Optics & Laser Technology 88 (2017) 111–120

Contents lists available at ScienceDirect

Optics & Laser Technology

journal homepage: www.elsevier.com/locate/optlastec

Full length article

Image authentication based on double-image encryption and partial phase decryption in nonseparable fractional Fourier domain

Lin Yuan[a,b,*], Qiwen Ran[a,c], Tieyu Zhao[a]

[a] State Key Laboratory of Tunable Laser Technology Research, Institute of Optic-Electronics, Harbin Institute of Technology, Harbin, 150001 China
[b] College of Mathematics, Physics and Information Engineering, Zhejiang Normal University, Jinhua, 321004 China
[c] Nature Science Research Center of Science and Technology, Harbin Institute of Technology, Harbin, 150001 China

ARTICLE INFO

Keywords:
Double-image encryption
Nonseparable fractional Fourier transform
Image authentication
Nonlinear correlation algorithm

ABSTRACT

In this paper an image authentication scheme is proposed based on double-image encryption and partial phase decryption in nonseparable Fractional Fourier transform domain. Two original images are combined and transformed into the nonseparable fractional Fourier domain. Only part of the phase information of the encrypted result is kept for decryption while the rest part of phase and all the amplitude information are discarded. The two recovered images are hardly recognized by visual inspection but can be authenticated by the nonlinear correlation algorithm. The numerical simulations demonstrate the viability and validity of the proposed image authentication scheme.

1. Introduction

In past decades, the optical image encryption techniques have been widely studied due to its advantage of potential fast computational processing and the parallelism achievable. The double random phase encoding (DRPE) [1–4] is a classical method among various optical encryption techniques. However, it has been testified that under certain conditions DRPE is vulnerable to some kinds of attacks [5–10]. Although the probability of being broken decreases by using iterative random phase encoding, the computation and storage costs increase simultaneously. Other than DRPE, multiple-image encryption has been proposed later and developed considerably for its convenience of encrypting multiple images at the same time and its applicability to color images [11–15]. In recent years, many different optical transforms have been employed in image encryption schemes, such as gyrator transform (GT) [16–19], fractional Fourier transform (FRFT) [20–23], nonseparable fractional Fourier transform (NFRFT) [24,25]. One of advantages of NFRFT is that it cannot be expressed as a tensor product of two one-dimensional transforms neither in the space domain nor in the Wigner space-frequency domain. Therefore, it adequately mixes the information of the signal not only inside each dimension but also between two dimensions [24]. When used in encryption, it enhances the security level of the cryptosystem. In this paper, an image authentication scheme is proposed based on double-image encryption and partial phase decryption in NFRFT domain. Two original images are respectively taken as the real and imaginary part of the input signal. Perform NFRFT on the input signal with the transform order and the coefficient parameters as encryption keys. Not all the encrypted data are kept for decryption but merely partial phase information. The rest phase information and the whole amplitude information of the encrypted result are discarded so as to reduce the costs of transmission and storage. Due to being decrypted from only partial phase information, the two recovered images cannot be identified by naked eyes but can be verified by means of correlation algorithms [26–31] among which we chose the nonlinear correlation algorithm as our tool. One of the advantages of the proposed double-image authentication scheme is that it is capable of authenticating two images using only one encryption-decryption process. To our knowledge, the authentication technique is proposed for the first time that can achieve two respective images authentications only by a single encryption-decryption operation.

The rest of the paper is organized as follows. Section 2 presents the details of the proposed image authentication scheme. Section 3 gives the numerical simulations and results to demonstrate the performance and verify the validity of the proposed scheme. The conclusion is drawn and stated in the final section.

2. Image authentication based on double-image encryption and partial phase decryption in NFRFT domain

2.1. Double-image encryption in NFRFT domain

We first recall the knowledge of NFRFT. NFRFT with transform order α is mathematically defined as [24].

* Corresponding author at: College of Mathematics, Physics and Information Engineering, Zhejiang Normal University, Jinhua 321004, China.
E-mail address: ylin2002@126.com (L. Yuan).

http://dx.doi.org/10.1016/j.optlastec.2016.09.004
Received 22 June 2016; Received in revised form 31 July 2016; Accepted 8 September 2016

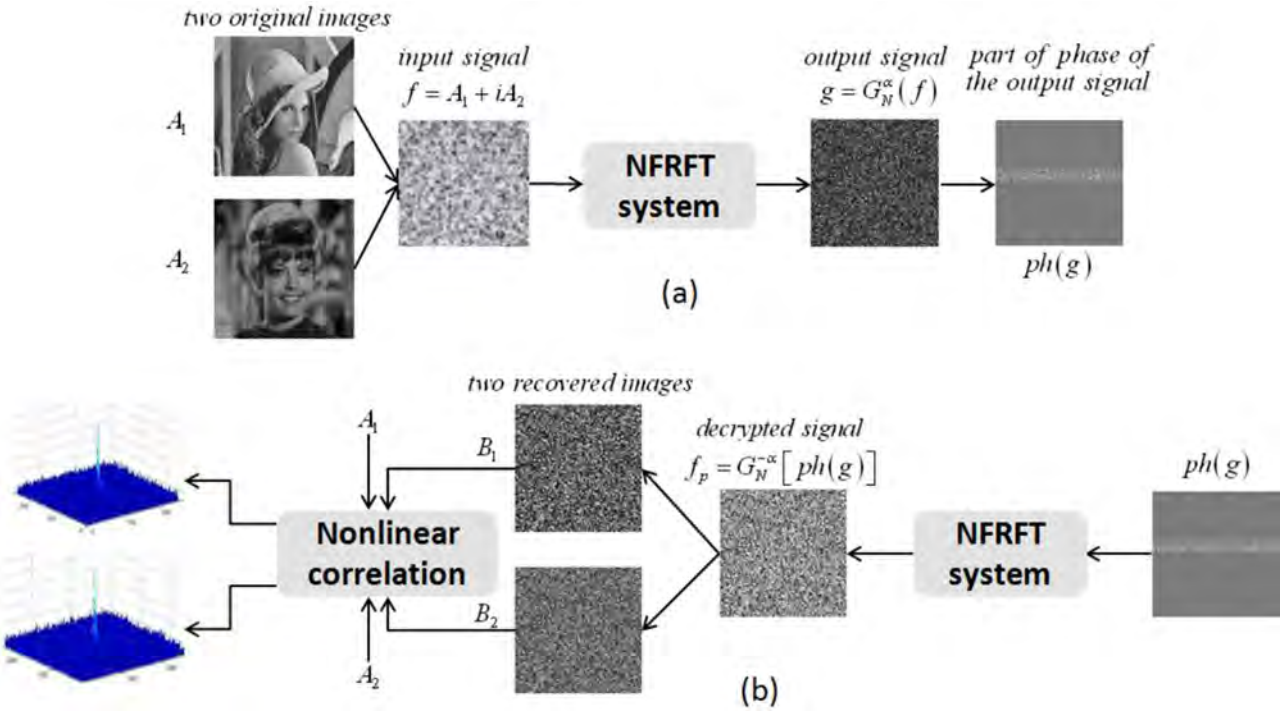

Fig. 1. The flowchart of the encryption and decryption-authentication. (a) The encryption process, (b) the decryption and authentication based on partial phase of encrypted image.

