Position 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

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

A position multiplexing method based on the modified Gerchberg-Saxton algorithm (MGSA) and a cascaded phase modulation scheme in the Fresnel transform domain is proposed in the multiple-image-encryption framework. First of all, each plain image is encoded into a complex function using the MGSA. The phase components of the created complex functions are then multiplexed with different position parameters, and summed. The phase part of the summation result is recorded in the first phase-only mask (POM). The MGSA is applied on the amplitude part of the summation result to determine another phase only function which is then recorded in the second POM. The simulation results show that the crosstalk between multiplexed images is significantly reduced compared with an existing similar method [20]. Therefore, the multiplexing capacity in encrypting multiple grayscale images can be increased accordingly.

keywords: Position multiplexing, multiple-image encryption, phase retrieval, Gerchberg-Saxton algorithm, Fresnel transform domain.

1. Introduction

Optical image encryption techniques have played an important role in optical information processing. Many algorithms and architectural implementations for optical image encryption have been proposed for their 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], subsequent optical encryption methods based on the Fourier transform (FT) [1], Fresnel transform (FrT) [7, 8], or fractional Fourier transform (FrFT) [9-11] have 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 prevailed with much interest, many studies focused on the related applications [1-12]. The DRPE architecture in optical image encryption technique uses two random phase keys: The first key is placed in the input domain and the second in the Fourier domain. If the two random phase keys are generated 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 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 security system keys. Instead of placing one of the 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 remove the requirement for lenses in the 4-f Fourier optical system. It is difficult for intruders to directly retrieve the key phase distribution because of its novel encoding algorithm property [7, 15].

Compared with previous studies, the technique that iteratively encodes the original image into a POM system has three main significant advantages: First, it is lensless and therefore can minimize the number of optical components such as lenses and is easy to implement. Second, except for the native random noise-like distribution function property 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 lines and the decryption process achieved using the correct wavelength and the position parameters at the legitimate receiver.

A multiple-image case has been developed in addition to single image encryption. Many studies have been exploited multiple-image optical encryption. For example, the random phase matching [16], spread-space spread-spectrum multiplexing [17], multichannel encryption [18], and frequency domain truncation schemes [26]. Recently, Situ and Zhang proposed two optical multiple-image multiplexing methods which employed the wavelength and position multiplexing techniques [19, 20]. Although the architecture can be easily implemented, however, annoy crosstalk inevitably exists 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 because the quality of the decrypted images would be worse than that of binary images due to the obvious crosstalk [19, 20].

In our previous study [25], a novel method of position 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.

2. Gerchberg-Saxton algorithm and the modified Gerchberg-Saxton algorithm

The conventional Gerchberg-Saxton algorithm (GSA) is generally employed to reconstruct the lost phases if the corresponding intensities at their respective optical planes are known [21-23]. Figure 1(a) shows a block diagram of the conventional GSA. 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 ψ_i from one of the two optical planes via GSA because the phase distribution ψ_o on the other plane can be obtained by performing a FT on the signal in the retrieved plane. The GSA algorithm iteratively performs FTs back and forth between the object and the Fourier domains. It also sets the measured data or prescribed constraints into each domain in Fig. 1(a). The GSA was often applied to two-dimensional signal applications and also the one-dimensional ones.

Rather than recovering the lost phase information between two intensities on the spatial and Fourier domains, we adopted the MGSA [24] 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(b). 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 is not constrained to the intensity of the 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 $H(x_2, y_2)$. As shown in Fig. 1(b), instead of using the FT and IFT, the MGSA can also be performed 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 $\hat{T}(x_1, y_1)$ shown in Fig. 1(b) can be obtained. 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 (for example, the correlation coefficient ρ achieves a predefined value), the resultant phase distributions $\psi_H(x_2, y_2)$ and $\psi_T(x_1, y_1)$ in the input and output domains can be obtained [24], respectively. Consequently, any two arbitrary 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(b) in the optical FT domain is

$$\begin{aligned}
&\mathrm{FT}\left\{ H(x_2, y_2)\exp\left[j\psi_h(x_2, y_2)\right]; \lambda; z \right\} \\
&= \iint H(x_2, y_2)\exp[j\psi_h(x_2, y_2)]\cdot\exp\left\{\frac{-j2\pi(x_2x_1 + y_2y_1)}{\lambda z}\right\}\mathrm{d}x_2\mathrm{d}y_2 \qquad (1) \\
&= \hat{T}(x_1, y_1)\exp\left[j\psi_G(x_1, y_1)\right],
\end{aligned}$$

or in the optical FrT domain is

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

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 $H(x_2, y_2)$ constraint of a unity amplitude ($H(x_1, y_1) = 1$) is used in the MGSA to generate the phase distribution $\psi_H(x_2, y_2)$, 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 is 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. In retrieving the POFs in the lensless Fresnel diffraction scheme, the MGSA [21, 22] based on the FrT [24] is used. To reduce the annoying crosstalk [19, 20] in the encryption of grayscale or color images, the retrieved phase functions for all images to be encrypted are then modulated to determine the two POFs.

