Opt Quant Electron (2016) 48:396
DOI 10.1007/s11082-016-0669-9

Securing color image by using hyperchaotic system in gyrator transform domains

Hang Chen[1,2] · Camel Tanougast[1] · Zhengjun Liu[2] · Boya Hao[3]

Received: 3 June 2016 / Accepted: 22 July 2016 / Published online: 26 July 2016
© Springer Science+Business Media New York 2016

Abstract A color image encryption scheme is proposed by using a hyperchaotic system in gyrator transform domains. The red, green and blue (RGB) components of the original color image are encoded into one dimensional stream, respectively. Four chaotic sequences generated by a hyperchaotic system are blended into the streams to synthesize complex sequences. Subsequently the one dimensional complex streams are scrambled by employing discrete cosine transform and then encoded back to image format. Finally, the scrambled complex functions are encoded and transformed in gyrator domains. The parameters in the hyperchaotic system and the gyrator optical system are regarded as the extra keys for improving the security of the proposed scheme. Some numerical simulations are made to test the validity and capability of the proposed color encryption algorithm.

Keywords Color image encryption · Hyperchaotic · Cryptography · Optical transform

1 Introduction

The optical information security technology has been deeply researched since (Refregier and Javidi 1995) proposed an optical image encryption system based on double random phase encoding (DRPE). Optical image encryption technology is extensively explored due

✉ Hang Chen
hitchenhang@foxmail.com

[1] Laboratoire Conception Optimisation et Modélisation des Systèms, University de Lorraine, 57070 Metz, France

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

[3] Research Institute of Special Mechanical and Electrical Technology of Beijing, Beijing 100012, China

to its parallel processing and high speed. Various encryption algorithms have been reported based on different optical systems, such as optical transforms (Liu and Liu 2007; Alfalou and Brosseau 2009; Liu et al. 2011; Lang 2012; Chen et al. 2013a, b; Mehra et al. 2014; Abuturab 2014; Sui et al. 2014), interference (Zhu et al. 2009), holography (Chen et al. 2012) and interferometry (Meng et al. 2006). In some optical encryption systems, like double random phase encoding technology (Refregier and Javidi 1995), the secret image is modulated and the pixel value is randomized by random phase function. Moreover some scrambling operations, such as jigsaw transform and Arnold transform, are considered to change the sequence of image pixels (Hennelly and Sheridan 2003; Zhong et al. 2012; Chen et al. 2015). Typically a secret image can be randomized by encryption scheme composed of random reversible process.

As a trend of optical information security, various color image encryption algorithms (Chen et al. 2009, 2015; Liu et al. 2015; Abuturab 2012, 2013) have been reported in recent years. In these encryption schemes (Chen et al. 2009, 2015; Liu et al. 2015; Abuturab 2012, 2013), the color image is separated into red, green and blue components, which are regarded as the corresponding channels. Subsequently the corresponding color components can be encoded by some encryption method of gray-level image. Different optical systems, such as dual fractional Fourier–wavelet transform (Chen et al. 2009), Fresnel transform (Liu et al. 2015) and fractional Fourier transform (Chen et al. 2015), have been introduced for hiding color image encryption. Some latest color image encryption schemes in gyrator transform domain have been proposed (Abuturab 2012, 2013, 2014), the gyrator transform are well used in these schemes and the security, validity and capability of the algorithms are improved.

In this work, we present a novel color image encryption scheme based on a hyperchaotic system in gyrator domains. In the encryption process, three hyperchaotic phases generated by a 4D Lorenz system are considered and utilized. To enhance the security of the encryption algorithm, the original color image will be divided into RGB components and converted into one dimension format. Subsequently the hyperchaotic sequences are blended into the one dimensional data as the imaginary part. Then the complex function is scrambled by employing discrete cosine transform (DCT) and then encoded back to image format. Finally the three scrambled components will be changed as the real part and the imaginary part of a light field in the gyrator transform. The random hyperchaotic sequences are regarded as the main keys in this cryptosystem and the parameters in the hyperchaotic system and the gyrator transform can serve as the extra keys for enhancing the security. Numerical simulation is given to validate the performance of the proposed color image encryption.

The rest of the paper is organized in the following sequence. In Sect. 2, the proposed encryption/decryption algorithm is addressed in detail. In Sect. 3, numerical simulation results are made to demonstrate the validity of the algorithm. Concluding remarks are summarized in the final section.

2 Color image encryption algorithm

In this section, a new 4D Lorenz hyperchaotic system and gyrator transform are introduced briefly in this section. Thereafter, the intact encryption algorithm in gyrator transform domains is addressed in detail.

2.1 Hyperchaotic system

Referring to (Chee and Xu 2005; Lin et al. 2010; Zhu 2012), hyperchaotic dynamics provides a fast approach for building superior performance cryptosystem. The properties of hyperchaotic maps, like sensitive to initial conditions and random-like behavior, makes it suitable for protecting the secret information. Besides, it is believed that higher dimensional chaotic systems have larger key space and can improve the security of encryption scheme by generating more complex dynamical behavior or high randomness (Zhu 2012).

