Double image encryption based on random phase encoding in the fractional Fourier domain

Ran Tao*, Yi Xin, and Yue Wang

Department of Electronic Engineering, Beijing Institute of Technology, Beijing 100081, China
rantao@bit.edu.cn

Abstract: A novel image encryption method is proposed by utilizing random phase encoding in the fractional Fourier domain to encrypt two images into one encrypted image with stationary white distribution. By applying the correct keys which consist of the fractional orders, the random phase masks and the pixel scrambling operator, the two primary images can be recovered without cross-talk. The decryption process is robust against the loss of data. The phase-based image with a larger key space is more sensitive to keys and disturbances than the amplitude-based image. The pixel scrambling operation improves the quality of the decrypted image when noise perturbation occurs. The novel approach is verified by simulations.

©2007 Optical Society of America

OCIS codes: (070.4560) Fourier optics and signal processing: Data processing by optical means; (090.0090) Holography: Holography; (100.2000) Image processing: Digital image processing.

References and links

1. Introduction

With the rapid development of networked multimedia technique, the information security of images is facing more and more challenges nowadays. Optical systems are of growing interests for image encryption because of their distinct advantages of processing two-dimensional complex data in parallel and at high speed. In the past decade, a number of optical encryption methods have been proposed [1-23]. Among them, the most widely used and highly successful optical encryption scheme is double random phase encoding proposed by Refregier and Javidi [1]. This method uses two random phase masks, one in the input plane and the other in the Fourier plane, to encrypt the primary image into stationary white noise [1, 2]. As the generalization of the conventional Fourier transform, the fractional Fourier transform (FRFT) [24] has recently shown its potential in the field of optical security. Unnikrishnan and Singh [4, 5] first proposed an optical encryption method using random phase encoding in the fractional Fourier domain and its optically-implemented approach. The two Fourier transform operators in Ref. 1 were replaced by two FRFT operators. The remarkable feature of optical encryption based on the FRFT is the fractional order, which enlarges the key space and further enhances the security of encryption systems. Various optical encryption schemes based on the FRFT have been reported since 2000 [4-15, 23].

Most of these encryption techniques in the literature are dealing with a single amplitude image (i.e. binary text, greyscale or color image). However, in some cases, one need to encrypt two images with certain relations such as two pictures of an object or a picture and its binary text for description, etc., which are often stored or transmitted together. Encrypting the two images directly using the single-image encryption algorithms mentioned in the literature results in two separate encrypted images with random noise distribution, and sometimes, there arises the difficulty in distinguishing between them before decryption; and the decryption has to be conducted twice to recover the two images. Recently, a number of multiplexing techniques for double or multiple image encryption have been proposed, including a prior work on encrypted optical memory system in the Fresnel domain [18], but images are not encrypted simultaneously because the multiplexing is achieved by the rotation...
of the LiNbO$_3$ crystal, and the encrypted images are recorded at different locations individually in the crystal. Reference [19] proposed a method of multiple signal encoding and simultaneous authentications. The two reference images, both encoded to phase functions, were encrypted to a single complex-amplitude image; the authentication without decryption was accomplished by an optical processor which involves a nonlinear joint transform correlator (JTC) and a classical 4f correlator. Multiple images can also be encrypted by using wavelength multiplexing [20] or position multiplexing methods [21], but the qualities of decrypted images are not perfect due to the cross-talk effects between images. Meng and Cai [22] presented a double image encryption and watermarking method with amplitude-phase separate modulations, which avoids cross-talk between two images in reconstruction. Z. Liu and S. Liu [23] also proposed a scheme by which two images can be simultaneously encrypted into a single one by the phase retrieval algorithm based on the FRFT. Both Ref. 22 and 23 made good use of the amplitude and phase information of complex values. However, the former used a lensless system whose key space can be enlarged further, while the latter must adopt a constant to equalize the energies of the two input images to satisfy the Parseval energy conservation theorem, and the encrypted image is not a stationary white noise.

Inspired by the architecture of the fully phase encoding [3, 6, 7] and pixel scrambling (random shifting) techniques [12, 14, 15], we propose a novel method which can convert two images into one encrypted image based on the double random phase encoding in the fractional Fourier domain. The effects of noise perturbations on the encrypted data are also studied. The novel approach does not have a symmetrical response on the two decrypted images when noise perturbation or blind decryption occurs. It provides flexibility in security hierarchy when required.