The proposed method for multiple-image encryption with position multiplexing is implemented using the cascaded POFs recorded on the two POMs, respectively. Figure 3 illustrates a systematic block diagram of the proposed method. Firstly, *N* individual images $\{g_n(x_0, y_0) \mid n = 1, 2, 3, \ldots, N\}$ is encrypted as to its corresponding phase functions $\{\psi_{z_n}(x_1, y_1) \mid n = 1, 2, 3, \ldots, N\}$ in accordance with different lateral positions $\{z_n, n = 1, 2, 3, \ldots, N\}$ of the

incident plane wave based on the MGSA shown in Fig. 1(b). That is, each phase function $\psi_{z_n}(x_1, y_1)$ satisfies

$$\mathrm{FrT}\left\{\exp\left[j\psi_{z_n}(x_1, y_1)\right]; \lambda; z_n\right\} = \hat{g}_n^z(x_0, y_0)\exp\left[j\psi_{\hat{g}_n}^z(x_0, y_0)\right], \tag{3}$$

where $\psi_{\hat{g}_n}^z(x_0, y_0)$ is the accompanied phase term for each image $g_n(x_0, y_0)$. These N position-specific phase functions, $\{\psi_{z_n}(x_1, y_1) \mid n = 1, 2, 3,\ldots, N\}$ 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 $\hat{g}_n^z(x_0, y_0)$ in Eq. (3). However, the crosstalk between a specifically reconstructed image $\hat{g}_k^z(x_0, y_0)$ and the other reconstructed images $\{\hat{g}_n^z(x_0, y_0) \mid n = 1, 2, 3,\ldots, N, n \neq k\}$ makes the error perceivable, even the position key z_k for deciphering is correct. To reduce the annoying crosstalk, therefore, the approximation images $\{\hat{g}_n^z(x_0, y_0) \mid n = 1, 2, 3,\ldots, N\}$ are spatially translated into different positions using the phase modulation property of FrT:

$$\mathrm{FrT}\{\exp[j\psi'_{z_n}(x_1, y_1)]; \lambda; z_n\} = \hat{g}_n^z(x_0 - \mu_0, y_0 - \nu_0)\exp[j\omega(x_0, y_0)], \tag{4}$$

where

$$\psi'_{z_n}(x_1, y_1) = \psi_{z_n}(x_1, y_1) + \frac{2\pi(\mu_n x_1 + \nu_n y_1)}{\lambda z_n}, \tag{5}$$

and $\omega(x_0, y_0)$ is the accompanied phase term, and μ_n and ν_n denote the respective shifting distances of $\hat{g}_n^z(x_0, y_0)$ 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 at least greater than the width D_w and the height D_h of the target image to prevent

the possible overlap between two adjacent images.

To synthesize a POF that can achieve multiple-image encryption, the phase functions $\{\psi'_{z_n}(x_1, y_1) \mid n = 1, 2, 3, ..., N\}$ obtained from Eq. (5) are summed to yield the total phase function $\exp\left[j\psi^z_{\mathrm{T}}(x_1, y_1)\right]$:

$$A^z_T(x_1, y_1)\exp[j\psi^z_T(x_1, y_1)] = \sum_{n=1}^{N}\exp[j\psi'_{z_n}(x_1, y_1)], \tag{6}$$

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

$$\mathrm{FrT}\left\{\exp\left[j\phi(x_2, y_2)\right]; \lambda; z'_1\right\} = \hat{A}^z_{\mathrm{T}}(x_1, y_1)\exp\left[j\varphi(x_1, y_1)\right], \tag{7}$$

where λ denotes the wavelength of an incident plane wave and z'_1 represents a distance between the input (POM_2) and filter (POM_1) planes.

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

$$
\begin{aligned}
&\left|\mathrm{FrT}\left(\mathrm{FrT}\left\{\exp\left[j\phi(x_2,y_2)\right];\lambda;z_1'\right\}\exp\left[-j\varphi(x_1,y_1)+j\psi_{\mathrm{T}}^{z}(x_1,y_1)\right];\lambda;z_n\right)\right| \\
&=\left|\mathrm{FrT}\left\{\hat{A}_{\mathrm{T}}^{z}(x_1,y_1)\exp\left[j\varphi(x_1,y_1)\right]\exp\left[-j\varphi(x_1,y_1)+j\psi_{\mathrm{T}}^{z}(x_1,y_1)\right];\lambda;z_n\right\}\right| \\
&=\left|\mathrm{FrT}\left\{\hat{A}_{\mathrm{T}}^{z}(x_1,y_1)\exp\left[j\psi_{\mathrm{T}}^{z}(x_1,y_1)\right];\lambda;z_n\right\}\right| \\
&=\left|\mathrm{FrT}\left\{\sum_{n=1}^{N}\exp\left[j\psi_{z_n}(x_1,y_1)+\frac{j2\pi(\mu_n x_1+\nu_n y_1)}{\lambda z_n}\right];\lambda;z_n\right\}\right| \\
&=\left|\mathrm{FrT}\left\{\sum_{n=1}^{N}\exp\left[j\psi_{z_n}'(x_1,y_1)\right];\lambda;z_n\right\}\right| \\
&=\left|\hat{g}_n^{z}(x_0-\mu_n,\ y_0-\nu_n)\exp\left[j\omega(x_0,y_0)\right]+n_{z_n}(x_0,y_0)\right| \\
&\approx \hat{g}_n^{z}(x_0-\mu_n,\ y_0-\nu_n)+\left|n_{z_n}(x_0,y_0)\right|,
\end{aligned}
\tag{8}
$$

