Multiple-image encryption and multiplexing using modified Gerchberg-Saxton algorithm and phase modulation in Fresnel transform domain

Hone-Ene Hwang[1, 3,*], Hsuan T. Chang[2], and Wen-Nung Lie[1]

[1]Department of Electrical Engineering, National Chung Cheng University, Chiayi, 62107 Taiwan ROC
[2]Photonics and Information Laboratory, Department of Electrical Engineering, National Yunlin University of Science and Technology, Douliu Yunlin, 64002 Taiwan ROC
[3]Department of Electronic Engineering, Chung Chou Institute of Technology, Yuan-lin, 510 Taiwan ROC

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

A new technique, based on a modified Gerchberg-Saxton algorithm (MGSA) and a phase modulation scheme in the Fresnel-transform (FrT) domain, is proposed to reduce crosstalks existing in multiple-image encryption and multiplexing. First, each plain image is encoded and multiplexed into a phase function by using the MGSA and a different wavelength/position parameter. Then all the created phase functions are phase-modulated to result in different shift amounts of the reconstruction images before being combined together into a single phase only function. 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 grayscale and color images.

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

Optical multiplexing to achieve multiple-image storage has been popular for a long time. Different from storing thousands of images in a single photo-refractive crystal [3, 4], multiple-image encryption uses two statistically independent phase only function (POFs) to record several images based on the Fourier-transform (FT) [5], Fresnel-transform (FrT) [6, 7], or fractional Fourier-transform (FrFT) domain [8].

For multiple-image encryption, an important issue is to reduce the crosstalks between encrypted images and accordingly increase the number of images that can be encrypted simultaneously (or, the multiplexing capacity). Situ and Zhang proposed to use wavelength multiplexing [1] and position multiplexing [2] for binary images. Their methods, however, present limited applicability if the annoying crosstalks cannot be further reduced for grayscale images.

A novel scheme is proposed here to overcome the above crosstalk problem, aiming to enable the encryption of grayscale, or even color, images. To simplify the system complexity, the traditional Gerchberg-Saxton algorithm (GSA) [9, 10] was modified to operate on the FrT domain (rather than the FT domain) for retrieving the phase function of an image. The retrieved phase functions for all encrypted are then modulated and combined to form a single POF for storage.

Figure 1 shows the block diagram of the proposed modified GSA (MGSA) [11], which starts with inverse FrT (abbreviated as IFrT) on the input image $g(x_1, y_1)$, and then gets an intermediate phase function $\psi_g(x_0, y_0)$. Next, $\psi_g(x_0, y_0)$ is constrained with a unity amplitude and then Fresnel-transformed to obtain an approximation $\hat{g}(x_1, y_1)$ with a phase function $\psi_{\hat{g}}(x_1, y_1)$. Again, the target image $g(x_1, y_1)$ with an updated $\psi_{\hat{g}}(x_1, y_1)$ 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 $g(x_1, y_1)$.

Figure 2 (a) illustrates the multiple-image encryption and multiplexing 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 $\psi_{\lambda_n}(x_0, y_0)$ or $\psi_{z_n}(x_0, y_0)$, in accordance with different wavelength λ_n (of the incident plane wave) or different position z_n (the distance between the input and the output planes), that is, each $\psi_{\lambda_n}(x_0, y_0)$ and $\psi_{z_n}(x_0, y_0)$ should satisfy:

(for wavelength multiplexing)

$$\mathrm{FrT}\left\{\exp\left[j\psi_{\lambda_n}(x_0, y_0)\right]; \lambda_n; z\right\} = \hat{g}_n^{\lambda}(x_1, y_1)\exp\left[j\psi_{\hat{g}_n}^{\lambda}(x_1, y_1)\right], \tag{1}$$

or (for position multiplexing)

