Int. J. Communications, Network and System Sciences, 2014, 7, 114-121
Published Online April 2014 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2014.74013

Color Information Encoding Based on Phase-Truncated Gyrator Transform Domain

Muhammad Rafiq Abuturab[1]*, Tajuddin Ali Ahmad[2]

[1]Department of Physics, Maulana Azad College of Engineering and Technology, Patna, India
[2]Department of Electronics and Communication Engineering, Maulana Azad College of Engineering and Technology, Patna, India
Email: *rafiq.abuturab@gmail.com

Received 16 February 2014; revised 16 March 2014; accepted 30 March 2014

Abstract

A color information encryption method using phase-truncated gyrator transform domain is proposed. In this technique, the color image is decomposed into R, G and B channels. The decomposed three RBG channels evade the interference of crosstalks efficiently. Each channel is separately modulated to the first random phase mask and then gyrator transformed. The transformed image is phase-truncated to get first encoded image and amplitude-truncated to produce first asymmetric phase key. The obtained image is modulated to the second random phase mask and then again gyrator transformed. The resulted image is phase-truncated to obtain second encoded image and amplitude-truncated to generate second asymmetric phase key. The proposed system includes transformation angles of GT and asymmetric phase keys as decryption keys. The proposed system can be implemented digitally or optically. The optical setup is free from optical misalignment problem. The theoretical analysis and numerical simulation results both validate the proposed technique.

Keywords

Asymmetric Cryptosystem, Gyrator Transform

1. Introduction

Optical cryptography techniques have emerged as one of the next generation technologies, in which optical image

*Corresponding author.

How to cite this paper: Abuturab, M.R. and Ahmad, T.A. (2014) Color Information Encoding Based on Phase-Truncated Gyrator Transform Domain. *Int. J. Communications, Network and System Sciences*, **7**, 114-121.
http://dx.doi.org/10.4236/ijcns.2014.74013

encryption techniques have been widely studied because of their inherent advantages of high-speed and parallel-optical signal processing. Refregier and Javidi first proposed a double random phase encoding (DRPE) based on the 4-*f* optical correlator to encode an input image into stationary white noise [1]. Since then, various subsequent DRPE based optical encryption schemes have been introduced [2]-[6]. In all these image encryption techniques, as a monochromatic light is used to illuminate a real color image, color information is lost during decryption process. Since color images provide more information than gray scale images and also the additional color information contribute to a higher level of security. Zhang and Karim proposed a color encryption method based on an indexed image and DRPE [7]. The color image encryption techniques have been further extended [8]-[11]. However, the above proposed optical encryption techniques belong to the category of symmetric cryptosystems, in which the encryption keys are identical to the decryption keys. Qin and Peng proposed an asymmetric cryptosystem based on a phase-truncated Fourier transform (PTFT) to remove the linearity of the DRPE [12]. Recently, the PTFT-based encryption method has been found to be vulnerable to a specific attack based on iterative Fourier transforms, when the two random phase masks (RPMs) are used as public keys to encrypt different plaintexts [13]. The PTFT-based cryptosystem has been researched to resist against specific attack [14]-[16].

In this paper, for the first time, to our knowledge, a new asymmetric color image cryptosystem based on gyrator transform (GT) domain is proposed. In this method, the color image is divided into R, G and B channels. Each of these channels is independently attached to the first RPM placed at the image plane and then gyrator transformed. The transformed image is phase-truncated to get first encoded image and amplitude-truncated to produce first decryption phase key. The transformed image is attached to the second RPM placed at the gyrator transform plane and then again gyrator transformed. The resulted image is phase-truncated to get second encoded image and amplitude-truncated to generate second decryption phase key. The proposed system provides transformation angles of GT as additional keys and decryption phase keys as asymmetric keys. Consequently, a high robustness against existing attacks can be achieved. Numerical simulations show the validity and viability of the proposed technique.

