International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 05 | May 2022 www.irjet.net p-ISSN: 2395-0072

A REVIEW PAPER ON THE OPTICAL ENCRYPTION AND DECRYPTION TECHNOLOGY

Aswathy A P[1], Meril Cyriac[2]

[1]PG Student Dept of Electronics & communication Engineering LBSITW, Kerala, India
[2]Assistant Professor, Dept of Electronics & Communication Engineering, LBSITW, Kerala, India

---

Abstract - *Encryption is the process of transforming plain text data (plaintext) into something that appears random and meaningless (ciphertext). The process of transforming ciphertext to plaintext is known as decryption. Optical encryption secures in-flight data in the network's transport layer as it travels over optical waves over fiber-optic cables. Because the technology integrates directly into the network element, optical encryption provides maximum throughput without compromising performance and transparent transfer of any protocol without the need for additional hardware. The main focus of this paper is to make a comparative analysis of existing optical encryption and decryption technologies.*

Key Words: **Optical Encryption, Ciphertext, Plaintext**

1. INTRODUCTION

Digital photos may now be widely distributed around the world over open networks, thanks to the rapid development of the Internet and current communication systems. The protection of image data from unauthorized copying and distribution has become critical. As a result, image encryption, authentication, and watermarking techniques have been extensively researched. Various image encryption algorithms have been presented in recent years. Optical image encryption techniques have gained a lot of attention because of its inherent capacity to process data in parallel and hide information in several dimensions. Asymmetric and symmetric encryption are the two forms of encryption commonly used today. The name derives from the fact that the same key is used for both encryption and decryption.

The same key is used to encrypt and decrypt data in symmetric encryption. It is also necessary to consider a secure way for transferring the key between the sender and the recipient. The concept of a key pair is employed in asymmetric encryption, with each key being used for encryption and decryption. One of the keys is usually referred to as the private key, while the other is referred to as the public key. Data encrypted using the recipient's public key can only be decrypted with the recipient's private key, which is kept private by the owner. As a result, data can be shared without fear of unauthorized or illegal access.

The image is multiplied by random phase diffusers (masks) both in the input (space) and Fourier (spatial frequency) domains in one major optical encryption system known as "Double Random Phase Encoding (DRPE)". The DRPE can be improved by adding additional degrees of freedom, and the DRPE has been extended to include the Fresnel transform (FrT) domain, fractional Fourier transform (FrFT) domain, Gyrator transform (GT)domain, and other special transform domains for this purpose. Other optical image encryption techniques investigated include interference, digital holography, phase retrieval algorithm, compressive sensing technique, diffractive imaging technique, ghost imaging technique, and integral imaging technique.

The most successful approach to digitalize encrypted information is digital holography, often known as CGH (computer generated holography). CGH also has the capability of selecting any wavelength, adjusting system structure parameters arbitrarily, and recording virtual objects that do not exist in nature. Compressive sensing (CS) technology, which has been used in the field of image encryption, can reduce the amount of data and is beneficial to data preservation and transmission. Biometric keys have recently been introduced into the field of optical encryption. Biometric keys, which are unique and immutable, such as fingerprints, iris, face, and voiceprint, can strengthen security. We looked at some of the known optical encryption algorithms in this paper.

2. REVIEW OF THE DIFFERENT PAPERS

Xueru Sun, Tao Hu, Lihong Ma and Weimin Jin proposed the encryption and decryption technology with chaotic iris and compressed sensing based on computer-generated holography [1]. Combining chaotic mapping, iris phase mask, CGH, and CS, a new symmetric–asymmetric hybrid encryption technique was presented. In the encryption process, the encryption keys are chaotic iris phase mask (CIPM), Fresnel diffraction distance, and wavelength, which are still the decryption keys, known as public keys, in a symmetric key cryptography system. The two-phase masks obtained from phase reservation operations are the decryption keys, which are distinct from the CIPMs used as encryption keys, which are referred to as private keys, and so make up the asymmetric key cryptography system.

