Published in final edited form as:
Opt Commun. 2012 October 1; 285(21-22): 4262–4267. doi:10.1016/j.optcom.2012.06.056.

Dual-channel in-line digital holographic double random phase encryption

Bhargab Das, **Chandra S Yelleswarapu**, and **D V G L N Rao***
Physics Department, University of Massachusetts Boston, MA 02125

Abstract

We present a robust encryption method for the encoding of 2D/3D objects using digital holography and virtual optics. Using our recently developed dual-plane in-line digital holography technique, two in-line digital holograms are recorded at two different planes and are encrypted using two different double random phase encryption configurations, independently. The process of using two mutually exclusive encryption channels makes the system more robust against attacks since both the channels should be decrypted accurately in order to get a recognizable reconstruction. Results show that the reconstructed object is unrecognizable even when the portion of the correct phase keys used during decryption is close to 75%. The system is verified against blind decryptions by evaluating the SNR and MSE. Validation of the proposed method and sensitivities of the associated parameters are quantitatively analyzed and illustrated.

Keywords

Double random phase encryption; information security; digital holography; virtual optics

1. Introduction

With rapid advancements in internet, computer networking and global communications, information security to protect data from unauthorized use and counterfeiting has become an issue of supreme concern [1]. To this end, optical encryption techniques have received a great deal of attention mainly due to its natural ability to perform high speed parallel processing of two- or three-dimensional (2D/3D) information, and the security associated with an optical hardware implementation. One such method of optical encryption is the double random phase encoding (DRPE) technique [2].

Refregier and Javidi pioneered the work on double random phase encoding (DRPE) for optical security and encryption systems [3]. DRPE involves the use of two 2D random phase keys, one placed in the input image domain and one placed in the Fourier domain of an optical 4f imaging system. The input image is transformed into a stationary white noise by using these two statistically independent phase keys [4-8]. This DRPE technique was also put forward for encrypting information in the fractional Fourier domain with various architectures [9-11]. High security can be obtained because the scale factors and the fraction orders of the fractional Fourier transform provide additional security. Researchers have also

*Corresponding author: Tel: 617-287-6065; Fax: 617-287-6053, raod@umb.edu.

extended the DRPE technique to the Fresnel domain where the distances between the random phase masks, the wavelength parameters, as well as the phase codes serve as the key to the system [12]. Several other optical encryption techniques based on fractional wavelet transform, integral imaging, and photon counting method can also be found in the literature [13-15].

However, the physical implementation of such an optical system gives rise to many practical issues such as lack of flexibility of optical hardware, non-availability of low-cost optoelectronics devices, and the need to manufacture physical random phase masks (RPMs) and difficulty in their alignment during the decryption process etc. Thus most of these encryption methods are difficult to be used in real world application. To overcome these problems, encryption methods based on the concepts of virtual optics (VO) have been proposed using digital holography techniques such as off-axis and phase-shifting digital holography [16-21]. VO enables to digitally control the RPMs and dispenses with the need to manufacture the RPMs physically. It also brings higher degrees of freedom into information hiding as there is no issue of physical limitations and no difficulty of optical alignment.

In this paper, we present a robust encryption method of 2D/3D objects using dual plane in-line digital holography [22-23], and VO. Digital holograms of an object pattern are optically recorded and are digitally encrypted using two independent DRPE channels. The decryption of the encrypted digital holograms and the reconstruction of the original object is performed digitally on a computing device. The proposed method has the advantages of cost effective utilization of the detector spatial bandwidth compared to off-axis holography and of fewer recorded holograms compared to phase-shifting holography [17, 18, 20-23]. Moreover, the use of two DRPE channels with phase keys $\Phi(x, y)$ to obtain the final encrypted data together with the reconstruction distances, z & Δz; and wavelength, λ remarkably enhances the security level of the encrypted information. In addition, digital recording of holograms enables us to store, transmit, and reconstruct data digitally, and offers several advantages over traditional methods.

2. Principle of Dual-channel digital holographic DRPE

The schematic of the experimental setup for recording in-line digital hologram is shown in figure 1. Linearly polarized light from an Ar-Kr laser (λ = 488 nm) is used. The object is placed in one arm of the interferometer and the transmitted light is collected and interfered with the reference beam. The two beams are combined by a beam splitter with no angular offset between them. The interference pattern between the two beams is recorded in two separate planes located at distances z and $z+\Delta z$ from the image plane.

