Hybrid Domain Encryption Method of Hyperspectral Remote Sensing Image

Wenhao Geng[1], Jing Zhang[1(✉)], Lu Chen[1], Jiafeng Li[1], and Li Zhuo[1,2]

[1] Signal and Information Processing Laboratory, Beijing University of Technology, Beijing, China
{gengwh, chenlu}@emails.bjut.edu.cn, {zhj, lijiafeng, zhuoli}@bjut.edu.cn
[2] Collaborative Innovation Center of Electric Vehicles in Beijing, Beijing, China

Abstract. With the rapid development of remote sensing technology, hyperspectral remote sensing image as foundation data containing abundant sensitive information has been widely applied in many fields, such as agriculture, resources, ocean, city, and environment, etc. A hybrid domain encryption method is proposed for securely transmitting and storing hyperspectral remote sensing images. Considering the spatial and spectral characteristics, the hyperspectral image is encrypted in hybrid domain (spatial and spectral). Spatial domain encryption is done by using the composite chaos sequences. Then, the spectral sequence is scrambled by the cipher sequence for protecting the spectral feature of the hyperspectral image. Finally, the spectral and spatial information is mixed by a one-to-one mapping. Experimental results on NASA datasets show that our method can effectively protect both spectral and spatial feature of hyperspectral image compared with the other methods.

Keywords: Remote sensing · Hyperspectral image · Encryption
Hybrid domain · Recombination chaos sequences

1 Introduction

In recent years, hyperspectral imaging has been an active area of remote sensing research and development, which can image the same ground object with several tens to hundreds of spectral bands from ultraviolet to the microwave range [1–3]. Because hyperspectral remote sensing image as foundation data containing abundant sensitive information has been widely applied in many fields, such as agriculture, resources, ocean, city, and environment, etc., it is very necessary to ensure to securely transmit and store hyperspectral remote sensing images (hyperspectral image for short).

Image encryption is a technique to prevent the information leakage of the image by using the characteristics of digital images [4]. Researchers have proposed hundreds of encryption algorithms for common image [5–7]. It has been proved that image encryption based on chaos theory can achieve better performance [8, 9], which uses the chaotic characteristic to transform the pixel values. But with the development of image encryption technology, the encryption effect of chaotic system based on a single

B. Zeng et al. (Eds.): PCM 2017, LNCS 10736, pp. 890–899, 2018.
https://doi.org/10.1007/978-3-319-77383-4_87

chaotic sequence shows weaker obviously. Therefore, composite chaos containing two chaos sequences become a new solution to improve the security of image encryption.

Nowadays, remote sensing image encryption has attracted more attention due to the abundant information of surface features, but there is little research about hyperspectral images. Huang et al. [10] proposed an encryption scheme using chaotic system to build up the compressed sensing framework. A two-dimensional generalized Arnold map is adopted to protect the remote sensing image. Yin et al. [11] proposed to use secured TD-ERCS chaotic model to shuffle important EZW coefficients. Muhaya et al. [12] proposed a secure satellite image encryption technique based on chaotic and Advanced Encryption Standard (AES) techniques. These methods can protect the spatial information of the remote sensing images effectively, but ignore the important spectral information of the hyperspectral image. Considering high dimensionality and spectral characteristics of hyperspectral image, traditional encryption methods for common images [13–15] cannot be directly utilized to protect both spectral and spatial information of hyperspectral image.

In this paper, a hybrid domain encryption method of hyperspectral remote sensing image is proposed by combining spatial domain encryption and spectral domain encryption in order to ensure the security of hyperspectral image. Considering the spatial and spectral characteristics, the hyperspectral image is encrypted in hybrid domain (spatial and spectral). Spatial domain encryption is done by using the composite chaos sequences. Then, the spectral sequence is scrambled by the cipher sequence in spectral domain. Finally, the spectral and spatial information is mixed by a one-to-one mapping.

The remainder of this paper is organized as follows: Sect. 2 states the hybrid domain encryption method in detail, which includes spatial domain encryption, spectral domain encryption and hybrid domain encryption. Experimental results are analyzed in Sect. 3 and the conclusions are drawn in Sect. 4.

