Multiple Phases Retrieval for Optical Security Systems Using Random-Phase Encoding

Hsuan T. Chang, Wei C. Lu[†], and Chung J. Kuo[†]

Department of Electrical Engineering
National Yunlin University of Science and Technology
Touliu Yunlin, TAIWAN 64002 R.O.C.

[†]Signal and Media (SAM) Laboratory
Department of Electrical Engineering
National Chung Cheng University
Chiayi, TAIWAN 62107 R.O.C.

Abstract

The technique of the multiple phases encoding for optical security and verification systems is presented in this paper. This technique is based on a 4-f optical correlator that is a common architecture for optical image encryption and verification systems. However, two or more phase masks are iteratively retrieved by using the proposed multiple phases retrieval algorithm (MPRA) to obtain the target image. The convergent speed of the iteration process in the MPRA is significantly increased and the recovered image is much more similar to the target one than those in previous approaches. On the other hand, the quantization effects due to the finite resolution of the phase levels in practical implementation are discussed. The relationships between the number of phase masks and the quantized phase levels are also investigated. According to the simulation results, two and three phase masks are enough to design an efficient security verification system with 64 and 32 phase levels, respectively.

Please send correspondence to Prof. Chang.
Fax: 886-5-5312065, E-mail: htchang@pine.yuntech.edu.tw
September 3, 2009

1 Introduction

Optical techniques for data security have received great deal of attention recently.[1,2] The characteristics of fast computing and parallelism for optics are very useful in real-time applications. There are many research works[3−13] proposed to demonstrate the excellent capability for data encryption. The use of optical processing systems for the purpose of security verification is very promising due to the difficulty it presents to impostors. Conventional optical image encryption techniques are based on the 4-f correlator architecture that use two fixed random phase masks (one is located in the input plane and the other is located in the Fourier plane). As shown in the previous phase encryption methods,[4,10,12,13] the verified image is transformed into complex-value stationary white noise in the output plane. However, a camera can record only the light intensity that is proportional to the squared magnitude of the electromagnetic field. The verified image cannot be recovered by using the magnitude information only. Therefore, the complex-value data should be recorded as the encrypted data by, for example, using the photo-refractive crystals. In decryption, the encrypted data is placed in the input plane of the 4-f correlator. With the conjugate phase functions of the original phase functions in encryption, the verified image can be obtained in the output plane. Alternatively, two security verification systems shown in Refs. 7 and 13 were proposed to find two phase masks, the phase distribution in a mask is fixed and the other is iteratively retrieved, located in two different planes (the input plane and the Fourier plane) of the 4-f correlator, which together should obtain in the output plane some function whose magnitude is equal to a predefined target image. Therefore, the phase distribution in an image actually creates a degree of freedom for the present problem, meaning that it can get any value between 0 and 2π.

Figure 1 shows the optical architecture of the 4-f correlator. Three planes are defined

as the input plane (space domain) in which the input phase mask $\varphi_1(x, y)$ is displayed, the Fourier plane (frequency domain) in which the phase mask $\varphi_2(u, v)$ is displayed, and the output plane (space domain) in which the camera should record the output target image $g(x, y)$. Instead of using both the amplitude and phase information in conventional image encryption techniques, only the phase information is used in the decryption for the image verification systems. However, the encryption is not so straightforward. It is hard to directly find the two phase functions such that the target image can be recovered in the output plane. To determine both phase functions, an iteration process should be employed. In other words, the problem is actually an optimization under constraints, in which one needs to find two phase-only functions that yield the result closest to the target image. The phase retrieval algorithms[14] can be used to solve the problem described above.

Given the different initial phase distributions, all the corresponding solutions of the retrieved phase information are different. Thus the multiple retrieved phase information can be used as the keys of the security system. In Refs. 7 and 13, one phase mask is fixed and only the other phase mask is retrieved with the iteration process. The main drawback in previous studies is the long iteration process required to achieve the convergence of the iterated image. One of the phase masks is employed as a key, while another phase mask is used as a lock that always exists within the system. The target image can be reconstructed only if the correct key appears in the correct plane. Otherwise, a scattered and meaningless image is expected at the output plane. However, the security system cannot distinguish that whether the owner of the key is illegal or not. Once an illegal user steals a valid key, the system is no longer secure. Therefore, this drawback motivates us to design a more secure system that can recognize an illegal user who even has the phase key.

To increase the system security and improve the recovered image quality, two or more phase masks should be used. The phase distributions in the multiple masks are iteratively

and sequentially retrieved with the proposed MPRA. That is, in each iteration, one phase distribution is retrieved with a phase constraint while the others are fixed. Similar ideas can be found in other research areas. For example, in the adaptive vector quantization (VQ) of images,[15] the algorithm of two-phase codebook design generates the optimal gain-normalized codebook for the forward and backward VQ. The adaptive neural-fuzzy inference systems[16] use a hybrid learning procedure to update the parameters in an adaptive network such that the convergent time and the mean squared error (MSE) can be reduced. The two passes in the hybrid learning procedure are similar to the two phases updated in the proposed method. Previous methods modify the phase distribution in either the space or frequency domain with the constraint that only the phase information is preserved. By modifying the phase distribution in both the space and frequency domains, a better-recovered image can be expected due to the higher degree of freedom in modifying the phase values.

For the case of using two-phase masks in the proposed method, both the phase masks are required to recover the target image. However, carrying two phase keys is troublesome and unsafe. Moreover, the effects of mis-alignment are very critical in the proposed system since the alignment for two or more phase masks are more difficult than that for one phase mask only. Instead of using two phase masks as the keys, therefore, the proposed optical verification systems should cooperate with some digital system. For each pair of masks, one of the phase mask serves as the key and the other phase mask stored in the database of the security system as an active lock. The mis-alignment problem of the second phase key is thus eliminated since the phase mask has been fixed in the system. The phase stored in the database can be recalled and loaded into the second phase mask. In addition to a correct phase key, a valid user needs to enter the correct code or password to access the corresponding phase mask such that the target image can be recovered in the output plane for the purpose of verification. Illegal users cannot recover the target image to access the

system without the correct access code or password

The advantages of the proposed optical security system include:

(1) the security level is increased since more than one keys are employed,

(2) the stolen phase key cannot be used to access the security system without the correct access code or password.

(3) faster convergence for the iteration process is achieved since more than one phase masks are modified during the iteration process,

(4) a higher correlated image can be obtained in only few iterations.

The items (3) and (4) will be proved by our simulation results. In addition to the proposed MPRA, the quantization effects on the phase levels are considered since the resolution of the phase levels is finite in practical implementation. This investigation is very important and helpful for designing practical optical security and verification systems.

For the image encryption applications, the encryption process in the proposed system is iterative and digital. The decryption can be implemented either digitally or optically. Compared with other methods in which the encrypted data are complex-value functions, here the encrypted data appear as two phase-only functions, which are difficult to read with conventional intensity-detection devices. On the other hand, compared with the previous studies in which one phase mask is fixed and the encrypted data appear as the other phase function, the proposed method requires two pair-wise phase functions to recover the target image. To prevent carrying two phase keys, the optical system can cooperate with the digital system with a phase database such that one of the two phase-only functions can be recalled by an access code or password.

The organization for the rest part of the paper is as follows. The mathematical analysis of the multiple phase encoding by the proposed MPRA is given in Section 2. Section 3 deals with the quantization effects due to the finite phase levels in practical implementation. The

simulation results are provided in Section 4. Finally, Section 5 concludes the paper.

2   multiple phases retrieval Algorithm (MPRA)

Figure 2 shows the general representation of the optical setup of the security system using the proposed MPRA. The phase distributions in the first mask are denoted as $\varphi_1(x,y)$ and $_1(u,v)$ when the numbers of the phase masks, m and n, are even and odd, respectively. The phase distributions in these masks are determined by the proposed MPRA, which is composed of the forward and backward iteration steps. The forward step digitally simulates the propagation of light from the left side to the right side of the optical setup, while the backward step simulates in the reversed direction. Both iteration steps act in an interlaced sequence. The iteration process stops when the iterated image $\hat{g}(x,y)$ converges to the target image $g(x,y)$. In decryption, with the retrieved phase masks, the iterated image $\hat{g}(x,y)$ can be directly recovered in the output plane by using intensity detection devices such as charge-coupled devices (CCDs).

