Image encryption using separable amplitude-based virtual image and iteratively retrieved phase information

Hsuan T. Chang, Member SPIE

Department of Electrical Engineering
National Yunlin University of Science and Technology
Touliu Yunlin, 640 TAIWAN R.O.C.
E-mail: hank1524@ms17.hinet.net

Abstract

An image cryptosystem that encrypts a plain image using an amplitude-based virtual image and a separable phase function is proposed. The proposed cryptosystem is based on a $4f$ optical correlator that is a common architecture for image encryption. Unlike the noise-like amplitude distribution of the encrypted data in conventional phase encoding techniques, the amplitude distribution in the proposed cryptosystem is meaningful and represented as a virtual image. Therefore, the illegal users who steal the virtual image could be confused or treat it as a plain image. The plain image, in fact, is encrypted by a separate phase function, which is iteratively retrieved by using the plain image, an arbitrary virtual image, and another fixed random phase function. The phase function is determined when both the iterated image and the plain image are identical or the error between both images is less than a threshold value. Two types of the cryptosystem are proposed such that the separate phase function can be located in either the input plane or the Fourier plane in a $4f$ correlator. The decryption process can be performed in digital methods or implemented by optics at high speed.

Subjective terms: image hiding, cryptosystem, image encryption, phase retrieval

Please send correspondence to Prof. Chang.

September 7, 2009

1 Introduction

With the fast progress of the data exchange in electronic commerce, information security becomes more and more important in data storage and transmission. Images are widely used in our daily life and thus the image encryption is important to protect data from counterfeiting and unauthorized access. Optical technologies have recently been employed in data security. Several algorithms and architectures for optical image encryption have been proposed.[1–5] The double random phase encryption techniques[1,2] for security purpose have been proposed to encrypt a plain (original) image into a noise-like cipher image. The plain image cannot be retrieved without using two correct phase keys. Although the encrypted result protects the plain image, illegal users will be interested in breaking the encryption since they will think the encrypted image is very important. Thus the noise-like cipher image will decrease the security of the cryptosystem. On the other hand, photorefractive crystals or holographic techniques are required to record the complex-value information (both the amplitude and the phase components) of the encrypted data. If the encrypted data consist of only the phase or the amplitude component, their recording and storage should be easier. As shown in previous studies[10,11] the phase component in the encrypted data is more important than the amplitude component for recovering the plain image. It is desirable to encrypt the original image into a phase function only. As to the amplitude component, an arbitrary virtual image is used to camouflage the original image such that the illegal users could be confused.

Two previous approaches[8,9] demonstrate the optical security systems in which the encrypted data of a plain image can appear as a phase-only function. Both encryption systems are based on a $4f$ correlator that correlates two phase-only functions. Figure 1 shows an optical correlator in a $4f$ configuration with three planes: the input plane in which the

input phase mask $p_1(x, y)$ is displayed, the Fourier plane in which the filter phase mask $P_2(u, v)$ is displayed, and the correlation plane in which the camera should record the output predefined image. The input phase mask $p_1(x, y)$ is employed as one kind of key, while the filter phase mask $P_2(u, v)$ is used as a lock that always exists within the system. The predefined image is recovered at the output (correlation) plane only if the true key $p_1(x, y)$ appears in the input. Otherwise, a scattered meaningless light distribution is expected there. The problem is to find two phase-only masks located in two different planes of the correlator. Both should yield on the output plane of some function whose amplitude is equal to a predefined image. On the other hand, the phase can get any value from 0 to 2π. Thus the phase part of the function at the output plane creates a degree of freedom. 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 desired image. The phase retrieval algorithms[7] and the projection-onto-constraint sets (POCS) algorithm[13] can be used to solve the problem described here. The phase retrieval algorithm produces the phase mask at the spatial-frequency domain (i.e., the Fourier plane) with constraints via Fourier transform methods. On the other hand, in the POCS algorithm, a function is transformed back and forth between two domains. Appropriate constraints are employed until the function converges, in the sense that the error between the desired and the recovered image is minimal.

