Optics Communications 282 (2009) 3680–3685

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Optical color image encryption based on Arnold transform and interference method

W. Chen, C. Quan *, C.J. Tay

Department of Mechanical Engineering, National University of Singapore, 9 Engineering Drive 1, Singapore 117576, Singapore

ARTICLE INFO

Article history:
Received 24 February 2009
Received in revised form 3 June 2009
Accepted 5 June 2009

PACS:
42.25.Hz
42.66.Ne
87.19.ls

Keywords:
Color image encryption
Image decryption
Arnold transform
Interference

ABSTRACT

In this paper, we propose a novel method to encrypt a color image based on Arnold transform (ART) and interference method. A color image is decomposed into three independent channels, i.e., red, green and blue, and each channel is then encrypted into two random phase masks based on the ART and interference method. Light sources with corresponding wavelengths are used to illuminate the retrieved phase-only masks during image decryption. The influence of security parameters on decrypted images is also analyzed. Numerical simulation results are presented to illustrate the feasibility and effectiveness of the proposed method.

1. Introduction

Optical encryption techniques have become an important field for information security. Since optical encryption based on double random phase encoding was firstly proposed by Refregier and Javidi [1], many techniques, such as digital holography [2,3] and fractional Fourier transform [4,5], have been proposed. Recently, multiple-image encryption and image hiding are one attractive topic in optical security, and several techniques, such as wavelength multiplexing [6], have been proposed. In addition, some algorithms based on phase retrieval method [7,8] have also been proposed for image hiding. In optical image encryption, as a monochromatic light is used to illuminate a real color image, color information of a decrypted image is lost. In practice, color information of an input image would have many useful applications and not just in its beauty.

Zhang and Karim [9] proposed a method based on an indexed image and double phase random masks to encrypt a color image. Chen and Zhao [3] proposed a color image encryption using wavelength multiplexing [6] based on lensless Fresnel transform holograms. Joshi et al. [5] have proposed a method for the encryption of twin color images using fractional Fourier transform. In their work, color images are converted into indexed images before encryption. Chen and Zhao [10] also proposed color information processing with fractional Fourier transforms and digital hologram. In Ref. [10], the images are fused and subtracted by the use of conventional phase-shifting technique. Joshi et al. [11] proposed a non-linear approach based on a logarithm to encrypt a color image in fractional Fourier domain, while Ge et al. [12] proposed a technique for color image hiding based on fractional Fourier transform with double random phase masks. In addition, some color image watermarking techniques have also been investigated in spectral domain [13]. Recently, Huang and Nien [14] proposed to use the chaotic sequences generated by chaotic systems as encryption codes and then implement color image encryption.

In this paper, we propose a novel method to encrypt a color image based on Arnold transform (ART) and interference method. A color image which usually consists of red, green and blue values with certain proportions is firstly decomposed into three channels. Each channel is then encrypted into two random phase-only masks. For image decryption, a light source with a corresponding wavelength is used to illuminate the retrieved phase-only masks for each channel. Numerical simulations are presented to illustrate the feasibility and effectiveness of the proposed method.

2. Principle of the methods

A schematic numerical experimental arrangement is shown in Fig. 1a. Collimated plane light sources, respectively, illuminate two retrieved phase-only masks at each channel, and the two beams are combined at the image plane. To obtain the original

* Corresponding author. Tel.: +65 6516 8089; fax: +65 6779 1459.
E-mail address: mpeqcg@nus.edu.sg (C. Quan).

0030-4018/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2009.06.014

color image at the image plane, a digital approach should be used to embed each channel of an original input image into two phase-only masks. In addition, a different distance is preset for each channel to enhance the security level, but within a channel the two phase-only masks are placed at the same distance from the image plane. Before an original color image is hidden, an ART method is employed to process the color image. For simplicity, only the red channel of an input image is analyzed theoretically. For a given image $O(x,y)$ with $N \times N$ pixel number at the red channel (non-negative values), the ART of a pixel (x,y) in the input image $O(x,y)$ can be expressed as

