This document is downloaded from DR-NTU (https://dr.ntu.edu.sg)
Nanyang Technological University, Singapore.

Color image encryption based on interference and virtual optics

Quan, Chenggen; Tay, Cho Jui; Fu, Yu; Chen, Wen

2009

Tay, C. J., Quan, C., Chen, W., & Fu, Y. (2009). Color image encryption based on interference and virtual optics. Optics and Laser Technology, (42), 409-415.

https://hdl.handle.net/10356/92123

https://doi.org/10.1016/j.optlastec.2009.08.016

This is the author created version of a work that has been peer reviewed and accepted for publication by Optics and Laser Technology, Elsevier. It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [DOI: http://dx.doi.org/10.1016/j.optlastec.2009.08.016]

Downloaded on 24 Aug 2022 22:36:51 SGT

Color image encryption based on interference and virtual optics

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

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

*Corresponding author. Tel.:+6565168089; fax: +6567791459.

E-mail address: mpeqcg@nus.edu.sg (C.Quan).

ABSTRACT

We propose two approaches to encrypt color images based on interference and virtual optics. In the first method, a color image is first decomposed into three independent channels, i.e., red, green and blue. Each channel of the input image is encrypted into two random phase-only masks based on interference. In the second method, a color image is first converted into an image matrix and a color map, and only the image matrix is encrypted into random-phase masks based on interference. After the phase masks are retrieved, a concept based on virtual optics is further applied to enhance the security level. Numerical simulations are demonstrated to show the feasibility and effectiveness of the proposed methods.

Keywords: Color image encryption, Interference, Fractional Fourier transform (FRFT)

1. Introduction

With the rapid development of modern communication techniques, the unauthorized distributions of information have become a serious problem, and optical encryption techniques are an important field for information security. Numerous methods, such as double random-phase masks encoding [1,2], digital holography [3], virtual optics [4] and fractional Fourier transform (FRFT) [5,6], have been proposed. In addition, a phase retrieval method based on an iterative algorithm [7] was proposed, and to avoid the iteration operation a simpler algorithm using a wave superposition approach without any iteration [8] has also been demonstrated. However, as a monochromatic light is used to illuminate a color image, the real color information of a decrypted image will be lost. Since the color information of an image is useful in practical applications, color image encryption [3,6,9–13] has become an important issue. 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] presented a color image encryption using wavelength multiplexing based on lensless Fresnel transform holograms. Chen and Zhao [10] also proposed color information processing with fractional Fourier transforms and digital hologram. Joshi et al. [11] proposed a nonlinear 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. Recently, Huang and Nien [13]

demonstrated the use of the chaotic sequences generated by a chaotic system as an encryption code in color image encryption.

In this paper, we propose two approaches to encrypt color images based on interference [8] and virtual optics. In the first method, a color image is first decomposed into three independent channels, i.e., red, green and blue. Each channel of the input image is then encrypted into two random phase-only masks based on interference. In the second method, a color image is first converted into an image matrix and a color map, and only the image matrix is then converted into two random-phase masks based on interference. After the phase masks are retrieved, a concept based on virtual optics is further applied to enhance the security level. Numerical simulations are demonstrated to show the feasibility and effectiveness of the proposed methods.

2. Theoretical description

A schematic numerical experimental arrangement is described in Fig. 1. A color image usually consists of red, green and blue values with certain proportions, and is first decomposed into three channels. To obtain the input 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 this study, two phase-only masks are placed at the same distance from the image plane within a channel. As a plane wave illuminates phase-only masks M_1 and M_2 at red channel, an interference in the image plane is described by

$$\sqrt{O(x,y)}\exp[j2\pi P_1(x,y)] = FT^{-1}\left[H\left(f_\xi, f_\eta; d_1\right)M_1\left(f_\xi, f_\eta\right)\right] + FT^{-1}\left[H\left(f_\xi, f_\eta; d_1\right)M_2\left(f_\xi, f_\eta\right)\right], \quad (1)$$

