applied sciences

MDPI

Article

Optical Hyperspectral Image Cryptosystem Based on Affine Transform and Fractional Fourier Transform

Hang Chen [1,2,*], Zhengjun Liu [3], Camel Tanougast [2] and Jie Ding [4,*]

1 School of Electrical Engineering and Automation, Jiangxi University of Science and Technology, Ganzhou 341000, China
2 Laboratoire Conception Optimisation et Modélisation des Systèms, University de Lorraine, 57070 Metz, France; camel.tanougast@univ-lorraine.fr
3 Department of Automation Measurement and Control, Harbin Institute of Technology, Harbin 150001, China; zjliu@gmail.com
4 Department of information engineering, College of Technology of Hubei Engineering University, Xiaogan 432000, China
* Correspondence: hang.chen@univ-lorraine.fr (H.C.); dingjie@hbeu.cn (J.D.)

Received: 12 December 2018; Accepted: 16 January 2019; Published: 18 January 2019

Abstract: An encryption algorithm for hyperspectral data in fractional Fourier domain is designed. Firstly, the original hyperspectral image is separated into single bands and then each pair of bands are regarded as the real and imaginary part of a complex function by using an affine transform. Subsequently, the complex functions are encoded and transformed in fractional Fourier domain (FrFT). The parameters in affine transform and FrFT serve as the key of the encryption system. The proposed encryption scheme can not only protect the image information in spatial domains but also the spectrum information in spectral domains. Various experiments are given to demonstrate the validity and capability of the proposed encryption scheme.

Keywords: hyperspectral data; cryptography; optical transform

1. Introduction

With the rapid development of modern communication technology, information security has attracted more and more attention from researchers around the world. Since Refregier and Javidi proposed double random phase encoding (DRPE) in 1995 [1], a great number of concerns have been raised for this novel optical security technique. In the past decade, many encryption schemes based on different optical systems have been reported [2–8]. In particular, multiple-image encryption raises the attention of many researchers in the optical encryption area and many algorithms have been proposed [9–13]. Referring to [13], the cascaded interference structure and vector stochastic decomposition algorithm are introduced into a multiple-image encryption cryptosystem, in which the silhouette problem in the traditional two-beam interference cryptosystem can be removed successfully. Moreover, the cryptosystem for multispectral and hyperspectral image has also been studied in recent years [14–16]. In [15], by using the 3D Arnold transform, the hyperspectral image is extended from the spatial domain into the spectrum domain in an optical gyrator domain. The robustness of this cryptosystem is improved since secret data in the spectrum domain is impossible to retrieve from the spatial domain. Recently, an optical encryption algorithm for multiple spectral image was presented [17]. To enhance the security, the hyperspectral image was converted into binary data and improved Chirikov mapping was designed to scramble the intermediate data. The feasibility and robustness of the encryption algorithm was verified. However, the large calculation limited the encryption speed in practical implementation.

Hyperspectral data contains rich information in both the spatial and spectral domains. With the help of spectral information, researchers are able to identify and distinguish the material of the object in the data. This special characteristic is useful in many military and civilian applications involved in the detection of the target or activity, like military vehicles or vehicle tracks [18]. Besides, the ability of differentiating materials in recycling waste has made spectral information become a research focus in the field of laboratory measurements in medical diagnosis and chemical imaging [19]. In this paper, we propose an optical cryptosystem for hyperspectral data in fractional Fourier transform (FrFT) domain. Firstly, the original hyperspectral cube is divided into various independent bands before the encryption. Then, an affine transform is designed to scramble each pair of bands in the original data and then these two images become the real and imaginary part of a complex mask. Subsequently, the converted data are encoded and transformed into the optical FrFT transform. The parameters used in FrFT serve as the extra keys of the encryption. Finally, the discrete cosine transform (DCT) is considered to improve the security of the keys. One of the novelties of the proposed scheme is that we expand the ordinary image into hyperspectral image cryptosystem, which encrypts both the spatial and spectrum information synchronously. Moreover, compared to the encryption schemed presented in [17], the proposed method reduces the calculation and storage space of the encrypted data. Besides, the optical setup of FrFT is more simple and feasible compared to the gyrator transform.

The rest of the paper is summarized as follows. In Section 2, the intact cryptosystem is introduced in detail. Various numerical experiment results are given to test the validity of the scheme in Section 3. In the final section, the discussion and conclusions are given.

2. The Hyperspectral Encryption Scheme

2.1. Fractional Fourier Transform

Firstly, the FrFT will be introduced briefly. In the signal processing field, the FrFT can be regarded as time-frequency joint representation and it has been widely utilized in signal and image processing [20,21]. The mathematical definition of FrFT can be written as

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

where $F(u,v)$ and $g(x,y)$ represent the output and input function of FrFT, respectively. In the proposed algorithm, $g(x,y)$ denotes a single band of the hyperspectral data. The symbol α denotes the order in this transform and the definition of Equation (1) is effective when $\alpha \neq 0$. Besides, the function A_{α} is a constant phase factor decided by α.