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}\ N) = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}\ N), \tag{1}$$

where $A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$, mod denotes the modulus after division, and (x', y') denotes a new pixel position after ART operation. Hence, a discrete ART of the image can be described by

$$\begin{aligned} \mathrm{ART}[O(x,y),N] &= \{[v,(x',y')]|(x',y')^T \\ &= A(x,y)^T (\mathrm{mod}\ N), [v,(x,y)] \in O(x,y)\}, \end{aligned} \tag{2}$$

where T denotes a transpose operation, v denotes a value at the pixel (x,y) in the original image, and the terms on the right-hand side of "|" denote the algorithm conditions or operation procedures. In the ART method, an Arnold scrambling period is determined by

$$\mathrm{Period} = \min\{n|\{\mathrm{ART}[O(x,y),N]\}^n = O(x,y)\}, \tag{3}$$

where min denotes a minimum value, and n is a positive integer which denotes the number of iterations. In this study, N is larger than 2 and the period usually satisfies the requirement of Period $\leqslant N^2/2$ [15].

The complex amplitude for phase-only masks M1 and M2 at the red channel which interfere in the image plane can be expressed as

$$\begin{aligned} \sqrt{O(x',y')}\exp[jP(x',y')] &= FT^{-1}[H(f_\xi,f_\eta;z_1)M_1(f_\xi,f_\eta)] \\ &\quad + FT^{-1}[H(f_\xi,f_\eta;z_1)M_2(f_\xi,f_\eta)], \end{aligned} \tag{4}$$

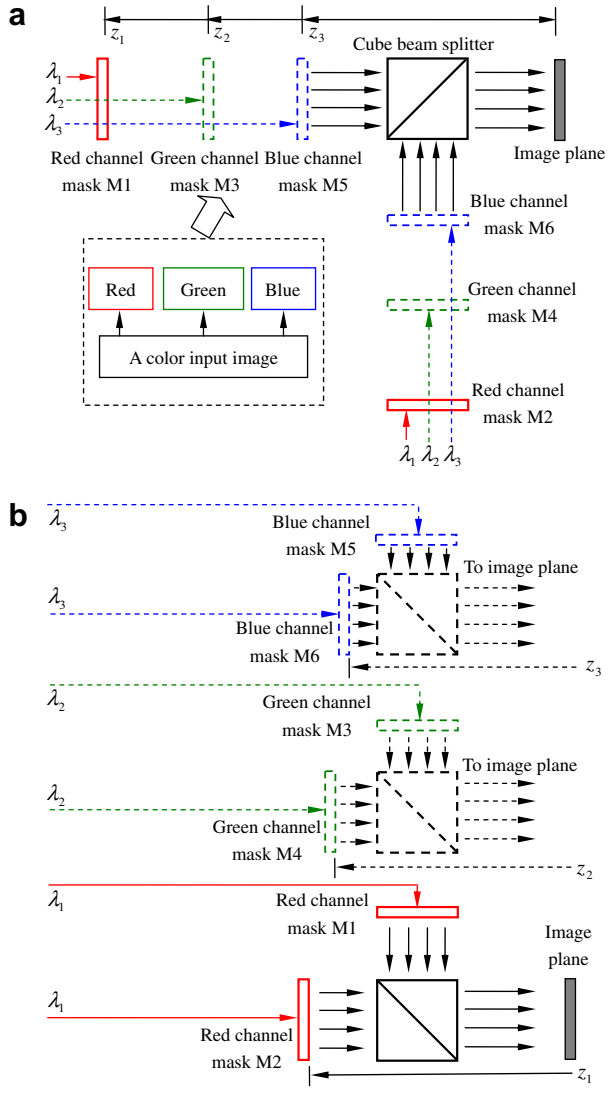

Fig. 1. (a) A schematic numerical experimental arrangement; (b) a schematic optical arrangement with three independent channels.