where $n_{z_n}(x_1,y_1)$ represents the crosstalk, which is located at the coordinate (x_0,y_0) and derived from deciphering the remaining images with incorrect keys. 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. (8) can recover the encrypted images $\{\hat{g}_n^{z}(x_0,y_0)\,|\,n=1,2,3,...,N\}$, with different position parameters z_n and spatial translations (μ_n,ν_n) to artfully avoid crosstalk $n_{z_n}(x_0,y_0)$.

The computational and algorithmic complexity of the proposed method in the encoding stage depends on several factors: First of all, the POF of each of the multiplexed images is extracted using the MGSA, in which both the FrFT and IFrFT are required for each iteration step. For the images of size B x B, the computation complexity of performing discrete FrFT and IFrFT

based on the 2D fast Fourier transform (FFT) has been shown to be $O(B^2 \log_2 B^2)$ [27]. To achieve high correlation coefficient between the original and recovered images, the iteration number is set at 100. The computation load depends directly on the image size and the iteration number. Therefore, there are N-time computation load for N images. The N POFs are separately modulated using Eqs. (4) and (5) for the multiplexing purpose. The N POFs are finally summarized to obtain a complex function, in which the amplitude part is used to extract another POF in the POM_1 by again using an iteration process in the MGSA. The most time consuming part in the above factors is the FrFT and IFrFT of the image in the spatial and frequency domains in the MGSA, respectively.

4. Simulation results

Computer simulations are performed to verify the proposed method. A personal computer with Intel Core2 Duo CPU T6600@2.20GHz and 2G DRAM, and the coding language MATLAB 2010b is used to perform the computer simulation. Figure 4 shows nine original grayscale images of size 64×64 pixels. The size of the POFs is $5\ \mathrm{mm} \times 5\ \mathrm{mm}$ in the simulation. In the proposed position multiplexing scheme, a fixed position $z_1' = 0.25\ \mathrm{m}$, fixed wavelength $\lambda = 632.8\ \mathrm{nm}$, and the variable positions $z_n = 0.25 + 0.05n\ \mathrm{m}$, n=1, …, 9, are adopted. Figures 5(a) and 5(b) show the noise-like POFs recorded in POM_1 and POM_2, respectively, determined using Eqs. (3)-(7).

Consider the case of choosing the position parameter $z_3 = 0.4\ \mathrm{m}$ 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 $\hat{g}_3^z(x_1, y_1)$ corresponding to the original image $g_3(x_1, y_1)$ in Fig. 4, respectively. Another case of using the position parameter $z_6 = 0.55\ \mathrm{m}$ in Figs. 6(c) and 6(b)

show the entire decrypted result in the reconstruction plane and the magnified version of the image $\hat{g}_6^z(x_1, y_1)$ corresponding to the original image $g_6(x_1, y_1)$ in Fig. 4, respectively. Compared to the original $g_3(x_1, y_1)$ with Fig. 6(b) and the original $g_6(x_1, y_1)$ with Fig. 6(d), the corresponding correlation coefficients are ρ =0.875 and ρ =0.885, respectively. The shift amounts are designated to be $(\mu_n, \nu_n) = (\alpha D_w, \beta D_h)$, 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 image, respectively.

Figure 7 shows a comparison result of the correlation coefficient between the original and the decrypted images for the proposed method and the method in Ref. [20], which is also a position multiplexing scheme. The advantages of the proposed method are twofold: First, low crosstalk in position multiplexing for the multiple-image encryption technique can be achieved to increase the multiplexing capacity substantially. Second, the lensless optical architecture with Fresnel transform increases the security level for the encryption purpose.

As we mention in Section 2, the computation complexity depends mainly on the number and the size of the multiplexed images. In performing a computer simulation of nine test images encryption and decryption, the program execution times in several stages of the proposed method are given as follows: (1) 316.77 seconds for the phase extraction of nine test images using the MGSA; (2) 9.01 seconds for performing the spatial translation and the phase summarization process; (3) 37.69 seconds for transforming the amplitude part in Eq. (6) to the phase function which will be sent to POM2; (4) 364.59 seconds for the whole encryption process; (6) 1.11 seconds for decrypting one of the nine original images.