2.1   Double Phase Masks

Consider the case of two phase masks in the proposed MPRA. Once a coherent plane wave is incident to the input plane, the recovered image in the output plane is expressed by

$$g(x,y) = \text{IFT}\{\text{FT}\{\exp[i2\pi\varphi_1(x,y)]\}\exp[i2\pi \ _2(u,v)]\}, \qquad (1)$$

where FT and IFT denote the Fourier transform and the inverse Fourier transform, respectively. Both the phase functions $\varphi_1(x,y)$ and $_2(u,v)$ in the optical architecture are iteratively modified during the iteration process. Finally, the retrieved phases are obtained when the iterated image converges. That is, we can obtain an approximate image $\hat{g}(x,y)$ in the output plane using two retrieved phases in the input plane and Fourier plane, respectively.

The block diagram of the proposed MPRA for the case of two phase masks is shown in

Figure 3. Initially, the phase $\varphi_1(x, y)$ is randomly generated and distributed in 0 to 2π, while the phase $\varphi_2(u, v)$ is determined by selecting the phase part of

$$\frac{G(u, v)}{P_1(u, v)},$$

where $G(u, v)$ and $P_1(u, v)$ are the Fourier transform of the target image $g(x, y)$ and the phase term $\exp[i2\pi\varphi_1(x, y)]$, respectively. As indicated by the dashed diagonal line in Fig. 3, two phase functions $\varphi_1(x, y)$ and $\varphi_2(u, v)$ are separately and sequentially modified during the forward and backward iteration steps. In the upper-right part of the diagram, we fix the first phase key $\varphi_1(x, y)$ and determine the second phase key $\varphi_2(u, v)$ in the kth iteration. Then, in the lower-left part of the diagram, we fix the second phase key $\varphi_2(u, v)$ and determine the first phase key $\varphi_1(x, y)$ in the next iteration. Note that both the upper-right and lower-left parts in the block diagram are composed of the forward and backward iteration steps.

Suppose the iteration process reaches kth step ($k = 1, 2, 3, \ldots$), the second phase mask $\varphi_2^k(u, v)$ is determined based on the fixed phase mask $\varphi_1^{k-1}(x, y)$ determined in the previous iteration step. By tracing the upper-right part of Fig. 3, we obtain the complex function

$$\bar{P}_2^k(u, v) = \frac{\text{FT}\{g^{k-1}(x, y)\}}{\text{FT}\{\exp[i2\pi\varphi_1^{k-1}(x, y)]\}} \tag{2}$$

in the Fourier plane and the phase part of $\bar{P}_2^k(u, v)$,

$$\varphi_2^k(u, v) = \angle\bar{P}_2^k(u, v), \tag{3}$$

can be obtained with the frequency domain constraint. Then the kth iterated image $\bar{g}^k(x, y)$ is obtained in the output plane, which is expressed by

$$\bar{g}^k(x, y) = \text{IFT}\{\text{FT}\{\exp[i2\pi\varphi_1^{k-1}(x, y)]\} \exp[i2\pi\varphi_2^k(u, v)]\}. \tag{4}$$

The iterated image $\bar{g}^k(x, y)$ is then compared with the target image by measuring the MSE between the target and the iterated images, which is defined by

$$\text{MSE} = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} [g(x, y) - \bar{g}^k(x, y)]^2, \tag{5}$$

7

where $M \times N$ is the size of the image. Another measurement on the correlation coefficient of two images is also investigated. The correlation coefficient of two images can be expressed by

$$C = \frac{\text{COV}(g, \bar{g}^k)}{\sigma_g \sigma_{\bar{g}^k}},\tag{6}$$

where $\text{COV}(g, \bar{g}^k)$ denotes the covariance of two images g and $\bar{g}^k$, σ_g and $\sigma_{\bar{g}^k}$ denote the standard deviation of the images g and $\bar{g}^k$, respectively. The joint transform correlators,[17] for example, are optical processors that can generate the signals that are proportional to the correlation coefficients of two two-dimensional image signals. If the MSE is less than the threshold value γ_{th} or the correlation coefficients have converged, the iteration process stops. Otherwise, the iterated image is modified to satisfy the expected image constraint as follows:

$$g^k(x, y) = \begin{cases} \bar{g}^k(x, y), & \text{if } |\bar{g}^k(x, y) - g(x, y)| \leq \gamma_{\text{th}}, \\ g(x, y), & \text{if } |\bar{g}^k(x, y) - g(x, y)| > \gamma_{\text{th}}, \end{cases}\tag{7}$$

where γ_{th} is a pre-defined threshold value. Once the kth iterated image $g^k(x, y)$ has been generated, the first phase key $\varphi_1^{k+1}(x, y)$ at next iteration will be determined based on the fixed phase mask $\phi_2^k(u, v)$ determined in the previous iteration. The similar mathematical deviations of the forward and backward iterations are given as follows: By tracing the lower-left part of Fig. 3, we obtain

$$\bar{p}_1^{k+1}(x, y) = \text{IFT}\{\frac{\text{FT}\{g^k(x, y)\}}{\exp[i2\pi \phi_2^k(u, v)]}\},\tag{8}$$

in the input plane and the phase part of $\bar{p}_1^{k+1}(x, y)$,

$$\varphi_1^{k+1}(x, y) = \angle \bar{p}_1^{k+1}(x, y),\tag{9}$$

can be obtained with the frequency domain constraint. The $(k+1)$th iterated image $\bar{g}^{k+1}(x, y)$ is obtained in the output plane, which is expressed by

$$\bar{g}^{k+1}(x, y) = \text{IFT}\{\text{FT}\{\exp[i2\pi\varphi_1^{k+1}(x, y)]\}\exp[i2\pi \phi_2^k(u, v)]\},\tag{10}$$

8

The iterated image $\bar{g}^{k+1}(x, y)$ is then compared with the target image by measuring the MSE or the correlation coefficients between the target and the iterated images. If the MSE is less than the threshold value γ_{th} or the correlation coefficients have converged, the iteration process stops. Otherwise, the iterated image is modified to satisfy the expected image constraint as follows:

$$g^{k+1}(x, y) = \begin{cases} \bar{g}^{k+1}(x, y), & \text{if } |\bar{g}^{k+1}(x, y) - g(x, y)| \leq \gamma_{\text{th}}, \\ g(x, y), & \text{if } |\bar{g}^{k+1}(x, y) - g(x, y)| > \gamma_{\text{th}}. \end{cases} \tag{11}$$

In the following iteration steps, k is replaced by $k + 1$ and the iterated image $\hat{g}(x, y)$ will be finalized when the MSE or the correlation coefficient converges. In decryption, the determined phase masks $\varphi_1(x, y)$ and $\varphi_2(u, v)$ are placed in the input plane and the output plane, respectively. To recover the target image, the first phase term $\exp[i2\pi\varphi_1(x, y)]$ in the input plane is Fourier transformed and multiplied by the second phase term $\exp[i2\pi\varphi_2(u, v)]$. Finally, they are inverse-Fourier-transformed by a lens to obtain the target image (exists in an amplitude form), which can be detected by a CCD camera.

The initial phase distribution in the iteration process is randomly generated. This results in obtaining the different pairs of the iteratively retrieved phases. Apparently, plenty of solutions for the paired phase masks can recover the target image. Therefore, in the security system for verification, each legal user is assigned to a paired phase keys. One of the phase keys appears as a phase mask and the other appear as the access code or password, which corresponds to the phase mask pre-stored in the security system. Even an illegal user steals the phase key, the target image cannot be recovered without the corresponding access code or password. Hence higher security of the system is obtained by the proposed method.

