Digital Holographic Encryption with Multiple-key Encoding using Micro Phase-shifting Interferometry

Huang-Tian Chan[1], Yang-Kun Chew[1], Min-Tzung Shiu[2] and Chi-Ching Chang[1]
[1]Institute of Electro-Optical & Energy Engineering, Ming Dao University, Taiwan, ROC
[2]School of Defense Science, National Defense University, Taiwan, ROC

Keywords: Digital Holography, Encryption, Phase-shifting Interferometry, Computer-Generated Hologram.

Abstract: This paper proposes a novel phase-shifting digital in-line holography with computer-generated holograms (CGHs) to achieve the goal of encryption via multiple-key encoding. Multiple keys will also be required in order to complete the decryption. These keys include the amplitude and the phase distribution of the primary encryption key, the reconstruction distance of the image, and the phase value modulated via micro phase-shifting interferometry. Experiments in this research have proved that the decryption would not be possible without a primary key. The autocorrelation between the original and the decrypted images shows very high similarity.

1 INTRODUCTION

Holographic encryption technology allows the simultaneous encryption of both the phase and the amplitude of 3-dimensional (3D) images. The traditional holographic optical encryption allows storing and fast accessing of high-density information. Also, the complex encryption conditions and restrictions make the encrypted information hard to crack. This technology is an important research area in the information encryption. (Javidi 1994, Refregier 1995, Javidi 1997, Matoba 1999, Chang 2001, Sun 2002)

Denz *et al*. (Denz 1991) has used deterministic orthogonal phase codes in a reference-based multiplexing technique to obtain a system for the retrieval of multiple images with high diffraction efficiency without energy losses, adjustment problems, or time delay. However the system has actual limitations that arise from imperfections in the phase modulator. Among these limitations, spatial phase fluctuations may destroy the orthogonality between different phase addresses, which in turn, causes cross-correlation noise.

Refregier and Javidi (Refregier 1995) have proposed an optical encoding method of images for security applications via random-phase encoding in both the input and the Fourier planes. This method is widely use in the field of optical encryption. One of the simplest phase multiplexing techniques that have been investigated by many researchers (Wang 2000, Chang 2002, Su 2004) is to use ground glasses to perform random phase multiplexing. Random phase encoding allows the information to be stored within the recording medium in a more secured way.

However, the zero-order diffraction image and the conjugate image interferences accompanied traditional in-line holographic optical image encryption technique tend to cause image distortion. The strict reconstruction conditions of such technique can also complicate the decryption and sometimes cause information loss. Thanks to charged coupled devices (CCDs) with suitable numbers and sizes of pixels and computers with sufficient speed, digital holography (DH) became feasible.

Schnars and Jüptner (Schnars 1994) have established the foundation of DH development using a CCD as a holographic recording medium to reconstruct a real image of an object from digitally sampled hologram via numerical methods. Accessing holographic information via CCD instead of conventional recording media has been proved feasible by many researchers (Liebling 2004, Yamaguchi 1997, Zhang 1998, Javidi 2000, Yamaguchi 2001). In the digital holographic encryption, many researchers have been using object beam or reference beam via phase mask or wavefront modulation for encryption (Javidi 1996,

Chan H., Chew Y., Shiu M. and Chang C..
Digital Holographic Encryption with Multiple-key Encoding using Micro Phase-shifting Interferometry.
DOI: 10.5220/0004836601270133
In *Proceedings of 2nd International Conference on Photonics, Optics and Laser Technology* (PHOTOPTICS-2014), pages 127-133
ISBN: 978-989-758-008-6

Javidi 2000, Tajahuerce 2000, Lai 2000, Arizaga 2003, Nishchal 2004, Naughton 2004, Carnicer 2005, Meng 2006, Cheng 2008, Chen 2008, Zhang 2008, Liang 2009, Jeon 2011). Kim *et al*. (Kim 2004) have encrypted a digital hologram of a 3D object into a stationary white noise using virtual optics, in which a computer-generated random phase key is used. Tsang *et al*. (Tsang 2011) have proposed a method for fast numerical generation and encryption of a Fresnel hologram. CCD does not work well when the resolution of the interference fringes, due the complexity of the encryption key, is beyond the resolution limit of the CCD (Schnars 2002). Therefore, this paper proposes to use in-line setup to encrypt digital hologram. However, unavoidable disturbance from zero-order diffraction image and conjugate image will inevitably cause image distortion.

