AWERProcedia Information Technology & Computer Science

Vol 03 (2013) 732-739

3rd World Conference on Information Technology (WCIT-2012)

Single-channel Color Image Encryption Based on Iterative Fractional Fourier Transform

Sui Liansheng *, School of Computer Science and Engineering, Xi'an University of Technology, Xi'an, 710048, China.

Gao Bo, School of Computer Science and Engineering, Xi'an University of Technology, Xi'an, 710048, China.

Wang Wengang, School of Computer Science and Engineering, Xi'an University of Technology, Xi'an, 710048, China.

Suggested Citation:

Liansheng, S., Bo, G. & Wengang, W. Single-channel Color Image Encryption Based on Iterative Fractional Fourier Transform, *AWERProcedia Information Technology & Computer Science*. [Online]. 2013, 4, pp 732-739. Available from: <http://www.world-education-center.org/index.php/P-ITCS> *Proceedings of 3rd World Conference on Information Technology (WCIT-2012)*, 14-16 November 2012, University of Barcelona, Barcelona, Spain.

Received 19 March, 2013; revised 6 July, 2013; accepted 23 September, 2013.

Selection and peer review under responsibility of Prof. Dr. Hafize Keser.

©2013 Academic World Education & Research Center. All rights reserved.

Abstract

A single-channel color image encryption is proposed based on iterative fractional Fourier transform. The color image to be encrypted is first separated into three independent channels: red, green and blue. Then, the red and green components are encrypted into a single one based on iterative fractional Fourier transform. Similarly, the interim image and blue component are encrypted into the final gray scale ciphertext with stationary white noise distribution, which has camouflage property to some extent. In the process of encryption and decryption, three different groups of fractional orders, five private phase functions and one common phase function are used as keys to enhance the security of the proposed system. Additionally, the proposed iterative fractional Fourier transform algorithm has faster convergent speed. Simulation results verify the feasibility and effectiveness of this method.

Keywords: Color image encryption; iterative fractional Fourier transform; single-channel;

* ADDRESS FOR CORRESPONDENCE: **Sui Liansheng**, School of Computer Science and Engineering, Xi'an University of Technology, Xi'an, 710048, China, E-mail address: liudua2010@gmail.com / Tel.: +0-86-29-82312884

1. Introduction

With the issues about illegal data access on internet being more and more serious, information security, especially image information security, has attracted a lot of attention. Because of high speed for processing two dimensional data in parallel, optical encryption techniques have become an important field for information security. In the past two decades, researchers have proposed various methods for image encryption based on different domain such as fractional Fourier transform (FrFT) domain, Fresnel transform domain and Gyrator transform domain [1

The rest of this article is organized as follows. In Section 2, the basic principles are introduced in detail. In Section 3, numerical simulation results are given. Finally, the conclusion is given in Section 4.

1. Encryption and decryption process

1.1. Iterative fractional Fourier transform

The fractional Fourier transform at order α of a two-dimensional function $f(x_i, y_i)$ can be expressed as

$$f_0(x_0, y_0) = \mathcal{F} \{ f_i(x_i, y_i) \} (x_0, y_0) = \mathcal{H}(x_i, y_i; x_0, y_0) f(x_i, y_i) dx_i dy_i,$$

where (x_i, y_i) and (x_0, y_0) indicates the input and output coordinates respectively, and the transform kernel is denoted as

$$\mathcal{H}(x_i, y_i; x_0, y_0) = A \exp i \left(\frac{x_i^2 + y_i^2 - x_0^2 - y_0^2}{2} \cot \phi - 2(x_i x_0 + y_i y_0) \csc \phi \right), \tag{2}$$

$$A = \frac{\exp[i \operatorname{sgn}(\sin \phi) / 2]}{|\sin \phi|}. \tag{3}$$

The A_ϕ is a trivial phase parameter and $\phi_\alpha = \alpha\pi/2$ is the transform angle. The FrFT is linear and has the property that it is index additive