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

where $\psi_{\hat{g}_n}^{\lambda}(x_1, y_1)$ and $\psi_{\hat{g}_n}^{z}(x_1, y_1)$ are the accompanied phase terms. These N wavelength (or position)-multiplexed phase functions, $\psi_{\lambda_n}(x_0, y_0)$ (or $\psi_{z_n}(x_0, y_0)$), $n = 1 \sim N$, can be combined (e.g., by direct summation or the manner introduced later) and 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 $\hat{g}_n^{\lambda}(x_1, y_1)$ (or $\hat{g}_n^{z}\ (x_1, y_1)$), plus a crosstalk term, even the key for deciphering is correct. To reduce these annoying crosstalks, $\hat{g}_n(x_1, y_1)$'s are spatially translated to different positions by using the phase modulation property of FrT (taking, e.g., the wavelength multiplexing):

$$\mathrm{FrT}\left\{\exp\left[j\psi'_{\lambda_n}(x_0, y_0)\right]; \lambda_n; z\right\} = \hat{g}_n^{\lambda}(x_1 - \mu_n,\ y_1 - \nu_n)\exp\left[j\phi(x_1, y_1)\right], \tag{3}$$

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

$\phi(x_1,y_1)$ is the accompanied phase term, and μ_n and ν_n denote the respective shift amounts of $\hat{g}_n^\lambda(x_1,y_1)$ in the x_1 and y_1 directions, respectively, at the output plane. It is obvious from Figs. 2(b) and 2(c) 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 $\psi'_{\lambda_n}(x_0,y_0), n=1\sim N,$ are summed and normalized to get $\exp\left[j\psi_{\mathrm{T}}^{\lambda}(x_0,y_0)\right]$: (for wavelength multiplexing)

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

where *arg* denotes the argument operator. A similar derivation for $\exp\left[j\psi_{\mathrm{T}}^{z}(x_0,y_0)\right]$ is omitted here. To the best of our knowledge, this method is new for multiplexing (encrypting) *N* images with only one POF!

The image decryption (extraction) process with different λ_n for wavelength de-multiplexing can be expressed as:

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

where $n_{\lambda_n}(x_1,y_1)$ represents the noise term or crosstalk resulting from deciphering of the remaining images with incorrect keys. Fortunately, the proposed technique based on Eqs. (5) and (6) can recover the encrypted images, $\hat{g}_n^{\lambda}(x_1,y_1)$'s, with different spatial translations (μ_n,ν_n)'s to artfully avoid the crosstalk $n_{\lambda_n}(x_1, y_1)$. A similar formula for position de-multiplexing is omitted here due to the limited space.

Computer simulations are performed to verify our proposed method. Figure 3(a) shows nine original grayscale images of 64×64 pixels. The size of the POF is $5\,\mathrm{mm}\times 5\,\mathrm{mm}$ in the simulation. For wavelength multiplexing, a fixed $z = 0.25\,\mathrm{m}$ and variable $\lambda_n = 300{+}50n\ \mathrm{nm}$, $n = 1,\ldots, N$, are adopted. Figures 3(b) and 3(c) show the original $g_6(x_1, y_1)$ and the decrypted $\hat{g}_6^{\lambda}(x_1, y_1)$, respectively, and Figs. 3(e) and 3(f) show the original $g_3(x_1, y_1)$ and the decrypted $\hat{g}_3^{z}(x_1, y_1)$, respectively. Comparing Fig. 3(b) with Fig. 3(d) (the enlarged version of one part in Fig. 3(c)), a correlation coefficient of ρ=0.93 is obtained. A similar performance can be achieved $(\rho = 0.91)$ for position multiplexing, where a fixed $\lambda = 632.8\ \mathrm{nm}$ and variable $z_n = 100{+}10n$ mm, $n = 1,\ldots, N$, are adopted. The shift amounts are designated to be $(\mu_n, \nu_n) = (\alpha D, \beta D)$, where α and β are integers within the range [−3, 3] and D is the width of the original image. Figure 4 shows the comparison on the correlation coefficient between the original and the decrypted images for our proposed and the methods in Refs. [1, 2]. The proposed method evidently causes lower crosstalks (i.e., larger correlation coefficient) and hence achieves higher storage capacity (i.e., a larger N at a specified crosstalk).

In conclusion, our proposed method is new (with only one POF) and effective (low crosstalks) for multiple-image encryption and multiplexing. By the way, a lensless optical system based on FrT could be constructed accordingly [11], which is advantageous of compactness and simplicity. Optical experiments will be soon conducted in our future research.

This research was supported in part by National Science Council under contract number NSC 97-2221-E-235-003. Hone-Ene Hwang’s e-mail address is n741@ms26.hinet.net.

References with titles:

1. G. Situ and J. Zhang, “Multiple-image encryption by wavelength multiplexing,” Opt. Lett. **30**, 1306–1308 (2005).

2. G. Situ and J. Zhang, “Position multiplexing for multiple-image encryption,” J. Opt. A: Pure Appl. Opt. **8**, 391-397 (2006).