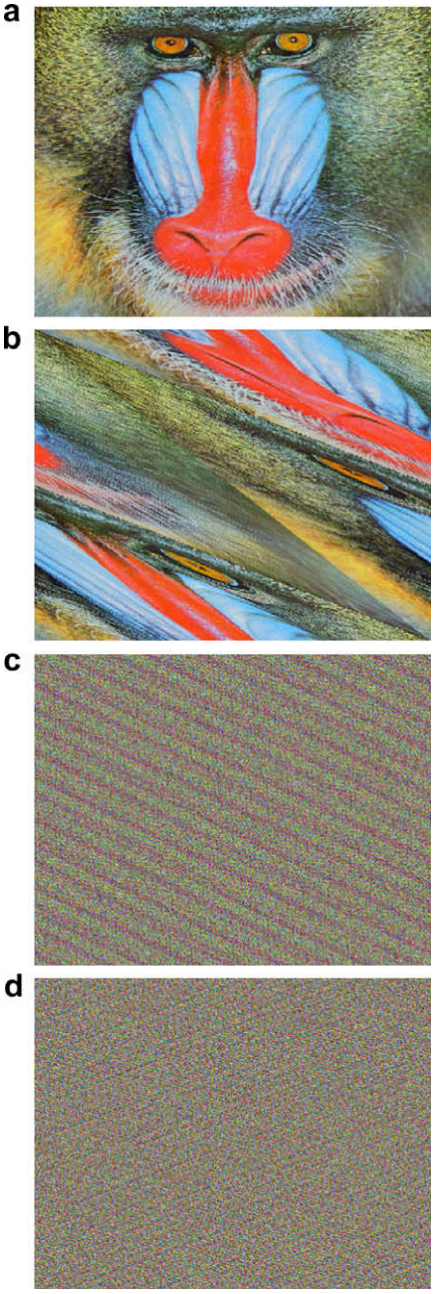

Fig. 2. (a) An original color image of Mandrill; the images after ART using different number of iterations of (b) red = 1, green = 1 and blue = 1; (c) red = 60, green = 70 and blue = 80; (d) red = 205, green = 215 and blue = 225. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

where $O(x',y') = \{\mathrm{ART}[O(x,y),N]\}^n, P(x',y')$ is a map randomly distributed in $[0,2\pi]$, $j=\sqrt{-1}, f_\xi$ and f_η are spatial frequencies, FT^{-1} denotes a 2D inverse Fourier transform, $M_1(f_\xi,f_\eta)$ and $M_2(f_\xi,f_\eta)$ denote 2D Fourier transforms of phase masks $M_1(\xi,\eta)$ and $M_2(\xi,\eta)$, z_1 denotes the distance between the phase mask plane (M1 or M2) and the image plane, and $H(f_\xi,f_\eta;z_1)$ is a transfer function described by

$$H(f_\xi,f_\eta;z_1)=\begin{cases}\exp\{-jk_1z_1[1-(\lambda_1f_\xi)^2-(\lambda_1f_\eta)^2]^{1/2}\} & \text{if } (f_\xi^2+f_\eta^2)^{1/2}<(1/\lambda_1),\\ 0 & \text{Otherwise,}\end{cases} \tag{5}$$

where λ_1 denotes a wavelength for red channel, and wave number $k_1=2\pi/\lambda_1$. In practice, the bandwidth is determined by some factors, such as CCD pixel size. It is assumed in this study that f_ξ and f_η are always within the above bandwidth range. It is worth noting that a different random map $P(x',y')$ is used for each channel, and the implementation of ART with the iteration number (Period $-n$) is called an inverse ART.

With a proper derivation of Eqs. (4) and (5) [8], the red channel of the input image can be encrypted into two phase-only masks as

$$M_1(\xi,\eta)=\mathrm{angle}(FT^{-1}\{FT[O_w(x',y')]/H(f_\xi,f_\eta;z_1)\}) - \arccos[\mathrm{abs}(FT^{-1}\{FT[O_w(x',y')]/H(f_\xi,f_\eta;z_1)\})/2], \tag{6}$$

$$M_2(\xi,\eta)=\mathrm{angle}(FT^{-1}\{FT[O_w(x',y')]/H(f_\xi,f_\eta;z_1)\}-\exp[jM_1(\xi,\eta)]), \tag{7}$$

