Image Authentication Using Only Partial Phase Information from a Double-Random-Phase-Encrypted Image in the Fresnel Domain

Jiecai Zheng* and Xueqing Li

*Department of Computer Science and Technology, Shandong University,
No.1500, Shunhua Road, Gaoxin District, Jinan, Shandong 250101, China*

(Received March 5, 2015 : revised April 20, 2015 : accepted May 4, 2015)

The double-random phase encryption (DRPE) algorithm is a robust technique for image encryption, due to its high speed and encoding a primary image to stationary white noise. Recently it was reported that DRPE in the Fresnel domain can achieve a better avalanche effect than that in Fourier domain, which means DRPE in the Fresnel domain is much safer, to some extent. Consequently, a method based on DRPE in the Fresnel domain would be a good choice. In this paper we present an image-authentication method which uses only partial phase information from a double-random-phase-encrypted image in the Fresnel domain. In this method, only part of the phase information of an image encrypted with DRPE in the Fresnel domain needs to be kept, while other information like amplitude values can be eliminated. Then, with the correct phase keys (we do not consider wavelength and distance as keys here) and a nonlinear correlation algorithm, the encrypted image can be authenticated. Experimental results demonstrate that the encrypted images can be successfully authenticated with this partial phase plus nonlinear correlation technique.

Keywords : Double-random phase encryption, Three-dimensional image processing, Image authentication, Nonlinear correlation

OCIS codes : (100.6890) Three-dimensional image processing; (070.4340) Nonlinear optical signal processing; (200.4740) Optical processing; (110.2960) Image analysis; (110.3000) Image quality assessment

I. INTRODUCTION

Since the double-random phase encryption (DRPE) algorithm was proposed by Refregier and Javidi in 1995 [1], it has been widely used in the fields of image authentication, hiding, encryption, and watermarking [2-17]. This algorithm can be implemented quickly due to its parallel property. Also, the encrypted image from DRPE is stationary white noise, which cannot be predicted by using part of its information. At first the DRPE scheme was only implemented in the Fourier domain, but later algorithms based on DRPE with a Fresnel transform and a fractional Fourier transform were also presented [18-19].

Even though the DRPE technique has achieved good performance in the field of image security, it was also reported that DRPE is not completely robust to chosen-cipher text attacks [20, 21]. To make up for the deficiency of DRPE in the

Fourier domain, many new methods were proposed [12-14, 22-26]. In [26], W. Chen and X. Chen used only phase information of an encrypted image resulting from DRPE in the Fourier domain to enhance the security of DRPE. It was also demonstrated that this algorithm is beneficial to data transmission, and can thwart several attack algorithms. In [12, 13], Pérez-Cabré *et al.* combined the DRPE scheme with a photon-counting imaging algorithm to improve the performance of the conventional DRPE technique, since this method can yield an image unrecognizable to the naked eye. On the other hand, the encrypted image can be recognized with a nonlinear correlation algorithm. However, the photon-counting strategy used in [12, 13] is much more complicated in practice, while the phase-preservation scheme in [26] is much easier to implement.

In [27], I. Moon *et al.* have shown that DRPE in the Fresnel domain can achieve a better avalanche effect than

*Corresponding author: zhengjiecai@sdu.edu.cn

Color versions of one or more of the figures in this paper are available online.

that in Fourier domain in bit units. It can be concluded to some extent that DRPE in the Fresnel domain makes a security system much safer. Consequently, new methods based on DRPE in the Fresnel domain would definitely enhance the security of a designed system. In this paper, an image-authentication approach using partial phase information from a double-random-phase-encrypted image in the Fresnel domain is proposed. In this proposed method, only part of the phase information of the encrypted image is preserved, while all of the amplitude information is removed. In this case the decrypted image is not visually recognizable and can improve the security of an encryption system. On the other hand, the decrypted image can be verified with a nonlinear correlation algorithm that can achieve image authentication [28, 29]. Experimental results illustrate that this method is feasible. Also, we show that an image can be successfully authenticated even if only a small part of the phase information of the encrypted image is preserved.

This paper is organized as follows: In Section II we describe double-random phase encryption in the Fresnel domain. In Section III we give the procedures for our proposed algorithm, in Section IV we present simulation results based on our method, and we conclude the paper in Section V.