2. Principle of encryption/decryption

The FRFT is the generalization of the conventional Fourier transform. One-dimensional notation is used to simplify the symbols. Let $x_0$ and $x_a$ denote the coordinates of the input spatial domain and the output $a$th fractional domain, respectively. The FRFT of function $f(x_0)$ with order $a$ can be defined [24] as

$$F_a[f(x_0)] = \int_{-\infty}^{\infty} f(x_0) K_a(x_0, x_a) dx_0 ,$$

where

$$K_a(x_0, x_a) = \begin{cases} A_a \exp \left[ i \pi \left( x_0^2 \cot \phi - 2 x_0 x_a \csc \phi + x_a^2 \cot \phi \right) \right] & \text{if } a \neq 2n \\ \delta(x_0 - x_a) & \text{if } a = 4n \\ \delta(x_0 + x_a) & \text{if } a = 4n \pm 2 \end{cases} ,$$

and

$$A_a = \left| \sin \frac{\phi}{2} \right|^{1/2} \exp \left[ -i \frac{\pi \text{sgn}(\phi)}{4} + i \frac{\phi}{2} \right] , \quad \phi = \frac{a \pi}{2} .$$

Our proposed encryption method can be illustrated by Fig. 1. Let $f(x_0)$ and $g(x_0)$ represent the two primary normalized amplitude images to be encrypted together; $J$ denotes the pixel scrambling operation [14], which interchanges the pixels according to some random permutation, and the image can be retrieved by repositioning the disturbed image according to the special order. For encryption, the pixel scrambling is applied to one of the primary images $g(x_0)$, and then, the scrambled result $J[g(x_0)]$ is encoded into a phase-only function [3, 6, 7], which can be mathematically expressed as $\exp[i \pi J[g(x_0)]]$, within the
range \([0, \pi]\) of the phase variation. The resulting function is multiplied by the other primary image \(f(x_0)\) to obtain the complex combination signal

\[
C(x_0) = f(x_0) \exp[i\pi J\left[g(x_0)\right]].
\]  

(4)

In the following steps, we employ the configuration of double random phase encoding in the fractional Fourier domain [4]. Let \(M_1(x_0) = \exp[i2\pi p(x_0)]\) and \(M_2(x_0) = \exp[i2\pi q(x_0)]\) present the two random phase masks, where \(p(x_0)\) and \(q(x_0)\) are statistically independent white sequences uniformly distributed in \([0, 1]\). As shown in Fig. 1, \(C(x_0)\) is first multiplied by the first random phase mask \(M_1(x_0)\), then transformed by FRFT with order \(a\), multiplied by the second random phase mask \(M_2(x_0)\), and fractional Fourier transformed with order \(b-a\). Thus, we obtain the final distribution of the output encrypted image \(\psi(x_0)\), which is given by

\[
\psi(x_0) = F_{b-a} \left\{ F_{a} \left[ C(x_0) M_1(x_0) \right] M_2(x_0) \right\}
\]

\[
= F_{b-a} \left\{ F_{a} \left[ f(x_0) \exp[i\pi J\left[g(x_0)\right]] M_1(x_0) \right] M_2(x_0) \right\}.
\]  

(5)

In the encryption process, it is clear that the complex combination signal \(C(x_0)\), which is the synthesis from the two primary real valued images, is double phase encoded in the fractional Fourier domain. Unnikrishnan and Singh [5] have demonstrated that the encrypted result of double random phase encoding is a stationary white noise. Accordingly, the output encrypted image \(\psi(x_0)\) of the proposed method has a stationary white distribution.
The Decryption shown in Fig. 2 is the reverse process of the encryption. For decryption, \( \psi(x_0) \) is first double phase decoded as follows: \( \psi(x_0) \) is transformed by the \((a-b)\) th FRFT and the resultant function is multiplied by the conjugate of the second random phase mask \( M_2(x_0) \) in the \( a \) th fractional domain, the FRFT of order \(-a\) is then applied, resulting in the following decrypted combination function \( C(x_0) \) after multiplying by the conjugate of the first random phase mask \( M_1(x_0) \)

\[
C(x_0) = F_{a} \left\{ F_{a-b} \left[ \psi(x_0) \right] M_2^*(x_0) \right\} M_1^*(x_0) = f(x_0) \exp \left\{ i \pi J \left[ g(x_0) \right] \right\}.
\]