2. Gyrator Transform

The gyrator transform (GT) is defined as a linear canonical transform which produces the twisted rotation in position-spatial frequency planes of phase space. Thus, the GT operation of a two-dimensional function $f_i(x_i, y_i)$ with parameter α, known as transformation angle, is defined as [17]

$$\begin{aligned} f_o(x_o, y_o) &= G^{\alpha}\left[f_i(x_i, y_i)\right](x_o, y_o) \\ &= \frac{1}{|\sin\alpha|}\int\int_{-\infty}^{+\infty} f_i(x_i, y_i)\exp\left(i2\pi\frac{(x_o y_o + x_i y_i)\cos\alpha - (x_i y_o + x_o y_i)}{\sin\alpha}\right)\mathrm{d}x_i\mathrm{d}y_i \end{aligned} \tag{1}$$

where G^{α} denotes gyrator transform operator, (x_i, y_i) and (x_o, y_o) are the input and output coordinates, respectively. The GT can be realized by an optimized flexible optical system having plano-convex cylindrical lenses. The angle parameter α is changed by the proper rotation of these lenses [18]. Recently, the gyrator transform-based security systems for gray image [19] [20] and color image [11] [15] [16] have been extensively studied.

3. Proposed Method

In this method, an original color image is segregated into *R*, *G* and *B* color components. For simplicity, only red component is considered for the proposed cryptosystem. Let $f(x_i, y_i)$ be original color image. $f_r(x_i, y_i)$, $f_g(x_i, y_i)$ and $f_b(x_i, y_i)$ be its red, green and blue components, respectively. For simplicity, only red channel is illustrated. The subscript *r* has been used for red component. Let $R_{r_1}(x_i, y_i)$ and $R_{r_2}(x, y)$ be independent random phase masks at input and transform planes, respectively. The RPM $R_{r_1}(x_i, y_i)$ multiplied by $f_r(x_i, y_i)$ is gyrator transformed at rotation angles α_{r_1} and then phase truncated to obtain encoded image $E_{r_1}(x, y)$. The resulted image $E_{r_1}(x, y)$ multiplied by $R_{r_2}(x, y)$ is gyrator transformed at rotation α_{r_2} and then phase truncated to get final encoded image $E_{r_2}(x_o, y_o)$ [12].

$$E_{r_1}(x, y) = PT\left\{G^{\alpha_{r_1}}\left[f_r(x_i, y_i)R_{r_1}(x_i, y_i)\right]\right\} \tag{2}$$

$$E_{r_2}(x_o, y_o) = PT\left\{G^{\alpha_{r_2}}\left[E_{r_1}(x, y)R_{r_2}(x, y)\right]\right\} \tag{3}$$

The operator $PT[\,]$ denotes phase truncation. Similarly, the amplitudes truncations of both $E_{r_1}(x,y)$ and $E_{r_2}(x_o,y_o)$ generate first and second asymmetric phase keys.

$$k_{r_1}(x,y) = AT\left\{G^{\alpha_{r_1}}\left[f_r(x_i,y_i)R_{r_1}(x_i,y_i)\right]\right\} \tag{4}$$

$$k_{r_2}(x_o,y_o) = AT\left\{G^{\alpha_{r_2}}\left[E_{r_1}(x,y)R_{r_2}(x,y)\right]\right\} \tag{5}$$

where $AT[\,]$ indicates the operator of amplitude truncation.

The decryption process is straightforward and much simpler compared with encryption process.

$$D_{r_2}(x,y) = PT\left\{G^{-\alpha_{r_2}}\left[E_{r_2}(x_o,y_o)k_{r_2}(x_o,y_o)\right]\right\} \tag{6}$$

$$f_r(x_i,y_i) = D_{r_1}(x_i,y_i) = PT\left\{G^{-\alpha_{r_1}}\left[D_{r_2}(x,y)k_{r_1}(x,y)\right]\right\} \tag{7}$$

The blue and green channels are encrypted and decrypted by the same procedure.

The encryption process is performed digitally whereas the decryption process can be implemented using opto-electronic device. The GT can be implemented by using three generalized lenses (indicated as L_1, L_2 and L_3) with fixed equal distances z between them. Each generalized lens corresponds to the combination of two identical plano-convex cylindrical lenses of the same power. The first and third identical generalized lenses of focal length $f_1 = z$ are rotated with respect to each other. The second generalized lens of a focal length $f_2 = z/2$ is fixed. These lenses are properly rotated to vary the transformation angle α [18].