II. DOUBLE-RANDOM PHASE ENCRYPTION

The DRPE encryption technique has been widely used in image security, hiding, and watermarking since it was proposed by Refregier and Javidi [1] in 1995. For DRPE in the Fourier domain [1], the primary image is encoded into a stationary-white-noise image using two random phase masks. All of the points in the stationary-white-noise image are statistically independent and thus cannot be predicted using information from any part of the image. In [18] Situ and Zhang proposed the DRPE method in the Fresnel domain and demonstrated that much higher security is achieved for DRPE in the Fresnel domain than that in the Fourier domain. In [27], I. Moon *et al.* also showed that DRPE in the Fresnel domain can result in a better avalanche effect in bit units than that in the Fourier domain. Thus it can be expected that methods based on DRPE in the Fresnel domain are promising. The schematic diagram of the DRPE system in the Fresnel domain is given in Fig. 1.

For a DRPE system in the Fresnel domain, the input image $f(x,y)$ is first modulated with a random phase mask of the same size as the input image. Then the modulated image is Fresnel-propagated for a distance of D_1 under a plane wave of wavelength λ . After Fresnel propagation to D_1 , a second random phase mask is used to modulate the Fresnel-propagated image. Finally, the doubly modulated image is Fresnel-propagated for a distance D_2 to yield an encrypted image $g(x,y)$. During this process the two random phase masks are distributed randomly on the interval $[0, 2\pi]$ and can be represented as $\exp(j2\pi n(x,y))$ and $\exp(j2\pi n(\mu, \nu))$ where $n(x,y)$ and $n(\mu, \nu)$ are uniformly located on the

FIG. 1. Schematic diagram of a DRPE system in the Fresnel domain.

interval $[0, 1]$. As a result, DRPE in the Fresnel domain can be expressed by following equation [18, 27].

$$g(x,y) = FrT_{\lambda} \left\{ FrT_{\lambda} \left\{ f(x,y) \exp(j2\pi n(x,y)); D_1 \right\} \exp(j2\pi n(\mu, \nu)); D_2 \right\} \quad (1)$$

where FrT_{λ} denotes Fresnel propagation with respect to wavelength λ . In Eq. (1) the wavelength λ and two distances D_1 and D_2 , but not solely the two random phase masks, can be considered as encryption keys. In the decryption process for DRPE in the Fresnel domain, the same optical setup of Fig. 1 can be employed in the reverse direction by using the complex conjugate of the encrypted image $g(x,y)$ [18].

III. PROCEDURES OF THE PROPOSED AUTHENTICATION METHOD

In our proposed method, the input image is first encrypted with a double-random-phase-encryption technique in the Fresnel domain. Usually the entire encrypted image resulting from DRPE is kept for decryption, the decrypted image being used for further processes such as image authentication and display. However, the encrypted data burden transmission, because all of the encrypted images from DRPE are complex data consisting of amplitude and phase information. Here we discard all of the amplitude data in the encrypted image and keep only the phase information of the encrypted image. To improve the security of the system, only part of the phase information, not all of it, is used. By using partial phase information, the decrypted image is not visually recognizable, which can enhance security [12, 13]. Even though an image decrypted from partial phase information cannot be authenticated visually by comparison to a reference, it is indeed recognized with a nonlinear cross-correlation algorithm. This nonlinear cross correlation is described by the following equation [27, 28].

$$C(x,y) = IFT \left\{ \left[FT[D(x,y)] FT[R(x,y)]^* \right] \times \exp \left[i \left(\phi(FT[D(x,y)]) - \phi(FT[R(x,y)]) \right) \right] \right\} \quad (2)$$

where $D(x, y)$ is the decrypted image decoded using partial phase information of an encrypted image from the DRPE algorithm in the Fresnel domain [see Fig. 2]), $R(x, y)$ is the reference image, FT indicates Fourier transform and IFT inverse Fourier transform, $\phi(FT(D(x, y)))$ denotes the phase information of $FT(D(x, y))$, and the parameter k defines the strength of the applied nonlinearity. That is, the parameter k will affect the cross-correlation result that relates to the final image-authentication performance [12, 13, 27, 28]. Eq. (2) tends to be a phase extractor when $k=0$, and it becomes a linear correlation method when $k=1$. Since different values of k yield different cross-correlation results, it is necessary to find a value for k that achieves better verification in an application [12, 13]. Usually the appropriate value of k is found using peak-to-correlation energy (PCE) or discrimination-ratio metrics. The PCE, which is defined as the ratio of the maximum intensity-peak value to the total energy of the output plane ($C(x, y)$ in Eq. (2)), indicates the sharpness and height of the output correlation peak. The formula for PCE is given as follows [12, 13, 27]:

$$PCE = \frac{\max \left[|C(x, y)|^2 \right]}{\sum_{i=1}^M \sum_{j=1}^N |C(x_i, y_j)|^2} \quad (3)$$

where M and N are the numbers of rows and columns of the image, and $C(x, y)$ is the nonlinear cross correlation between decrypted and reference image as defined in Eq. (2). A given value of the parameter k is “good” if it yields a high PCE value per Eq. (3). From the literature in [27, 30, 31], $k=0.3$ is an appropriate value for nonlinear cross-correlation authentication. Consequently, the flow chart for our proposed image-authentication algorithm can be described as in Fig. 2. In brief, an image is first encrypted with a DRPE algorithm in the Fresnel domain. Then the amplitude information is discarded, while partial phase information from the encrypted image is preserved, which is beneficial to data

transmission. Finally, the partial-phase image is decrypted with the correct keys and authenticated with the nonlinear cross-correlation method.

IV. SIMULATION RESULTS

One “true class” image and one “false class” image, shown in Fig. 3, are used to illustrate our proposed authentication method. Both are grayscale images of size 250×250 pixels.

Before conducting image authentication with this proposed algorithm, the parameter k in Eq. (1) is selected by measuring the PCE (see Eq. (2)) values for the true class image. The PCE curve for varying k is given in Fig. 4. It is noted that the best PCE value is achieved when $k \approx 0.3$, consistent with the results reported in [27].

Next the encrypted true class image following DRPE in the Fresnel domain is given in Fig. 5, in which both amplitude and phase information are shown. However, for the image authentication in our proposed algorithm, only part of the phase information is preserved. In this study we randomly choose the phase information that should be kept from the

FIG. 3. Grayscale test images. (a) true class image, (b) false class image.

FIG. 2. Flow chart for image authentication with partial phase information.

FIG. 4. PCE results for varying parameter k with true class test image.

double-random-phase-encrypted image, and a percentage is used to describe the amount of preserved phase information in the encrypted image. A pixel's grayscale value is set to zero for any location with discarded phase information. In Fig. 6 two encrypted images with respectively 20% and 50% phase information preserved are presented.

There is no doubt that the nonlinear cross-correlation values would be different for different preservation fractions of phase information in the original encrypted image. It is necessary to check the minimum percentage of phase information that may be kept while still achieving successful image authentication. Consequently, we varied the percentage of

retained phase information in the encrypted image from 9% to 100%, with an interval of 10% (after the value of 10%). In Fig. 7 some of the images decrypted with correct keys in the Fresnel domain are illustrated. Figs. 7(a), (c), (e), and (g) show the true class images decrypted from encrypted

FIG. 5. Encrypted images. (a) amplitude image, (b) phase image.

FIG. 6. Partial phase images. (a) 20% phase information, (b) 50% phase information.

FIG. 7. Decrypted true class images. (a), (c), (e), and (g) are decrypted images resulting respectively from encrypted images with 20%, 50%, 70%, and 100% of phase information preserved. (b), (d), (f), and (h) are decrypted images resulting respectively from encrypted images with 20%, 50%, 70%, and 100% of both phase and amplitude information preserved.

images with respectively 20%, 50%, 70%, and 100% preserved phase information. It is noted from these four figures that the silhouette of the decrypted true class images cannot be recognized visually, even when the complete phase information from the encrypted image (see Fig. 7(e)) is preserved, without *a priori* knowledge of the image. On the contrary, decrypted true class images from encrypted images with both partial amplitude and phase information preserved can be recognized with the naked eye even if only 20% of phase and amplitude information is preserved. Figs. 7(b), (d), (f), and (h) are the decrypted true class images decoded from encrypted images with respectively 20%, 50%, 70%, and 100% phase and amplitude information preserved. The comparisons also show that our proposed image authentication method with only partial phase information preserved in the encrypted image can enhance the security of system, because the decrypted image cannot be easily recognized with the naked eye. Moreover, the encrypted image with partial phase

information is beneficial to data transmission, because it requires less bandwidth.

On the other hand, the maximum nonlinear cross-correlation values for true class images are given in Fig. 8. It is noted that the maximum nonlinear cross-correlation values decrease as phase information preserved in the encrypted image decreases. From Fig. 8, it is not easy to visually determine the threshold in terms of percentage that should be preserved from the encrypted image for successful image authentication. Thus it is better to show the maximum nonlinear cross-correlation values using false class images.