2.2. Affine Transform

To complete the encryption, an affine transform is considered and utilized. The definition of the affine transform can be expressed as

$$F(\theta) = \begin{bmatrix} \psi(x,y)\cos[\theta(x,y)] & -\psi(x,y)\sin[\theta(x,y)] \\ \frac{\sin[\theta(x,y)]}{\psi(x,y)} & \frac{\cos[\theta(x,y)]}{\psi(x,y)} \end{bmatrix}, \tag{2}$$

where the symbol ψ and θ represent two random real number function satisfying uniform distribution. In fact, to enhance the security of the encryption system, the form of ψ can be defined by many nonlinear types. By simple deduction, the inverse matrix of $F(\theta)$ can be expressed as

$$F^{-1}(\theta) = \begin{bmatrix} \frac{\cos[\theta(x,y)]}{\psi(x,y)} & \psi(x,y)\sin[\theta(x,y)] \\ -\frac{\sin[\theta(x,y)]}{\psi(x,y)} & \psi(x,y)\cos[\theta(x,y)] \end{bmatrix}, \quad (3)$$

where the function $\theta(x,y)$ and $\psi(x,y)$ are two random real number matrices having the same size as the image, and satisfying uniform distribution. The affine transform described in Equations (2) and (3) will be employed in the encryption and decryption approaches to complete the cryptosystem.

2.3. Discrete Cosine Transform

DCT was first proposed by Nurzaman Ahmed in 1974 and soon expanded to the area of digital processing, especially in pattern recognition and encryption [22]. DCT is utilized to change the spatial distribution of the pixel value of an image in many cryptosystems. The mathematical definition of DCT with input sequence $x_0, x_1, \ldots, x_{n-1}$ or matrix having $n \times n$ pixels can be expressed as

$$f_m = \frac{1}{2}(x_0 + (-1)^m x_{n-1}) + \sum_{k=1}^{n-2} x_k \cos[\frac{\pi}{n-1}mk], \quad (4)$$

where the function f_m is the output sequence or matrix having the same size with input function, but the spatial distribution of pixel value is changed. The symbol "m" represents the serial number of the output function. To complete the cryptosystem, the DCT is considered and utilized in scrambling the parameters in FrFT generated in the encryption scheme.

2.4. The Encryption Scheme

The flowchart of the intact encryption algorithm is displayed in Figure 1. As shown in the Figure 1, the original hyperspectral image was separated into single bands and then each possible pair of bands was combined by employing the affine transform. Subsequently, the scrambled data were converted in FrFT domain. Finally, the parameters α in FrFT generated in the encryption scheme were calculated by DCT. The output result of DCT serves as the key of the cryptosystem. In the encryption approach, two bands are combined into one complex function and then transformed in the FrFT domains. Therefore, the final encrypted data obtained in the output plane has only 50% bands of the original hyperspectral image. For instance, the original hyperspectral image having 100 bands is encrypted, and the corresponding encrypted data has 50 bands. Accordingly, the storage space of the encrypted data is reduced.

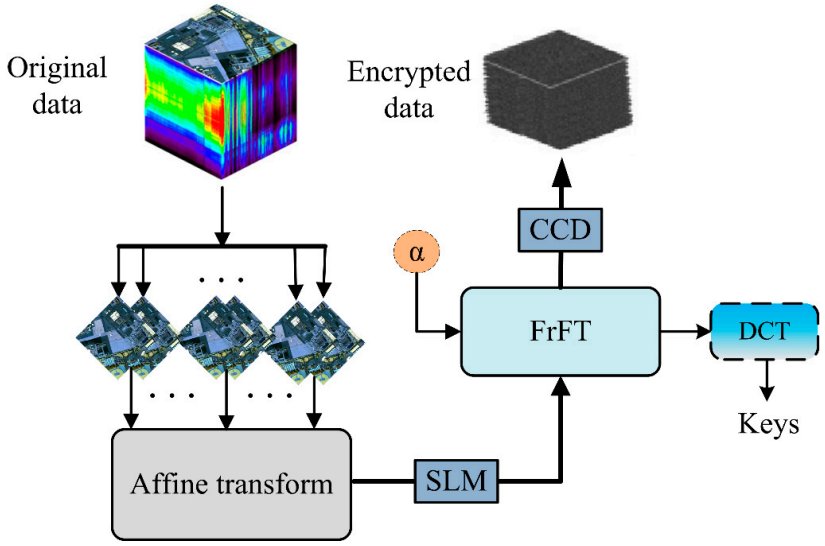
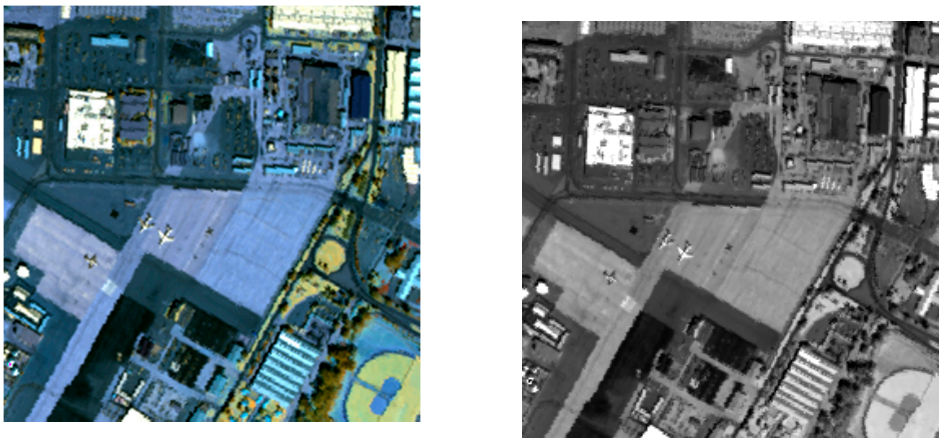