The optical setup is shown in **Figure 1** & **Figure 2**. For convenience, only the red channel is considered. The encrypted red-channel $E_{r_2}(x_o,y_o)$ is multiplied with decryption phase key $k_{r_2}(x_o,y_o)$, displayed on first Spatial Light Modulator (SLM), illuminated by a collimated beam and then optically transformed by first GT. The intensity of image recorded by a CCD 1 camera. Now the transformed image is multiplied with decryption phase key $k_{r_1}(x,y)$, displayed on the second SLM, illuminated by the collimated beam and then optically transformed by second GT. The intensity of image is recorded by the CCD 2 camera. The same process is repeated with encrypted green- and blue-channels to obtain corresponding green and blue channels. Finally, the decrypted color channels are combined into decrypted color image by using a computer system.

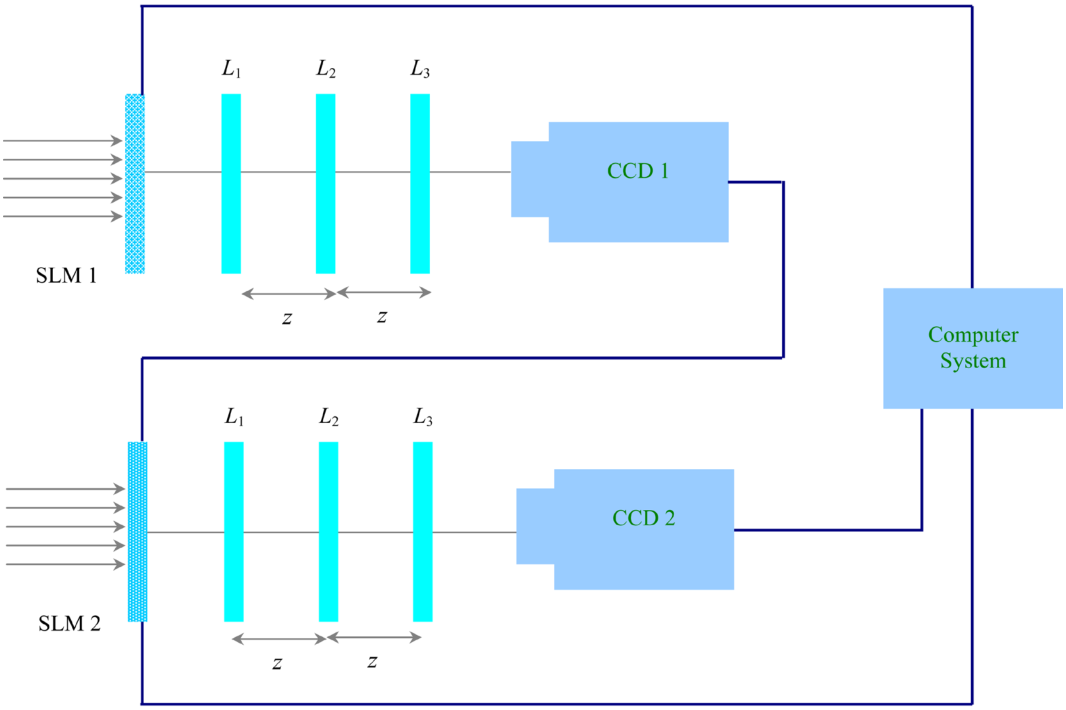
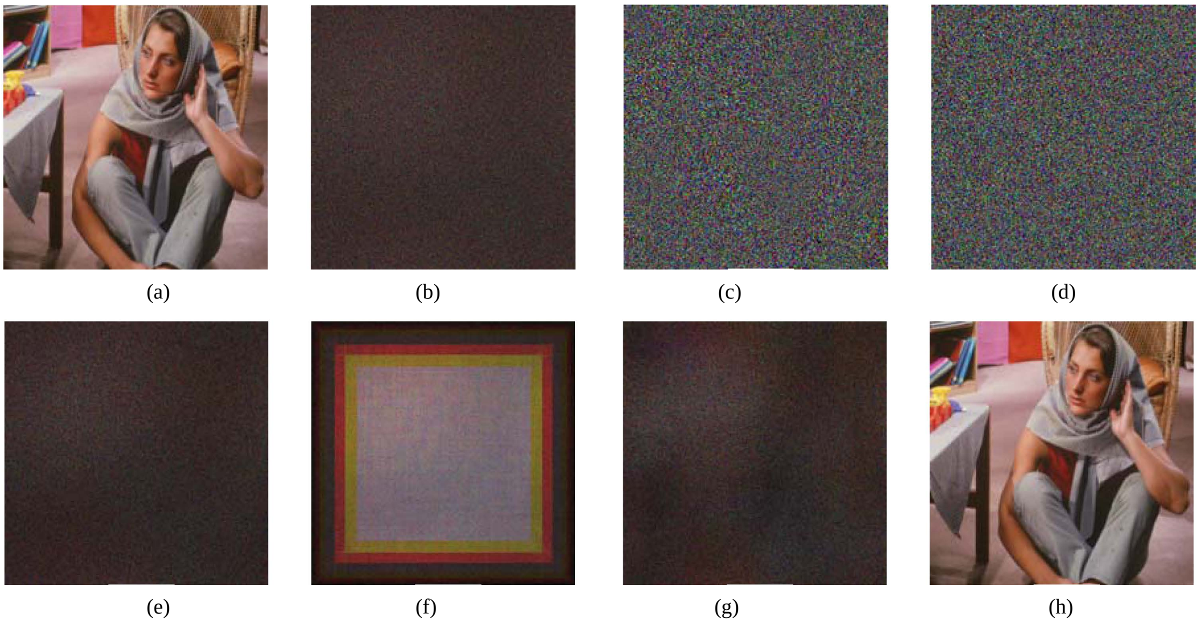