In this paper, we propose the image cryptosystem that employs the amplitude-based virtual image to camouflage the original one in addition to the two phase-only masks described above. The plain image in fact is hidden in one of two phase-only functions. The virtual image can be arbitrarily chosen and then be compressed by various coding schemes. It cannot be correctly decoded without knowing the correct coding scheme. Even if illegal users steal the encrypted data, which is composed of the amplitude (virtual

image) and phase components, most of them will treat the decoded amplitude (virtual image) as an original image, ignore the phase component, and will not intend to break it. The current problem is to find a phase mask, together with a given virtual image and a fixed phase mask, to yield on the output plane of some function whose amplitude is equal to a predefined image. The desired phase mask can be placed either at the input plane or at the Fourier plane. Previous studies[8,9] have shown that only the phase component can recover the original image with minimal error. Therefore, the proposed cryptosystem provides an additional flexibility in selecting a virtual image, which is independent of the phase component. The methods shown in Refs8 and 9 can thus be considered as the special cases of the proposed cryptosystem when the normalized pixel value in the virtual image is unity. A digital virtual image cryptosystem based on vector quantization technique has been reported in Ref. 6. However, compared to the optics-based methods, its algorithm is very complicated and (hard to be implemented by hardware.

2 Proposed Cryptosystem

Due to the separable property, the amplitude-based virtual image and the retrieved phase component can be placed in either the same plane or different planes in a $4f$ correlator. Figures 2 and 3 show the Type-1 and Type-2 architectures of the proposed cryptosystem respectively. In Type-1 architecture, the retrieved phase $p_s(x, y)$ is located in the input plane. The virtual image can be located in either the input plane (Type-1(a) configuration shown in Fig. 2(a)) or the Fourier plane (Type-1(b) configuration shown in Fig. 2(b)). In Type 2 architecture, on the other hand, the retrieved phase $P_s(u, v)$ is located in the Fourier plane. The virtual image can be located in either the input plane (Type-2(a) configuration shown in Fig. 3(a)) or the Fourier plane (Type-2(b) configuration shown in Fig. 3(b)). Four optical configurations are used in the proposed cryptosystem. In the rest of this paper,

we focus on two configurations (Type-1(a) and Type-2(a)) since the other configurations can be analyzed in similar ways.

The phase for encrypting the plain image can be retrieved based on a predefined image $f(x, y)$, a random phase, and an arbitrary virtual image. To recover the plain image in the output plane, the amplitude-based virtual image, the retrieved phase, and a fixed random phase mask are all required and must be located in their corresponding planes. A noise-like cipher image is expected when any of the three components above is not located in the correct plane. Therefore, the positions of the phase masks and the virtual image also create a degree of freedom. In the transmitting or storing stage, the virtual image can be compressed by some coding technique to reduce the data amount. Illegal users cannot decompress the virtual image without knowing the correct decoding scheme. Moreover, if there are the same image databases at both the transmitter and the receiver, the virtual image can be transmitted by its name or an index in the database. Thus the amount of the data in a virtual image is reduced and negligible. Illegal users without owning the same image database or knowing the indexing scheme used in the database cannot retrieve the virtual image. The security in the proposed cryptosystem is increased.

The purpose of this work will focus on the retrieval of the phase component $P_s(u, v)$ in Type-1 architecture and $p_s(x, y)$ in Type-2 architecture such that the plain image $f(x, y)$ can be obtained in the output plane. In encryption, the phase retrieval algorithm[7] is employed to determine the phase component based on an arbitrary virtual image $g(x, y)$, a fixed phase mask, and a predefined plain image $f(x, y)$. The iteration process in the phase retrieval algorithm is composed of backward and forward operations. The iteration process stops when the error between the plain image $f(x, y)$ and the iterated image $\hat{f}(x, y)$ is less than a threshold value. In decryption, with the retrieved phase component, the given virtual image, and the same fixed phase mask in encryption, the iterated image $\hat{f}(x, y)$ can

be directly recovered in the output plane by using intensity detection devices. Alternatively, as shown in the method of fully phase encryption in Ref. 2, the virtual image can also be represented in the phase format such that a plain image can be obtained in the output plane.

3 Iterative Phase Retrieval

3.1 Type-1(a) configuration

Figures 4(a) and 4(b) show the block diagrams of the iterative phase retrieval algorithm for the proposed Type-1(a) and Type-2(a) configurations shown in Figs. 2(a) and 3(a), respectively. In Type-1(a) configuration, the separate phase component $p_s(x, y)$ is located in the input plane together with the virtual image $g(x, y)$. As shown in Fig. 4(a), the plain image $f(x, y)$ is first Fourier transformed and then divided by the phase term $\exp[i2\pi P_1(u, v)]$ obtained from the fixed phase key. Let $\bar{F}(u, v) = \mathrm{FT}\{f(x, y)\}/\exp[i2\pi P_1(u, v)]$, where FT denotes the Fourier transform. The initial phase key $p_s^0(x, y)$ can be selected by the phase part of $\mathrm{IFT}\{\bar{F}(u, v)\}/g(x, y)$ or be randomly generated to avoid possible zero values in $g(x, y)$. The backward and forward operations in the iteration process are traced as follows: Suppose the iteration reaches kth step ($k = 1, 2, 3, \ldots$), the iterated image $f^{k'}(x, y)$ is obtained in the output plane. By tracing the backward operation shown in Fig. 4(a), we obtain

