Multiple-Image Multiplexing Encryption Based on Modified Gerchberg-Saxton Algorithm and Phase Modulation in Fractional Fourier Transform Domain

Hsuan-Ting Chang[1] and Hone-Ene Hwang[2,*]

[1] Photonics and Information Laboratory, Department of ElectricalEngineering, National Yunlin University of Science and Technology, Douliu Yunlin, 64002 Taiwan R.O.C.
[2] Department of Electronic Engineering, Chung Chou Institute of Technology, Yuan-lin, 510 Taiwan R.O.C.
n741@ms26.hinet.net

Abstract. A technique, based on a modified Gerchberg-Saxton algorithm (MGSA) and a phase modulation scheme in the fractional Fourier-transform (FrFT) domain, is proposed to reduce crosstalks in multiple-image encryption and multiplexing. First, each plain image is encoded into a phase function by using the MGSA. Then all the created phase functions are multiplexed, with different fractional order of FrFT, and phase-modulated before being combined together into a single phase only function (POF). Simulation results show that the crosstalks between multiplexed images have been significantly reduced, compared with prior methods [1, 2], thus presenting high promise in increasing the multiplexing capacity and encrypting graylevel and color images.

Keywords: Modified Gerchberg-Saxton algorithm, fractional Fourier-transform, multiple-image multiplexing encryption.

The use of opticall multiplexing to achieve multiple-image encryption has been popular for a long time [1-4]. Differing from storing thousands of images in a single photorefractive crystal [5-8], multiple-image encryption uses two phase only function (POFs) to record several images [3, 4]. Image encryption using two statistically independent POFs is conventionally based on the Fourier-transform (FT) domain [9, 10], Fresnel-transform (FrT) domain [11, 12], or fractional Fourier-transform (FrFT) domain [13].

For multiple-image encryption purpose, the most important issue is to increase the multiplexing capacity (i.e., the number of images that can be encrypted simultaneously), or, to reduce the crosstalks on extracting the desired information encrypted therein. Situ and Zhang proposed the schemes of wavelength multiplexing [3] and position multiplexing [4] for binary images. Their methods, however, present limited applicability if the crosstalks can not be further reduced. The annoying crosstalk also prevents Situ and Zhang's schemes from applications to graylevel images.

* Corresponding author.

J.-S. Pan, S.-M. Chen, and N.T. Nguyen (Eds.): ICCCI 2010, Part I, LNAI 6421, pp. 74–80, 2010.

A novel multiple-image encryption scheme is proposed here to overcome the above crosstalk problem, aiming to increase the multiplexing capacity and enable the encryption of grayscale, or even color, images. To simplify the system complexity, we propose a modified Gerchberg-Saxton algorithm (MGSA) [15-17], operating on the FrFT domain (rather than the FT domain for conventional GSA [15, 16]), to retrieve the phase function of an image. The retrieved phase functions for all images to be encrypted are then modulated and combined (in a multiplexing manner) to form a single POF for storage.

Figure 1 shows the block diagram of the proposed MGSA. The algorithm starts with performing the inverse FrFT (abbreviated as IFrFT) on the input target image $g(x_1, y_1)$, which then gets an intermediate phase function $\psi_g(x_0, y_0)$. Next, the phase function $\psi_g(x_0, y_0)$ is constrained with a unity amplitude and then Fresnel-transformed to obtain an approximation $\hat{g}(x_1, y_1)$ with a phase function $\psi_{\hat{g}}(x_1, y_1)$ can be obtained. Again, the target image $g(x_1, y_1)$ with an updated phase function $\psi_{\hat{g}}(x_1, y_1)$ is inversely Fresnel-transformed. The above process is iterated until a required correlation (similarity) between $g(x_1, y_1)$ and $\hat{g}(x_1, y_1)$ is achieved. The converged $\psi_g(x_0, y_0)$ is then determined as the retrieved phase of $g(x_1, y_1)$, i.e., $\psi_g(x_0, y_0)$ will satisfy:

$$\begin{aligned}
&\mathrm{FrFT}\left\{\exp\left[j\psi_g(x_0, y_0)\right]; \alpha\right\} \\
&= (1 - j\cot\alpha)\iint \exp\left[j\psi_g(x_0, y_0)\right] \exp\left[\frac{-j2\pi x_0 x_1 + j\pi(x_0^2 + x_1^2)\cos\alpha}{\sin\alpha}\right] \\
&\quad \times \exp\left[\frac{-j2\pi y_0 y_1 + j\pi(y_0^2 + y_1^2)\cos\alpha}{\sin\alpha}\right] \mathrm{d}x_0 \mathrm{d}y_0 \\
&= \hat{g}(x_1, y_1)\exp\left[j\psi_{\hat{g}}(x_1, y_1)\right],
\end{aligned} \tag{1}$$

where $\alpha = \pi p/2$ and p is a fractional order of FrFT. When the input POF recorded with $\psi_g(x_0, y_0)$ which is FrFTed, the approximation image $\hat{g}(x_1, y_1)$ will be reconstructed at the (x_1, y_1) plane.

