Opt Quant Electron (2016) 48:12
DOI 10.1007/s11082-015-0291-2

Optical spectrum encryption in associated fractional Fourier transform and gyrator transform domain

Hang Chen[1] · Xiaoping Du[1] · Zhengjun Liu[2]

Received: 6 July 2015 / Accepted: 9 September 2015 / Published online: 14 December 2015

Abstract An optical spectrum encryption algorithm for hyperspectral image is proposed in this paper, in which the spatial and spectrum information can be encrypted simultaneously. The Baker mapping is utilized to scramble each band of the hyperspectral cube before the optical transform. Subsequently, 100 bands are divided into real part and imaginary part of the complex function expressing light field. Then, the scrambled data is imported into fractional Fourier transform and gyrator transform system. A random binary vector is designed and employed in the optical transform for enhancing the security of the encryption system. The amplitude and phase information in the output plane can be regarded as the encrypted information. Some numerical simulations are made to demonstrate the performance of the proposed encryption system.

Keywords Hyperspectral image · Cryptography · Optical transform

1 Introduction

The optical system has been deeply investigated in obtaining and processing information in the past decades and the optical information security technique is becoming an important method in the process of transmission and storage due to its parallel processing and high speed. Since Refregier and Javidi (1995) first proposed double random phase encoding (DRPE) in 1995, many kinds of optical transform or optical information system have been developed for protecting the secret image (Matoba and Javidi 1999; Liu and Liu 2007; Meng et al. 2006; Zhu et al. 2009; Abuturab 2013; Alfalou and Brosseau 2010; Chen et al.

✉ Hang Chen
hitchenhang@foxmail.com

[1] Department of Space Equipment, The Academy of Equipment, Beijing 101416, China

[2] Department of Automation Measurement and Control, Harbin Institute of Technology, Harbin 150001, China

2011), such as Fresnel transform, fractional Fourier transform (FrFT), Mellin transform and interference. The random phase encoding is employed as the main key in most of these encryption algorithms and Peng et al. (a, b) have testified that the DRPE is vulnerable to chosen-plaintext attack and know-plaintext attack. Note that the storage space of the random phase is close to the original data (Kumar et al. 2011). Chaotic mapping has also been introduced to generate random data in some encryption scheme (Alfalou and Brosseau 2010; Chen et al. 2011; Lang 2012). In addition, some pixel scrambling operations have been utilized in some newly image hiding technique, for instance, jigsaw transform, Baker mapping and Arnold transform (Abuturab 2012; Liu et al. 2009a; Sui et al. 2014). Some parameters generated in these scramble operation will be chosen as the additional keys to enhance the security of the encryption system (Abuturab 2012; Liu et al. 2009a, 2013; Sui et al. 2014; Enayatifar et al. 2014; Chen et al. 2013).

A new concept of multi-image encryption has caused much attention since Situ and Zhang (2004) first proposed a multi-image encryption based on wavelength multiplexing. Subsequently several kinds of double images encryption, triple images encryption and RGB image encryption schemes have been deeply researched in the past decade (Chen et al. 2013; Tao and Xin 2007; Liu et al. 2009b, 2010). However, the multispectral image and hyperspectral image which are considered as the most important data of space remote sensing (especially in the field of military detection), have seldom been researched in recent years (Zhang et al. 2012). We recently proposed a new concept of spectrum information hidden technology (Chen et al. 2015).

The hyperspectral image contains rich information both in spatial and spectral domain, which makes it possible to identify and discriminate the target in spectral domain (Nakauchi and Nishino 2012). In this paper, we present an optical spectrum encryption algorithm for hyperspectral image by using chaotic map and associated FrFT and gyrator transform. The proposed encryption system can protect the information both in spectral domain and spatial domain, simultaneously. Firstly, an original hyperspectral image is divided into ever single band and the Baker mapping is utilized to changing the pixels sequence of each band. Subsequently, the scrambled images generated by Baker mapping operation are separated into real part and imaginary part of the complex function expressing light field. These complex functions are then put into the input plane of the optical transform system, which is composed of FrFT and gyrator transform. A random binary vector is designed and introduced as the parameters in optical transformation to strengthen the security of the proposed encryption system. Numerical simulation experiments are performed to demonstrate the validity of the encryption scheme.

The rest of this paper is organized in the following sequence. In Sect. 2, the proposed spectrum encryption/decryption algorithm is introduced in detail. In Sect. 3, numerical simulation results are made and given to test the validity of the algorithm. Concluding remarks are summarized in the Sect. 4.

2 Hyperspectral image encryption algorithm

Firstly, both the chaotic map, Baker mapping, FrFT and gyrator transform are introduced in this section. Thereafter, the intact encryption algorithm is addressed in detail.

2.1 Random binary series

Chaotic map can generate random series by iteration. For instance, a logistic map can be defined mathematically as follows

$$S_{n+1} = p \cdot S_n(1 - S_n) \tag{1}$$

where p is the coefficient of the map. In fact, the logistic map has the chaotic behavior called Pomeau–Manneville scenario, which means that all the value of $\{S_n\}$ stay in the range of [0, 1] if the coefficient p located in the interval [3.57, 3.82] (Jeffries and Perez 1982). Referring to Liu et al. (2010), we designed a new logistic map as follows

$$S_{n+1} = (3.82 - S_n/4) \cdot S_n(1 - S_n) \tag{2}$$

where the coefficient of this map is $p = (3.82 - S_n/4)$. The Eq. 2 can be utilized to generate the random binary data. Here the initial value in calculation is $S_1 = 0.82$ and $p = 3.62$. According to the logistic map, the value of the random binary data $\{S_n\}$ completely depends on the initial value and iterative time.

2.2 Baker mapping

Baker mapping is a kind of two-dimensional chaotic process (Fridrich 1998), which can be utilized to scramble every single band of the hyperspectral image before performing the optical transform. Mathematically, the Baker mapping can be expressed as

$$\begin{cases} r' = \dfrac{N}{n_j}\left(r - N_j\right) + \mathrm{mod}\left(s, \dfrac{N}{n_j}\right), \\ s' = \dfrac{n_j}{N}\left(s - \mathrm{mod}\left(s, \dfrac{N}{n_j}\right)\right) + N_j, 0 \le r,\ s < N. \end{cases} \tag{3}$$

where the vectors (r, s) and (r', s') denote the pixel of the image before and after Baker mapping operation, respectively. The integer n_j is the input parameter of Baker mapping, while N/n_j is also an integer. And the parameter N is the size of the square image, which obeys the relationship as $N_j = n_1 + n_2 + \cdots + n_j$, which is an accumulated value of the first j elements of all the parameters n_j in the mapping, $N_0 = 0$. Moreover, the parameter n_j should satisfy the equation $n_1 + n_2 + \cdots n_j + \cdots + n_{J-1} + n_J = N$, $j = 1, 2, \ldots, J$.

