A REVIEW OF THE EXPANDED DIFFIE-HELLMAN ALGORITHM BASED VIRTUAL OPTICAL HOLOGRAPHIC ENCRYPTION SYSTEM

Amina Seyyadali S[1], Prof. 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 - *Optical encryption is used to secure data in the transport layer of the network as it is carried over optical waves across fiber-optic cables. The acquisition and processing of holograms with a digital sensor array are called digital holograms. Combining both yields holographic encryption VOHE is a method of encrypting information over a Virtual Optical Holographic Encryption system. It includes a virtual optical system based on digital holography and Fourier lens. The VOHE system provides parameters such as propagation wavelength (λ) and focal length (f) of the Fourier lens which are keys that are used for encryption and decryption processes. This review highlights different optical encryption and decryption methods using different algorithms and reviews digital holograms. Diffie-Hellman and Expanded Diffie-Hellman key exchange were also briefly discussed.*

Key Words: Optical encryption, Digital Hologram, Fourier lens, Holographic encryption, Diffie-Hellman

1. INTRODUCTION

One of the most important challenges in today's world is data security. A lot of methods have been proposed in the last decades to encrypt data signals to make them more secure and robust. The field of information security has grown and evolved significantly. The vast outspread of the internet and advance in digital techniques have made it possible to copy and edit images, audio, video, and other types of multimedia data. Digital information is exposed to a variety of vulnerabilities including loss, misuse, duplication, and unauthorized usage of information. Optical techniques provide great potential in information security applications. This paper gives a brief comparison between different optical encryption and decryption techniques. This study extends to the performance parameters used in the encryption process and analyzes their security issues.

Diffie-Hellman, Expanded Diffie-Hellman, RSA, Expanded RSA, etc., are different algorithms that are used in different techniques for better security during the key exchange process. Since key exchange through the public channel is not secure, the important challenge is to find a better algorithm that provides more security and authentication, which must be efficient, accurate and robust.

Topics to be discussed in this review are: Virtual Optical Holographic Encryption System which provides optical holographic encryption using Diffie-Hellman and Expanded DiffieHellman algorithms. One of its applications, the VOHE system for underwater communications is proposed using RSA and ERSA algorithms. Some other optical encryption methods we were going to discuss in this paper include angular multiplexing of multiple images, encryption and decryption of chaotic systems, multi-user encryption and authentication system using joint transform correlation, angle multiplexing of optical image encryption in the Fresnel transform domain using a phase-only computer-generated hologram, etc.

The conclusion is drawn based on the efficiency, accuracy and computational complexity of these techniques.

2. REVIEW PART

Yang Peng, Tomoyuki Nagase, Oshiki Kanamoto et.al [1] introduced the concept of the Virtual Optical Holographic Encryption [VOHE] System using Expanded Diffie-Hellman [EDH] Algorithm. The propagation wavelength (λ) and focal length (f) of the Fourier lens are used as keys for encryption and decryption processes. Encryption is provided through the EDH-C algorithm. C corresponds to a two-dimensional complex function which makes keys stronger.

Pollard's Rho method, NIST tests, etc., were also performed for security evaluation. NIST test results show that the message that was encrypted by the proposed EDH-C algorithm had higher security than DH in case of the unpredictability and complexity of the transmitted message over an insecure channel.

Y. Peng, T. Nagase, S. You, and T. Kanamoto et.al [2] present a new method for encrypting holographic information based on optical and acoustic signals. It is called the VOHE system for underwater communications. The simulation was done based on the COMSOL Multiphysics tool for holograms and Fourier lenses. The wavelength λ was considered the first key, and the focal length f was considered the second key. Expanded RSA[ERSA] algorithm sends system information as a message to the receiver. Pollard's method is used for comparison between RSA mad ERSA. ERSA can achieve a more significant security level than RSA. Pollard's method is used for comparison between RSA mad ERSA. Its applications include communications between deep submergence research vehicles. Utilizing the optical and acoustic waves together will provide high communication stability also.