(6)

The amplitude-based image \( f(x_0) \) can be retrieved from the intensity distribution of the decoded \( C(x_0) \), whereas the phase-based image \( g(x_0) \) requires extracting the phase of \( C(x_0) \), and dividing it by \( \pi \), then taking the inverse pixel scrambling transform denoted by \( J^{-1} \). The usage of \( J \) will be discussed in Section 4.

The proposed method can be carried out both optically and electronically. Since the encryption and decryption process described above employs the well-known double phase-coding scheme, a possible optoelectronic hybrid system adopted to implement the proposed method is shown in Fig. 3. Lohmann’s single-lens configuration is used to perform the FRFT [25]. The computer-controlled spatial light modulators (SLM) are used to display complex data. For encryption, the two original images are calculated to achieve the combination function \( C(x_0) = f(x_0) \exp \left\{ i \pi J \left[ g(x_0) \right] \right\} \), and then multiplied by the random phase mask \( M_1 \) in computer; the result \( C(x_0) M_1(x_0) \) is displayed on SLM1 which is located in the input plane. The pixel scrambling technique can also be implemented by an optical pixel scrambling device (OPSD) [14]. The SLM2 serves to display the random phase mask \( M_2 \). At the output plane, the resultant encrypted signal with complex value should be recorded by a holographic scheme, and then fed into the computer. Digital holographic recording methods used in optical security systems before [9, 17, 22] can be employed here.

![Fig. 3. Optical implementation of the encryption](image-url)

The decryption process can be implemented by a configuration which is almost similar to the schematic shown in Fig. 3. In this case, SLM1 displays the encrypted image, while SLM2 displays the conjugate of the random phase mask \( M_2^* \). Moreover, the corresponding fractional Fourier orders \( a \) and \((b-a)\) performed by Lens1 and Lens2 are substituted with \((a-b)\) and \(-a\) by adjusting the two stretches of free space separated by each Lens respectively [25]. \( C(x_0) M_1(x_0) \) is achieved at the output plane after passing the encrypted...
image from left to right. The amplitude-based image \( f(x_0) \), which is the intensity of \( C(x_0)M_1(x_0) \), can be recovered by an intensity detector (like a CCD camera) at the output plane. To obtain the other image \( g(x_0) \), a digital holographic scheme at the output plane is required again to record \( C(x_0)M_1(x_0) \), which is fed to the computer for post-processing.

The decrypted phase-based image is obtained by multiplying \( C(x_0)M_1(x_0) \) with the conjugate of the random phase mask \( M_1 \), followed by the extraction of the phase information of the result, and finally applying the inverse pixel scrambling. The proposed algorithm can also be adopted to perform digital image encryption in the computer by using fast computation of the FRFT.

Encrypting two images together by this novel approach only creates one encrypted image, whereas other single-image encryption methods create two encrypted images. In this sense, this method can raise the efficiency when encrypting, storing or transmitting.

### 3. Noise perturbation of the encrypted image

We further investigate the effect of noise on the two \( f(x_0) \) and \( g(x_0) \) decrypted images. In the presence of additive noise \( n(x_0) \) [3, 7], the distorted encrypted image can be represented as

\[
\psi'(x_0) = \psi(x_0) + n(x_0),
\]

where \( \psi(x_0) \) is the encrypted image defined by Eq. (5).