$$\bar{F}^k(u, v) = \mathrm{FT}\{f^{k'}(x, y)\}/\exp[i2\pi P_1(u, v)] \tag{1}$$

in the Fourier plane and

$$h^k(x, y) = \bar{f}^k(x, y)/g(x, y) \tag{2}$$

in the input plane, where $\bar{f}^k(x, y)$ is the inverse Fourier transform (IFT) of $\bar{F}^k(u, v)$. To satisfy the space domain (input plane) constraint, only the phase part of $h^k(x, y)$ is extracted.

Thus,

$$\exp[i2\pi p_s^k(x,y)] = h^{k'}(x,y), \tag{3}$$

where $h^{k'}(x,y)$ is the phase part of $h^k(x,y)$. In forward operation, the $(k+1)$th iterated image $f^{k+1}(x,y)$ obtained in the output plane is expressed by

$$f^{k+1}(x,y) = \mathrm{IFT}\{\exp[i2\pi P_1^k(u,v)]\mathrm{FT}\{g(x,y)\exp[i2\pi p_s^k(x,y)]\}\}. \tag{4}$$

To calculate the error between the iterated image and the plain image, only the amplitude of the complex function $f^{k+1}(x,y)$, $|f^{k+1}(x,y)|$, is used. The error function in Fig. 4(a) determines the mean-squared error (MSE) between the original and the iterated image, which is defined by

$$\mathrm{MSE} = \frac{1}{m \times n}\sum_{x=1}^{m}\sum_{y=1}^{n}[|f(x,y)| - |f^{k+1}(x,y)|]^2, \tag{5}$$

where $m \times n$ denotes the size of the image. MSE can be used to control the iteration number. If the MSE is less than a threshold value, the iterated phase $p_s(x,y)$ is determined (i.e., $p_s(x,y) = p_s^{k+1}(x,y)$) and the iteration process stops. The iterated image here will turn to the recovered image $\hat{f}(x,y)$ in decryption. Otherwise, an expected image constraint is applied to the iterated image. To satisfy the expected image constraint, we set a threshold for the pixel value in the iterated image $f^{k+1}(x,y)$. If the MSE between the iterated image and the original image is greater than a threshold value η_{th}, the pixel value in the iterated image is set to the value in original image. Otherwise, the pixel values in the iterated image are preserved. That is,

$$|f^{k'+1}(x,y)| = \begin{cases} |f^{k+1}(x,y)|, & \text{if } |\bar{g}^k(x,y) - g(x,y)| \le \eta_{\mathrm{th}}, \\ f(x,y), & \text{if } |\bar{g}^k(x,y) - g(x,y)| > \eta_{\mathrm{th}}, \end{cases} \tag{6}$$

and this completes the forward operation. In decryption, the determined phase is placed in the input plane together with the virtual image $g(x,y)$. To recover the original image, the phase component $\exp[i2\pi p_s(x,y)]$ and the virtual image $g(x,y)$ in the input plane are

Fourier transformed and multiplied by the phase function $\exp[i2\pi P_1(u,v)]$. Finally, they are inverse Fourier transformed by lens to obtain the original image, which can be detected by a CCD camera. When the normalized amplitude in the virtual image is unity, this is the special case shown in Ref. 9, in which only the retrieved phase located in the input plane is required.