Figure 1. The flowchart of the encryption algorithm. SLM: spatial light module; CCD: charge-coupled device; DCT: discrete cosine transform; FrFT: fractional Fourier transform.

The encryption system can be carried out by an electro-optical hybrid setup depicted in Figure 1. The FrFT is achieved in an optical system and the affine transform and DCT are calculated in computer. Furthermore, the spatial light module (SLM) and charge-coupled device (CCD) are considered and utilized to accomplish data communication between the computer and optical system.

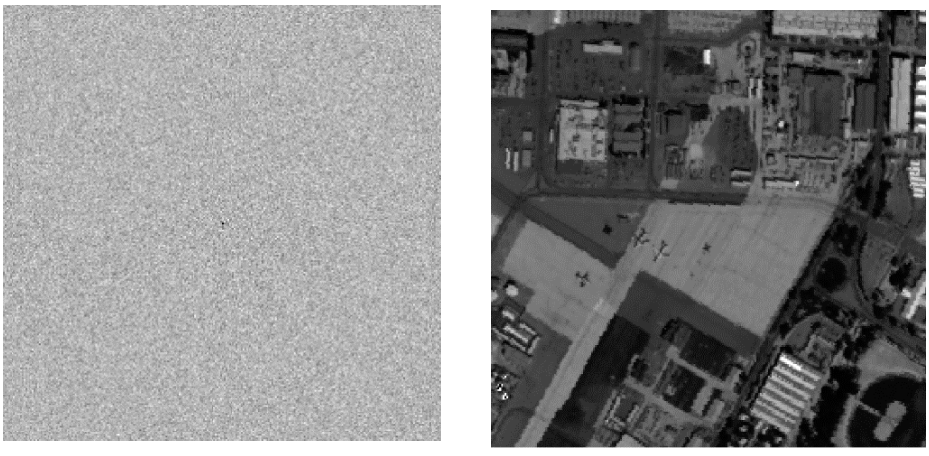
3. Numerical Simulations

In this section, various numerical simulations are given to validate the performance of the proposed hyperspectral image encryption scheme. As shown in Figure 2, one hyperspectral image named "Sandiego", having 189 bands, which was captured by AVIRIS (Jet Propulsion Laboratory, USA), was used in the following experiment. In fact, any other hyperspectral image or multiband data can be used to process the presented cryptosystem. To simplify the calculation, we selected the first 100 bands from the 189 bands in the original hyperspectral image. Therefore, the dataset was used in the following experiments having the size $256 \times 256 \times 100$. The random function ψ and θ in affine transform are the random functions having 256×256 pixels in the range of $[0, 1]$ and $[0, 2\pi]$, respectively. To simplify the encryption process, the parameter of FrFT was set to 0.5 in our encryption scheme. In fact, the parameters can be different for each band to enhance the security. The hardware parameters of the computer used in the simulation experiment are Core 2, CPU 2.1GHz, and 2048 Mb memory (T430, Thinkpad Lenove, Beijing, China). By using the conditions described above, the encryption results are displayed in Figure 3. As shown in Figure 3, the encrypted result is a noise-like image.



(**a**) (**b**)

Figure 2. The (**a**) RGB color composite and (**b**) 88th band data of the original hyperspectral image.



(**a**) (**b**)

Figure 3. Experimental results: (**a**) the encrypted image and (**b**) decrypted image.

The peak signal-to-noise ratio (PSNR) is considered and introduced to weight the discrepancy between the decrypted and original data. The mathematical definition of PSNR is expressed as follows:

$$PSNR(I_d, I_0) = 10\log_{10}\frac{255^2 M \times N}{\sum_{\forall x,y}[I_d(x,y) - I_0(x,y)]^2}(\text{dB}), \quad (5)$$

where the symbol I_d and I_0 represent the decrypted data and original data, respectively. In addition, the sizes of the data can be represented by M and N. Here, the value of M and N are fixed at 256.