2.2 Multiple Phase Masks

Consider the cases that the number of phase masks is greater than two. Figure 2(a) and (b) show a general representation of the optical setup for the cases that the number m and n

are odd and even, respectively. The first phase mask is placed at either the space domain or the frequency domain according the number of masks. For the cases of the numbers m and n are odd and even, the first phase mask should be placed at the frequency domain and the space domain, respectively. The mathematical analyses of these cases would be similar to that shown in Subsection 2.1. Initially, the phase distribution of all masks can be randomly generated. To speed up the iteration process, $m-1$ and $n-1$ phase distributions are randomly given and the first phase distribution are determined by

$$\varphi_1^1(x, y) \tag{12}$$
$$= \angle \mathrm{IFT}\{\mathrm{FT}\{\ldots \mathrm{IFT}\{\mathrm{FT}\{\mathrm{IFT}\{\frac{G(u,v)}{P_m(u,v)}\}/p_{m-1}(x,y)\}/P_{m-2}(u,v)\}\ldots\}/P_2(u,v)\}$$

for m is even and

$$\varphi_1^1(u, v) \tag{13}$$
$$= \angle \mathrm{FT}\{\mathrm{IFT}\{\ldots \mathrm{IFT}\{\mathrm{FT}\{\mathrm{IFT}\{\frac{G(u,v)}{P_n(u,v)}\}/p_{n-1}(x,y)\}/P_{n-2}(u,v)\}\ldots\}/p_2(x,y)\}$$

for n is odd, respectively. The brief representation of the proposed MPRA is shown in Fig. 4. During the iteration process, $m-1$ phases are fixed and only one phase can be modified with the constraint. The mathematical analysis in each macro block is similar to that for double phases retrieval. Therefore, each of the m phases is modified once during m steps in the iteration process. When the iteration process stops, more than two phase keys will be determined. To obtain the target image in decryption, all the retrieved phase keys should be required and placed in the corresponding planes. If the phase keys are distributed to different users, anyone of the user loses the phase key will fail to recover the target image. Therefore, the proposed MPRA can be also employed in the security-sharing systems.

3 Finite-Resolution Phase Encoding

The values of the phase distribution in above description are real values, which means that they are represented by real numbers. In practical implementation and applications, however, the available phase levels in optical devices such as the diffraction elements are finite due to the state-of-the-art manufacture technologies. Therefore, the quantization effects caused from the finite levels of the phase resolution should be considered. According to our survey, the maximum available phase level for a single diffraction element is around 64. We here investigate the quantization effects corresponding to different finite phase levels (from 8 to 64, which are uniformly quantized). The minimum phase levels to obtain an acceptable quality for the recovered image in the proposed optical system are also discussed. Finally, the relationship between the phase levels and the number of the phase masks will be investigated. We expect that the required phase levels for obtaining an acceptable image quality is inversely proportional to the number of phase keys used in the security systems. That is, if the phase levels are limited in low resolution, we could use more phase masks to increase the recovered image quality.

In addition to the uniform quantization for the phase levels, a non-uniform quantization technique for designing efficient diffraction optical elements was proposed in Ref. 18. More degrees of freedom is provided in quantizing the phase function of a diffraction optical element and higher diffraction efficiency can be achieved. Thus better quality of the recovered image can be expected using the non-uniform quantization techniques.

4 Simulation Results

In computer simulation, the Jetplane image of size 128×128 with 256 graylevels is used as the target image. The sizes of both phase masks are the same as the Jetplane image. Initially ($k = 0$), the first phase mask $\varphi_1^0(x, y)$ is randomly generated. Then the iteration process

proceeds based on the block diagram shown in Fig. 3 and Eqns. 2–10.

In comparison, two measurements between the iterated image and the target image are investigated are used: (1) the MSE calculation by digital ways; (2) the correlation coefficient that can be obtained by the optical correlation technique. First of all, the proposed method with two phase masks is compared with two previous methods. Let Algorithm 1 and Algorithm 2 denote the methods shown in Refs. 13 and 7, respectively. The optical setups in both methods are based on the 4-f correlator. A predefined target image is located in the output plane such that a corresponding phase mask can be retrieved by the use of the projection onto constraint sets (POCS) algorithm.[19] Both methods use a fixed phase mask as a lock and iteratively retrieve another phase mask as a key. In Algorithm 1, the retrieved phase is located in the Fourier plane, while the retrieved phase is located in the input plane in Algorithm 2. The simulation results of the MSE and the correlation coefficient between the iterated and the target image are shown in Figure 5. Figure 5(a) shows the MSE comparison among three methods, while the effects of finite phase levels are not considered yet. That is, the full floating point representation for the phase value is used. Algorithm 1 owns the slowest convergence during the iteration process. The proposed method achieves the lowest MSE in few iterations although the MSE slowly increases after ten iterations. On the other hand, the correlation coefficient shown in Figure 5(b) provides a different perspective. The correlation coefficient in the proposed method is very close to one after ten iterations. The iterated image thus is the most correlated with the target image among three methods. The original and the corresponding iterated images of three methods at 100th iteration are shown in Fig. 6. Although the MSEs for three methods are similar, the recovered image in Fig. 6(b) corresponding to Algorithm 1 is obviously worse than other recovered images in Fig. 6(c) and (d). Looking into the cloud region in three recovered images, Fig. 6(d) is the closest to the original target image. The contrast ratio in Fig. 6(d) is obviously higher

than the original target image shown in Fig. 6(a). This is the reason why larger MSE is obtained. Figure 7(a)–(c) shows the difference images (biased at the graylevel 128) between the original and the retrieved images shown in Fig. 6(b)–(d). The error images shown in Fig. 7(a) and (b) are meaningless, while the error images shown in Fig. 7(c) is very similar to the original image. Obviously, the latter image is simply a small bias in graylevel left. Therefore, Figure 6(d) is expected to be with a higher correlation coefficient than that of Fig. 6(b) and (c) although the corresponding MSE is the highest among three methods. Apparently, the measurement of correlation coefficient is more suitable for comparing the recovered image quality. In the rest part of the simulation results, we will make the comparison on the correlation coefficients for three methods.

For different initial phase distributions, the iteratively retrieved phase pairs are also different. Therefore, only the phase pairs retrieved together in the same iteration process can recover the target image. Having only one phase key, or having two phase keys but not belonging to the same pair will fail to recover the target image. Even an illegal user acquires the target image in the output plane and reproduces two phase masks, the security system cannot be broke. This feature is demonstrated in the table shown in Fig. 8. Five pairs of the phase masks, $\varphi_{1,i}(x, y)$ and $\varphi_{2,i}(u, v)$, $i = 1, 2, \ldots, 5$, are retrieved by the iteration process for the same target image. This table demonstrates that only the correct phase pairs can recover the target image, as seen along the diagonal of the table. When the mismatched phase pairs are used, only the noise-like meaningless images are generated. Therefore, it is impossible to deduce the right phase mask $\varphi_1(x, y)$ for an unknown phase mask $\varphi_2(u, v)$. Higher security than previous approaches is thus achieved.

Consider the finite phase resolution in optical phase masks. The comparison result of the correlation coefficients using four resolutions: 8, 16, 32, and 64 phase levels between 0 and 2π in the proposed methods are given in Fig. 9. Generally, the phase masks with

higher phase resolutions can achieve higher correlation coefficients. However, the cost to obtain higher phase resolutions is much higher than that for lower resolutions. To obtain high correlation coefficients by using lower phase resolutions, multiple phase masks should be employed. Consider the cases of using two, three, and four phase masks. Figures 10–13 shows the correlation coefficients for the iterated images based on the proposed methods with different phase masks and different phase resolutions. As shown in these figures, all the correlation coefficients are lower than 0.9 when only eight phase levels are used in the phase masks. The correlation coefficients for three and four phase masks are similar when the phase resolution is 16 levels and above. Using more than four phase masks would be inefficient in increasing the coefficients when the phase resolution is 32 levels and above. On the other hand, 32 phase levels are good enough to recover the target image with high correlation coefficients when three phase masks are used in the proposed method. Therefore, there is a trade-off between the phase resolution and the number of phase masks. If we use two phase masks in the proposed optical system, 64 phase levels are suggested. However, if three phase masks are employed, 32 phase levels are good enough to recover the target images with the correlation coefficients around 0.93. Regarding to the alignment issue in the multiple phase masks, the more the phase masks are used, the harder the mask can be achieved. Obviously, the mis-alignment problem is more serious when more phase masks leads are used in the proposed system. On the other hand, for a digital implementation, four or more phase masks would not be a problem. This would be very useful in the application such as for secure image transmission over the internet.

The joint space-frequency domain iteration of the proposed MPRA converges very quickly to a stable solution. This is very useful in designing the diffraction optical elements (DOEs). In designing the phase element, the similar cascaded architecture has been used to obtain equally spaced levels of phase modulation. For example, multiple plane DOEs have

been proposed by the use of cascaded ferroelectric liquid crystal spatial light modulators (FLCSLMs).[20] Theoretically, n FLCSLMs can be cascaded to achieve 2^n phase levels.[21] Therefore, the phase resolutions higher than 64 levels are possible. On the other hand, the cascaded diffractive phase elements are also used for programmable optical interconnection,[22] optical networks,[23] and three-dimensional multi-wavelength optical interconnects.[24] The possibility of programmability and the manipulation of multi-wavelength beams greatly extend the applications of cascaded phase elements. Extra flexibility and higher security will be expected if the abilities above are combined with the proposed system.