3.2 Type-2(a) configuration

Figure 4(b) shows the block diagram of the iteration algorithm for the Type-2(a) configuration. The retrieved phase $P_s(u,v)$ is located in the Fourier plane. The virtual image $g(x,y)$ is located in the input plane together with the fixed phase mask $p_1(x,y)$. Let $\bar{G}(u,v) = \mathrm{FT}\{g(x,y)\exp[i2\pi p_1(x,y)]\}$. The initial phase key $P_s^0(u,v)$ can be selected by the phase part of $\mathrm{FT}\{f(x,y)\}/\bar{G}(u,v)$ or randomly generated to avoid possible zero values in $\bar{G}(u,v)$. Suppose the iteration reaches kth step ($k = 1, 2, 3, \ldots$), the iterated image $f^{k'}(x,y)$ is obtained in the output plane. Then, by tracing the backward operation shown in Fig. 4(b), we obtain

$$H^k(u,v) = F^{k'}(u,v)/\bar{G}(u,v), \tag{7}$$

where $F^k(u,v) = \mathrm{FT}\{f^{k'}(x,y)\}$. To satisfy the frequency domain (Fourier plane) constraint, only the phase part of $H^k(u,v)$ is extracted. Thus

$$\exp[i2\pi P_s^k(u,v)] = H^{k'}(u,v), \tag{8}$$

where $H^{k'}(u,v)$ denotes the phase part of $H^k(u,v)$. In forward operation, the $(k+1)$th iterated image $f^{k+1}(x,y)$ obtained in the output plane is expressed by

$$f^{k+1}(x,y) = \mathrm{IFT}\{\exp[i2\pi P_s^k(u,v)]\bar{G}(u,v)\}. \tag{9}$$

To calculate the error between the iterated image and the plain image, only the amplitude of the complex function $f^{k+1}(x,y)$, $|f^{k+1}(x,y)|$, is used. The expected image constraint

and the error function are the same as that in Type-1(a) configuration. If the MSE is less than a threshold value, the iteration process stops and the retrieved phase component is determined. That is, $p_s(x,y) = p_s^{k+1}(x,y)$. To recover the original image, the retrieved phase $p_s(x,y)$ together with the virtual image $g(x,y)$ placed in the input plane are Fourier transformed , multiplied by the phase function $\exp[i2\pi P_1(u,v)]$, and finally inverse Fourier transformed by a lens to obtain the plain image $\hat{f}(x,y)$, which can be detected by a CCD camera. When the normalized amplitude in the virtual image is unity, this is the special case shown in Ref. 8, in which only the retrieved phase located in the Fourier plane is required.

4 Simulation Results

In computer simulation, the Lena and the Jetplane images shown in Fig. 5 are used as the plain and the virtual image respectively. Both images are of size 128×128 and 8-bit resolution. The threshold value η_{th} used for the expected image constraint in Eqn. 6 is 3. In Type-1(a) configuration, the iterative algorithm shown in Fig. 4(a) is used to determine the separate phase component $p_s(x,y)$ in the input plane. By using Eqns. 1–5, the calculated MSE corresponding to each iteration is shown in Fig. 6 and represented by a dotted line. The final phase distribution of the phase key $p_s(x,y)$ is shown in Fig. 7(a). Here, the range of phase distribution, $[0, 2\pi]$, is normalized to the range of gray scale, [0, 255]. Figure 7(b) shows the recovered image $\hat{f}(x,y)$ with a correct phase key and a correct virtual image in Type-1(a) configuration. As shown in this figure, the decrypted image is well recovered since the MSE in Fig. 6(a) is small. With regard to Type-2(a) configuration, the iterative phase retrieval algorithm shown in Fig. 4(b) is used to determine the separate phase key $P_s(u,v)$, which is placed in the Fourier plane. By using Eqns. 5–9, the calculated MSE corresponding to each iteration is shown in Fig. 6 and represented by a solid line. The

final phase distribution of the phase key $P_s(u, v)$ is shown in Fig. 8(a). Figure 8(b) shows the recovered image $\hat{f}(x, y)$ by using a correct phase key and a correct virtual image in Type-2(a) configuration. Obviously, this image quality is very close to that in Fig. 7(b) since Type-1(a) and Type-2(a) configurations have similar MSE.

Two phase masks are used in the proposed cryptosystem. The phase mask $P_1(u, v)$ or $p_1(x, y)$ is fixed as a lock and independent of plain images. The other $p_s(x, y)$ or $P_1(u, v)$ is iteratively retrieved as a key and dependent on the plain images. We cannot recover the plain image without the correct virtual image and the retrieved phase component. The recovered image will be noise-like if we use a wrong phase key or a wrong virtual image. The accuracy for optical alignment and the shift tolerance for conventional double-random phase encryption have been discussed in Ref. 11. The accuracy requirements of the three components (the virtual image and two phase masks) for the proposed cryptosystem would be studied in our future work. On the other hand, other configurations, such as Type 1(b) and Type 2(b), are expected to obtain similar performance to Type 1(a) and Type 2(a). We can obtain their simulation results based on the similar procedure for Type-1(a) and Type-2(a) configurations.