From Eq. (6), the decoded combination signal is given as follows

\[
C'(x_0) = f'(x_0) \exp[i\pi \tilde{g}(x_0)] = f(x_0) \exp[i\pi J[g(x_0)]] + n'(x_0),
\]

where

\[
n'(x_0) = F_{\alpha} \left[ F_{\beta-\alpha} \left[ n(x_0) \right] \right] M_2^*(x_0) M_1^*(x_0),
\]

is the perturbation influence on the decrypted combination signal \( C(x_0) \). We note that both the amplitude and phase of \( C(x_0) \) are disturbed since \( n'(x_0) \) is a zero-mean complex Gaussian noise [7]. Consequently, the two decrypted images denoted by \( f'(x_0) \) and \( g'(x_0) \), are disturbed too. \( \tilde{g}(x_0) \), the phase of \( C(x_0) \) in Eq. (8), represents the recovered \( g'(x_0) \) without inverse pixel scrambling.

As described in Section 2, the following decryption process is performed to Eq. (8) to retrieve the two images

\[
f'(x_0) = |C'(x_0)|, \quad g'(x_0) = J^{-1} \left[ \arg \left\{ C'(x_0) \right\} / \pi \right],
\]

where \( \arg(*) \) denotes the angle of complex quantity. \( f'(x_0) \) and \( g'(x_0) \) are the distorted decrypted version of the two primary images \( f(x_0) \) and \( g(x_0) \), respectively.

The square modulus of the decrypted image \( f'(x_0) \) recovered from the amplitude of Eq. (8) in the presence of additive noise is

\[
|f'(x_0)|^2 = |f(x_0) \exp[i\pi J[g(x_0)]] + n'(x_0)|^2
= |f(x_0)|^2 + |n'(x_0)|^2 + f(x_0) \exp\{-i\pi J[g(x_0)]\} n'(x_0) + f(x_0) \exp\{i\pi J[g(x_0)]\} n'(x_0).
\]
We note that the second term is a noise with Rayleigh distribution, and both the third and forth terms are Gaussian white noise. It is shown that the decrypted image \( f'(x_0) \) recovered from the amplitude of \( C'(x_0) \) is disturbed by these additive random noises.

For the case of retrieving the image \( g(x_0) \) from the phase of Eq. (8), we consider how to reduce the influence of perturbation. Since the primary \( g(x_0) \) and its pixel scrambled form are both normalized amplitude images which range from 0 to 1, the phase of Eq. (8) ranges between 0 and \( \pi \) if there is no noise perturbation in the encrypted image. But the noise component \( n'(x_0) \) causes the phase to range between \( \pi \) and \(-\pi\). Javidi, et al, [3, 26] discussed a thresholding method to reduce the distortions caused by noise. They considered the phase value to be \( \pi \) if the noisy phase is in the third quadrant, and zero if the noisy phase is in the fourth quadrant. In this paper, we suggest in supplement to the thresholding method that, on condition that \( g(x_0) \) is a binary image, the phase value of Eq. (7) could be considered as \( \pi \) if the noisy phase is in the second or third quadrant, and zero if the noisy phase is in the first or fourth quadrant.

To be specific, our motivation of applying the pixel scrambling operation to the phase-based image \( g(x_0) \) before encryption is mainly to diffuse the influence of noise perturbation to the whole recovered image \( g'(x_0) \) while decrypting. This will be verified in the following section.

4. Numerical simulation results and discussion

Computer simulations are performed to verify the proposed encryption technique for double images. Two types of amplitude image, grayscale image of Lena [Fig. 4(a)] and binary text [Fig. 4(b)], are serving as the two primary images to be encrypted together. Each of them has a size of \( 256 \times 256 \) pixels. We use Lena as the amplitude-based image \( f(x_0) \), and the binary text as the phase-based image \( g(x_0) \). The two random phase masks are generated from a random number generator in MATLAB. The orders of the first 2D-FRFT is (0.82, 0.82), and of the second 2D-FRFT is (0.45, 0.45). Figure 4(c) shows the amplitude of the complex-valued encrypted image.

