Double color image encryption using iterative phase retrieval algorithm in quaternion gyrator domain

Zhuhong Shao,[1] Huazhong Shu,[1,6,*] Jiasong Wu,[1,4,6] Zhifang Dong,[2] Gouenou Coatrieux,[3] and Jean Louis Coatrieux[1,4,5,6]

[1]*Laboratory of Image Science and Technology, School of Computer Science and Engineering, Southeast University, Nanjing 210096, China*
[2]*School of Electronic Science and Engineering, Southeast University, Nanjing 210096, China*
[3]*Institut Mines-Telecom, Telecom Bretagne, INSERM U1101 Latim, Brest, F-29238, France*
[4]*INSERM, U1099, Rennes, F-35000, France*
[5]*Université de Rennes 1, LTSI, Rennes, F-35042, France*
[6]*Centre de Recherche en Information Médicale Sino-français (CRIBs), Rennes, F-35000, France*
[*]*shu.list@seu.edu.cn*

Abstract: This paper describes a novel algorithm to encrypt double color images into a single undistinguishable image in quaternion gyrator domain. By using an iterative phase retrieval algorithm, the phase masks used for encryption are obtained. Subsequently, the encrypted image is generated via cascaded quaternion gyrator transforms with different rotation angles. The parameters in quaternion gyrator transforms and phases serve as encryption keys. By knowing these keys, the original color images can be fully restituted. Numerical simulations have demonstrated the validity of the proposed encryption system as well as its robustness against loss of data and additive Gaussian noise.

1. Introduction

The image encryption technique, by its capability to ensure the security of information transmission and communication, has attracted a growing attention since the double random phase encoding technique was proposed by Refregier and Javidi [1] in 1995. In general, the input image is encrypted into an undistinguishable image and decrypted when received with the proper granted keys. In the past decades, various optical or digital encryption algorithms for gray images have been developed [1-4]. Some advanced techniques of optical encryption have emerged lately, such as the spatially incoherent image encryption system [5], ptychography based encryption [6] as well as asymmetric cryptosystem using random binary phase modulations [7]. Furthermore, a new and effective optical system using phase modulation with sparse representation was reported in [8], which achieves higher security by employing optical authentication method.

Color images remain however of major importance in many applications [9, 10]. Zhang and Karim [11] were the first to introduce a single-channel encryption algorithm for color image using double random phase encoding in the Fourier domain. Multiple channels encryption algorithms for color image were meanwhile investigated by applying the existing encryption algorithms for gray image on the red, green and blue channels independently. They make use, for example, of Fresnel transform [12], fractional Fourier transform [13, 14] or gyrator transform [15, 16]. Based on the quaternion theory [17], recent works introduced color image encryption algorithms in a fully vectorial form. They rely on the discrete quaternion Fourier transform [18] and the quaternion gyrator transform [19], respectively. The interest of the quaternion gyrator transform is that the presence of rotation angle enlarges the keys space and thus enhances the system security.

In addition to the aforementioned encryption algorithms for single gray or color image, multiple-image encryption algorithm capable to fuse more than one target image into a single illegible image has attracted great interest [20-37]. The superiority of multiple-image

encryption relies on the minimization of storage requirements for secret data and the improvement in transmission efficiency. Although the previous encryption algorithms for single gray or color image can be directly used for successive encryption of multiple images, the cost and the complexity of such systems will be expected to significantly increase. The drawbacks of such approach have been discussed for the double random phase (DRP) encoding technique in [25]. To surmount these deficiencies, advanced encryption algorithms for multiple images have been proposed these last years. By combining the iterative Fourier transform algorithm with the classical double random phase encryption system, Alfalou and Mansour [25] proposed a two level encryption/decryption system to encode multiple images. Meanwhile, the iterative phase retrieval algorithm for gray or binary images associated or not with other techniques in Fresnel transform domain [21-24], fractional Fourier transform domain [28-35] as well as in gyrator transform domain [36, 37] were also intensively investigated. The fractional Fourier transform is widely used due to the fact that its parameter, the fractional order, enlarges the key space. In contrast, the gyrator transform has not received so far much attention and in particular for image encryption.

Throughout the literature, however, there are few studies focused on the encryption algorithm for double or multiple color images. An encryption algorithm for double color images implemented in the fractional Fourier domain was reported in [34], where two color images were in a first step converted into their indexed formats, a data matrix and a colormap matrix. Afterwards, the encryption is implemented on both data matrices. In most cases, such method will degrade the quality of the restituted images due to the approximation made in the transformation between the RGB color space and its indexed format. The same pre-processing strategy was used for four color images encryption scheme in [35], this encryption being carried out through cascaded fractional Fourier transforms.

In this paper, our main objective is the design of a double color image encryption algorithm based on quaternion algebra. The rest of the paper is organized as follows. Section 2 briefly reviews the main features of quaternions and quaternion gyrator transform (QGT) for describing color images. In section 3, the algorithm for encryption and decryption of double color images in quaternion gyrator domain is described. Numerical simulations are reported in section 4 to demonstrate the performance of the proposed solution. Some conclusions are drawn in section 5.