2 Hybrid Domain Encryption

As we know, hyperspectral image contains both spectral and spatial features. Traditional image encryption method only protects the spatial domain information, which is not security enough for hyperspectral image once the spectral information leakage. Therefore, we propose to encrypt the hyperspectral image in hybrid domain. The overall architecture is shown in Fig. 1. Firstly, we use composite chaos to encrypt the hyperspectral image in spatial domain. Then the spectral bands are scrambled by the cipher sequence. Finally, the spatial and spectral feature is scrambled by domain mixing encryption.

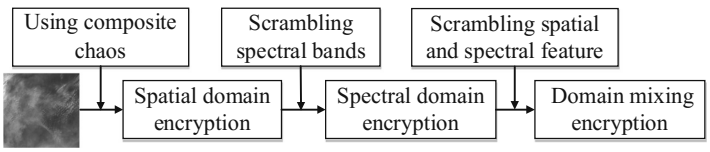

Fig. 1. The process of proposed encryption method.

2.1 Encryption in Spatial Domain

Generally, hyperspectral image encryption in spatial domain is accomplished by changing pixels' values or scrambling the position of pixels. As above mentioned, the security of single chaos sequence is not appropriate enough. Therefore, composite chaos is used in hyperspectral image encryption in spatial domain.

In this paper, the composite chaos is used to obtain the secret key. The composite chaos is composed of chaotic sequence generated by Logistic Map and Chebyshev Map.

Logistic Map: The Logistic Map is described as follows:

$$x_{n+1} = \mu x_n(1 - x_n) \tag{1}$$

where $\mu \in (0, 4]$, $x_i \in (0, 1)$. When $\mu \in (3.5699456\ldots, 4]$, the Logistic Map works in chaos state. The sequence $\{x_i, i = 1, 2, 3,\ldots\}$, generated by the initial value x_0, is non-periodic, non-convergence and sensitive to the initial value.

Chebyshev Map: The Chebyshev Map is described as follows:

$$x_{n+1} = \cos(k \arccos(x_n)) \tag{2}$$

where k is nonlinear strength coefficient of the system. When $k \geq 2$, the Chebyshev Map works in chaos state. The chaos sequence $\{x_i, i = 1, 2, 3,\ldots\}$ is generated by the initial value x_0.

Let $\mathbf{L}(l_1, l_2, l_3,\ldots)$ be the sequence of Logistic Map and $\mathbf{C}(c_1, c_2, c_3,\ldots)$ be the sequence of Chebyshev Map. The composite chaos is generated by:

$$\mathbf{R} = \mathbf{L} \cdot \mathbf{C} \tag{3}$$

where $\mathbf{R}(r_1, r_2, r_3,\ldots)$ is the composite chaos and $r_i = l_i \times c_i$.

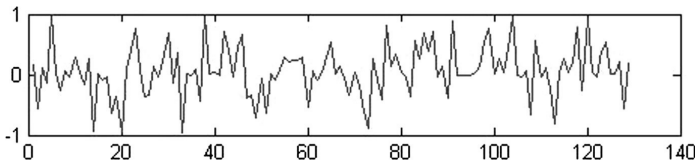

Fig. 2. The composite chaos.

Figure 2 shows the composite chaos generated by two chaos sequences. As can be seen in Fig. 2, the value range of the composite chaos is [−1, 1]. To compute with pixel values (all integers), the composite chaos need to be transformed to integers, which can be expressed as:

$$\mathbf{Z} = \lfloor \mathbf{R} \times n \rfloor \tag{4}$$

where $\mathbf{Z}(z_1, z_2, z_3,\ldots)$ is the integers sequence, $\mathbf{R}$ is the composite chaos, n is a integer which is related to the image pixels values and $\lfloor\ \rfloor$ is rounding down process. Equation (4) can transform the value to integer at the same value range with pixel values. Then we use sequence $\mathbf{Z}(z_1, z_2, z_3,\ldots)$ to encrypt the hyperspectral remote sensing image in spatial domain. Specific procedures are as follows:

Step 1: The parameter μ of Logistic Map, the parameter k of Chebyshev Map and the initial values l_1 and c_1 are determined first.
Step 2: To improve the key sensitivity, we introduce the auxiliary key Ak computed by the input images, which is defined as:

$$Ak = \frac{\mathrm{mod}(\sum I_i, 256)}{256} \tag{5}$$

where Ak is the auxiliary key and I_i is the pixel values of the input image. Then the new initial values l_1' and c_1' is obtained by multiplying l_1 and c_1 by Ak. Due to Ak is computed by pixel values, the initial values will be changed with different input images, which can improve the sensitivity of the initial values.
Step 3: The sequences of Logistic Map and Chebyshev Map are generated by the new initial values l_1' and c_1' according to Eqs. 1 and 2. Here we introduce an integer S to change the range of the chaos sequences. Let n be the number of the pixels of the input image. The chaos sequences are generated by iterating $n + S - 1$ times. Then the first S elements are dropped and the rest sequences can generate the final secret sequence $\mathbf{Z}(z_1, z_2, z_3,\ldots)$ according to Eq. 3 to Eq. 5.
Step 4: Due to $\mathbf{Z}(z_1, z_2, z_3,\ldots)$ is a integer sequence, the pixels' values of input image are computed by:

$$x_i' = x_i \wedge z_i \tag{6}$$

where $\wedge$ is Binary XOR operation, x_i is the pixel values of original image, z_i belongs to $\mathbf{Z}(z_1, z_2, z_3,\ldots)$. Then sequence $\mathbf{Z}'(z_1, z_2, z_3,\ldots z_{M+N})$ is gained from $\mathbf{Z}(z_1, z_2, z_3,\ldots)$ which is used to scramble the position of the pixels, which is defined as:

$$X = \begin{cases} m_i \rightarrow z_i,\ i \in [1, M] \\ n_i \downarrow z_i,\ i \in [M+1, M+N] \end{cases} \tag{7}$$

where $\rightarrow$ and $\downarrow$ are the cyclic shift operation of right orientation and down orientation, m_i and n_i are the column vector and row vector of the image, $z_i \in \mathbf{Z}'(z_1, z_2, z_3,\ldots\ z_{M+N})$.

2.2 Encryption in Spectral Domain

Hyperspectral images are acquired simultaneously in dozens of narrow, adjacent wave-length bands. A continuous spectrum can be extracted from endmembers, which can be used to identify surface materials [1]. Therefore, hyperspectral images contain much sensitive information including minerals, city construction, military base and so on. While traditional encryption methods for remote sensing images ignore to further

protect the spectral information which increase the risk of spectral information leakage. A hyperspectral image is made up of hundreds of 2D images which are ranked by the spectrum order. Hence, the spectral information can be protected by changing the spectral bands order. In this section, we propose to scramble the spectral bands order of the hyperspectral image with secret key. The procedures can be summarized as follows:

Step 1: The secret key is obtained by the final secret sequence $\mathbf{Z}(z_1, z_2, z_3,\ldots)$, which is computed in Sect. 2.1.
Step 2: Let the hyperspectral image includes n spectral bands. Then n values are selected from $\mathbf{Z}(z_1, z_2, z_3,\ldots)$, which is $\mathbf{Z}''(z_1, z_2, z_3,\ldots, z_n)$.
Step 3: As Eq. 8, a matrix [**B** $\mathbf{Z}''$] is constructed by sequence $\mathbf{Z}''$ and band order **B**. Then the matrix is transformed by reranking $\mathbf{Z}'$ in descending order, and we gain a new vector $\mathbf{B}'$ which is the new band order.

$$[\mathbf{B}\mathbf{Z}''] \overset{Rank\mathbf{Z}''}{\longrightarrow} [\mathbf{B}'\mathbf{Z}''']. \tag{8}$$

2.3 Encryption by Domain Mixing

The hyperspectral remote sensing image is a 3D data. Therefore, the analytical approach of cube data may acquire the information of a hyperspectral image. Considering the hyperspectral image contain both spatial and spectral information, and the spatial domain is orthogonal to spectral domain, correlation of two domains is changed to improve the security. Here we introduce to use a Mapping method to shuffle the two domains. The mapping mode is shown in Fig. 3.

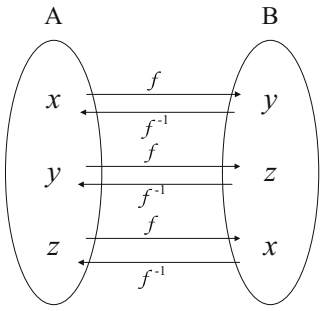

Fig. 3. The mapping mode of domain confusion.

