Wavelength multiplexing multiple-image encryption using cascaded phase-only masks in Fresnel transform domain

Hsuan T. Chang
Photonics and Information Laboratory, Department of Electrical Engineering, National Yunlin University of Science and Technology, Douliu Yunlin, 64002 Taiwan

Hone-Ene Hwang*
Department of Electronic Engineering, Chung Chou Institute of Technology, Yuan-lin, 510 Taiwan

Cheng-Ling Lee
Department of Electro-Optical Engineering, National United University, Miaoli, 360, Taiwan

Mn-Ta Lee
Department of Electronic Engineering, Kao Yuan University, Kaohsiung, Taiwan

**Corresponding author: n741@ms26.hinet.net*

A method of wavelength multiplexing based on a modified Gerchberg-Saxton algorithm (MGSA) and a cascaded phase modulation scheme in the Fresnel transform domain is proposed to reduce the crosstalk in the multiple-image-encryption framework. First, each plain image is encoded as to a complex function by using the MGSA. Next, the phase components of the created complex functions are multiplexed with different wavelength parameters, and then are modulated before being combined together as a phase only function (POF), which is recorded in the first phase-only mask (POM). Finally, the second POM is generated by applying the MGSA again on the amplitude derived from the summation of total created complex functions. Simulation results show that the crosstalk between multiplexed images has been significantly reduced compared with an existing similar method [19]. Therefore, the multiplexing capacity in encrypting multiple grayscale images can be increased accordingly.

OCIS codes: (100.5070) Phase retrieval; (100.3010) Image reconstruction techniques; (060.4785) Optical security and encryption;

1. Introduction

Recently, optical image encryption techniques have played an important role in optical information processing area. Many algorithms and architectural implementations for optical image encryption have been proposed for its multi-parameter selection, high speed, and high parallelism in various applications [1-6]. Since Réfrégier and Javidi first proposed the double random phase encoding (DRPE) algorithm in 1995 [1], the subsequent optical encryption methods based on the Fourier transform (FT) [1], Fresnel transform (FrT) [7, 8], or fractional Fourier transform (FrFT) [9-11] all focused on encoding information using this algorithm. Only the correct phase keys and system parameters can recover the plain image in decryption. Since DRPE has been prevailed with much interest, many studies focused on the related applications [1-12]. The architecture of DRPE in optical image encryption technique uses two random phase keys: one is placed in the input domain and the other is in the Fourier domain. If the two random phase keys are generated by using two statistically independent functions and become two noise-like distributions, the encrypted image can also be as random as stationary white noise. The major advantage of DRPE is that it can be easily implemented with a 4-f optical architecture.

After that, Wang et al. [4] proposed an alternative approach that iteratively encodes the original image into a phase-only mask (POM) in the Fourier plane of a 4-f correlator. This method was modified by Li et al. [13] to encrypt the image into a single POM in the input plane for the sake of convenient arrangement in applications, and by Chang et al. [14] into two POMs in both planes for higher recovered quality and security. The computer generated POM(s) can also be used as the key(s) of the security system. Instead of placing one of POMs in the Fourier plane, Situ and Zhang developed a lensless optical image encryption method in which the second POM can be located at any position in the Fresnel plane [7, 15] and thus can remove the requirement of lenses in the 4-f Fourier optical system. It is difficult for intruders to directly

retrieve the phase distribution of the key(s) because of the property of its novel encoding algorithms [7, 15].

Compared with previous studies, the technique that iteratively encodes the original image into a POM-based system has three main significant advantages: First, it is lensless and therefore can minimize the number of optical components such as lenses. Second, except for the native property of random noise-like distribution functions encoded in POMs which can serve as the main keys, two additional keys (wavelength and position parameters) can consequently achieve higher security. Finally, the encrypted data can be directly transmitted via communication channels and then the decryption process can be achieved by using the correct wavelength and the position parameters at the legitimate receiver.

In addition to single image encryption, the multiple-image case has been developed as well. Many studies have been exploited for multiple-image optical encryption. For example, the schemes of random phase matching [16], spread-space spread-spectrum multiplexing [17], and multichannel encryption [18], etc. Recently, Situ and Zhang proposed two optical multiple-image multiplexing methods which employed the techniques of wavelength and position multiplexing [19, 20]. Although the architecture can be easily implemented, however, the annoy crosstalk exists inevitably in the decrypted results. Thus the number of total encrypted images is limited. Hence Situ and Zhang did not suggest encrypting multiple grayscale images in their methods since the quality of the decrypted images will be worse than that of binary images due to the obvious crosstalk [19, 20].

In our previous study [25], a method of wavelength multiplexing for the multiple-image encryption based on the modified Gerchberg-Saxton algorithm (MGSA) [24] is proposed to solve the above problems. In this paper, we propose a new system architecture in which one

more POM is utilized in the Fresnel transform domain to increase the security level. In addition to only using the phase function retrieved from the MGSA, the amplitude and phase information of the light field propagated from the other phase function under a given distance in between is also considered. Therefore, much more information is required to correctly decrypt the multiplexed images and thus the system security can be enhanced.

The rest of this paper is organized as follows: Section 2 briefly introduces the MGSA, which is an important primitive in the proposed method. The proposed method is described in Section 3. The numerical computer simulation is given in Section 4. Finally, Section 5 concluded this paper.

2. Modified Gerchberg-Saxton Algorithm (MGSA)

The conventional Gerchberg-Saxton algorithm (GSA) is generally employed to reconstruct the lost phases if the corresponding intensities at their respective optical planes (for example, corresponding to the spatial and Fourier domains) are known [21-23]. The measured intensity in the Fourier domain must be the FT of the known intensity in the object domain. It is often sufficient to retrieve the phase distribution from one of the two optical planes via GSA because the phase distribution on the other plane can be obtained by performing a FT on the signal in the retrieved plane. The GSA algorithm iteratively performs the FTs back and forth between the object and the Fourier domains. The GSA was often applied to the applications of not only the two-dimensional signals but also the one-dimensional ones.