3 . J. F. Heanue, M. C. Bashaw, and L. Hesselink, “Encrypted holographic data storage based on orthogonal-phase-code multiplexing,” Appl. Opt. **34**, 6012-6015 (1995).

4. X. Zhang, G. Berger, M. Dietz, and C. Denz, “Unitary matrices for phase-coded holographic memories,” Opt. Lett. **31**, 1047-1049 (2006).

5. B. Javidi, G. Zhang and L. Li, “Encrypted optical memory using double-random phase encoding,” Appl. Opt. **36**, 1054-1058 (1997).

6. 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)

7. G. Situ and J. Zhang, “Double random-phase encoding in the Fresnel domain,” Opt. Lett. **29**, 1584–1586 (2004).

8. Z. Liu and S. Liu, “Double image encryption based on iterative fractional Fourier transform,” Opt. Comm. **272**, 324-329 (2007).

9. R.W. Gerchberg and W.O. Saxton, “Phase determination for image and diffraction plane pictures in the electron microscope,” Optik **34**, 275-284 (1971).

10. 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).

11. 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).

References without titles:

1. G. Situ and J. Zhang, Opt. Lett. **30**, 1306–1308 (2005).

2. G. Situ and J. Zhang, J. Opt. A: Pure Appl. Opt. **8**, 391-397 (2006).

3. J. F. Heanue, M. C. Bashaw, and L. Hesselink, Appl. Opt. **34**, 6012-6015 (1995).

4. X. Zhang, G. Berger, M. Dietz, and C. Denz, Opt. Lett. **31**, 1047-1049 (2006).

5. B. Javidi, G. Zhang and L. Li, Appl. Opt. **36**, 1054–1058 (1997).

6. C.H. Yeh, H.T. Chang, H.C. Chien, and C.J. Kuo, Appl. Opt. **41**, 6128-6134 (2002)

7. G. Situ and J. Zhang, Opt. Lett. **29**, 1584–1586 (2004).

8. Z. Liu and S. Liu, Opt. Comm. **272**, 324-329 (2007).

9. R.W. Gerchberg and W.O. Saxton, Optik **34**, 275-284 (1971).

10. R.W. Gerchberg and W.O. Saxton, Optik **35**, 237-246 (1972).

11. H.E. Hwang, H.T. Chang, and W.N. Lie, Opt. Express **17**, 13700-13710 (2009).

List of figure captions:

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

Fig. 2. (a) Block diagram of the proposed multiple-image encryption and multiplexing. (b) Wavelength de-multiplexing, and (c) position de-multiplexing for an optical decryption system based on one POF and lensless Fresnel domain.

Fig. 3. (a) Nine images for encryption; (b) and (e): $g_6(x_1, y_1)$ and $g_3(x_1, y_1)$ for wavelength and position multiplexing, respectively; (c) and (f): decryption results corresponding to images in (b) and (e); (d) and (g): the enlarged version of the selected region in (c) and (f), respectively.

Fig. 4. Comparison between the proposed method and the Situ and Zhang's [1, 2] in terms of correlation coefficient.