5 Conclusion

In conclusion, we propose an optical image cryptosystem in which the encrypted data are composed of a meaningful virtual image and a separate phase component. While stealing the virtual image, the illegal users could be confused or treat it as the original image. Moreover, the flexibility provided from the virtual image also enhances the additional security in the proposed cryptosystem. The original image is, in fact, hidden in the retrieved phase component, which is obtained by the iterative phase retrieval algorithm. Two types of optical architectures are proposed such that the retrieved phase component can be placed

either in the input plane or the Fourier plane. According to the simulation results, both types of the proposed cryptosystem can successfully encrypt a plain image by a virtual image and a separable phase function.

Acknowledgment

This work is partially supported by National Science Council under the contract NSC 89-2213-E-324-050.

References

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

2. 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)

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

5. B. Zhu and S. Liu, "Optical image encryption based on multifractional Fourier transformation," *Optics Letters*, **25**(16) pp. 1159–1161 (2000)

6. T.-S. Chen, C.-C. Chang, and M.-S. Hwang, "A virtual image cryptosystem based upon vector quantization," *IEEE Trans. Image Process*, **7**(10) pp. 1485–1488 (1998)

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

8. R.K. Wang and I.A. Watson, "Random phase encoding for optical security," *Optical Engineering*, **35**(9) pp. 2464–2469 (1996)

9. 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)

10. M.H. Hayes, "The reconstruction of a multidimensional sequence from the phase or amplitude of its Fourier transform," *IEEE Trans. on Acoust., Speech, and Sig. Proc.,* **ASSP-30** pp. 140–154 (1982)

11. B. Wang, C.-C. Sun, W.-C. Su, and Arthur E.T. Chiou, "Shift-tolerance property of an optical double-random phase-encoding encryption system," *Applied Optics*, **39**(26) pp. 4788–4793 (2000)

12. 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, Feb. 1998

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

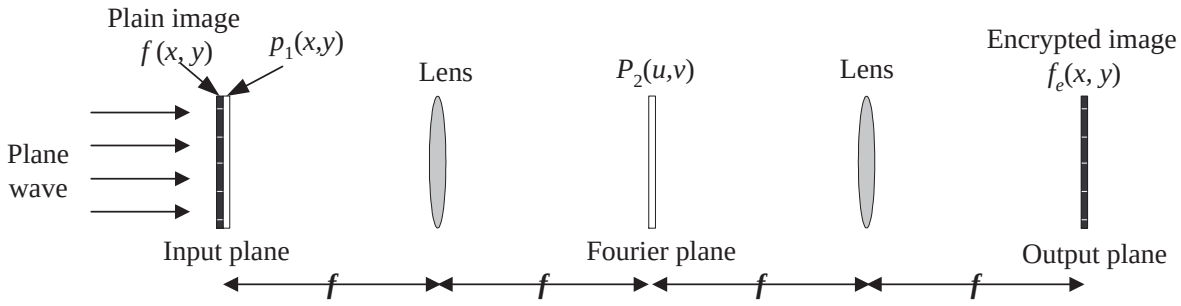


Figure 1: $4f$ correlator used for optical security verification.