5   Conclusion

An optical security and encryption system based on multiple-phase encoding is proposed in this paper. The multiple phase masks are iteratively retrieved by using the proposed MPRA. Compared with two previous methods, the proposed MPRA has faster convergence for the iteration process and better image quality for the recovered target image. On the other hand, the proposed method achieves higher security since only the phase pair generated together can recover the target image. The illegal users who steal only one phase key or have acquired the target image cannot access the security system without the corresponding access code or password. The quantization effects of the phase masks due to the finite phase resolutions in practical implementation are also discussed. Finally, we also investigate the trade-off between the different numbers of phase masks and the different phase resolutions, which is quite significant in designing practical optical security systems.

Acknowledgment

References

[1] J. Horner and B. Javidi, *Optical Engineering,* **35**(9), Special issue on Optical Security (1996)

[2] J. Horner and B. Javidi, *Optical Engineering,* **38**(1), Special issue on Optical Security (1999)

[3] J.-W. Han, C.-S. Park, D.-H. Ryu, and E.-S. Kim, "Optical image encryption based on XOR operations," *Optical Engineering*, **37**(1), pp. 47–54 (1999)

[4] B. Javidi and E. Ahouzi, "Optical security with Fourier Plane encoding," *Applied Optics*, **37**(26), pp. 6247–6255 (1998)

[5] B. Javidi and J.L. Horner, "Optical pattern recognition for validation and security verification," *Optical Engineering*, **33**(6), pp. 1752–1756 (1994)

[6] B. Javidi, A. Sergent, and E. Ahouzi, "Performance of double phase encoding encryption technique using binarized encrypted images," *Optical Engineering*, **37**(2), pp. 565–569 (1998)

[7] Y. Li, K. Kreske, and J. Rosen, "Security and encryption optical systems based on a correlator with significant output images," *Applied Optics*, **39**(29), pp. 5295–5301 (2000)

[8] L. G. Neto and Y. Sheng, "Optical implementation of image encryption using random phase encoding," *Optical Engineering*, **35**(9), pp. 2459–2463 (1996)

[9] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," *Optical Engineering*, **39**(8), pp. 2031–2035 (2000)

[10] P. Refregier and B. Javidi, "Optical image encryption using input plane and Fourier plane random encoding," *Optics Letters*, **20**(7), pp. 767–769 (1995)

[11] J.-L. de Bougrenet de la Tocnaye, E. Que'mener, and G. Keryer, "Principle of pattern-signature synthesis and analysis based on double optical correlators," *Applied Optics*, **39**(2), pp. 199-211 (2000)

[12] N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," *Journal of Optical Society of America, A*, **16**(8), pp. 1915–1927 (1999)

[13] R.K. Wan, I. A. Watson, and C. Chatwin, "Random phase encoding for optical security," *Optical Engineering*, **35**(9), pp. 2464–2469 (1996)

[14] J.R. Fienup, "Phase retrieval algorithm: a comparison," *Applied Optics*, **22**(15) pp. 2758–2769 (1982)

[15] J.-H. Chen and A. Gersho, "Gain-adaptive vector quantization with application to speech coding," *IEEE Trans. on Communications*, **COM-35**(9), pp. 918–930 (1987)

[16] J.-S. R. Jang, "ANFIS: Adaptive-network-based fuzzy inference system," *IEEE Trans. on System, Man, and Cybernetics*, **23**(3), pp. 665–685 (1993)

[17] J.W. Goodman, *Introduction to Fourier Optics*, Second Edition, (McGraw-Hill, Singapore 1996), pp. 243–246 *Optical Engineering*, **38**(1), pp. 47–54 (1999)

[18] C.J. Kuo, H. Chien, N. Chang, and C.H. Yeh, "Diffractive optical element design by irregular etching-depth sequence," *Applied Optics*, **40**(32), pp. 5894–5897 (2001)

[19] J. Rosen, "Learning in correlators based on projection onto constraint sets," *Optics Letters*, **18**, pp. 1183–1185 (1993)

[20] S. E. Broomfield, M. A. A. Neil, E. G. S. Paige, "Programmable multiple-level phase modulation that uses ferroelectric liquid-crystal spatial light modulators," *Applied Optics-IP*, **34**(29), pp. 6652-6665 (1955)

[21] M.O. Freeman, T.A. Brown, and D.M. Walba, "Quantized complex ferroelectric liquid crystal spatial light modulators," *Applied Optics-IP*, **31**(20), pp. 3917–3929 (1992)

[22] H. Hamam, "Programmable multilayer diffractive optical elements," *Journal of Optical Society of America, A*, **14**(9), pp. 2223–2230 (1997)

[23] H. Sasaki, I. Fukuzaki, Y. Katsuki, and T. Kamijoh, "Design considerations of stacked multilayers of diffractive optical elements for optical network units in optical subscriber-network applications," *Applied Optics-IP*, **37**(17), pp. 3735–3745 (1998)

[24] X. Deng and R. Chen, "Design of cascaded diffractive phase elements for three-dimensional multi-wavelength optical interconnects," *Optics Letters*, **25**(14), pp. 1046–1048 (2000)

