Indian Journal of Science and Technology, *Vol 8(19), DOI: 10.17485/ijst/2015/v8i19/76230, August 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Securing Digital Holographic Complex Information using Double Random Phase Fresnel Plane Encoding and Diffie-Hellman Key Exchange

Aswathy Sankaran*, Praveen Phinehas and Anith Nelleri

School of Electronics Engineering, VIT University, VIT Chennai Campus, Chennai - 600 127, Tamil Nadu, India;
aswathywarrier05@gmail.com, praveen.phinehas2012@vit.ac.in, anith.nelleri@vit.ac.in

Abstract:

Background/Objectives: Using digital holography, one can detect and retrieve 3D information as digital complex images. Such information from digital holography can be secured by the use of virtual optics encryption algorithms. **Methods/ Statistical Analysis**: The paper demonstrates a new method for securing digital holographic information using optical encryption algorithms implemented in digital domain. A double random phase encoding in input plane and Fresnel plane is implemented to secure the retrieved digital holographic data. The Diffie-Hellman key exchange implemented along with this scheme enhances the security level. The Diffie-Hellman secret key has been generated using the sender's private key and receiver's public key. **Findings:** The Diffie-Hellman key exchange gives another protective layer to the double random phase plane encrypted information. An unauthentic user attempts to decode the information with incorrect encoding parameters such as symmetric secret key, wavelength and the propagation distance would fail to retrieve the original information. The Signal to Noise Ratio (SNR) is very low and the Mean Square Error (MSE) is very high when an attacker user uses any one of the wrong encoding parameters. This clearly demonstrates that the unauthenticated user either gets wrongly decrypted information or the original information is totally lost. **Conclusion/Improvements:** The effectiveness and advantages of the proposed method are demonstrated by simulation results. The proposed method can provide a greater confidentiality and authenticity of the digital information because the system incorporates two layers of protection.

Keywords: Diffie-Hellman Key Exchange, Digital Holography, Double Random Phase Fresnel Plane Encoding, Encryption

1. Introduction

Optoelectronic techniques for information security have gained prominence in the recent years. The rapid development in digital holographic processors as led to the demand for novel methods to secure 3D holographic information in processing, transmission and storage. Refriger and Javidi proposed a method of securing information using optical encoding technique called double random phase Fourier plane encoding[1-3]. This is an efficient method to process data optically using 4f filtering. Later Situ and Zhang proposed double random phase encoding in Fresnel domain to secure information[4].

In digital holography optically produced holograms are electronically detected using a CCD or CMOS sensor. The numerical reconstruction of digital hologram enables the amplitude and phase information of the object in a computer in the form of digital complex images. This can be further processed for various 3D information processing applications. Since digital holography is a hybrid technique, the information can be secured either in optical or digital domains. Optical algorithms can be mapped into digital domain to secure digital information which ensures same degree of information encoding as in optical domain[5]. In the present paper, we demonstrate an algorithm to secure digital holographic information. In this we adopt security measures in digital domain. A

*Author for correspondence

double random phase Fresnel plane encoding is applied to the reconstructed complex information. In addition to this the security level is enhanced by incorporating Diffie-Hellman key exchange in the digital domain.

In Diffie-Hellman algorithm sender and receiver have their own public key and private key. The Diffie-Hellman secret key is generated by using sender's private key and receiver's public key. The public key is known to both sender and receiver but the private key is highly confidential[6-10]. The present paper demonstrates the proof of the concept of the proposal. The paper is organized in the following manner. Section 2 gives the brief introduction of double random phase Fresnel plane encoding technique. Section 3 gives the idea of Diffie-Hellman algorithm. Section 4 gives the flow chart of proposed method for securing digital holographic information and its implementation. Section 5 gives results and discussions and finally Section 6 deals with the conclusions derived from the studies.