The resolution of the phase signals in the two POMs is limited in actual optical implementation. That is, only a finite bit number can be used to represent the phase signals. Therefore, the POFs are quantized with a finite bit number and the errors induced by this

quantization should be investigated as well. Figure 8 shows the quantization effects on the POFs. The reconstructed images are with good quality with eight-bit quantization. The correlation coefficients decrease to be less than 0.8 when the number of encrypted images is nine. If the eight-bit quantization is employed, the correlation coefficients dramatically reduce to less than 0.6, which is not acceptable image quality. Therefore, at least seven-bit resolution is suggested in representing the POFs in the two POMs.

In addition to the quantization effects, the misalignment effects caused by the position shifting of z_1' between the two POMs should also be considered. In the encryption stage of the proposed method, determination of the two POFs is performed using digital methods. If the decryption stage is implemented using optics, the distance parameter could be distorted due to the possible misalignment between two POMs. If the distance z_1 is not identical to that in the encryption stage, the reconstructed image quality will be degraded. Figure 9 shows the misalignment effects caused by the position shifting of z_1' between the two POMs. The shifting distance range is from 0.006 m to -0.006 m. As shown in this figure, the correlation coefficients gradually decrease as the misaligned distance gradually increases. The position shifting of z_1' should be less than 0.5 mm. Otherwise, the correlation coefficient is less than 0.8 and the reconstructed image quality will be unacceptable.

5. Conclusion

In conclusion, the proposed method is a novel algorithm based on the POFs in the Fresnel domain and significantly reduces the crosstalk for multiple-image encryption with position multiplexing. In addition, a lensless optical system based on the FrT could be constructed accordingly [24] to be advantageous of compactness and simplicity. Increasing multiple-image multiplexing encryption security is also achieved in this study. The effects on phase quantization

and the misalignment of the two POMs, which could happen in actual optical implementation, are also investigated. 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 domain,” 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. X. Wang and D. Zhao, “Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain,” Opt. Commun. **284**, 148-152 (2011)

27. H. M. Ozaktas, O. Arikan, M. A. Kutay, and G. Bozdagt, “Digital computation of the fractional Fourier transform,” IEEE Trans. on Signal Processing, **44**, 2141-2150 (1996)

List of figure captions:

Fig. 1: (a) The flow chart of Gercherg-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 position multiplexing based on cascaded phase-only masks in the Fresnel transform domain.

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

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

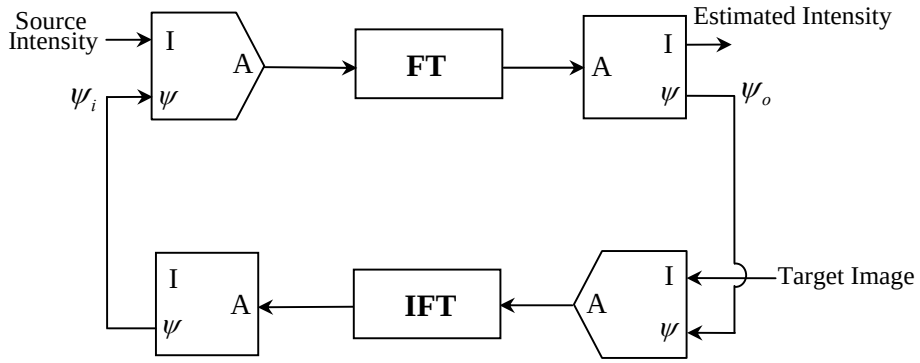
Fig. 5: (a) The noise-like POF recorded in POM_1. (b) The noise-like POF recorded in POM_2.

Fig. 6: (a) The entire decrypted image with the position $z_3 = 0.4$ m in the reconstruction plane; (b) The enlarged decrypted image $\hat{g}_3^z(x_1, y_1)$ corresponding to the original image $g_3(x_1, y_1)$ in Figure 6(a); (c) The entire decrypted image with the position $z_6 = 0.55$ m in the reconstruction plane; (d) The enlarged decrypted image $\hat{g}_6^z(x_1, y_1)$ corresponding to the original image $g_6(x_1, y_1)$ in Figure 6(c).

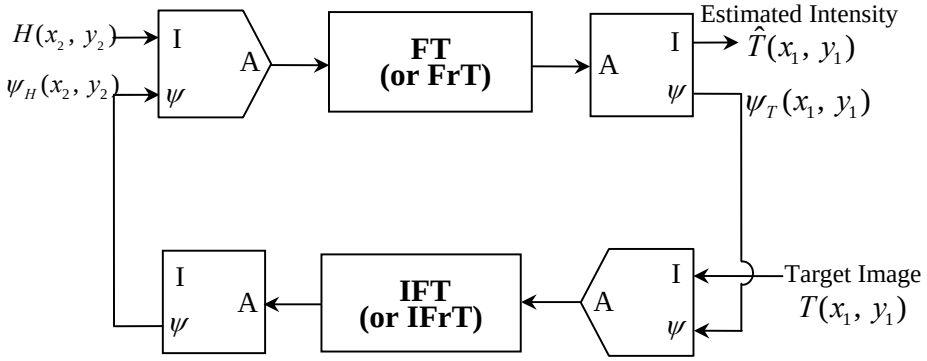
Fig. 7: Comparison result between the proposed method and the Situ's [20] in terms of the correlation coefficient.

