wenqi He, and Xiang Peng. "Cryptanalysis of random-phase-encoding-based optical cryptosystem via deep learning." Optics express 27, no. 15 (2019): 21204-21213.
12. Lyu, Meng, Wei Wang, Hao Wang, Haichao Wang, Guowei Li, Ni Chen, and Guohai Situ. "Deep-learning-based ghost imaging." Scientific reports 7, no. 1 (2017): 1-6.
13. Wang, Xiaogang, Guoquan Zhou, Chaoqing Dai, and Junlang Chen. "Optical image encryption with divergent illumination and asymmetric keys." IEEE Photonics Journal 9, no. 2 (2017): 1-8.
14. Chen, Wen. "Optical multiple-image encryption using three-dimensional space." IEEE Photonics Journal 8, no. 2 (2016): 1-8.
15. Yi, Kang, Zhang Leihong, and Zhang Dawei. "Optical encryption based on ghost imaging and public key cryptography." Optics and Lasers in Engineering 111 (2018): 58-64.
16. Zea, Alejandro Velez, John Fredy Barrera, and Roberto Torroba. "Experimental optical encryption of grayscale information." Applied optics 56, no. 21 (2017): 5883-5889.
17. Nishchal, Naveen K., and Thomas J. Naughton. "Flexible optical encryption with multiple users and multiple security levels." Optics Communications 284, no. 3 (2011): 735-739.
18. Maluenda, David, Artur Carnicer, Rosario Martínez-Herrero, Ignasi Juvells, and Bahram Javidi. "Optical encryption using photon-counting polarimetric imaging." Optics express 23, no. 2 (2015): 655-666.
19. Luan, Guangyu, Aichuan Li, Zhengguang Chen, and Caojun Huang. "Asymmetric optical image encryption with silhouette removal using interference and equal modulus decomposition." IEEE Photonics Journal 12, no. 2 (2020): 1-8.
20. Zhou, Lina, Yin Xiao, and Wen Chen. "Vulnerability to machine learning attacks of optical encryption based on diffractive imaging." Optics and Lasers in Engineering 125 (2020): 105858.
21. Chen, Mingming, Guangbiao Ma, Chen Tang, and Zhenkun Lei. "Generalized optical encryption framework based on Shearlets for medical image." Optics and Lasers in Engineering 128 (2020): 106026.
22. Wang, Xiaogang, Wen Chen, and Xudong Chen. "Optical encryption and authentication based on phase retrieval and sparsity constraints." IEEE Photonics Journal 7, no. 2 (2015): 1-10.