Fig. 2. The two original images. (a) 'Lena', (b) 'Zelda', (c) the phase of the encrypted result.

$$\left(G_N^{\alpha} f\right)\left(\mathbf{r}_o\right) = \frac{1}{4}\sum_{k=0}^{3}\sum_{l=0}^{3} \exp\left\{-\frac{i\pi}{2}\left[\left(\alpha - k\right)l\right] + air_l\right\} f_k\left(\mathbf{r}_o\right). \tag{1}$$

where $f_0(\mathbf{r}_o)=f(x_o, y_o)$, $f_1(\mathbf{r}_o)=F(y_o, x_o)$, $f_2(\mathbf{r}_o)=f(-x_o, -y_o)$, $f_3(\mathbf{r}_o)=F^3(y_o, x_o)$ are four basic functions and r_l, l=0,1,2,3 are any real numbers. $F(y_o, x_o)$ is the transposed Fourier transform of $f(x_i, y_i)$ and $\mathbf{r}_{i,o}=(x_{i,o}, y_{i,o})$ represent the input/output coordinates respectively. NFRFT has many common properties like FRFT and GT such as additive, unitary, etc. But unlike FRFT and GT, it is not periodic and does not belong to the class of linear canonical transforms (LCTs). The transform can be implemented by a photoelectric setup. The detailed description of the configuration of the setup is given in [24,25].

Two original images taken as the real or imaginary part respectively combine into a complex function (input signal). Performing the NFRFT on the input signal leads to the output signal (another complex function) in NFRFT domain. In the encryption system, the transform order and the coefficient parameters serve as secret keys. The flowchart of the encryption process is shown in Fig. 1(a). In classical cryptosystems, the recovering of the original image is to decrypt the whole encoded data. Such regular practice needs more transmission and storage costs on one hand and on the other hand causes security deficiency. To avoid these imperfections, in the proposed scheme, only partial phase of the encoded data is reserved for decryption. The two recovered images cannot reveal any useful visual information thereby enhance the security level of the cryptosystem.

2.2. Double-image authentication based on partial phase

First, selecting partial phase information of the output signal g to construct a new signal pH(g) which is then decoded with all the correct keys. Due to not all the encoded data involving in the decryption, the recovered images are hardly recognized by naked eyes. In order to

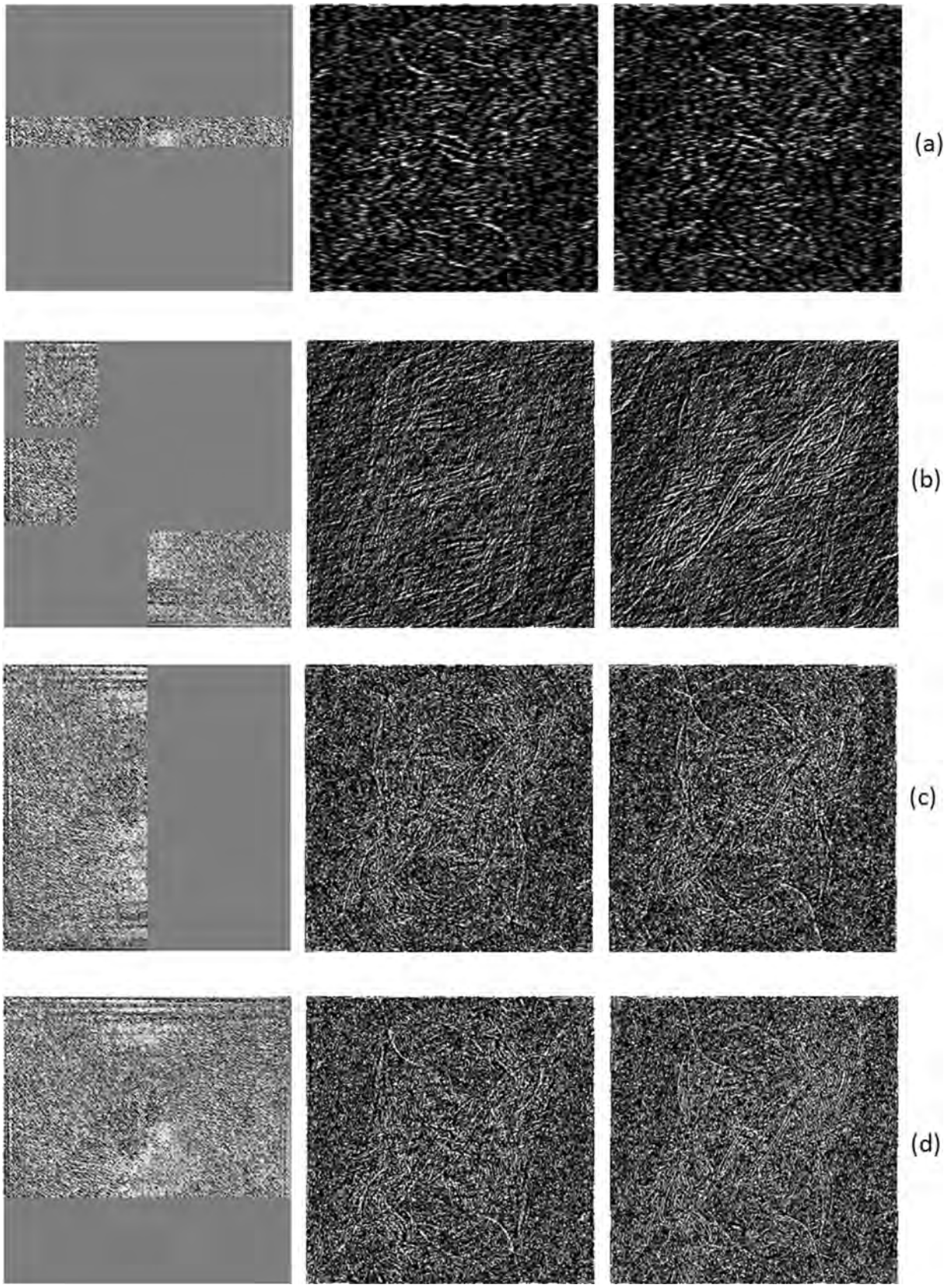

Fig. 3. The preserved phase and two corresponding recovered images. (a) 10% phase preserved, (b) 30% phase preserved, (c) 50% phase preserved, (d) 70% phase preserved.