1.1 Double Random Phase Fresnel Plane Encoding Technique

The Fresnel plane data encoding enjoys more degrees of data encoding freedom. The use of Fresnel domain keys for optical data encoding is well documented in research literatures[11-17,20-23]. A lens-less optical security system based on DRPE in the Fresnel or free-space propagation domain has been proposed by Situ and Zhang[4]. This technique can encrypt a primary image to a random noise by use of two statistically independent random phase masks in the input and intermediate transform planes, respectively. The positional planes of random phase masks, the propagation wavelength, and the random phase codes are important keys to recover the primary image from the encrypted data. Since the mask locations are arbitrary in the free-space domain, primary mask can be bonded either with image or displaced from input plane. In this work we use former case. Figure 1 shows schematic of the encoding scheme and the algorithm is presented in flow chart given in Figure 2a. The decryption process can be depicted in Figure 2b. In Figure 1 Oi is the original image and Ei is the encrypted image and Z1, Z2 are the propagation distances RP1 and RP2 are the random phase mask in the input plane and Fresnel plane respectively.

1.2 Diffie-Hellman Key Exchange

The Diffie-Hellman key exchange is one of the best algorithms that is used in the field of cryptography[14,27].

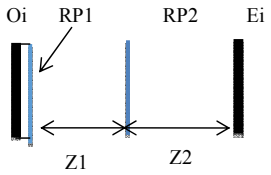


Figure 1. The Schematic of double random phase Fresnel plane encoding.

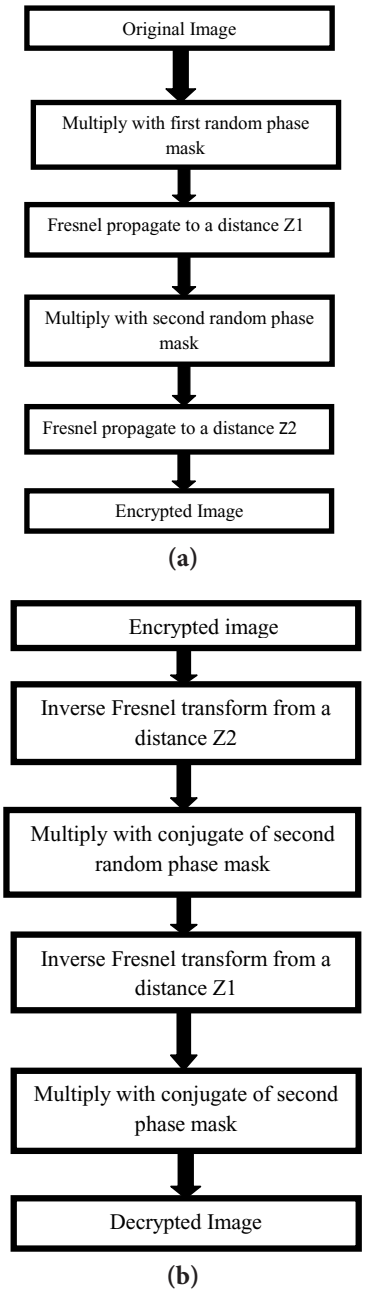


Figure 2. **(a)** Encoding process of double random phase Fresnel plane encoding and **(b)** Decoding process of double random phase Fresnel plane encoding.

The algorithm is based on the difficulty of computing discrete logarithms of large numbers. It is a method by which two users can establish a secured connection over an untrusted channel. The working principle of the algorithm is as follows. The users A and B select two numbers, P a prime number and I and primitive of P. Both P and I are publicly available numbers. The users pick a random secret number R which is usually less than P. The major advantage of using Diffie-Hellman key exchange is that the symmetric secret key is never transmitted in the channel. The secret key is generated using the following equations. The public values of x and y are exchanged. Algebraically ka = kb. Hence users A and B now have a symmetric secret key to encrypt the digital information. The schematics for generating Diffie-Hellman key is shown in Figure 3.

$$x = I^{R1} \bmod P \tag{1}$$

$$y = I^{R2} \bmod P \tag{2}$$

$$ka = x^{R1} \bmod P \tag{3}$$

$$kb = x^{R1} \bmod P \tag{4}$$

1.3 Algorithm for the Proposed Method

A single off axis digital hologram is recorded in transmission mode using Mach Zehnder interferometric geometry as shown in Figure 4. The angle of interference between object wave and reference wave is approximately 1.6 degree. A CCD sensor of square pixel pitch Δ = 6.7 micron is used to detect hologram. The wavelength of the laser λ, is 532 nm and distance from the object to CCD camera 'd' is 21.5 cm. The object used for this experiment is letter 'E'. An