The position of the pixel in hyperspectral image will change and the value is multiplied by a factor which can be defined as (Chen et al. 2015)

$$I(r', s') = \begin{cases} I(r, s)/t, & \textit{if } \phi(r, s) \ge 0, \\ I(r, s) \cdot t, & \textit{otherwise}. \end{cases} \tag{4}$$

where ϕ is the phase function and limited in the interval $[-\pi, \pi)$. Besides, $I(r', s')$ represents the randomized image after the operation expressed as Eq. 2. Finally, the inverse operation of Baker mapping with pixel value modulation can be calculated by the equation as follows as (Chen et al. 2015)

$$I(r, s) = \begin{cases} I(r', s')/t, & \textit{if } \phi(r, s) \ge 0, \\ I(r', s') \cdot t, & \textit{otherwise}. \end{cases} \tag{5}$$

where the vector (r', s') is calculated by Eq. 3 and note the coefficient t in Eqs. 4 and 5 is set as 0.5 in the following section of this paper.

2.3 Gyrator transform and FrFT

The gyrator transform is a kind of linear canonical transform which only has a two-dimensional format (Rodrigo et al. 2007a, b). The transform of a two-dimensional image $g(x, y)$ is expressed as

$$\begin{aligned} G(u,v) &= \xi^{\alpha}[g(x,y)](u,v) \\ &= \frac{1}{|\sin\alpha|}\iint g(x,y)\exp\left[i2\pi\frac{(xy+uv)\cos\alpha - xv - yu}{\sin\alpha}\right]\mathrm{d}x\mathrm{d}y, \end{aligned} \tag{6}$$

where $G(u, v)$ is the output of the gyrator transform which usually be regarded as the additional key in image encryption schemes. This transformation has the properties of linearity, energy conversation and index additivity. The inverse gyrator transform of ξ^{α} is $\xi^{-\alpha}$ or $\xi^{2\pi-\alpha}$. When $\alpha \in [0, 2\pi]$, the gyrator transform can be implemented in the optical system composed of six thin cylinder lenses (Rodrigo et al. 2007b). In addition, when

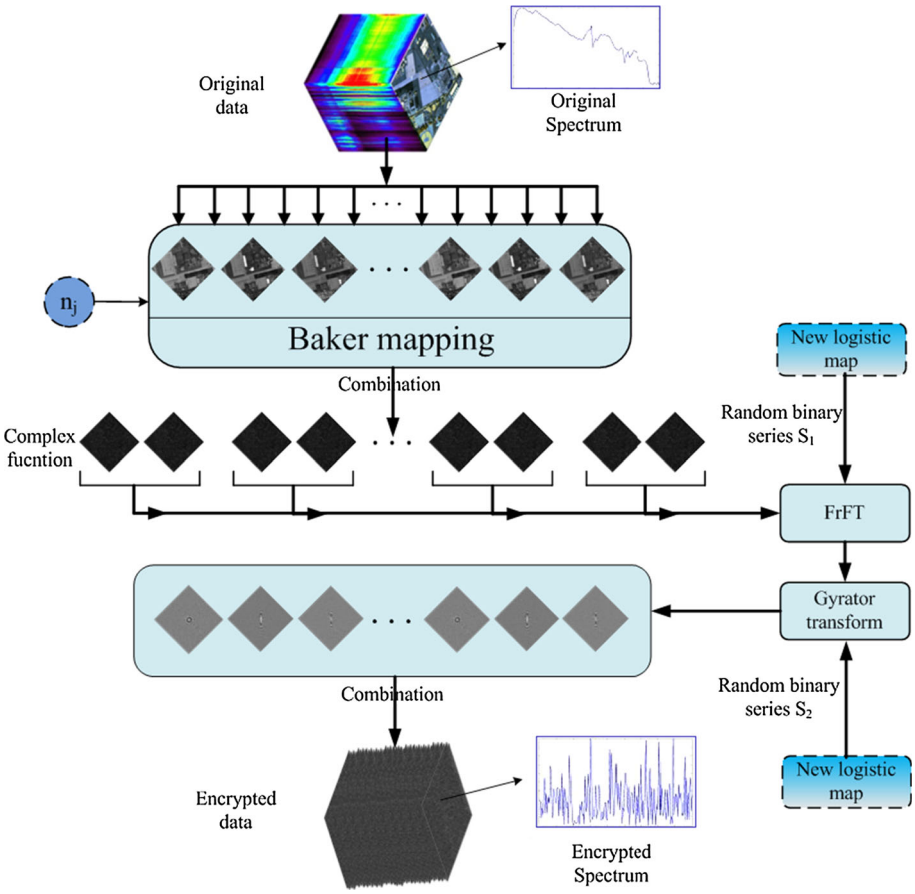


Fig. 1 The flowchart of the hyperspectral cube encryption algorithm

$\alpha = \pi/2$, the expression of the transform becomes a Fourier transform with the rotation of the coordinates (u, v).

The FrFT is an expanded version of Fourier transform, which is similar to Gyrator transform (Lohmann 1993; Ozaktas et al. 2001). The mathematical definition of the two-dimensional image $g(x, y)$ can be expressed as

$$\begin{aligned} F(u,v) &= \xi^{\alpha}[g(x,y)](u,v) \\ &= A_{\alpha}\iint g(x,y)\exp\left[i\pi\frac{(x^2+y^2+u^2+v^2)\cos\phi_{\alpha}-2(xu+yv)}{\sin\phi_{\alpha}}\right]\mathrm{d}x\mathrm{d}y, \\ A_{\alpha} &= 1-i\cot\phi_{\alpha}, \quad \phi_{\alpha}=\alpha\pi/2, \end{aligned} \tag{7}$$

where $F(u, v)$ and $g(x, y)$ are the output and input of the FrFT, respectively. The symbol α represents the fractional order. When $\alpha = 1$, the transform becomes conventional Fourier transform and the inverse transform of ξ^{α} is $\xi^{-\alpha}$, which is similar to the Gyrator transform mentioned above. FrFT can be implemented in the optical system composed of a single or double lens setup, which has been proposed by Lohmann to balance the quadratic phase effects caused by the Fresnel diffraction (Lohmann 1993).

Both the gyrator transform and FrFT will be adopted in our hiding algorithm. Actually, some other optical transforms, such as Fresnel transform and Hartley transform can also be utilized in this algorithm.

2.4 Spectrum encryption for hyperspectral image

The flowchart of the spectrum encryption is illustrated in Fig. 1. To complete the proposed encryption, Baker mapping, random binary series, FrFT and gyrator transform are considered and utilized. Firstly, the original hyperspectral image is separated and every band of the cube is regarded as an ordinary two-dimensional image in the following operation. Then every single band image is scrambled by using Baker mapping with different parameter n_j as depicted in the flowchart.