where $O_w(x',y')=\sqrt{O(x',y')}\exp[jP(x',y')], FT$ denotes a 2D Fourier transform, and angle denotes an arc–tangent operation. In this paper, the values of $\mathrm{abs}(FT^{-1}\{FT[O_w(x',y')]/H(f_\xi,f_\eta;z_1)\})/2$ are compared with a threshold value of one, and values larger than the threshold value are set as 1. It is illustrated in Eqs. (6) and (7) that the red channel of a color image is encrypted into two phase-only masks. Similarly, phase-only masks M3 and M4 for the green channel and M5 and M6 for the blue channel can also be obtained. The most obvious advantage of the interference method is that compared with other phase retrieval methods [7], it does not require any iteration operation. It is worth noting that with the extracted random phase masks (M1–M6) the security level is high, but the security level can be further enhanced using the proposed ART method.

For image decryption, a light source with a corresponding wavelength is used to illuminate the two retrieved phase-only masks at each channel. As the incident wavelength of each channel is close to the wavelength of the basic color, the original color information can be obtained at the image plane [3]. A decrypted real color image can be obtained by an inverse ART with a correct number of iterations for each channel and the incorporation of three decrypted channels. With a proper modification of the experimental arrangement as shown in Fig. 1a, a practical real-time optical implementation of image decryption is feasible. In addition, a constant value, such as 2π, can be added to all the retrieved phase