Takaki et al. (Kreis 1997) have applied two shutters and one phase modulator to the electro-optical holographic recording system to change the recording parameters for the elimination of zero-order and conjugate images. Yamaguchi and Zhang Yamaguchi 1997) have used piezoelectric transducer to modulate the phase of the reference beam via digital calculation, the double image interference of the zero-order and conjugate images can be avoided and phase information of the object beam obtained (Zhang 1998). Cai et al. (Takaki 1999) have proposed an approach to reconstruct the object wave front in phase-shifting interferometry with arbitrary unknown phase steps. The same research team Cai 2003) has proposed a method to extract the arbitrary unknown and unequal phase steps in phase-shift interferometry from interferograms recorded on the diffraction field of an object. The object wave front can then be digitally reconstructed with the formulas they have derived. Throughout the years, researchers have proposed similar techniques with different formulas in a variety of experiments to suppress double image interferences for the reconstruction of object wave information Cai 2004, Xu 2008, Meng 2008, Chang 2009, Hsieh 2009, Hsieh 2010).

Another traditional digital technology like encryption, decryption key information acquisition, due to slight changes of environmental conditions and CCD resolution and stability factors and the key information in the different encryption, so will certainly result in decrypt the information about the error and loss. Implementation of the digital holographic encryption and decryption work entirely by numerical calculation, although we can to ensure the invariance of the encryption key, but the biggest drawback is the need to deal with complex 3D images and phase information, as well as the interference angle of diffraction transmission and consideration of the 3D images with the polarization direction and other issues, such as to achieve true and a complete 3D image information, caused a great deal of the burden must be on the operator and time.

This paper uses micro phase-shifting (MPS) digital in-line holography with CGHs for encryption and decryption within the CCD resolution. The comprehensive and low-noised holographic information of the object wave and the encryption keys are obtained after the elimination of the conjugate and the zero-order diffraction images. The decryption can be accomplished with CGHs as keys without losses. Based on this hybrid approach, the information that has been encrypted can only be correctly obtained by not only the correct multiple keys but also correct parameters. Therefore, it demonstrates that this approach can be used enhance the feasible performance of digital holographic encryption.

2 WORKING PRINCIPLE

The experiment is conducted using Mach-Zehnder interference setup as shown in Fig. 1. The light source of this setup is a He-Ne laser with a power of 30 *m*W and a wavelength of 632.8 *nm*. The setup adopts two λ/2 wave-plates and a polarized beam splitter (PBS) to adjust the ratio of the object beam and the reference beam. Both beams are collimated as plane waves via a lens and a spatial filter. The phase object is a 1.77 mm glass plate (refractive index = 1.52) placed in the path of the reference wave. The plate can be rotated to micro adjust the phase of the reference beam and thereby modify the optical path of the beam. The hologram is recorded using a CCD sensor (Pixera-150SS CCD camera, 1392×1040 pixels, 6.5 *mm* by 4.84 *mm*). The CCD acquires and stores the digital image of the interferences of the reference beam and the object beam. The object beam is thereby reconstructed while the beam's phase change can be obtained via calculation.

This research starts with traditional digital holographic optical encryption methods for the encryption and decryption testing. And then improves the procedure with the optical capture image along with the computer-generated hologram encryption for simple and high security encryption.

Using reference beam modulated by arbitrary phase or amplitude device $T(x, y)$ and conducting

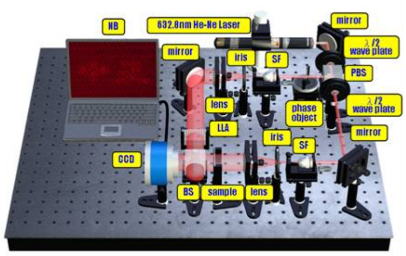


Figure 1: Experiment setup of AMPS modulated digital holographic microscopy encryption.