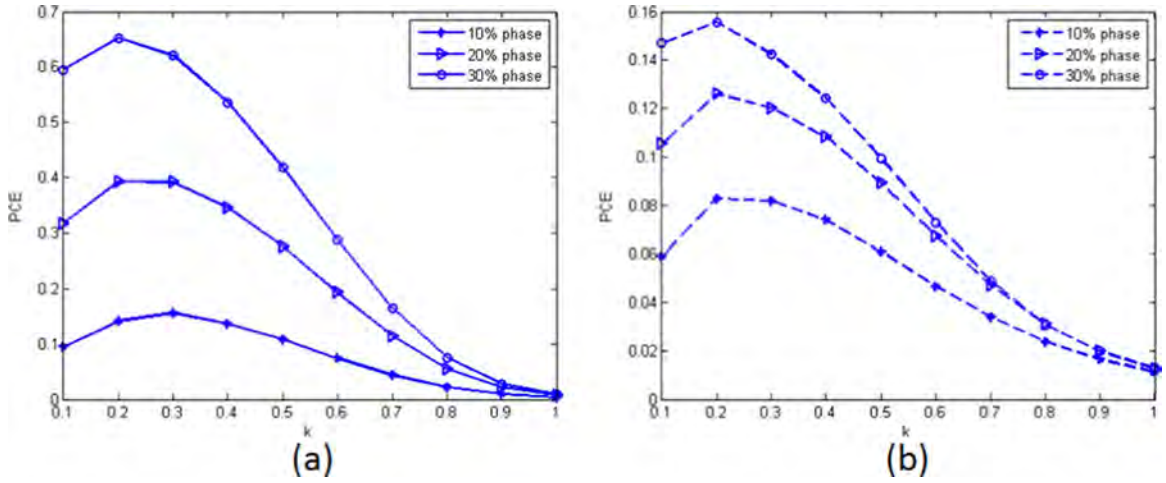

Fig. 4. The PCE with respect to k for 10%, 20%, 30% phase preserved respectively. (a) PCE corresponding to 'Lena', (b) PCE corresponding to 'Zelda'.

address the authentication problem, subsequently the nonlinear correlation algorithm is utilized to verify the authenticity of the two recovered images. The nonlinear correlation is mathematically expressed as

$$\mathrm{NC} = \mathrm{IFT}\left\{ |F_p(u,v)\cdot F(u,v)|^k \cdot \exp\left[2\pi i\left(\phi\left[F_p(u,v)\right] - \phi\left[F(u,v)\right]\right)\right]\right\} \tag{2}$$

where the uppercase denotes the Fourier transform of the corresponding lowercase function, 'IFT' denotes the inverse Fourier transform and $\phi[\cdot]$ denotes the phase of the function in the brackets. NC denotes the cross-correlation value of two compared images. The parameter k, $k\in[0,1]$ controls the strength of the nonlinearity and determines the performance of the cross-correlation of the result. k=0 corresponds to a phase extractor and k=1 to a linear correlation processor. Because the value of k varies and different value corresponds to different correlation performance, it is of necessity to choose an appropriate value of k for the authentication. PCE (peak-to-correlation energy) is defined as the ratio between the maximum peak intensity value and the total energy of the nonlinear correlation plane and indicates the sharpness and height of the output correlation peak. PCE is one of measures to determine the appropriate k.

$$\mathrm{PCE} = \frac{\max_{i,j}\left[\left|\mathrm{NC}(i,j)\right|^2\right]}{\sum_{i,j}\left|\mathrm{NC}(i,j)\right|^2} \tag{3}$$

where $1\le i\le M, 1\le j\le N, M\times N$ is the size of the image to be authenticated. According to the references [27,29,30], k=0.3 usually corresponds to a perfect performance of NC with a sharp and high peak.

3. Simulations and analysis

In the simulations, we choose two images 'Lena' and 'Zelda' of size 256×256 and with 256 graylevels as the true class test images, 'Mena' and 'Barb' as the false class test images. We first encrypt two true images using double-image encryption in NFRFT domain. The transform order is defined as α=1.01, and the coefficient parameters are (r_0, r_1, r_2, r_3)=(0.02, 0.1, 0.04, 0.1). The original images and the phase of the encrypted result are shown in Fig. 2.

3.1. Decryption based on partial phase

To enhance the security level of the cryptosystem, we only take part of the phase information of the encrypted result for decryption. There is no doubt that different percentage of the preserved phase information corresponds to different decryption result and further to different nonlinear correlation performance. In the test to illustrate the difference, we preserve 10%, 30%, 50%, 70% phase respectively with the discarded phase values being set zero. With all the correct keys, the decrypted results are shown in Fig. 3.

3.2. Authentication of the recovered images

It can be seen in Fig. 3 that the recovered images are hardly recognized visually, but can be authenticated by using nonlinear correlation algorithm, i.e., compared with two original images respectively. First of all, we plot the PCE curves with respect to k for 10%, 20% and 30% phase information preserved cases in Fig. 4. Fig. 4(a) corresponds to PCE of NC between the original image 'Lena' and recovered 'Lena' and Fig. 4(b) corresponds to PCE of NC between the original 'Zelda' and recovered 'Zelda'. We can learn from Fig. 4 that k gives better results in terms of PCE when $k\in[0.2,0.4]$. We select k=0.3 for the following simulations. The correlation results in Fig. 5 show the choice gives perfect sharpness and intensity of the correlation peak.