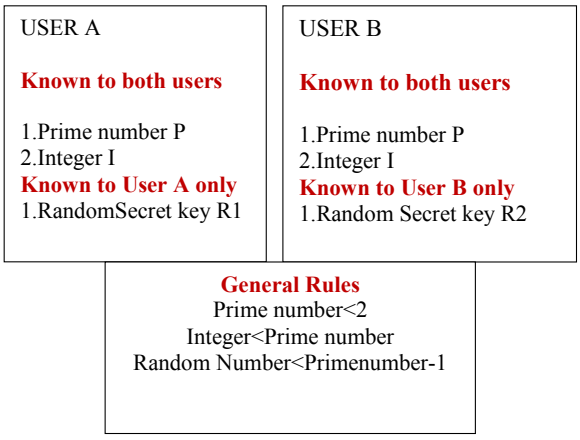


Figure 3. Diffie-Hellman key exchange algorithm.

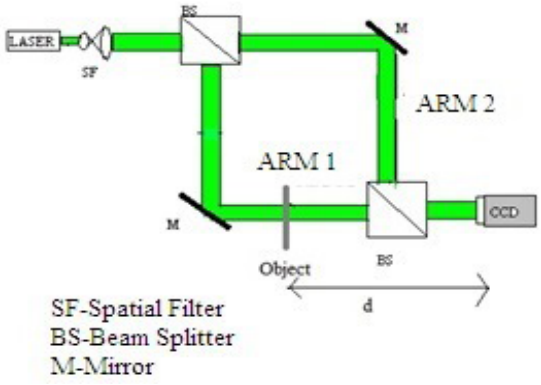


Figure 4. Optical set up used to record off axis digital hologram.

off-axis hologram is formed by the interference between the Fresnel transform of the object field from arm1 and reference beam from arm 2 of the interferometer. The resulting hologram is detected using the CCD sensor. The complex Fresnel transform of the object (Fresnel field) can be retrieved from the sensed digital hologram by a nonlinear method proposed by Liebling et al[18]. The object distribution at a distance d from the CCD is obtained by doing an inverse digital Fresnel transform of the retrieved Fresnel field from the single off-axis hologram[19].

The reconstructed object information from hologram is a digital complex image in the computation domain[24-26]. This complex object information is secured using the proposed method of double random phase Fresnel plane encoding and Diffie-Hellman key exchange. The reconstructed complex image is multiplied by the Diffie-Hellman key followed by another multiplication of the first random phase mask. The encoded image is Fresnel transformed at a distance Z1. The second phase mask is applied to this image and again Fresnel transformed at a distance Z2. Figure 5a shows the encryption of the proposed algorithm for securing complex object information retrieved from a digital hologram. The decrypted image can be obtained by following the flow chart as shown in Figure 5b. The encrypted image is back propagated to a distance Z2 and Z1 and each time multiplying it with the conjugate of the random phase mask respectively. Finally this image is multiplied with inverse of the secret key.

2. Results and Discussion

The robustness of the proposed method is analyzed as discussed below. The amplitude and phase of the