where $O(x, y)$ denotes a normalized input image with non-negative values at red channel, $P_1(x, y)$ a map randomly distributed in [0,1], $j = \sqrt{-1}$, f_ξ and f_η 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 $M_1(\xi, \eta)$ and $M_2(\xi, \eta)$, d_1 denotes a distance between the phase-only mask and the image plane, and $H(f_\xi, f_\eta;\ d_1)$a transfer function given by

$$H\left(f_\xi, f_\eta;\ d_1\right) = \exp\left[-jk_1 d_1(1 - \lambda_1^2 f_\xi^2 - \lambda_1^2 f_\eta^2)^{1/2}\right], \quad (2)$$

where λ_1 denotes a wavelength of light source at the red channel, and wave number $k_1 = 2\pi/\lambda_1$.

Hence, the red channel of the original image is embedded into two phase-only masks as [8]

$$M_1(\xi,\eta) = ang(T) - \arccos\left[abs(T)/2\right], \quad (3)$$

$$M_2(\xi,\eta) = ang\{T - \exp[jM_1(\xi,\eta)]\} \quad (4)$$

where $T = FT^{-1}(FT\{\sqrt{O(x,y)}\exp[j2\pi P_1(x,y)]\}/H(f_\xi, f_\eta;\ d_1))$, ang denotes an arc-tangent operation, *FT* denotes a 2D Fourier transform, and abs denotes modulus of a complex amplitude. In this study, the values of $abs(T)/2$ are compared with a threshold value of 1, and values larger than the threshold value are set as 1. Similarly, phase-only masks M_3 and M_4 for the green channel, and phase-only masks M_5 and M_6 for the blue channel can also be obtained. In practice, a constant value, such as 2π can be added to all the retrieved phase masks M_1–M_6 to avoid negative values when a spatial light modulator is used. To enhance the security level, phase-only masks M_1–M_6 are further processed in fractional Fourier domain based on the concept of virtual optics. For simplicity, an one-dimensional FRFT [14] is analyzed, and FRFT with an order a is described by

$$FRFT_a[M_1(\xi)] = \int_{-\infty}^{+\infty} M_1(\xi)\exp[j2\pi Q_1(\xi)]\,T_a(x_a,\xi)d\xi, \tag{5}$$

where

$$T_a(x_a,\xi) = \begin{cases} R\exp\{j\pi[x_a^2\cot(a\pi/2) + \xi^2\cot(a\pi/2) - 2x_a\xi\csc(a\pi/2)]\} & if\ a \neq 2m \\ \delta(x_a - \xi) & if\ a = 4m \\ \delta(x_a + \xi) & if\ a = 4m \pm 2 \end{cases},$$

m denotes an integer, $Q_1(\xi)$ denotes the values randomly distributed in [0, 1] and $R = \sqrt{1 - jcot(a\pi/2)}$. In this study, different random maps of $P_1(x,y)$ and $Q_1(\xi,\eta)$ are used in different channels.

For image decryption, FRFT with an order of $(-a)$ is first carried out, and a complex conjugate of $\exp[j2\pi Q_1(\xi,\eta)]$ is then multiplied. A light source with a correct wavelength is used to illuminate the two retrieved phase-only masks at each channel, and a decrypted color image is obtained by incorporating the three decrypted channels.

The first method described above is based on a combination of multiple wavelengths, interference and virtual optics. To avoid the multiple-step operation, a concept based on an indexed image [9] is employed. An original color image is first converted into an image matrix and a color map. The image matrix is divided by a constant value before image encryption, and is then encrypted based on interference method and virtual optics. Hence, two random-phase masks (M_7 and M_8) before FRFT and a color map are obtained. For image decryption, FRFT with an order of $(-a)$ is also carried out, and a complex conjugate of $\exp[j2\pi Q_1(\xi,\eta)]$ is then multiplied. A light source is used to illuminate the two retrieved phase masks, and a decrypted color image is obtained by a combination of the decrypted image matrix (multiplied by the constant value) and the color map. Since complex amplitudes are obtained by the use of the FRFT method, the proposed techniques mentioned above are more suitable for a digital usage.