In Fig. 5, the left ones are recovered images corresponding to original image 'Lena' and the right ones to image 'Zelda'. The MSEs between the recovered images and the corresponding original images in the case of 10% are as large as 1.7701×10^4 and 9.9458×10^3 respectively. Nevertheless, it is noted that the primary peak of the nonlinear correlation is intense and sharp in the correlation plane especially in the case of 50%. Note that the maximum peak values of Fig. 5(d) are less than those of Fig. 5(c). To further illustrate the 'bizarre' behavior, we draw the PCE curves with respect to different percentage phase in the Fig. 6(a) which demonstrates that in the sense of PCE, it is not the case that the more phase is persevered, the higher PCE gets. For both PCEs corresponding to 'Lena' and 'Zelda', when preserving 50% phase information, the PCEs achieve their maximum. Such behavior is because two images are encrypted simultaneously so that the information of both images is mixed up. Therefore overmuch percentage of phase information means more information mixture of two images and leads to worse authentication which we can also learn by comparing Fig. 3(c) with 3(d) or Fig. 5(c) with 5(d). As a matter of fact, such behavior is exact an advantage of the proposed scheme because there is no need of storing and transmitting too much phase for authentication. Fig. 6(b) gives the PCEs of lower percentage of preserved phase cases and shows that the PCE value in low percentage cases is approximately monotonic increasing with the increase of the percentage of preserved phase.

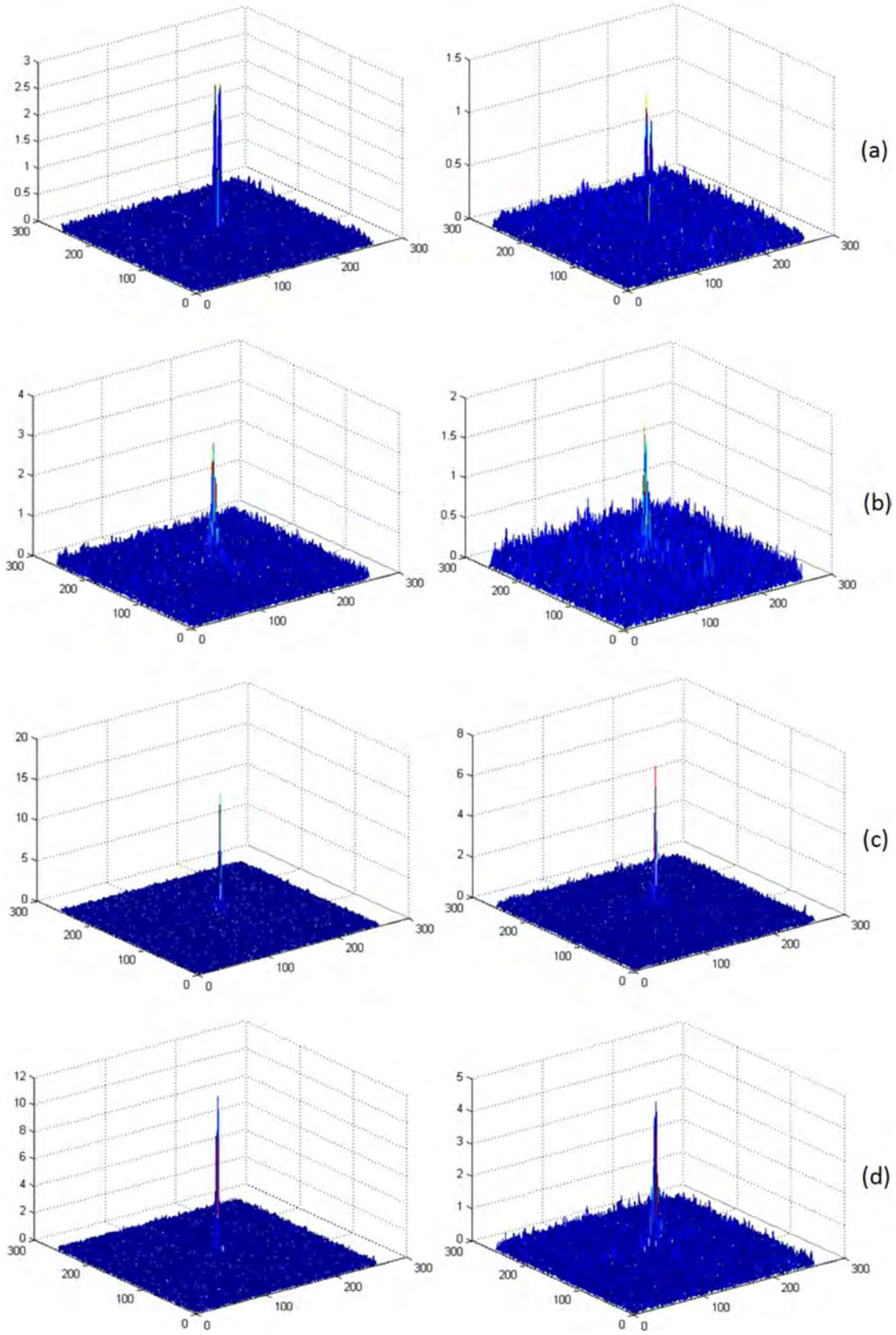

Fig. 5. The NC between the recovered image and the original image based on different percentage of preserved phase. (a) 10% case, (b) 30% case, (c) 50% case, (d) 70% case.