S.Xi, N. Yu, X. Wang, X. Wang, L. Lang, H. Wang, W. Liu, and H. Zhai et.al [3] proposed a system such that in the encryption process original images are firstly modulated by two random phase keys in Fresnel Transform with different diffraction distances. In decryption, SLM is used as an experimental system and multiple images can be encrypted synchronously with high efficiency. It provides high storage efficiency and simple calculations. So that this optical multiple-image encryption system improves the efficiency of information transmission and multi-user authentication. It has multiple kinds of keys also.

S.Zhao and Y. Chi et.al [4] proposed a system where multiple users utilize their fingerprints to encrypt the plain text in the encryption process. The decryption process can only be performed by people with legitimate identities. This system can prevent the overlapping of images at the output when the distance is low. They also proposed a multi-user double-image encryption method, that can meet the needs of different security environments.

R. Ren, Z. Jia, J. Yang, N. K. Kasabov, and X. Huang et.al [5] proposed a system that combines automatic GrabCut and guided filtering to solve the problem of blurred image details in filtering reconstruction. The new algorithm achieves quasi-noise-free (approximate the noisefree state) DH reconstruction and realizes the retention of details in the image. The quality of the resulting holographic reconstruction is comparable with that achieved incoherent technology, which exceeds the current level of DH and produces a good visual effect. When compared with other international advanced methods, the algorithm is more prominent in terms of detail processing and background noise suppression.

H. T. Chang, Y.-T. Wang, and C.-Y. Chen et.al [6] proposed a new angle multiplexing method, implemented by three different types of angle manipulation on the POCGH and/or image reconstruction planes. It is optics-based image encryption using a phase-only computergenerated hologram (POCGH) in the tilted Fresnel transform (TFrT) domain. Modified Gerchberg-Saxton algorithms are used. The methods proposed here show great potential for 3D image projection, as the rotated images are no longer within the same two-dimensional plane. Due to the encrypted nature of the multiplexed images, a higher system security level can be also achieved.

E. Swathika, N. Karthika, and B. Janet et.al [7] aim to develop an efficient encryption system that should accomplish confidentiality, integrity, and security and also prevents the access of images by unauthorized users. This system used two important techniques which are based on chaos theory namely: Confusion and Diffusion. This system also protects from statistical and differential attacks. Mathematical results showed that the security of the images has been preserved at a higher level and also prevents unauthorized access to sensitive information.

Aryan et.al [8] proposed an extended Diffie-Hellman algorithm by using the concept of the Diffie-Hellman algorithm to get a stronger secret key. This secret key is further exchanged between the sender and the receiver so that for each message, a new secret shared key will be generated. This helps to avoid so many threats like Man in the middle attack, access denial, etc., that are present in the public channel while transmitting valuable information.

COMPARISON OF REVIEW PAPERS

YEAR AND WORK	ALGORITHM/ METHOD USED	DESCRIPTION	LIMITATION	RESULTS
2021 A Virtual Optical Holographic Encryption System Using Expanded Diffie-Hellman Algorithm	EDH-C	Using a complex function increases the security of encryption in the VOHE system.	Key Calculation Complexity while using complex function	EDH-C algorithm had higher security than DH in case of the unpredictability and complexity of the transmitted message over an insecure channel.