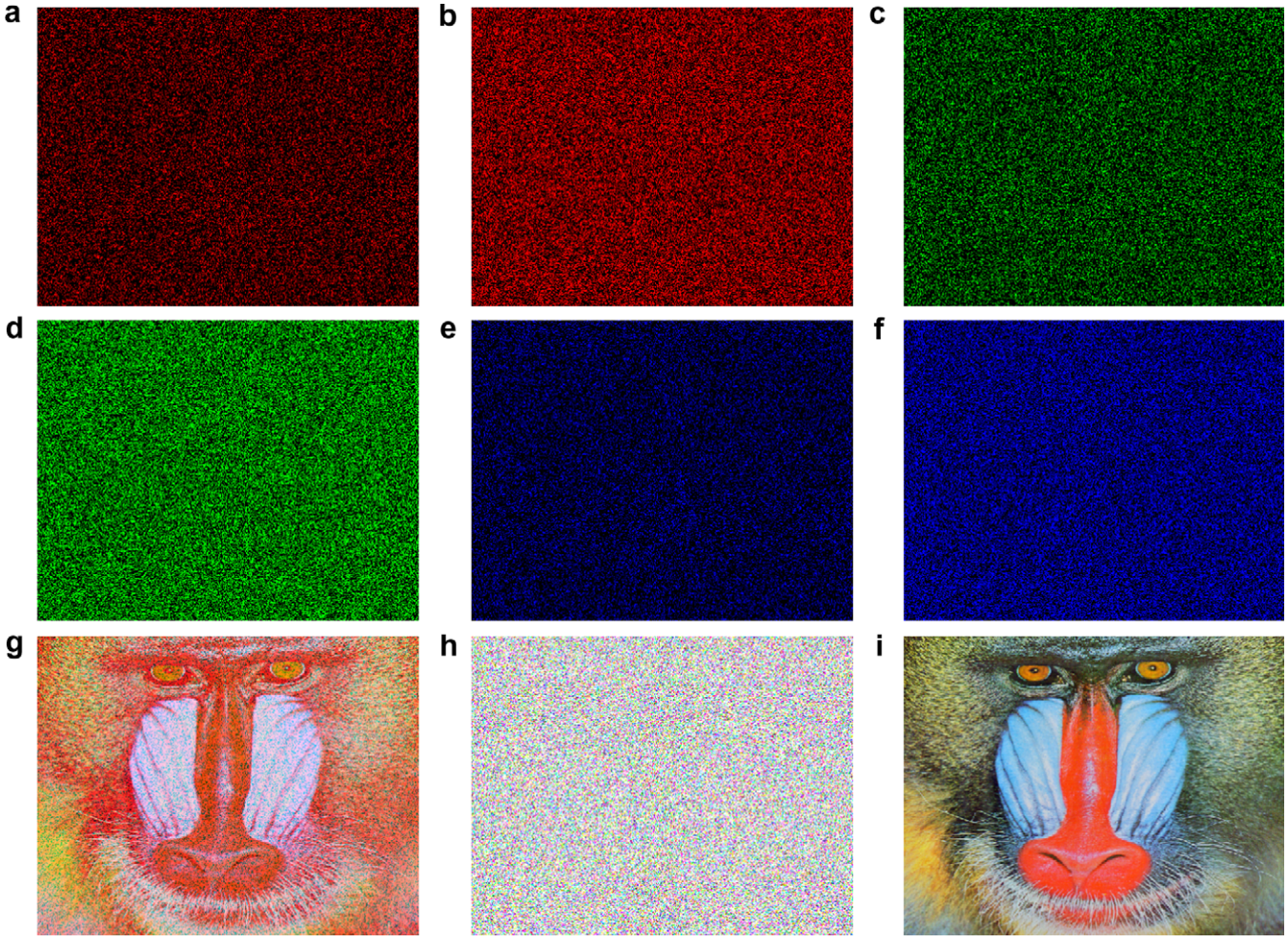

Fig. 3. Retrieved phase-only masks (a) M1 and (b) M2 for red channel, (c) M3 and (d) M4 for green channel, (e) M5 and (f) M6 for blue channel; decrypted images with (g) wrong phase masks M1 and M2, (h) wrong phase masks M1-M6 and (i) all correct security keys. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

masks (M1–M6) to avoid the negative values when a spatial light modulator is used. This operation will not affect the finally decrypted image.

To evaluate the similarity between the original color image $O(x, y)$ and a decrypted image $O_r(x, y)$, correlation coefficients (CC) are calculated by

$$\mathrm{CC} = \mathrm{cov}(O, O_r)/(\sigma_O \cdot \sigma_{O_r}). \quad (8)$$

Where $\mathrm{cov}(O, O_r)$ denotes the cross-covariance, and σ denotes the standard deviation.

3. Simulation work and results discussion

A numerical experiment as shown in Fig. 1a is conducted to show the feasibility and effectiveness of the proposed method. An inset shown in Fig. 1a illustrates the separation of a color image into three independent channels. Fig. 1b shows a schematic optical arrangement with three independent channels. The distances between the phase-only mask planes for red, green and blue channels and the image plane are respectively $z_1 = 64$ cm, $z_2 = 54$ cm and $z_3 = 44$ cm, and the respective wavelengths are $\lambda_1 = 636$ nm, $\lambda_2 = 537.8$ nm and $\lambda_3 = 441.6$ nm. An original color image of Mandrill [16] with 512×512 pixel number is shown in Fig. 2a, and the pixel size in the image plane is 10 μm.

It is worth noting that in this study, the original color image is normalized. Fig. 2b shows an image after the ART operation as the number of iterations for red, green and blue channels of the input image is 1, 1 and 1, respectively. Fig. 2c shows an image after the ART operation as the respective iterations are 60, 70 and 80, while in Fig. 2d the respective iterations are 205, 215 and 225. The resultant CC values in Fig. 2b for red, green and blue channels are (−0.083, 0.040, −0.071), while the corresponding CC values in Fig. 2c and d are $(-8.97 \times 10^{-4}, 6.68 \times 10^{-4}, -9.64 \times 10^{-4})$ and $(-3.37 \times 10^{-4}, -0.0029, 0.0023)$. It is shown in Fig. 2b–d that the input image is highly blurred after ART, and no information about the original color image can be observed.