Input plane:
First phase mask
$\varphi_1(x, y)$

Lens

Fourier plane:
Second phase mask
$\psi_2(u, v)$

Lens

Output plane:
Recovered image
$g(x, y)$

$\longleftarrow f \longrightarrow$ $\longleftarrow f \longrightarrow$ $\longleftarrow f \longrightarrow$ $\longleftarrow f \longrightarrow$
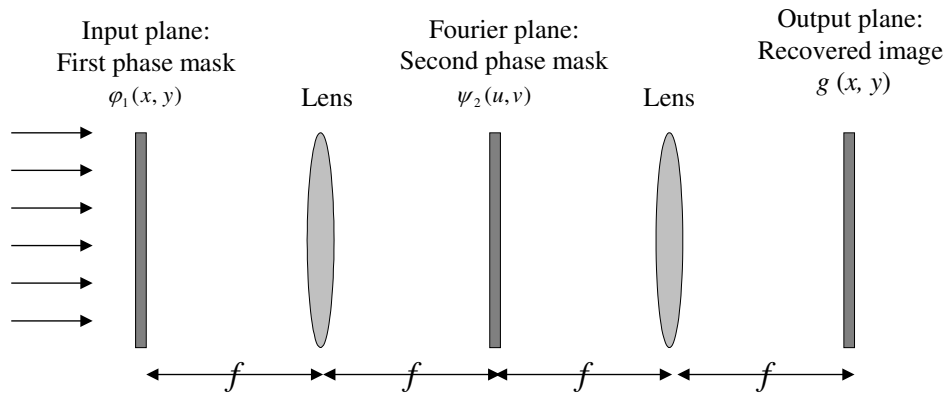
Figure 1: Optical setup of the 4-f correlator for optical security verification.
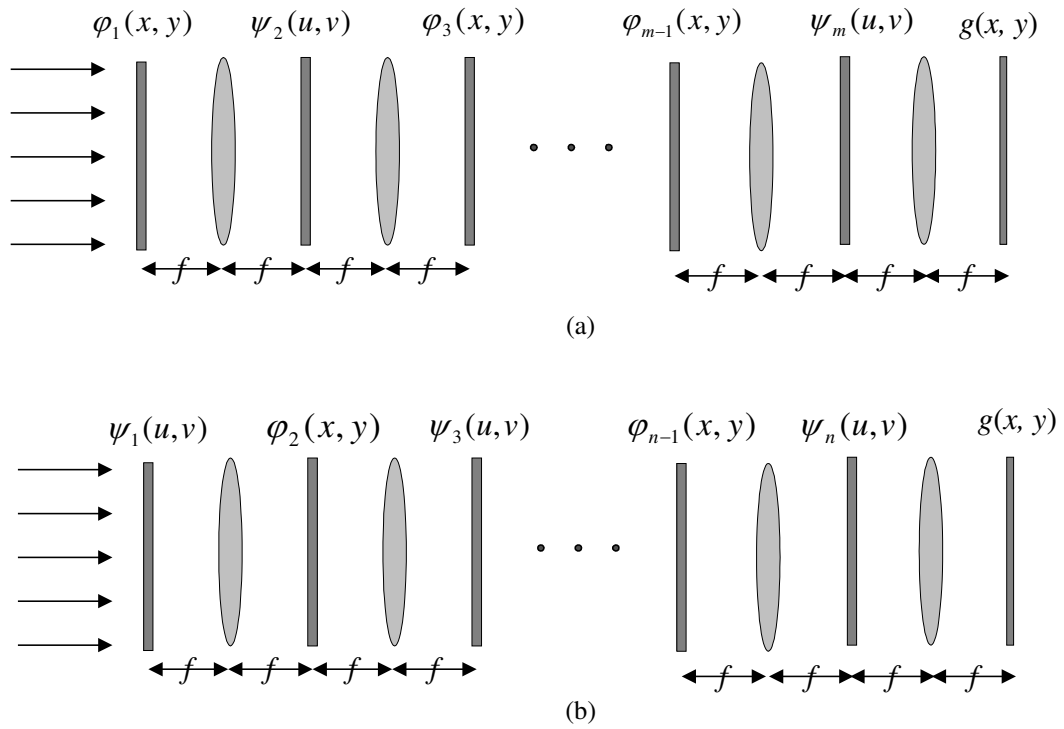
Figure 2: Optical setup of the multiple phase masks for optical verification systems: (a) the number of phase masks m is even, (b) the number of phase masks n is odd.
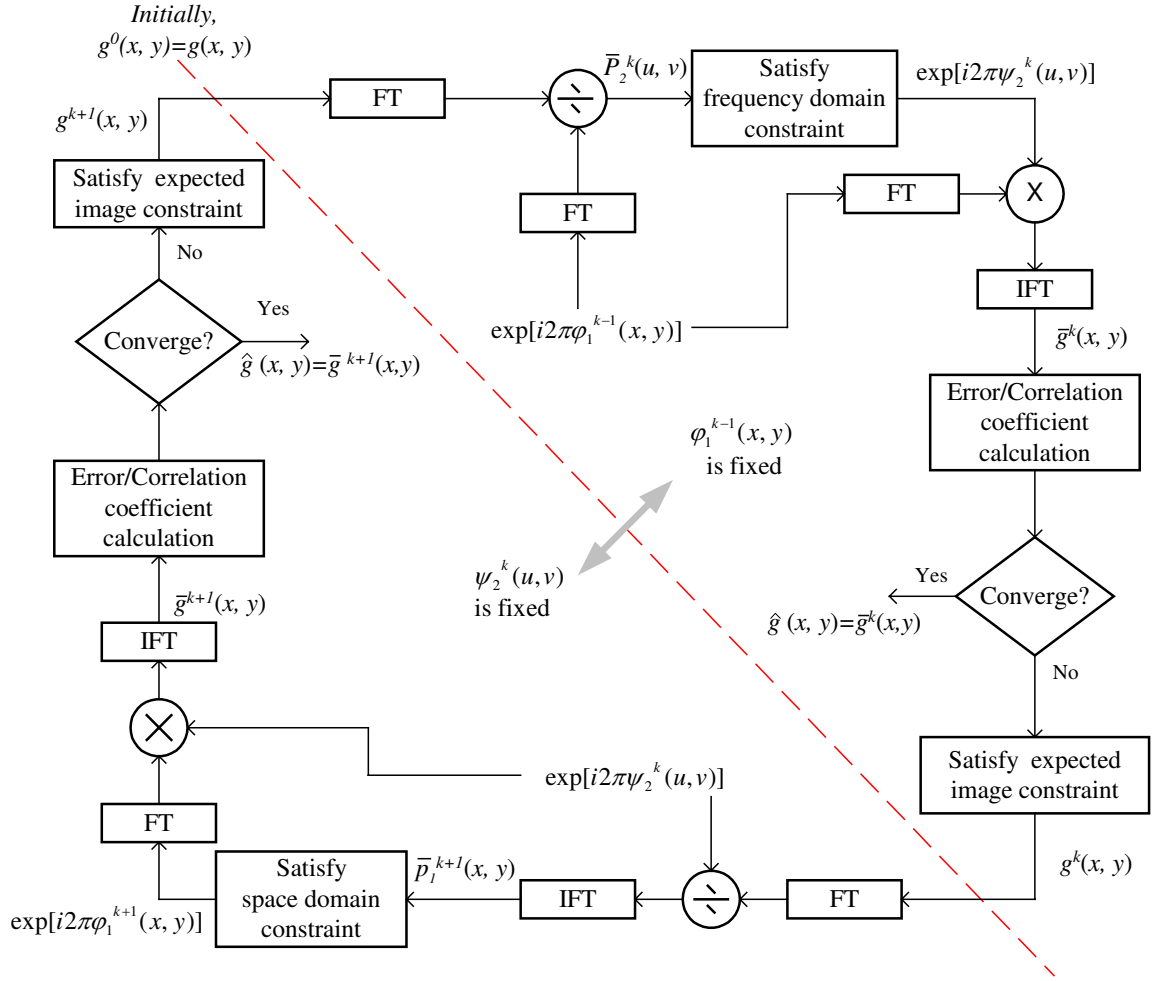
Figure 3: Block diagram of the double phases retrieval using the iteration algorithm.
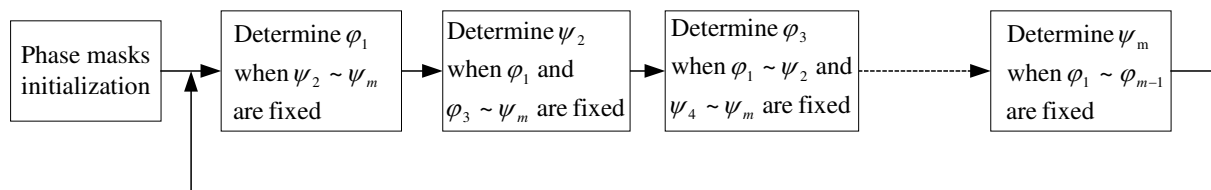
Figure 4: Block diagram of the multiple phases retrieval using the iteration algorithm.

(a)

(b)
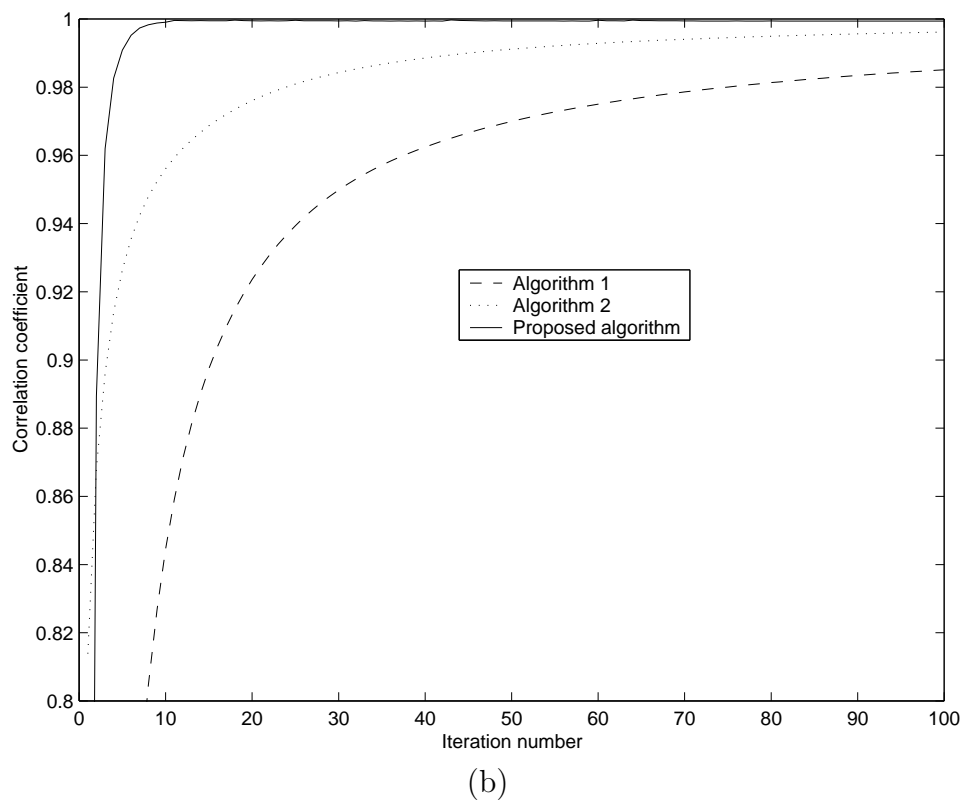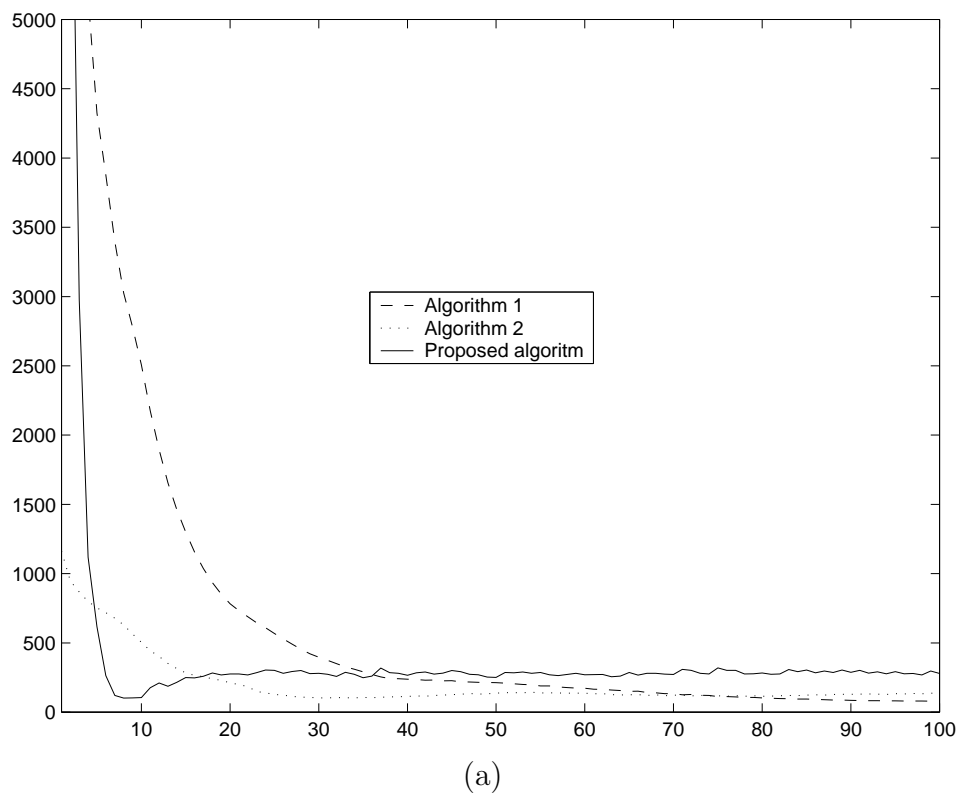
Figure 5: The comparison of the (a) MSE and (b) correlation coefficients between the recovered and the original images.