Rather than recovering the lost phase information between two intensities on the spatial and Fourier domains, we have adopted the MGSA [24, 25] based on the GSA with intent to generate pure phase distributions $\psi_H(x_2, y_2)$ and $\psi_T(x_1, y_1)$ with a faster iteration process from the two independent prescribed intensities $H(x_2, y_2)$ and $T(x_1, y_1)$, as shown in Fig. 1. The difference

between the GSA and MGSA is that at the beginning of the iteration process, the source intensity $H(x_2, y_2)$ in the MGSA has not to be constrained to the intensity of inverse Fourier transform (IFT) of the target image $T(x_1, y_1)$, while in the GSA the IFT relationship must be obeyed. For example, an arbitrary image $H(x_2, y_2)$ and a prescribed intensity $T(x_1, y_1)$ can be chosen as the host and target images, respectively, in the data embedding procedure. That is, the target image $T(x_1, y_1)$ is not obliged to be defined as the FT of the image $H(x_2, y_2)$. Furthermore, instead of using the FT and IFT, the MGSA can also be performed by using the FrT and IFrT [24, 25], respectively. Then involving the two images $T(x_1, y_1)$ and $H(x_2, y_2)$ into the MGSA, a desired approximation image $\hat{T}(x_1, y_1)$ can be obtained purposely. When the required correlation/similarity between the target image $T(x_1, y_1)$ and the approximation image $\hat{T}(x_1, y_1)$ is reached (i.e., the correlation coefficient ρ achieves a predefined value), the resultant phase distributions $\psi_H(x_2, y_2)$ and $\psi_G(x_1, y_1)$ in the input and output domains, can be obtained [24], respectively. Consequently, any two arbitrary and independent images can be imposed on building the FT and IFT (or FrT and IFrT) relationships in the MGSA. The mathematical derivation of Fig. 1 in the optical FrT domain is

$$\begin{aligned}
&\mathrm{FrT}\left\{ H(x_2, y_2)\exp\left[j\psi_h(x_2, y_2)\right]; \lambda; z \right\} \\
&= \frac{\exp(\frac{j2\pi z}{\lambda})}{j\lambda z} \iint H(x_2, y_2)\exp[j\psi_h(x_2, y_2)]\exp\left\{\frac{j\pi}{\lambda z}\left[(x_2 - x_1)^2 + (y_2 - y_1)^2\right]\right\} \mathrm{d}x_2 \mathrm{d}y_2 \qquad (1) \\
&= \hat{T}(x_1, y_1)\exp\left[j\psi_G(x_1, y_1)\right],
\end{aligned}$$

where λ is the wavelength of the incident plane wave and z represents the distance between the input spatial domain (x_2, y_2) and output frequency domain (x_1, y_1). If a POF $\psi_H(x_2, y_2)$ is

required, the image constraint of a unity amplitude ($H(x_1, y_1) = 1$) is used in the MGSA to generate the phase distribution $\psi_G(x_1, y_1)$, which is then written into a POM. On the other hand, the phase distribution $\psi_T(x_1, y_1)$ contributes one of the components, which are then written into the other POM. The detailed discussions will be given in the next section.

3. The proposed method

The optical architecture of the lensless Fresnel diffraction is employed in the proposed system. Figure 2 shows the system configuration of the proposed double-POF-based multiple-image encryption method, in which one POF is located between the input (x_2, y_2) and filter (x_1, y_1) planes and the other is located between the filter (x_1, y_1) and output (x_0, y_0) planes. As the coherent plane wave with the wavelength λ_n is incident from the left-hand side of POM_2, the corresponding image $\hat{g}_n^{\lambda}(x_0, y_0)$ will be obtained in a specific position in the output (x_0, y_0) plane after the light wave passing through POM_1. In retrieving the POFs in the lensless Fresnel diffraction scheme, the MGSA based on the FrT [24, 25] is used. To reduce the annoying crosstalk [19, 20] in the encryption of grayscale or color images, the retrieved phase functions for all the encrypted images are then modulated to synthesis the two POFs.

The proposed method for multiple-image encryption with wavelength multiplexing is implemented by using the cascaded POFs recorded on the two POMs, respectively. Figure 3 illustrates the systematic block diagram of the proposed method. First, N individual target images $\{ g_n(x_0, y_0) \mid n = 1, 2, 3, \ldots, N\}$ is encrypted as to its corresponding phase functions $\{ \psi_{\lambda_n}(x_1, y_1) \mid n = 1, 2, 3, \ldots, N\}$ in accordance with different wavelengths $\{ \lambda_n, n = 1, 2, 3, \ldots, N\}$ of the incident plane wave based on the MGSA. That is, each phase function $\psi_{\lambda_n}(x_1, y_1)$ satisfies

$$\mathrm{FrT}\left\{\exp\left[j\psi_{\lambda_n}(x_1,y_1)\right];\lambda_n;z_1\right\}=\hat{g}_n^{\lambda}(x_0,y_0)\exp\left[j\psi_{\hat{g}_n}^{\lambda}(x_0,y_0)\right], \tag{2}$$

where $\psi_{\hat{g}_n}^{\lambda}(x_0,y_0)$ is the accompanied phase term for each image $g_n(x_0, y_0)$. These N wavelength-specific phase functions, $\{\psi_{\lambda_n}(x_1,y_1) \mid n = 1, 2, 3,\ldots, N\}$ can be summed and then recorded together into a single POF. Each target image $g_n(x_0, y_0)$ can then be extracted or recovered from the POF as the approximation image $\hat{g}_n^{\lambda}(x_0,y_0)$ in Eq. (2). However, the crosstalk between a specifically reconstructed image $\hat{g}_k^{\lambda}(x_0,y_0)$ and the other reconstructed images $\{\hat{g}_n^{\lambda}(x_0,y_0) \mid n = 1, 2, 3,\ldots, N, n\neq k\}$ makes the error perceivable, even the wavelength key λ_k for deciphering is correct. To reduce the annoying crosstalk, therefore, the approximation images $\{\hat{g}_n^{\lambda}(x_0,y_0) \mid n = 1, 2, 3,\ldots, N\}$ are spatially translated to different positions by using the phase modulation property of FrT:

$$\mathrm{FrT}\{\exp[j\psi'_{\lambda_n}(x_1,y_1)];\lambda_n;z_1\}=\hat{g}_n^{\lambda}(x_0-\mu_0,y_0-\nu_0)\exp[j\omega(x_0,y_0)], \tag{3}$$

where

$$\psi'_{\lambda_n}(x_1,y_1)=\psi_{\lambda_n}(x_1,y_1)+\frac{2\pi(\mu_n x_1+\nu_n y_1)}{\lambda_n z_1}, \tag{4}$$

and $\omega(x_0,y_0)$ is the accompanied phase term, and μ_n and ν_n denote the respective shifting distances of the n^{th} constructed image $\hat{g}_n^{\lambda}(x_0,y_0)$ in the x_0 and y_0 directions, respectively, at the output plane. The crosstalk can be significantly reduced with a proper arrangement of the shifting distance μ_n and ν_n. For example, the differences between two consecutive distances (μ_i and μ_{i+1} or ν_i and ν_{i+1}) should be greater than the width D_w and the height D_h of the target image.