Fig. 3a–f shows the retrieved phase-only masks M1 and M2 for red channel, M3 and M4 for green channel and M5 and M6 for blue channel, respectively. In this case, the Arnold scrambling period is 384, and the number of iterations in ART for red, green and blue

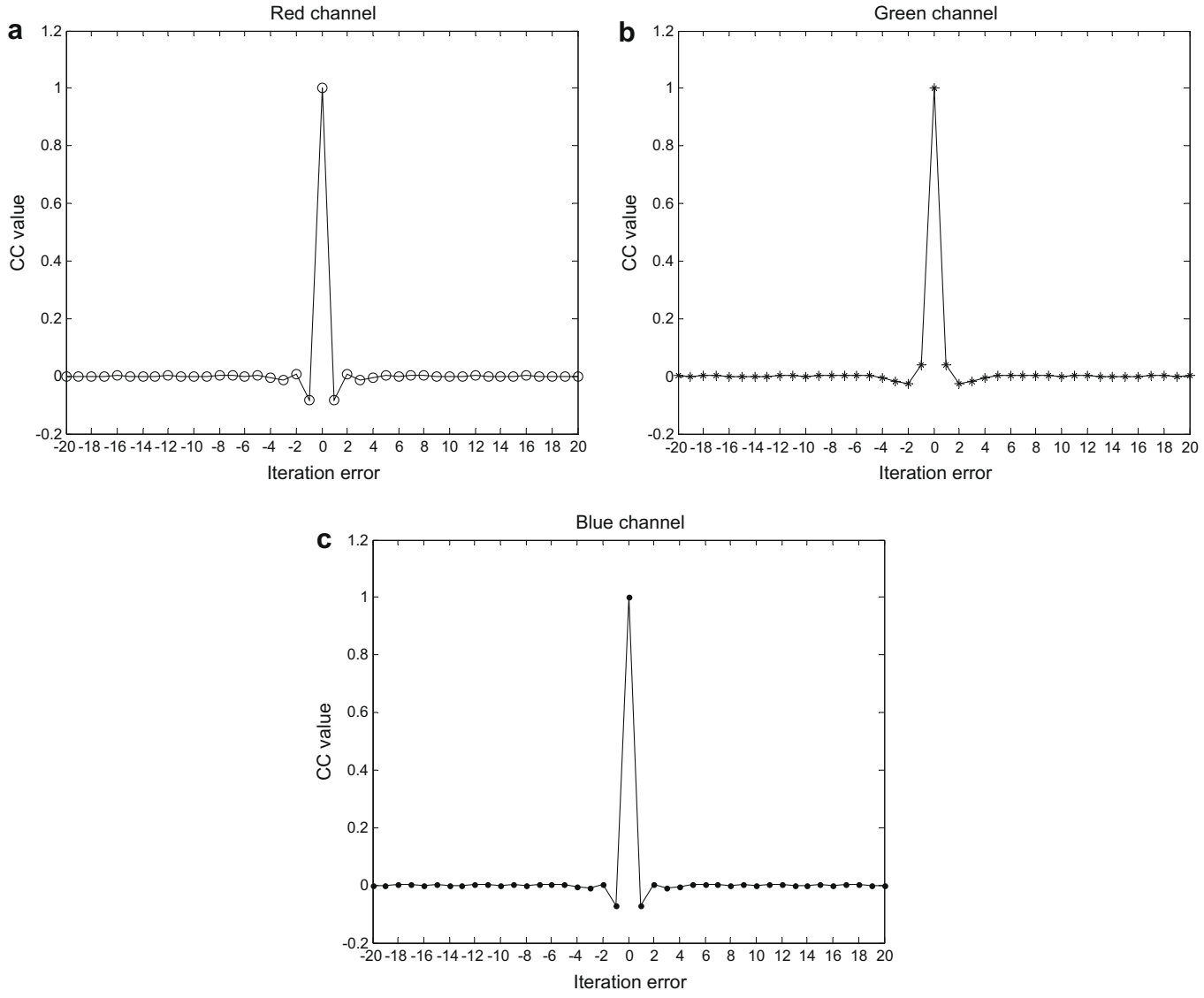

Fig. 4. Relationships between CC values and iteration errors only for (a) red channel, (b) green channel, (c) blue channel; (d) a decrypted image without the inverse ART operation during image decryption; decrypted images with iteration error of (e) 1 at red channel, (f) 1 at green channel, (g) 1 at blue channel, and (h) 1 at all three channels. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