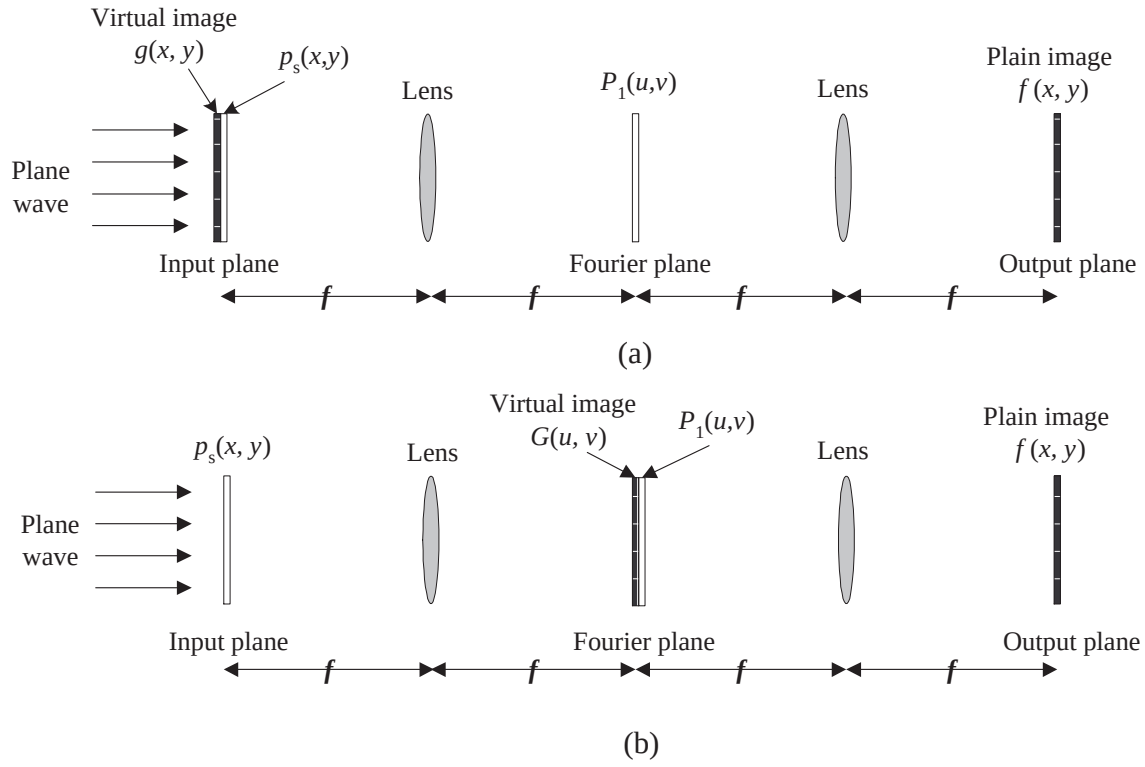


Figure 2: Type-1 architecture for the proposed image cryptosystem, in which the retrieved phase component $p_s(x, y)$ is located in the input plane. (a) The virtual image $g(x, y)$ is located in the input plane (Type-1(a) configuration). (b) The virtual image $G(u, v)$ is located in the Fourier plane (Type-1(b) configuration).

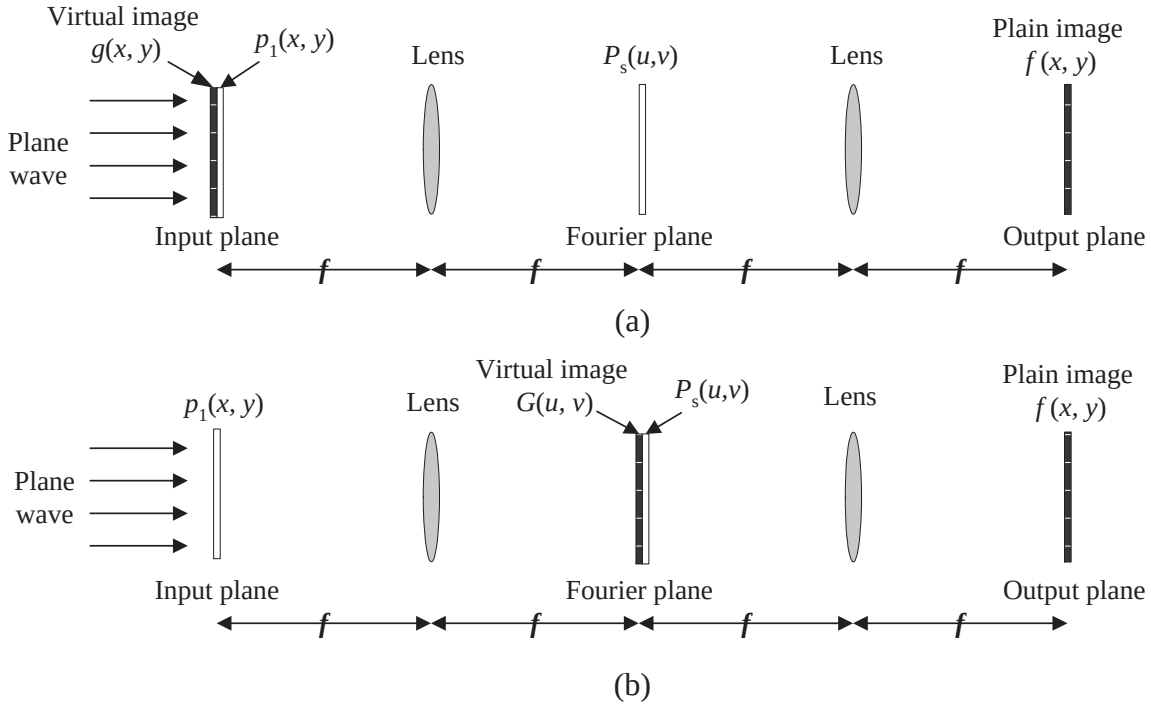


Figure 3: Type-2 architecture for the proposed image cryptosystem, in which the retrieved phase component $P_s(u, v)$ is located in the Fourier plane. (a)The virtual image $g(x, y)$ is located in the input plane (Type-2(a) configuration). (b) The virtual image $G(u, v)$ is located in the Fourier plane (Type-2(b) configuration).