Y. Su, W. Xu, T. Li, J. Zhao and S. Liu proposed an Optical color image encryption based on fingerprint key and phase-shifting digital holography [2]. The random phase masks generated from the fingerprint using the secure hash

technique (SHA-256) and chaotic Lozi map are only utilised as interim variables in the encryption process, and the fingerprint is used directly as a secret key. For the primary color image, the suggested encryption system can provide two levels of protection. The discrete wavelet transform hides the primary color image into a greyscale carrier image in the first security level (DWT). The changed carrier image is Fresnel converted at the second security level, and then encrypted into three noise-like holograms using fingerprint-based random phase encoding (FRPE) in the LCT domain and three-step phase-shifting digital holography.

Hazer and R. Yıldırım proposed Multiple-image hybrid encryption based on compressive sensing and diffractive imaging [3]. A hybrid-II approach was created in this study by combining a CS method, simple modified diffractive imaging-based encoding (SMDIBE), space multiplexing, and a method for lowering the pixel size of the carrier to be delivered. With the space multiplexing technology, separate encrypted images are mixed on a single plane, and different users are granted authorization. Using the hybrid technique, picture carrying capacity and cross talk difficulties between images are reduced.

Farah M A. Ben, R. Guesmi, A. Kachouri, and M. Samet proposed a novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation [4]. The approach is based on Shannon's confusion and diffusion properties. The confusion technique is based on DNA encoding and employing DNA XOR to confuse the image's pixel values. There are three stages to the image encryption algorithm. In the first part, we use the DNA encoding technique to encode the image. The second section focuses on creating three chaotic sequences for use in the diffusion phase. In the third step of the procedure, the fractional Fourier transform will be applied three times. Most known attacks, such as statistical analysis and exhaustive attacks, are also resistant to the suggested technique. All of these characteristics indicate that the technique is well-suited to digital image encryption.

Y. Su, W. Xu and J. Zhao presented an Optical image encryption based on chaotic fingerprint phase mask and pattern-illuminated Fourier ptychography [5]. The fingerprint image and chaotic parameters are directly employed as secret keys in the proposed encryption technique, while the CFPMs (chaotic fingerprint phase masks) are only used as interim variables and functions. Sharing the fingerprint image between the sender and authorized receivers can improve the security of the suggested encryption system. The proposed encryption system could benefit from the illumination pattern's added security.

N. Yu, S. Xi, X. Wang, L. Lang, X. Wang, L. Zhang, H. Han, Z. Dong, X. Jiao, H. Wang and H. Zhai proposed an Optical implementation of image encryption based on digital holography and computer-generated hologram [6]. Create a realistic optical image encryption technology that combines digital holography and CGH, allowing both digital and physical pictures to be encrypted and decoded in real time. The resulting encrypted image is a binary real value image with high anti-noise ability called Fourier CGH. The encrypted image and random phase key are encoded in multi-pixel units, which simplifies image decryption system setup alignment.

Y. Su, W. Xu, J. Zhao, L. Chen and X. Tian proposed Optical color image encryption based on chaotic fingerprint phase mask in various domains and comparative analysis [7]. Random phase masks are used as secret keys in the architecture of double random phase encoding. The chaotic masks in this paper. To encrypt color images, expand the chaotic fingerprint phase masks developed to the Fourier transform domain, fractional Fourier transform domain, Fresnel transform domain, and Gyrator transform domain. The chaotic fingerprint phase masks are only utilised as intermediate variables and functions, while the fingerprint and chaotic parameters serve as direct secret keys. The security of these four encryption systems can be considerably enhanced by fingerprint keys that are firmly linked to the sender or receiver.

S. Rajput and O. Matoba proposed a digital holography-based optical multimodal biometric encryption system [8]. Physiological biometrics, such as fingerprints or iris scans, are recorded alongside behavioral biometrics, such as voice, as multimodal biometrics employing multi-parameter off-axis digital holography. The Fresnel domain double random phase encoding method, in which keys are produced from biometric data via a phase retrieval algorithm, is used to encrypt numerous biometrics embedded in the same hologram. By utilizing the advantages of optical technology, the suggested method delivers multimodal biometrics with a greater level of security.