In the following step, the scrambled data is divided into real part and imaginary part of the complex function expressing light field. The complex function $I_1 + i \cdot I_2$ can be encoded into the format with amplitude $A(x, y)$ and phase $\varphi(x, y)$ as

$$A(x,y)\exp[i\varphi(x,y)] = I_1(x,y) + i \cdot I_2(x,y). \tag{8}$$

Subsequently, 100 of these complex functions are put into the input plane of the optical system and encoded by associated FrFT and gyrator transform with two random series S_1 and S_2 generated by Eq. 2. Specifically, the output of the FrFT is regarded as the input light field of the gyrator transform. The random series S_1 and S_2 are introduced into the FrFT and gyrator transform respectively as the rotation angle α to strengthen the security of the encryption system. Therefore, attacker cannot retrieve the other data if only some part of the keys and encryption data because each optical transform result in this system is unique.

Finally, the output light field of the optical system is the encrypted data of this encryption algorithm. Here, the decrypted hyperspectral image has the same size compare with the original hyperspectral data. The two random series S_1 and S_1 generated by new logistic map described in Eq. 2 are the main keys of this encryption scheme. Furthermore, the input parameter n_k and phase function ϕ in Baker mapping will be set as the additional keys. Some simulations will be given to show the decryption result of losing key in the following section.

All amplitudes and phases of the complex function mentioned above will be encoded into the optical transform by the modulation of the spatial light modulator (SLM) (Rodrigo et al. 2007b). The Baker mapping and the new logical map will be employed in the computer during encryption process. Note that every step of the encryption process is reversible. Therefore, the intact decryption process can be performed along with the reverse direction of the encryption process as depicted in the Fig. 1.

Here, the intact encryption algorithm is achieved by an electro-optical hybrid setup as illustrated in Fig. 2. The complicated calculation in Baker mapping and new logical map are accomplished by a high-performance computer in the hybrid setup, while the FrFT and gyrator transform are achieved by the optical system. Hundreds of beams encode every single band of the hyperspectral image. The encrypted field light will be recorded by in-line holography technique at the output plane of the hybrid system. Furthermore, the data communication between computer and optical system are accomplished by SLM and CCD in the hybrid setup.

3 Numerical simulation

Some numerical simulations in this section are made for demonstrating the validity of the encryption algorithm. A hyperspectral image 'Sandiego' from man-made satellite AVIRIS having 180 bands is regarded as the original secret image in the following simulation. For each single band of the secret image, the scene is a military airport and the size of the image is 256 $\times$ 256, which is shown in Fig. 3. Besides, the parameter n_j in Baker mapping can be set in different value and different combinations to enhance the security of the intact scheme. As mentioned above, the secret hyperspectral image is separated into 180 bands of two-dimensional image and each single band image is scrambled by using the Baker mapping before the date converted by optical transform. In the following step, every two

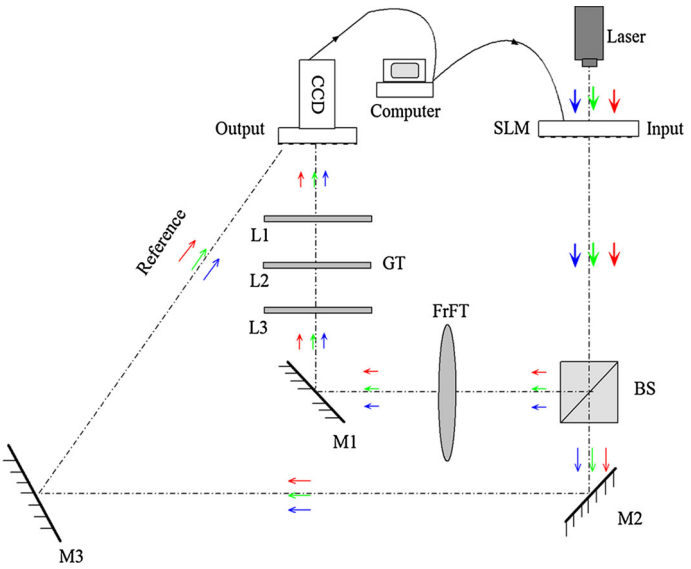
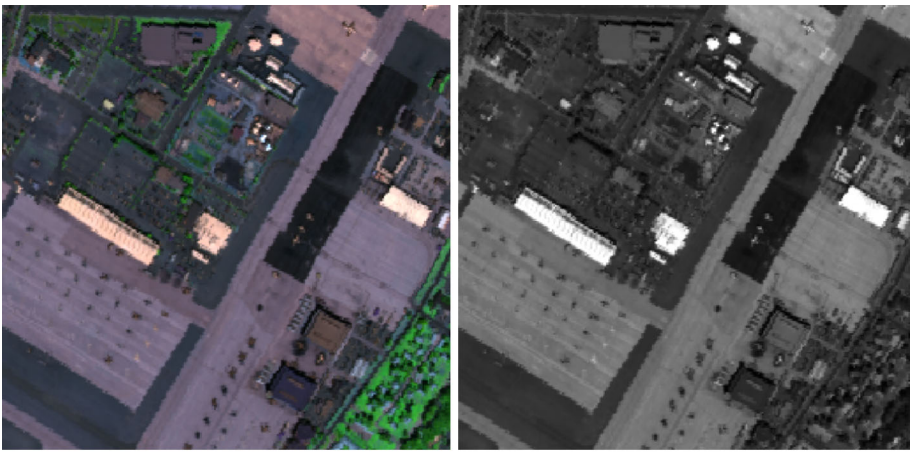


Fig. 2 The electro-optical setup of the encryption system



(a) **(b)**

Fig. 3 The **a** false color composite and **b** 30th band image of the original hyperpsectral image

the scrambled images are combined to be a complex function expressing light field. These interim data are then converted by FrFT and gyrator transform sequentially with two random binary series S_1 and S_2 generated by new logistic map described in Eq. 2. Here the random series serve as the rotation angle in the FrFT and gyrator transform, hence every encrypted band image is unique. Figure 4 gives the encrypted 50th and 120th band images and the corresponding decrypted images. Some quantitative analysis will be made in the next step.

In calculation we use a computer with Core2, CPU 2.1 GHz and 2048 Mb memory under Windows 7 system. The encryption process and decryption processes for the 70th band image take 0.31 and 0.35 s, respectively.

To test the difference between the recovered data and original data, the peak signal-to-noise ratio (PSNR) function is introduced and expressed as

$$PSNR(I_{\mathrm{d}}, I_0) = 10\log_{10}\frac{255^2 M \times N}{\sum_{\forall x,y}\left[I_d(x,y) - I_0(x,y)\right]^2}\ (\mathrm{dB}). \tag{9}$$

The I_{d} and I_0 denote the decrypted image and original image, respectively. The parameter M and N represent the size of the two images in this calculation.