Let a pixel in a hyperspectral image be $X(x, y, z)$. As we can see in Fig. 3, the x value is mapping to y-axis, the y value is mapping to z-axis and the z value is mapping to x-axis, which is defined as:

$$X(x, y, z) \overset{Mapping}{\longrightarrow} X'(y, z, x) \tag{9}$$

Then the spectral and spatial domains are mixed together and the correlation of two domains is broken. This process can disturb the attacker and prevent the space analysis

of the hyperspectral remote sensing image, which leads to further security. To prove the security of our method, the encryption results and analysis will be shown in the next section.

3 Experimental Results and Analysis

In order to evaluate the encryption performance of our method, we conducted experiments with a collection of the high-resolution hyperspectral data sets obtained from German Aerospace Center's (DLR) in Oberpfaffenhofen in Germany and NASA over the World Trade Center (WTC) area in New York. The AVIRIS images contain more than 125 spectral bands between 0.4 and 2.5 μm. The spatial resolution is 20 m, and the spectral resolution is 10 nm. The experimental platform is a PC with 3.30 GHz CPU, 4.00 G memory, Windows 7 operating system. Our dataset contains more than 2000 hyperspectral remote sensing images with different size of images.

In this experiment, we set the initial values of the Logistic Map and Chebyshev Map to 0.32. The parameter μ of Logistic Map is set to 4 and the parameter k of Chebyshev Map is set to 20. And the size of the image is $512 \times 614 \times 224$. Two different single chaotic sequences for image encryption [9] and an encryption method based on AES [12] are compared. In the next section, some well-known security analysis techniques are considered as quality measurement factors such as Histogram analysis, Correlation of adjacent pixels Information entropy, Key space analysis and Key sensitivity analysis.

3.1 Histogram Analysis

To prevent information leakage, it is important to ensure that the encrypted image and original image do not have any statistics similarities. The histogram reflects the distribution of the pixel values which is attacked most. As can be seen in Fig. 4, the histogram of the original image contains continuous rises and declines, while the histogram of encrypted image shows uniform distribution. The results show that our method has stronger ability to resist statistical analysis and attacks.

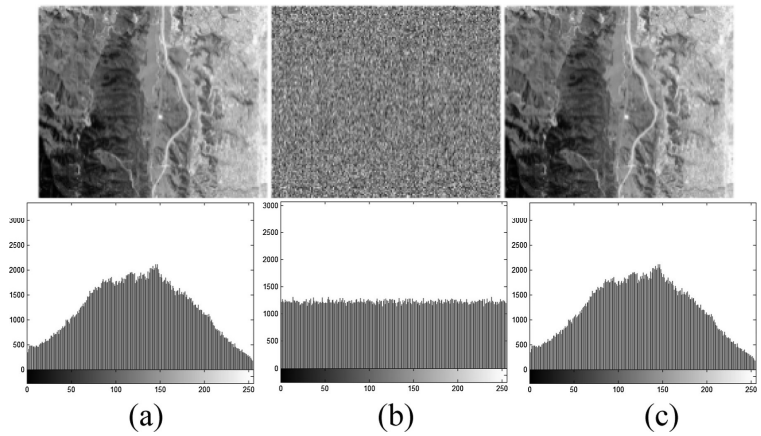

Fig. 4. The encryption results: (a) the original image, (b) the encrypted image, (c) the decrypted image.

3.2 Correlation of Adjacent Pixels

The high correlation between adjacent pixels is one of the major feature of an image. Therefore, the correlation between adjacent pixels of the encrypted image is broken to improve the security. Figure 5 shows the pixel correlation in vertical direction of our method. As can be seen that the points in the figure are uniform distribution after encrypted.

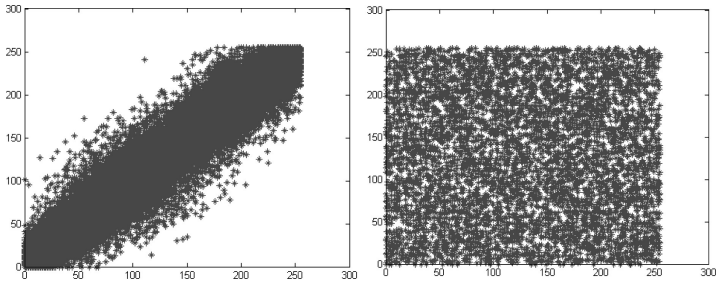

Fig. 5. The pixel correlation in vertical direction: (a) the original image, (b) the encrypted image.