A correlation coefficient (CC) is calculated to evaluate the decrypted image $O'(x,y)$.

$$CC = \frac{\sum_m \sum_n (O_{mn} - \bar{O})(O'_{mn} - \bar{O}')}{\sqrt{[\sum_m \sum_n (O_{mn} - \bar{O})^2][\sum_m \sum_n (O'_{mn} - \bar{O}')^2]}} \quad (6)$$

where $\bar{O}$ *or* $\bar{O}'$ denotes the mean of the elements of an image. A CC value of unity indicates that the original image is perfectly retrieved.

3. Numerical experiment and results discussion

A numerical experiment as shown in Fig. 1 is conducted to show the feasibility and effectiveness of the first method. For simplicity, collimation operations of the waves are not shown. The distances between the phase mask plane for red, green and blue channels and the image plane are respectively 60 cm, 50 cm and 40 cm, and the corresponding wavelengths are $\lambda_1 = 636$ nm, $\lambda_2 = 537.8$ nm and $\lambda_3 = 441.6$ nm. An original color image (512 x 512 pixels) with different types of peppers [15] is shown in Fig. 2(a), and in the image plane a pixel size of 10μm is used. In this study, the FRFT function orders for red, green and blue channels are (0.42, 0.44, 0.46, 0.48), (0.47, 0.49, 0.51, 0.53) and (0.52, 0.54, 0.56, 0.58), respectively. Note that two phase masks are retrieved for each channel, and two FRFT function orders are required for each extracted phase mask. As a light source with a single wavelength (λ_1 *or* λ_2, *or* λ_3)is used, the corresponding decrypted images are obtained as shown in Figs. 2(b)–(d). It can be seen that using a monochromatic light the real color information of the input image is lost. Phase masks M_1~M_6 are obtained with the proposed method, and Figs. 3(a) and (b) show two retrieved phase-only masks M_1 and M_2 (red channel) before the FRFT operation. It is seen in Figs. 3(a) and (b) that the retrieved phase-only masks are distributed randomly. In addition, random-phase masks M_3~M_6 (green and blue channels) can also be retrieved by the use of a similar approach. The obvious advantage of the interference method is that the phase retrieval method can be carried out without any iteration [8,16]. Note that since a color image contains three channels, a digital format with three channels is used to demonstrate the retrieved random-phase masks. Fig. 3(c) shows a decrypted image using all correct security parameters. The CC values for the three channels in Fig. 3(c) are 1. Fig. 3(d) shows a decrypted image using incorrect phase masks M_1–M_6 but with all other correct security parameters, such as FRFT function orders, wavelengths and distances. The average CC values for the red, green and blue channels are 5.95×10^{-4}, -1.70×10^{-4} and -5.93×10^{-4}, respectively. It is seen that no information on the original color image is obtained.

To evaluate the sensitivity of a function order in 2D FRFT, relationships between the CC value and a function order error are studied. In each channel, there are two extracted phase masks, and each phase mask requires two function orders for 2D FRFT. Fig. 4(a) shows that a relatively small function order error would render the CC values at the red channel as low as