As mentioned above, the parameter n_j in the Baker mapping serves as the additional key in this encryption scheme. Firstly, the contribution of the additional key will be tested and analyzed. Here, we suppose that the intact encryption process is filched and the additional key of the 90th band are destroyed or stolen by the illegal user, the PSNR curve of the decrypted hyperspectral image under this circumstance is shown in Fig. 5. Note that the additional key n_j will protect the other secret image because the additional keys in each band can be set in different combinations. And the numerical simulation shown in Fig. 5 testifies this verdict. As we can see from Fig. 5, The decrypted 90th band image is noise-like, while the decrypted image next to 90th band is clear and equal to the original data to the human vision. Therefore, the additional key can protect the secret image successfully

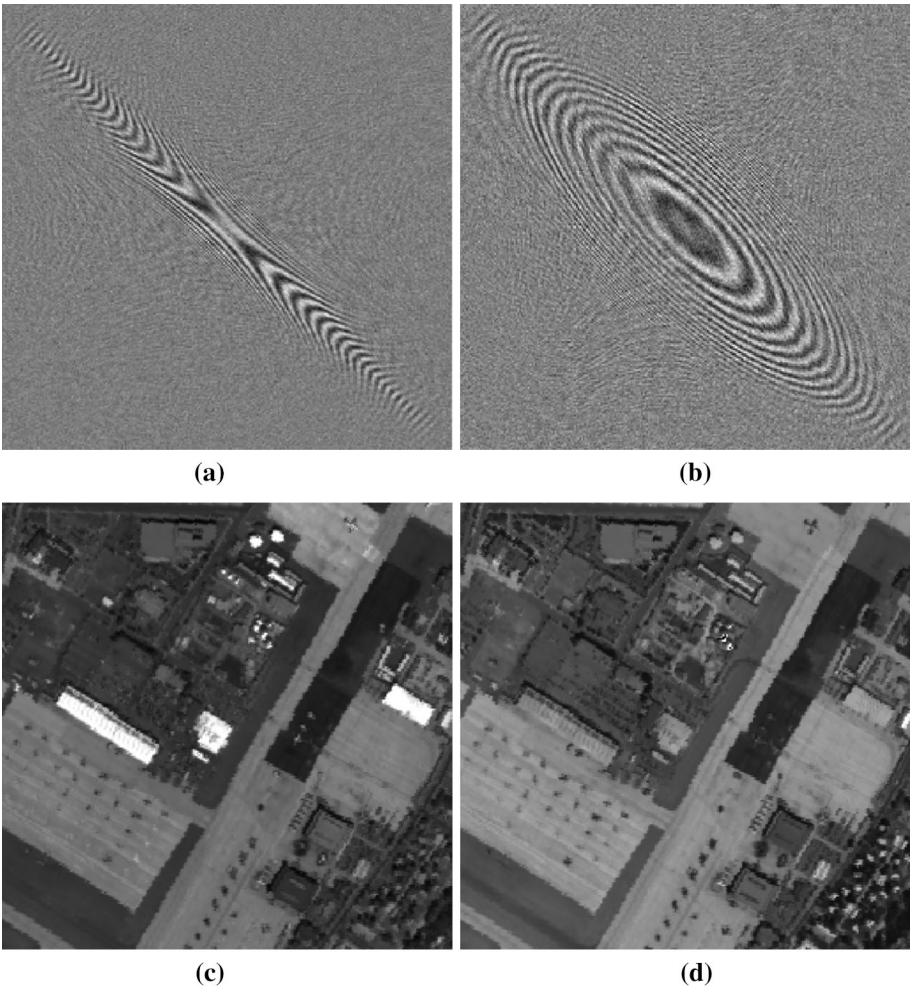


Fig. 4 Encrypted results: **a** the encrypted 50th band, **b** encrypted 120th band, **c** decrypted 50th band and **d** decrypted 120th band

even the 90th key is stolen by the attacker. Of course, the spectrum information of the hyperspectral image is still under the protection of our encryption algorithm.

The phase function ϕ in the Baker mapping operation serves as the other additional key in this encryption system. Another experiment is designed to prove the capability of other additional key ϕ. When the phase function is incorrect and other keys are correct, some decryption results are illustrated in Fig. 6. In numerical simulation, the incorrect key ϕ is designed in different situations. Firstly, when a quarter of the phase function in 50th band is destroyed, the decrypted image is shown in Fig. 6a. More precisely, the values of ϕ at the left-top corner are replaced with 0 and the main information of the decrypted image can be recognized in vision but far different from the original one. Secondly, the decrypted process is performed with a complete incorrect phase function ϕ and the result is displayed in Fig. 6b. The decrypted image is almost a scrambled image and has lost most of the

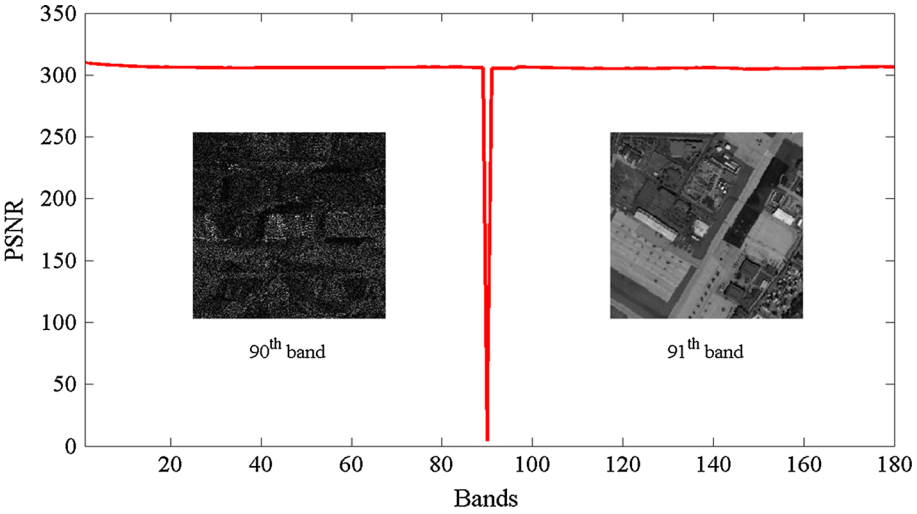


Fig. 5 The PSNR curve calculated by using a inaccurate parameter n_{90}

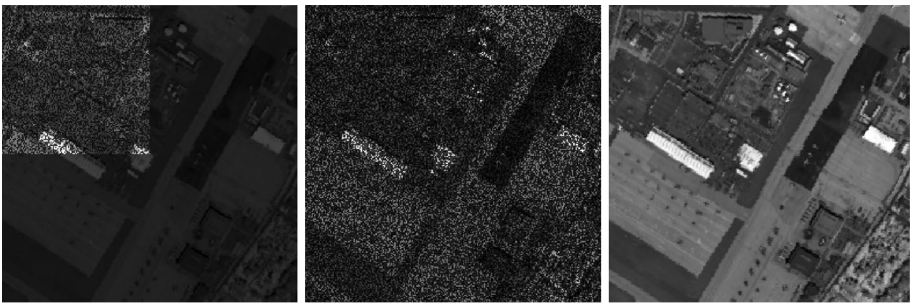


Fig. 6 The test of decryption: **a** a quarter of phase function ϕ is destroyed, **b** using the incorrect phase function ϕ and **c** the correct decrypted 50th band image

information of the original secret image. The decrypted data with correct key is shown in Fig. 6c.