In Fig. 9 the maximum nonlinear cross-correlation values obtained using the same method with a false class image are illustrated. Comparing the results shown in Figs. 8 and Fig. 9, it is found that images can be authenticated when the percentage of preserved phase information is greater than 10%, since the maximum nonlinear cross-correlation values below 10% on the x axis in Fig. 8 are much bigger than the corresponding values in Fig. 9, which means that the true and false class images can be distinguished. However, the true and false class images cannot be distinguished when the preserved phase information in the encrypted image is

FIG. 8. Maximum nonlinear cross-correlation values for varying percentage of preserved phase information in encrypted true class images.

FIG. 9. Maximum nonlinear cross-correlation values for varying percentage of preserved phase information in encrypted false class images.

FIG. 10. Nonlinear cross-correlation planes with 9%, 10%, and 20% preserved phase information, for both true and false class image authentication. (a), (c), and (e) are nonlinear cross-correlation planes for true class images with 9%, 10%, and 20% preserved phase information respectively. (b), (d), and (f) are nonlinear cross-correlation planes for false class image with 9%, 10%, and 20% preserved phase information respectively.

FIG. 11. Maximum nonlinear cross-correlation values for varying percentage of preserved phase information for a true class image, using correct ($\square$) and incorrect ($\circ$) keys.

less than 10%, as the corresponding maximum nonlinear cross-correlation values are very similar. For our system 10% phase information may be the threshold for successful image authentication. In other words, at least 10% of the phase information should be retained in the encrypted image to tell the difference between true and false class images. For a clear illustration concerning the percentage of preserved phase information in an encrypted image, the nonlinear cross-correlation planes are given in Fig. 10 for 9%, 10%, and 20% phase preservation, respectively.

Figure 10 demonstrates that the proposed authentication method can be used to tell true class images from false ones when the percentage of preserved phase information in encrypted images is greater than or equal to 10%. However, an authentication algorithm should satisfy the condition that an image cannot be recognized as true class when an incorrect key is given. In Fig. 11 the maximum nonlinear cross-correlation values between correct and incorrect keys (phase keys) are given for a true class image. It is noted from Fig. 11 that the images cannot be authenticated when the key is wrong, as all of the resulting maximum nonlinear cross-correlation values are very small and similar to those for a false image (see Fig. 9).

In addition, in Fig. 12 the nonlinear cross-correlation planes are given for 9%, 10%, and 20% preserved phases using a true class image, after right and wrong keys have been applied. These results also show that the images cannot be authenticated when the wrong keys for DRPE are used. Moreover, it is seen in Fig. 12 that the percentage of preserved phase information should be at least 10% for successful image authentication.

V. CONCLUSION

In this paper we have proposed an image-authentication

FIG. 12. Nonlinear cross-correlation planes for 9%, 10%, and 20% preserved phase information for a true class image, with correct and incorrect phase keys. (a), (c), and (e) are for 9%, 10%, and 20% preserved phase information respectively, with correct keys. (b), (d), and (f) are for 9%, 10%, and 20% preserved phase information respectively, with incorrect keys.

method based on a double-random-phase-encryption technique in the Fresnel domain. Numerical simulations showed that the decrypted image based on partial phase information in the encrypted image cannot be visually recognized, which can enhance the security of the system. On the other hand, the unrecognizable decrypted image can be authenticated with a nonlinear cross-correlation technique. We have demonstrated the feasibility of this proposed authentication system using both true and false class images. In addition, the image cannot be authenticated if an incorrect key is given. This image-authentication system can achieve superior bandwidth reduction, since only partial phase information from an encrypted image is preserved. Moreover, it is shown that a true class image can be successfully authenticated even when only a small percentage of phase information from the encrypted image is preserved.

REFERENCES

1. P. Refregier and B. Javidi, "Optical image encryption using input plane and Fourier plane random encoding," *Proc. SPIE* **2565**, 62-68 (1995).
2. B. Wang, C. C. Sun, W. C. Su, and A. E. Chiou, "Shift-