2. Quaternions and Quaternion gyrator transform

2.1 Quaternions

A quaternion number can be written as: $q = a + ib + jc + kd$, where a, b, c, d are real numbers and i, j, k are orthogonal imaginary parts obeying the following rules: $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$. Any quaternion q can also be rewritten as: $q = (a + ib) + (c + id)j$. It must be noticed that the quaternion multiplication is non-exchangeable. The conjugate of q is: $\bar{q} = a - ib - jc - kd$. When $a = 0$, q becomes a pure quaternion. The quaternion q can also be expressed in polar form as: $q = |q|e^{I\theta}$, where

the norm is $|q| = \sqrt{a^2 + b^2 + c^2 + d^2}$, with $I = \dfrac{ib + jc + kd}{\sqrt{b^2 + c^2 + d^2}}$ and $\theta = \tan^{-1}\left(\dfrac{\sqrt{b^2 + c^2 + d^2}}{a}\right)$

representing the eigenaxis and the eigenangle, respectively.

An RGB image $f(x, y)$ can be represented by a pure quaternion matrix as

$$f(x, y) = if_R(x, y) + jf_G(x, y) + kf_B(x, y). \tag{1}$$

where the subscripts {R, G, B} represent the color components of the image. Based on the quaternion representation, each color pixel is encoded as a pure quaternion, thus the

correlations between them can be effectively preserved.

2.2 Quaternion gyrator transform

The gyrator transform, with rotation angle α, has been introduced by Rodrigo et al. in the field of optics [38]. Some applications have been already reported for image encryption and specific noise reduction [15, 16, 36-39]. Like the fractional Fourier transform, the gyrator transform belongs to a class of linear canonical integral transform and can be viewed as an extension of the Fourier analysis. Its advantage is also to enlarge the key space and consequently strengthen the system security. The traditional gyrator transform for gray image can be extended to quaternion domain for describing color image.

Due to the non-commutative property of quaternion multiplication, the right-side quaternion gyrator transform (QGT) with rotation angle α is defined as [19]

$$QG^{\alpha}[f(x,y)](u,v) = \frac{1}{|\sin\alpha|} \iint f(x,y) \exp\left(\mu 2\pi \frac{(uv+xy)\cos\alpha - (uy+vx)}{\sin\alpha} \right) dxdy, \qquad (2)$$

where μ is a pure unit quaternion and $\mu = (i+j+k)/\sqrt{3}$ is chosen in this paper. For $\alpha = \pi/2$, the right-side of Eq. (2) reduces to the right-side quaternion Fourier transform with the rotation of coordinates at $\pi/2$; for $\alpha = 3\pi/2$, to the inverse quaternion Fourier transform with the rotation of coordinates at $\pi/2$. The inverse quaternion gyrator transform corresponds to the QGT at angle $-\alpha$. The implementation of QGT is achieved through two left-side quaternion Fourier transforms (for more details about quaternion Fourier transform and quaternion gyrator transform, refer to [19, 40]).

3. Principle of encryption and decryption

Encryption algorithms using iterative phase retrieval technique for double gray images have been reported in [28, 37]. They consist of a series of forward and backward iterations. To deal with double color images, three groups of gray images (the color image is decomposed into red, green and blue channels and each component is viewed as a gray image) will be respectively encrypted. However, this approach does not make use of the inter-relationships between color components. It also leads to three times larger iteration loops and phase functions (e.g. the phase functions will go up to 12). Obviously, this can be a serious handicap for modern applications. Here, a novel encryption algorithm for double color images is proposed by combining the iterative phase retrieval algorithm with quaternion gyrator transform.

3.1 Description of the proposed algorithm

Without loss of generality, suppose that $f(x, y)$ and $g(x, y)$ be two color images to be encrypted, and $h(x, y)$ the ciphertext image. The phase functions ϕ_1, ϕ_2, φ_1, φ_2 and θ are distributed in the interval $[0, 2\pi]$, and assume that the following relationship between the images and the phases holds

$$h \exp(I\theta) = G^{\alpha_2}\{G^{\alpha_1}\{f \exp(\mu_{11}\phi_1)\} \exp(\mu_{12}\phi_2)\}$$
$$= G^{\beta_2}\{G^{\beta_1}\{g \exp(\mu_{21}\varphi_1)\} \exp(\mu_{22}\varphi_2)\} \qquad (3)$$

where $\mu_{11}, \mu_{12}, \mu_{21}$, and μ_{22} are the unit pure quaternions and the five phase functions are unknown at the beginning. With the expression in Eq. (3), the information of both color images can be hidden into the single image h. Hereinafter, an iterative phase retrieval algorithm is used to obtain the phase functions ϕ_1, ϕ_2, φ_1 and φ_2. According to Eq. (3), the following formula can be derived

$$g \exp(\mu_{21}\varphi_1) = G^{-\beta_1}\{G^{-\beta_2}\{G^{\alpha_2}\{G^{\alpha_1}\{f \exp(\mu_{11}\phi_1)\} \exp(\mu_{12}\phi_2)\}\} \exp(-\mu_{22}\varphi_2)\}. \qquad (4)$$