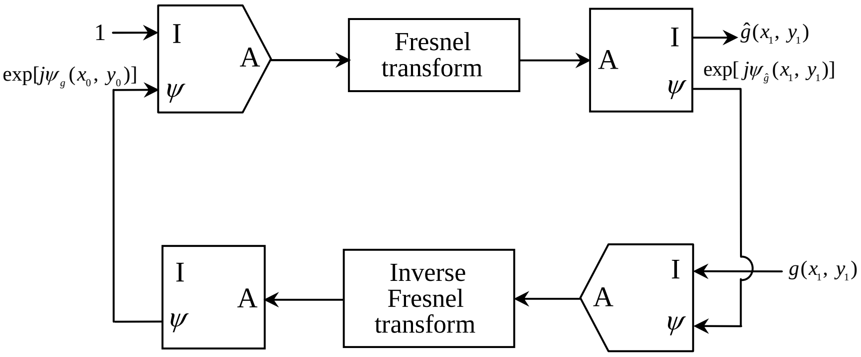
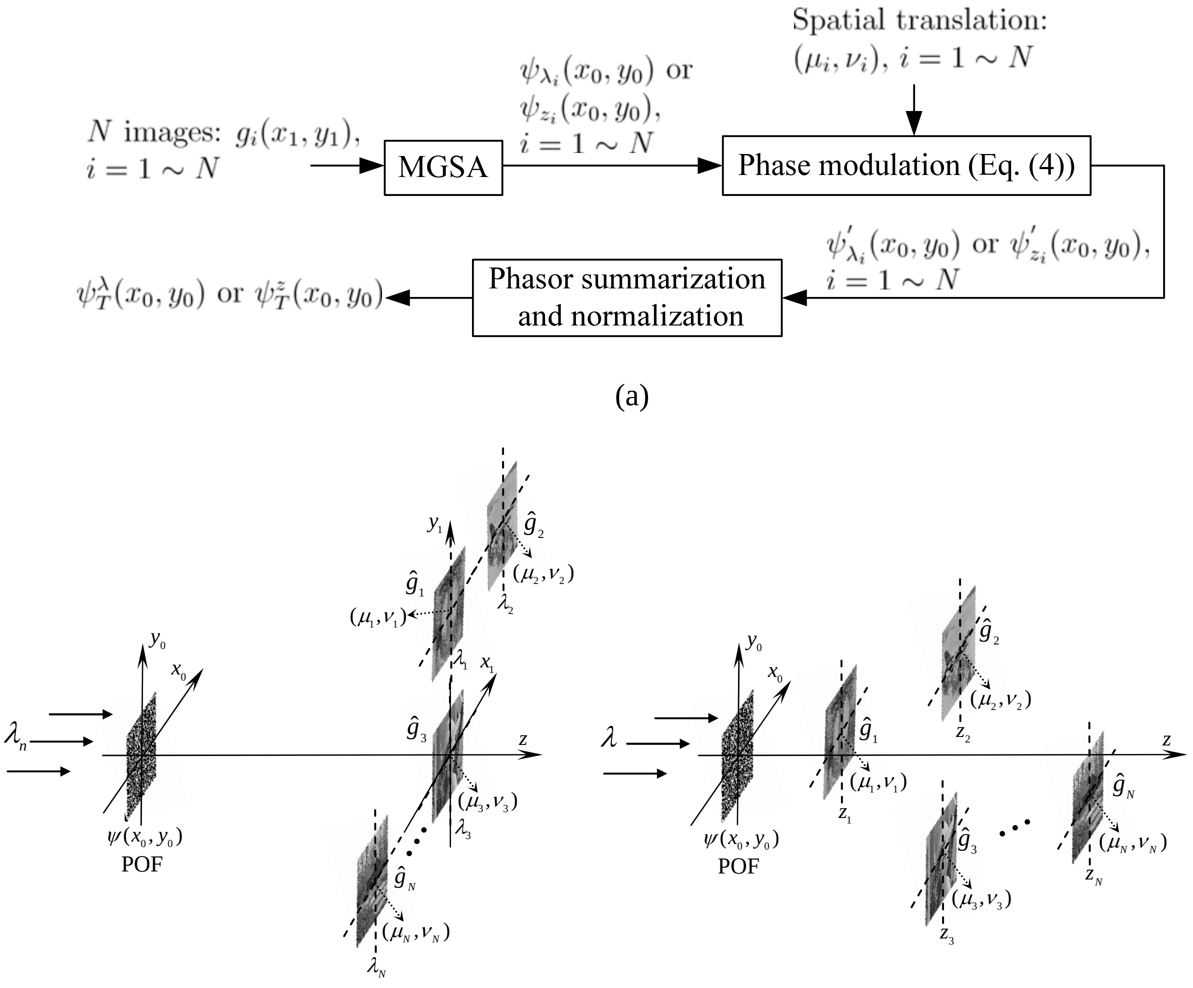

1
exp[$j\psi_g(x_0, y_0)$]
I
ψ
A
Fresnel transform
A
I
ψ
$\hat{g}(x_1, y_1)$
exp[$j\psi_{\hat{g}}(x_1, y_1)$]
I
ψ
A
Inverse Fresnel transform
A
I
ψ
$g(x_1, y_1)$