Fresnel diffraction at distance d in free space, the phase modulated reference beam ψ_{key} can be obtained via Eq. (1) (Goodman 2005):

$$\psi_{key}(\xi,\eta)=T\otimes h=\Im^{1}\{\Im\{T\}\Im\{h(z=d)\}\} \quad (1)$$

Then interfere the coaxial structure and the object beam on the recording plane, $\psi_0(\xi,\eta)$, to speedily and securely encrypt the information of the beam with hologram, I_{enc1}, via equation (2):

$$I_{enc1}=|\psi_{key}+\psi_O|^2=|\psi_{key}|^2+|\psi_O|^2+\psi^*_{key}\psi_O+\psi_{key}\psi^*_O \quad (2)$$

The input image of this experiment is shown in Fig. 2(a). The encrypted image obtained when the distance from CCD to the input image is 21.5 cm and to the lenticular lens array (LLA) is 7.6 cm is shown in Fig. 2(b).

(a) (b)

Figure 2: (a) Input mage and (b) image with LLA encryption.

The first step of the holographic information decryption is zero order term suppression:

$$I'_{enc1}=I_{enc1}-|\psi_{key}|^2+|\psi_O|^2=\psi^*_{key}\psi_O+\psi_{key}\psi^*_O \quad (3)$$

This is the first decryption key. The reduced intensity of the hologram after complete suppression of the zero order term is:

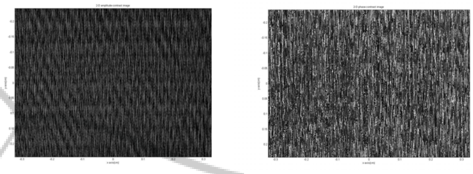
$$I'_{enc2}=\left|\psi_O+\psi_{key}\exp(i\Delta\varphi)\right|^2-|\psi_{key}|^2+|\psi_O|^2$$
$$=\psi^*_{key}\psi_O\exp(-i\Delta\varphi)+\psi_{key}\psi^*_O\exp(i\Delta\varphi) \quad (4)$$

Where $\Delta\varphi$ can be any value other than $\pm n\pi$ (n can any integer) (Zhang, 2004).

This is the second decryption key. To suppress the conjugate image, multiply Eq. (5) with $\exp(-j\Delta\varphi)$ then subtract it from Eq. (4) to obtain:

$$I'_{enc1}-\exp(-i\Delta\varphi)I'_{enc2}=[1-\exp(-i2\Delta\varphi)]\psi_O\psi^*_{key} \quad (5)$$

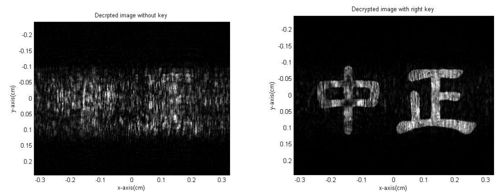
When $\Delta\varphi$ is 1.30 *rad*, the image and the phase contrast image of primary key (LLA) after traveling 7.6 cm in the free space are shown in Figs 3(a) and 3(b).



(a) (b)

Figure 3: (a) Image of primary key (LLA) and (b) phase contrast image of primary key.

As per Eq. (5), ψ^*_{key}, the conjugate information of the primary key needs to be removed in order to obtaind the complete information of the original object beam, This process is the fourth decryption key, which is the most difficult to obtain. As shown in Fig 4(a), It is impossible to complete decrypt the image without this key even if all other keys are compromised. Fig. 4(b) shows the complete image decrypted with this primary key.



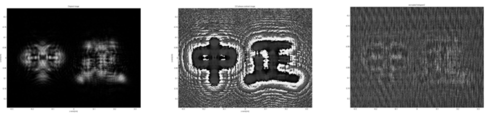
(a) (b)

Figure 4: (a) Decrypted image before applying primary key and (b) image after complete decryption.

The last decryption key is the distance between the encrypted image and the CCD (d), which is used for final decryption.

The object beam as well the image and the phase of the key obtained via experiment are shown in Figs 5(a), 5(b), 3(a), and 3(b). The digital holographic encryption as shown in Fig 5(C) can then be achieved via computer generated hologram production technique.

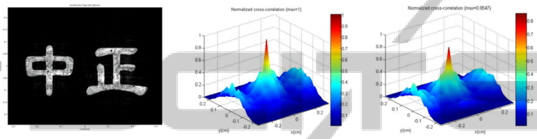
The image decrypted with all the required decryption keys is shown in Fig. 6(a). The cross-correlation of the decrypted image and the original input image is shown in Fig. 6(b). The similarity of



(a) (b) (c)

Figure 5: Comparison of (a) image (not encrypted) at 21.5 cm from CCD, (b) phase comparison image, and (c) image after holographic encryption.

these two images is close to 100%, compared to the result of 85% similarity, as shown in Fig. 6(c), via traditional decryption technique. This result indicates that the proposed encryption technique can provide effective and highly secured digital holographic encryption without distortion.