In proposed encryption scheme, a new hyperchaotic system is used in key scheming, which can be modeled as follows

$$\begin{cases} \dot{x} = a(y - x), \\ \dot{y} = cx - y - xz + u, \\ \dot{z} = xy - bz, \\ \dot{u} = -kx. \end{cases} \tag{1}$$

where a, b, c and k are constant parameters. When $a = 35$, $b = 8/3$, $c = 28$ and $k = 5$, the Lyapunov exponents of the hyperchaotic system are $\lambda_1 = 0.3997$, $\lambda_2 = 0.3113$, $\lambda_3 = 0$ and $\lambda_4 = -14.3776$. Here, the fourth order Runge–Kutta algorithm has been performed to solve Eq. 1 with the initial conditions $x_0 = y_0 = z_0 = u_0 = -10$ and the $(x - y)$ hyperchaotic Lorenz attractor is illustrated in Fig. 1.

For better randomness (Zhu 2012), a considerable pretreatment for the hyperchaotic sequences is applied as follows

$$s_i^* = s_i \times 10^4 - round\left(s_i \times 10^4\right), \quad (i = 1, 2, 3, 4). \tag{2}$$

where s_i represents the value of the original chaotic sequence from the hyperchaotic system mentioned above, which is x_i, y_i, z_i or u_i. The symbol s_i* denotes the improved sequences corresponding to s_i.

The hyperchaotic Lorenz attractor sequences will be employed to design the proposed algorithm.

2.2 Gyrator transform

The mathematical definition of gyrator transform is given briefly in this subsection. The gyrator transform (Simon and Wolf 2000; Rodrigo et al. 2007) is a kind of linear canonical transform (Ozaktas et al. 2000) and only has a two-dimensional format. For the two-dimension function $g(x, y)$, the gyrator transform can be expressed as

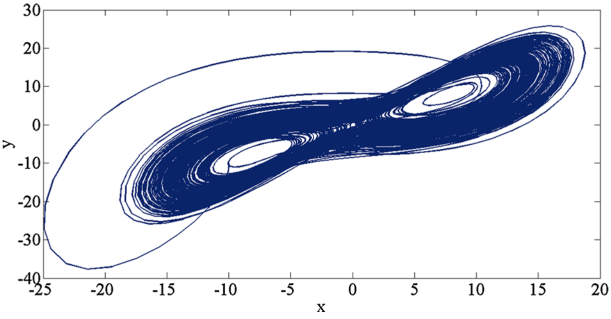


Fig. 1 The (x–y) hyperchaotic Lorenz attractor used in this paper

$$
\begin{aligned}
G(u,v) &= \xi^{\alpha}[g(x,y)](u,v) \\
&= \frac{1}{|\sin\alpha|}\iint g(x,y)\exp\left[i2\pi\frac{(xy+uv)\cos\alpha - xv - yu}{\sin\alpha}\right]\mathrm{d}x\mathrm{d}y,
\end{aligned}
\tag{3}
$$

where $G(u, v)$ and $g(x, y)$ are the output and input of the gyrator transform, respectively. The parameter α is a fractional order and the gyrator transform will becomes a Fourier transform when $\alpha = \pi/2$ with the rotation of the coordinates (u, v). Besides, the gyrator has some properties similar to fractional Fourier transform, such as index additivity, energy conversation and linearity. For hardware architecture, the gyrator transform can be implemented in the optical system composed of six thin cylinder lenses (Simon and Wolf 2000).

2.3 Encryption algorithm

The flowchart of the proposed image encryption is depicted in Fig. 2. Both the hyperchaotic system and gyrator transform are considered and utilized to complete the intact secure scheme. In the initial stage of the encryption process, the original color image is separated into RGB components and then encoded into one dimensional stream, respectively. Simultaneously, three random sequences generated by the hyperchaotic system are blended into the corresponding stream as the imaginary part. Here the blending operation can be calculated as follows

$$
\begin{cases}
Se1 = \cos\left(sr.*\left[\left(0.01*s_4^*\right)+0.005\right]\right)+i*\cos\left(s_1^**\pi/2\right)\\
Se2 = \cos\left(sg.*\left[\left(0.01*s_4^*\right)+0.005\right]\right)+i*\cos\left(s_2^**\pi/2\right)\\
Se3 = \cos\left(sb.*\left[\left(0.01*s_4^*\right)+0.005\right]\right)+i*\cos\left(s_3^**\pi/2\right)
\end{cases}
\tag{4}
$$

where Se and $s*$ denote the blended sequences and the improved sequences calculated by