At the initialization stage, ϕ_1^1, ϕ_2^1, φ_2^1 distributed in $[0, 2\pi]$ are randomly generated. After n-th iteration, with the known of the phase functions ϕ_1^n, ϕ_2^n and φ_2^n, we define

$$\hat{g}^n = G^{-\beta_1}\{G^{-\beta_2}\{G^{\alpha_2}\{G^{\alpha_1}\{f\exp(\mu_{11}\phi_1^n)\}\exp(\mu_{12}\phi_2^n)\}\}\exp(-\mu_{22}\varphi_2^n)\}. \tag{5}$$

Then, the phase φ_1^n can be determined by

$$\varphi_1^n = \arg\{\bar{g}\cdot\hat{g}^n\} \tag{6}$$

where $\bar{g}$ is the conjugate of g, and $\arg\{\cdot\}$ denotes the phase extraction operator. Subsequently substituting the phase function φ_1^n into Eq. (4), the functions φ_2^{n+1}, ϕ_2^{n+1}, ϕ_1^{n+1} in the next iteration are updated as belows,

$$\varphi_2^{n+1} = \arg\left\{\frac{1}{G^{\beta_1}\{g\exp(\mu_{21}\varphi_1^n)\}}G^{-\beta_2}\{G^{\alpha_2}\{G^{\alpha_1}\{f\exp(\mu_{11}\phi_1^n)\}\exp(\mu_{12}\phi_2^n)\}\}\right\} \tag{7}$$

$$\phi_2^{n+1} = \arg\left\{\frac{1}{G^{\alpha_1}\{f\exp(\mu_{11}\phi_1^n)\}}G^{-\alpha_2}\{G^{\beta_2}\{G^{\beta_1}\{g\exp(\mu_{21}\varphi_1^n)\}\exp(\mu_{22}\varphi_2^{n+1})\}\}\right\} \tag{8}$$

$$\phi_1^{n+1} = \arg\left\{\bar{f}\cdot G^{-\alpha_1}\{G^{-\alpha_2}\{G^{\beta_2}\{G^{\beta_1}\{g\cdot\exp(\mu_{21}\varphi_1^n)\}\cdot\exp(\mu_{22}\varphi_2^{n+1})\}\}\cdot\exp(-\mu_{12}\phi_2^{n+1})\}\right\} \tag{9}$$

To evaluate the quality of the recovered color image with respect to the reference one and also to end the iteration, the correlation coefficient (CC) in color space is used

$$CC = \sum_{c\in\{R,G,B\}}\frac{E\{[g_c - E(g_c)][g_c^n - E(g_c^n)]\}}{3\sqrt{E\{[g_c - E(g_c)]^2\}}\sqrt{E\{[g_c^n - E(g_c^n)]^2\}}}. \tag{10}$$

where g_c^n denotes the R, G, B channels of the recovered color image at the n-th iteration step, and $E\{\cdot\}$ the expected value operator. Once the CC value, selected as the convergence criterion, reaches a predefined threshold, then the iteration process stops.

Finally, the optimized four phases are obtained as follows

$$\phi_1 = \phi_1^n, \phi_2 = \phi_2^n, \varphi_1 = \varphi_1^{n-1}, \varphi_2 = \varphi_2^n. \tag{11}$$

According to Eq. (3), the final encrypted image $h(x, y)$ is obtained by the cascaded QGT performed on color image $f(x, y)$ with rotation angles α_1, α_2 and phase functions ϕ_1, ϕ_2 as

$$h = \left|G^{\alpha_2}\{G^{\alpha_1}\{f\exp(\mu_{11}\phi_1)\}\exp(\mu_{12}\phi_2)\}\right| \tag{12}$$

Alternatively, it can be achieved by the cascaded QGT performed on color image $g(x, y)$ with rotation angles β_1, β_2 and phase functions φ_1, φ_2 as

$$h = \left|G^{\beta_2}\{G^{\beta_1}\{g\exp(\mu_{21}\varphi_1)\}\exp(\mu_{22}\varphi_2)\}\right| \tag{13}$$

As pointed in [25], a perfect encryption algorithm should parallel a decryption algorithm to allow us retrieving the secret information by means of the granted keys as a receiver. In other words, the encryption algorithm should be reversible. In the proposed encryption algorithm, the accompanied phase function θ can be considered as the public key. The rotation angles α_1, α_2 and the phase masks ϕ_1, ϕ_2 are private keys for recovering the color image $f(x, y)$, while the angles β_1, β_2 and the phase masks φ_1, φ_2 are private keys for recovering the color image $g(x, y)$. The parameters μ, μ_{11}, μ_{12}, μ_{21}, μ_{22} can be viewed as auxiliary keys. With the above known essential keys, the two target color images $f(x, y)$ and $g(x, y)$ can be restituted by implementing the inverse encryption algorithm process as follows

$$f = G^{-\alpha_1}\{G^{-\alpha_2}\{h\exp(I\theta)\}\exp(-\mu_{12}\phi_2)\}\exp(-\mu_{11}\phi_1). \tag{14}$$

$$g = G^{-\beta_1}\{G^{-\beta_2}\{h\exp(I\theta)\}\exp(-\mu_{22}\varphi_2)\}\exp(-\mu_{21}\varphi_1). \tag{15}$$