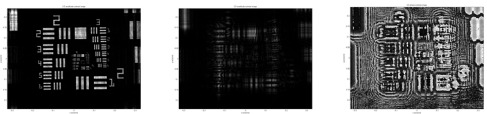
(a) (b) (c)

Figure 6: (a) Image after complete decryption (b) cross-correlation of the input image and Fig. 7(a)., and (c) cross-correlation of the input image and Fig. 5(b).

3 RESULTS AND DISCUSSION

The experiment is conducted using Mach-Zehnder interference setup slightly different from the one shown in Fig. 1. In this setup, a plane wave is used as the recording reference beam. With the position of CCD unchanged, the object beam as well as the image and phase information of all the primary keys are acquired individually.

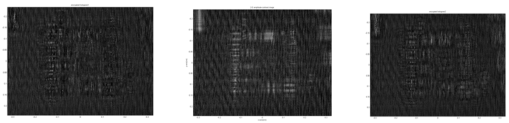
The system resolution tests have been performed using a Newport resolution target (RES-1) as an object. The original input image acquired by the CCD is shown in Fig. 7(a). The image acquired at a 9.4 cm distance between the CCD and the resolution target and the phase comparison image are shown in Figures 7(b) and 7(c), respectively.



(a) (b) (c)

Figure 7: Comparison of (a) original input image, (b) image at 9.35 cm from CCD, and (c) phase comparison image of (a) and (b).

Use computer-generated hologram to encrypt the target image (Fig. 8(a)). For the purpose of decryption testing, the numerical summation of Figs 3(a) and 7(b) are used to produce encrypted image of no interference (Fig. 8(b)). Apply Eq. (5) at $\Delta\varphi = \pi/2$ to produce another encrypted hologram of modulated reference beam phase (Fig. 8(c)).



(a) (b) (c)

Figure 8: The encryption images of analytical target. (a) holographic encryption image without phase modulation, (b) encryption image without interference, and (c) holographic encryption image with phase modulation.

The sensitivity analysis of key rotation and key shifting tests are conducted to verify the integrity of the proposed technique. To produce the adjusted images for analysis, the key image is digitally rotated and shifted. The obtained images are then decrypted with the accordingly adjusted keys. The tolerance of rotation and shifting are then examined through the cross correlation between these decrypted images and the image treated via ordinary procedure. Figure 9 shows that the similarity is below 30% when the decryption key is rotated over 0.4 degree. Figure 10 shows that the image becomes not decryptable when the decryption key is shifted over two pixels (9.34 μm).

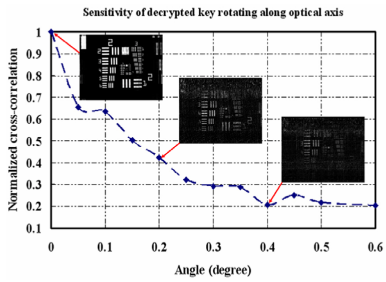


Figure 9: Sensitivity analysis of key rotation at decryption.

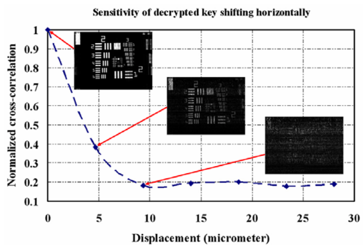
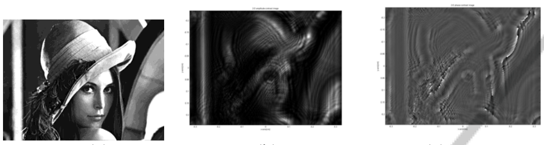


Figure 10: Sensitivity analysis of key shifting at decryption.

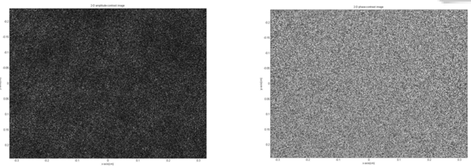
The image of Lena as shown in Fig. 11(a), which is commonly used for image analysis and processing, is used in this research to verify the researched technique's influence to the encrypted image. In addition, a numerical equation is used to simulate the condition in which the distance between CCD and the Lena image is 10.0 cm. The result of the simulation and the obtained relative phase-contrast image and the phase information are shown in Fig. 11(b) and Fig. 11(c).