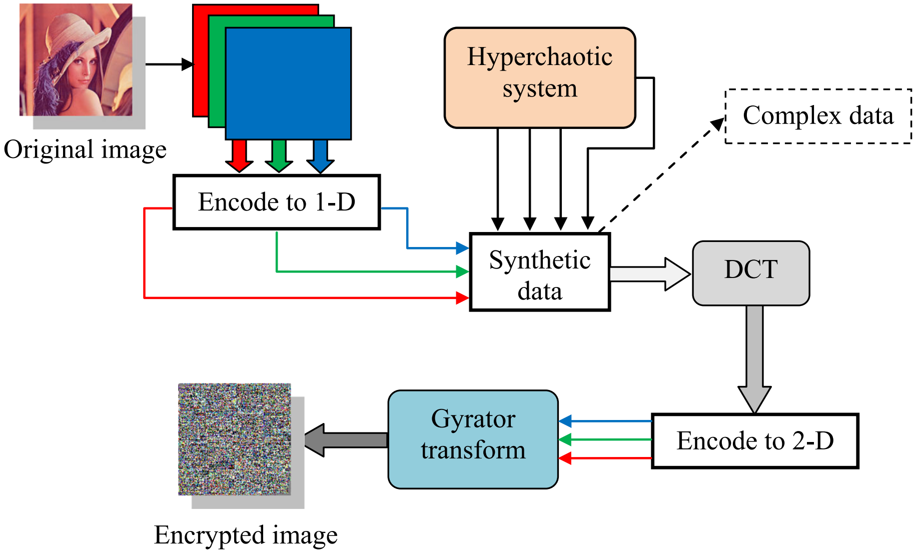


Fig. 2 The flowchart of the *color image* encryption algorithm. (Color figure online)

using Eq. 2, respectively. Here *sr*, *sg* and *sb* are the one dimension sequences of the RGB components.

In the following step, DCT is employed in the process of image encryption. After the blending the stream, the mixed data is converted by DCT. DCT can change the distribution of pixel value of the whole stream to achieve a higher level random output pattern. Subsequently, the output stream of DCT is encoded back to RGB components with the format as complex function. Finally, the results from the calculations described above are encoded by using gyrator transform simultaneously. The amplitude of the output from gyrator transform is regarded as the final encrypted image in this paper.

For decryption process, the inverse gyrator transform and inverse DCT are performed along the reverse direction of the encryption process. Since every steps of the encryption flowchart is reversible, the secret image can be retrieved completely with the correct keys. Moreover, the phase function of the encrypted result is the main key for our encryption algorithm for their high random-like behavior and sensitivity to initial conditions properties. The rotation angle α_1, α_2 and α_3 used in each gyrator transform can be regarded as the extra keys to enhance to the security of the encryption scheme. To retrieve the original image, the users must provide both the main keys and extra keys. It is impossible to decrypt the intact information if any keys are inexistence. Some simulations will be given to test the result of missing keys in next section.

The encryption/decryption scheme proposed in this paper can be implemented with an electro-optical setup illustrated in Fig. 3. The gyrator transform G^{α} and its inverse transform $G^{-\alpha}$ are achieved by an optical system (Simon and Wolf 2000). Three kinds of optical beam (red, green and blue) are utilized to encode the RGB channels of the color image. Here, the amplitudes and phases will be encoded into the optical encryption system of the

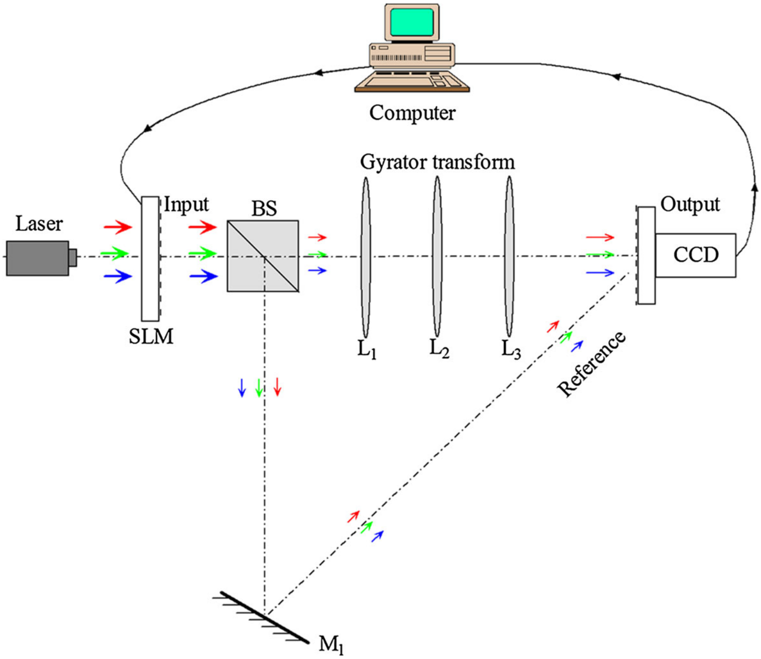


Fig. 3 The electro-optical setup of the proposed encryption scheme

gyrator transform by using the spatial light modulator (SLM) (Simon and Wolf 2000). At the output plane, we record the phase information by using in-line holography technique. Besides, the calculation of dimension encoding and DCT can be performed on the computer. Moreover, the devices SLM and CCD will accomplish the data communication between computer and optical system will be the SLM and CCD. The algorithm can serve in the hardware-based cryptographic.

3 Numerical simulation

Numerical simulation is considered to demonstrate the effectiveness of the encryption algorithm. In this section, we select a color image 'Lena' having 256 × 256 pixels shown in Fig. 4 to serve as the original image. The rotation angles in gyrator transform are set in 0.2, 0.3, 0.5, respectively. In addition, the first 65,536 values of the hyperchaotic sequences are calculated and encoded. In calculation we use a computer with Core 2, CPU 2.5 GHz and 2048 Mbytes memory under Windows 7 system. The encryption process and decryption processes for this picture take 0.1815 and 0.1882 s, respectively. By using the parameters mentioned above, the encrypted data is displayed in Fig. 5. For showing the complex function, the encrypted/decrypted images in the following section are shown for their real part.