Fig. 8: The quantization effects represented by the correlation coefficients versus the encrypted images under using the eight, seven, and six-bit resolutions for the POFs.

Fig. 9: The misalignment effects represented by the correlation coefficients versus the position shifting between two POMs.


Source
Intensity
I
A
ψ_i
ψ
FT
A
I
ψ
Estimated Intensity
ψ_o
I
A
ψ
IFT
A
I
ψ
Target Image

(a)


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

(b)

Fig. 1

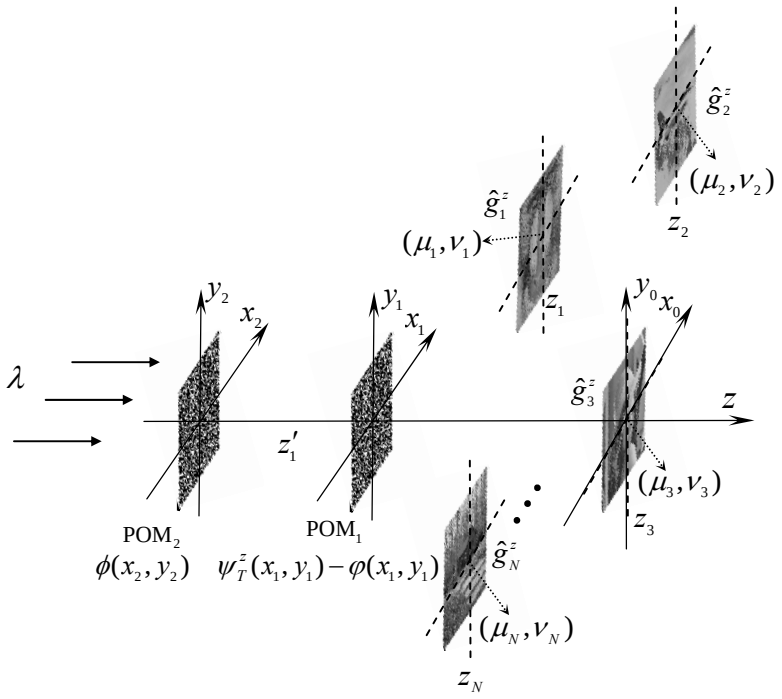

$\hat{g}_2^z$
(μ_2,ν_2)
z_2
$\hat{g}_1^z$
(μ_1,ν_1)
z_1
y_2
x_2
y_1
x_1
y_0
x_0
λ
$\hat{g}_3^z$
z
z_1'
(μ_3,ν_3)
z_3
POM$_2$
$\phi(x_2,y_2)$
POM$_1$
$\psi_T^z(x_1,y_1)-\varphi(x_1,y_1)$
$\hat{g}_N^z$
(μ_N,ν_N)
z_N