zero. Similarly, the effect of a function order error for the green and blue channels is shown in Figs. 4(b) and (c), respectively. Fig. 4(d) shows a decrypted image with only one FRFT function order error of 0.03 at the red channel but with all other correct security parameters. Fig. 4(e) shows a decrypted image with only one function order error of 0.03 at the red channel and another function order error of 0.03 at the green channel. Fig. 4(f) shows a decrypted image with only one function order error of 0.03 at the green channel and another function order error of 0.03 at the blue channel. It is shown in Figs. 4(d)–(f) that a real color image cannot be obtained when incorrect parameters are used. As one FRFT function order error of 0.03 occurs in each channel, the decrypted image becomes totally random and no information can be observed. Fig. 4(g) shows a decrypted image with errors of 8 nm for wavelengths λ_1, λ_2 and λ_3 at both wave paths but with all other correct security keys. The CC values for red, green and blue channels in Fig. 4(g) are 0.16, 0.38 and 0.33, respectively. Fig. 4(h) shows a decrypted image using distance errors of 10 mm at both wave paths for all three channels but with all other correct security keys. The CC values for the red, green and blue channels in Fig. 4(h) are 0.14, 0.33 and 0.28, respectively. It is shown again that the real color information is lost when incorrect security keys are used. We have also investigated the tolerance to the loss of encrypted data and the occlusions of certain percentage of pixels from the encrypted complex masks (after the FRFT operation) before image decryption. Figs. 5(a) and (b) show the decrypted images with 6.25% and 50% occlusions of all encrypted complex masks. The CC values in Figs. 5(a) and (b) for the red, green and blue channels are respectively (0.16, 0.29, 0.18) and (0.07, 0.03, 0.03). It is demonstrated that the quality of the decrypted image degrades with an increase of occlusion. The influence of noise on the decrypted image is also studied, and it is found that the decrypted image is sensitive to noise. For instance, when the Gaussian noise (mean zero and variance 0.02) is added to all encrypted complex masks, the CC values of a decrypted image at red, green and blue channels are -0.01, -0.02 and -0.01, respectively. The small CC values might be due to the relatively small values of the retrieved phase masks (before FRFT) and the FRFT operation.

The numerical experimental arrangement as shown in Fig. 1 is modified as only one channel to demonstrate the feasibility and effectiveness of the second method. The distance between the phase mask plane and the image plane is d = 70cm and a wavelength of λ = 636 nm is used. A color image as shown in Fig. 2(a) is studied, and pixel size in the image plane is$10\mu m$. The FRFT function orders for the retrieved phase masks M_7 and M_8 are set as (0.42, 0.44) and (0.46, 0.48), respectively. Figs. 6(a) and (b) show an image matrix (512 ×512 pixels) and a color map (256 ×3 pixels), respectively. To effectively implement the interference algorithm, the image matrix is divided by a constant value of 1000 before the encryption operation. Figs. 6(c) and (d) show two retrieved phase masks M_7 and M_8 before the implementation of FRFT. It is shown that the retrieved phase masks have been distributed randomly and no information on the original image can be observed. Fig. 7(a) shows a decrypted image using incorrect phase masks M_7 and M_8 but with all other correct security keys. Average CC value for the decrypted image in Fig. 7(a) is 0.0025. It is shown again that the original color image

cannot be observed. Figs. 7(b)–(d) show decrypted images with only one function order error of 0.03 for 2D FRFT (in phase mask M_7), a wavelength error of 8 nm at both wave paths, and a recording distance error of 10mm at both wave paths, respectively. It is shown that a real color image cannot be obtained. We have also investigated the influence of the occlusion and noise on decrypted images when the indexed image method is applied. For brevity, the detailed results are not presented. It is also found that the decrypted images are shown to be sensitive to noise and occlusion operations. Fig. 7(e) shows a decrypted image using all correct security parameters, and the resultant CC value is 1.

4. Conclusions

In this paper, we have proposed two approaches to encrypt color images based on interference and virtual optics. The first method employs three channels and wavelengths multiplexing, while the second method employs an indexed image. Through a combination of interference method and virtual optics, the original image can be effectively encrypted into random maps. Compared with conventional phase retrieval methods, the interference method can be carried out without any iteration. Hence, the proposed methods are able to effectively encrypt color images based on a combination of multiple wavelengths or an indexed image, interference and virtual optics. Numerical results demonstrate that the proposed methods are feasible and effective for color image encryption.

References

[1] Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding. Opt Lett 1995; 20:767–9.

[2] Javidi B. Securing information with optical technologies. Phys Today 1997; 50:27–32.

[3] Chen L, Zhao D. Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms. Opt Express 2006; 14:8552–60.