These interferograms can be expressed [24] as

$$\begin{aligned} I_1(x_1, y_1; z) &= |1 + u_1(x_1, y_1; z)|^2 \\ &= 1 + |u_1(x_1, y_1; z)|^2 + u_1(x_1, y_1; z) + u_1^*(x_1, y_1; z) \end{aligned} \quad (1)$$

$$\begin{aligned} I_2(x_2, y_2; z+\Delta z) &= |1 + u_2(x_2, y_2; z+\Delta z)|^2 \\ &= 1 + |u_2(x_2, y_2; z+\Delta z)|^2 + u_2(x_2, y_2; z+\Delta z) + u_2^*(x_2, y_2; z+\Delta z) \end{aligned} \quad (2)$$

where the reference beam is considered to be an on-axis plane wave of unit amplitude, and $u_1(x_1, y_1; z)$ and $u_2(x_2, y_2; z + \Delta z)$ are the diffraction patterns of the object $u_0(x_0, y_0; 0)$ at recording distances of z and $z+\Delta z$ from the image plane.

These two diffraction patterns can be expressed using the Rayleigh-Sommerfeld diffraction formula [24] as

$$\begin{aligned} u_i(x_i, y_i; z_i) &= P\{u_0(x_0, y_0; 0); z_i\} \\ &= -\frac{1}{2\pi}\int\int u_0(x_0, y_0; 0)\frac{\partial}{\partial z_i}\left[\frac{\exp[jkr_i]}{r_i}\right]dx_0 dy_0 \end{aligned} \quad (3)$$

where i=1, 2, $z_1 = z$, $z_2 = z + \Delta z$, $r_i = [(x_i - x_0)^2 + (y_i - y_0)^2 + z_i^2]^{1/2}$, $k = 2\pi/\lambda$ and the operator $P\{\cdot; z\}$ stands for propagation in free space over a distance z.

The two recorded digital holograms at distances z and $z+\Delta z$ are then encrypted using the DRPE technique with two independent encryption channels as depicted by the block diagram in Figure 2. For this purpose, we followed the DRPE technique proposed in [2] and the required RPMs with uniform distribution in the range [0, 2π] are obtained digitally. To encode I_1 in to a stationary white sequence, we perform two operations. First we multiply, I_1 by a phase mask $\Phi_{11} = \exp(i2\pi n_{11})$. The Fourier transform (*FFT*) of the above product is then multiplied by another phase mask $\Phi_{12} = \exp(i2\pi n_{12})$. Here, n_{11} and n_{12} denote two independent white sequences uniformly distributed in [0, 1]. Finally, the encrypted information for the 1st channel is obtained by performing a further inverse Fourier transformation (*IFFT*). Thus the encrypted hologram for the 1st channel can be expressed as

$$\Psi_1(x, y) = IFFT\left[FFT(I_1(x, y) \times \Phi_{11}) \times \Phi_{12}\right] \quad (4)$$

The encrypted hologram for the 2nd encryption channel Ψ_2 is obtained by using two more phase masks Φ_{21} and Φ_{22}, and can be expressed as

$$\Psi_2(x, y) = IFFT\left[FFT(I_2(x, y) \times \Phi_{21}) \times \Phi_{22}\right] \quad (5)$$

It is required that the encrypted holograms should be a stationary white noise for it to be robust against blind decryptions. The stationary whiteness can be verified by using the autocorrelation function given by

$$E\{\Psi^*(x, y)\Psi(x+p, y+q)\} = \frac{1}{N}\sum_{\xi=0}^{N-1}\sum_{\eta=0}^{N-1}|\Psi(\xi, \eta)|^2\delta(p, q) \quad (6)$$

where $E\{\bullet\}$ represents an ensemble average over a random phase, the asterisk denotes the complex conjugate, and $\delta(p, q)$ is Kronecker delta function. This property will be verified numerically in section 3 below by calculating the autocorrelation function of the encrypted holograms.