To weight the difference between the decrypted image and original image, the peak signal-to-noise ratio (PSNR) function is performed and expressed as

$$\mathrm{PSNR}(I_{\mathrm{d}}, I_o) = 10\log_{10}\frac{255^2 M \times N}{\sum\limits_{\forall x,y}\left[I_{\mathrm{d}}(x,y) - I_o(x,y)\right]^2}(\mathrm{dB}). \tag{5}$$

where I_{d} and I_0 represent the decrypted image and original image, respectively. The symbols '*d*' and '*o*' are short for 'decrypted' and 'original'. Moreover, the parameter M and N denote the size of the two images in this calculation.

In the aspect of security, the sensitivity of fractional order α in gyrator transform is calculated first. As mentioned above, the parameters $\alpha 1$, $\alpha 2$ and $\alpha 3$ used in RGB channels are regarded as the additional keys in this encrypted scheme. Therefore, all these three extra keys are selected to serve as a variable to test the sensitivity in the encryption

Fig. 4 The original secret image used in this paper

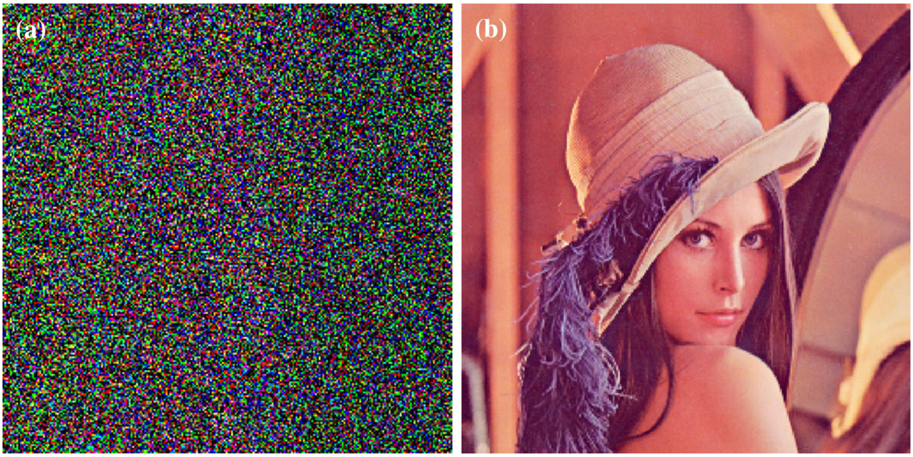


Fig. 5 Encrypted results: **a** the encrypted image and **b** decrypted image

algorithm, respectively. In this experiment, we suppose that the main keys and the initial conditions of the hyperchaotic system are stolen by the attacker. Therefore, the additional keys α have to protect the secret color image. In numerical simulations, the angle parameters $\alpha1$, $\alpha2$ and $\alpha3$ in RGB channels are taken at 0.52, 0.5 and 0.48, respectively. When the main key (the encrypted phase data) and the initial conditions of hyperchaotic system are correct, the angles $\alpha1$, $\alpha2$ and $\alpha3$ are changed around the correct value and the corresponding PSNR curve is illustrated in Fig. 6. Here the sampling step length of the additional keys in the experiments is taken at 0.005. As we can see from the experiment result, the left image in Fig. 6 is almost random pattern and the right one has critical noise even if the keys α are very close to the correct value. In other words, the parameters α regarding as the additional key perform well in protecting the secret image.

In addition, the normalized correlation coefficient (NCC) is also considered to judge the correctness between the encrypted/decrypted image and the original color image. The mathematical definition of NCC can be expressed as

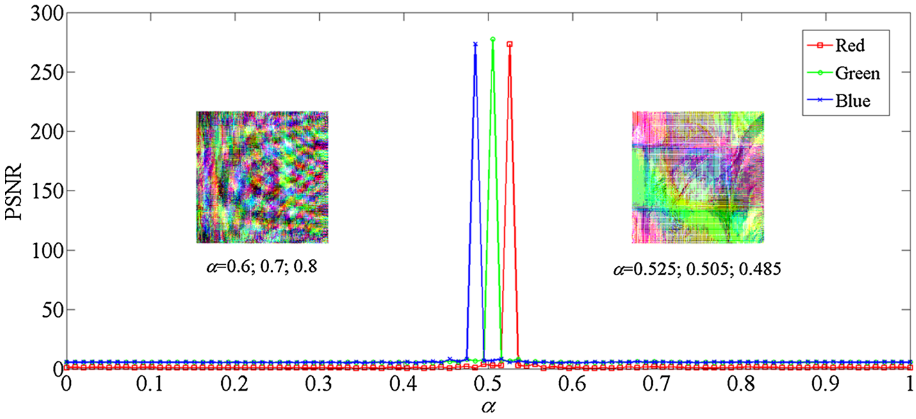


Fig. 6 The PSNR calculated by the different values of the parameter α in gyrator transform

$$\mathrm{NCC}(I_r, I_o) = \frac{1}{h \times w} \sum_{x=1}^{h} \sum_{y=1}^{w} I_r(x, y) I_o(x, y) \tag{6}$$

where w and h denote the width and height of the secret image, respectively. Similarly, I_r and I_o represent the retrieved image and original image, the pixel values of which have been normalized in the range [−1, 1]. Moreover, the value of NCC is in the range of [−1, 1]. The value of NCC between the original secret image displayed in Fig. 4 and the decrypted image displayed in Fig. 5b is 1, which implies that there is no difference between the two images. Furthermore, the NCC values between the original image and the incorrect decrypted images shown in Fig. 6 are 0.2187 and 0.3688, which also indicate the sensitivity of the extra key α. The small effective interval of the additional keys will cause prodigious difference of the decrypted results.