3.2 Complexity analysis

The computational complexity of the proposed encryption algorithm will be analyzed next. It depends on two main factors. First, to extract each phase function in the n-th loop, the quaternion gyrator transform and its inverse transform must be computed four times. Here, the left-side quaternion Fourier transform is obtained via the 2D fast complex-valued Fourier transform [40] and introduced into the calculation of quaternion gyrator transform. For an image with size $M \times N$, the computation complexity of the 2D fast Fourier transform has been shown to be $O(MN\log_2 MN)$ [23]. The second factor is the number of iterations. It has been set to 1000 in all experiments, a value considered as a good balance between time computation and accuracy in image recovery. In short, the computation load depends largely upon the image size and the iteration number.

4. Numerical simulation results

To corroborate the validity and the effectiveness of the proposed encryption algorithm, numerical simulations were carried out on a computer with Intel Core2 Duo CPU E8400@3.00GHz and 3G DRAM and with the MATLAB 2011a. The tested color images selected from USC-SIPI image database [41] consist of four groups as shown in Fig. 1, all with size 256×256. The system parameters are $\mu_{lm} = (i+k)/\sqrt{2}$ (l, m = 1, 2), α_1=0.16, α_2=0.25, β_1=0.21, β_2=0.45 (other values can be selected). The normalized mean square error (NMSE) [12, 36] were used to evaluate the similarity between the decrypted image $\hat{f}(x,y)$ and its reference $f(x,y)$, which is defined by

$$\text{NMSE} = \frac{\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}\left|f(x,y)-\hat{f}(x,y)\right|^2}{\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}\left|f(x,y)\right|^2}. \tag{16}$$

Simulations have been done first to test the security and the reversibility of the algorithm. The four phase functions for each tested group were obtained after 1000 iteration loops. The evolution of CC values is displayed in Fig. 2, where the images in the upper row and the lower row for each tested group shown in Fig. 1 are respectively used as the reference image to terminate the iteration in the phase retrieval process. Table 1 lists the NMSE values of decrypted images, where all the images in the lower row are used as reference image to obtain the four phases. It should be noted that for any tested group, four sets of decrypted results can be obtained due to the fact that each of them can be used as the reference to determine the convergence or for encryption. From the results of table 1, it can be observed that for each tested group, the error of the first decrypted image is larger due to the fact that the encpted data h obtained from the second tested image $g(x, y)$ is used as the public keys. When using Eq. (12), the error of the second decrypted image will be larger which is caused by the smaller residual error when obtaining phase functions by means of the phase retrieval algorithm. Figure 3 shows the results of encryption and granted decryption of the first tested group (Lena and Pepper). It can be seen that with the knowledge of the granted keys, the original color images can be restituted with a high quality. In contrast, without knowing the rotation angles or phase functions, almost no useful information can be recovered from the decrypted results, as demonstrated in Fig. 4.
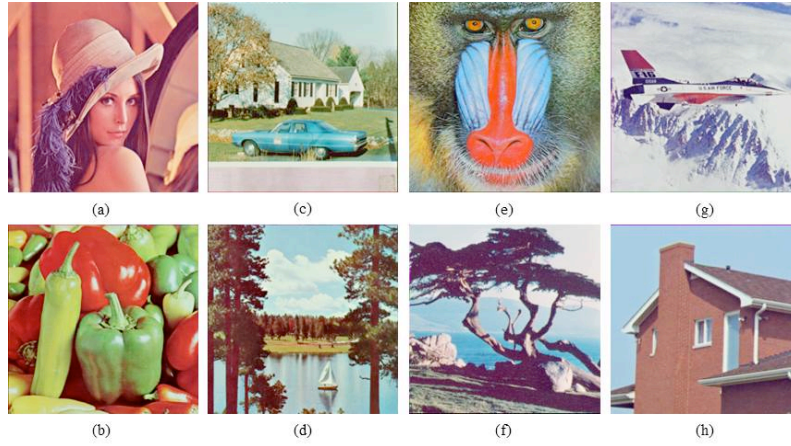
Fig. 1. Tested color images: each column constitutes a tested group (Primary color images are selected from USC-SIPI image database).