$$\mathcal{F} \{ \mathcal{F} [f(x, y)] \} = \mathcal{F} [f(x, y)]. \tag{4}$$

In addition, the FrFT is additive, the

$$\angle \left\{ \frac{\mathcal{F}^{-2} \{ \mathcal{F}^{-1} \{ g \exp(i \frac{k}{2}) \} \exp(i \frac{k}{2}) \}}{\mathcal{F}^{-1} \{ f \exp(i \frac{k}{2}) \}} \right\}, \quad (11)$$

$$\angle \left\{ \mathcal{F}^{-1} \{ \mathcal{F}^{-2} \{ \mathcal{F}^{-1} \{ g \exp(i \frac{k}{2}) \} \exp(i \frac{k}{2}) \} \exp(i \frac{k}{2}) \} \}. \quad (12)$$

In order to decide when the iteration may stop, the correlation coefficient (CC) or the mean square error (MSE) between the iterated image and the original one is used as convergent criterion. These criterion are expressed as

$$CC = \frac{E\{[g - E[g]][g^k - E[g^k]]\}}{\sqrt{E\{[g - E[g]]^2\}} \sqrt{E\{[g^k - E[g^k]]^2\}}} \quad (13)$$

$$MSE = \frac{\sum_{m=1}^M \sum_{n=1}^N |g - g^k|^2}{M \cdot N}, \quad (14)$$

where g and g_k denote the original image and the iterated one, and $E\{\cdot\}$ denotes the expected value operator. In the process of iteration, if CC is larger than a predefined threshold which is close to 1 or MSE is lower than a predefined threshold which is close to 0, the iterative phase retrieval algorithm ends. Suppose the number of iteration is N , then we can obtain the optimized phase functions and encrypted image as follows

$$\phi_1 = \angle \{ \hat{g}^N \}, \quad \phi_2 = \angle \{ \hat{h}^N \}, \quad (15)$$

$$\phi_1 = \angle \{ \hat{g}^N \}, \quad \phi_2 = \angle \{ \hat{h}^N \}, \quad (16)$$

$$\angle \{ \hat{g}^N \}, \quad h = \text{amplitude} \{ \hat{g}^N \}. \quad (17)$$

where $\angle\{\cdot\}$ and $\text{amplitude}\{\cdot\}$ denote the phase and amplitude extraction operator respectively. The fractional orders α_1 , α_2 and β_1 , β_2 , ϕ_2 and φ_2 are regarded as private keys, and the phase ψ is regarded as common key. In decryption, with the common and private keys, encrypted image and FrFT, the original images can be obtained by

$$f = \text{amplitude} \{ \mathcal{F}^{-1} \{ \mathcal{F}^{-2} \{ h \exp(i \frac{\psi}{2}) \} \exp(i \frac{\psi}{2}) \} \}, \quad (18)$$

$$g = \text{amplitude} \{ \mathcal{F}^{-1} \{ \mathcal{F}^{-2} \{ h \exp(i \frac{\psi}{2}) \} \exp(i \frac{\psi}{2}) \} \}. \quad (19)$$

1.2. Color image encryption and decryption algorithm

The proposed single-channel color image encryption and decryption is based on iterative FrFT. The encryption process is shown in Fig. 2. Supposing the size of the plain color image is $M \times N$ pixels, the encryption algorithm is described as follows

Step 1: In the image decomposition module, we decompose the color image to be encrypted into red, green and blue channels, which are denoted by I_R , I_G and I_B respectively.