(a) (b) (c)

Figure 11: (a) Original input image, (b) image at 10 cm from CCD, and (c) phase comparison image of (a) and (b).

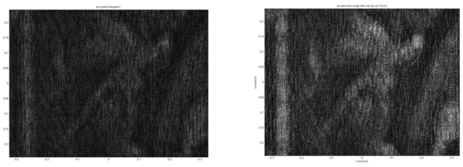
Multiple digital holographic encryptions are performed using LLA and the primary key (diffuser), the image and the phase information obtained as contrast to the CCD are shown in Figs 3(a), 3(b), 12(a), and 12(b).



(a) (b)

Figure 12: (a) Image of primary key (diffuser) and (b) phase comparison image of primary key.

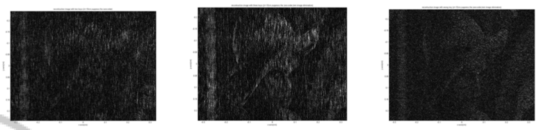
The hologram encrypted with these two primary keys is shown in Fig. 13(a). This multi-digital holographic encryption is able to process and achieve the encryption effect that is difficult for the conventional optical hologram encryption technique. Figure 13(b) shows the image decrypted with a reconstruction distance of 10.0 cm.



(a) (b)

Figure 13: (a) Encrypted image after multiple digital encryption and (b) decrypted image when reconstruction distance (d = 10.0 cm) is the only known key.

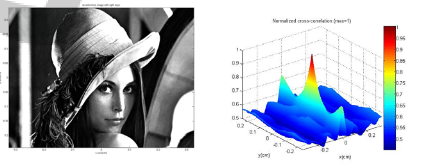
The decryption test of the second key set is conducted using zero-order term elimination technique. The result is shown in Fig. 14(b). The test of the third key set is conducted via conjugate term elimination with the result shown in Fig. 14(a). Even if all other key sets including the primary key (LLA) are cracked, it is still impossible to obtain complete image information without another primary key (the diffuser).



(a) (b) (c)

Figure 14: Resulted image (a) after applying two sets of decryption keys, (b) after applying three sets of decryption keys, and (c) before applying primary key (diffuser).

The image decrypted with all the required decryption keys is shown in Fig. 15 (a). The result of the cross-correlation operation of the decrypted image and the original input image is shown in Fig. 15 (b). The similarity of these two images is close to 100%, which indicates that the proposed encryption technique can provide effective and highly secured digital holographic encryption without distortion.



(a) (b)

Figure 15: (a) Image after complete decryption; (b) related operation result of input image and Fig. 14 (a).

4 CONCLUSIONS

This research uses optical interferometry and digital image processing technique to capture, via in-line setup and within the CCD resolution limit, the holographic information of the object beam and the encryption key. The encryption can be completed using the computer generated holograms with multiple keys that include 1) the amplitude and the phase distribution of the primary encryption key, 2) the reconstruction distance of the image, 3) the elimination of zero-order term, and 4) the phase value modulated via arbitrary micro phase-shift interferometry.

This study has shown that the decryption is not achievable without a primary key. The encrypted image can be transmitted to and captured by a CCD at the receiving end, and then decrypted via simple logical operations. The autocorrelation between the original and the decrypted images shows 100% similarity. The decrypted 3D image can be displayed via the holographic display technology. Having the integrity that is comparable to that of traditional optical holographic encryption, this technique has the convenience and simplicity of digital holographic processing and thus provides a secured solution for holographic information transmission.

ACKNOWLEDGEMENTS

The authors would like to thank the National Science Council of the Republic of China, Taiwan, for financially supporting this research under Contract No. NSC 102-2221-E-451-019.

REFERENCES

Javidi, B., Horner, J. L., 1994. *Optical pattern recognition for validation and security verification* .Opt. Eng. 33 (6): pp. 1752-1756.

Refregier, P., Javidi, B., 1995. *Optical image encryption based on input plane and Fourier plane random encoding*. Opt. Lett. 20(7): pp. 767-769.

Javidi, B., Zhang, G., Li, J., 1997. *Encrypted optical memory using double-random phase encoding*. Appl. Opt. 36(5): pp.1054-1058.