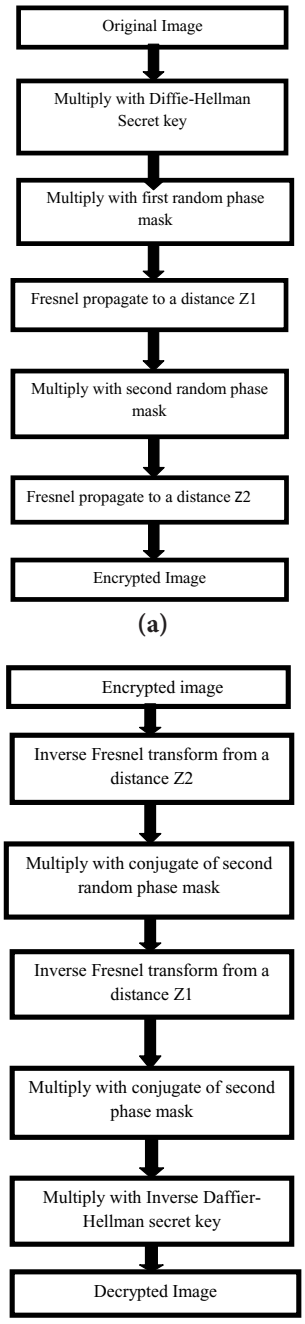
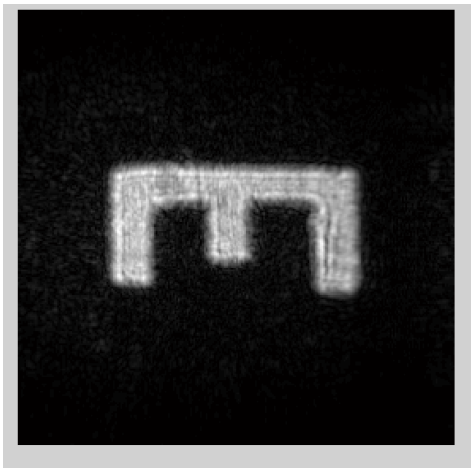
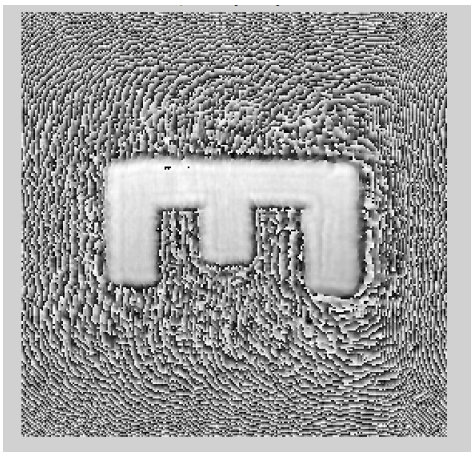


Figure 5. **(a)** Flow chart for proposed encryption scheme and **(b)** Flow chart for the proposed decryption scheme.

reconstructed object field from the single off axis digital hologram is shown in Figure 6a and 6b respectively. The image is encrypted using the proposed method as shown in Figure 7. This is a white noise and is highly secure for transmission and storage. An authentic user can correctly use the Diffie-Hellman key and encoding parameter such as wavelength, propagation distance, and



(a)



(b)

Figure 6. **(a)** Amplitude of the object and **(b)** Phase of the object.

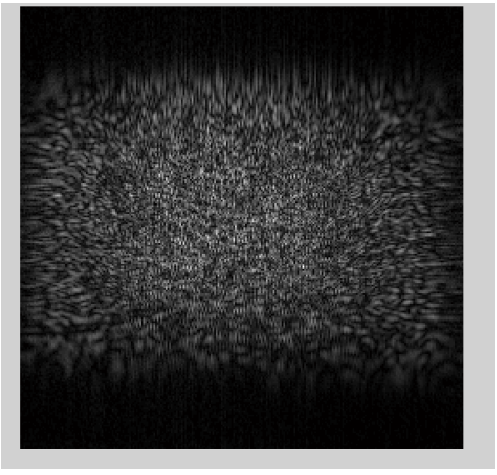
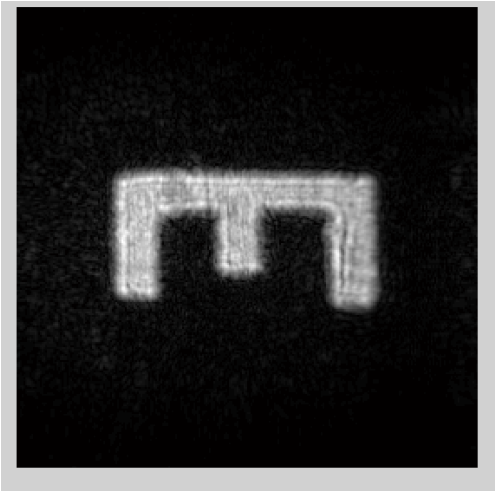