Table 1. NMSE values of decrypted images with granted keys

Images	Fig. 1 (a)	Fig. 1 (b)	Fig. 1 (c)	Fig. 1 (d)	Fig. 1 (e)	Fig. 1 (f)	Fig. 1 (g)	Fig. 1 (h)
NMSE	1.59e-2	3.74e-30	3.36e-2	3.67e-30	2.32e-2	3.64e-30	4.38e-2	3.59e-30
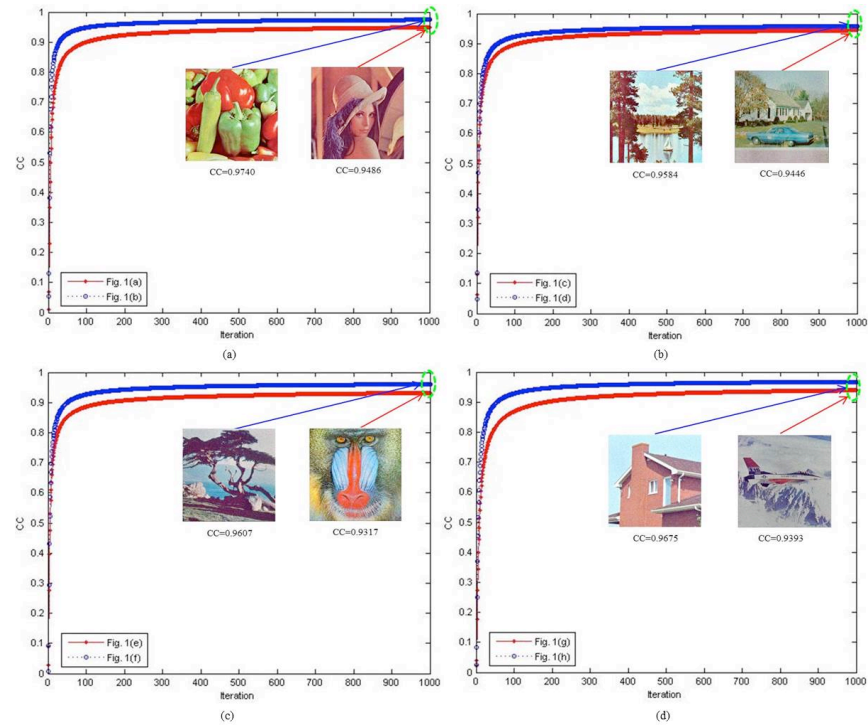
Fig. 2. The evolution of CC values over the 1000 iteration loops.

Fig. 3. Examples of encryption and granted decryption for double color images: (a) encrypted image; (b) and (c), decrypted results.
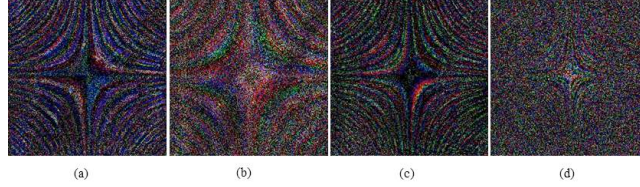
Fig. 4. Decrypted results with randomly guessed keys: (a) and (b) correspond to Lena, (c) and (d) correspond to Pepper: (a) and (c) correspond to phases randomly guessed, (b) and (d) correspond to angles randomly guessed.

In order now to test the sensitivity of rotation angles to small changes, the decryption was performed by fixing one angle value and by varying the other, where the deviation Δ ranges from -0.10 to 0.10 with step 0.005. Others keys used for encryption and decryption in this simulation are set to the correct values. From the NMSE values shown in Fig. 5, it can be concluded that when the deviation is equal or greater than 0.01, the decrypted images (for brevity not displayed here) cannot be recognized clearly. Therefore, the rotation angles of QGT are sensitive keys.
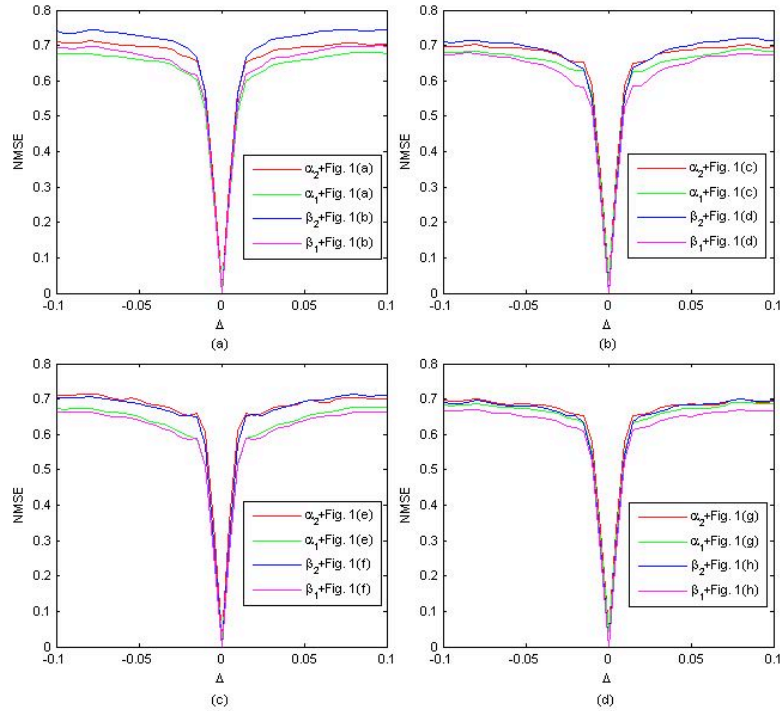