Figure 2(a) illustrates the multiple-image encryption process based on the proposed MGSA. First, each individual image $g_n(x_1, y_1)$, $n = 1 \sim N$, is encrypted into its corresponding phase function $\psi_{g_n}(x_0, y_0)$. Then, the iteration process of generating phases based on MGSA in accordance with different fractional order p_n of FrFT is performed to obtain $\psi_{p_n}(x_0, y_0)$. For different fractional order p_n multiplexing, each $\psi_{p_n}(x_0, y_0)$ satisfies:

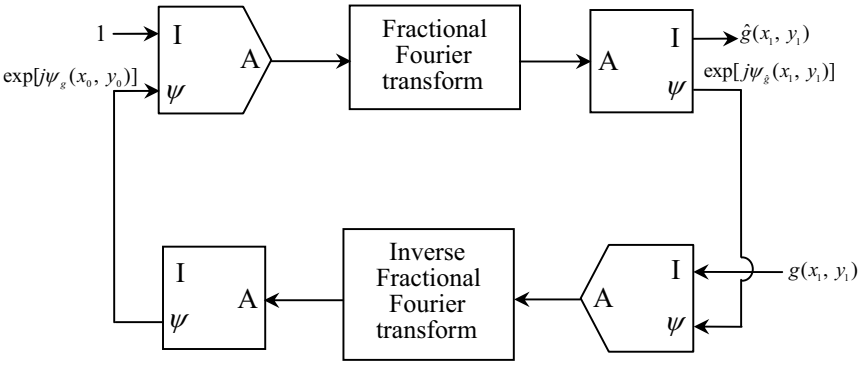

Fig. 1. Block diagram of the proposed MGSA based on FrFT domain

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

where different fractional order p_n satisfies the relation: $\alpha_n = \pi p_n / 2$ and $\psi_{\hat{g}_n}^{p}(x_1, y_1)$ is the accompanied phase term. These N different fractional order p_n multiplexed phase functions, $\psi_{p_n}(x_0, y_0)$, $n = 1 \sim N$, can be recorded together into one POF. Each encrypted image $g_n(x_1, y_1)$ can then be extracted or recovered from the POF as the approximation $\hat{g}_n^{\,p}(x_1, y_1)$ in Eq.(2). However, since crosstalks exist between the encrypted images which are different fractional order p_n multiplexed, the error of $\hat{g}_n(x_1, y_1)$ may be perceivable even the key for deciphering is correct. To reduce the annoying crosstalks among multiplexed images, the N encrypted images $\hat{g}_n(x_1, y_1)$ are spatially translated to different positions by using the phase modulation property of FrFT:

$$\begin{aligned}&\mathrm{FrFT}\left\{\exp\left[\, j\psi'_{p_n}(x_0, y_0)\right]; p_n\right\}\\ &\quad = \hat{g}_n^{\,p}(x_1 - \mu_n \sin\alpha_n,\ y_1 - \nu_n \sin\alpha_n)\exp\left[\, j\phi(x_1, y_1)\right],\end{aligned} \tag{3}$$

where $\psi'_{p_n}(x_0, y_0) = \psi_{p_n}(x_0, y_0) + 2\pi(\mu_n x_0 + \nu_n y_0),$ (4)

$\phi(x_1, y_1)$ is the accompanied phase term, and μ_n and ν_n denote the respective shift amounts of $\hat{g}_n^{\,p}(x_1, y_1)$ in the x_1 and y_1 direction, respectively, at the output plane. It is obvious from Fig. 2(b) that crosstalks can be reduced significantly with a proper arrangement of (μ_n, ν_n)'s .

To synthesize a POF for the purpose of multiple-image encryption, phasors corresponding to $\psi'_{p_n}(x_0, y_0)$, $n = 1 \sim N$, obtained from Eq.(4) are summed to get $\exp\left[\, j\psi_{\mathrm{T}}^{p}(x_0, y_0)\right]$:

$$\psi_{\mathrm{T}}^{p}(x_0, y_0) = arg\left\{\frac{\sum_{n=1}^{N}\exp\left[j\psi'_{p_n}(x_0, y_0)\right]}{\left|\sum_{n=1}^{N}\exp\left[j\psi'_{p_n}(x_0, y_0)\right]\right|}\right\}, \tag{5}$$

where *arg* denotes the argument operator. To the best of our knowledge, this method is new for multiplexing (encrypting) N images with only one POF!