On the other hand, we demonstrate that the secret color image is impossible to be recovered without the main key. In the following experiment, some situations, like missing the main key or using the modified main key, are considered and simulated. Firstly, we suppose that the additional keys are known by the illegal user, the decrypted result by using an incorrect main key is drawn in Fig. 7a. Subsequently the decryption result without main key is illustrated in Fig. 7b. As we can see from Fig. 7, the decrypted results are noise-like pattern and lost the detail information of the image. The NCC values between the original image and these two decrypted results are 0.2973 and 0.0312, which indicate the results are far different from the secret image.

In the follow step, a worse situation is considered. When the main key and the additional keys α are revealed, the initial conditions of the hyperchaotic system will serve as the last protection key for the total encryption scheme. As described above, the initial conditions of the hyperchaotic system is set as $x_0 = y_0 = z_0 = u_0 = -10$ for the encryption/decryption experiment shown in Fig. 5. In the following experiment, we suppose that x_0, y_0 and z_0 are cracked by the illegal user, and u_0 is set as -9.9999, which is very close to the correct value -10. Besides, another case is considered as follows, y_0, z_0 and u_0 are known and x_0 is set as -10.0001 for the decryption process. The decrypted images of these two

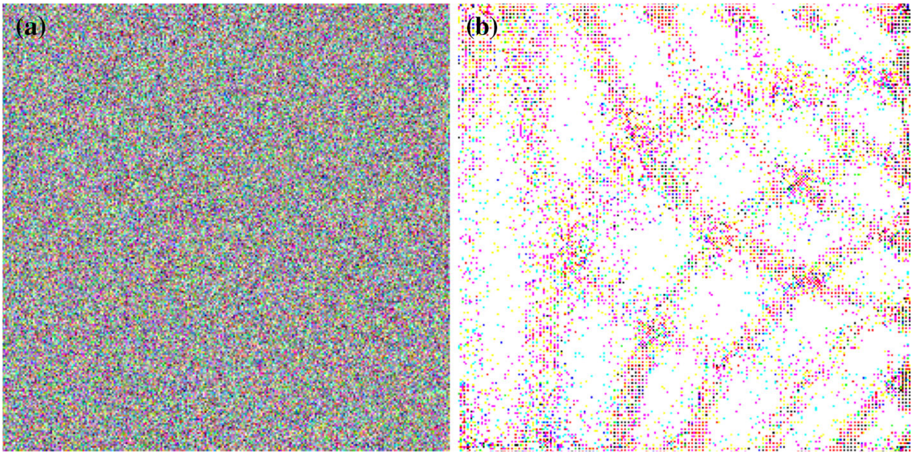


Fig. 7 The test of decryption: **a** main key is incorrect while additional keys are known, **b** main key is missing while the additional keys are known

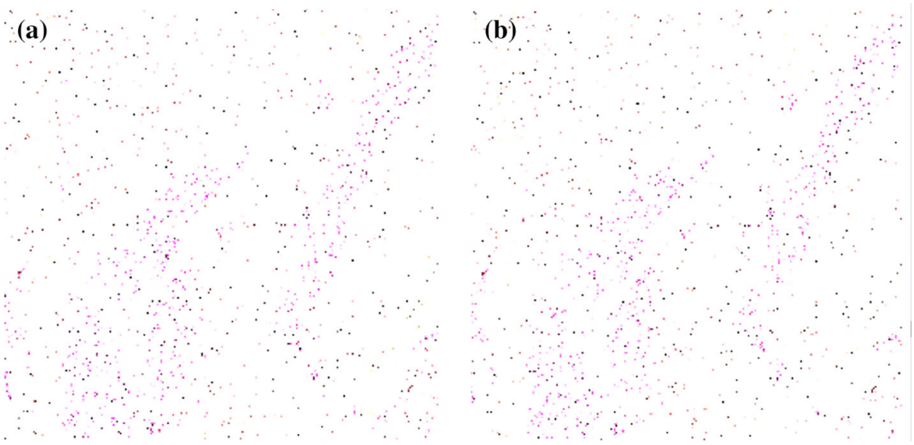


Fig. 8 The decryption results: **a** using the initial condition [−10 −10 −10 −9.9999], **b** using the initial condition [−10.0001 −10 −10 −10]

situations have been displayed in Fig. 8a, b, from which the secret information of the original image is completely under protect. The NCC values between the original image and the two decrypted results are 0.0793 and 0.0684, respectively. Therefore, the initial conditions of the chaotic system are very sensitive for protecting the color image, the small change of the initial values cause prodigious difference. Furthermore, more decryption experiments have been designed to test the sensitivity of the initial values and the results are listed in Table 1, in which the NCC and PSNR value are calculated between the decrypted results and original image. Here, we suppose that all the other keys are known and the initial value of the chaotic system serve as the last protection instrument. The result listed in Table 1 proves the capability of x_0, y_0, z_0 *and* u_0 in protecting the secret data.