Fig. 2

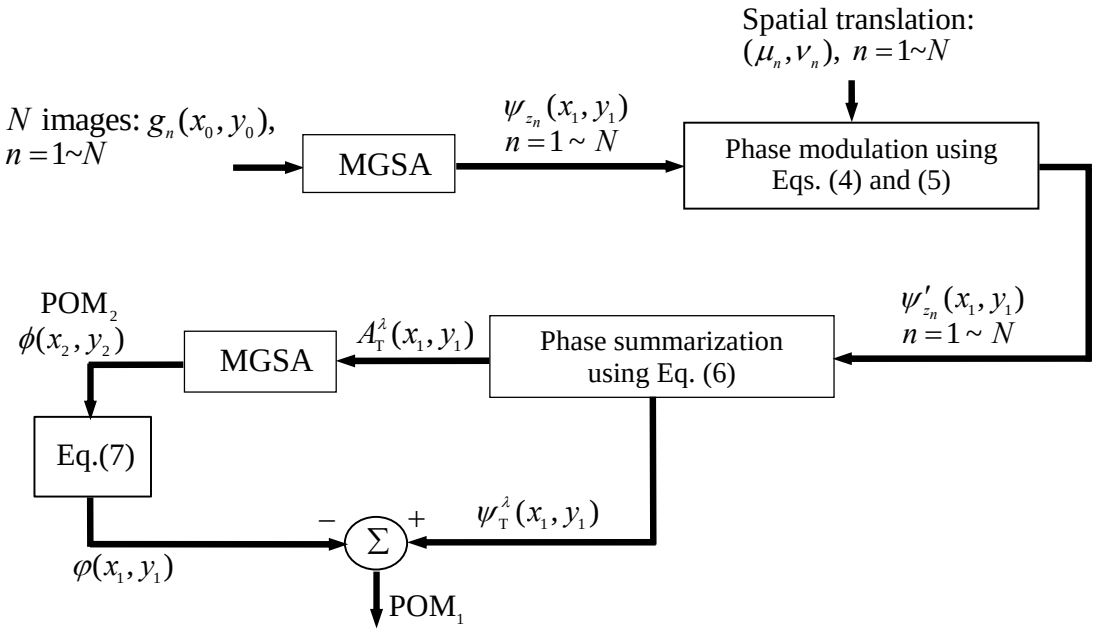
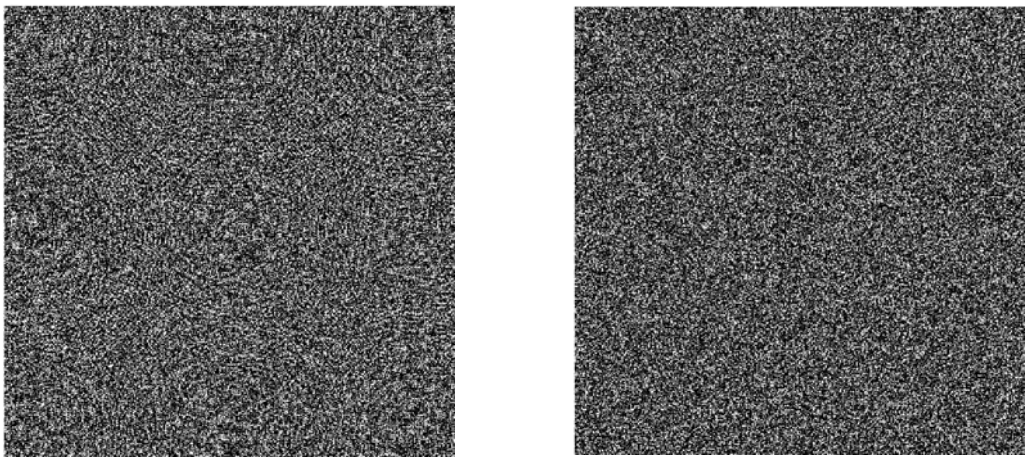

Spatial translation:
(μ_n, ν_n), $n = 1 \sim N$
N images: $g_n(x_0, y_0)$,
$n = 1 \sim N$
MGSA
$\psi_{z_n}(x_1, y_1)$
$n = 1 \sim N$
Phase modulation using
Eqs. (4) and (5)
$\psi'_{z_n}(x_1, y_1)$
$n = 1 \sim N$
Phase summarization
using Eq. (6)
$A_T^{\lambda}(x_1, y_1)$
MGSA
POM$_2$
$\phi(x_2, y_2)$
Eq.(7)
$\varphi(x_1, y_1)$
$-$
$+$
Σ
$\psi_T^{\lambda}(x_1, y_1)$
POM$_1$

Fig. 3

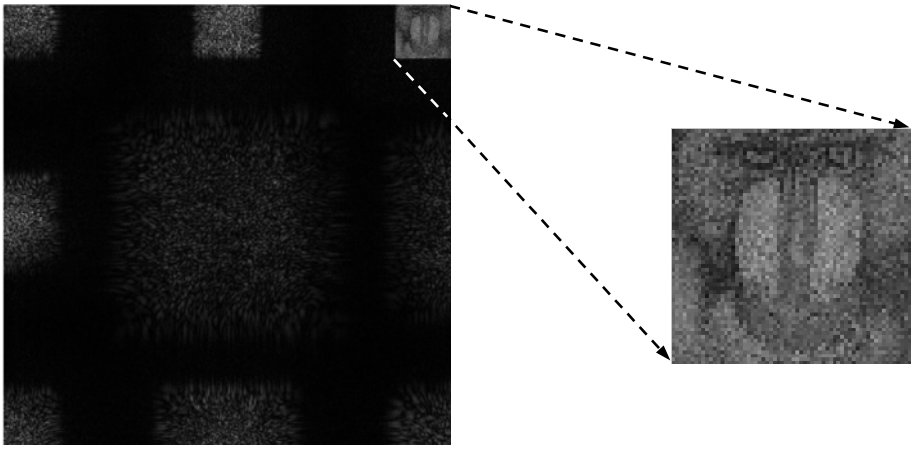

$g_1(x_0, y_0)$
$g_2(x_0, y_0)$
$g_3(x_0, y_0)$
$g_4(x_0, y_0)$
$g_5(x_0, y_0)$
$g_6(x_0, y_0)$
$g_7(x_0, y_0)$
$g_8(x_0, y_0)$
$g_9(x_0, y_0)$