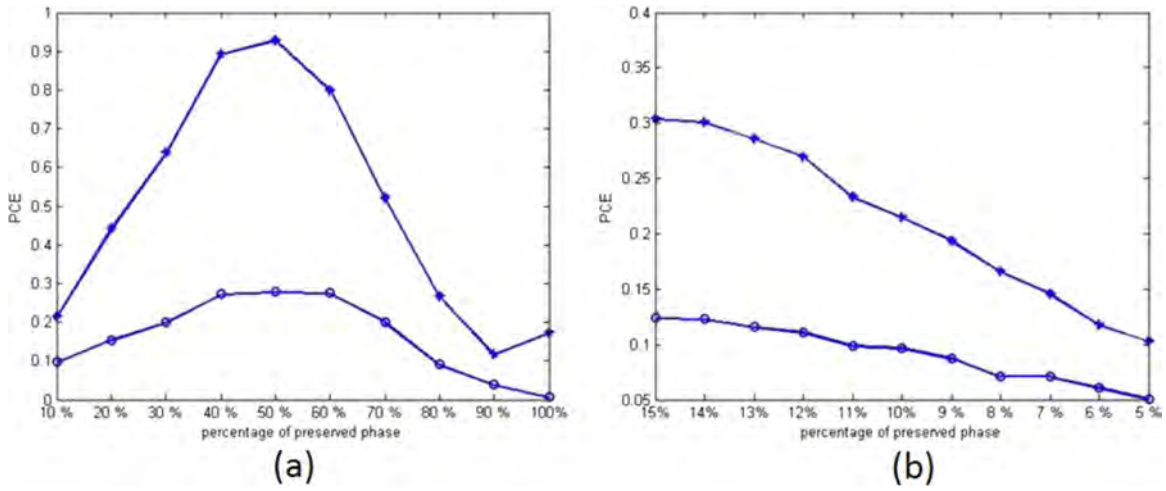

Fig. 6. The PCE values of NC between the recovered and original image based on different percentage of preserved phase. (a) 10–100% cases, (b) lower percentage cases.

3.3. The selection mode of phase information for decryption

The pattern we adopt to preserve the phase for decryption in previous section is choosing block-shape phase information as shown in Fig. 3, that is to say, the selected phase is of a block shape or of several-blocks shape. Such practice guarantees the feasibility of the proposed scheme. The location of the blocks can be randomly chosen. Of course, even for the same percentage of preserved phase information, different location yields different decryption and nonlinear correlation performance. But the difference is not obvious which here is not demonstrated in detail. While the phase information is sparsely chosen, the two recovered images cannot be authenticated. Fig. 7 shows some examples of decryption-authentication performance based on sparsely chosen phase.

As it can be seen in Fig. 7, for the lower percentage and sparsely chosen phase, the nonlinear correlation results are unsatisfactory. In the case of 50% phase, the recovered image corresponding to 'Lena' can be verified by nonlinear correlation algorithm, but it is not true for recovered 'Zelda'. Therefore, for the proposed scheme, the sparse phase information is not suitable for authentication. To address this problem, we adopt the sparse version of the complex amplitude of the encrypted result for decryption and authentication. We preserve 10% encrypted data as an example. The simulation results are shown in Fig. 8 from which we can see that, though the kept information is as little as 10% and the recovered images are hardly recognized visually, the authentication based on sparsely chosen version of the encrypted data is quite satisfactory.

3.4. Security analysis of the authentication scheme

A good authentication scheme is capable of distinguishing the right from wrong. As far as this scheme is concerned, it has two meanings: the scheme has effective discriminating ability when (1). using false image to compare with the recovered image; (2). using incorrect keys for decryption and comparing the recovered image with the original image. Fig. 9 demonstrates the NC between images decrypted from 50% phase information and false class images which are 'Mena' and 'Barb' respectively. It shows that when false image is taken as the reference image to compare with the recovered image, the NC plane is a noisy background without any remarkable correlation peak. The NC between the original and recovered image decrypted with wrong key is shown in Fig. 10 from which we can learn that even when 50% phase is used for decryption, the comparison between the recovered images and the original images is not satisfactory.

To verify the noise resistance of the proposed scheme, the noise attack simulations are performed first by adding multiplicative 'speckle' noise to the partial-phase encrypted result $ph(g)$ using the equation $ph(g)=ph(g)+n\times ph(g)$, where n is uniformly distributed random noise with mean 0 and variance 0.6 and second by adding Gaussian white noise of mean 0 and variance 0.3 to the image $ph(g)$. In the simulations, the decrypted image is recovered by from 15% of the phase information. It can be seen (Fig. 11) that although being polluted by the noises, the recovered images can still be authenticated. Therefore the proposed authentication scheme has robust capability against the noise attacks.

4. Conclusions

In this paper, we propose an image authentication based on double-image encryption and partial phase decryption in NFRFT domain. Two original images respectively taken as the real and imaginary part of the input signal are encrypted simultaneously using NFRFT. The employment of the double-image scheme lowers the time cost due to the parallel processing of two images in one time and the partial phase mode for decryption reduces the storage and transmission costs. The proposed authentication scheme achieves respective authentication of both images by single encryption-decryption operation. In the scheme, only partial phase information of the encrypted data is preserved for decryption so that the recovered images cannot be recognized visually. However, both recovered images can be authenticated using the nonlinear correlation algorithm. The security level of the cryptosystem increases because the recovered images cannot be recognized by direct visual inspection. The simulations show that even low percentage of the phase information suffices to recover two authenticable images; false images including false reference image or image recovered with wrong key cannot be authenticated; in addition, the proposed scheme has satisfactory robustness resisting noise attacks.