To synthesize a POF that can achieve multiple-image encryption, the phase functions $\{\psi'_{\lambda_n}(x_1,y_1) \mid n=1,2,3,...,N\}$ obtained from Eq. (4) are summed to yield the total phase function

$\exp\left[j\psi_{\mathrm{T}}^{\lambda}(x_1, y_1) \right]$:

$$A_{\mathrm{T}}^{\lambda}(x_1, y_1)\exp\left[j\psi_{\mathrm{T}}^{\lambda}(x_1, y_1) \right] = \sum_{n=1}^{N} \exp\left[j\psi'_{\lambda_n}(x_1, y_1) \right], \tag{5}$$

where $A_{\mathrm{T}}^{\lambda}(x_1, y_1)$ denotes the total amplitude of the summation $\sum_{n=1}^{N} \exp\left[j\psi'_{\lambda_n}(x_1, y_1) \right]$. Next, to increase the security of the multiple-image multiplexing encryption system, the other POF is written into POM_2. Therefore, the amplitude $A_{\mathrm{T}}^{\lambda}(x_1, y_1)$ is encoded into the phase function $\phi(x_2, y_2)$ by again using the MGSA with setting the condition $H(x_2, y_2)=1$ and with applying the IFrT on the total amplitude $A_{\mathrm{T}}^{\lambda}(x_1, y_1)$. The phase function $\phi(x_2, y_2)$ satisfies

$$\mathrm{FrT}\left\{ \exp\left[j\phi(x_2, y_2) \right]; \lambda_n; z'_n \right\} = \hat{A}_{\mathrm{T}}^{\lambda}(x_1, y_1) \exp\left[j\varphi(x_1, y_1) \right], \tag{6}$$

where λ_n denotes the N different wavelengths and z'_n represents the N different positions between the input and filter planes. If the product of the wavelength and distance parameters $\lambda_n z'_n$ is a fixed value, the same result will be obtained from Eq. (6). That is, different wavelengths λ_n will lead the Eq. (6) to be the same result $\hat{A}_{\mathrm{T}}^{\lambda}(x_1, y_1)\exp\left[j\varphi(x_1, y_1) \right]$ under the different positions z'_n if the condition $\lambda_n z'_n = \text{constant}$ holds.

In the final step, the phase functions $\phi(x_2, y_2)$ and $-\varphi(x_1, y_1) + \psi_{\mathrm{T}}^{\lambda}(x_1, y_1)$ are recorded into POM_2 and POM_1, respectively. The multiple-image decryption process for the case of wavelength multiplexing under a specific wavelength λ_n (shown in Fig. 3) can be expressed as

$$
\begin{aligned}
&\left|\mathrm{FrT}\left(\mathrm{FrT}\left\{\exp\left[j\phi(x_2,y_2)\right];\lambda_n;z_n'\right\}\exp\left[-j\varphi(x_1,y_1)+j\psi_{\mathrm{T}}^{\lambda}(x_1,y_1)\right];\lambda_n;z_1\right)\right| \\
&=\left|\mathrm{FrT}\left\{\hat{A}_{\mathrm{T}}^{\lambda}(x_1,y_1)\exp\left[j\varphi(x_1,y_1)\right]\exp\left[-j\varphi(x_1,y_1)+j\psi_{\mathrm{T}}^{\lambda}(x_1,y_1)\right];\lambda_n;z_1\right\}\right| \\
&=\left|\mathrm{FrT}\left\{\hat{A}_{\mathrm{T}}^{\lambda}(x_1,y_1)\exp\left[j\psi_{\mathrm{T}}^{\lambda}(x_1,y_1)\right];\lambda_n;z_1\right\}\right| \\
&=\left|\mathrm{FrT}\left\{\sum_{n=1}^{N}\exp\left[j\psi_{\lambda_n}(x_1,y_1)+\frac{j2\pi(\mu_n x_1+\nu_n y_1)}{\lambda_n z}\right];\lambda_n;z_1\right\}\right| \\
&=\left|\mathrm{FrT}\left\{\sum_{n=1}^{N}\exp\left[j\psi_{\lambda_n}'(x_1,y_1)\right];\lambda_n;z_1\right\}\right| \\
&=\left|\hat{g}_n^{\lambda}(x_0-\mu_n,\,y_0-\nu_n)\exp\left[j\omega(x_0,y_0)\right]+n_{\lambda_n}(x_0,y_0)\right| \\
&\approx \hat{g}_n^{\lambda}(x_0-\mu_n,\,y_0-\nu_n)+\left|n_{\lambda_n}(x_0,y_0)\right|,
\end{aligned}
\tag{7}
$$

where $n_{\lambda_n}(x_1,y_1)$ represents the crosstalk, which is located at the coordinate (x_0,y_0) and is derived from deciphering the remaining images with an incorrect wavelength key λ_n. Note that the approximation holds if the two terms are spatially separated enough. That is, the consecutive distances in both the horizontal or vertical directions should be at least greater than the width and height of the target image, respectively. The proposed method based on Eq. (7) can recover the encrypted images, $\{\hat{g}_n^{\lambda}(x_0,y_0)\,|\,n=1,2,3,...,N\}$, with different wavelengths and spatial translations (μ_n,ν_n) to artfully avoid the crosstalk $n_{\lambda_n}(x_0,y_0)$.

4. Simulation results

Computer simulations are performed to verify the proposed method. Figure 4 shows nine original grayscale images of size 64×64 pixels. The size of the POFs is $5\ \mathrm{mm}\times5\ \mathrm{mm}$ in the

simulation. In the proposed wavelength multiplexing scheme, a fixed position $z_1 = 0.25$ m, variable wavelengths $\lambda_n = 400+20n$ nm , and the fixed product value $\lambda_n z_n' = 1.5\times10^{-7}$ m^2 , $n = 1,\ldots,9$, are adopted. Figures 5(a) and 5(b) show the noise-like POFs recorded in POM_1 and POM_2 , respectively, which are determined by using Eqs. (2)-(6).