Fig. 4

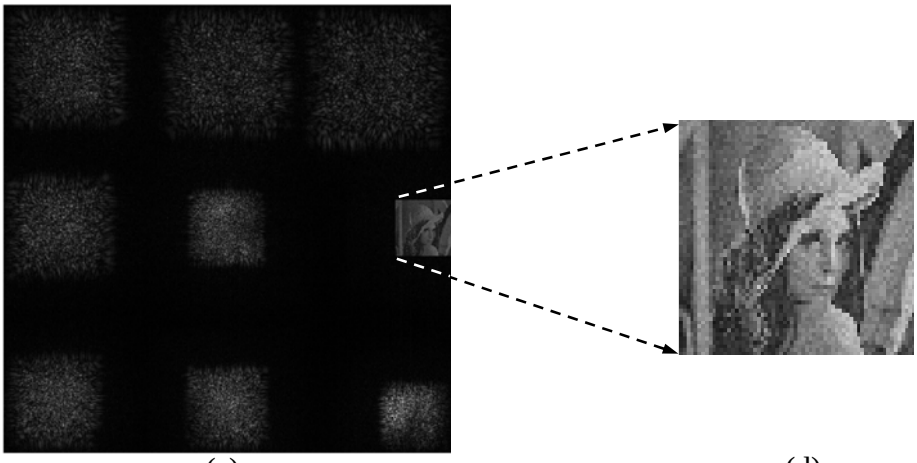


(a) (b)

Fig. 5



(a) (b)



(c) (d)

Fig. 6

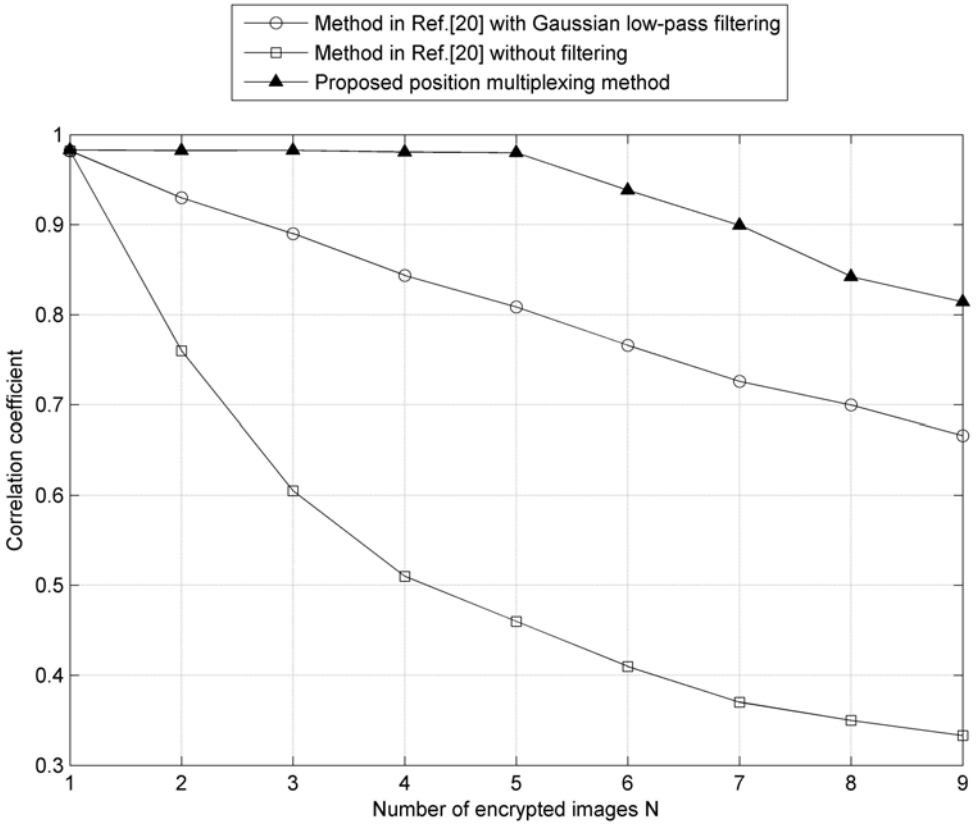

Method in Ref.[20] with Gaussian low-pass filtering
Method in Ref.[20] without filtering
Proposed position multiplexing method
Correlation coefficient
Number of encrypted images N
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
1
2
3
4
5
6
7
8
9