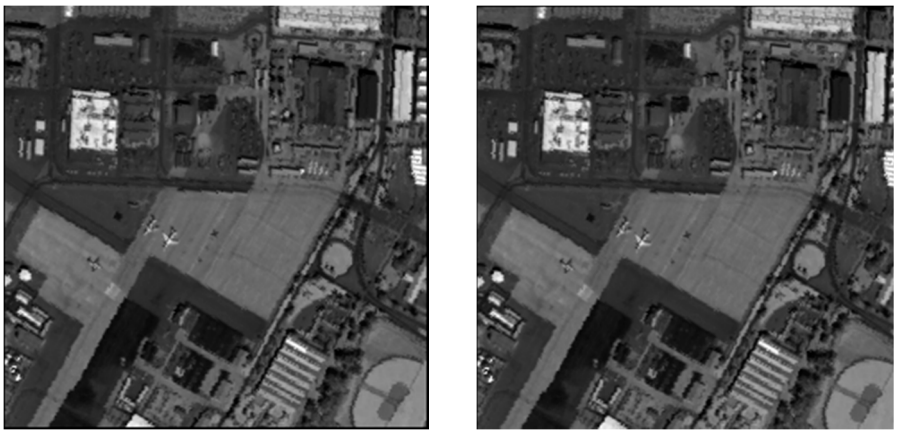
3.1. Validation of the Encryption Scheme

As mentioned above, the encryption data of this encryption has 50 single bands. Therefore, it is difficult to estimate the difference between two different size hyperspectral images. To show the results convincingly, a random band extracted from the original hyperspectral image is used to calculate the PSNR with each band of the ciphertext. In this experiment, the 27th band of the original image is chosen, and the PSNR values are listed in Table 1.

Table 1. The peak signal-to-noise ratio (PSNR) values between decrypted image and original image.

Original Data	Encrypted Data	PSNR Value	Original Data	Encrypted Data	PSNR Value
27th band	1st band	1.7448	27th band	26th band	1.6473
27th band	2nd band	1.7585	27th band	27th band	1.6227
27th band	3rd band	1.8941	27th band	28th band	1.6121
27th band	4th band	1.9966	27th band	29th band	1.5297
27th band	5th band	2.0217	27th band	30th band	1.5440
27th band	6th band	2.0593	27th band	31st band	1.5559
27th band	7th band	2.1267	27th band	32nd band	1.5143
27th band	8th band	2.1079	27th band	33rd band	1.4688
27th band	9th band	2.1345	27th band	34th band	1.5078
27th band	10th band	2.1461	27th band	35th band	1.5293
27th band	11th band	2.1677	27th band	36th band	1.4922
27th band	12th band	2.1658	27th band	37th band	1.5312
27th band	13th band	2.1601	27th band	38th band	1.6441
27th band	14th band	2.1570	27th band	39th band	1.7525
27th band	15th band	2.1597	27th band	40th band	1.9264
27th band	16th band	2.1613	27th band	41st band	2.1018
27th band	17th band	2.1546	27th band	42nd band	2.2063
27th band	18th band	2.1134	27th band	43rd band	2.2255
27th band	19th band	2.0445	27th band	44th band	2.2755
27th band	20th band	2.0357	27th band	45th band	2.3308
27th band	21st band	1.9524	27th band	46th band	2.4062
27th band	22nd band	1.9040	27th band	47th band	1.5091
27th band	23rd band	1.8623	27th band	48th band	1.5546
27th band	24th band	1.7898	27th band	49th band	1.5592
27th band	25th band	1.7250	27th band	50th band	1.6136

As we can see from Table 1, the PSNR values between the decrypted data and original date range from 1.4699 to 2.4062, which indicate that the images are very different. In other words, the proposed cryptosystem can protect the original information successfully. In addition, to examine the PSNR values between the original band and correct decrypted band, another experiment is done. In the decryption approach, all the keys are given and the 27th band is decrypted completely. The PSNR value between the 27th image and the retrieved 27th image is 295.7293, which indicates that the proposed algorithm recovered the original image completely. The original 27th band and decrypted 27th are displaced in Figure 4.



(a) **(b)**

Figure 4. The (**a**) original 27th band and (**b**) the decrypted 27th band. The peak signal-to-noise ratio (PSNR) value of (a) and (b) is 295.7293.

3.2. The Sensitivity Test of the Extra key α

The parameter α in FrFT can be severed as an extra key for this cryptosystem. To test the sensitivity of the parameter α, an experiment was designed as follows. In the encryption approach, α is set as 0.5. In the decryption process, suppose that the main key is known, the additional key α is changed around 0.5, and the corresponding PSNR curve is illustrated in Figure 5. In calculation, the sampling step length of α is 0.01 between 0.25 and 0.75. As we can see from Figure 5, the 24th band and 26th band of the decrypted image are the noise pattern; even the values of α are so close to the correct value 0.5. In the decryption result, only the 25th band image is decrypted successful. The experimental result indicates that the parameter α is sensitive and can protect the secret hyperspectral image well.