Step 2: In the module for encrypting I_R and I_G into a single one, we firstly set up the relationship between I_R and I_G by using Eq. (6), and then carry out the iterative phase retrieval algorithm by using Eq. (7) - (12). The convergent criterion is set to a MSE threshold. When the MSE is lower than the threshold, we end iteration process and compute the optimized phase functions and encrypted image by using Eq. (15) - (17). In the process of iterative FrFT, the fractional orders α_1 , α_2 is used for I_R , and β_1 , β_2 for I_G . In this module, two phase functions P_R and P_G are obtained as private keys. In addition, the important output is the complex image $\hat{g}_{RG}$, which is used to compute the phase function P_{RG} as common key by using $\angle\{\cdot\}$ and the encrypted interim image I_{RG} by using $\text{amplitude}\{\cdot\}$.

Step 3: In the module for encrypting I_{RG} and I_B , the encryption process is similar to encrypting I_R and I_G . The fractional orders γ_1 , γ_2 for I_{RG} , and $\alpha_1 + \beta_1$, $\alpha_2 + \beta_2$ is used for I_{RG} . Finally, two phase functions P_{RGB} and P_B are obtained as private keys. The complex image $\hat{g}_{RGB}$ is used to compute the phase function P_{final} as common key by using $\angle\{\cdot\}$ and the final ciphertext image I_{RGB} by using $\text{amplitude}\{\cdot\}$.

Fig. 2. Flowchart of encryption process.

Compared with the encryption, the decryption process is relatively simple as shown in Fig. 3. Obviously, it includes four groups of FrFT used for obtaining the components I_B , I_{RG} , I_R and I_G . In FrFT with fractional orders $-\gamma_2$ and $-\gamma_1$, we firstly constitute a complex image $I_{RGB} \exp(iP_{final})$ with the ciphertext I_{RGB} and common key P_{final} . Secondly, we carry out FrFT with the fractional order $-\gamma_2$ to $I_{RGB} \exp(iP_{final})$ and multiply the result by $\exp(-iP_2)$. Finally, we carry out FrFT with the fractional order $-\gamma_1$ to the result and use $amplitude\{\cdot\}$ to extract the amplitude of the final complex image as I_B . Similarly, we can obtain I_{RG} which is used to extract I_R and I_G . Finally, we use I_R , I_G and I_B to recover the original color image.

Fig. 3. Flowchart of decryption process

In the process of encryption and decryption, there are two common keys P_{RG} and P_{final} . The phase function P_{RG} only is common key between I_R and I_G . In order to increase security, we substitute P_{RG} with $P_{final} - P_{RG}$ as a private key. Thus, there are five private keys and one common key in the process of iterative FrFT. With three groups of fractional orders, the cryptosystem enlarge the key space greatly.

2. Numerical simulation

Fig. 4. (a) Image “Lena”, (b) Ciphertext image, (c) Common phase distribution, (d) Decrypted image with correct keys.

We carry out the proposed algorithm on the color image “Lena” with 256×256 pixels shown in Fig. 4 (a). Three groups of fractional orders are set as $\alpha_1 = 0.2$, $\alpha_2 = \alpha_1 + 0.5$, $\beta_1 = \alpha_1 + 0.1$, $\beta_2 = \alpha_2 + 0.1$, $\gamma_1 = \alpha_1 + 0.2$ and $\gamma_2 = \alpha_2 + 0.2$. The *MSE* threshold is set to 1.0e-9. The ciphertext image and the common phase distributions are shown in Fig. 4 (b) and (c) respectively. The decrypted image with all correct keys is shown in Fig. 4 (d). When encrypting red, green and blue components into a single one, the iterative FrFT algorithm has fast convergent speed. After 25 iterations, the *MSE* values are lower than 1.0e-10 in these two iterative FrFT process.

Fig. 5 shows the decrypted images with incorrect keys. Fig. 5 (a) displays the decrypted image with the incorrect fractional order α_1 while other keys are correct. Fig. 5 (b) displays the decrypted image only with the incorrect common phase function P_{final} .

Fig. 5. Decrypted image with (a) incorrect order $\alpha_1 = 0.21$, (b) incorrect common phase P_{final} .