Fig. 1


Spatial translation: (μ_i, ν_i), $i = 1 \sim N$
N images: $g_i(x_1, y_1)$, $i = 1 \sim N$
MGSA
$\psi_{\lambda_i}(x_0, y_0)$ or $\psi_{z_i}(x_0, y_0)$, $i = 1 \sim N$
Phase modulation (Eq. (4))
$\psi'_{\lambda_i}(x_0, y_0)$ or $\psi'_{z_i}(x_0, y_0)$, $i = 1 \sim N$
Phasor summarization and normalization
$\psi^{\lambda}_T(x_0, y_0)$ or $\psi^{z}_T(x_0, y_0)$
λ_n
y_0
x_0
$\psi(x_0, y_0)$
POF
y_1
x_1
z
$\hat{g}_1$
$\hat{g}_2$
$\hat{g}_3$
$\hat{g}_N$
(μ_1, ν_1)
(μ_2, ν_2)
(μ_3, ν_3)
(μ_N, ν_N)
λ_1
λ_2
λ_3
λ_N
λ
y_0
x_0
$\psi(x_0, y_0)$
POF
z
$\hat{g}_1$
$\hat{g}_2$
$\hat{g}_3$
$\hat{g}_N$
(μ_1, ν_1)
(μ_2, ν_2)
(μ_3, ν_3)
(μ_N, ν_N)
z_1
z_2
z_3
z_N

(a)

(b)

(c)