Fig. 7

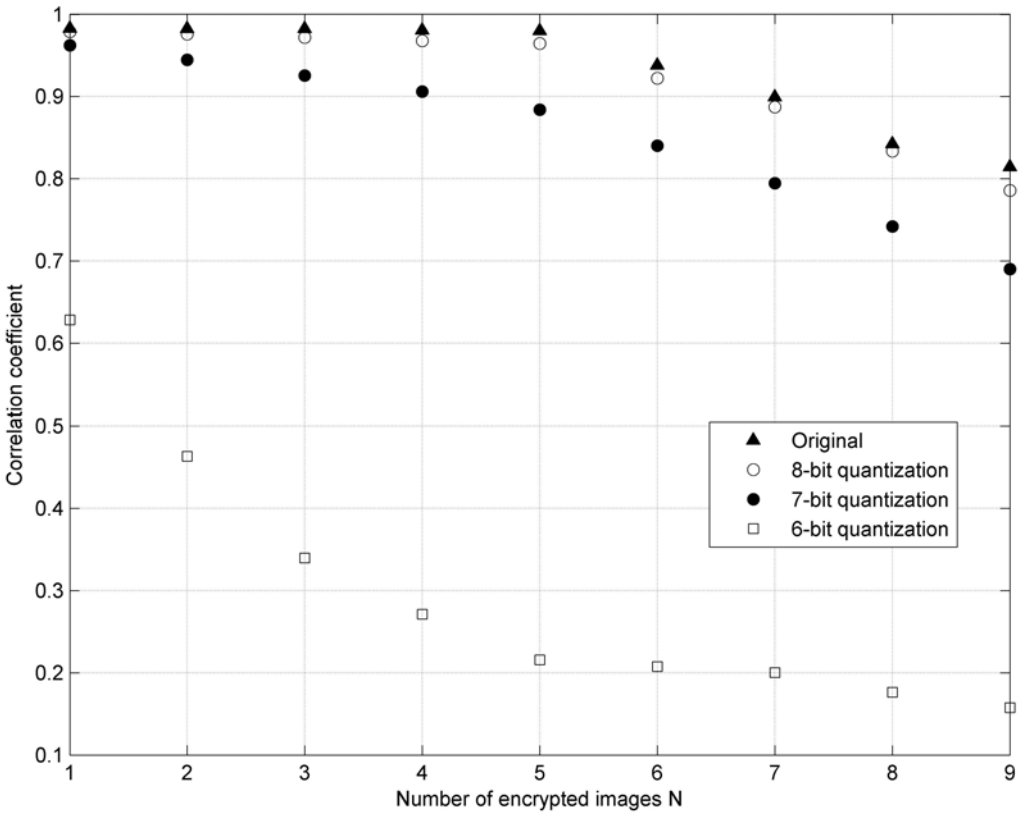

Correlation coefficient
Number of encrypted images N
Original
8-bit quantization
7-bit quantization
6-bit quantization
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
1
2
3
4
5
6
7
8
9

Fig. 8

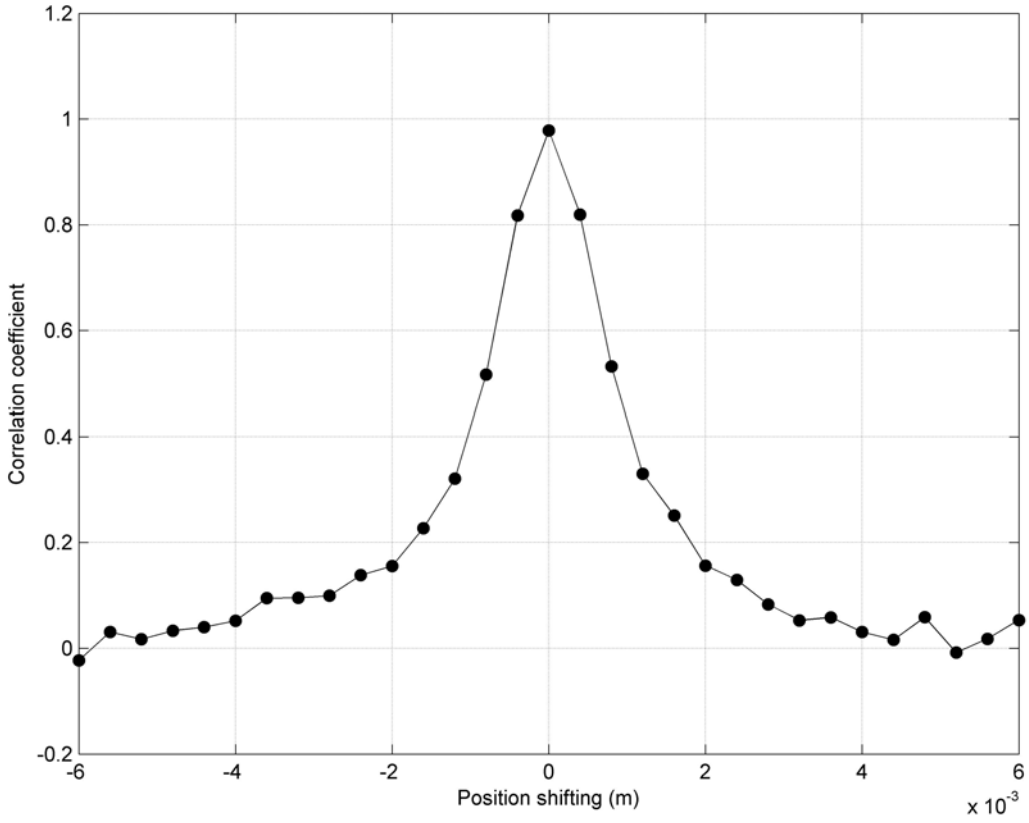

1.2
1
0.8
0.6
0.4
0.2
0
-0.2
Correlation coefficient
-6
-4
-2
0
2
4
6
Position shifting (m)
x 10-3

Fig. 9