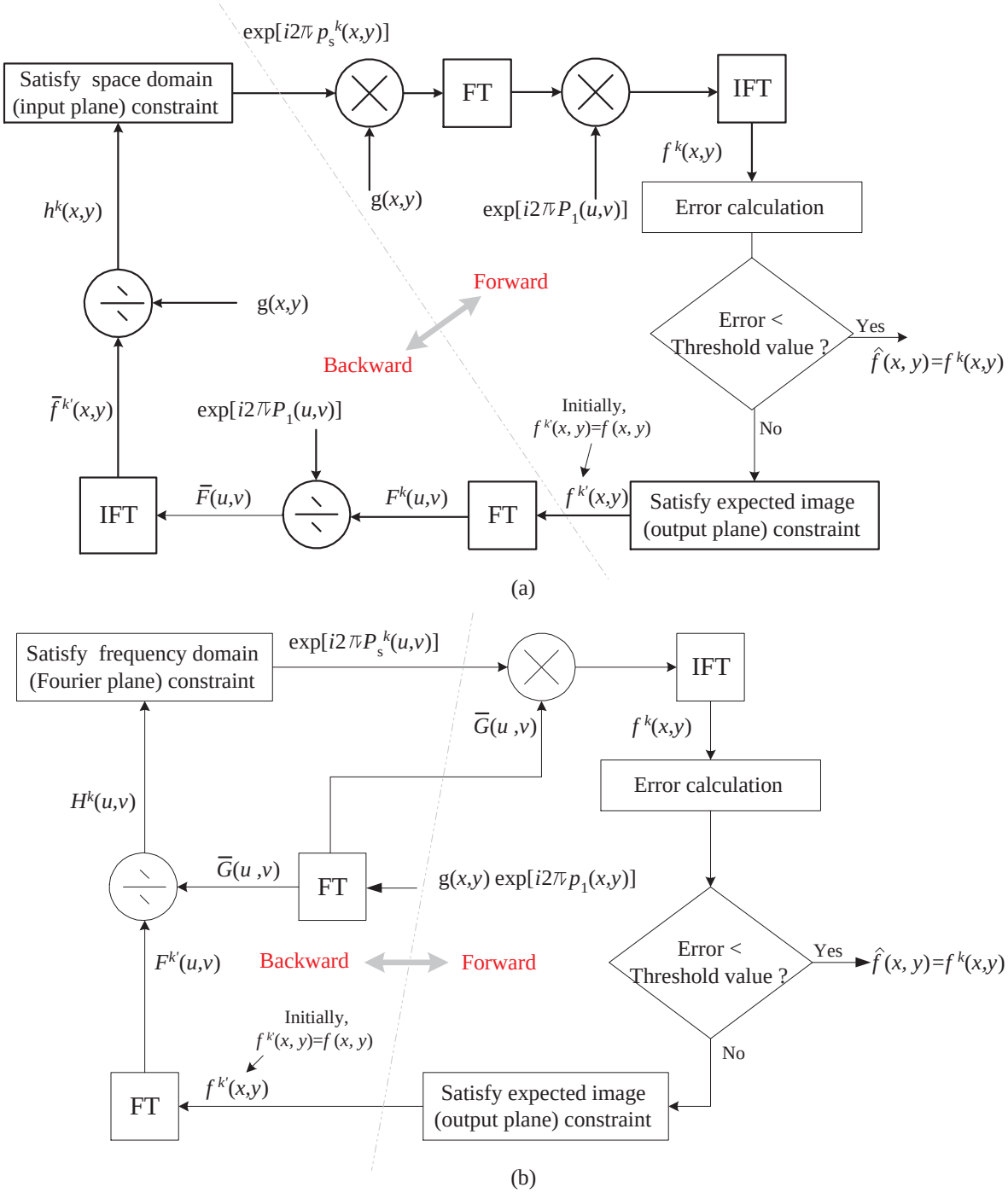


Figure 4: Block diagram of the iterative phase retrieval algorithm in the proposed cryptosystem with: (a) Type-1(a) configuration and (b) Type-2(a) configuration.