The encrypted image will be checked by occlusion attack and noise attack as the aspect of robustness analysis. In the attack experiments, the decryption process is performed with the correct key from an encryption image occluded partly, which is shown in Fig. 9a, b. Supposing that the encrypted image is lost or destroyed partly and the values of occluded pixels are replaced with 0 and the corresponding results are represented in Fig. 9c, d. As shown in Fig. 9, the main information of the original input image can be recognized in vision even if there are serious noises in the recovered images. The recovered image shown in Fig. 9c is more clear than that in Fig. 9d because of the different occluded acreage.

For the noise attack experiment, the noise data are added into the secret data by using the following model

Table 1 The decrypted results by using different initial conditions

x_0	y_0	z_0	u_0	NCC
−10	−10	−10	−10	1.0000
−10.0001	−10	−10	−10	0.0684
−10	−10	−10	−9.9999	0.0793
−10	−10.0001	−9.9999	−10	0.0657
−5	−6	−7	−8	0.0275

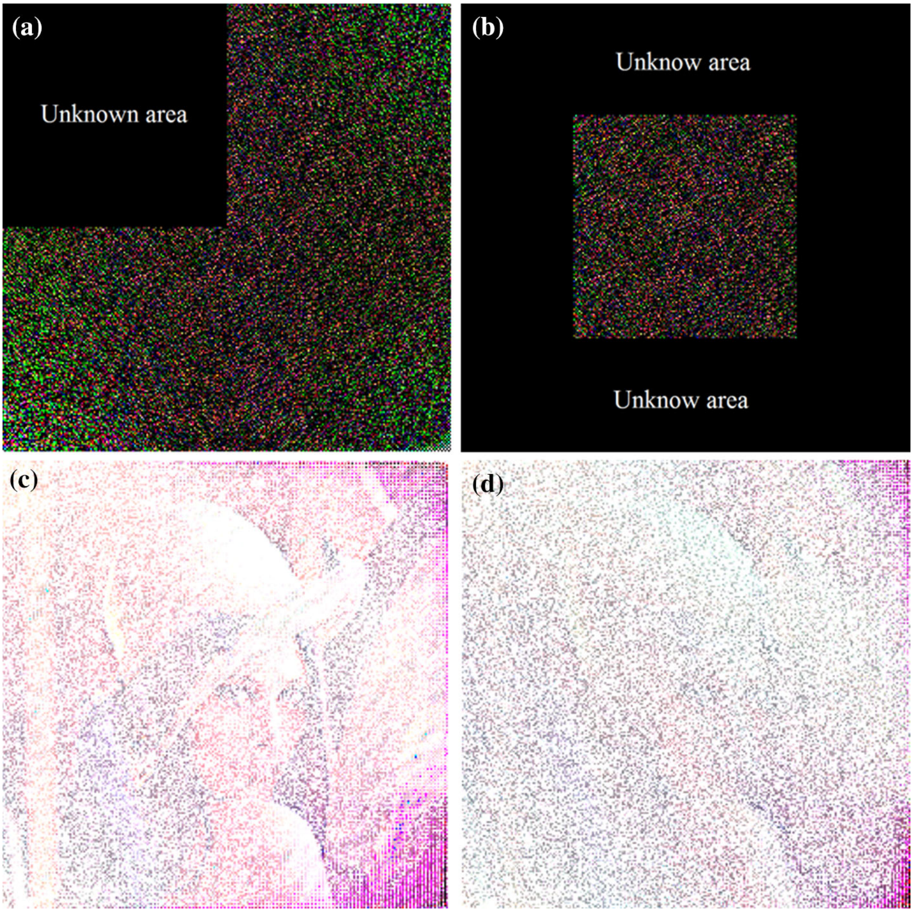


Fig. 9 The test of occlusion attack: **a** the occluded encrypted image 1, **b** the occluded encrypted image 2, **c** the recovered result of (**a**) and **d** the recovered result of (**b**)

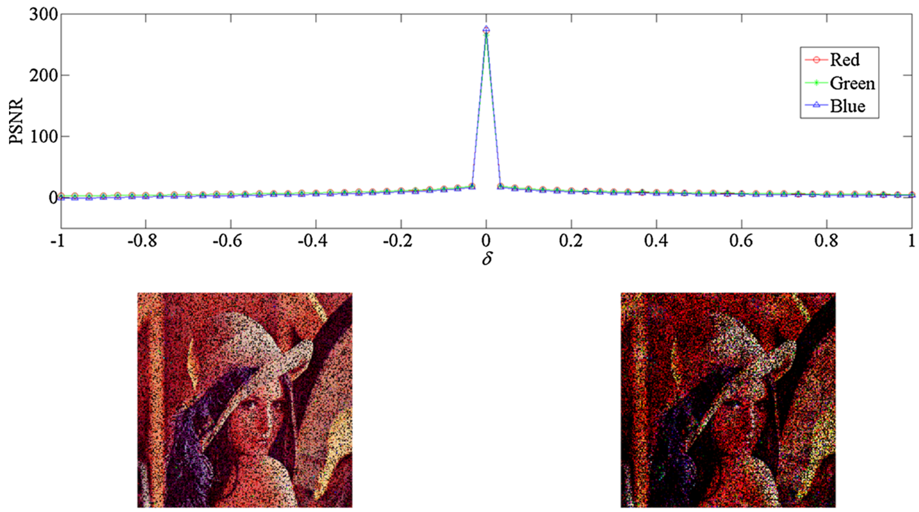
$$I'(x,y) = I(x,y)\left[1 + \delta \cdot \sigma_{0,1}(x,y)\right], \tag{7}$$