![Fig. 4. (a). Primary grayscale image of Lena; (b) Primary binary text; (c) The encrypted result.](image)

To retrieve the grayscale image which is the amplitude of the combined complex signal, the keys of decryption process consist of the orders of the two 2D-FRFTs and the random phase mask \( M_2 \). Whereas, to retrieve the phase-based binary image, not only the knowledge of the above parameters but also the random phase mask \( M_1 \) and the pixel scrambling operator \( J \) are required. In the following simulations, different keys are investigated with respect to blind decryption. Figure 5 and Fig. 6 show the decrypted results obtained with incorrect random phase mask \( M_1 \) and \( M_2 \), respectively. The two decrypted images without
cross-talk obtained when the correct keys are used are shown in Fig. 7. We note that the phase-based image could be exactly retrieved if no error occurs on the two phase masks. Figure 8 shows the recovered phase-based image with wrong inverse pixel scrambling operator while other keys are correctly applied. It is very difficult for an unauthorized user to access the right decrypted phase-based images without the correct pixel scrambling operator. It can also be noted that, the key space of the phase-based image is larger than that of the amplitude-based image. This would lead to the provision of some security hierarchy in applications. The image with the higher requirement of security can be converted into pure phase function in the proposed encryption process. Otherwise, the key space can be further enlarged by using the extended FRFT [27] instead of the FRFT, which can provide more parameters in the encryption systems [8, 17, 28].

![Fig. 5. When decrypting with wrong mask $M_1$: (a) The recovered amplitude-based image; (b) The recovered phase-based image.](image1)

![Fig. 6. When decrypting with wrong mask $M_2$: (a) The recovered amplitude-based image; (b) The recovered phase-based image.](image2)

![Fig. 7. When decrypting with correct keys: (a) The recovered amplitude-based image; (b) The recovered phase-based image.](image3)
In addition, we study the sensitivities of the fractional orders which are parts of the decryption keys. The mean square error (MSE) is employed here to measure the robustness against the blind decryption with respect to the fractional orders. Mathematically, if \( I(i,j) \) and \( H(i,j) \) denote the values of the original and the decrypted image of the pixel \((i,j)\), respectively, then the total MSE can be defined as follows:

\[
MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (I(i,j) - H(i,j))^2,
\]

where \( N \) and \( M \) are the sizes of the images. In the following simulation as depicted in Fig. 9, different errors are introduced to the orders of the two inverse 2D-FRFTs, i.e., we use the FRFT orders \((-0.45+\Delta, -0.45+\Delta)\) and \((-0.82+\Delta, -0.82+\Delta)\) instead of the correct orders \((-0.45, -0.45)\) and \((-0.82, -0.82)\) in the decryption process, where \( \Delta \) denotes the deviation from correct order, and varies from -0.5 to 0.5. We calculate the MSE between the two original images and their corresponding decrypted images, respectively, and plot their curves as a function of the order deviation \( \Delta \) in each 2D-FRFT in Fig. 9. Other keys used for encryption and decryption are the correct ones in this simulation. When decoding with \((-0.45+\Delta, -0.45+\Delta)\) and \((-0.82, -0.82)\), \(\bullet\) stands for the MSE between the original and the decrypted phase-based image, while \(\rightarrow\) for the case of the amplitude-based image; and when decoding with \((-0.45, -0.45)\) and \((-0.82+\Delta, -0.82+\Delta)\), \(\downarrow\) stands for the MSE between the original and the decrypted phase-based image, while \(\leftarrow\) for the case of the amplitude-based image.
Deviation from correct fractional orders

Mean Square Error

The decrypted amplitude-based Image with orders (-0.45 + Δ, -0.45 + Δ) and (-0.82, -0.82)

The decrypted phase-based Image with orders (-0.45, -0.45) and (-0.82 + Δ, -0.82 + Δ)

The decrypted phase-based Image with orders (-0.45 + Δ, -0.45 + Δ) and (-0.82, -0.82)

The decrypted amplitude-based Image with orders (-0.45, -0.45) and (-0.82 + Δ, -0.82 + Δ)

Fig. 9. MSE between the original image and the decrypted image when errors are introduced in fractional order parameters

It is noted from Fig. 9 that an error of 0.02 or more in any of the two 2D-FRFTs will result in sufficiently high MSE between the original image and the decrypted image; so the orders can be used as keys to protect the two images due to the sensitivity. When decryption procedure undergoes the same deviation from correct orders, the retrieved phase-based image gets higher MSE than the amplitude-based image. From Fig. 9 we also realize that the fractional orders should be matched more precisely when recovering the correct phase-based image, which is consequently more sensitive to the variations of fractional orders when decrypting. For unauthorized user, blind decryption is considerably difficult to perform. The security of the proposed method can be further enhanced by using iterative FRFT with a random phase mask at each stage [9].