[4] Peng X, Cui Z, Tan T. Information encryption with virtual-optics imaging system. Opt Commun 2002; 212:235–45.

[5] Unnikrishnan G, Joseph J, Singh K. Optical encryption by double-random phase encoding in the fractional Fourier domain. Opt Lett 2000; 25:887–9.

[6] Joshi M, Shakher C, Singh K. Color image encryption and decryption for twin images in fractional Fourier domain. Opt Commun 2008; 281: 5713–5720.

[7] Situ G, Zhang J. A lensless optical security system based on computer-generated phase only masks. Opt Commun 2004; 232:115–22.

[8] Zhang Y, Wang B. Optical image encryption based on interference. Opt Lett 2008; 33:2443–5.

[9] Zhang SQ, Karim MA. Color image encryption using double random phase encoding. Microwave Opt Technol Lett 1999;21:318–23.

[10] Chen L, Zhao D. Color information processing (coding and synthesis) with fractional Fourier transforms and digital holography. Opt Express 2007; 15:16080–9.

[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; 47:721–7.

[12] Ge F, Chen L, Zhao D. A half-blind color image hiding and encryption method in fractional Fourier domains. Opt Commun 2008; 281:4254–60.

[13] Huang CK, Nien HH. Multi chaotic systems based pixel shuffle for image encryption. Opt Commun 2009; 282:2123–7.

[14] Ozaktas HM, Zalevsky Z, Kutay MA. The fractional Fourier transform with applications in optics and signal processing. Singapore: Wiley; 2001.

[15] http://sipi.usc.edu/database.

[16] Chen W, Quan C, Tay CJ. Optical color image encryption based on Arnold transform and interference method. Opt Commun 2009; 282:3680–5.

List of Figures

Fig. 1. (Color online) A schematic numerical experimental arrangement

Fig. 2. (Color online) (a) An original color image of peppers; decrypted images with (b) a single wavelength λ_1, (c) a single wavelength λ_2, and (d) a single wavelength λ_3.

Fig. 3. (Color online) Retrieved phase-only masks (a) M_1 and (b) M_2 at red channel; decrypted images with (c) all correct security keys and (d) incorrect masks M_1–M_6.

Fig. 4. (Color online) Relationships between CC values and one FRFT function order error at (a) red channel, (b) green channel, (c) blue channel; decrypted images with (d) one incorrect FRFT function order at red channel, (e) two incorrect FRFT function orders, (f) two other incorrect FRFT function orders, (g) incorrect wavelengths, (h) incorrect distances.

Fig. 5. (Color online) Decrypted images with an occlusion of (a) 6.25%; and (b) 50% on all encrypted complex masks.

Fig. 6. (a) An image matrix; (b) a color map; (c) a retrieved phase mask M_7; (d) a retrieved phase mask M_8.

Fig. 7. (Color online) Decrypted images with (a) incorrect phase masks M_7 and M_8; (b) one incorrect FRFT function order in the phase mask M_7; (c) incorrect wavelengths; (d) incorrect distances; (e) all correct security parameters.

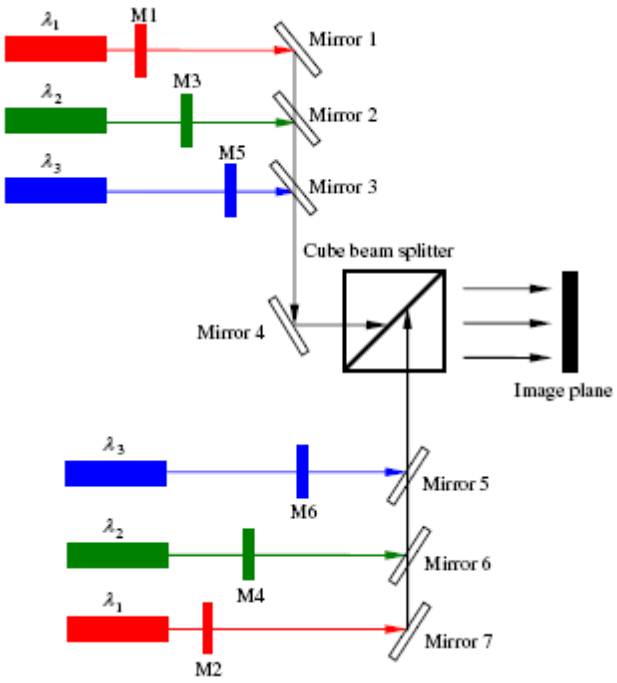
λ1
M1
Mirror 1
λ2
M3
Mirror 2
λ3
M5
Mirror 3
Cube beam splitter
Mirror 4
Image plane
λ3
M6
Mirror 5
λ2
M4
Mirror 6
λ1
M2
Mirror 7