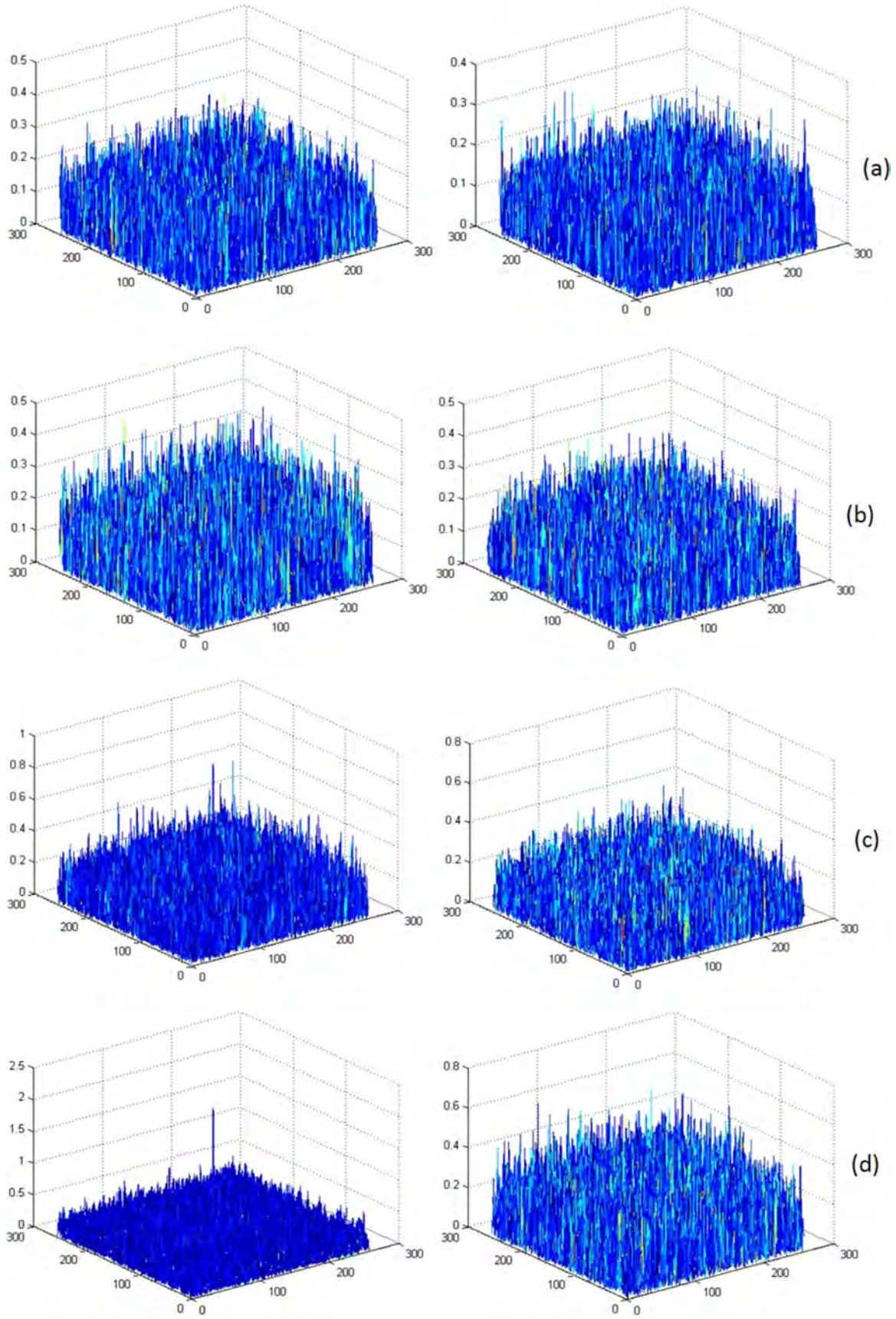

Fig. 7. The NC between the recovered and original image based on different percentage of sparsely chosen phase. The case of (a) 10%, (b) 15%, (c) 25%, (d) 50%.

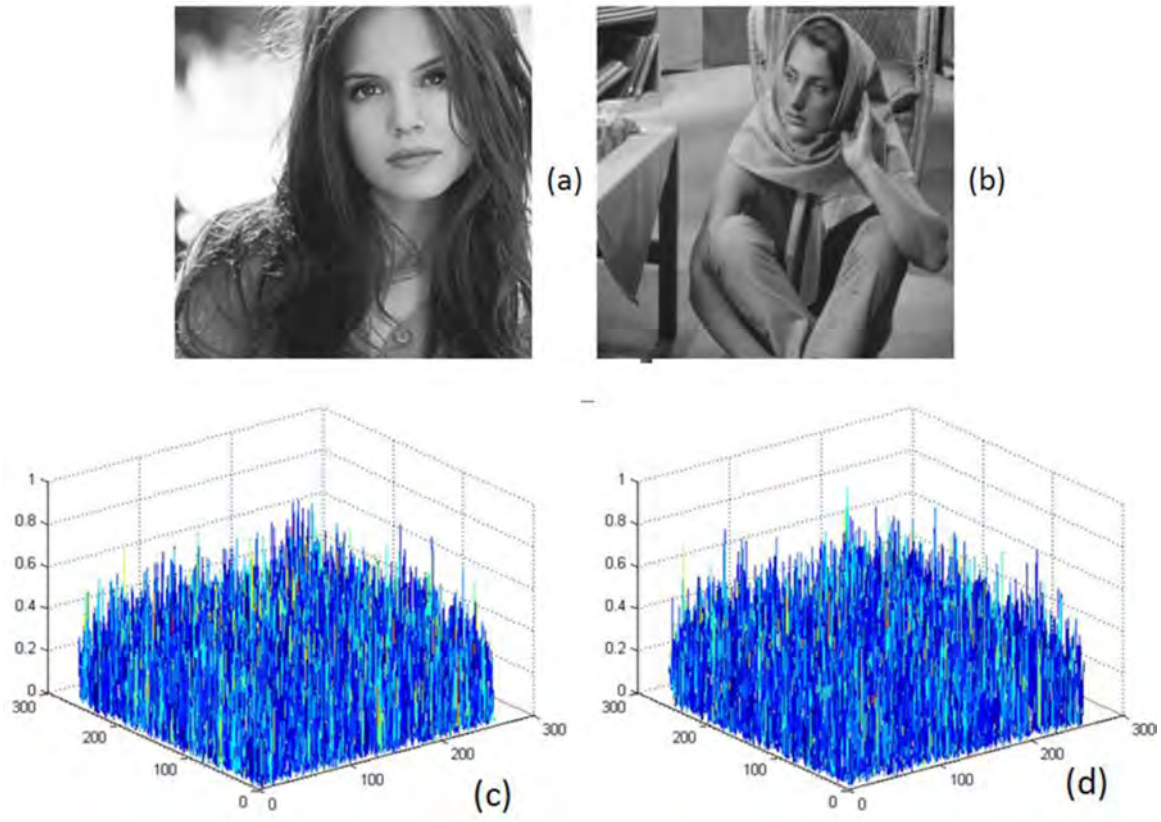

Fig. 8. The recovered images and NC based on sparsely chosen version of the encrypted data. (a) The decrypted 'Lena', (b) NC between the original and recovered 'Lena', (c) the recovered 'Zelda', (d)NC between the original and recovered 'Zelda'.