3. Conclusion

In summary, we have proposed a single-channel algorithm to encrypt a color image into a gray scale ciphertext based on iterative FrFT. The original image fails to be recovered unless all of the correct keys including the fractional orders and the phase functions are known. The proposed cryptosystem has high convergent speed in the process of iterative FrFT. Moreover the proposed cryptosystem is a single-channel encryption system for color image which is more convenient than conventional three-channel encryption systems. A set of numerical simulations have illustrated the feasibility and effectiveness of the proposed algorithm.

Acknowledgements

This work was supported by Foundation of Shaanxi Education Department of Shaanxi Province under grant 11JK1032.

References

- [1] Unnikrishnan G, Joseph J, Singh K. Optical encryption by double-random phase encoding in the fractional Fourier domain. *Opt Lett* 2000; 25: 887-889.
- [2] Liu S, Yu L, Zhu B. Optical image encryption by cascaded fractional Fourier transforms with random phase filtering. *Opt Commun* 2001; 187:57-63.
- [3] Zhu B, Liu S, Ran Q. Optical image encryption based on multifractional Fourier transforms. *Opt Lett* 2000; 25:1159-1161.
- [4] Hennelly B, Sheridan J T. Optical image encryption by random shifting in fractional Fourier domains. *Opt Lett* 2003; 28: 269-271.
- [5] Nischal N K, Joseph J, Singh K. Securing Information Using Fractional Fourier Transform in Digital Holography. *Opt Commun* 2004; 235: 253-259.
- [6] Li H J, Wang Y R. Double-image encryption based on iterative gyrator transform. *Opt Commun* 2008; 281: 5745-5749.
- [7] Liu Z J, Liu S T. Double image encryption based on iterative fractional Fourier transform. *Opt Commun* 2007; 275: 324-329.
- [8] Chen L F, Zhao D M. Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms. *Opt Express* 2006; 14: 8552-8560.
- [9] Chen L F, Zhao D M. Color information processing (coding and synthesis) with fractional Fourier transforms and digital holography. *Opt Express* 2007; 15: 16080-16089.
- [10] Joshi M, Shakher C, Singh K. Color image encryption and decryption using fractional Fourier transform. *Opt Commun* 2007; 279: 35-42.
- [11] Joshi M, Shakher C, Singh K. Logarithms-based RGB image encryption in the fractional Fourier domain: A non-linear approach. *Opt Lasers Eng* 2009; 47: 721-727.
- [12] Chen W, Quan C, Tay C J. Optical color image encryption based on Arnold transform and interference method. *Opt Commun* 2009; 282: 3680-3685.
- [13] Liu Z J, Xu L, Liu T, Chen H, Li P F, Lin C, Liu S T. Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. *Opt Commun* 2011; 284: 123-128.
- [14] Muhammad R A. Color information security system using discrete cosine transform in gyrator transform domain radial-Hilbert phase encoding. *Opt Lasers Eng* 2012; 50: 1209-1216.
- [15] Muhammad R A. Securing color information using Arnold transform in gyrator transform domain. *Opt Lasers Eng* 2012; 50: 772-779.
- [16] Hwang H E. Optical color image encryption based on the wavelength multiplexing using cascaded phase-only masks in Fresnel transform domain. *Opt Commun* 2012; 285: 567-573.
- [17] Liu H J, Wang X Y. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Opt Commun* 2011; 284: 3895-3903.
- [18] Chen W, Chen X D. Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain. *Opt Commun* 2011; 284: 3913-3917.

- [19] Zhou N R, Wang Y X, Gong L H, He H, Wu J H. Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform. *Opt Commun* 2011; 284: 2789-2796.
- [20] Zhou N R. Wang Y X, Gong L H, Chen X B, Yang Y X. Novel color image encryption algorithm based on the reality preserving fractional Mellin transform. *Opt Laser Tech* 2012; 44: 2270-32281.
- [21] Deng X P, Zhao D M. Single-channel color image encryption based on asymmetric cryptosystem. *Opt Laser Tech* 2012; 44: 136-140.