The reconstruction of the object pattern information from the encrypted digital hologram can be performed digitally in a computer. Initially each encrypted digital hologram is decrypted separately using conjugate of the corresponding phase masks [2]. For the 1st encryption channel, Ψ_1 is inverse Fourier transformed and is multiplied by the phase mask $\Phi_{12}^* = \exp(-i2\pi n_{12})$. The Fourier transform of the above product is then multiplied by the phase mask $\Phi_{11}^* = \exp(-i2\pi n_{11})$. Similarly the 2nd encryption channel is also decrypted by performing a similar operation on Ψ_2. Then the object information at the image plane can be reconstructed [22, 23] as follows:

$$U(x,y) = \Im^{-1}\left\{\frac{\delta I(f_x, f_y; z)}{H(f_x, f_y; z) \times \left[1 - H(f_x, f_y; 2\Delta z)\right]}\right\} \quad (7)$$

where $\Im^{-1}\{\bullet\}$ stands for the inverse Fourier transform and

$$\delta \mathrm{I}(f_x, f_y) = I(f_x, f_y; z) - I(f_x, f_y; z+\Delta z) H(f_x, f_y; \Delta z), \quad (8)$$

$$\mathrm{I}(f_x, f_y; z_i) = \int\int I(x, y; z_i) \exp\left[-i2\pi(f_x x + f_y y)\right] dxdy \quad (9)$$

$I(x, y; z_i)$, $i = 1, 2$, are the decrypted digital holograms, $H(f_x, f_y; z_i)$ is the transfer function for free space propagation, and fx and f_y are the spatial frequency components along x and y directions respectively [24].

We notice from Eq. (7) and Eq. (8), that the decryption and reconstruction of the object information requires information from both the two channels. Thus the method proposed in this paper is bound to be more robust against attacks since both the two channels should be decrypted correctly in order to get a recognizable reconstruction. In the following section, we present encryption and decryption results based on the above proposed architecture. We show that the encrypted digital holograms become a white noise like pattern. We also calculate the signal-to-noise ratio (SNR) and mean-square-error (MSE) of the reconstructed object for various decryption conditions validating the robustness of the proposed dual-channel encryption technique.

3. Encryption and decryption results

For proof of concept, an USAF resolution chart (elements of Group 6 and 7) is used as the object. The holograms are recorded using a SPOT Insight™ 2 MP Firewire CCD with square pixels of size 7.4 μm. The two recorded holograms at distances 130.5 mm and 130.6 mm (from the image plane, $\Delta z = 0.1$ mm) are shown in figures. 3(a) and 3(b) respectively.

The encryption of the recorded digital holograms is performed using two independent DRPE channels. Each encryption channels involves the use of two 2D random phase keys (i.e. Φ_{11}, Φ_{22}, Φ_{21}, and Φ_{22} as shown in the block diagram of figure 2), one placed in the hologram image domain and one placed in the Fourier domain of a 4f virtual optical imaging system. If these phase keys are generated by using statistically independent random sequences, then the encrypted information becomes stationary white noise. For example, figures 4(a) and 4(b) represent the real and imaginary parts of the encrypted digital hologram Ψ_1 for one of the two channels. Figure 4(c) shows the autocorrelation function of the complex encrypted digital hologram Ψ_1. The autocorrelation calculated using Eq. (6) is very small everywhere else except at $(p, q) = (0, 0)$. This implicates that the encrypted hologram in our system becomes a stationary white noise. For further verification, we obtained the histograms of the real and imaginary parts of encrypted digital hologram Ψ_1, as shown in figures 4(d) and 4(e). The theoretical Gaussian distribution fits very well to the histograms, and the mean and variance is calculated to be 0.0 and 0.3, respectively. This shows that the encrypted digital hologram Ψ_1 can be a considered as a Gaussian stationary white noise. Similar studies are also performed for the other encrypted hologram Ψ_2 which is not shown here. Ψ_2 also becomes a Gaussian stationary white noise.

The decryption of the encrypted digital holograms and the reconstruction of the data pattern is performed digitally. The object information at the image plane can be reconstructed using

Eq. (7). Figure 5(a) shows the recovered image when the decryption and the reconstruction is performed using the correct system parameters. The quality of the object reconstruction in the presence of errors in different parameters in both the encryption channels are tested using the metrics of SNR and MSE defined respectively as [17],

$$SNR = \frac{\sum_{\xi=0}^{N-1}\sum_{\eta=0}^{N-1} |U_1(\xi,\eta)|^2}{\sum_{\xi=0}^{N-1}\sum_{\eta=0}^{N-1} \left[|U_1(\xi,\eta)| - |U_2(\xi,\eta)| \right]^2} \quad (10)$$

$$MSE = \frac{\sum_{\xi=0}^{N-1}\sum_{\eta=0}^{N-1} \left[|U_1(\xi,\eta)| - |U_2(\xi,\eta)| \right]^2}{N \times N} \quad (11)$$