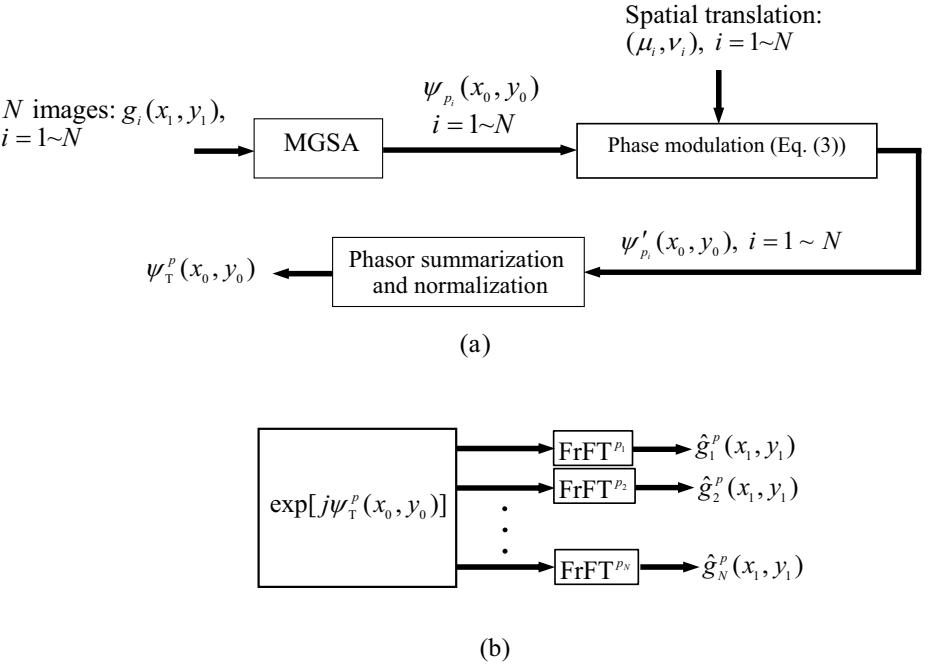

Fig. 2. (a) Block diagram of the proposed multiple-image encryption method. The optical/digital decryption system based on one POF in the fractional Fourier domain can be performed by: (b) the different FrFT order based de-multiplexing (with different order p_n).

The image decryption (extraction) process with different fractional order p_n can be expressed, respectively, as

$$\begin{aligned}&\left|\mathrm{FrFT}\left\{\exp\left[j\psi_{\mathrm{T}}^{p}(x_0, y_0)\right]; p_n\right\}\right| \\ &= \left|\hat{g}_n^{p}(x_1-\mu_n, y_1-\nu_n)\exp\left[j\psi_{\hat{g}_n}^{p}(x_1-\mu_n, y_1-\nu_n)\right] + n_{p_n}(x_1, y_1)\right| \\ &\approx \left|\hat{g}_n^{p}(x_1-\mu_n, y_1-\nu_n)\right| + \left|n_{p_n}(x_1, y_1)\right|,\end{aligned} \tag{6}$$