Fig. 1

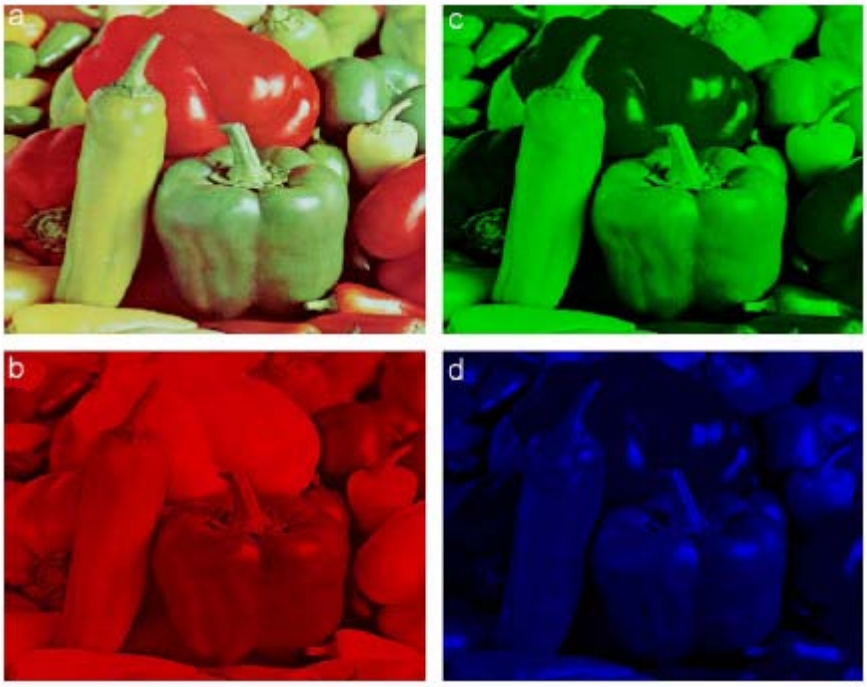

Fig. 2

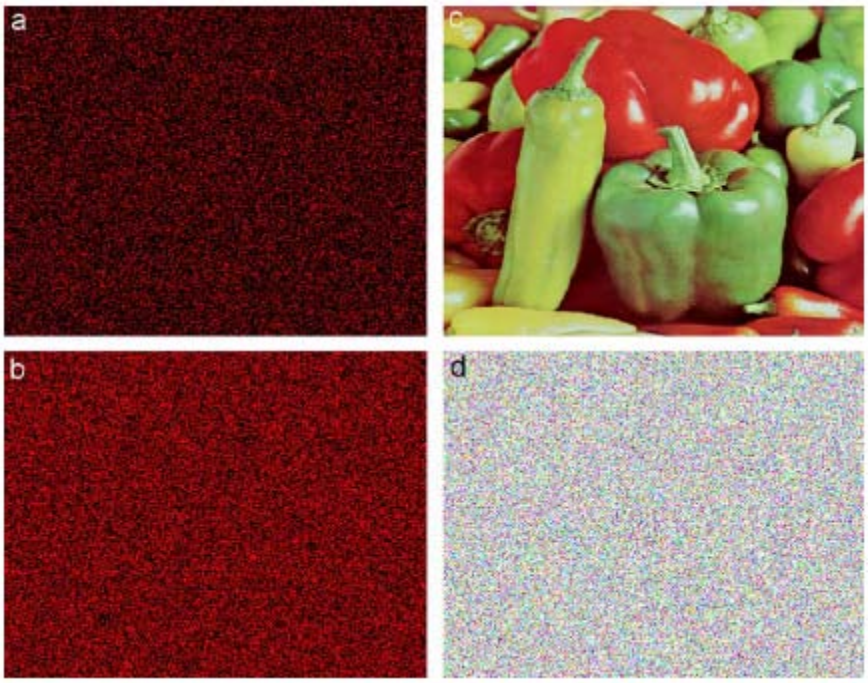

Fig. 3

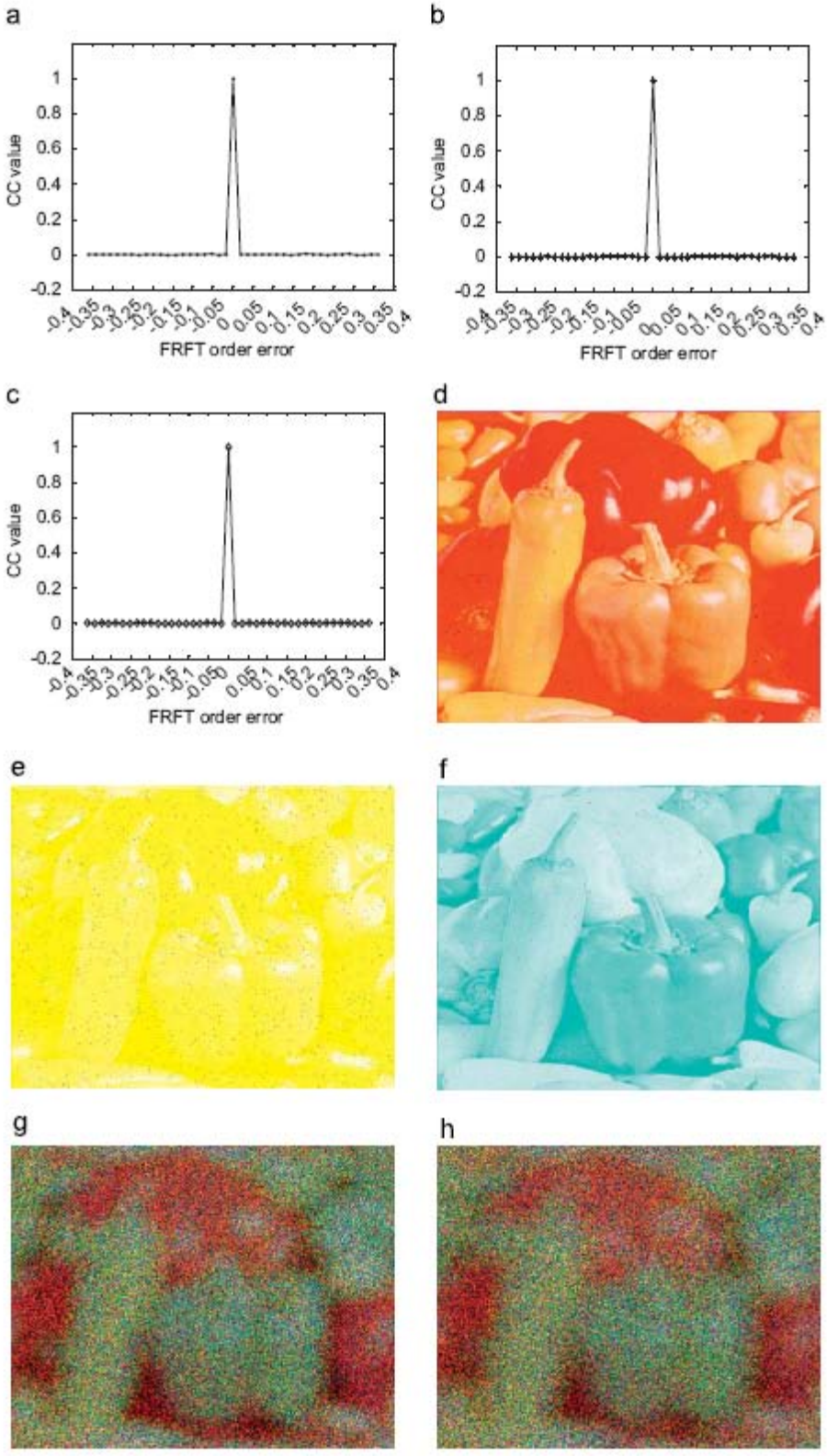
a
b
c
d
e
f
g
h
CC value
FRFT order error
1
0.8
0.6
0.4
0.2
0
-0.2
-0.4
-0.35
-0.3
-0.25
-0.2
-0.15
-0.1
-0.05
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0.4