(a)

(b)

(c)

(d)

Figure 6: (a) The original image and the iterated images in the output plane after 100 iterations based on (b) Algorithm 1, (c) Algorithm 2, and (d) the proposed MPRA.
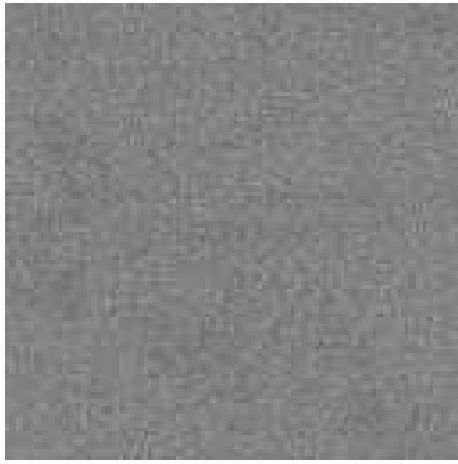
(a)
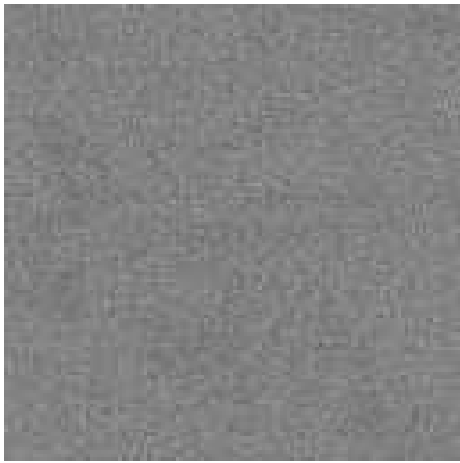
(b)

(c)