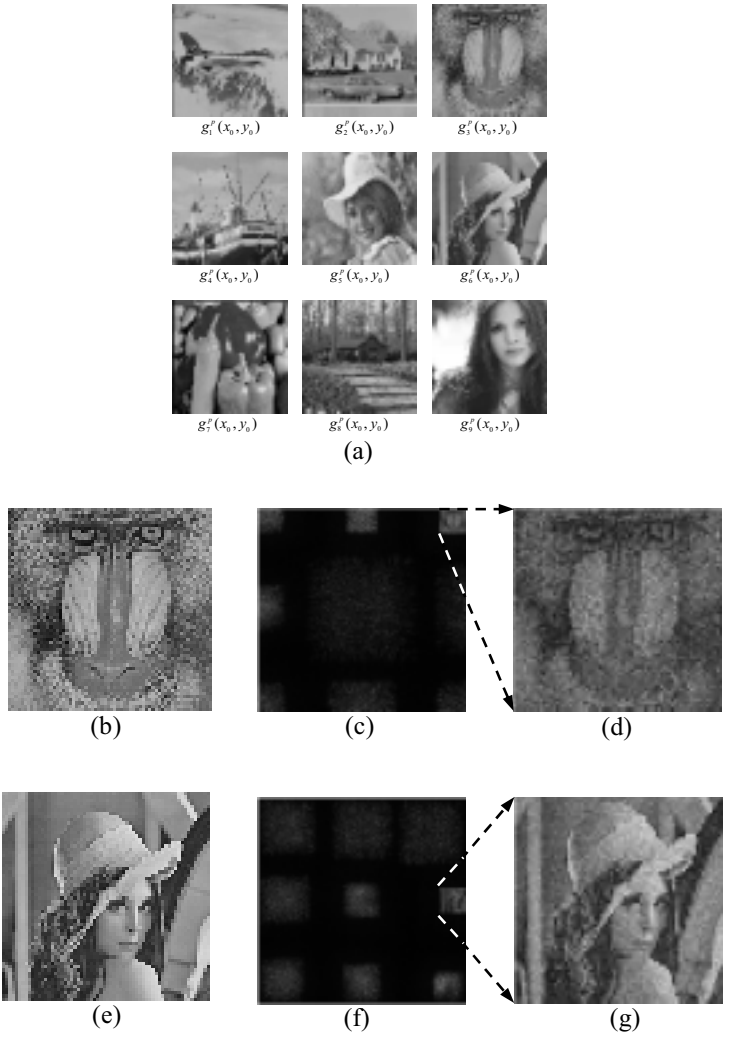

Fig. 3. (a) Nine images $g_1(x_1, y_1) \sim g_9(x_1, y_1)$ for encryption; (b) and (e) are $g_3(x_1, y_1)$ and $g_6(x_1, y_1)$ chosen for FrFT order $p_3 = 1.25$ and $p_6 = 2.0$ multiplexing, respectively; (c) and (f) are the decryption results corresponding to images in (b) and (e); (d) and (g) are the enlarged version of the selected regions in (c) and (f) , respectively.

where $n_{p_n}(x_1, y_1)$ represents the noise terms or crosstalks resulting from deciphering of the remaining images with incorrect keys. Fortunately, the proposed technique based on Eq. (6) can recover the encrypted images, $\hat{g}_n^p(x_1, y_1)$, with different spatial translations to artfully avoid the crosstalks $n_{p_n}(x_1, y_1)$.

Computer simulations are performed to verify our proposed method. Figure 3(a) shows nine original grayscale images of size 64×64 pixels. For different fractional Fourier transform order p_n based multiplexing, the order p_n are varied as $p_n = 0.5+0.25n$, where $n = 1, \ldots, 9$. Figures 3(b) and 3(c) show the original $g_3(x_1, y_1)$ and the decrypted $\hat{g}_3^p(x_1, y_1)$ ($p_3 = 1.25$), respectively, and Figs. 3(e), (g) depict the original $g_6(x_1, y_1)$ and the decrypted $\hat{g}_6^p(x_1, y_1)$ ($p_6 = 2.0$), respectively. Comparing Fig. 3(b) with Fig. 3(d) (the enlarged version of one part in Fig. 3(c)), a correlation coefficient of ρ =0.95 is obtained. A similar performance can be achieved (ρ =0.94) for order $p_6 = 2.0$ multiplexing. The shifting amounts are designated to be $(\mu_n, \nu_n) = (aD, bD)$, where a and b are integers within the range [–3, 3] and $D = 64$. Figure 4 shows the comparison on the correlation coefficient between the original and the decrypted images for our proposed and the methods in Refs. [3, 4]. The proposed method evidently causes lower crosstalks (i.e., larger correlation coefficient) and hence achieves a higher storage capacity (i.e., larger N at a specified crosstalk).