Figure 1. Optical setup for proposed color image decryption system.


(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 2. Simulation results of the proposed method: (a) Original color image with 512 × 512 pixels to be encoded; (b) encrypted image with all correct keys (c) real part of the first decryption phase key; (d) real part of the second decryption phase key; (e) retrieved image with arbitrary phase key; (f) recovered image with no phase keys; (g) reconstructed image with the transformation angle for each channel changed by 0.3 but all the other parameters are correct; (h) decrypted image with all right keys.

4. Numerical Simulation Results

Numerical simulations have been carried out on a Matlab 7.11.0 (R2010b) platform to test the feasibility and security of the new proposal. The original color image having size $512 \times 512 \times 3$ pixels is shown in **Figure 2(a)**. The first and second transformation angles of the GT for red, green and blue channels are, respectively, $\left(\alpha_{r_1} = 0.45^\circ, \alpha_{g_1} = 0.55^\circ, \alpha_{b_1} = 0.65^\circ\right)$ and $\left(\alpha_{r_2} = 0.75^\circ, \alpha_{g_2} = 0.85^\circ, \alpha_{b_2} = 0.95^\circ\right)$. The encrypted image produced by three-multiplexed channels is shown in **Figure 2(b)**. The real parts of three-multiplexed channels of first and second asymmetric phase keys are, respectively, illustrated in **Figure 2(c)** and **Figure 2(d)**. The retrieved images with arbitrary phase key and with no phase keys are demonstrated in **Figure 2(e)** and **Figure 1(f)**, respectively. The recovered images with the transformation angle for each channel changed by 0.3° and with all correct keys are demonstrated in **Figure 2(g)** and **Figure 2(h)**, respectively. As can be seen from **Figures 2(e)-(g)**, corresponding decrypted images provide no valuable information about the original color image. That means the original image can only be obtained if all the decryption keys are accurate as shown in **Figure 2(h)**.

To evaluate the reliability of the proposed algorithm quantitatively, the mean square error (MSE) is introduced and defined as

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| I_o(m,n) - I_d(m,n) \right|^2 \tag{8}$$

where $I_o(m,n)$ and $I_d(m,n)$ indicate the original and decrypted image at pixel position (m,n), respectively. $(M \times N)$ represents the size of the image.

In **Figure 2(b)**, the MSE values of encrypted result with all the correct keys are $\left(7.0835 \times 10^3, 4.8988 \times 10^3, 5.0688 \times 10^3\right)$ for red, green and blue channels, respectively. These values are very high, which indicate that no information about the original image can be obtained. The calculated MSE values corresponding to **Figure 2(e)** and **Figure 2(f)** for red, green and blue channels are $\left(6.8119 \times 10^3, 4.7307 \times 10^3, 4.9128 \times 10^3\right)$ and $\left(8.8345 \times 10^3, 6.5785 \times 10^3, 7.8403 \times 10^3\right)$, respectively. The high MSE values, for arbitrary phase key and no phase keys, sufficiently reveal the strength of the proposed algorithm. The MSE values for a very small error of 0.3° in transformation angle of GT for red, green and blue is $\left(6.5514 \times 10^3, 4.5162 \times 10^3, 4.5629 \times 10^3\right)$. The high MSE results adequately demonstrate the robustness of the proposed system.