- tolerance property of an optical double-random phase-encoding encryption system," *Appl. Opt.* **39**, 4788-4793 (2000).
3. X. C. Cheng, L. Z. Cai, Y. R. Wang, X. F. Meng, H. Zhang, X. F. Xu, and G. Y. Dong, "Security enhancement of double-random phase encryption by amplitude modulation," *Opt. Lett.* **33**, 1575-1577 (2008).
 4. I. H. Lee and M. Cho, "Double random phase encryption based orthogonal encoding technique for color images," *J. Opt. Soc. Korea* **18**, 129-133 (2014).
 5. I. H. Lee, "Accumulation encoding technique based on double random phase encryption for transmission of multiple images," *J. Opt. Soc. Korea* **18**, 401-405 (2014).
 6. I. H. Lee and M. Cho, "Double random phase encryption using orthogonal encoding for multiple-image transmission," *J. Opt. Soc. Korea* **18**, 201-206 (2014).
 7. I. H. Lee and M. Cho, "Optical encryption and information authentication of 3D objects considering wireless channel characteristics," *J. Opt. Soc. Korea* **17**, 494-499 (2013).
 8. A. Alfalou and A. Mansour, "Double random phase encryption scheme to multiplex and simultaneous encode multiple images," *Appl. Opt.* **48**, 5933-5947 (2009).
 9. Z. Xin, L. Dong, Y. Sheng, L. Da-hai, and H. Jian-Ping, "A method for hiding information utilizing double-random phase-encoding technique," *Opt. Laser Technol.* **39**, 1360-1363 (2007).
 10. Y. Sheng, Z. Xin, M. S. Alam, L. Xi, and L. Xiao-Feng, "Information hiding based on double random-phase encoding and public-key cryptography," *Opt. Express* **17**, 3270-3284 (2009).
 11. S. Kishk and B. Javidi, "Information hiding technique with double phase encoding," *Appl. Opt.* **41**, 5462-5470 (2002).
 12. E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," *Opt. Lett.* **36**, 22-24 (2009).
 13. E. Pérez-Cabré, H. C. Abril, M. S. Millán, and B. Javidi, "Photon-counting double-random-phase encoding for secure image verification and retrieval," *J. Opt.* **14**, 094001 (2012).
 14. M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," *Opt. Lett.* **38**, 3198-3201 (2013).
 15. M. Z. He, L. Z. Cai, Q. X. Liu, X. C. Wang, and X. F. Meng, "Multiple image encryptions and watermarking by random phase matching," *Opt. Commun.* **247**, 29-37 (2005).
 16. C. Yao-yao, Z. Xin, X. Yong-liang, Y. Sheng, and W. Xiu-ling, "An improved watermarking method based on double random phase encoding technique," *Opt. Laser Technol.* **42**, 617-623 (2010).
 17. F. Yi, I. Moon, and Y. H. Lee, "A Multispectral photon-counting double random phase encoding scheme for image authentication," *Sensors* **14**, 8877-8894 (2014).
 18. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Opt. Lett.* **29**, 1584-1586 (2004).
 19. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Opt. Lett.* **25**, 887-889 (2000).
 20. X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Opt. Lett.* **31**, 1044-1046 (2006).
 21. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys," *Opt. Lett.* **30**, 1644-1646 (2005).
 22. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," *Opt. Express* **15**, 10253-10265 (2007).
 23. X. C. Cheng, L. Z. Cai, Y. R. Wang, X. F. Meng, H. Zhang, X. F. Xu, and G. Y. Dong, "Security enhancement of double-random phase encryption by amplitude modulation," *Opt. Lett.* **33**, 1575-1577 (2008).
 24. B. Wang, C. C. Sun, W. C. Su, and A. E. Chiou, "Shift-tolerance property of an optical double-random phase-encoding encryption system," *Appl. Opt.* **39**, 4788-4793 (2000).
 25. P. Kumar, A. Kumar, J. Joseph, and K. Singh, "Impulse attack free double-random-phase encryption scheme with randomized lens-phase functions," *Opt. Lett.* **34**, 331-333 (2009).
 26. W. Chen and X. Chen, "Double random phase encoding using phase reservation and compression," *J. Opt.* **16**, 025402 (2014).
 27. I. Moon, F. Yi, Y. H. Lee, and B. Javidi, "Avalanche and bit independence characteristics of double random phase encoding in the Fourier and Fresnel domains," *J. Opt. Soc. Am. A* **31**, 1104-1111 (2014).
 28. B. Javidi, "Nonlinear joint power spectrum based optical correlation," *Appl. Opt.* **28**, 2358-2367 (1989).
 29. B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.* **33**, 1752-1756 (1994).
 30. E. Perez-Cabre and B. Javidi, "Scale and rotation invariant optical ID tags for automatic vehicle identification and authentication," *IEEE T. Veh. Technol.* **54**, 1295-1303 (2005).
 31. E. Perez-Cabre and B. Javidi, "Distortion-invariant ID tags for object identification," in *Proc. European Symposium on Optics and Photonics for Defence and Security, International Society for Optics and Photonics* (2004, November), pp. 33-41.