Correlation coefficient can reflect the correlation between pixels objectively. First, $E(x)$ is the means of series x_i. Correlation coefficient r is described as:

$$r_{x,y} = \frac{\sum_{i-1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i-1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i-1}^{N}(y_i - E(y))^2}} \tag{10}$$

The correlation coefficients of the encrypted image in vertical and horizontal direction is shown in Table 1. The results show that the correlation of encrypted image is very low, and our method and AES-256 are much better.

Table 1. The correlation coefficients of different encryption methods.

Encryption method	Vertical direction	Horizontal direction
Original image	0.973810	0.977445
Logistic Map [9]	0.025141	0.017214
Chebyshev Map [9]	0.032118	0.022741
AES-256 [12]	0.010221	0.013217
Our method	0.010012	0.012014

3.3 Information Entropy

Information entropy was first proposed by Shannon [16, 17]. The entropy and related information measures provide useful descriptions of the random process behavior. The information entropy is defined as:

$$H(m) = \sum_{i=0}^{2N-1} P(m_i)\log_2 \frac{1}{P(m_i)} \tag{11}$$

The calculated information entropy value is given in Fig. 6. The value obtained from the computed experiment results is very near to the theoretical ideal value of 8. And our method and AES-256 has a great impact and improve the security level.

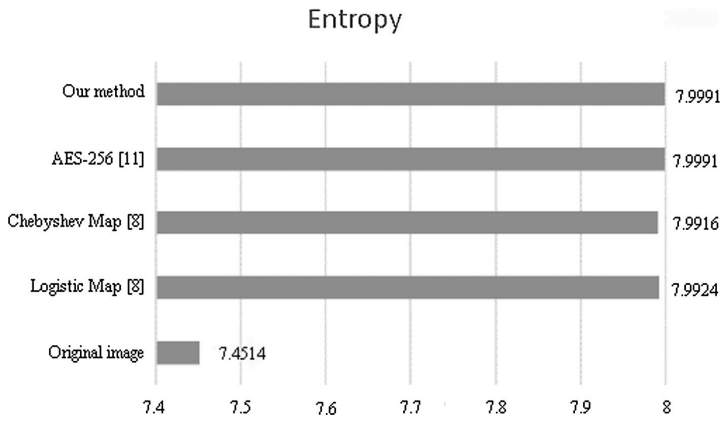

Fig. 6. The information entropy of different encryption methods

3.4 Key Space Analysis

To secure hyperspectral image from brute-force and similar attacks, the key space should be large enough. In our method, the key consists of initial values of Logistic and Chebyshev Map, parameter μ and k. Due to the value range of μ, k and initial values, the key space is more than 10^{28}. Therefore, the key space is large enough to reduce the risk of a brute-force attack.

3.5 Key Sensitivity Analysis

The encryption algorithm should be sensitive to the secret key. The change of a single bit in the secret key should produce completely different output results. In our method, the key sensitivity is related to the initial values and parameters sensitivity for the chaotic sequences. As can be seen in Fig. 7, the initial values and k changing a little will produce a completely different chaotic sequences. This can be explained by the fact that Chebyshev Map is sensitive to the initial value.

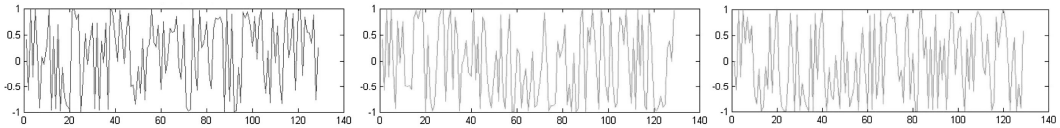

Fig. 7. The chaos sequences: (a) $x_1 = 0.4113$, $k = 20$, (b) $x_1 = 0.4113001$, (c) $k = 20.000001$.

3.6 Performance Analysis

Besides the security analysis by evaluating statistical analysis and measurements, the time consumption is also an important issue. From Fig. 7, Tables 1 and 2, the security of our method and AES-256 is stronger, but the time consumption of AES-256 is much higher than other methods. Therefore, our method has a better performance.

Table 2. Time consumption results for different encryption methods.