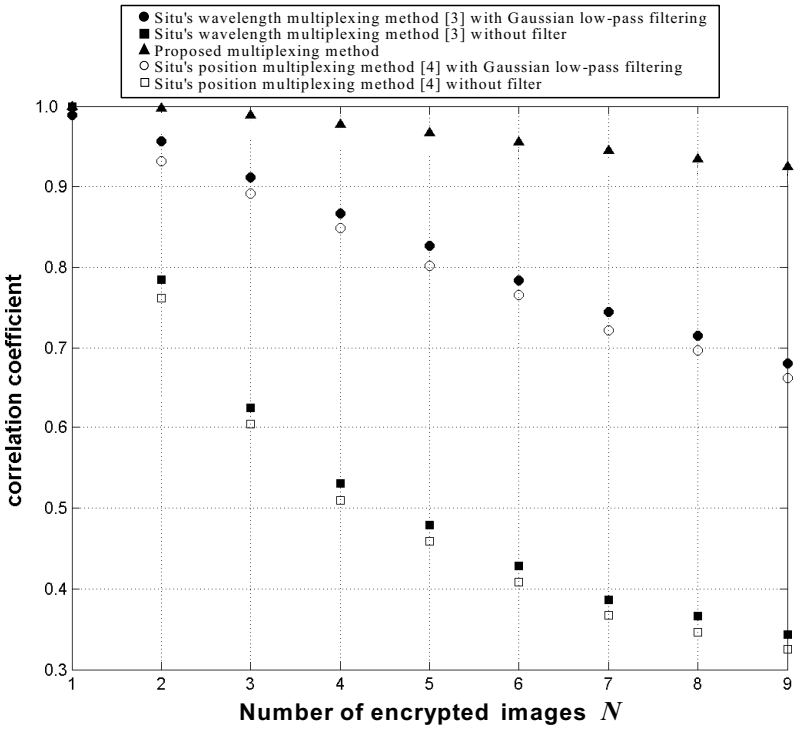

Fig. 4. Comparison of the proposed method with the Situ's methods [3, 4] in terms of correlation coefficient

In conclusion, our proposed method is new and efficient (low crosstalks) for multiplexing (encrypting) N images with only one POF (in contrast to traditional works which require two POFs). By the way, a lensless optical system based on FrFT is more compact, simpler and easier to implement owing to its minimization of the hardware requirement. Optical experiments will be soon conducted in our future research.

Acknowledgements

This research is supported in part by National Science Council under contract number NSC98-2221-E-235-002-MY2. Hone-Ene Hwang's e-mail address is n741@ms26.hinet.net.

References

1. Nomura, T., Mikan, S., Morimoto, Y., Javid, B.: Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator. Appl. Opt. 42, 1508–1514 (2003)
2. He, M.Z., Cai, L.Z., Liu, Q., Wang, X.C., Meng, X.F.: Multiple image encryption and watermarking by random phase matching. Opt. Commun. 247, 29–37 (2005)
3. Situ, G., Zhang, J.: Multiple-image encryption with wavelength multiplexing. Opt. Lett. 30, 1306–1308 (2005)
4. Situ, G., Zhang, J.: Position multiplexing for multiple-image encryption. J. Opt. A: Pure Appl. Opt. 8, 391–397 (2006)
5. Denz, C., Pauliat, G., Roosen, G., Tschudi, T.: Volume hologram multiplexing using a deterministic phase encoding method. Opt. Commun. 85, 171–176 (1991)
6. Heanue, J.F., Bashaw, M.C., Hesselink, L.: Encrypted holographic data storage based on orthogonal-phase-code multiplexing. Appl. Opt. 34, 6012–6015 (1995)
7. Taketomi, Y., Ford, J.E., Sasaki, H., Ma, J., Fainman, Y., Lee, S.H.: Incremental recording for photorefractive hologram multiplexing. Opt. Lett. 16, 1774–1776 (1991)
8. Zhang, X., Berger, G., Dietz, M., Denz, C.: Unitary matrices for phase-coded holographic memories. Opt. Lett. 31, 1047–1049 (2006)
9. Réfrégier, P., Javidi, B.: Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. 20, 767–769 (1995)
10. Javidi, B., Zhang, G., Li, L.: Encrypted optical memory using double-random phase encoding. Appl. Opt. 36, 1054–1058 (1997)
11. Situ, G., Zhang, J.: A lensless optical security system based on computer-generated phase only masks. Opt. Commun. 232, 115–122 (2004)
12. Situ, G., Zhang, J.: Double random-phase encoding in the Fresnel domain. Opt. Lett. 29, 1584–1586 (2004)
13. Liu, Z., Liu, S.: Double image encryption based on iterative fractional Fourier transform: Opt. Comm. 272, 324–329 (2007)
14. Chen, L., Zhao, D.: Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms. Opt. Express 14, 8552–8560 (2006)
15. Gerchberg, R.W., Saxton, W.O.: Phase determination for image and diffraction plane pictures in the electron microscope. Optik 34, 275–284 (1971)
16. Gerchberg, R.W., Saxton, W.O.: A practical algorithm for the determination of phase from image and diffraction plane pictures. Optik 35, 237–246 (1972)
17. Hwang, H.E., Chang, H.T., Lie, W.N.: Fast double-phase retrieval in Fresnel domain using modified Gerchberg-Saxton algorithm for lensless optical security systems. Opt. Express 17, 13700–13710 (2009)