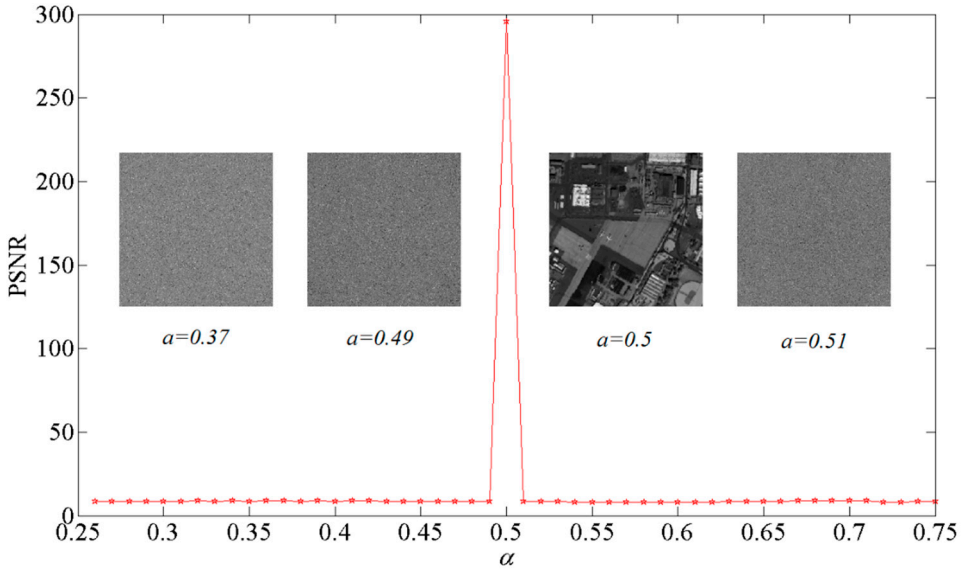


Figure 5. The PSNR curve calculated by different values of parameter α.

3.3. Occlusion Attack and Noise Attack Experiments

The occlusion attack and noise attack are considered and utilized for the robustness analysis of the proposed cryptosystem. To simplify the calculation, the 27th encrypted band is considered and utilized in occlusion and noise attack, analysis. In fact, the other encrypted band can also obtain the same result. In the occlusion attack experiment, the decryption approach is employed by using the

correct key from the partly occluded 27th band image, which is displayed in Figure 6a. Note that the occluded pixels are substituted with 0 in the experiment, and the corresponding recovered result is presented in Figure 6b. Apparently, the outline information of the secret image is recognizable.

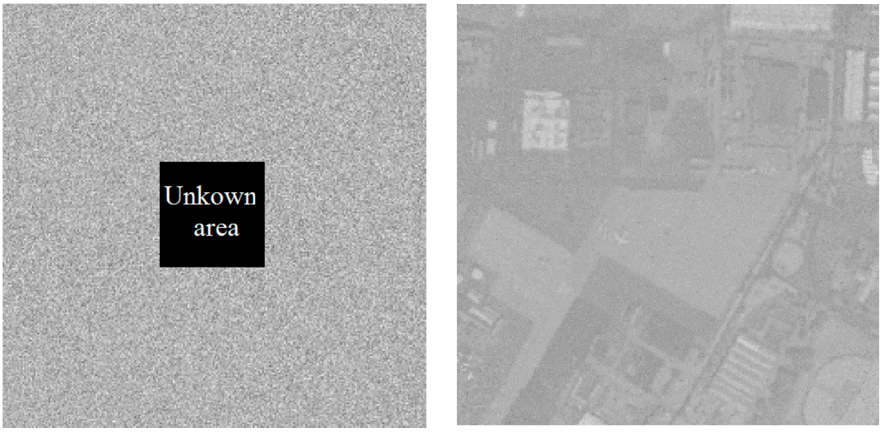


Figure 6. The experiment result of occlusion attack: (**a**) the occluded 27th band encrypted image and (**b**) decrypted image.

To complete the noise attack experiment, a noise model is designed as follows:

$$I'(x,y) = I(x,y)[1+p \cdot \sigma_{0,1}(x,y)], \tag{6}$$

where the function $I(x,y)$ is the 27th band of the encrypted data and $I'(x,y)$ denotes $I(x,y)$ with noise. The function $\sigma_{0,1}(x,y)$ represents the random data-satisfied uniform distribution. Besides, the parameter p is the coefficient representing the noise intensity. By using this noise model, the noise data can be added into the secret encrypted 27th band image with different intensity noise. The corresponding PSNR curve is depicted in Figure 7 by decrypting the data $I'(x,y)$ with various values of p. In addition, the two decrypted images drawn in Figure 7 are calculated with the noise intensity p = 0.4 and p = 0.9, respectively. The main information of the 27th band image can be recognized.