In attack analysis, first the known plaintext attack is considered, in which an attacker knows all the transformation angles and attempts to produce decryption keys from a fake color image of size $512\times512\times3$ pixels as shown Figure 3(a); the real parts of the first fake decryption key and second fake decryption key are displayed in Figure 3(b) and Figure 3(c). The decrypted image with all fake keys with correct transformation angles is illustrated in Figures 3(d). That means an unauthorized user can not retrieve the original image. So, the proposed technique can resist against brute force attack.

Second, the robustness of the proposed technique against occlusion attacks on the encrypted data has been examined. The 50%- and 70%- occluded encrypted images are shown in Figure 4(a) and Figure 4(c), respectively. The calculated MSE values corresponding to recovered images with all correct keys as displayed in Figure 4(b) and Figure 4(d) for red, green and blue channels, are $\left(4.5739\times10^3, 2.4107\times10^3, 2.0700\times10^3\right)$ and $\left(9.4785\times10^3, 5.0062\times10^3, 4.2190\times10^3\right)$, respectively.

Third, the robustness of the proposed method against noise attacks on the encrypted data has also been checked. The Gaussian and speckle noised encrypted images with variance 0.1 are displayed in Figure 5(a) and Figure 5(c), respectively. The resulted MSE values corresponding to retrieved images with all right keys as depicted in Figure 5(b) and Figure 5(d) for red, green and blue channels, are $\left(1.2345\times10^3, 1.2890\times10^3, 1.2991\times10^3\right)$ and $\left(1.8374\times10^3, 1.2360\times10^3, 1.1208\times10^3\right)$, respectively.

From above results, it can be concluded that if the encrypted data is destroyed by occlusion or degraded by noise in storage and transmission process, the decrypted image with all right keys is recognizable. Therefore, the proposed method has certain robustness against occlusion and noise attacks.

The sensitive degree of the transformation angle is analyzed and then calculated. The sampling interval is fixed at the range $[0.0,1.0]$, sampling length is taken at 0.01 and other decryption keys are used with correct values. The corresponding MSE curves between original red, green and blue channels and their corresponding decrypted images are depicted in Figures 6(a)-(c). These MSE curves have very narrow downward peaks. The MSE of red channel is quite sensitive as compared to green and blue channels. The value of MSE function becomes zero at $\alpha = 0.50$ with correct decryption keys. The zero-MSE value indicates that the original image is decrypted completely.

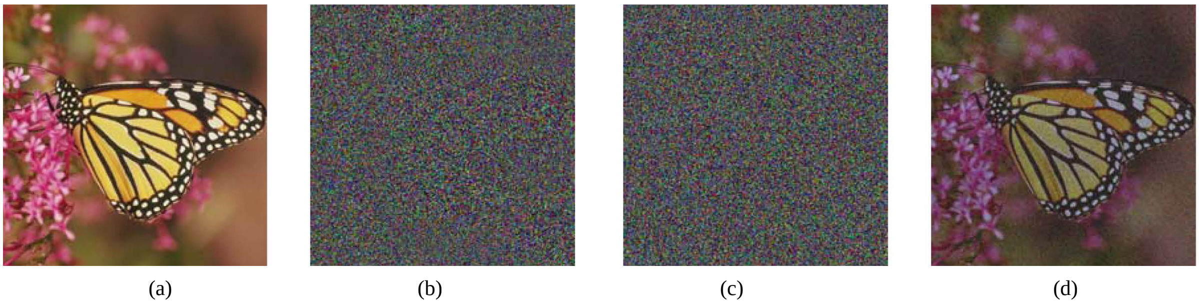


Figure 3. Known plaintext attack: (a) Fake color image with 512×512 pixels; (b) real part of the first fake decryption key; (c) real part of the second fake decryption key; (d) retrieved image with all fake keys with correct transformation angles.