In the following experiment, the contribution of the main key random binary series S_1 and S_2 is analyzed. The encrypted hyperspectral is impossible to be decrypted without the main key due to the strong randomness of the random binary series. More importantly, the main key can protect the intact hyperspectral image, including the spectrum information of the military target in the image. As mentioned above, the random binary series are generated by the new logical map and the every key is unique in the encryption process. It means that the main keys and the encrypted data have the one-to-one relationship. The decrypted result with the wrong main key and correct additional keys is displayed in Fig. 7. Suppose that the series S_1 and S_2 are falsified by the attacker, the decryption in this case is considered and simulated. When the assaulted series S_1' is close to the real one and all the other keys are under protection, the corresponding decrypted result are shown in Fig. 7a, b.

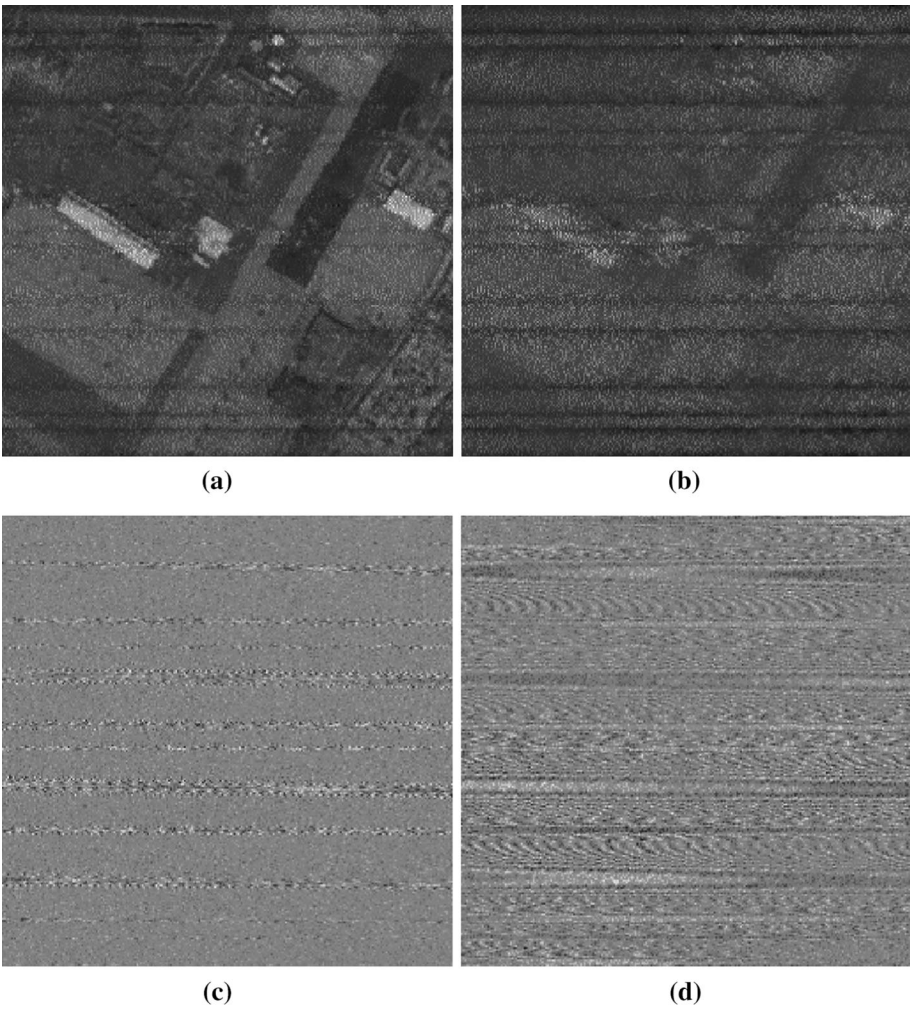


Fig. 7 The test of decryption: **a** using $S_1 \times 0.999$, **b** $S_1 \times 0.995$, **c** using incorrect S_1 and **d** using incorrect S_2

Here, the S_1' tested in this experiment is set as $S_1' = 0.999 \times S_1$ and $S_1' = 0.995 \times S_1$. From Fig. 7, the detail information is under protection by the main keys. In addition, the experiment of the main key S_2 shows the similar results. When the illegal user decrypted the data by using the wrong main keys, the decrypted data are complete noise pattern as shown in Fig. 7c, d. Note that in calculation we use the 50th band image as the experiment data.

To measure the sensitivity of the main key in decryption process, a tiny variable t is introduced into the random binary series S_1. The 90th band image is tested in this experiment and the $S_1(90) = 0.9050$. In this case, all the other main and additional keys are known, the value of $S_1(90)$ is changed around the correct value and the corresponding PSNR curve is illustrated in Fig. 8. Here the sampling step length of the key in this