Encryption method	Encryption time (s)	Decryption time (s)
Logistic Map [9]	66.24	66.21
Chebyshev Map [9]	66.17	66.05
AES-256 [12]	2480.21	2488.13
Our method	67.96	67.74

4 Conclusions

In this paper, a hybrid domain encryption method of hyperspectral remote sensing image is proposed for securely transmitting and storing hyperspectral images. Considering the spatial and spectral characteristics, the hyperspectral image is encrypted in hybrid domain (spatial and spectral). Spatial domain encryption is done by using the composite chaos sequences. Then, the spectral sequence is scrambled by the cipher sequence for protecting the spectral feature of the hyperspectral image. Finally, the spectral and spatial information is mixed by a one-to-one mapping. Three methods are compared in our experiments, our method was successfully implemented and showed a better encryption performance for hyperspectral image. In the future work, we will further reduce the correlation between adjacent pixels and enlarge the key space by improving the construction to enhance the security of our proposed method.

Acknowledgments. The work in this paper is supported by the National Natural Science Foundation of China (No. 61370189, No. 61531006, No. 61372149, and No. 61471013), the Beijing Natural Science Foundation (No. 4163071), the Science and Technology Development Program of Beijing Education Committee (No. KM201510005004), the Importation and Development of High-Caliber Talents Project of Beijing Municipal Institutions (No. CIT&TCD20150311), Funding Project for Academic Human Resources Development in Institutions of Higher Learning Under the Jurisdiction of Beijing Municipality.

References

1. Smith, R.B.: Introduction to Hyperspectral Imaging, pp. 1–24. Microimages (2006)
2. Zhang, E., Zhang, X., Yang, S.: Improving hyperspectral image classification using spectral information divergence. IEEE Geosci. Remote Sens. Lett. **11**(1), 249–253 (2014)
3. Veganzones, M., Tochon, G., Dalla-Mura, M., Plaza, A., Chanussot, J.: Hyperspectral image segmentation using a new spectral unmixing-based binary partition tree representation. IEEE Trans. Image Process. **23**(8), 3574–3589 (2014)

4. Chen, G., Mao, Y., Chui, C.K.: A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals **2**(3), 749–776 (2004)
5. Cao, W., Zhou, Y., Chen, C.P., Xia, L.: Medical image encryption using edge maps. Sign. Process. **132**, 96–109 (2017)
6. Zhang, S., Gao, T.: An image encryption scheme based on DNA coding and permutation of hyper-image. Multimed. Tools Appl. **75**(24), 17157–17170 (2016)
7. Ayoup, A.M., Hussein, A.H., Attia, M.A.: Efficient selective image encryption. Multimed. Tools Appl. **75**(24), 17171–17186 (2016)
8. Yi, X., Tan, C.H., Siew, C.K.: A new block cipher based on chaotic tent maps. IEEE Trans. Circ. Syst. I Fundam. Theory Appl. **49**(12), 1826–1829 (2002)
9. Usama, M., Khan, M.K., Alghathbar, K., Lee, C.: Chaos-based secure satellite imagery cryptosystem. Comput. Math Appl. **60**(2), 326–337 (2010)
10. Huang, X., Ye, G., Chai, H., Xie, O.: Compression and encryption for remote sensing image using chaotic system. Secur. Commun. Netw. **8**(18), 3659–3666 (2015)
11. Yin, L., Zhao, J., Duan, Y.: Encryption scheme for remote sensing images based on EZW and chaos. In: The 9th International Conference for Young Computer Scientists, Hunan, China, pp. 1601–1605 (2008)
12. Muhaya, F.T.B.: Chaotic and AES cryptosystem for satellite imagery. Telecommun. Syst. **52** (2), 573–581 (2013)
13. Liu, Z., Xu, L., Liu, T., Chen, H., Li, P., Lin, C., Liu, S.: Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. Opt. Commun. **284**(1), 123–128 (2011)
14. Zhou, N., Wang, Y., Gong, L., He, H., Wu, J.: Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform. Opt. Commun. **284**(12), 2789–2796 (2011)
15. Tan, R.C., Lei, T., Zhao, Q.M., Gong, L.H., Zhou, Z.H.: Quantum color image encryption algorithm based on a hyper-chaotic system and quantum Fourier transform. Int. J. Theor. Phys. **55**(12), 5368–5384 (2016)
16. Shannon, C.E.: A mathematical theory of communication. Bell Syst. Tech. J. **27**(3), 379–423, 623–656 (1948)
17. Shannon, C.E.: Coding theorems for a discrete source with a fidelity criterion. IRE Nat. Convention Rec. **7**, 142–163 (1959)