Figure 7: The error images between the original and the images retrieved from (a) Algorithm 1, (b) Algorithm 2, and (c) the proposed MPRA.
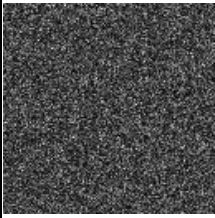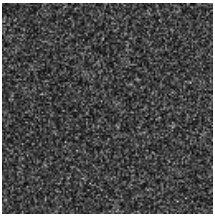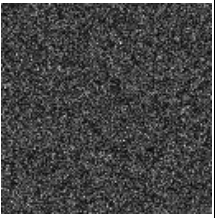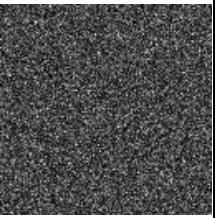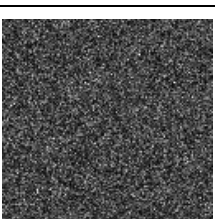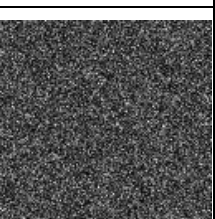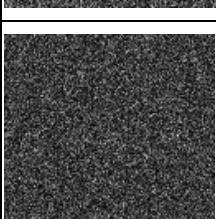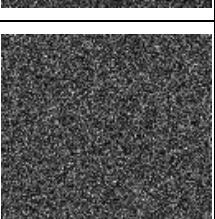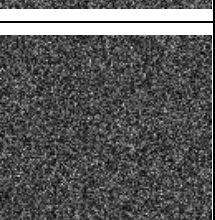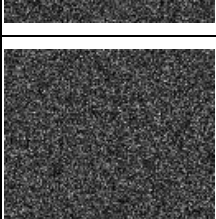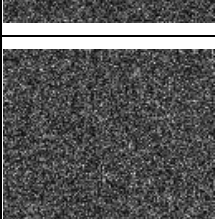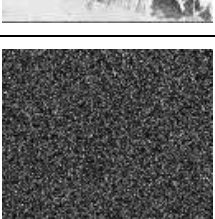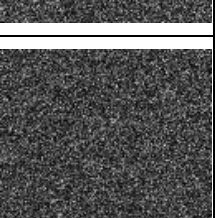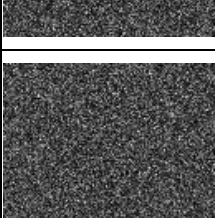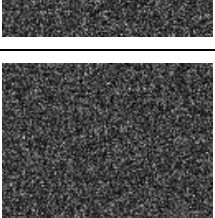
Figure 8: Table of all correlation results between five phase pairs, $\varphi_{1,i}(x,y), i = 1, \ldots, 5$ and $\psi_{2,j}(u,v), j = 1, \ldots, 5$. Only the phase pairs retrieved together from the same iteration process can recover the target image.