where $U_1(\xi, \eta)$ and $U_2(\xi, \eta)$, respectively, represent the reconstructed object from the encrypted holograms using the correct encryption parameters and the reconstructed object from the encrypted hologram without using the correct encryption parameters. Both $U_1(\xi,\eta)$ and $U_2(\xi,\eta)$ are normalized by, the maximum of $U_1(\xi,\eta)$. For figure 5(a), the SNR and the MSE is calculated to be 159.5 and 3.31×10^{-4} respectively. Further we studied the decryption of the encrypted holograms by choosing various system parameters. Figure 5(b) and 5(c) show the variation of SNR and the MSE values for different reconstruction distances on either side of the actual reconstruction distance. The SNR drops very sharply on either side, by about 50% of the maximum value when the reconstruction distance is altered as small as 0.5 mm. This shows the dependence of SNR and MSE of the recovered object on the reconstruction distances.

In order to test the robustness of the system, we reconstructed the object information from the encrypted digital holograms through blind decryption, where none of the parameters such as the phase keys $\Phi(x, y)$, the reconstruction distances, z and Δz; and wavelength, λ are known. In this case the reconstructed object is given by a white noise like pattern regardless of the reconstruction distance as shown in figure 6(a) and the average SNR and MSE are calculated to be 0.42 and 0.12, respectively. Figure 6(b) shows the SNR and MSE as functions of the reconstruction distance.

Next the encrypted digital holograms are decrypted using the correct system parameters but using only a portion of the correct decryption phase keys in both the two channels. Figure 7 shows the SNR and MSE as a function of percentage of correct phase keys. Figure 8 shows the reconstructed object when the portion of the correct phase keys used in the decryption process is 25%, 50%, 75% and 90% respectively. In this case the reconstructed object was recognizable only when the portion of the correct phase keys used are greater than 75%. For comparison, the method proposed in [17] shows that a recognizable reconstructed image can be obtained when the decryption key used is only 5%. Thus our proposed method of dual channel DRPE is found to be more robust leading to a remarkable increase in the security level.

To further demonstrate the robustness of the dual channel DRPE technique, we decrypted the object information by considering a situation where the correct phase masks for one of the channel is 100% known. As shown in the figure 9, the reconstructed data pattern is still unrecognizable with very poor SNR and MSE values. This illustrates the robustness of the proposed method against a single channel DRPE technique. Furthermore, the distance between the two recording planes (Δz) is another vital parameter which serves as an important key. Figure 10 shows the recovered image obtained considering Δz=0.15 mm

(correct Δz is 0.1 mm) during reconstruction assuming the best case scenario i. e. with correct system parameters for both the encryption channels. Even in this case the decrypted data pattern is not decipherable, and the SNR and MSE are found to be 0.86 and 0.06 respectively. Thus we see that the reconstruction algorithm and the decryption process are also very sensitive to the parameter Δz, and can be used as an effective encryption key together with the RPMs.

7. Conclusion

In summary, we present the method of encryption of 2D/3D objects using digital holography and VO. Two in-line digital holograms recorded at two different planes are encrypted using a dual channel DRPE configuration. The robustness of the proposed system is verified against blind decryptions by evaluating the SNR and MSE. The reconstructed object shows a pattern of white noise irrespective of the reconstruction distance. It is also shown in the results that the reconstructed object is unrecognizable even when the portion of the correct phase keys used in the reconstruction is close to 75%. The method of inline digital holography makes the proposed method cost effective both in terms of utilizing the detector spatial bandwidth (compared to off-axis recording) and in terms of recording fewer holograms compared to phase shifting holography. Furthermore, the process of using two mutually exclusive encryption channels makes the system more robust against attacks since both the two channels should be decrypted properly in order to get a recognizable reconstruction. The reconstruction distances, z and Δz; and wavelength, λ offers additional security level to the encrypted information.

Acknowledgments

This work is in part supported by National Center for Research Resources, National Institute of Health (NIH) grant 1R21RR024429-01A1.

References

[1]. Javidi, B. Optical and Digital Techniques for Information Security. Springer Verlag; 2005.

[2]. Alfalou A, Brosseau C. Optical image compression and encryption methods. Adv. Opt. Photon. 2009; 1:589–636.