(a) (b)

Figure 5: (a) The original image $f(x, y)$: Lena (b) The virtual image $g(x, y)$: Jetplane.

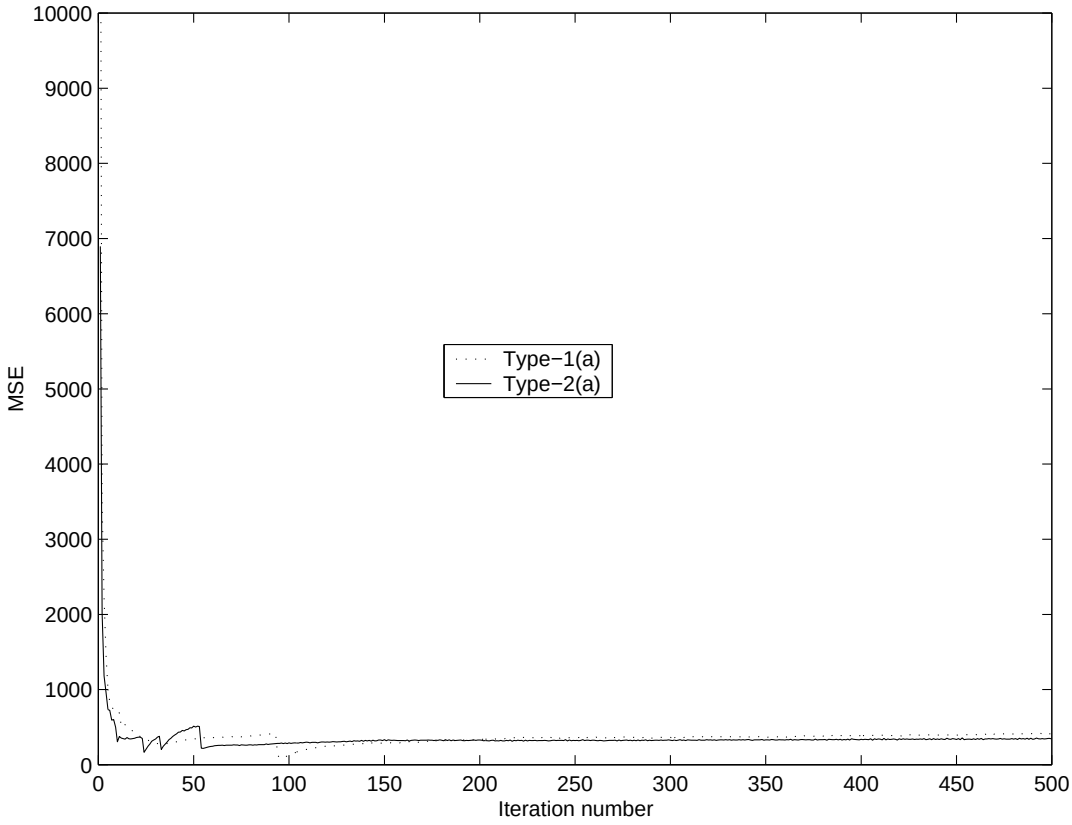
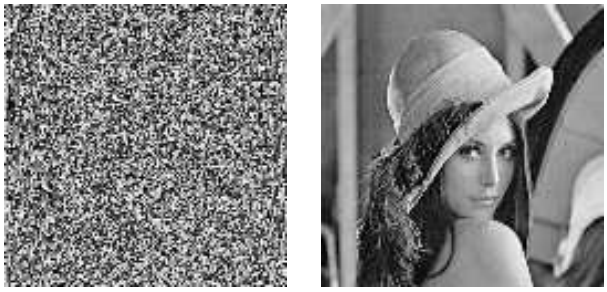


Figure 6: MSE for Type-1(a) and Type-2(a) configurations during the iteration process.



(a) (b)

Figure 7: (a) The separate phase key $p_s(x, y)$ generated by using the iterative phase retrieval algorithm and (b) the recovered image $\hat{f}(x, y)$ from Type-1(a) configuration.

(a) (b)

Figure 8: (a) The separate phase key $P_s(u, v)$ generated by using the iterative phase retrieval algorithm and (b) the recovered image $\hat{f}(x, y)$ from Type-2(a) configuration.