Fig. 5. The NMSE values of decrypted images when varying one rotation angle while the other

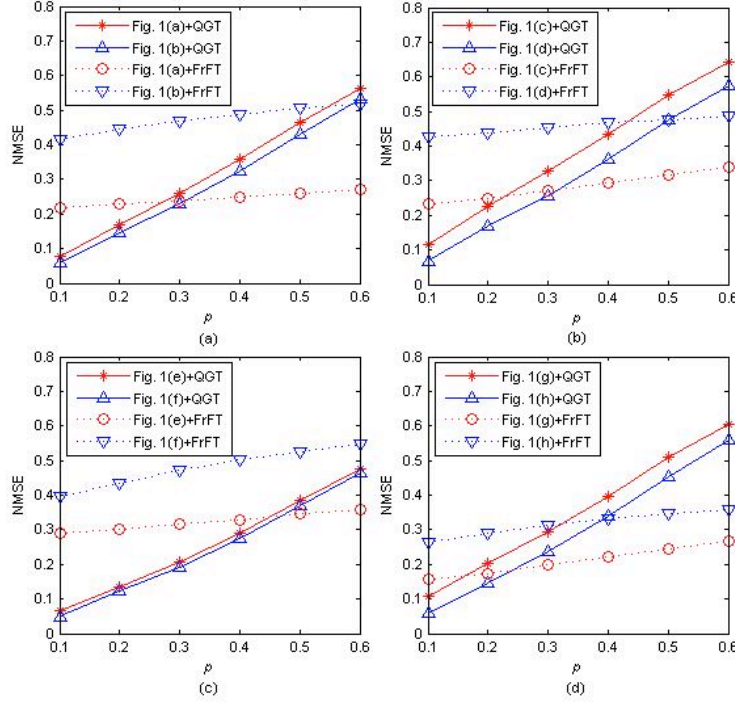keys are set to the right value.

Fig. 6. The NMSE values of decrypted images with different information loss severities.

Fig. 7. Decrypted results of encrypted data with 50% information loss.

During data transmission, information loss or noise contamination may occur. Another simulation was carried out so as to evaluate the performance of the proposed encryption algorithm against loss of data. To demonstrate the interest of the present encryption algorithm for double color images, a comparison with the encryption algorithm based on fractional Fourier transforms (FrFT) [34] is provided. To do so, the information loss severity p (varying from 10% to 60% with an increment 10%) around the center is regarded as an occlusion attack to the encrypted data. From the results illustrated in Fig. 6, it can be seen that the NMSE values of the FrFT-based encryption algorithm are more stable. However, the NMSE values of the present algorithm evolve linearly with the percentage p. When increasing the occlusion percentage p, the similarity between recovered image and its original one becomes obviously smaller. This behavior can be explained by the fact that a significant part of the QGT information is distributed around the image center considered as the origin. Although the NMSE values of the FrFT-based encryption algorithm are smaller in some limited intervals, we found that no useful information can be recovered from the decrypted image even when the smallest occlusion percentage 10% is used in reduplicative experiments. Conversely, as displayed in Fig. 7, relevant decrypted information can be obtained when using the proposed algorithm for p values up to 50%. In other words, the proposed encryption

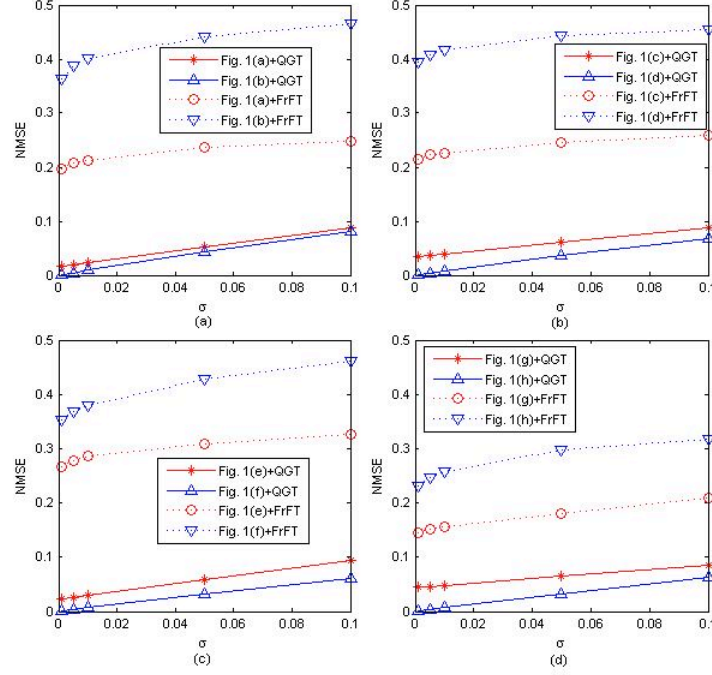algorithm shows more robustness against loss of encrypted data.