Consider the case of choosing the wavelength $\lambda_3 = 460$ nm in the input plane. Figures 6(a) and 6(b) show the entire decrypted result in the reconstruction plane and the magnified version of the image $\hat{g}_3^{\lambda}(x_1, y_1)$ corresponding to the original target image $g_3(x_1, y_1)$ in Fig. 4, respectively. As to another case of using the wavelength $\lambda_6 = 520$ nm , Figs. 6(c) and 6(b) show the entire decrypted result in the reconstruction plane and the magnified version of the image $\hat{g}_6^{\lambda}(x_1, y_1)$ corresponding to the original image $g_6(x_1, y_1)$ in Fig. 4, respectively. Comparing the original target images $g_3(x_1, y_1)$ and $g_6(x_1, y_1)$ to the reconstructed images $\hat{g}_3^{\lambda}(x_1, y_1)$ and $\hat{g}_6^{\lambda}(x_1, y_1)$ shown in Figs. 6(b) and 6(d), the correlation coefficients are ρ=0.887 and ρ=0.892, respectively. The shift amounts are designated to be (μ_n, ν_n) = (αD_w, βD_h), where α and β are integers within the range [–3, 3] and D_w and D_h are the width and height of the original target image, respectively.

In addition to the grayscale images shown in Fig. 6(a), the binary images are also used to test the proposed method. Figure 7 (a) depicts nine test binary images used in the proposed multiple-image multiplexing encryption. Figures 7(b) and 7(e) show the original binary images $g_3(x_1, y_1)$; and $g_6(x_1, y_1)$, respectively. The entire decrypted images in the reconstruction planes with the wavelengths $\lambda_3 = 460$ nm and $\lambda_6 = 520$ nm are shown in Figs. 7(c) and 7(f), respectively. (d) The enlarged decrypted binary images $\hat{g}_3^{\lambda}(x_1, y_1)$ and $\hat{g}_6^{\lambda}(x_1, y_1)$ corresponding to the original binary

images in Figs. 7(b) and 7(e) are shown in Figs. 7(d) and 7(g), respectively. Comparing the original binary images $g_3(x_1, y_1)$ and $g_6(x_1, y_1)$ to the reconstructed images $\hat{g}_3^{\lambda}(x_1, y_1)$ and $\hat{g}_6^{\lambda}(x_1, y_1)$ in Figs. 7(d) and 7(g), the corresponding correlation coefficients are ρ =0.973 and ρ =0. 975, respectively, which are higher than that of the reconstructed grayscale images in Figs. 6(b) and 6(d).

Figure 8 shows the comparison result of the correlation coefficient between the original and the decrypted images for the proposed method and the method in Ref. [19], which is also a wavelength multiplexing scheme. Higher correlation coefficients are obtained in the proposed method for both the grayscale and binary images. The superiority of the proposed method is especially obvious when a large number of images are multiplexed. Therefore, the proposed method significantly reduces the crosstalk and hence achieves higher storage capacity (a larger number *N* at specified crosstalk).

The maximum limit of multiplexing the encrypted images actually is dependent on the acceptable maximum crosstalk or the required minimum correlation coefficient in real applications. As shown in Fig. 8, if the minimum correlation coefficient is chosen as 0.95, the numbers of the maximum encrypted binary and grayscale images are nine and six, respectively. On the other hand, the system parameters such as the distance z_1 between two POMs, the wavelength difference $\Delta\lambda$, and the size of the encrypted images could affect the crosstalk performance as well. Some studies also regarding to the capacity of multiplexed images were presented in Refs. [26-28]. In addition to the system parameters used in these methods, the capacity may also depend on (1) the size of multiplexed images; (2) the optical architecture used; (3) the device specification of optical components; (4) the number and the arrangement of employed phase functions. Obviously, the determination of the capacity in the proposed image

multiplexing system would be a complicated issue while simultaneously taking account on all the factors above. A thoughtful investigation will conducted in our future work.

5. Conclusion

In conclusion, the proposed method is a novel wavelength multiplexing algorithm based on the cascaded POF architecture and significantly reduces the crosstalk for multiple-image encryption. In addition, a lensless optical system based on the FrT could be constructed accordingly to be advantageous of compactness and simplicity. Besides, the increasing of the multiple-image multiplexing encryption security is also achieved in this study. Optical experiments will be soon conducted in our future research.

Acknowledgements

This study was supported by National Yunlin University of Science and Technology, Chung Chou Institute of Technology, and the National United University. It was supported also by the National Science Council of Taiwan under contracts NSC 98-2221-E-235-002-MY2. The authors also thank the reviewers for their thoughtful and helpful comments.

Corresponding author H.-E. Hwang can be reached by phone at 886-4-8311498, ext. 2247; fax at 886-4-8314515; e-mail at n741@ms26.hinet.net or hiko@dragon.ccut.edu.tw.

References

1. P. Refregier and B. Javidi, “Optical image encryption using input and Fourier plane random phase encoding,” Opt. Lett. **20,** 767-769 (1995).
2. C. H. Yeh, H. T. Chang, H. C. Chien, and C. J. Kuo, “Design of cascaded phase keys for hierarchical security system,” Appl. Opt. **41**, 6128-6134 (2002).
3. G. H. Lin, H. T. Chang, W. N. Lai, and C. H. Chuang, “Public-key-based optical image cryptosystem with data embedding techniques,” Opt. Eng. **42**, 2331-2339, (2003).
4. R. K. Wang, I. A. Watson, and C. Chatwin, “Random phase encoding for optical security,” Opt. Eng. **35,** 2464-2469 (1996).
5. Y.C. Chang, H. T. Chang, and C.J. Kuo, “Hybrid image cryptosystem based on dyadic phase displacement in the Fourier domain,” Opt. Commun. **236**, 245-257 (2004).
6. H. T. Chang, “Image encryption using separate amplitude-based virtual image and iteratively-retrieved phase information,” Opt. Eng. **40**, 2165-2171 (2001).
7. G. Situ and J. Zhang, “Double random-phase encoding in the Fresnel domain,” Opt. Lett. **29,** 1584-1586 (2004).
8. H. E. Hwang and P. Han, “Fast algorithm of phase masks for image encryption in the Fresnel domain,” J. Opt. Soc. Am. A, 23, 1870-1874 (2006).
9. G. Unnikrishnan, J. Joseph, and K. Singh, “Optical encryption by double-random phase encoding in the fractional Fourier domainB,” Opt. Lett. 25, 887–889 (2000).
10. S. T. Liu, Q. L. Mi, and B. H. Zhu, “Optical image encryption with multistage and multichannel fractional Fourier-domain filtering,” Opt. Lett. **26,** 1242-1244 (2001).
11. Y. Zhang, C. H. Zheng, and N. Tanno, “Optical encryption based on iterative fractional Fourier transform,” Opt. Commun. **202,** 277-285 (2002).