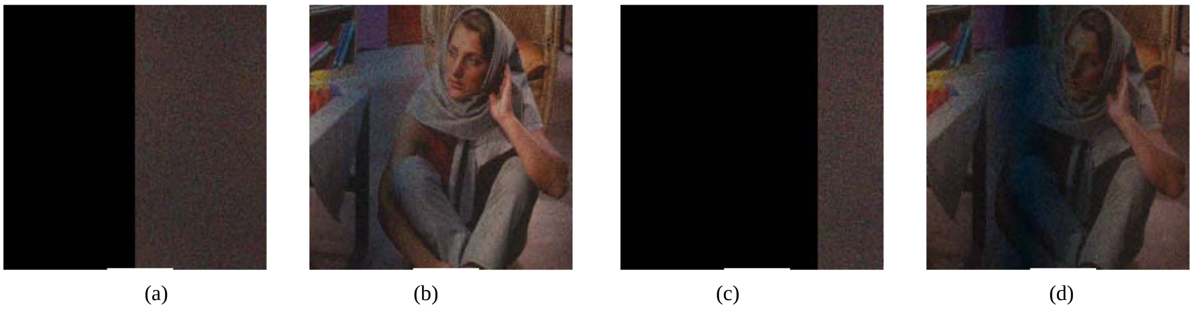
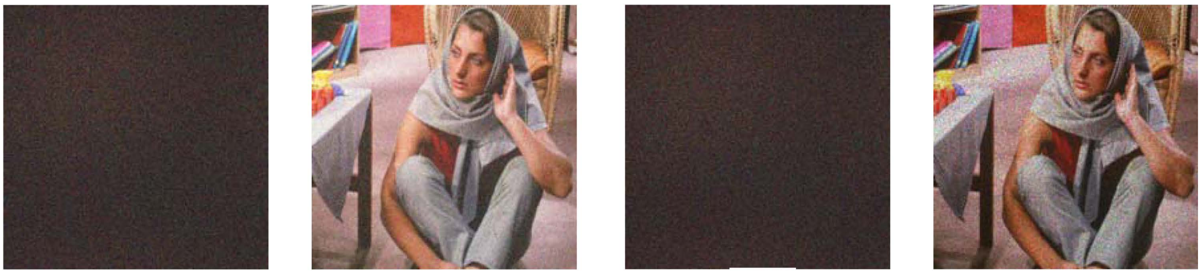
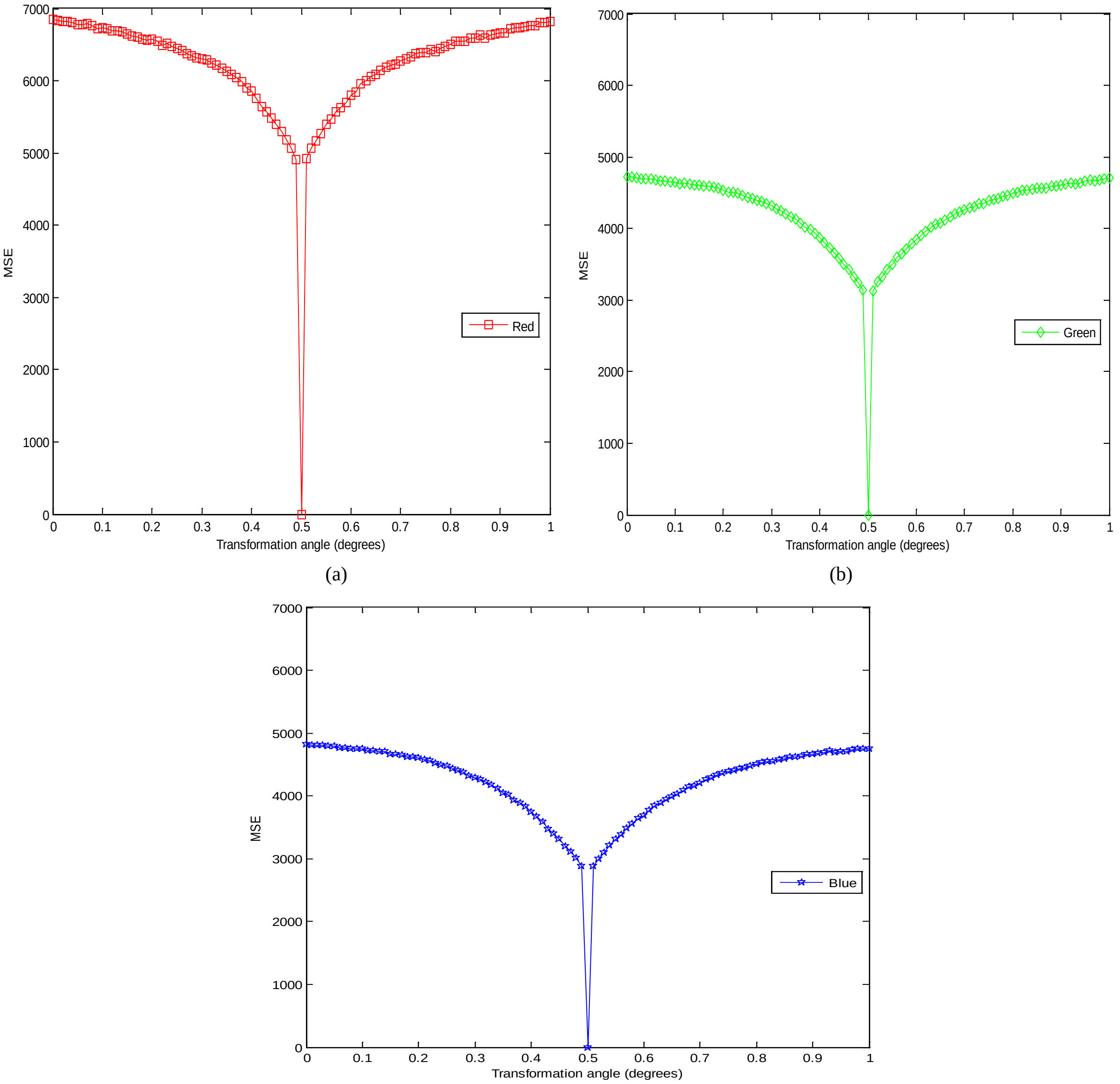