Fig. 8. The NMSE values of decrypted images with different Gaussian white noise using different encryption algorithms.
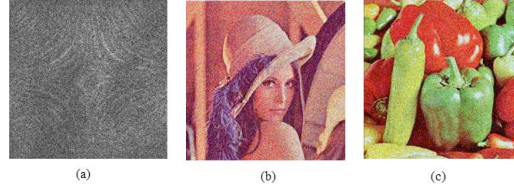

Fig. 9. Examples of decrypted images from noisy encrypted data with standard deviation 0.05.

In order to test the robustness of our approach against noise attack, a white Gaussian noise with zero mean and varying standard deviations σ was added to the four tested group images. The same noise was added to the encrypted images obtained with fractional Fourier transforms [34] for comparison purpose. Fig. 8 displays the NMSE values of the decrypted images from these noisy encrypted images with the FrFT-based and the QGT-based encryption algorithm. The NMSE values corresponding to the proposed algorithm are much smaller. Two examples of the resulting decrypted images are shown in Fig. 9, where the noise standard deviation is 0.05. It can be concluded that the proposed encryption algorithm shows here also more robustness against noise.

5. Conclusion

A novel double color image encryption algorithm was presented in this paper. The originality stands on the holistic representation for color image by using quaternion algebra and iterative phase retrieval algorithm in quaternion gyrator domain. The phase masks used for encryption are obtained through iterative phase retrieval algorithm in quaternion gyrator domain, and the encrypted image is obtained via cascaded quaternion gyrator transforms. Knowing all the

granted keys, as the parameters of quaternion gyrator and phases, two color images can be restituted with a high quality. The results of the numerical simulations have demonstrated the feasibility and the effectiveness of the proposed encryption system. When compared with the double color images encryption algorithm in the fractional Fourier domain, the proposed encryption algorithm has shown a better robustness to occlusions and additive Gaussian noise. It must be also emphasized that, when both color images need to be encrypted for the FrFT-based encryption algorithm, our encryption approach only requires to encrypt one image, and thus provides savings in data storage while improving the transmission efficiency. To further reinforce the encryption system, other techniques such as sparse representation will be taken into consideration in the near future. In addition, the proposed encryption algorithm can also be extended to encrypt multiple gray or colored images.

References and links

1. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**(7), 767-769 (1995).
2. S. T. Liu, L. Yu, and B. H. Zhu, "Optical image encryption by cascaded fractional Fourier transforms with random phase filtering," Opt. Commun. **187**(1-3), 57-63 (2001).
3. B. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," Opt. Lett. **28**(4), 269-271 (2003).
4. N. K. Nishchal, J. Joseph, and K. Singh, "Securing information using fractional Fourier transform in digital holography," Opt. Commun. **235**(4-6), 253-259 (2004).
5. J. L. Zang, Z. W. Xie, and Y. Zhang, "Optical image encryption with spatially incoherent illumination," Opt. Lett. **38**(8), 1289-1291 (2013).
6. Y. S. Shi, T. Li, Y. L. Wang, Q. K. Gao, S. G. Zhang, and H. F. Li, "Optical image encryption via ptychography," Opt. Lett. **38**(9), 1425-1427 (2013).
7. W. Liu, Z. J. Liu, and S. T. Liu, "Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm," Opt. Lett. **38**(10), 1651-1653 (2013).
8. W. Chen, X. D. Chen, A. Stern, and B. Javidi, "Phase-modulated optical system with sparse representation for information encoding and authentication," IEEE Photonics J. **5**(2), 6900113 (2013).
9. M. J. Swain and D. H. Ballard, "Color indexing," Int. J. Computer. Vision **7**(1), 11-32 (1991).
10. T. Gevers and A. W.M. Smeulders, "Color-based object recognition," Pattern Recogn. **32**(3), 453-464 (1999).
11. S. Q. Zhang and M. A. Karim, "Color image encryption using double random phase encoding," Microwave Opt. Technol. Lett. **21**(5), 318-323 (1999).
12. L. F. Chen and D. M. Zhao, "Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms," Opt. Express **14**(19), 8552-8560 (2006).
13. L. F. Chen and D. M. Zhao, "Color information processing (coding and synthesis) with fractional Fourier transforms and digital holography," Opt. Express **15**(24), 16080-16089 (2007).
14. L. S. Sui, M. T. Xin, A. L. Tian, and H. Y. Jin, "Single-channel color image encryption using phase retrieve algorithm in fractional Fourier domain," Opt. Lasers Eng. **51**, 1297-1309 (2013).
15. M. R. Abuturab, "Color image security system using double random-structured phase encoding in gyrator transform domain," Appl. Opt. **51**(15), 3006-3016 (2012).
16. L. S. Sui and B. Gao, "Color image encryption based on gyrator transform and Arnold transform," Opt Laser Technol, **48**, 530-538 (2013).
17. W. R. Hamilton, *Elements of Quaternions* (Longmans Green, 1866).