12. G. Situ, J. Zhang, “A cascaded iterative Fourier transform algorithm for optical security applications,” Optik **114,** 473-477 (2004).
13. Y. Li, K. Kreske, and J. Rosen, “Security and encryption optical systems based on a correlator with significant output images,” Appl. Opt. **39**, 5295–5301 (2000).
14. H. T. Chang, W. C. Lu, C. J. Kuo, “Multiple-Phase Retrieval for Optical Security Systems by Use of Random-Phase Encoding,” Appl. Opt. **41,** 4815-4834 (2002).
15. G. Situ and J. Zhang, “A lensless optical security system based on computer-generated phase only masks,” Opt. Commun. **232,** 115-122 (2004).
16. M. Z. He, L. Z. Cai, Q. Liu, X. C. Wang and X. F. Meng, “Multiple image encryption and watermarking by random phase matching,” Opt. Commun. **247,** 29-37 (2005).
17. B. M. Hennelly, T. J. Naughton, J. McDonald, J. T. Sheridan, G. Unnikrishnan, D. P. Kelly and B. Javidi, “Spread-space spread-spectrum technique for secure multiplexing,” Opt. Lett. **32,** 1060-1066 (2007).
18. D. Amaya, M. Tebaldi, R. Torroba, and N. Bolognini, “Multichanneled encryption via a joint transform correlator architecture,” Appl. Opt. **47,** 5903-5907 (2008).
19. G. Situ and J. Zhang, “Multiple-image encryption by wavelength multiplexing,” Opt. Lett. **30,** 1306-1308 (2005).
20. G. Situ and J. Zhang, “Position multiplexing for multiple-image encryption,” J. Opt. A: Pure Appl. Opt. **8,** 391-397 (2006).
21. R. W. Gerchberg and W. O. Saxton, “Phase determination for image and diffraction plane pictures in the electron microscope,” Optik **34,** 275–284 (1971).
22. R. W. Gerchberg and W. O. Saxton, “A practical algorithm for the determination of phase from image and diffraction plane pictures,” Optik **35,** 237–246 (1972).

23. H. E. Hwang and P. Han, “Signal reconstruction algorithm based on a single intensity in the Fresnel domain,” Opt. Express **15,** 3766-3776 (2007).
24. H. E. Hwang, H. T. Chang, and W. N. Lie, “Fast double-phase retrieval in Fresnel domain using modified Gerchberg-Saxton algorithm for lensless optical security systems,” Opt. Express **17,** 13700-13710 (2009).
25. H. E. Hwang, H. T. Chang, and W. N. Lie, “Multiple-image encryption and multiplexing using modified Gerchberg-Saxton algorithm and phase modulation in Fresnel transform domain,” Opt. Lett. **34,** 3917–3919 (2009).
26. M. Paturzo, P. Memmolo, L. Miccio, A. Finizio, P. Ferrarro, A. Tulino, and B. Javidi, “Numerical multiplexing and demultiplexing of digital holographic information for remote reconstruction in amplitude and phase,” Opt. Lett. **33**, 2629-2631 (2008).
27. X. F. Meng, L. Z. Cai, Y. R. Wang, X. L. Yang, X. F. Xu, G. Y. Dong, X. X. Shen, H. Zhang, and X. C. Cheng, “Hierarchical image encryption based on cascaded iterative phase retrieval algorithm in the Fresnel domain,” J. Opt. A: Pure Appl. Opt. **9,** 1070 (2007).
28. N. K. Nishchal and T. J. Naughton, “Flexible optical encryption with multiple users and multiple security levels,” Opt. Commun. **284,** 735-739 (2011).

List of figure captions:

Fig. 1: (a) The flow chart of Gerchberg-Saxton algorithm is used for performing phase retrieval if their intensities at their respective optical planes are known; (b) The flow chart of modified Gerchberg-Saxton algorithm.

Fig. 2: Optical multiple-image encryption setup by wavelength multiplexing based on cascaded phase-only masks in the Fresnel transform domain.

Fig. 3: Block diagram of the proposed multiple-image encryption and wavelength multiplexing.

Fig. 4: Nine test grayscale images used in the proposed multiple-image multiplexing encryption.

Fig. 5: (a) The noise-like POF recorded in POM_1. (b) The noise-like POF recorded in POM_2.

Fig. 6: (a) The entire decrypted image with the wavelength $\lambda_3 = 460$ nm in the reconstruction plane; (b) The enlarged decrypted image $\hat{g}_3^{\lambda}(x_1, y_1)$ corresponding to the original image $g_3(x_1, y_1)$ in Fig. 6(a); (c) The entire decrypted image with the wavelength $\lambda_6 = 520$ nm in the reconstruction plane; (d) The enlarged decrypted image $\hat{g}_6^{\lambda}(x_1, y_1)$ corresponding to the original image $g_6(x_1, y_1)$ in Fig. 6(c).

Fig. 7: (a) Nine test binary images used in the proposed multiple-image multiplexing encryption method; (b) The original binary image $g_3(x_1, y_1)$; (c) The entire decrypted binary image with the wavelength $\lambda_3 = 460$ nm in the reconstruction plane; (d) The enlarged decrypted binary image $\hat{g}_3^{\lambda}(x_1, y_1)$ corresponding to the original binary image $g_3(x_1, y_1)$ in Fig. 7(c); (e) The original binary image $g_6(x_1, y_1)$; (f) The entire decrypted binary image with the wavelength $\lambda_6 = 520$ nm in the reconstruction plane; (g) The enlarged decrypted binary image $\hat{g}_6^{\lambda}(x_1, y_1)$ corresponding to the original binary image $g_6(x_1, y_1)$ in Fig. 7(f).