[3]. Refregier P, Javidi B. Optical-image encryption based on input plane and Fourier plane random encoding. Opt. Lett. 1995; 20:767–769. [PubMed: 19859323]

[4]. Javidi B, Nomura T. Securing information by use of digital holography. Opt. Lett. 2000; 25:28–30. [PubMed: 18059771]

[5]. Suzuki H, Yamaguchi M, Yachida M, Ohyama N, Tashima H, Obi T. Experimental evaluation of fingerprint verification system based on double random phase encoding. Opt. Express. 2006; 14:1755–1766. [PubMed: 19503504]

[6]. Nelleri A, Joseph J, Singh K. Digital Fresnel field encryption for three-dimensional information security. Opt. Eng. 2007; 46:045801.

[7]. Monaghan DS, Gopinathan U, Situ G, Naughton TJ, Sheridan JT. Statistical investigation of the double random phase encoding technique. J. Opt. Soc. Am A. 2009; 26:2033–2042.

[8]. Monaghan DS, Gopinathan U, Naughton TJ, Sheridan JT. Key-space analysis of double random phase encryption technique. Appl. Opt. 2007; 46:6641–6647. [PubMed: 17846658]

[9]. Unnikrishnan G, Joseph J, Singh K. Optical encryption by double random phase encoding in the fractional Fourier domain. Opt. Lett. 2000; 25:887–889. [PubMed: 18064216]

[10]. Nishchal NK, Unnikrishnan G, Joseph J, Singh K. Optical encryption using a localized fractional Fourier transform. Opt. Eng. 2003; 42:3566–3571.

[11]. Tao R, Xin Y, Wang Y. Double image encryption based on random phase encoding in the fractional Fourier domain. Opt. Express. 2007; 15:16067–16079. [PubMed: 19550895]

[12]. Situ G, Zhang J. Double random-phase encoding in the Fresnel domain. Opt. Lett. 2004; 29:1584–1856. [PubMed: 15309826]

[13]. Chen L, Zhao D. Optical image encryption based on fractional wavelet transform. Opt. Commun. 2005; 254:361–367.

[14]. Piao Y-R, Shin D-H, Kim E-S. Robust image encryption by combined use of integral imaging and pixel scrambling techniques. Opt. Lasers Eng. 2009; 47:1273–1281.

[15]. Perez-Cabre E, Cho M, Javidi B. Information authentication using photon-counting double-random-phase encrypted images. Opt Lett. 2011; 36:22–24. [PubMed: 21209674]

[16]. Peng X, Cui Z, Tan T. Information encryption with virtual-optics imaging system. Opt. Commun. 2002; 212:235–245.

[17]. Kim H, Kim DH, Lee YH. Encryption of digital hologram of 3-D object by virtual optics. Opt. Express. 2004; 12:4912–4921. [PubMed: 19484045]

[18]. Wang X, Zhao D, Jing F, Wei X. Information synthesis (complex amplitude addition and subtraction) and encryption with digital holography and virtual optics. Opt. Express. 2006; 14:1476–1486. [PubMed: 19503472]

[19]. Wang X, Chen Y. Securing information using digital optics. J. Opt. A: Pure Appl. Opt. 2007; 9:152–155.

[20]. Meng XF, Cai LZ, Xu XF, Yang XL, Shen XX, Dong GY, Wang YR. Two step phase shifting interferometry and its application in image encryption. Opt. Lett. 2006; 31:1414–1416. [PubMed: 16642123]

[21]. Meng XF, Peng X, Cai LZ, Li AM, Gao Z, Wang YR. Cryptosystem based on two-step phase-shifting interferometry and the RSA public key encryption algorithm. J. Opt. A: Pure Appl. Opt. 2009; 11:085402.

[22]. Das B, Yelleswarapu CS. Dual plane in-line digital holographic microscopy. Opt. Lett. 2010; 35:3426–3428. [PubMed: 20967088]

[23]. Das B, Yelleswarapu CS, Rao DVGLN. Quantitative phase microscopy using dual-plane in-line digital holography. Appl. Opt. 2012; 51:1387–1395. [PubMed: 22441487]

[24]. Goodman, JW. Introduction to Fourier Optics. 3rd Ed. Roberts & Company; 2004.