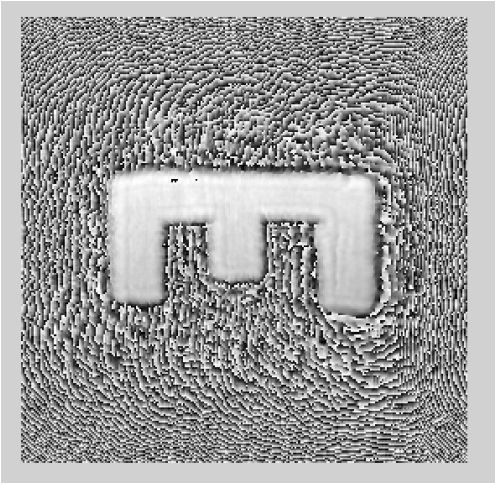
Figure 7. Encrypted image after applying Diffie-Hellman key and DRFPE.

random phase mask to decrypt the correct information. Figure 8a and 8b shows amplitude and phase of the correctly decrypted image. The Fresnel propagation distance of Z1 is 10 mm and Z2 is 20 mm respectively. The values used in the Diffie Hellman key is as follows Prime number P = 353, Integer I = 3, secret random keys R1 = 97, R2 = 233.

An unauthentic user attempt to decode the information with incorrect encoding parameters would end up in wrongly decrypted image. Figure 9a and 9b shows the amplitude and phase of the information when retrieved with incorrect propagation distance. Similarly when an unauthentic user tries to decode the digital information with the wrong wavelength, the result is that the original information cannot be retrieved as shown in Figure 10a and 10b. Likewise the attacker uses a wrong symmetric secret key to retrieve the encoded information the outcome is affirmative as shown in Figure 11a and 11b. The Mean Square Error (MSE) and Signal to Noise Ratio (SNR) quantifies the performance of the proposed method and this can be expressed in Equation 5 and 6.

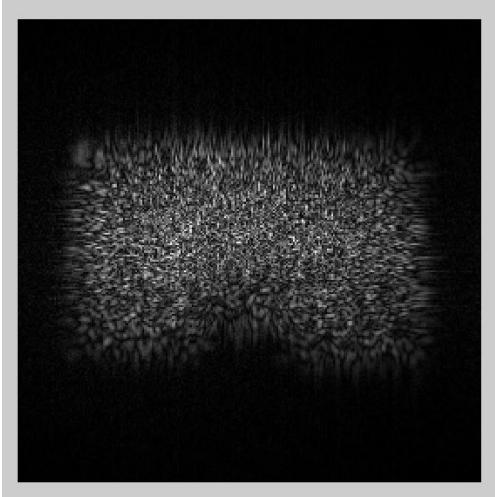


(a)

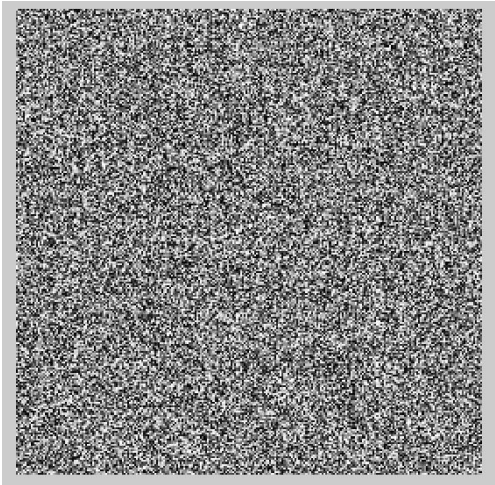


(b)

Figure 8. **(a)** Amplitude of the reconstructed image with correct parameters and **(b)** Phase of the reconstructed image with correct parameters.



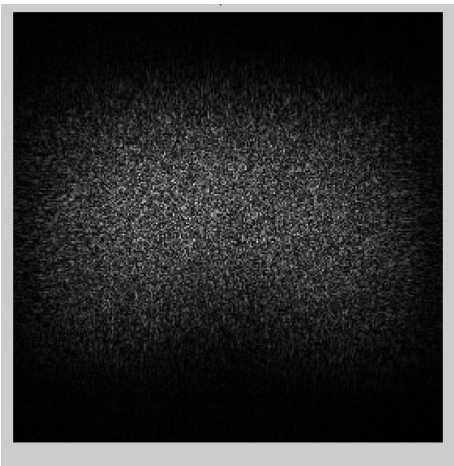
(a)