Fig. 2

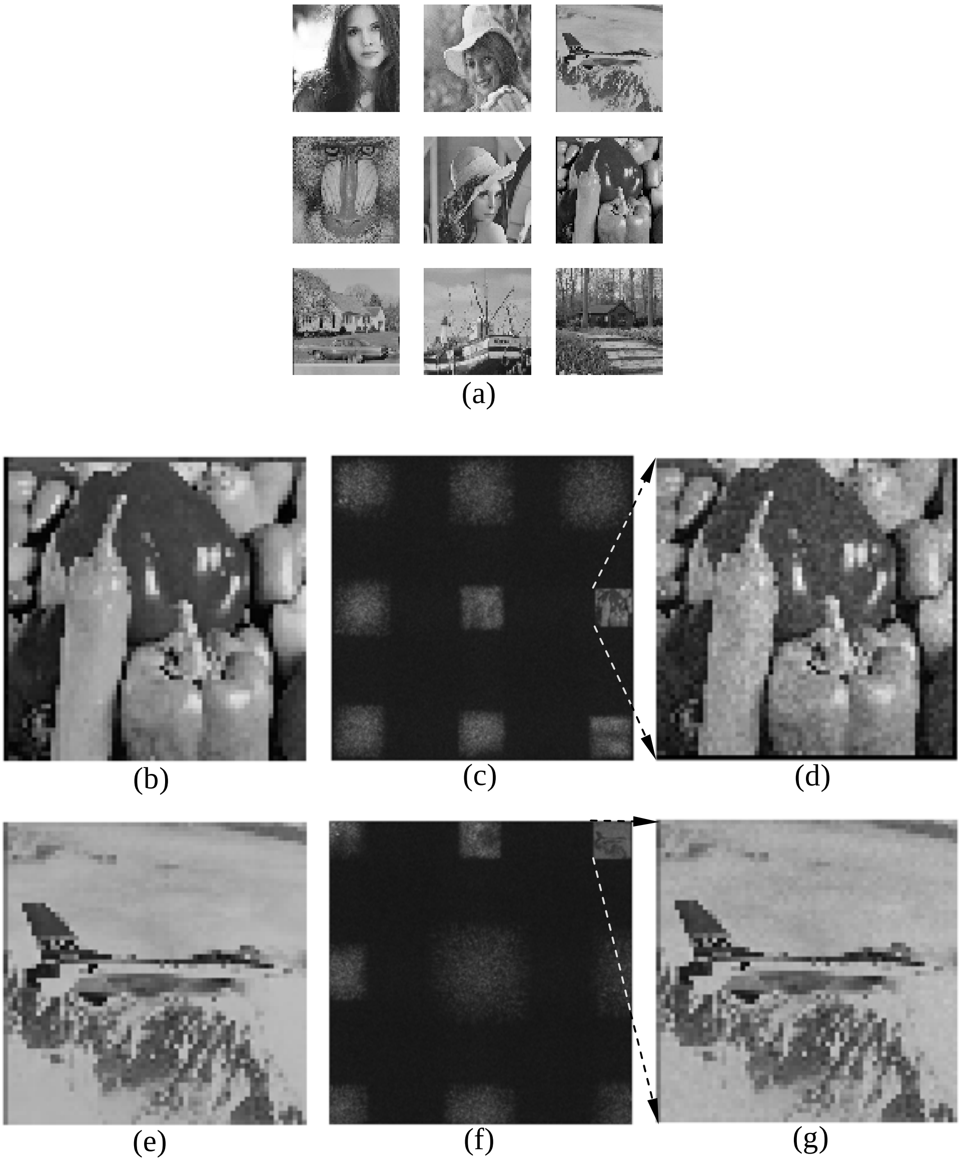


Fig. 3

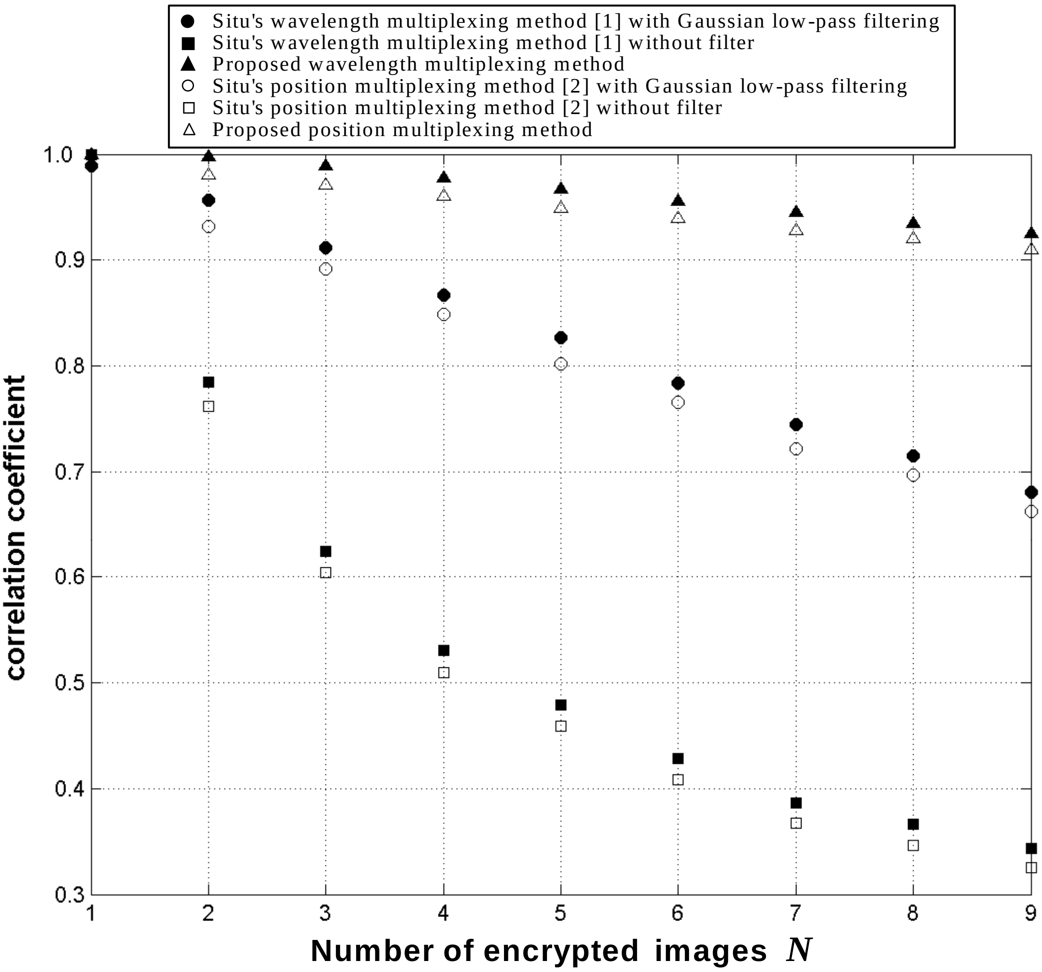

● Situ's wavelength multiplexing method [1] with Gaussian low-pass filtering
■ Situ's wavelength multiplexing method [1] without filter
▲ Proposed wavelength multiplexing method
○ Situ's position multiplexing method [2] with Gaussian low-pass filtering
□ Situ's position multiplexing method [2] without filter
△ Proposed position multiplexing method
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. 4