where $I(x,y)$ represents the original encrypted data. $I'(x, y)$ is the polluted by the noise $\sigma_{0,1}(x, y)$, which denotes random function with the mean value 0 and standard deviation 1. The parameter δ represents the intensity of the added noise and we named it intensity factor. The corresponding PSNR curve is calculated and depicted in Fig. 10 by using the images $I'(x, y)$ generated with various values of intensity factor δ. Also, for $\delta = -0.05$ and $\delta = 0.5$, two decrypted images have been attached in Fig. 10, in which the outline of the secret image can be identified.

Finally, the experiments of known plaintext attack (Peng et al. 2006) and chosen plaintext attack (Peng et al. 2006) are considered to test the random phase encoding of the proposed encryption scheme. An encryption model is defined as follows

$$E(u,v) = \xi^{\alpha}\{I(x,y)\exp[i \cdot \phi_1(x,y)]\}\exp[i \cdot \phi_2(x',y')], \tag{8}$$

where the function functions $\phi_1(x, y)$ and $\phi_2(x', y')$ represent two random phase masks and the symbol ξ^{α} denotes gyrator transform as mentioned before. $E(x, y)$ is the output



δ=-0.05

δ=0.5

Fig. 10 The PSNR curve of noise attack including decrypted images obtained with $\delta = -0.05$, and $\delta = 0.5$

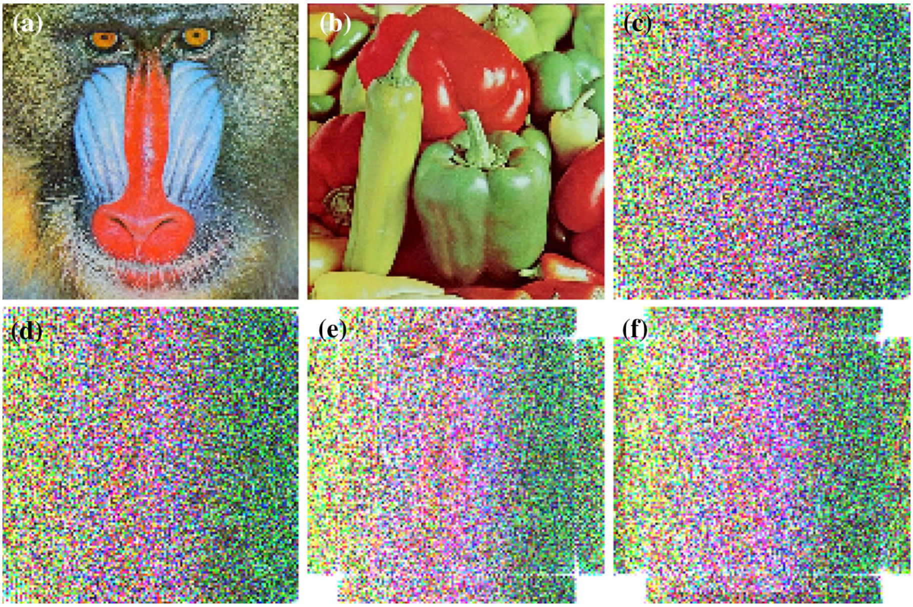


Fig. 11 The test of known plaintext attack and chosen plaintext attack: **a** original image, **b** original image, **c** the encrypted data of (**a**), **d** the encrypted data of (**b**), **e** the result of known plaintext attack and **f** the result of chosen plaintext attack

function, which can be regarded as the red, green and blue components of the encrypted image obtained by the proposed encryption algorithm. Therefore, iterative phase retrieval algorithm and impulse function can be used for the known plaintext attack (Peng et al. 2006) and chosen plaintext attack (Peng et al. 2006), respectively.

Two test color images ‘Baboon’ and ‘Peppers’ have 128 × 128 pixels are selected in the plaintext attack experiment. First of all, the test images are encrypted by using the algorithm described in Sect. 2 and the original images and encrypted data are illustrated in Fig. 11a–d, respectively. In the following step, we suppose that the original secret image ‘Baboon’ and its encrypted data are filched by the attacker. In this situation, the decrypted data of image ‘Peppers’ shown in Fig. 11d will be attacked in simulation. For the known plaintext attack experiment, the phase retrieval algorithm is employed with 500 iterations in gyrator domain for red, green and blue components, respectively. Besides, the impulse function is employed in chosen plaintext attack experiment. The experimental results obtained by known plaintext attack and chosen plaintext attack illustrated in Fig. 11e, f, respectively. As we can see from the results, the recovered images are random pattern and cannot be identified entirely.