Fig. 8: Comparison between the proposed and Situ's [19] methods in terms of the correlation coefficient.

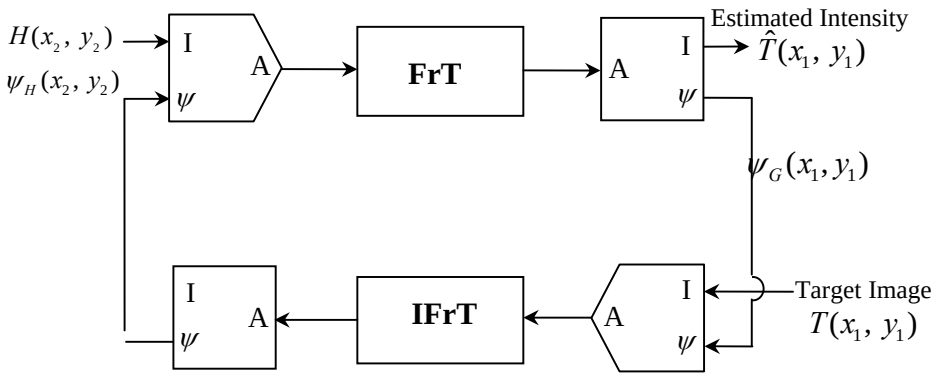

$H(x_2, y_2)$
$\psi_H(x_2, y_2)$
I
A
ψ
FrT
A
I
ψ
Estimated Intensity
$\hat{T}(x_1, y_1)$
$\psi_G(x_1, y_1)$
Target Image
$T(x_1, y_1)$
I
A
ψ
IFrT
A
I
ψ

Fig. 1

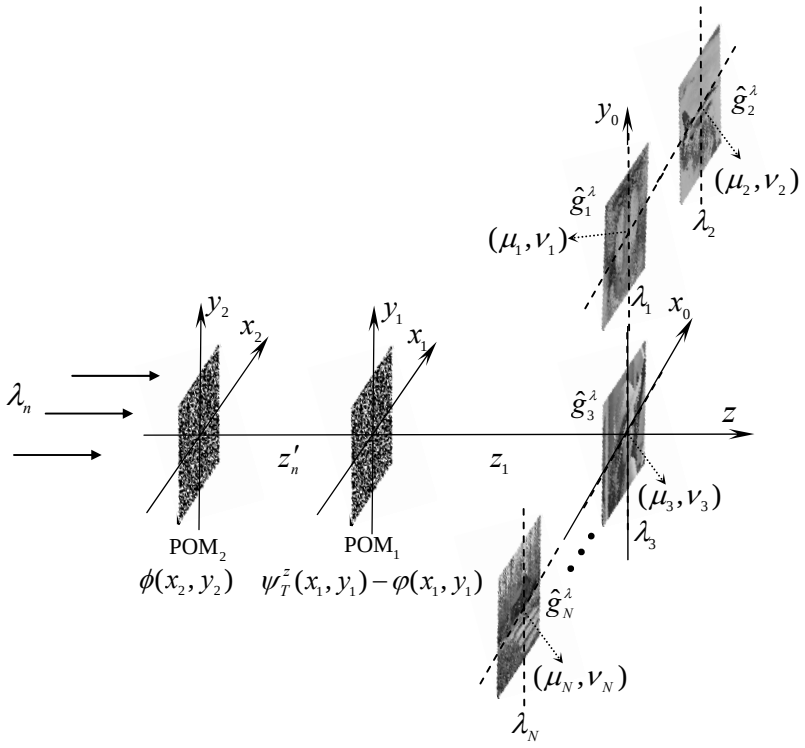

λ_n
y_2
x_2
y_1
x_1
z'_n
z_1
y_0
x_0
z
$\hat{g}_1^{\lambda}$
$\hat{g}_2^{\lambda}$
$\hat{g}_3^{\lambda}$
$\hat{g}_N^{\lambda}$
(μ_1, ν_1)
(μ_2, ν_2)
(μ_3, ν_3)
(μ_N, ν_N)
λ_1
λ_2
λ_3
λ_N
POM$_2$
$\phi(x_2, y_2)$
POM$_1$
$\psi_T^{z}(x_1, y_1) - \varphi(x_1, y_1)$

Fig. 2

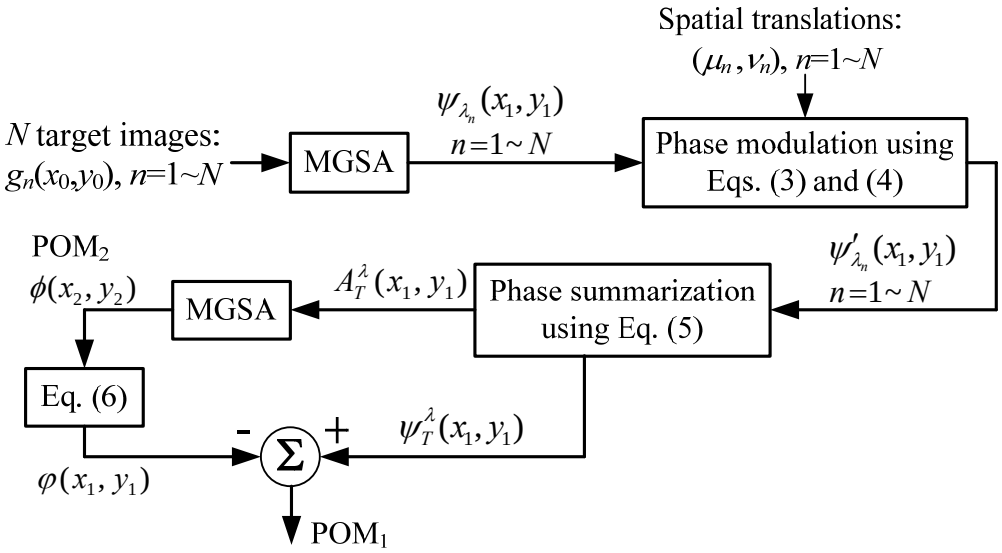
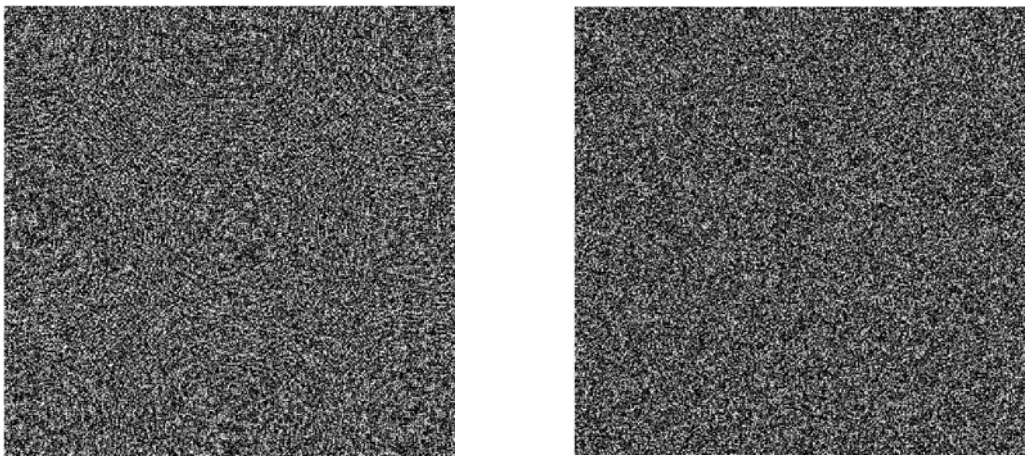