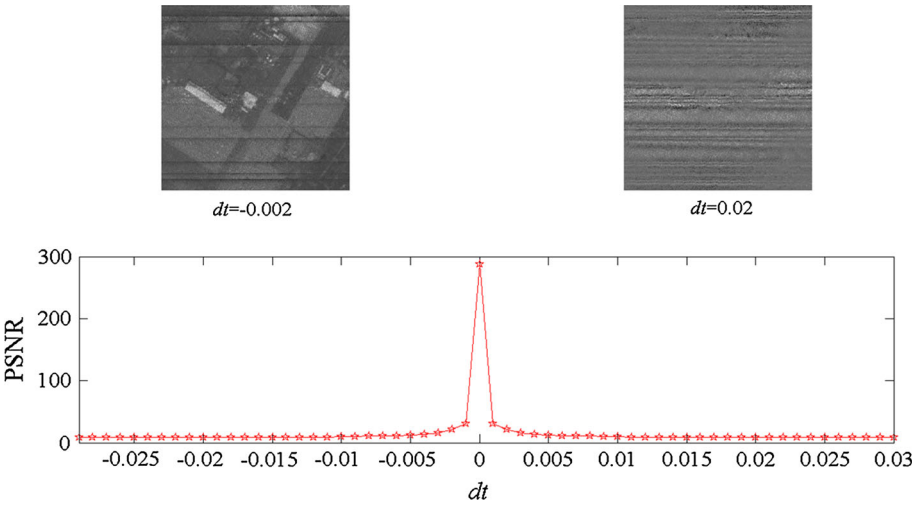


Fig. 8 PSNR curve calculated with various values of dt

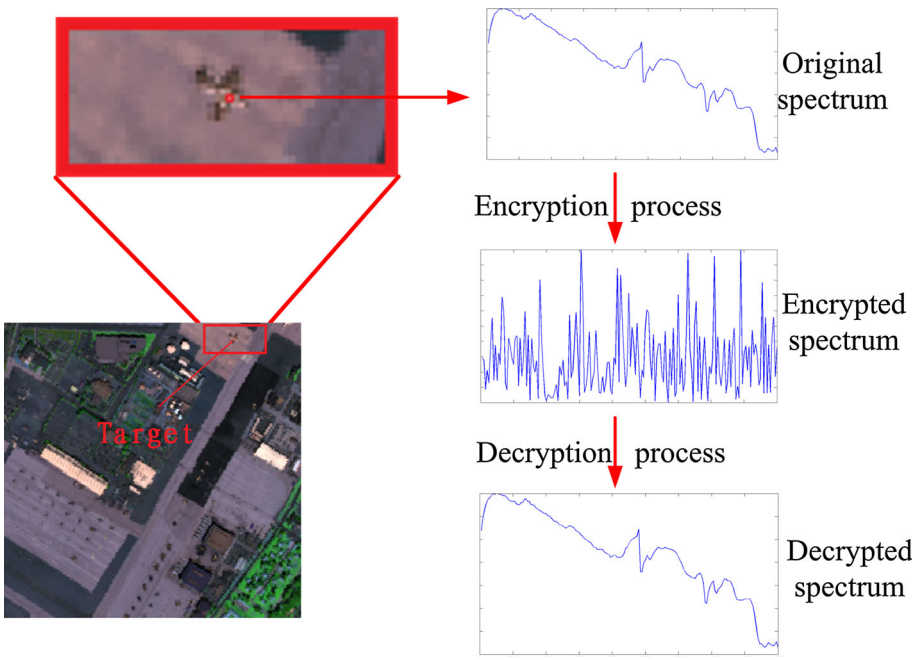


Fig. 9 PSNR curve calculated with various values of dt

experiment is taken as 0.001. From Fig. 8, the left-top and right-top decrypted image are almost noise like image even if the key $S_1(90)$ is very close to the correct one. Moreover, the PSNR curve shown in Fig. 8 proves the sensitivity and validity of the main key in

protecting the secret information. The hyperspectral data can be detected in a very small interval of S_1 and S_2.

According to the numerical simulation mentioned above, both the main keys and the additional keys perform well in protecting the secret single band image. In the following step, the capability in protecting the spectrum information of our algorithm is tested and analyzed. In this experiment, one of the aircraft in the airport is selected as the secret target whose spectrum information should be under protection. The flowchart of the encryption/decryption process of the spectrum is shown in Fig. 9. Here we chose the spectrum of specific pixel (200, 15) in the following experiment. To analyze the spectrum information of the aircraft, the original spectrum, encrypted spectrum and decrypted spectrum have been drawn in Fig. 10. It is obviously that the encrypted spectrum is far different from the original one. To measure the discrimination between these spectrum information, a

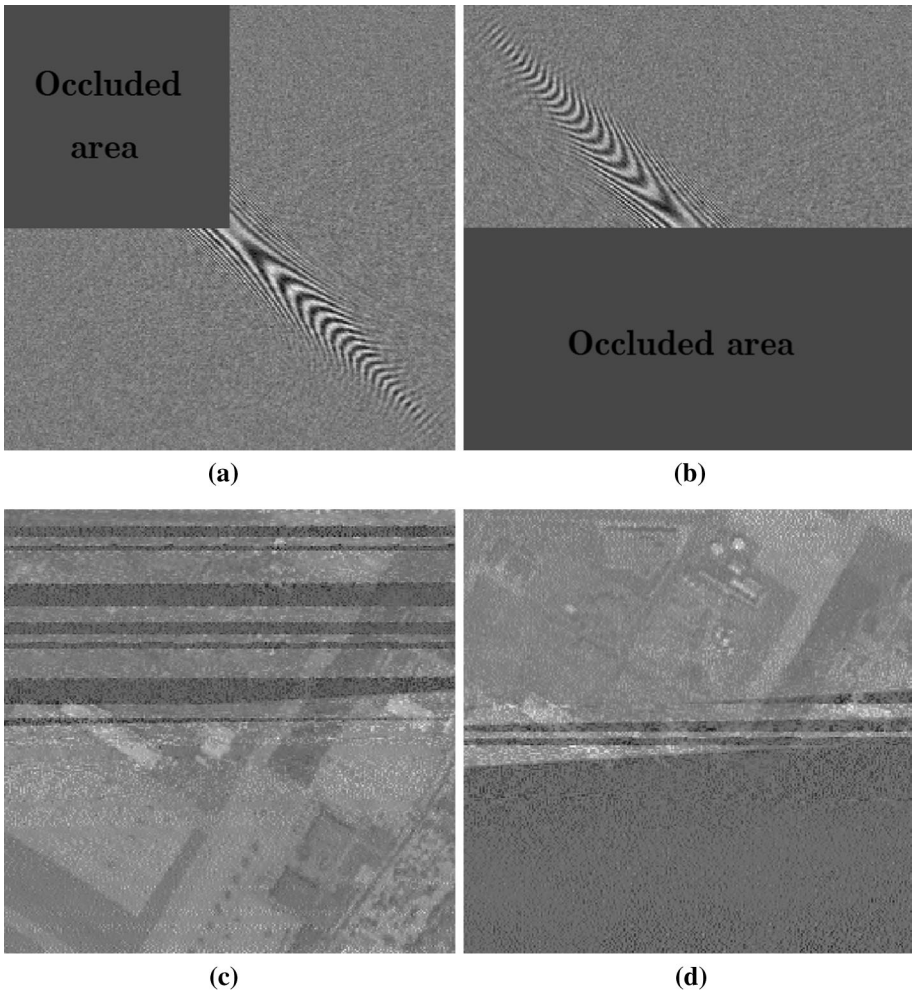


Fig. 10 The test of occlusion attack: **a** occluded image 1, **b** occluded image 2, **c** retrieved image 1 and **d** retrieved image 2

matching schemes named the spectral information divergence (SID) (Du et al. 2004) is introduced to quantify the difference of the spectrum curves. The value of SID represents the difference between two curves, while the bigger value of SID denotes that the higher similarity degree. The simulation results are list in the Table 1 and the results prove the validity and capability of the proposed spectrum encryption algorithm in protecting the secret spectrum information. The SID value between Original spectrum and decrypted spectrum is 2.4883×10^{31} indicating that our scheme can retrieve the spectrum perfectly. Besides, the encrypted/decrypted spectrum curves of the aircraft depicted in Fig. 9 reveal the strong difference between the spectra.