18. X. L. Wang, H. C. Zhai, Z. L. Li, and Q. Ge, "Double random-phase encryption based on discrete quaternion Fourier-transforms," Optik **122**(20), 1856-1859 (2011).

19. Z. H. Shao, J. S. Wu, J. L. Coatrieux, G. Coatrieux, and H. Z. Shu, "Quaternion gyrator transform and its application to color image encryption," in *Proceedings of IEEE International Conference on Image Processing* (Institute of Electrical and Electronics Engineers, New York, 2013), pp. 4579-4582.

20. G. H. Situ and J. J. Zhang, "Multiple-image encryption by wavelength multiplexing," Opt. Lett. **30**(11), 1306-1308 (2005).

21. Y. S. Shi, G. H. Situ, and J. J. Zhang, "Multiple-image hiding in the Fresnel domain," Opt. Lett. **32**(13), 1914-1916 (2007).

22. H. Hwang, H. T. Chang, and W. Lie, "Multiple-image encryption and multiplexing using a modified Gerchberg-Saxton algorithm and phase modulation in Fresnel-transform domain," Opt. Lett. **34**(24), 3917-3919 (2009).

23. H. T. Chang, H. Hwang, and C. Lee, "Position multiplexing multiple-image encryption using cascaded phase-only masks in Fresnel transform domain," Opt. Commun. **284**(18), 4146-4151 (2011).

24. H. T. Chang, H. E. Hwang, C. L. Lee, and M. T. Lee, "Wavelength multiplexing multiple-image encryption using cascaded phase-only masks in the Fresnel transform domain," Appl. Opt. **50**(5), 710-716 (2011).

25. A. Alfalou and A. Mansour, "Double random phase encryption scheme to multiplex and simultaneous encode multiple images," Appl. Opt. **48**(31), 5933-5947 (2009).

26. X. P. Deng and D. M. Zhao, "Multiple-image encryption using phase retrieve algorithm and intermodulation in Fourier domain," Opt. Laser Technol. **44**(2), 374-377 (2012).

27. X. G. Wang and D. M. Zhao, "Fully phase multiple-image encryption based on superposition principle and the digital holographic technique," Opt. Commun. **285**, 4280-4284 (2012).

28. L. S. Sui, M. T. Xin, and A. L. Tian, "Multiple-image encryption based on phase mask multiplexing in fractional Fourier transform domain," Opt. Lett. **38**(11), 1996-1998 (2013).

29. D. Z. Kong, X. J. Shen, Q. Z. Xu, W. Xin, and H. Q. Guo, "Multiple-image encryption scheme based on cascaded fractional Fourier transform," Appl. Opt. **52**(12), 2619-2625 (2013).

30. R. Tao, Y. Xin, and Y. Wang, "Double image encryption based on random phase encoding in the fractional Fourier domain," Opt. Express **15**(24), 16067-16079 (2007).

31. Z. J. Liu and S. T. Liu, "Double image encryption based on iterative fractional Fourier transform," Opt. Commun., **275**(2), 324-329 (2007).

32. Z. J. Liu, J. M. Dai, X. G. Sun, and S. T. Liu, "Triple image encryption scheme in fractional Fourier transform domains," Opt. Commun. **282**(4), 518-522 (2009).

33. J. H. Wu, X. Z. Luo, and N. R. Zhou, "Four-image encryption method based on spectrum truncation, chaos and the MODFrFT," Opt. Laser Technol. **45**, 571-577 (2013).

34. M. Joshi, C. Shakher, and K. Singh, "Color image encryption and decryption for twin images in fractional Fourier domain," Opt. Commun. **281**(23), 5713-5720 (2008).

35. M. Joshi, C. Shakher, and K. Singh, "Fractional Fourier transform based image multiplexing and encryption technique for four-color images using input images as keys," Opt. Commun. **283**(12), 2496-2505 (2010).

36. Z. J. Liu, Q. Guo, L. Xu, M. A. Ahmad, and S. T. Liu, "Double image encryption by using iterative random binary encoding in gyrator domains," Opt. Express **18**(11), 12033-12043 (2010).

37. H. J. Li and Y. R. Wang, "Double-image encryption based on iterative gyrator transform," Opt. Commun. **281**(23), 5745-5749 (2008).

38. J. A. Rodrigo, T. Alieva, and M. L. Calvo, "Gyrator transform: properties and applications," Opt. Express **15**(5), 2190-2203 (2007).

39. J. A. Rodrigo, T. Alieva, and M. L. Calvo, "Applications of gyrator transform for image processing," Opt. Commun. **278**(2), 279-284 (2007).

40. S. Said, N. L. Bihan, and S. J. Sangwine, "Fast complexied quaternion Fourier transform," IEEE Trans. Signal Process. **56**(4), 1522-1531 (2008).

41. Original color images: http://sipi.usc.edu/database/database.php.