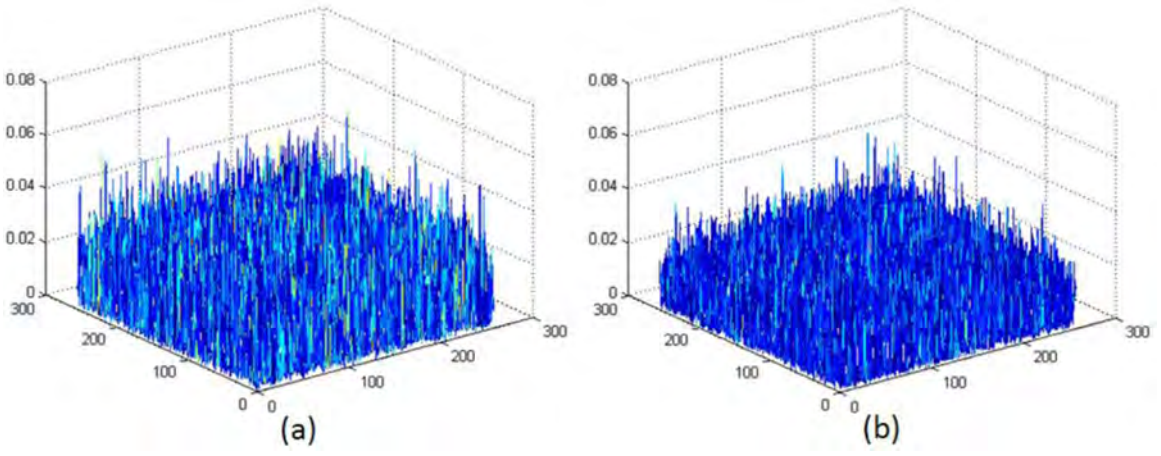

Fig. 9. The false reference image (a) 'Mena', (b) 'Barb', (c) NC between 'Mena' and recovered 'Lena', (d) NC between 'Barb' and recovered 'Zelda'.

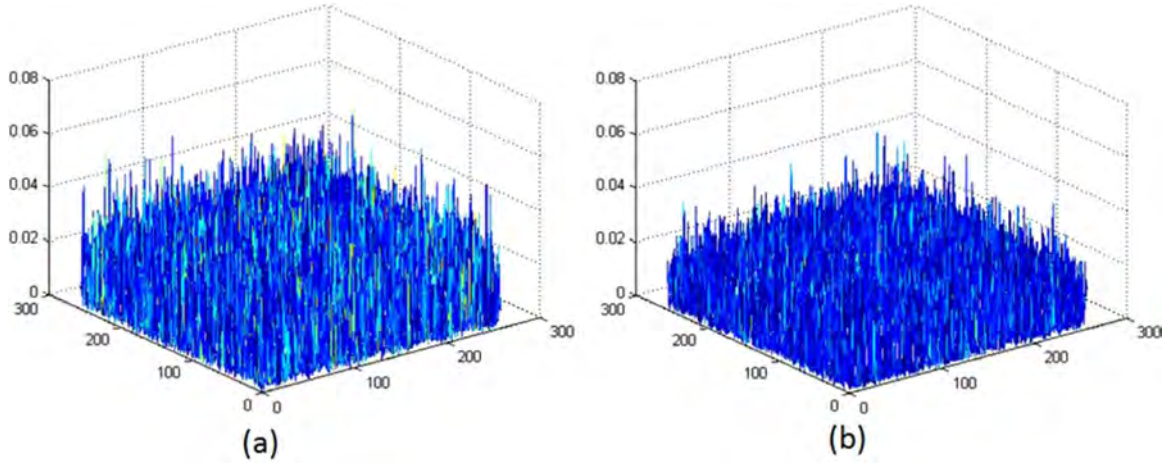

Fig. 10. NC between the original image and the recovered image decrypted from 50% phase information and with wrong decryption key. (a) 'Lena', (b) 'Zelda'.

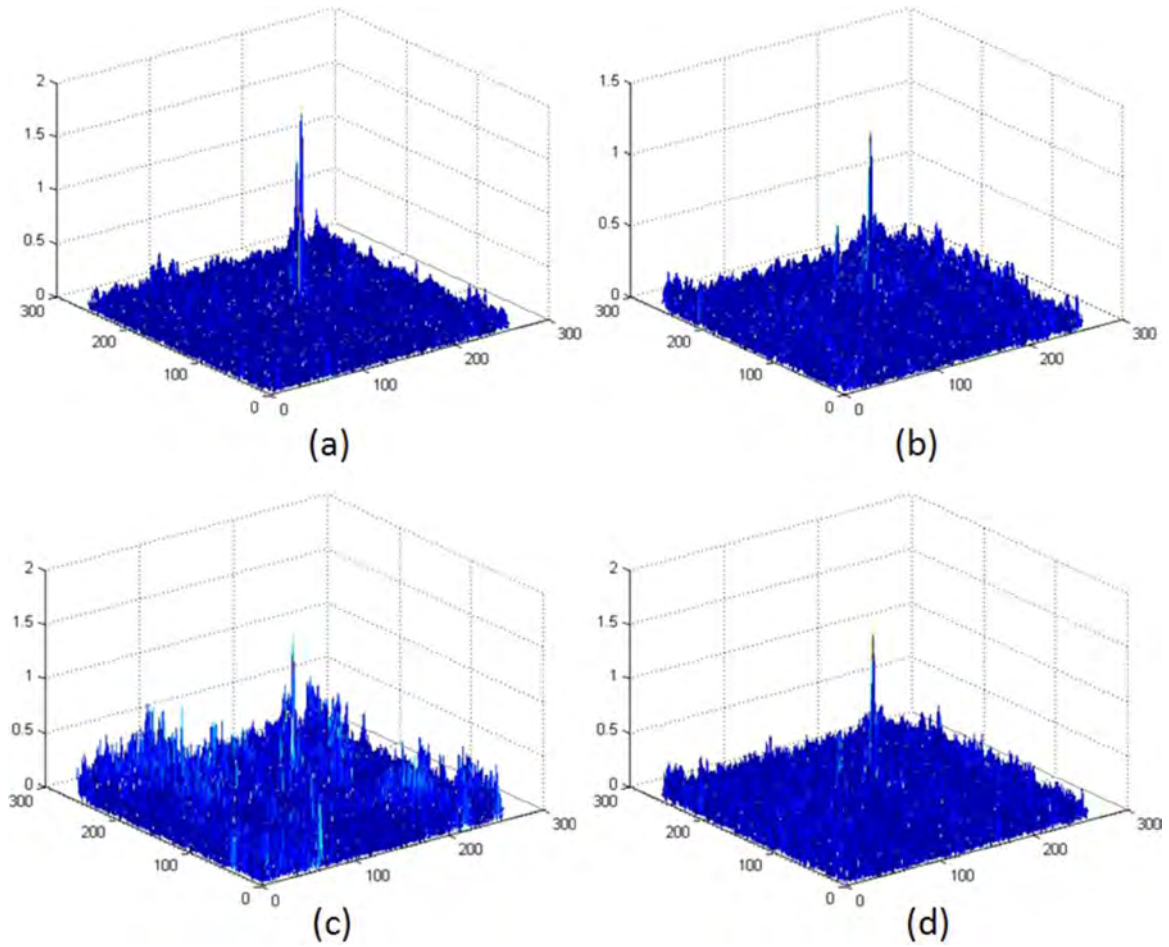

Fig. 11. Noise resistance when 15% phase is preserved for decryption. The NC between (a) the original 'Lena' and the recovered image of 'Lena' from contaminated phase with speckle noise, (b) the original 'Zelda' and the recovered image of 'Zelda' from contaminated phase with speckle noise, (c)the original 'Lena' and the recovered image of 'Lena' from contaminated phase with Gaussian noise,(d) the original 'Zelda' and the recovered image of 'Zelda' from contaminated phase with Gaussian noise.