At the aspect of robustness analysis, the encrypted image is checked by occlusion attack and noise attack, respectively. Firstly, the occlusion attack is performed with the correct key (including main key and additional keys) from the 80th encrypted hyperspectral band occlude partly, which depicted in Fig. 10a, b. Actually, any other single encrypted band can be used to replace the 80th band in this attack experiment and the simulation will gives the same result. Here the values of the occluded pixels at the left-top corner and bottom area are set with 0 in numerical experiment and the corresponding decrypted results are represented in Fig. 10c, d, respectively. As shown in Fig. 10, the main information of the secret image can be recognized in vision.

Now the robustness against noise attack is checked by using the following model

$$I'(x,y) = I(x,y)\left[1 + p \cdot \sigma_{0,1}(x,y)\right] \tag{10}$$

where $I(x, y)$ and $I'(x, y)$ represent one of the encrypted single band before and after adding noise, respectively. The coefficient p is the noise intensity controller in this noise model, while the function $\sigma_{0,1}(x,y)$ denotes a random data with the mean value 0 and standard deviation 1. By using the images $I'(x, y)$ generated with various values of coefficient p, a PSNR curve is drawn in Fig. 11. In addition, two decrypted images are calculated and illustrated in Fig. 11 with the noise intensity $b = -0.121$ and $b = 0.525$, in which the outline of the secret image can be identified. In calculation, we use the 180 bands image from the intact encrypted hyperspectral image and corresponding value of the noise intensity controller p is set in the range of $[-0.99, 0.98]$ with the step length 0.011.

Finally, the known-plaintext attack (Peng et al. 2006a) and chosen-plaintext attack (Peng et al. 2006b) are considered to test the proposed encryption algorithm. Generally speaking, by using the phase retrieval algorithm (Du et al. 2004) under known/chosen plaintext-ciphertext pair, the secret keys can be retrieved in DRPE process. Therefore, the encryption algorithm is vulnerable if the unknown/chosen plaintext can be recovered by using the equivalent keys. In this experiment, the Gerchberg–Saxton phase retrieval technique is applied to access the encryption keys in Gyrator domain. Here, the iterative phase retrieval algorithm can be employed in the known plaintext attack and the impulse function can be used for the chosen plaintext attack.

Two test image ‘elaine’ and ‘lena’ having 128×128 pixels are first encrypted by our encryption algorithm described in Sect. 2 with the same parameters. The original and

Table 1 The SID value between the spectrum curves

Spectra	SID value
Original spectrum and encrypted spectrum	0.0072
Encrypted spectrum and decrypted spectrum	0.0072
Original spectrum and decrypted spectrum	2.4883×10^{31}

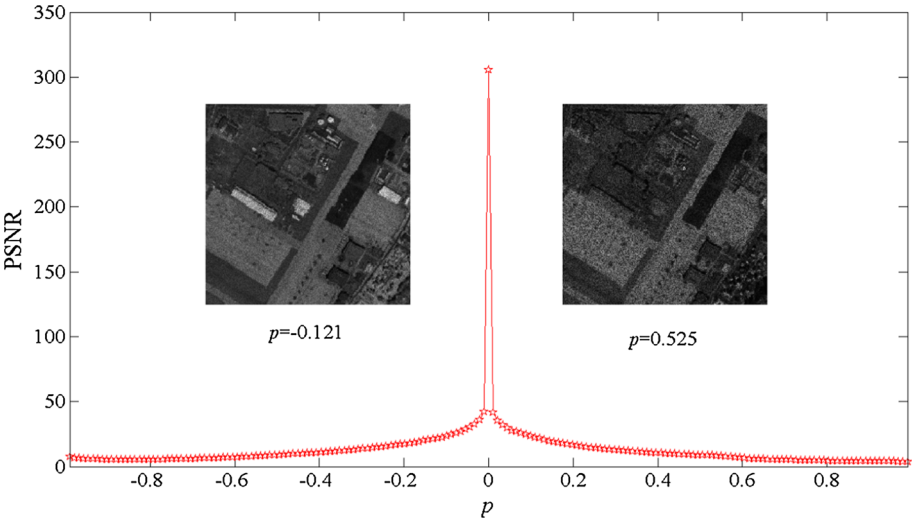


Fig. 11 The PSNR curve of noise attack including decrypted image obtained with b $= -0.121$, and decrypted image obtained with b $= 0.525$

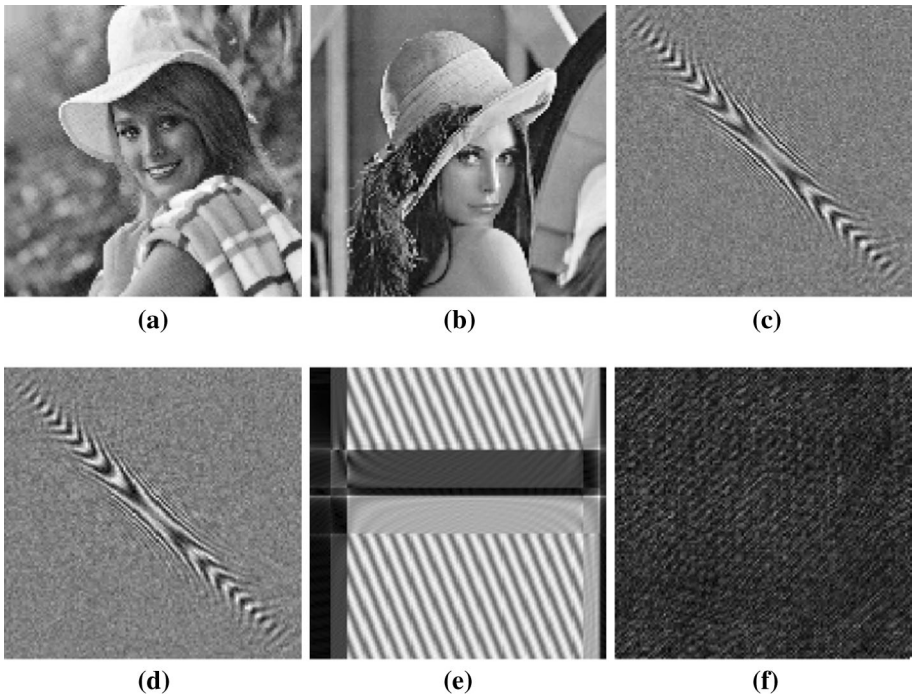


Fig. 12 Test of known plaintext attack and chosen plaintext attack: **a** original image 1, **b** original image 2, **c** the encrypted data of **a**, **d** the encrypted data of **b**, **e** the result of known plaintext attack and **f** the result of chosen plaintext attack

amplitude part of the encrypted images have been depicted in Fig. 12a–d, respectively. In calculation, we suppose that the original secret image 'elaine' and it encrypted image are received by the attacker, and then the encrypted data of 'lena' will be attacked in simulation. In the known plaintext attack, the phase retrieval algorithm is employed with 400 iterations. In addition, the impulse function is performed in the experiment of chosen plaintext attack. The experiment results from known plaintext attack and chosen plaintext attack are displayed in Fig. 12e, f. From the random pattern image, the proposed spectrum encryption algorithm is safe against known plaintext attack and chosen plaintext attack.