G. Verma, M. Liao, D. Lu, W. He, X. Peng and A. Sinha presented an optical asymmetric encryption scheme with biometric keys [9]. The encryption keys in the proposed system are optically created biometric keys and the PTFT (phase-truncated Fourier transforms) technique's random phase mask keys, while the decryption keys are preserved as the binary key and the generated phase-only mask of the PTFT scheme. The biometric key features are kept safe using digital holography and are used in both encryption and decryption operations to verify the authenticity of the ciphertext utilizing biometric keys during the decryption process.

L. Ma and W. Jin introduced Symmetric and asymmetric hybrid cryptosystem based on compressive sensing and computer-generated holography [10]. There are six encryption keys in this system, two of which are different from the two random phase masks used during the encryption process. As a result, the encryption system possesses both symmetric and asymmetric cryptography

capabilities. The suggested encryption approach improves security while also being resistant to noise and occlusion assaults.

P. Refregier and B. Javidi established an optical image encryption scheme based on input plane and Fourier plane random encoding. [11]. The proposed encryption technique is double random phase encoding (DRPE) in Fourier transform (FT) domain. Two statistically independent random phase masks situated at the input plane and the Fourier plane, respectively, can encrypt the principal picture into a noise-like pattern in this DRPE-based encryption approach. Because the cypher picture created by the DRPE-based encryption system is complex-valued, it is necessary to store both the amplitude and phase information of the cypher image using digital holography.

3. CONCLUSIONS

This paper looked at some of the most recent optical encryption techniques. Most of the optical encryption schemes are based on DRPE. Different techniques have been integrated with DRPE to increase security. To improve the security of DRPE-based encryption methods, biometric features that can be utilized for user authentication have been added. We can see from the review that optical encryption has developed into a strong and challenging field in recent years. Different techniques have been devised to improve data security while being transmitted via an unsecured connection. The latest optical encryption scheme is a combination of chaotic mapping, iris phase mask, CGH, and CS. This encryption method When compared to typical encryption schemes, the transmitted information can be substantially reduced if the chaotic map's initial value is transmitted without the CIPMs, which can greatly minimize the quantity of data transmitted. The RPMs are linked to iris, which further enhances the system's security.

REFERENCES

[1] Xueru Sun, Tao Hu, Lihong Ma, Weimin Jin, The encryption and decryption technology with chaotic iris and compressed sensing based on computer-generated holography. Journal of Optics volume 51, pages124–132 (2022).

[2] Y. Su, W. Xu, T. Li, J. Zhao, S. Liu, Optical color image encryption based on fingerprint key and phase-shifting digital holography. Opt. Lasers Eng. 140, 106550 (2021).

[3] A. Hazer, R. Yıldırım, Multiple-image hybrid encryption based on compressive sensing and diffractive imaging. J. Opt. 22, 1–11 (2020).

[4] Farah M A. Ben, R. Guesmi, A. Kachouri, M. Samet, A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. Opt. Laser Technol. 121, 105777 (2020).

[5] Y. Su, W. Xu, J. Zhao, Optical image encryption based on chaotic fingerprint phase mask and pattern-illuminated Fourier ptychography. Opt. Lasers Eng. 128, 106042(2020).

[6] N. Yu, S. Xi, X. Wang, L. Lang, X. Wang, L. Zhang, H. Han, Z. Dong, X. Jiao, H. Wang, H. Zhai, Optical implementation of image encryption based on digital holography and computer-generated hologram. J. Opt. 22, 075702 (2020).

[7] Y. Su, W. Xu, J. Zhao, L. Chen, X. Tian, Optical color image encryption based on chaotic fingerprint phase mask in various domains and comparative analysis. Appl. Opt. 59, 474–483 (2020).

[8] S. Rajput, O. Matoba, Optical multimodal biometric encryption that uses digital holography. J. Opt. 22, 115703 (2020).

[9] G. Verma, M. Liao, D. Lu, W. He, X. Peng, A. Sinha, An optical asymmetric encryption scheme with biometric keys. Opt. Lasers Eng. 116, 32–40 (2019).

[10] L. Ma, W. Jin, Symmetric and asymmetric hybrid cryptosystem based on compressive sensing and computer-generated holography. Opt. Commun. 407, 51–56 (2018).

[11] P. Refregier, B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. 20, 767–769 (1995).