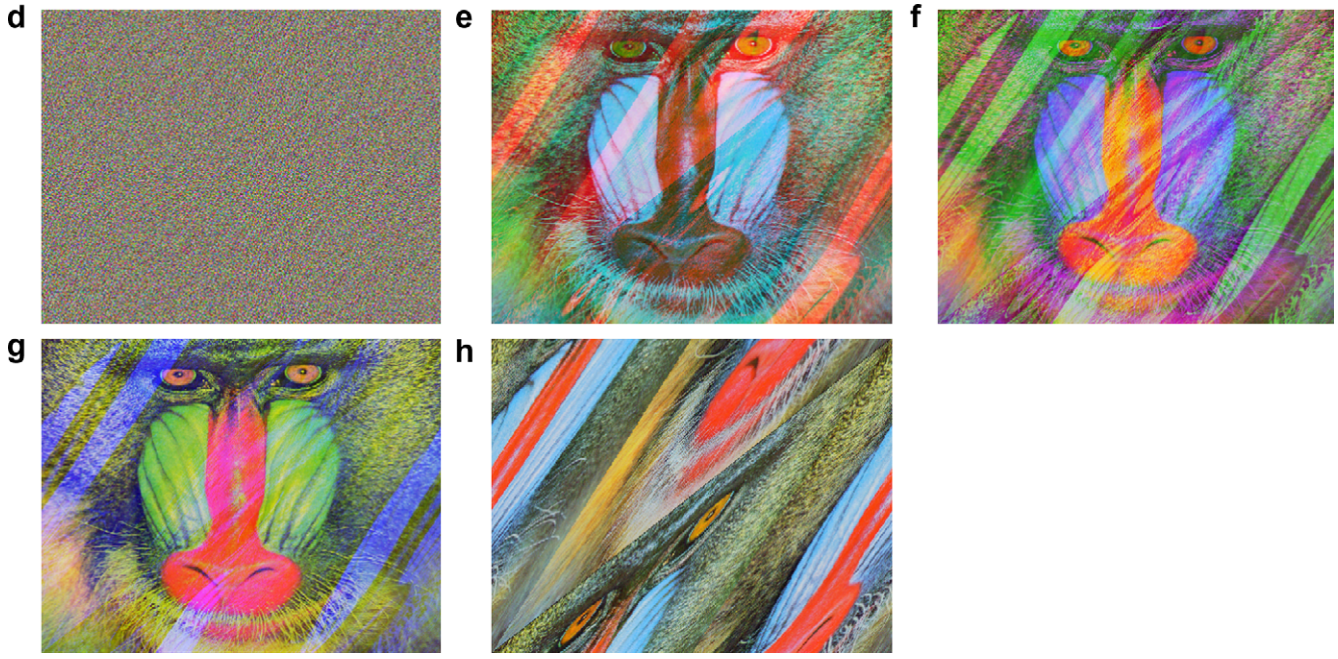

Fig. 4 (*continued*)

channels is set as 80, 90 and 100, respectively. It can be seen in Fig. 3a–f that the retrieved phase masks are distributed randomly, and the original color image is fully hidden. It is worth noting that since a color image usually contains three channels, a digital format with three channels is used to demonstrate the retrieved random phase masks. Fig. 3g shows a decrypted image using incorrect phase masks M1 and M2 but with other correct security parameters, such as wavelengths, distances, phase masks M3–M6 and iteration number in ART. Fig. 3h shows a decrypted image using incorrect phase masks M1–M6 but with other correct security parameters. The average CC values in Fig. 3h for the red, green and blue channels are -3.03×10^{-4}, -4.24×10^{-4} and 1.54×10^{-3}, respectively. It is shown in Fig. 3g and h that the real color image and some information on the input image are lost as incorrect security keys are used. Fig. 3i shows a decrypted image using all correct security parameters with CC ≈ 1, which means that the original color image is perfectly retrieved and the influence of the threshold operation in Eq. (6) can be ignored.