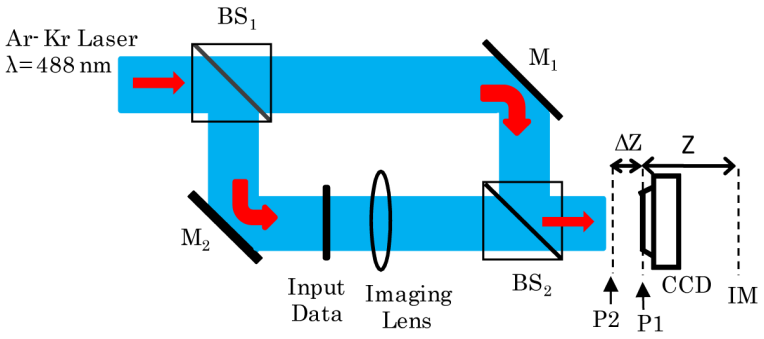


Figure 1.
Experimental set-up for recording in-line digital holograms. BS's, beam splitters; M's, mirrors; P1 and P2, recording planes; IM, image plane.

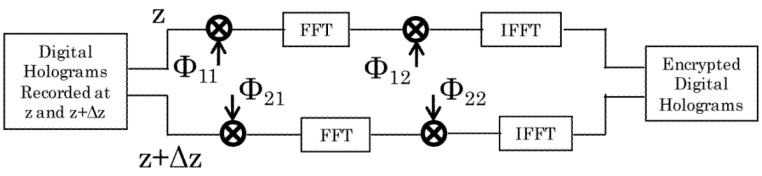


Figure 2.
Dual-channel DRPE encryption of recorded holograms. Φ's are RPMs, FFT and IFFT are Fourier and Inverse Fourier transforms respectively. The procedure is reversed for decryption using corresponding conjugate phase masks.

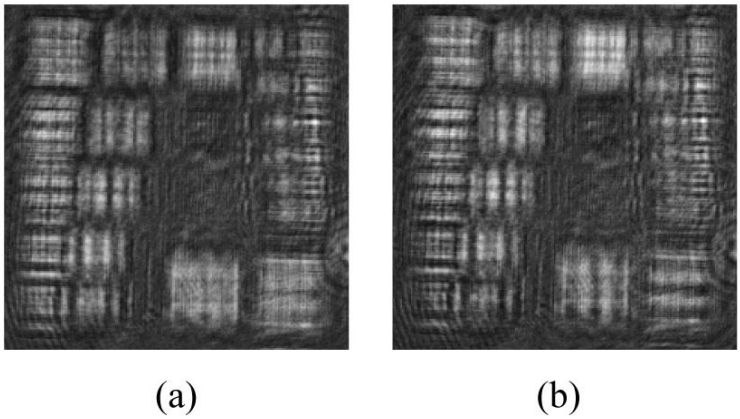


Figure 3.
The two recorded holograms at distances (a) 130.5 mm and (b) 130.6 mm

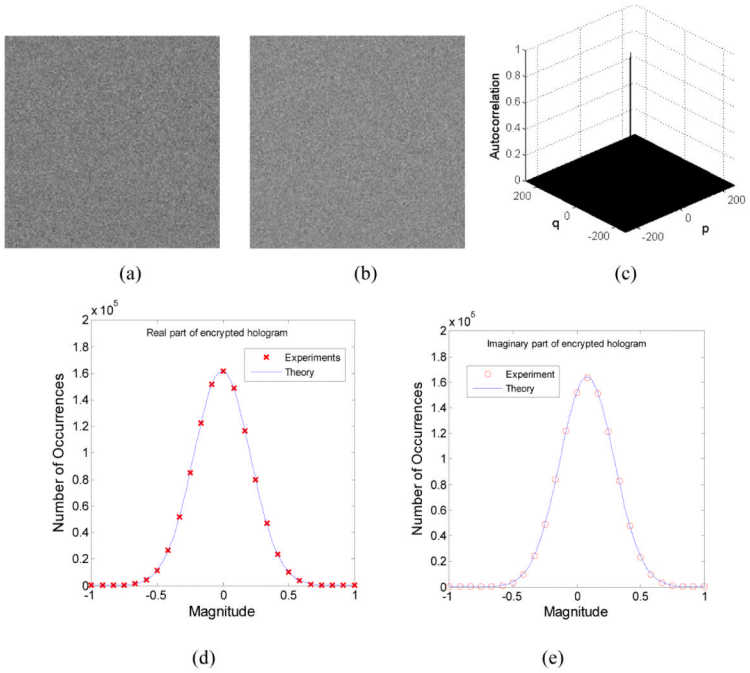


Figure 4.