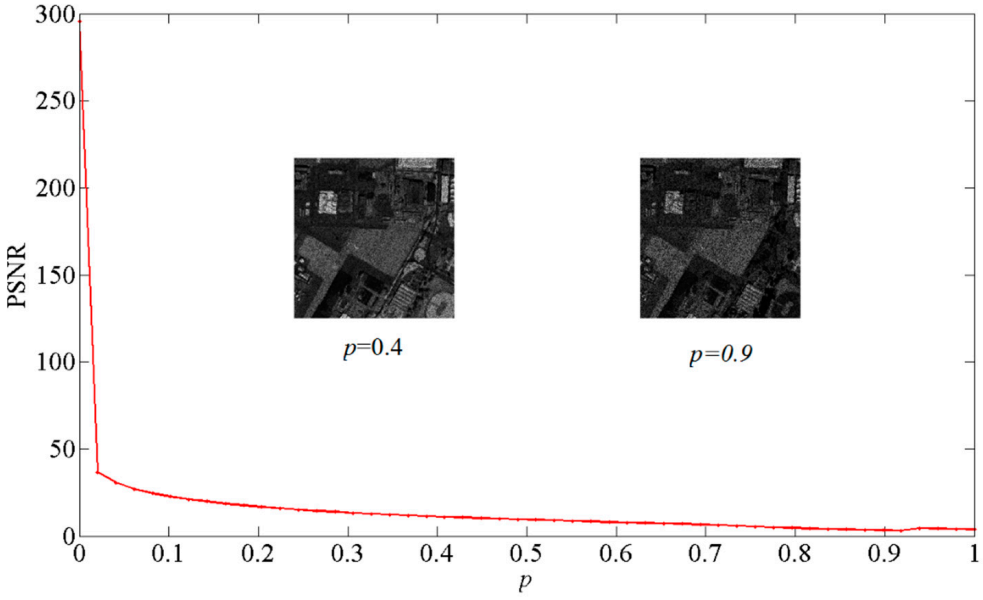


Figure 7. The PSNR curve of noise attack including the decrypted 27th band with p = 0.4 and p = 0.9.

3.4. Known Plaintext Attack and Chosen Plaintext Attack Experiments

Furthermore, the known plaintext attack and chosen plaintext attack [23,24] are also considered to demonstrate the robustness of the proposed algorithm. Firstly, an encryption model is designed to complete the attack experiment as follows:

$$E(u,v) = \wp^{\alpha}\{I(x,y)\exp[i\cdot\phi_1(x,y)]\}\exp[i\cdot\phi_2(x',y')], \tag{7}$$

where the phase functions $\phi_1(x,y)$ and $\phi_2(x',y')$ represent two random phase masks. The output function $E(u,v)$ denotes the encrypted image by using the proposed cryptosystem. In the attack experiments, the phase retrieval algorithm is used in known plaintext attack while the impulse function is employed in chosen plaintext attack.

Only the single band encryption process of the intact encryption scheme is tested because of the huge amount of calculations in the attack experiment. Two test images, "Peppers" and "Cameraman", having 128 × 128 pixels, are considered in the plaintext attack experiment. Firstly, two test images and their encrypted versions are shown in Figure 8a–e, respectively. Before the attack operation, assume that the original data "Peppers" and its encrypted pattern are obtained by the illegal user. Subsequently, the known plaintext attack and chosen plaintext attack are employed successively for the decrypted data of "Cameraman". The attack results are illustrated in Figure 8c–f, which are random patterns.