4 Conclusion

We have proposed a color image encryption algorithm by using a hyperchaotic system in gyrator transform domains. An original color image is divided into red, green and blue components and encoded as three 1-D streams. Subsequently the streams and three other hyperchaotic sequences are blended to synthesize new complex sequences. The complex functions are scrambled by employing discrete cosine transform and then encoded back to RGB channels. Then the RGB components are modulated in the optical gyrator transform system and the amplitude and phase in the output plane of optical system are regarded as the encrypted information and main key. The parameters of the optical system and the initial conditions of the hyperchaotic system can serve as additional keys for security enhancement. Some numerical simulations have demonstrated the validity, security and robustness of the color image encryption scheme.

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), the Program for New Century Excellent Talents in University (NCET-12-0148), and the China Postdoctoral Science Foundation (2013M540278). The authors wish to thanks Mr. Chengwei Yang in Baicheng Ordnance Test Center of China for the valuable discussion. The authors wish to thank the reviewers for their useful comments and suggestions.

References

Abuturab, M.R.: Color information cryptosystem based on optical superposition rinciple and phase-truncated gyrator transform. Appl. Opt. **51**, 7994–8002 (2012)

Abuturab, M.R.: Color image security system based on discrete Hartley transform in gyrator transform domain. Opt. Lasers Eng. **51**, 317–324 (2013)

Abuturab, M.R.: An asymmetric color image cryptosystem based on Schur decomposition in gyrator transform domain. Opt. Lasers Eng. **58**, 39–47 (2014a)

Abuturab, M.R.: Color information verification system based on singular value decomposition in gyrator transform domain. Opt. Lasers Eng. **57**, 13–19 (2014b)

Alfalou, A., Brosseau, C.: Optical image compression and encryption methods. Adv. Opt. Photonics **1**, 589–636 (2009)

Chee, C., Xu, D.: Secure digital communication using controlled projective synchronisation of chaos. Chaos, Solitons Fractals **23**, 1063–1070 (2005)

Chen, L., Zhao, D., Ge, F.: Color image encoding in dual fractional Fourier–wavelet domain with random phases. Opt. Commun. **282**, 3433–3438 (2009)

Chen, W., Chen, X., Sheppard, C.J.R.: Optical color-image encryption and synthesis using coherent diffractive imaging in the Fresnel domain. Opt. Express **20**, 3853–3865 (2012)

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 (2013a)

Chen, W., Situ, G., Chen, X.: High-flexibility optical encryption via aperture movement. Opt. Express **21**, 24680–24691 (2013b)

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 (2015a)

Chen, H., Du, X., Liu, Z., Yang, C.: Optical color image hiding scheme by using Gerchberg–Saxton algorithm in fractional Fourier domain. Opt. Lasers Eng. **66**, 144–151 (2015b)

Hennelly, B., Sheridan, J.T.: Optical image encryption by random shifting in fractional Fourier domains. Opt. Lett. **28**, 269–271 (2003)

Lang, J.: Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform and chaos permutation. Opt. Lasers Eng. **50**, 929–937 (2012)

Lin, J., Huang, C., Liao, T., Yan, J.: Design and implementation of digital secure communication based on synchronized chaotic systems. Digit. Signal Process. **20**, 229–237 (2010)

Liu, Z., Liu, S.: Random fractional Fourier transform. Opt. Lett. **32**, 2088–2090 (2007)

Liu, Z., Xu, L., Lin, C., Dai, J., Liu, S.: Image encryption scheme by using iterative random phase encoding in gyrator transform domains. Opt. Lasers Eng. **49**, 542–546 (2011)

Liu, Z., Guo, C., Tan, J., Liu, W., Wu, J., Wu, Q., Pan, L., Liu, S.: Securing color image by using phase-only encoding in Fresnel domains. Opt. Lasers Eng. **68**, 87–92 (2015)

Mehra, I., Rajput, S.K., Nishchal, N.K.: Cryptanalysis of an image encryption scheme based on joint transform correlator with amplitude- and phase-truncation approach. Opt. Lasers Eng. **52**, 167–173 (2014)

Meng, X.F., Cai, L.Z., Xu, X.F., Yang, X.L., Shen, X.X., Dong, G.Y., et al.: Two-step phase-shifting interferometry and its application in image encryption. Opt. Lett. **31**, 1414–1416 (2006)

Ozaktas, H.M., Zalevsky, Z., Kutay, M.A.: Fractional Fourier Transform with Applications in Optics and Signal Processing. Wiley, New York (2000)

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.A., Alieva, T., Calvo, M.L.: Experimental implementation of the gyrator transform. J. Opt. Soc. Am. A **24**, 3135–3139 (2007)

Simon, R., Wolf, K.B.: Structure of the set of paraxial optical systems. J. Opt. Soc. Am. A **17**, 342–355 (2000)

Sui, L., Lu, H., Wang, Z., Sun, Q.: Double-image encryption using discrete fractional random transform and logistic maps. Opt. Lasers Eng. **56**, 1–12 (2014)

Zhong, Z., Chang, J., Shan, M., Hao, B.: Fractional Fourier-domain random encoding and pixel scrambling technique for double image encryption. Opt. Commun. **285**, 18–23 (2012)

Zhu, C.: A novel image encryption scheme based on improved hyperchaotic sequences. Opt. Commun. **285**, 29–37 (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)