(a) Real part, (b) Imaginary part, and (c) autocorrelation of the encrypted digital hologram for one of the two channels; histogram of (d) real part, (e) imaginary part of the encrypted digital hologram

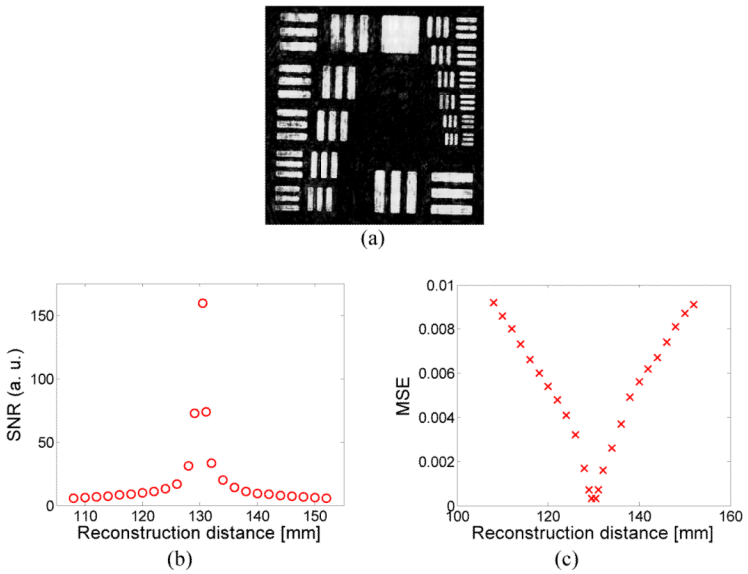
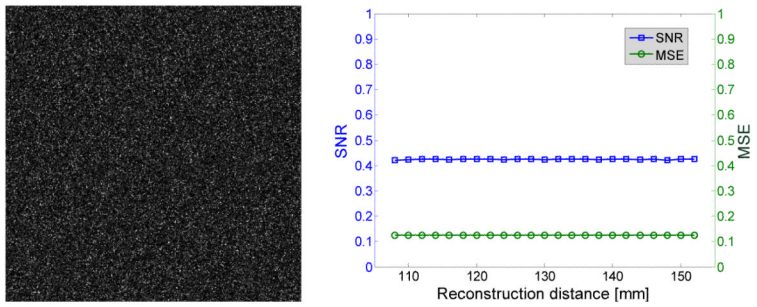


Figure 5.
(a) Reconstructed image using the correct system parameters; (b), (c) SNR and MSE versus reconstruction distance, respectively.



(a) (b)

Figure 6.
(a) Reconstructed image through blind decryption (SNR=0.42 and MSE=0.12); (b), (c) SNR and MSE versus reconstruction distance, respectively.

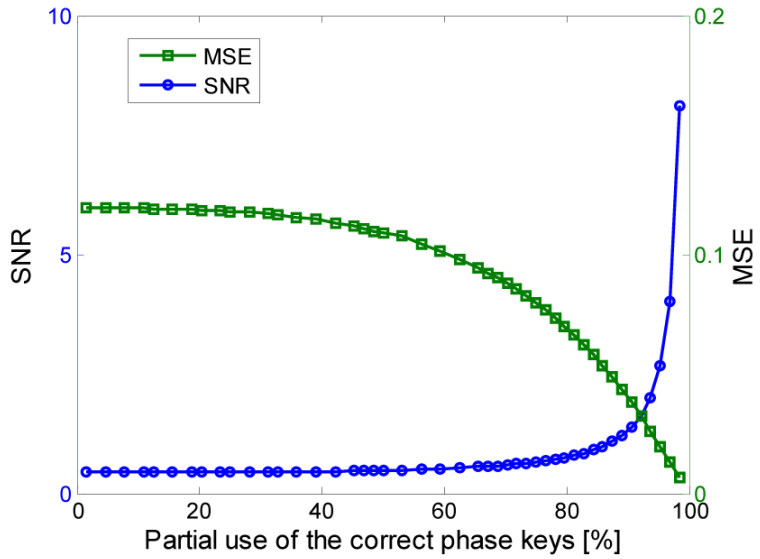
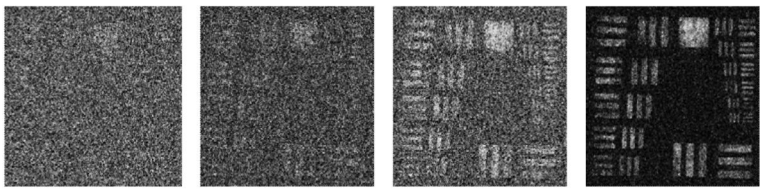


Figure 7.
SNR and MSE versus percentage of the correct phase keys used in the decryption process.