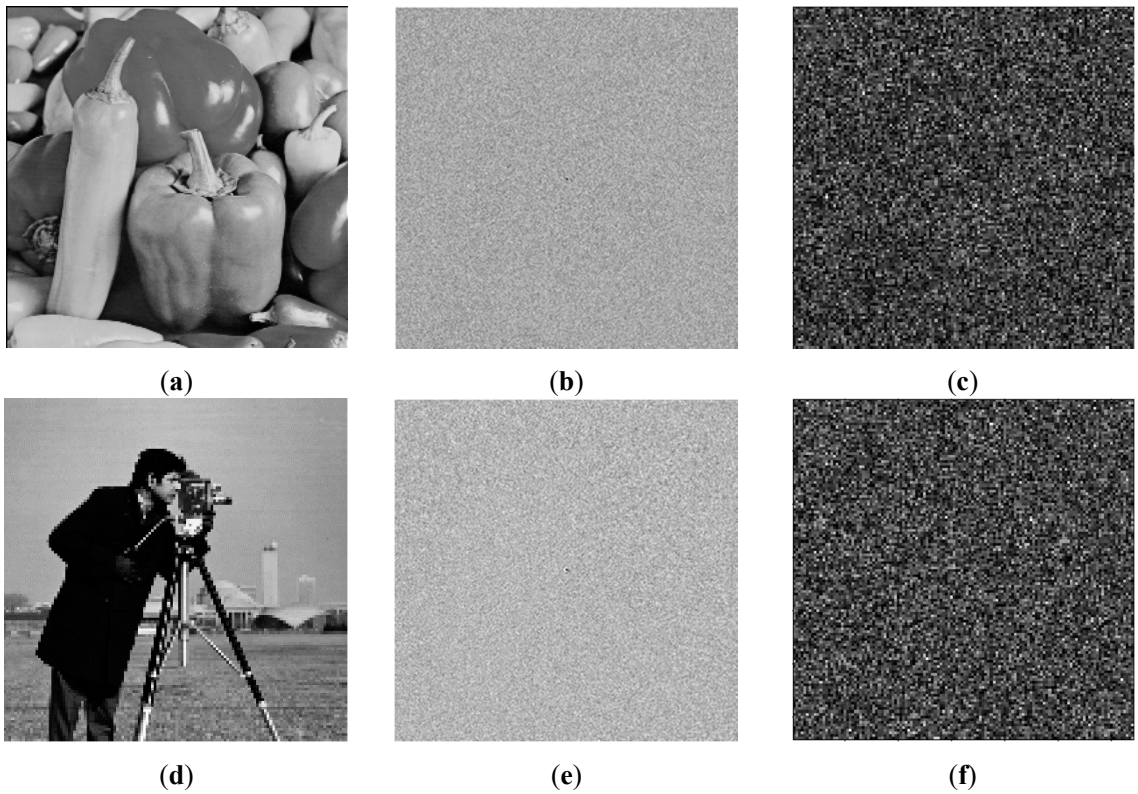


Figure 8. The experiment result: (**a**) test image, (**b**) the encrypted version of (a), (**c**) attack result, (**d**) test image, (**e**) the encrypted version of (d) and (**f**) attack result.

3.5. Test for Validity of Spectrum Information Encryption

Finally, the performance of protecting the spectrum information is tested. The spectrum curves of the pixel (100, 100) before and after the encryption process are illustrated in Figure 9. As we can see from Figure 9, it is apparent that the encryption spectrum curves greatly differ from the original spectrum. Note that the original and decrypted spectrum are drawn in the same color and the two spectrum curves coincide to form one curve, which indicates that the secret spectrum information is

retrieved completely. The result shown in Figure 9 demonstrates the performance of the cryptosystem in protecting the spectrum information. Here, the encrypted spectrum curves are separated into real part and imagery part because the encryption data of the proposed algorithm is a complex function. Therefore, the proposed encryption scheme can not only protect the image information in spatial domains, but also the spectrum information in spectral domains.

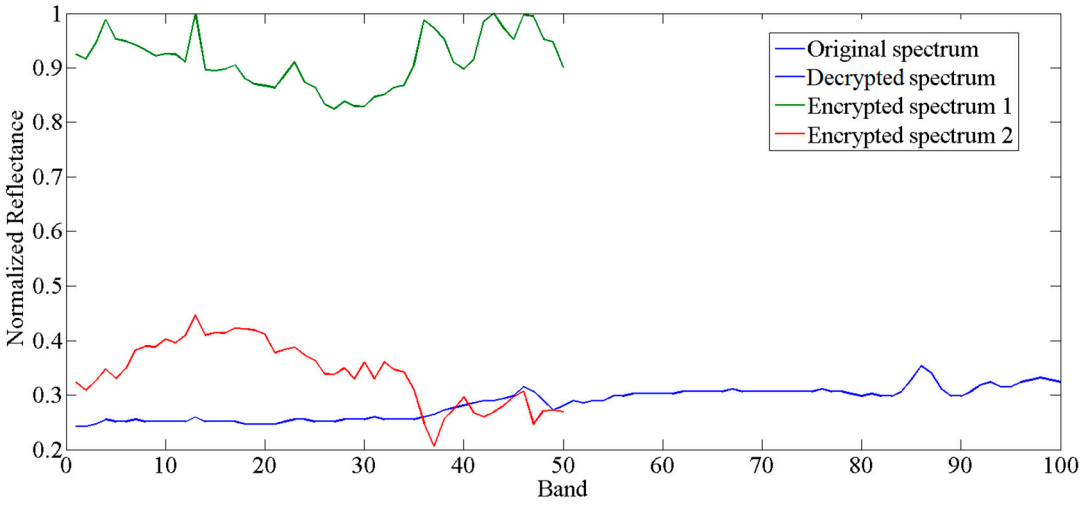


Figure 9. The spectrum curves of the secret spectrum, decrypted spectrum, and encrypted spectrum.

4. Conclusions

We have presented a cryptosystem for hyperspectral image in fractional Fourier transform domain, which can protect the spatial information and spectrum information simultaneously. An affine transform is used in the encryption approach to enhance the security. After performing DCT, the parameters generated in fractional Fourier transform can be regarded as keys of this encryption scheme. Various numerical simulations demonstrate the validity, security, and robustness of the proposed spectrum cryptosystem.

Author Contributions: H.C., Z.L. and C.T. conceived and designed the experiments; H.C. performed the experiments; H.C. and J.D. analyzed the data; H.C. wrote the paper.