Matoba, O. and Javidi, B., 1999. *Encrypted optical storage with wavelength-key and random phase codes*. Appl. Opt. 38(32): pp. 6785-6790.

Chang, C. C., Russell, K. L., Hu, G. W., 2001. *Optical holographic memory using angular-rotationally phase-coded multiplexing in a $LiNbO_3$:Fe crystal*. Appl. Phys. B. 72(3): pp. 307-310.

Sun, C. C., Su, W. C., 2002. *Three-dimensional shifting selectivity of random phase encoding in volume holograms*. Appl. Opt. 40 (8):pp. 1253-1260.

Denz, C., Pauliat, G., Roosen, G., 1991. *Volume hologram multiplexing using a deterministic phase encoding method*. Opt. Commun. 85(2-3): pp. 171-176.

Wang, B., Sun, C. C., Su, W. C., Chiou, A. E. T., 2000. *Shift-tolerance property of an optical double-random phase-encoding encryption system*. Appl. Opt. 39 (26): pp. 4788-4793.

Chang, H. T., Lu, W. C., Kuo, C. J., 2002. *Multiple-phase retrieval for optical security systems by use of random-phase encoding*. Appl. Opt. 41(23): pp. 4825-4834.

Su, W. C., Sun, C. C., Chen, Y. C., Ouyang, Y., 2004. *Duplication of phase key for random-phase-encrypted volume holograms*. Appl. Opt. 43(8): pp. 1728-1733.

Schnars, U., Jüptner, W., 1994. *Direct recording of holograms by a CCD target and numerical reconstruction*. Appl. Opt., 33 (2): pp. 179-181.

Liebling, M., Blu, T., Unser, M., 2004 .*Complex-wave retrieval from a single off-axis hologram*. J. Opt. Soc. Am. A. 21(3): pp. 367-377.

Yamaguchi, I., Zhang, T., 1997. *Phase-shifting digital holography*. Opt. Lett. 22(16): pp. 1268-1270.

Zhang, T., Yamaguchi, I., 1998. *Three-dimensional microscopy with phase-shifting digital holography*. Opt. Lett. 23(15): pp. 1221-1223.

Javidi, B., Tajahuerce, E., 2000. *Three-dimensional object recognition by use of digital holography*. Opt. Lett. 25(9): pp. 610-612.

Yamaguchi, I., Kato, J., Ohta, S., Mizuno, J., 2001. *Image formation in phase-shifting digital holography and applications to microscopy*. Appl. Opt. 40(34): pp. 6177-6186.

Yamaguchi, I., Ohta, S., Kato, J., 2001. *Surface contouring by phase-shifting digital holography*. Opt. & Lasr. Tech. 36(5):pp. 417-428.

Javidi, B., Zhang, G., Li, J., 1996. *Experimental demonstration of the random phase encoding technique for image encryption and security verification*. Opt. Eng. 35 (9): pp. 2506-2512.

Javidi, B., Nomura, T., 2000. *Securing information by use of digital holography*. Opt. Lett. 25(1): pp. 28-30.

Tajahuerce, E., Matoba, O., Verrall,S. C., Javidi, B.,2000. *Optoelectronic information encryption with phase-shifting interferometry*. Appl. Opt. 39(14): pp. 2313-2320.

Tajahuerce, E., Javidi, B., 2000. *Encrypting three-dimensional information with digital holography*. Appl. Opt. 39(35): pp. 6595-6601.

Lai, S., Neifeld, M. A., 2000. *Digital wavefront reconstruction and its application to image encryption*. Opt. Commun. 178(4-6): pp. 283-289.

Arizaga, R., Henao, R., Torroba, R., 2003. *Fully digital encryption technique*. Opt. Commun. 221(1-3) pp. 43-47.

Nishchal, N. K., Joseph, J., Singh, K., 2004. *Fully phase encryption using digital holography*. Opt. Eng. 43(12): pp. 2959-2966.

Naughton, T. J., Javidi, B., 2004. *Compression of encrypted three-dimensional objects using digital holography*. Opt. Eng. 43(10): pp. 2233-2238.

Carnicer, A., Montes-Usategui, M., Arcos, S., Juvells, I., 2005. *Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys*. Opt. Lett. 30(13): pp. 1644-1646.

Meng, X. F., Cai, L. Z., Xu, X. F., Yang, X. L., Shen, X. X., Dong, G. Y., Wang, Y. R., 2006. *Two-step phase-shifting interferometry and its application in image encryption*. Opt. Lett. 31(10): pp. 1414-1416.