Figure 4. Test of occlusion attack: (a) encoded image with 50% occlusion; (b) corresponding reconstructed image image with all accurate keys; (c) encoded image with 75% occlusion; (d) corresponding reconstructed image with all exact keys.



(a) (b) (c) (d)

Figure 5. Test of noise attack: (a) encoded image having Gaussian noise with variance 0.1; (b) corresponding decrypted image with all correct keys (c) encoded image having speckle noise with variance 0.1; (d) corresponding retrieved image with all right keys.



(a) (b)

(c)

Figure 6. (a) MSE versus variation in transformation angle for red channel; (b) MSE versus variation in transformation angle for green channel; and (c) MSE versus variation in transformation angle for blue channel.

5. Conclusion

A new information encryption system based phase-truncated gyrator transform domain is presented. The original color image is separated into R, G, and B channels. The separated three RBG channels avoid the interference of crosstalks efficiently. The two random phase masks are encryption keys which are used as public keys. The two asymmetric phase keys are decryption keys which are employed as private keys. That means only authorized users can decrypt the original information. The transformation angles of GT as supplementary keys significantly enhance the security of the proposed system. The numerical simulations have shown the effectiveness of this method.

References

[1] Refregier, P. and Javidi, B. (1995) Optical Image Encryption Based on Input Plane and Fourier Plane Random Encoding. *Optics Letters*, **20**, 767-769. http://dx.doi.org/10.1364/OL.20.000767

[2] Unnikrishnan, G., Joseph, J. and Singh, K. (2000) Optical Encryption by Double-Random Phase Encoding in the Fractional Fourier Domain. *Optics Letters*, **25**, 887-889. http://dx.doi.org/10.1364/OL.25.000887

[3] Situ, G. and Zhang, J. (2004) Double Random-Phase Encoding in the Fresnel Domain. *Optics Letters*, **29**, 1584-1586. http://dx.doi.org/10.1364/OL.29.001584

[4] Hwang, H.-E., Chang, H.T. and Lie, W.-N. (2009) Fast Double-Phase Retrieval in Fresnel Domain Using Modified Gerchberg-Saxton Algorithm for Lensless Optical Security Systems. *Optics Express*, **17**, 13700-13710. http://dx.doi.org/10.1364/OE.17.013700

[5] Tsang, P.W.M., Poon, T.-C. and Cheung, K.W.K. (2011) Fast Numerical Generation and Encryption of Computer-Generated Fresnel Holograms. *Applied Optics*, **50**, B46-B52. http://dx.doi.org/10.1364/AO.50.000B46