4 Conclusion

We have presented a kind of electro-optical spectrum encryption system for hyperspectral image by using random binary series and Baker mapping in associated FrFT and gyrator transform domain. Both the spatial information and spectrum information of the hyperspectral image can be encrypted simultaneously. The hyperspectral image is scrambled by Baker mapping and then divided into real part and imaginary part of the complex function expressing light field. Subsequently, the scrambled data is imported into FrFT and gyrator transform system with two random binary series. The random binary series are the main keys and some parameters generated during the encryption process will be regarded as the additional keys to enhancing the security of the encryption algorithms. The simulated results have demonstrated the validity, security and robustness of the spectrum encryption scheme.

Acknowledgments This work was supported by the National Natural Science Foundation of China (Grant 11104049), the Fundamental Research Funds for the Central Universities (No. HIT.BRETIII.201406), the Program for New Century Excellent Talents in University (NCET-12-0148), and the China Postdoctoral Science Foundation (2013M540278). The authors wish to thank the three reviewers for their useful comments and suggestions. The authors wish to thanks Mr. Chengwei Yang in Baicheng Ordnance Test Center of China for the valuable discussion. The authors are indebted to the anonymous reviewers for their valuable comments.

References

Abuturab, M.R.: Securing color information using Arnold transform in gyrator transform domain. Opt. Lasers Eng. **50**, 772–779 (2012)

Abuturab, M.R.: Noise-free recovery of color information using a joint-extended gyrator transform correlator. Opt. Lasers Eng. **51**, 230–239 (2013)

Alfalou, A., Brosseau, C.: Dual encryption scheme of images using polarized light. Opt. Lett. **35**, 2185–2187 (2010)

Chen, W., Chen, X., Sheppard, C.J.R.: Optical double-image cryptography based on diffractive imaging with a laterally-translated phase grating. Appl. Opt. **50**, 5750–5757 (2011)

Chen, H., Du, X., Liu, Z., Yang, C.: Color image encryption based on the affine transform and gyrator transform. Opt. Lasers Eng. **51**, 768–775 (2013)

Chen, H., Zhao, J., Liu, Z., Du, X.: Opto-digital spectrum encryption by using Baker mapping and gyrator transform. Opt. Lasers Eng. **66**, 285–293 (2015)

Du, Y., Chang, C.I., Ren, H., Chang, C., Jensen, J., D'Amico, F.: New hyperspectral discrimination measure for spectral characterization. Opt. Eng. **43**, 1777–1786 (2004)

Enayatifar, R., Abdullah, A.H., Isnin, I.F.: Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Opt. Lasers Eng. **56**, 83–93 (2014)

Fridrich, J.: Symmetric ciphers based on two-dimensional chaotic maps. Int. J. Bifurc. Chaos **8**, 1259–1284 (1998)

Gerchberg, R.W.: A practical algorithm for the determination of phase from image and diffraction plane pictures. Optik **35**, 227–246 (1972)
Jeffries, C., Perez, J.: Observation of a Pomeau–Manneville intermittent route to chaos in a nonlinear oscillator. Phys. Rev. A **26**, 2117 (1982)
Kumar, P., Joseph, J., Kingh, K.: Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator. Appl. Opt. **50**, 1805–1808 (2011)
Lang, J.: Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform and chaos permutation. Opt. Lasers Eng. **50**, 929–937 (2012)
Liu, Z., Liu, S.: Random fractional Fourier transform. Opt. Lett. **32**, 2088–2090 (2007)
Liu, Z., Li, Q., Dai, J., Zhao, X., Sun, X., Liu, S.: Image encryption based on random scrambling of the amplitude and phase in the frequency domain. Opt. Eng. **48**, 087005–087006 (2009a)
Liu, Z., Dai, J., Sun, X., Liu, S.: Triple image encryption scheme in fractional Fourier transform domains. Opt. Commun. **282**, 518–522 (2009b)
Liu, Z., Guo, Q., Xu, L., Ahmad, M.A., Liu, S.: Double image encryption by using iterative random binary encoding in gyrator domains. Opt. Express **18**, 12033–12043 (2010)
Liu, Z., Li, S., Liu, W., Liu, S.: Opto-digital image encryption by using Baker mapping and 1-D fractional Fourier transform. Opt. Lasers Eng. **51**, 224–229 (2013)
Lohmann, A.W.: Image rotation, Wigner rotation, and the fractional Fourier transform. J. Opt. Soc. Am. A **10**, 2181–2186 (1993)
Matoba, O., Javidi, B.: Encrypted optical memory system using three-dimensional keys in the Fresnel domain. Opt. Lett. **24**, 762–764 (1999)
Meng, X.F., Cai, L.Z., Xu, X.F., Yang, X.L., Shen, X.X., Dong, G.Y., Wang, Y.R.: Two-step phase shifting interferometry and its application in image encryption. Opt. Lett. **31**, 1414–1416 (2006)
Nakauchi, S., Nishino, K.: Yammashita. Selection of optimal combinations of band-pass filters for ice detection by hyperspectral imaging. Opt. Express **20**, 986–1000 (2012)
Ozaktas, H.M., Zalevsky, Z., Kutay, M.A.: The Fractional Fourier Transform with Applications in Optics and Signal Processing. Wiley, New York (2001)
Peng, X., Zhang, P., Wei, H., Yu, B.: Known-plaintext attack on optical encryption based on double random phase keys. Opt. Lett. **31**, 1044–1046 (2006a)
Peng, X., Wei, H., Zhang, P.: Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. Opt. Lett. **31**, 3261–3263 (2006b)
Refregier, P., Javidi, B.: Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. **20**, 767–769 (1995)
Rodrigo, J.U.A., Alieva, T., Calvo, M.Y.L.: Gyrator transform: properties and applications. Opt. Express **15**, 2190–2203 (2007a)
Rodrigo, J.U.A., Alieva, T., Calvo, M.Y.L.: Experimental implementation of the gyrator transform. J. Opt. Soc. Am. A **24**, 3135–3139 (2007b)
Situ, G., Zhang, J.: Double random-phase encoding in the Fresnel domain. Opt. Lett. **29**, 1584–1586 (2004)
Sui, L., Wang, Z., Sun, Q.: Double-image encryption using discrete fractional random transform and logistic maps. Opt. Lasers Eng. **56**, 1–12 (2014)
Tao, R., Xin, Y.: Double image encryption based on random phase encoding in the fractiona Fourier domain. Opt. Express **15**, 16067–16079 (2007)
Zhang, X., Zhu, G., Ma, S.: Remote-sensing imgae encryption in hybrid domains. Opt. Commun. **285**, 1736–1743 (2012)
Zhu, N., Wang, Y., Liu, J., Xie, J., Zhang, H.: Optical image encryption based on interference of polarized light. Opt. Express **17**, 13418–13424 (2009)