(a) (b) (c) (d)

Figure 8.
Reconstructed object when the portion of the correct phase keys used is (a) 25%, MSE= 0.12; (b) 50%, MSE= 0.11; (c) 75%, MSE= 0.08; and (d) 90%, MSE= 0.03.

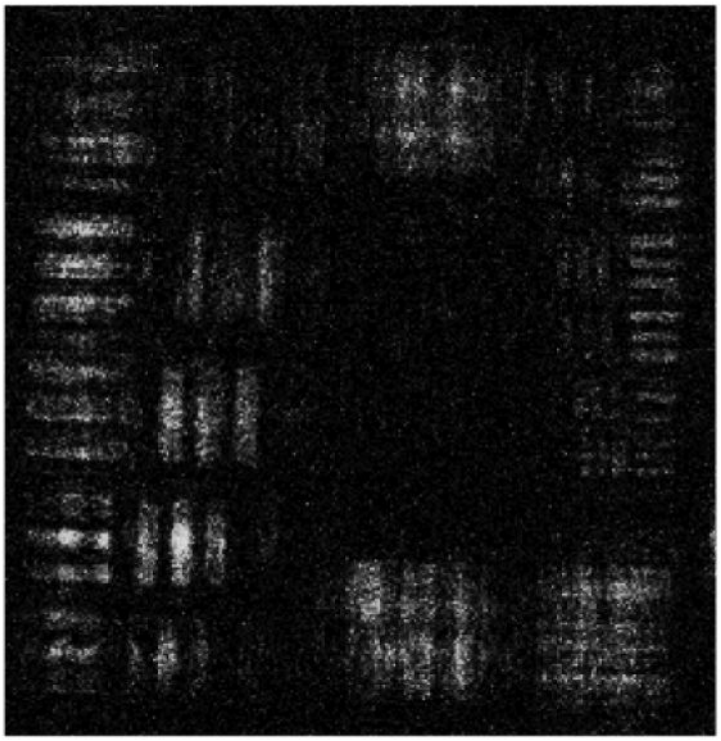


Figure 9.
Decrypted image with correct phase masks for one of the channels. SNR= 0.55 and MSE=0.096.

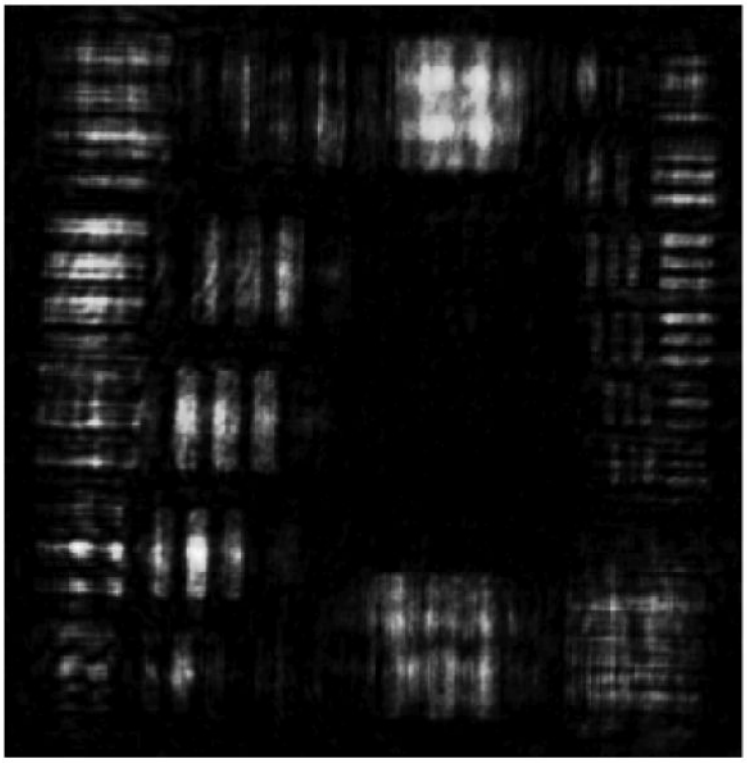


Figure 10.
Reconstructed image considering Δz=0.15 mm during reconstruction. Correct Δz is 0.1 mm.