To evaluate the influence of the iteration number on a decrypted image in ART method, a relationship between the CC values and iteration errors (for red channel) is shown in Fig. 4a. Corresponding relationships for the green and blue channels are shown in Fig. 4b and c, respectively. It is shown that a small iteration error of 1 results in the CC value close to zero. Fig. 4d shows a decrypted image without inverse ART during image decryption. The resultant CC values in Fig. 4d for red, green and blue channels are -2.12×10^{-4}, -7.60×10^{-4} and 3.21×10^{-4}, respectively. It is shown in Fig. 4d that no information on the original image is obtained. Fig. 4e–g shows respectively the decrypted images with an iteration number error of 1 at the red, green, or blue channel but with other correct security keys. Fig. 4h shows a decrypted image with iteration errors of 1 for all three channels but with other correct parameters. The CC values in Fig. 4h for the red, green and blue channels are -0.083, 0.040 and -0.071, respectively. It is seen again that the encrypted images cannot be correctly decrypted using incorrect parameters, and the actual color information is lost. It is also demonstrated that although the extracted random phase masks (M1–M6) render image decryption difficult for the attackers, decryption difficulty is further increased without the information on the usage of ART method. However, since a pixel scrambling period exists in the ART, the image decryption will not become much more complicated. The parameters, such as the distances and light source wavelengths, can also be employed as security parameters for image decryption, and for brevity they are not included in this investigation. Moreover, the ART of every pixel within a small region of each channel using a random number of iterations followed by the ART of every pixel within a relatively large region of each channel can be further investigated. This might significantly improve the security levels.

4. Concluding remarks

In this paper, we propose a novel method to encrypt a color image based on ART and interference. A color image is firstly decomposed into three independent channels, and each channel is then encrypted into two random phase masks based on ART and interference. For image decryption, a light source with a corresponding wavelength is used to illuminate two retrieved phase-only masks for each channel, and a decrypted real color image is obtained by inverse ART and incorporation of three decrypted channels. The results illustrate that the proposed method is feasible and effective for color image encryption. The proposed method would also be useful for double-color-image encryption. In addition, another format of color images known as indexed images [9] and noise and occlusion performances [17–19], can also be investigated.

Acknowledgements

The authors are grateful to the reviewers for their comments and constructive suggestions to further improve the original manuscript.

References

[1] P. Refregier, B. Javidi, Opt. Lett. 20 (1995) 767.
[2] B. Javidi, T. Nomura, Opt. Lett. 25 (2000) 28.
[3] L. Chen, D. Zhao, Opt. Express 14 (2006) 8552.
[4] B. Hennelly, J.T. Sheridan, Opt. Lett. 28 (2003) 269.

[5] M. Joshi, C. Shakher, K. Singh, Opt. Commun. 281 (2008) 5713.
[6] G. Situ, J. Zhang, Opt. Lett. 30 (2005) 1306.
[7] Y. Shi, G. Situ, J. Zhang, Opt. Lett. 32 (2007) 1914.
[8] Y. Zhang, B. Wang, Opt. Lett. 33 (2008) 2443.
[9] S.Q. Zhang, M.A. Karim, Microwave Opt. Technol. Lett. 21 (1999) 318.
[10] L. Chen, D. Zhao, Opt. Express 15 (2007) 16080.
[11] M. Joshi, C. Shakher, K. Singh, Opt. Lasers Eng. 47 (2009) 721.
[12] F. Ge, L. Chen, D. Zhao, Opt. Commun. 281 (2008) 4254.
[13] X.F. Meng, L.Z. Cai, X.L. Yang, X.F. Xu, G.Y. Dong, X.X. Shen, H. Zhang, Y.R. Wang, Appl. Opt. 46 (2007) 4694.
[14] C.K. Huang, H.H. Nien, Opt. Commun. 282 (2009) 2123.
[15] F.J. Dyson, H. Falk, Am. Math. Mon. 99 (1992) 603.
[16] http://sipi.usc.edu/database.
[17] X.F. Meng, L.Z. Cai, X.L. Yang, X.X. Shen, G.Y. Dong, Appl. Opt. 45 (2006) 3289.
[18] R. Tao, Y. Xin, Y. Wang, Opt. Express 15 (2007) 16067.
[19] B. Javidi, L. Bernard, N. Towghi, Opt. Eng. 38 (1999) 9.