Fig. 4

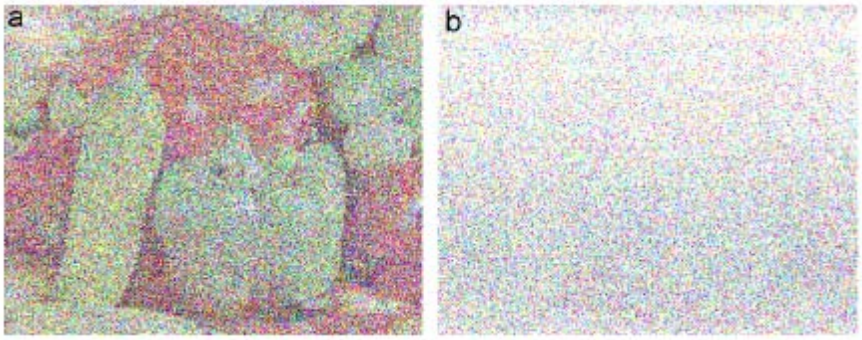

Fig. 5

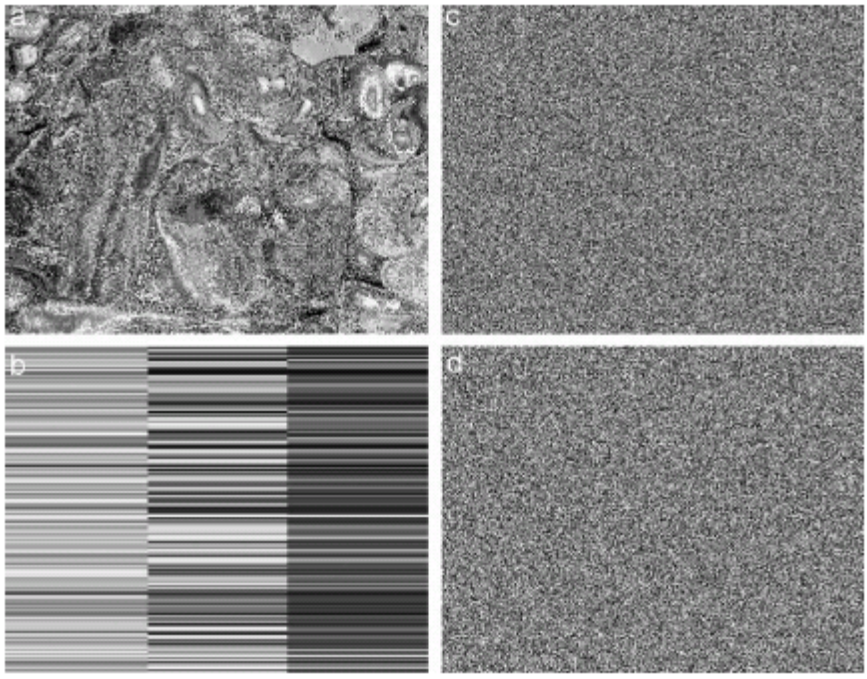

Fig. 6

Fig. 7