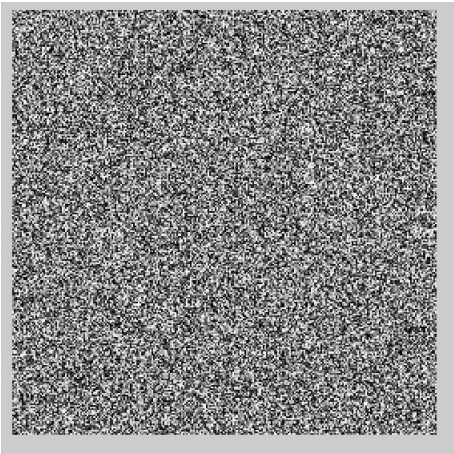
(b)

Figure 9. **(a)** Amplitude of the wrongly decrypted image with incorrect propagation distance and **(b)** Phase of the the wrongly decrypted image with incorrect propagation distance.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left[r(i)-o(i)\right]^2 \quad (5)$$

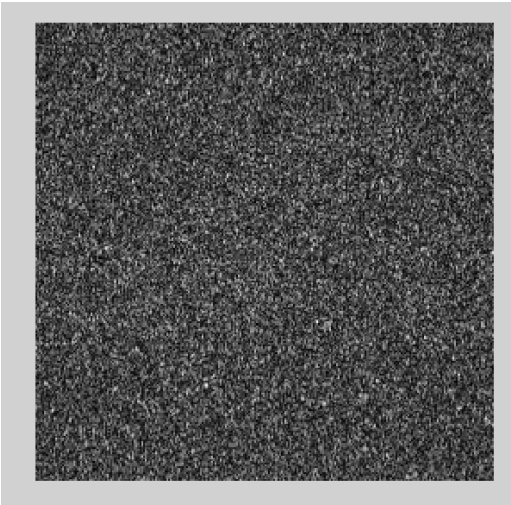


(a)

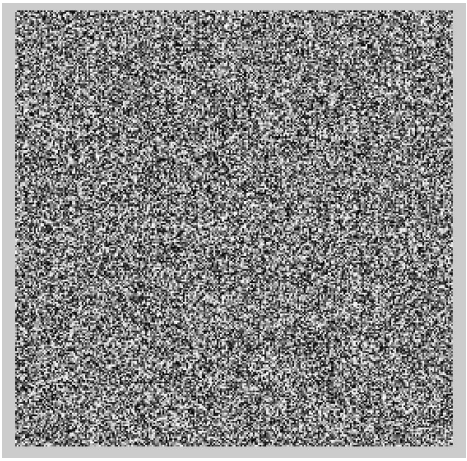


(b)

Figure 10. **(a)** Amplitude of the wrongly decrypted image with incorrect wavelength and **(b)** Phase of the the wrongly decrypted image with incorrect wavelength.



(a)



(b)

Figure 11. **(a)** Amplitude of the wrongly decrypted image with incorrect secret key and **(b)** Phase of the the wrongly decrypted image with incorrect secret key.

$$SNR = \frac{\sum_{i=1}^{n}\left[0(i)\right]^2}{\frac{1}{n}\sum_{i=1}^{n}\left[r(i)-0(i)\right]^2} \quad (6)$$

In the above Equation r(i) is the decrypted image and o(i) is the original image and n is the size of the image. The MSE and SNR for wrong propagation distance, wavelength and symmetric key are tabulated as shown in Table 1.

The Signal to Noise Ratio (SNR) is found to be very low when one applies incorrect parameters such as symmetric secret key or wavelength or the propagation distance. The result shows that digitally secured information is lost when an unauthenticated user tries to decode the information. The Mean Square Error (MSE) for wrong symmetric key is relatively high when compared with the wrong propagation distance or the wave length. This demonstrates that the Diffie-Hellman key provides another layer of information security in the digital domain.

Table 1. Mean square error and signal to noise ratio for wrongly decrypted information

Parameter	MSE	SNR
Propagation distance z	0.03	18.94
Wavelength λ	0.02	20.42
Symmetric Keys	0.08	13.96

3. Conclusion

We have demonstrated a robust method for securing digital holographic information using double random phase encoding in Fresnel plane together with Diffie-Hellman secret key in digital domain. The results are presented from an experiment to demonstrate the proof of the concept. The proposed algorithm enhances the security level of the holographic information in two fold ways. The Diffie-Hellman algorithm provides a strong layer of security followed by another layer of encryption using the double random phase mask.