In the following simulation, we check the tolerance against the loss of encrypted data. We occlude 25% and 50% of the encrypted image pixels. Figure 10 and Fig. 11 show the occluded encrypted images of Fig. 4(c) and the corresponding recovered images with correct keys. We calculate the MSE between the original and decrypted two images. In the case of 25% pixels of the encrypted image occluded, the MSE values are 1517.4 and 4220.0 for the amplitude-based image and phase-based image, respectively. In the case of 50% pixels of the encrypted image occluded, the MSE values are 3094.2 and 7723.0 for the amplitude-based image and phase-based image, respectively.

We perform another experiment to test the decryption effect when only the phase information of the encrypted image is used to recover the two images. Figure 12 shows the results, and the MSE values between original and decrypted images are 1420.0 and 3865.6 in the case of the amplitude-based image and phase-based image, respectively. As we can see, the recovered images are recognizable in despite of some noise degradation.
Simulations have also been performed to test the robustness against additive noise, which has a white Gaussian distribution with a zero mean in the simulation. Figure 13 gives the curves of the MSE between the original and decrypted images versus the noise standard deviation. The red line stands for the case of amplitude-based image, while the blue line stands for the phase-based one. We find that the noise perturbation has more influence on the phase-based image. According to the previous simulation results, we take cognizance of the sensitivity (to the keys and noise) of the phase-based image. Therefore, an image with higher security requirement is suggested to act as the phase-based image when using the proposed encryption method due to these properties.
In this paragraph, we demonstrate the usage of the initial pixel scrambling applied to the primary phase-based image. A white Gaussian noise with a zero mean and standard deviation of 0.02 is added to the encrypted image of Fig. 4(c). Without the use of the forward and inverse pixel scrambling, the two recovered images are as shown in Fig. 14, whereas our novel approach which makes use of the pixel scrambling produces Fig. 15. The calculated MSE values between the original and decrypted images are 319.2 and 1288.7 in the case of the amplitude-based image and phase-based image respectively in Fig. 14, while in Fig. 15 they are 318.5 and 1241.7. It is evident that the pixel scrambling process improves the quality of the decrypted phase-based image when the encrypted image undergoes noise perturbation. The influence of the cross-talk disturbance in Fig. 14 is scattered to the whole spatial distribution of the phase-based image by the inverse pixel scrambling operation in decryption. This result can also be obtained when the encrypted image undergoes loss of encrypted data. In addition, by introducing the pixel scrambling technique, the security can also be enhanced greatly as mentioned previously in this paper. Therefore, the pixel scrambling operation applied to the phase-based image plays a critical role in the novel approach.
Fig. 15. The recovered two images obtained from the noisy encrypted image when the forward and inverse pixel scrambling is applied. (a) The recovered amplitude-based image; (b) The recovered phase-based image

5. Conclusion

In this paper, a novel method is proposed to encrypt two images into stationary white noise. The synthesis of the combination complex signal from the two primary real valued images involves the fully phase encoding and pixel scrambling techniques. The combination complex signal is double phase encoded and afterwards decoded in the fractional Fourier domain. To retrieve the two images accurately, the knowledge of the two 2D-FRFTs orders, the two random phase masks and the pixel scrambling operator are necessary. The amplitude-based image can be retrieved from the intensity of the decoded combination signal, whereas the phase-based image requires further phase extraction and inverse pixel scrambling. A possible optical implementation of the proposed method is suggested. The effects of noise perturbations on the decrypted data are studied theoretically. The performance is analyzed with numerical simulations. It is shown that the proposed method is robust against the loss of data, and is sensitive to the variations of fractional orders during decryption. The phase-based image is more sensitive to the keys and noise disturbances than the amplitude-based image. The pixel scrambling technique employed in the novel approach can not only improve the quality of the decrypted phase-based image when noise perturbation occurs, but also enlarge the key space.

Acknowledgment

This work was supported by the National Science Foundation of China for Distinguished Young Scholars under Grant (No. 60625104), the Doctorship Foundation of China Educational Department (No. 1010036620602), and the National Defense Project of China for Fundamental Research (No. C1120060497).