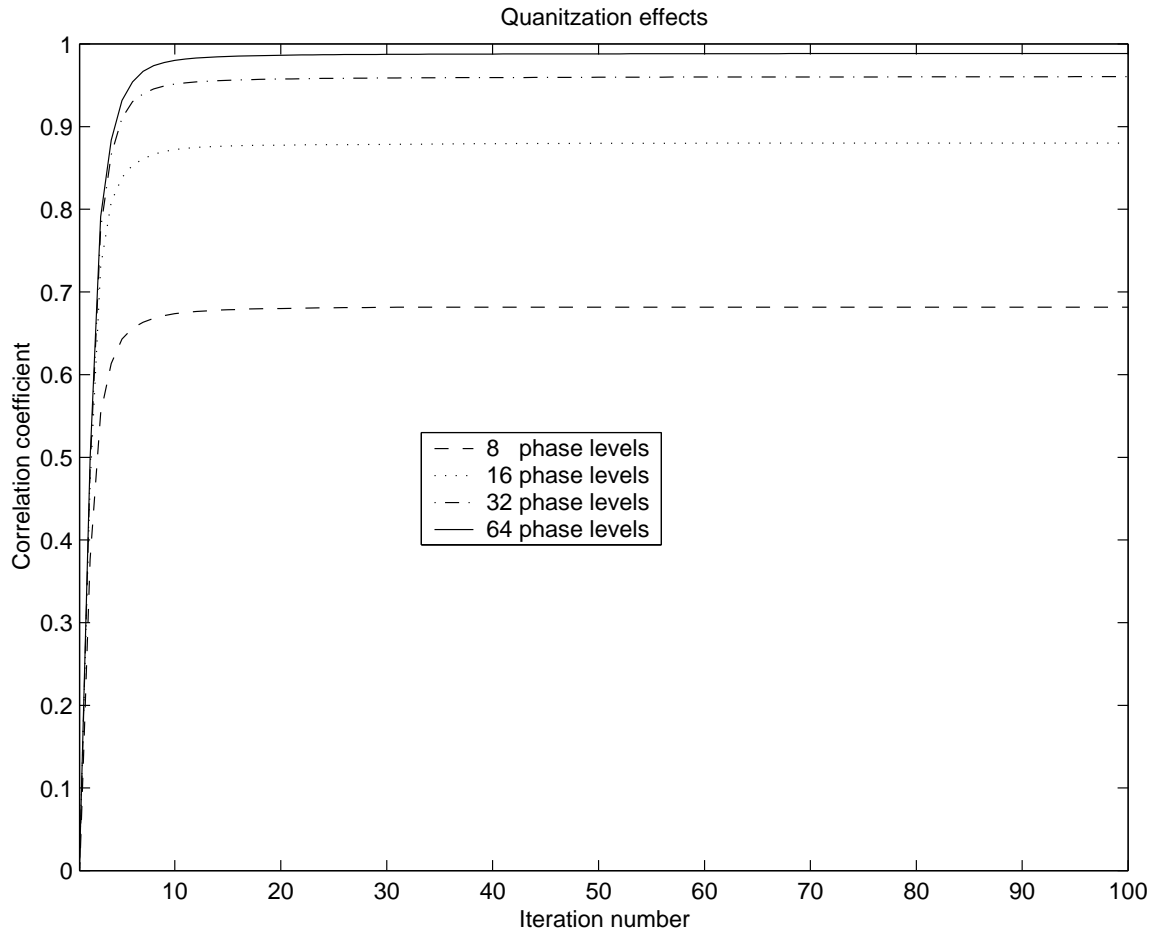
Figure 9: The comparison of the correlation coefficients under different phase resolutions (8, 16, 32, and 64 phase levels) for the proposed method with two phase masks.
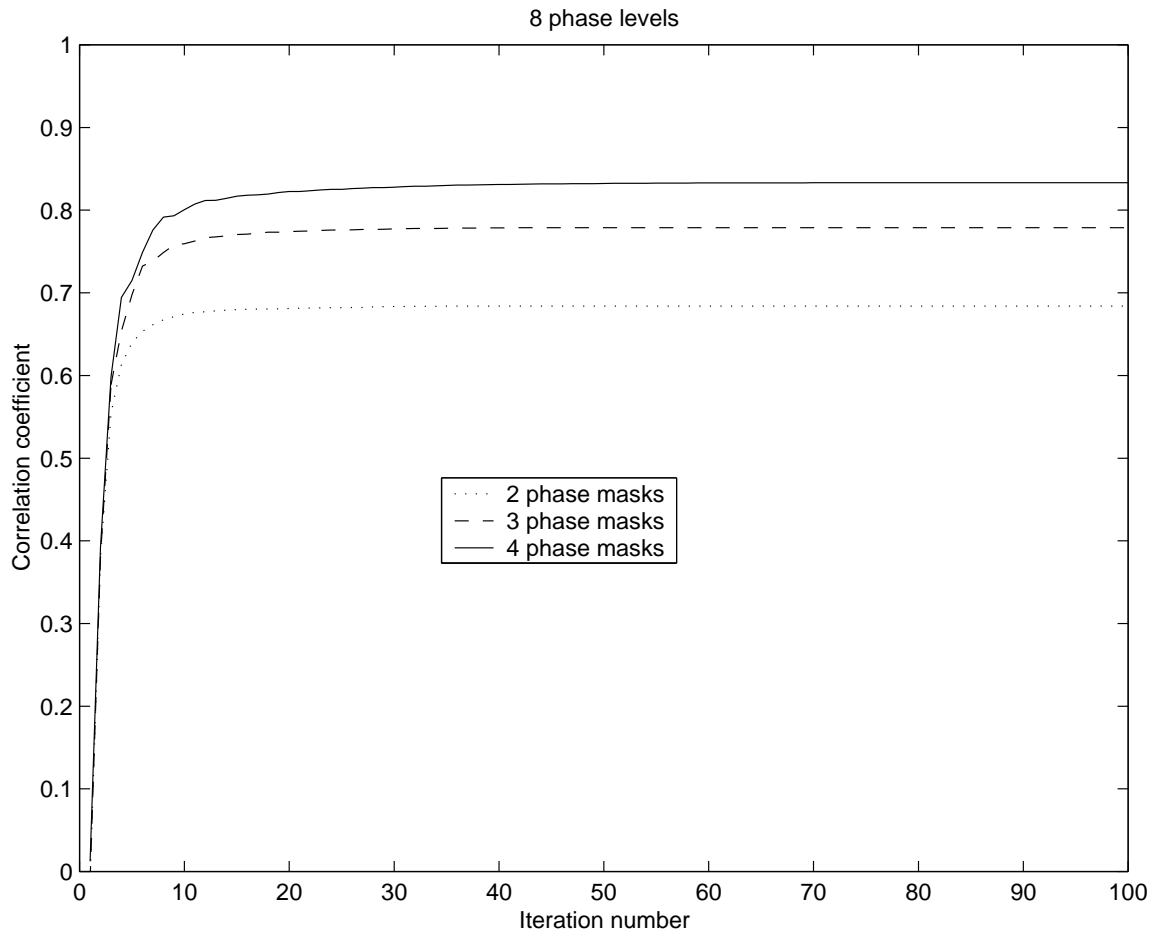
Figure 10: The comparison of the correlation coefficients using two, three, and four phase masks with eight phase levels in the proposed method.
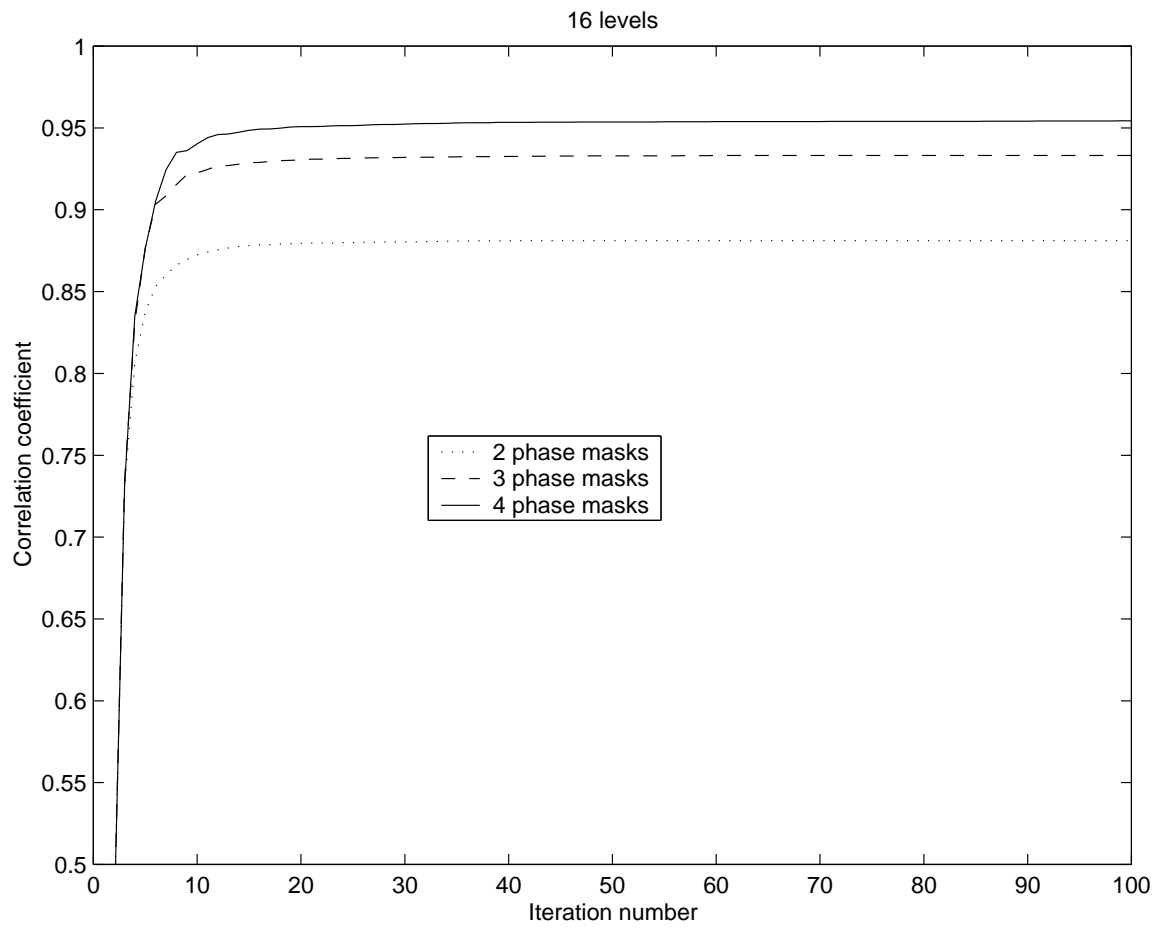
Figure 11: The comparison of the correlation coefficients using two, three, and four phase masks with 16 phase levels in the proposed method.
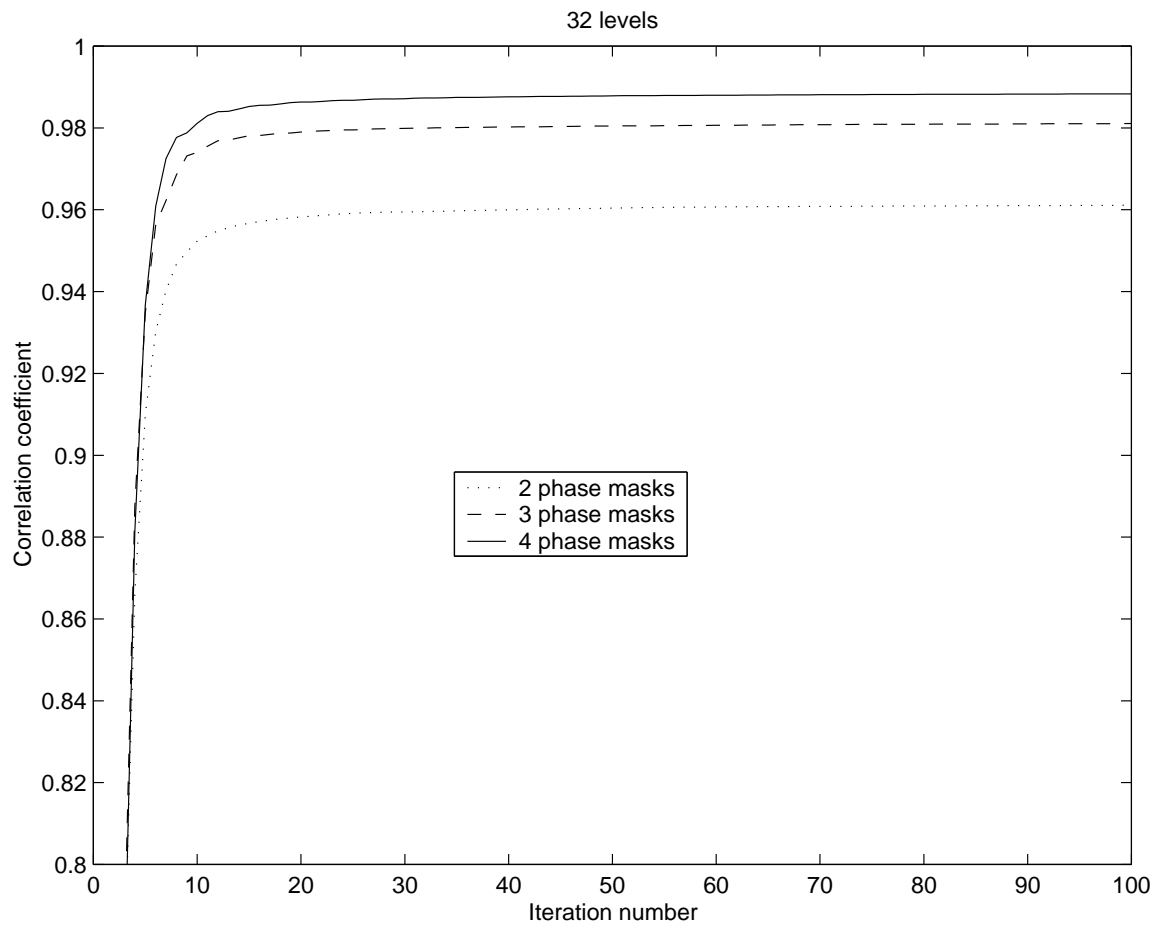
Figure 12: The comparison of the correlation coefficients using two, three, and four phase masks with 32 phase levels in the proposed method.
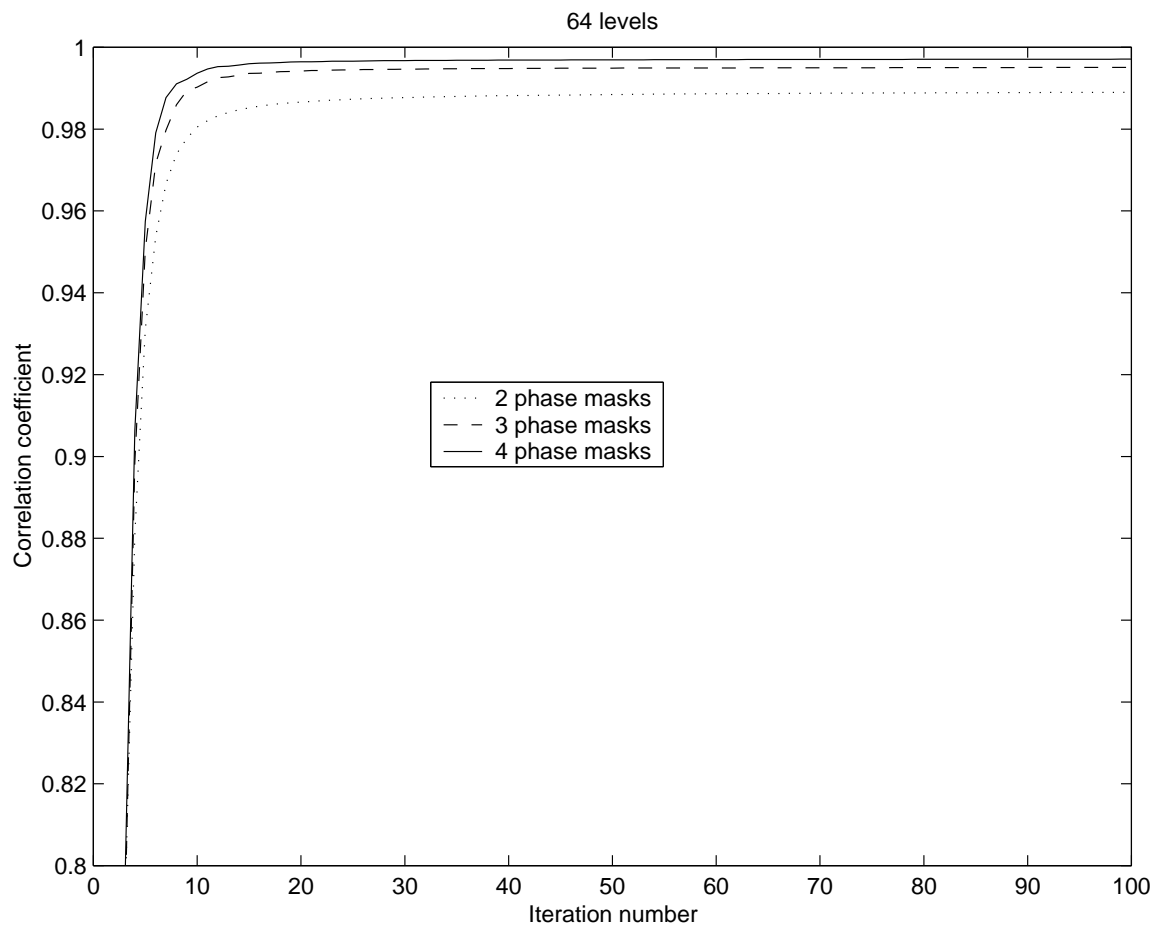
Figure 13: The comparison of the correlation coefficients using two, three, and four phase masks with 64 phase levels in the proposed method.