2020 A VOHE system for underwater communications	ERSA	Performing VOHE encryption scheme for underwater communications.	Data transmissions over multi-node network systems are not possible in this work	Utilizing the optical and acoustic waves together provided high communication stability
2020 Optical encryption scheme for multiple-image based on spatially angular multiplexing and a computer-generated hologram	Fresnel Transform	Multiple images are encrypted synchronously with high efficiency	Need multiple Keys	Improved efficiency of information transmission and multi-user authentication
2019 A multi-user encryption and authentication system based on joint transform correlation	JTC [Joint Transform Correlation]	Multiple users utilize their fingerprints to encrypt the plain text in the encryption process	Research only applies to Gray images.	JTC-based image encryption system can avoid overlapping images at the output
2019 Quasi-noise free and detail preserved digital holographic reconstruction	DH [Diffie-Hellman]	combines automatic GrabCut and guided filtering to solve the problem of blurred image details in filtering reconstruction	The segmentation is initialized by user interaction which may lead to bad segmentation if initialization quality is poor	The algorithm is more prominent in terms of detail processing and background noise suppression
2019 Angle multiplexing optical image encryption in the Fresnel transform domain using a phase-only computer-generated hologram	Modified GerchbergSaxton algorithm	A new angle multiplexing method, implemented by three different types of angle manipulation on the POCGH and/or image reconstruction planes	The pixilation and scaling effects due to the rotation of the POCGH and the pixel response of the device on which the POCGH is displayed have not been considered yet	The encrypted nature of the multiplexed images provides a higher system security level
2019 Image encryption and decryption using a chaotic system	Chaos theory	An efficient encryption system that accomplished confidentiality, integrity, and security and it also prevents the access of images by unauthorized users	Complexity in choosing input parameters	The security of the images has been preserved at a higher level and also prevents the unauthorized access to the sensitive information
2017 Enhanced Diffie-Hellman algorithm for reliable key exchange	Enhanced DH	Generates a stronger secret key by exchanging different keys for each message	Key calculation complexity while taking roots	Using different keys for each message preserves confidentiality

3. CONCLUSION

This paper presented a review of the optical encryption and decryption schemes using different currently available techniques. Throughout the review, we can understand that optical encryption has emerged as a strong and challenging field during the last years. Different algorithms were introduced so that better security of data is possible while transmission through an unsecured channel. Algorithms like RSA, ERSA, DH, EDH, etc., are used as encryption schemes in some methods. One of the latest algorithms EDH-C's security evaluation was also studied during this review. Multiple image encryption system improves the efficiency of information transmission and multi-user authentication. Angle multiplexing provides a higher security level. This paper also gives a brief comparison between different optical encryption and decryption techniques. This conclusion is drawn based on the efficiency, accuracy, and computational complexity of these techniques.

REFERENCES

[1] Yang Peng, Tomoyuki Nagase, Oshiki Kanamoto "A Virtual Optical Holographic Encryption System Using Expanded Diffie-Hellman Algorithm," Digital Object Identifier 10.1109/ACCESS. February 2021.3055866

[2] Y. Peng, T. Nagase, S. You, and T. Kanamoto, "A VOHE system for underwater communications," Electronics, vol. 9, no. 10, p. 1557, Sep. 2020

[3] S. Xi, N. Yu, X. Wang, X. Wang, L. Lang, H. Wang, W. Liu, and H. Zhai, "Optical encryption scheme for multiple-image based on spatially angular multiplexing and computer-generated hologram," Opt. Lasers Eng., vol. 127, Apr. 2020, Art. no. 105953.

[4] T. Zhao and Y. Chi, "A multi-user encryption and authentication system based on joint transform correlation," Entropy, vol. 21, no. 9, p. 850, Aug. 2019.

[5] R. Ren, Z. Jia, J. Yang, N. K. Kasabov, and X. Huang, "Quasi-noise-free and detailpreserved digital holographic reconstruction," IEEE Access, vol. 7, pp. 52155–52167, 2019.

[6] H. T. Chang, Y.-T. Wang, and C.-Y. Chen, "Angle multiplexing optical image encryption in the Fresnel transform domain using a phase-only computer-generated hologram," Photonics, vol. 7, no. 1, p. 1, Dec. 2019

[7] E. Swathika, N. Karthika, and B. Janet, "Image encryption and decryption using chaotic system," in Proc. IEEE 9th Int. Conf. Adv. Comput. (IACC), Dec. 2019, pp. 30–37

[8] Aryan, "Enhanced Diffie-hellman algorithm for reliable key exchange," 2017 IOP Conf. Ser.: Mater. Sci. Eng. 263 042015