4. References

1. Refregier Ph, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding. Optics Letters. 1995; 20(7):767–9.
2. Situ G, Zhang J. A lens-less optical security system based on computer-generated phase only masks. Optics Communication. 2004; 232(1–6):115–22.
3. Nomura T, Okazaki A, Kameda M, Morimoto Y. Image reconstruction from compressed encrypted digital hologram. Optics Engineering. 2005; 44(7):2313–20.
4. Situ G, Zhang J. Double random phase encoding in Fresnel domain. Optics Letters. 2004; 29(14):1584–6.
5. Xiang P, Zhpyong CTT. Information encryption with virtual optics imaging system. Optics Communications. 2002; 212(4–6):235–45.
6. Gil SK, Jeon SH, Kim N, Jeong JR. Successive encryption and transmission with phase shifting digital holography. Proceedings of SPIE. 2006; 6136:339–46.
7. Jeon SH, Gil SK. QPSK modulation based optical image cryptosystem using phase-shifting digital holography. Journal of the Optical Society of Korea. 2010; 14(2):97–103.
8. Jeon SH, Gil SK. 2-Step phase shifting digital holographic optical encryption and error analysis. Journal of Optical Society of Korea. 2011; 15(3):244–51.
9. Unnikrishnan G, Joseph J, Singh K. Optical encryption system that uses phase conjugation in photorefractive crystal. Applied Optics. 1998; 37(35):8181–6.
10. Matoba O, Javidi B. Encrypted optical memory system using three-dimensional keys in the Fresnel domain. Optics Letters. 1999; 24(11):762–4.
11. Javidi B, Nomura T. Securing information by use of digital holography. Optics Letters. 2000; 25(1):28–30.
12. Mogensen PC, Glckstad J. Phase-only optical encryption. Optics Letters. 2000; 25(8):566–8.
13. Carnicer A, Montessategui M, Arco S, Jevells I. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys. Optics Letters. 2005; 30(13):1644–6.
14. Frauel Y, Castro A, Naughton TJ, Javidi B. Security analysis of optical encryption. Proceedings of SPIE. 2005; 5986(598603):25–34.
15. Stallings W. Cryptography and Network security. 3rd ed. Prentice Hall; 2004.
16. Nieto-Vesperinas M, Navarro R, Fuentes JF. Performance of a simulated annealing algorithm for phase retrieval. Journal of Optical Society of America. 1998; A5(1):30–8.
17. Nelleri A, Gopinathan U, Joseph J, Sing K. Three dimensional object recognition from digital Fresnel hologram by wavelet matched filtering. Optics Communication. 2006; 259(2):499–506.
18. Liebling M, Blu T, Unser M. Complex wave retrieval from a single off axis hologram. Journal of Optical Society of America. 2004; 21(3):367–77.
19. Schnars U, Juptner W. Direct recording of hologram by a CCD target and numerical reconstruction. Applied Optics. 1994; 33(2):179–81.
20. Kishk S, Javidi B. Water marking of three dimensional objects by digital holography. Optics Letters. 2003; 28(3):167–9.
21. Nelleri A, Joseph J, Singh K. Digital Fresnel field encryption of three-dimensional information security. Optics Engineering. 2007; 46(4):045801.
22. Unnikrishnan G, Joseph J, Singh K. Optical encryption by double random phase encoding in the fractional Fourier domain. Optics Letters. 2000; 25(12):887–9.
23. Tajahuerce E, Javidi B. Encrypting three-dimensional information with digital holography. Applied Optics. 2000; 39(35):6595–601.
24. LeBlanc SP, Gaul EW, Matlis NH, Rundquist A, Downer MC. Single-shot measurement of temporal phase shifts by frequency domain holography. Optics Letters. 2000; 25(10):764–6.
25. Repetto L, Piano E, Pontiggia C. Lensless digital holographic microscope with light emitting diode illumination. Optics Letters. 2004; 29(10):1132–4.
26. Stetson KA, Powell RL. Surface deformation measurement using wave front reconstruction technique. Applied Optics. 1966; 5(4):595–602.
27. Amor L. All optical network: security issues analysis. Optical Communication and Networking. 2015; 7(3):136–45.