Spatial translations:
(μ_n, ν_n), n=1~N
$\psi_{\lambda_n}(x_1, y_1)$
n=1~N
N target images:
$g_n(x_0, y_0)$, n=1~N
MGSA
Phase modulation using Eqs. (3) and (4)
POM$_2$
$\phi(x_2, y_2)$
MGSA
$A_T^{\lambda}(x_1, y_1)$
Phase summarization using Eq. (5)
$\psi'_{\lambda_n}(x_1, y_1)$
n=1~N
Eq. (6)
-
+
$\psi_T^{\lambda}(x_1, y_1)$
$\varphi(x_1, y_1)$
Σ
POM$_1$

Fig. 3

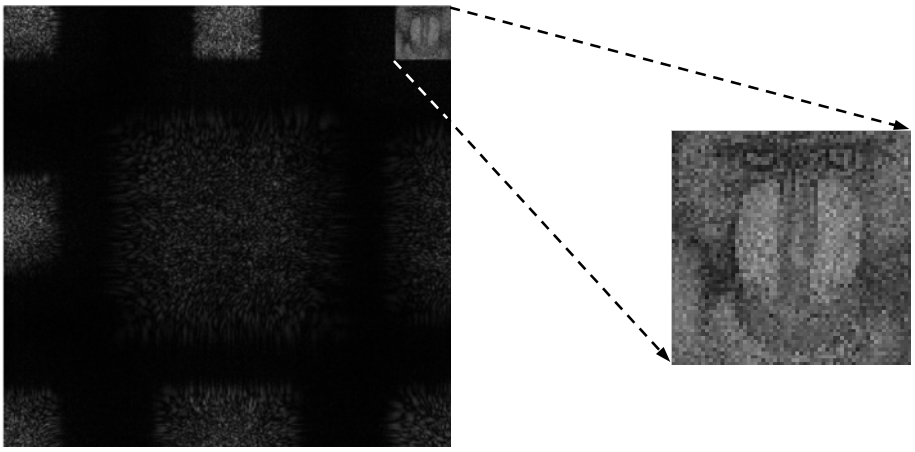

$g_1(x_0, y_0)$
$g_2(x_0, y_0)$
$g_3(x_0, y_0)$
$g_4(x_0, y_0)$
$g_5(x_0, y_0)$
$g_6(x_0, y_0)$
$g_7(x_0, y_0)$
$g_8(x_0, y_0)$
$g_9(x_0, y_0)$

Fig. 4

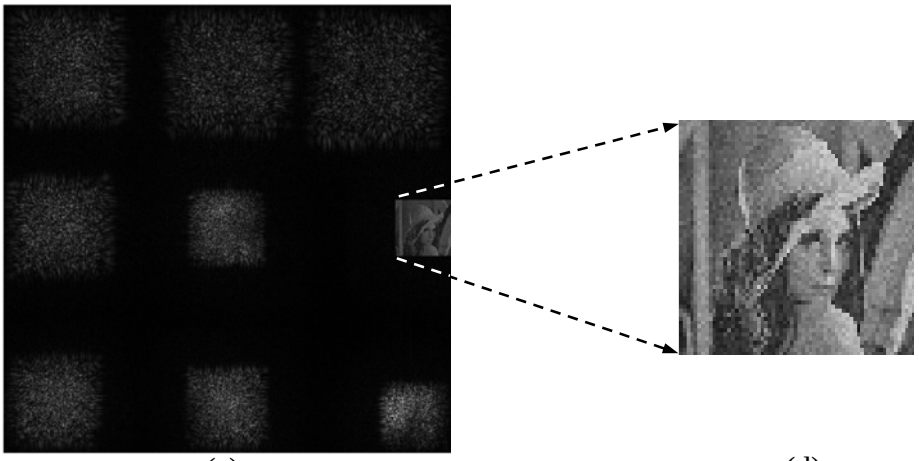


(a) (b)

Fig. 5



(a) (b)



(c) (d)