[6] Alfalou, A., Brosseau, C., Abdallah, N. and Jridi, M. (2013) Assessing the Performance of a Method of Simultaneous Compression and Encryption of Multiple Images and Its Resistance against Various Attacks. *Optics Express*, **21**, 8025-8043. http://dx.doi.org/10.1364/OE.21.008025

[7] Zhang, S.Q. and Karim, M.A. (1999) Color Image Encryption Using Double Random Phase Encoding. *Microwave and Optical Technology Letters*, **21**, 318-323. http://dx.doi.org/10.1002/(SICI)1098-2760(19990605)21:5<318::AID-MOP4>3.0.CO;2-A

[8] Chen, L. and Zhao, D. (2006) Optical Color Image Encryption by Wavelength Multiplexing and Lensless Fresnel Transform Holograms. *Optics Express*, **14**, 8552-8560. http://dx.doi.org/10.1364/OE.14.008552

[9] Liu, Z., Xu, L., Liu, T., Chen, H., Li, P., Lin, C. and Liu, S. (2011) Color Image Encryption by Using Arnold Transform and Color-Blend Operation in Discrete Cosine Transform Domains. *Optics Communications*, **284**, 123-128. http://dx.doi.org/10.1016/j.optcom.2010.09.013

[10] Chen, W., Chen, X. and Sheppard, C.J.R. (2012) Optical Color-Image Encryption and Synthesis Using Coherent Diffractive Imaging in the Fresnel Domain. *Optics Express*, **20**, 3853-3865. http://dx.doi.org/10.1364/OE.20.003853

[11] Abuturab, M.R. (2012) Color Image Security System Using Double Random-Structured Phase Encoding in Gyrator Transform Domain. *Applied Optics*, **51**, 3006-3016. http://dx.doi.org/10.1364/ao.51.003006

[12] Qin, W. and Peng, X. (2010) Asymmetric Cryptosystem Based on Phase-Truncated Fourier Transforms. *Optics Letters*, **35**, 118-120. http://dx.doi.org/10.1364/OL.35.000118

[13] Wang, X. and Zhao, D. (2012) A Special Attack on the Asymmetric Cryptosystem Based on Phase-Truncated Fourier Transforms. *Optics Communications*, **285**, 1078-1081. http://dx.doi.org/10.1016/j.optcom.2011.12.017

[14] Abuturab, M.R. (2013) Security Enhancement of Color Image Cryptosystem by Optical Interference Principle and Spiral Phase Encoding. *Applied Optics*, **52**, 1555-1563. http://dx.doi.org/10.1364/AO.52.001555

[15] Abuturab, M.R. (2012) Color Information Cryptosystem Based on Optical Superposition Principle and Phase-Truncated Gyrator Transform. *Applied Optics*, **51**, 7994-8002. http://dx.doi.org/10.1364/AO.51.007994

[16] Abuturab, M.R. (2013) Authentication System of Color Information Using Interference of Two Beams in Gyrator Transform Domain. *Applied Optics*, **52**, 5133-5142. http://dx.doi.org/10.1364/AO.52.005133

[17] Rodrigo, J.A., Alieva, T. and Calvo, M.L. (2007) Gyrator Transform: Properties and Applications. *Optics Express*, **15**, 2190-2203. http://dx.doi.org/10.1364/OE.15.002190

[18] Rodrigo, J.A., Alieva, T. and Calvo, M.L. (2007) Experimental Implementation of the Gyrator Transform. *Journal of the Optical Society of America A*, **24**, 3135-3139. http://dx.doi.org/10.1364/JOSAA.24.003135

[19] Liu, Z., Xu, L., Chen, C., Dai, J. and Liu, S. (2011) Image Encryption Scheme by Using Iterative Random Phase Encoding in Gyrator Transform Domains. *Optics and Lasers in Engineering*, **49**, 542-546.

http://dx.doi.org/10.1016/j.optlaseng.2010.12.005

[20] Liu, Z., Li, S., Liu, W., Liu, W. and Liu, S. (2013) Image Hiding Scheme by Use of Rotating Squared Sub-Image in the Gyrator Transform Domains. *Optics & Laser Technology*, **45**, 198-203. http://dx.doi.org/10.1016/j.optlastec.2012.07.004