Cheng, X. C., Cai, L. Z., Wang, Y. R., Meng, X. F., Zhang, H., Xu, X. F., Shen, X. X., Dong, G. Y., 2008. *Security enhancement of double-random phase encryption by amplitude modulation*. Opt. Lett. 33(14): pp. 1575-1577.

Chen, G. L., Yang, W. K., Wang, J. C., Chang, C. C., 2008. *Deterministic Phase Encoding Encryption in Single Shot Digital Holography*. Appl. Phys. B. 93(2-3): pp. 473-479.

Zhang, Y., Wang, B., 2008. *Optical image encryption based on interference*. 2008. Opt. Lett. 33(21): pp. 2443-2445.

Xiao, Y.L., Zhou, X., Wang, Q.H., Yuan S., Chen, Y.Y., 2009. *Optical image encryption topology*. Opt. Lett. 34(20): pp. 3223-3225.

Jeon, S. H., Gil, S. K., 2011. 2-step Phase-shifting Digital Holographic Optical Encryption and Error Analysis. *Journal of the Optical Society of Korea*. 15(3): pp. 244-251.

Kim, H., Kim, D. H., Lee, Y. H., 2004. *Encryption of digital hologram of 3-D object by virtual optics*. Opt. Express. 12(20): pp. 4912-4921.

Tsang, P. W. M., Poon, T. C., Cheung, K. W. K., 2011. *Fast numerical generation and encryption of computer-generated Fresnel holograms*. Appl. Opt. 50(7): pp. B46-B52.

Schnars, U., Juptner, W., 2002. Digital recording and numerical reconstruction of holograms. *Measurement Science and Technology*. 13(9): pp. R85- R101.

Kreis, T., Juptner, W., 1997. *Suppression of the dc term in digital holography*. Opt. Eng. 36(8):pp. 2357-2360.

Takaki, Y., Kawai, H., Ohzu, H., 1999. *Hybrid holographic microscopy free of conjugate and zero-order images*. Appl. Opt. 38(23): pp. 4990-4996.

Cai, L. Z., Liu, Q., Yang, X. L., 2003. *Phase-shift extraction and wave-front reconstruction in phase-shifting interferometry with arbitrary phase steps*. Opt. Lett. 28(19): pp. 1808-1810.

Cai, L. Z., Liu, Q., and Yang, X. L., 2004. *Generalized phase-shifting interferometry with arbitrary unknown phase steps for diffraction objects*. Opt. Lett. 29(2): pp. 183-185.

Xu, X. F., Cai, L. Z., Wang, Y. R., Meng, X. F., Sun, W. J. , Zhang, H., Cheng, X. C., Dong, G. Y., Shen, X. X., 2008. *Simple direct extraction of unknown phase shift and wavefront reconstruction in generalized phase-shifting interferometry: algorithm and experiments*. Opt. Lett. 33(8): pp. 776-778.

Meng, X. F. , Cai, L. Z. , Wang, Y. R. , Yang, X. L., Xu, X. F., Dong, G. Y., Shen, X. X., Cheng, X. C., 2008. *Wavefront reconstruction by two-step generalized phase-shifting interferometry*. Opt. Commun. 281(23): pp. 5701-5705.

Chang, C. C., Hsieh, W. T., Kuo, M. K., 2009. Digital Holography with arbitrary phase-step reconstruction using multiple holograms. *Proc. SPIE*, 7358: pp. 735813-1-735813-11.

Hsieh, W. T., Kuo, M. K. , Yau, H. F., Chang, C. C. 2009. *A simple arbitrary phase- step digital holography reconstruction approach without blurring using two holograms*. Opt. Rev. 16(4):pp. 466-471.

Hsieh, W. T., Kuo, M. K., Chang, C. C., 2010. Wavefront reconstruction with fresnel holograms by arbitrary phase-Step digital Holography. *Journal of C. C. I. T.* 39(1): pp. 229-238.

Goodman, J. W., 2005. *Fourier Optics, Roberts & Company*. Colorado, 3rd *ed*.

Zhang, Y., Pedrini, Osten, G., W., Tiziani, H. J., 2004. *Reconstruction of in-line digital holography from two intensity measurements*. Opt. Lett. 29(15): pp.1787-1789.