Fig. 6

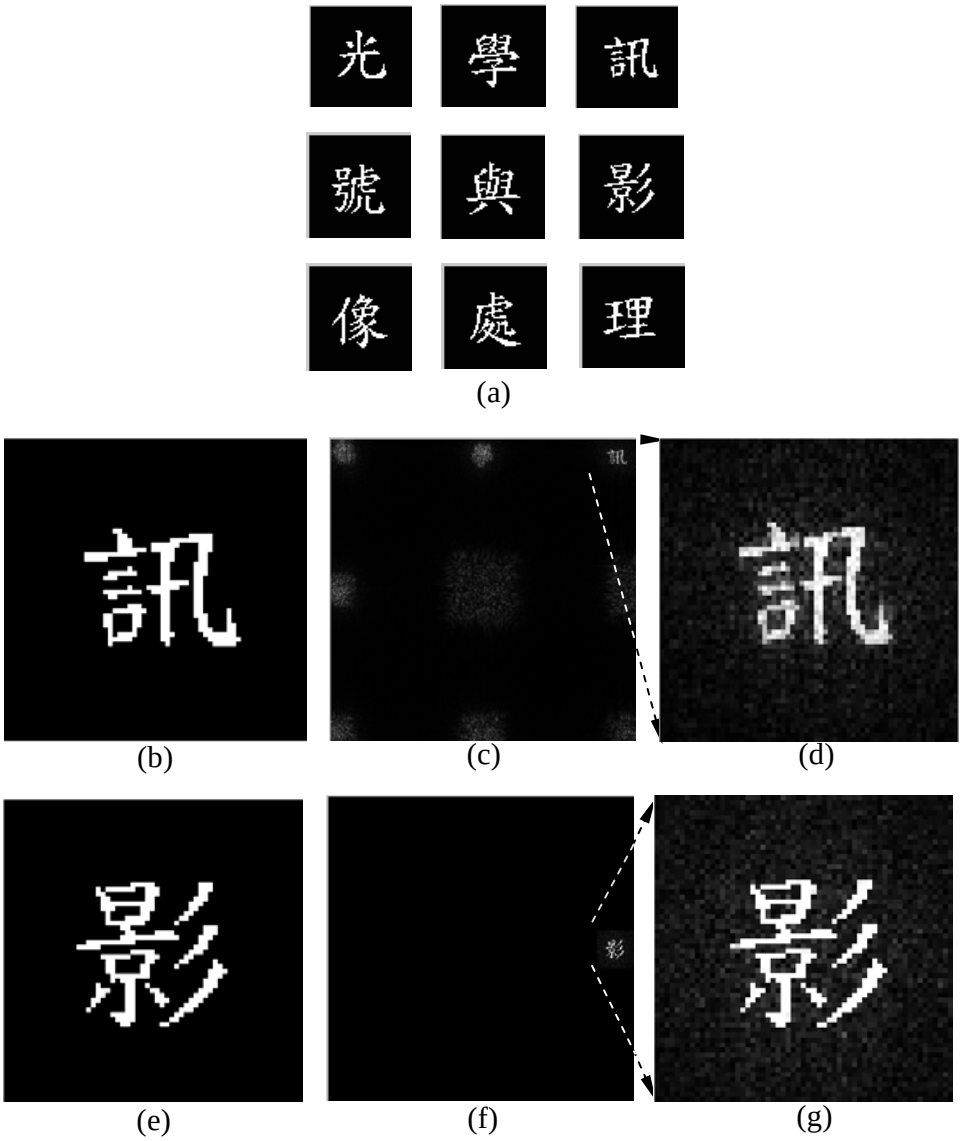


Fig. 7

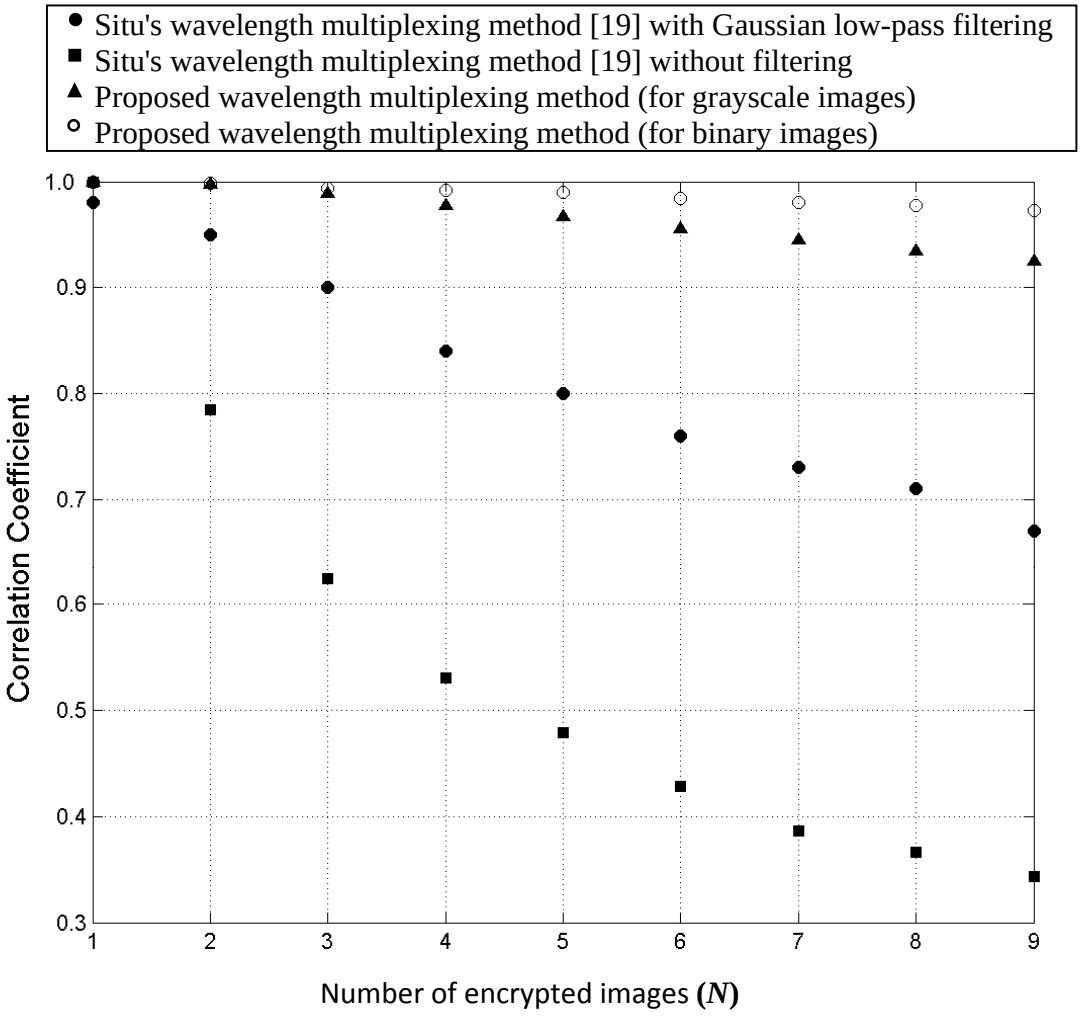

Situ's wavelength multiplexing method [19] with Gaussian low-pass filtering
Situ's wavelength multiplexing method [19] without filtering
Proposed wavelength multiplexing method (for grayscale images)
Proposed wavelength multiplexing method (for binary images)
Correlation Coefficient
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
1
2
3
4
5
6
7
8
9
Number of encrypted images (N)

Fig. 8