Acknowledgments: This work was supported by the National Natural Science Foundation of China (Grant 61575053), the Fundamental Research Funds for the Central Universities (No.HIT.BRETIII.201406), research project of the department of education in Hubei province (B2017501), CNRS SpectroLive project: Multimodal Spectro-Imaging for in vivo (skin) tissue characterization. The authors are indebted for the three anonymous reviewers for their helpful comments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Refregier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769. [CrossRef] [PubMed]
2. Alfalou, A.; Brosseau, C.; Abdallah, N. Simultaneous fusion, compression, and encryption of multiple images. *Opt. Express* **2011**, *19*, 24023–24029. [CrossRef]
3. Liu, Z.; Li, S.; Liu, W.; Wang, Y.; Liu, S. Image encryption algorithm by using fractional Fourier transform and scrambling operation based on double random phase encoding. *Opt. Lasers Eng.* **2013**, *51*, 8–14. [CrossRef]
4. Guo, Q.; Guo, J.; Liu, Z.; Liu, S. An adaptive watermarking using fractal dimension based on random fractional Fourier transform. *Opt. Laser Technol.* **2012**, *44*, 124–129. [CrossRef]
5. Liu, Z.; Zhang, Y.; Liu, W.; Meng, F.; Wu, Q.; Liu, S. Optical color image hiding scheme based on chaotic mapping and Hartley transform. *Opt. Laser Eng.* **2013**, *51*, 967–972. [CrossRef]

6. Chen, H.; Du, X.; Liu, Z.; Yang, C. Color image encryption based on the affine transform and gyrator transform. *Opt. Lasers Eng.* **2013**, *51*, 768–775. [CrossRef]
7. Kumar, P.; Joseph, J.; Singh, 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.* **2011**, *50*, 1805–1811. [CrossRef]
8. Abuturab, M.R. Securing color information using Arnold transform in gyrator transform domain. *Opt. Lasers Eng.* **2012**, *50*, 772–779. [CrossRef]
9. Millán, M.S.; Pérez-Cabré, E.; Javidi, B. Multifactor authentication reinforces optical security. *Opt. Lett.* **2006**, *31*, 721–723. [CrossRef]
10. Liu, Z.; Chen, H.; Liu, T.; Li, P.; Dai, J.; Sun, X.; Liu, S. Double-image encryption based on the affine transform and the gyrator transform. *J. Opt.* **2010**, *12*, 035407. [CrossRef]
11. Xiong, Y.; Quan, C.; Tay, C.J. Multiple image encryption scheme based on pixel exchange operation and vector decomposition. *Opt. Lasers Eng.* **2018**, *101*, 113–121. [CrossRef]
12. Zhou, N.; Jiang, H.; Gong, L.; Xie, X. Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging. *Opt. Lasers Eng.* **2018**, *110*, 72–79. [CrossRef]
13. Zhang, X.; Meng, X.; Wang, Y.; Yang, X.; Yin, Y.; Li, X. Hierarchical multiple-image encryption based on the cascaded interference structure and vector stochastic decomposition algorithm. *Opt. Lasers Eng.* **2018**, *107*, 258–264. [CrossRef]
14. Chen, H.; Zhao, J.; Liu, Z.; Du, X. Opto-digital spectrum encryption by using Baker mapping and gyrator transform. *Opt. Lasers Eng.* **2015**, *66*, 285–293. [CrossRef]
15. Chen, H.; Du, X.; Liu, Z. Optical hyperspectral data encryption in spectrum domain by using 3D Arnold and gyrator transforms. *Spectrosc. Lett.* **2016**, *49*, 103–107. [CrossRef]
16. Beşdok, E. Hiding information in multispectral spatial images. *AEU-Int. J. Electron. Commun.* **2005**, *59*, 15–24. [CrossRef]
17. Chen, H.; Tanougast, C.; Liu, Z.; Blondel, W.; Hao, B. Optical hyperspectral image encryption based on improved Chirikov mapping and gyrator transform. *Opt. Lasers Eng.* **2018**, *107*, 62–70. [CrossRef]
18. Manolakis, D.; Marden, D.; Shaw, G.A. Hyperspectral image processing for automatic target detection applications. *Linc. Lab. J.* **2003**, *14*, 79–116.
19. Chaddad, A.; Desrosiers, C.; Bouridane, A. Multi texture analysis of colorectal cancer continuum using multispectral imagery. *PLoS ONE* **2016**, *11*, e0149893. [CrossRef]
20. Lohmann, A.W. Image rotation, Wigner rotation, and the fractional Fourier transform. *J. Opt. Soc. Am. A* **1993**, *10*, 2181–2186. [CrossRef]
21. Ozaktas, H.M.; Zalevsky, Z.; Kutay, M.A. *The Fractional Fourier Transform with Applications in Optics and Signal Processing*; Wiley: Chichester, NY, USA, 2001.
22. Ahmed, N.; Natarajan, T.; Rao, K.R. Discrete cosine transform. *IEEE Trans. Comput.* **1974**, *100*, 90–93. [CrossRef]
23. Peng, X.; Zhang, P.; Wei, H.; Yu, B. Known-plaintext attack on optical encryption based on double random phase keys. *Opt. Lett.* **2006**, *31*, 1044–1046. [CrossRef] [PubMed]
24. Peng, X.; Wei, H.; Zhang, P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. *Opt. Lett.* **2006**, *31*, 3261–3263. [CrossRef] [PubMed]