References

[1] P. Refregier, B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding, Opt. Lett. 20 (1995) 767–769.
[2] G. Unnikrishnan, J. Joseph, K. Singh, Optical encryption by double-random phase encoding in the fractional Fourier domain, Opt. Lett. 25 (2000) 887–889.
[3] G. Situ, J. Zhang, Double random-phase encoding in the Fresnel domain, Opt. Lett. 29 (2004) 1584–1586.
[4] M. He, Q. Tan, L. Cao, Q. He, G. Jin, Security enhanced optical encryption system by random phase key and permutation key, Opt. Express 17 (2009) 22462–22473.
[5] A. Carnicer, M. Montes-Usategui, S. Arcos, I. Juvells, Vulnerability to chosen cyphertext attacks of optical encryption schemes based on double random phase keys, Opt. Lett. 30 (2005) 1644–1646.
[6] X. Peng, P. Zhang, H. Wei, B. Yu, Known-plaintext attack on optical encryption based on double random phase keys, Opt. Lett. 31 (2006) 1044–1046.
[7] X. Peng, H. Wei, P. Zhang, Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain, Opt. Lett. 31 (2006) 3261–3263.
[8] Y. Frauel, A. Castro, T.J. Naughton, B. Javidi, Resistance of the double random phase encryption against various attacks, Opt. Express 15 (2007) 10253–10265.
[9] D.S. Monaghan, U. Gopinathan, T.J. Naughton, J.T. Sheridan, Key-space analysis of double random phase encryption technique, Appl. Opt. 46 (2007) 6641–6647.
[10] W. Liu, G. Yang, H. Xie, A hybrid heuristic algorithm to improve known-plaintext attack on Fourier plane encryption, Opt. Express 17 (2009) 13928–13938.
[11] R. Tao, Y. Xin, Y. Wang, Double image encryption based on random phase encoding in the fractional Fourier domain, Opt. Express 15 (2007) 16067–16079.
[12] G. Situ, J. Zhang, Multiple-image encryption by wavelength multiplexing, Opt. Lett. 30 (2005) 1306–1308.
[13] Z. Liu, S. Liu, Double image encryption based on iterative fractional Fourier transform, Opt. Commun. 275 (2007) 324–329.
[14] H. Hwang, H. Chang, W. Lie, Multiple-image encryption and multiplexing using a modified Gerchberg–Saxton algorithm and phase modulation in Fresnel-transform domain, Opt. Lett. 34 (2009) 3917–3919.
[15] Z. Liu, Q. Guo, L. Xu, M. Ahmad, S. Liu, Double image encryption by using iterative random binary encoding in gyrator domains, Opt. Express 18 (2010) 2033–2043.
[16] J.A. Rodrigo, T. Alieva, M.L. Calvo, Gyrator transfrom: properties and applications, Opt. Express 15 (2007) 2190–2203.
[17] J.A. Rodrigo, T. Alieva, M.L. Calvo, Applications of gyrator transform for image processing, Opt. Commun. 278 (2007) 279–284.
[18] J.A. Rodrigo, T. Alieva, M.L. Calvo, Experimental implementation of the gyrator transform, J. Opt. Soc. Am. A 24 (2007) 3135–3139.
[19] L. Sui, B. Zhou, X. Ning, A. Tian, Optical multiple-image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain, Opt. Express 24 (2016) 499–515.
[20] V. Namias, The fractional Fourier transform and its application in quantum mechanics, Ins.t Math. 25 (1980) 241–265.
[21] H.M. Ozaktas, D. Mendlovic, Fractional Fourier transform and their optical implementation-I, J. Opt. Soc. Am. A 10 (1993) 1875–1881.
[22] H.M. Ozaktas, D. Mendlovic, Fractional Fourier transform and their optical implementation-II, J. Opt. Soc. Am. A 10 (1993) 2522–2531.
[23] H.M. Ozaktas, Z. Zalevsky, M. Alper Kutay, The Fractional Fourier Transform with Applications in Optics and Signal processing, John Wiley & Sons, New Jersey, USA, 2001.
[24] Q. Ran, L. Yuan, T. Zhao, Image encryption based on nonseparable fractional Fourier transform and chaotic map, Opt. Commun. 348 (2015) 43–49.
[25] L. Yuan, Q. Ran, T. Zhao, L. Tan, The weighted gyrator transform with its properties and applications, Opt. Commun. 359 (2016) 53–60.
[26] B. Javidi, Nonlinear joint power spectrum based optical correlation, Appl. Opt. 28 (1989) 2358–2367.
[27] E. Pérez-Cabré, M. Cho, B. Javidi, Information authentication using photon-counting double-random-phase encrypted images, Opt. Lett. 36 (2011) 22–24.
[28] W. Chen, X. Chen, A. Stern, B. Javidi, Phase-modulated optical system with sparse representation for information encoding and authentication, Photonics J. IEEE 5 (2013) 6900113-6900113.
[29] J. Chen, Z. Zhu, F. Chong, H. Yu, L. Zhang, Gyrator transform based double random phase encoding with sparse representation for information authentication, Opt. Laser Technol. 70 (2015) 50–58.
[30] J. Zheng, X. Li, Image authentication using only partial phase information from a double-random- phase encrypted image in the Fresnel domain, J. Opt. Soc. Korea 19 (2015) 241–247.
[31] W. Chen, Single-shot imaging without reference wave using binary intensity pattern for optically-secured-based correlation, IEEE Photonics J. 8 (2016) 6900209.