Image fusion using wavelet transform and its application to asymmetric cryptosystem and hiding

Isha Mehra and Naveen K. Nishchal*
Department of Physics, Indian Institute of Technology Patna, Patliputra, Patna-800 013, Bihar, India
nkn@iitp.ac.in

Abstract: Image fusion is a popular method which provides better quality fused image for interpreting the image data. In this paper, color image fusion using wavelet transform is applied for securing data through asymmetric encryption scheme and image hiding. The components of a color image corresponding to different wavelengths (red, green, and blue) are fused together using discrete wavelet transform for obtaining a better quality retrieved color image. The fused color components are encrypted using amplitude- and phase-truncation approach in Fresnel transform domain. Also, the individual color components are transformed into different cover images in order to result disguising information of input image to an attacker. Asymmetric keys, Fresnel propagation parameters, weighing factor, and three cover images provide enlarged key space and hence enhanced security. Computer simulation results support the idea of the proposed fused color image encryption scheme.

©2014 Optical Society of America

OCIS codes: (060.4785) Optical security and encryption; (070.0070) Fourier optics and signal processing; (100.2000) Digital image processing.

References and links
1. B. Javidi, Optical and Digital Techniques for Information Security (Springer, 2005).
2. S. Zhang and M. A. Karim, “Color image encryption using double random phase encoding,” Microw. Opt. Technol. Lett. 21(5), 318–323 (1999).
3. L. Chen and D. Zhao, “Color optical image encryption by wavelength multiplexing and lensless Fresnel transform holograms,” Opt. Express 14(19), 8552–8560 (2006).
4. M. Joshi, Chandrashakher, and K. Singh, “Color image encryption and decryption using fractional Fourier transform,” Opt. Commun. 279(1), 35–42 (2007).
5. X. Deng and D. Zhao, “Single-channel color image encryption using a modified Gerchberg-Saxton algorithm and mutual encoding in the Fresnel domain,” Appl. Opt. 50(31), 6019–6025 (2011).
6. H.-E. Hwang, “Optical color image encryption based on the wavelength multiplexing using cascaded phase-only masks in Fresnel transform domain,” Opt. Commun. 285(5), 567–573 (2012).
7. B. Javidi, P. Ferraro, S. H. Hong, S. De Nicola, A. Finizio, D. Alfieri, and G. Pierattini, “Three-dimensional image fusion by use of multiwavelength digital holography,” Opt. Lett. 30(2), 144–146 (2005).
8. B. Javidi, C. M. Do, S. H. Hong, and T. Nomura, “Multi-spectral holographic three-dimensional image fusion using discrete wavelet transform,” J. Disp. Technol. 2(4), 411–417 (2006).
9. D. C. Tseng, Y. L. Chen, and M. S. C. Liu, “Wavelet based multispectral image fusion” in Proceedings of Geoscience and Remote Sensing Symposium (IGARSS), 4, 1956–1958 (2001).
10. A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, “Simultaneous fusion, compression, and encryption of multiple images,” Opt. Express 19(24), 24023–24029 (2011).
11. S. Hong, W. M. Moon, H. Paik, and G. Choi, “Data fusion of multiple polarimetric SAR images using discrete wavelet transform” in Proceedings of IEEE Int. Geoscience and Remote Sensing Symp., 6, 3323–3325 (2002).
12. A. Garzelli, “Possibilities and limitations of the use of wavesets in image fusion” IEEE International Geoscience and Remote Sensing Symp. 1, 66–68 (2002).
13. G. Hong and Y. Zhang, “High resolution image fusion based on wavelet and HIS transformations” Proceedings of 2nd GRSS/ISPRS Joint Workshop on Remote Sensing and Data Fusion 99–104 (2003).
14. F. Sadjadi, “Invariant algebra and the fusion of multi-spectral information,” Inf. Fusion 3(1), 39–50 (2002).
15. A. Alfalou and C. Brosseau, “Optical image compression and encryption methods,” Adv. Opt. Photon. 1(3), 589–636 (2009).
16. A. Alfalou and C. Brosseau, “Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption,” Opt. Lett. 35(11), 1914–1916 (2010).
1. Introduction

Over the past few decades, securing information using optical methods has been an attractive research area because of inherent multidimensional nature and parallel processing capability [1]. Most of the optical schemes for information security reported in literature deal with binary or gray-scale images. Even the color images are encrypted and decrypted by a monochromatic light source and hence they do not preserve their original color information. Also, color images contribute to a higher level of security than binary and gray-value images. Zhang and Karim [2] for the first time reported a method using double random phase encoding (DRPE) for securing color images. Securing a high resolution color image is a challenging task and is of growing interest in the optical information processing field [3–6].

In the literature, usually for recording a digital hologram, a single wavelength is used but, if multiple wavelengths are used, then a high quality color object can be reconstructed. Javidi et al. [7] recorded two holograms using red and green wavelengths and then fused all reconstructed images to obtain a high quality colored image. Further, this idea was extended employing multiple wavelengths [8]. Fusion techniques play an important role in all such multi-wavelength phenomenon [9–14] and provide better quality fused image for interpreting the image data. Alfalou and Brosseau [15] discussed several optical compression and multi-wavelength phenomenon [9–14] and provide better quality fused image for interpreting employing multiple wavelengths [8]. Fusion techniques play an important role in all such multi-wavelength phenomenon [9–14] and provide better quality fused image for interpreting the image data. Alfalou and Brosseau [15] discussed several optical compression and encryption methods. They reported the relation between compression and encryption. Further, they also proposed an algorithm to compress and encrypt simultaneously multiple images [16].

The conventional DRPE technique [1] in which two random phase masks (RPMs) are used as the security keys to encrypt an input image, belongs to the class of symmetric cryptosystem. In such cryptosystems, the keys used for encryption are identical to the decryption keys. Hence, linearity makes such cryptosystems insecure. To overcome this issue,
asymmetric cryptosystem has been proposed [17–21]. Asymmetric cryptosystem due to its nonlinear behavior and asymmetric nature of keys makes the encryption system more strong.

Apart from encryption, image hiding is an attractive way to encode information into white noise or some other image. Kishk and Javidi [22] proposed a method to hide a double phase-encoded image in the spatial domain. Takai and Mifune [23] proposed a method to embed the watermarking image by digital holography. Several optical techniques for image hiding and watermarking employing various domains have been reported [23–30].

Wavelet transform (WT) is also one of the signal processing tools, which is used for analysis of optical and digital signals [31]. It has good local optimization features as well as the multi-resolution analysis features, which makes it suitable for optical information processing [31–33]. Dang and Chau [33] used WT for image encryption. They presented a scheme after combining discrete WT for image compression and block cipher data encryption standard for image encryption. Martin et al. [34] proposed efficient encryption scheme by using a stream cipher to encrypt only the significant bits for individual coefficients using color set partitioning in hierarchical trees (C-SPIHT) algorithm. Recently, Bao et al. [35] proposed an image encryption scheme in wavelet domain where input image is encrypted to some other image instead of a noisy distribution.

In this paper, we propose color image fusion technique using WT for security and image hiding applications. The different components of a color image corresponding to different wavelengths are fused together using discrete WT for obtaining a better quality color image. The individual fused color components are encrypted using amplitude- and phase-truncation approach in Fresnel transform domain. Also, the encrypted components are transformed into different cover images in order to result disguising information of input image to an attacker. Asymmetric keys, Fresnel propagation parameters, weighing factor, and three cover images provide enhanced security. The simulation results demonstrate that data fusion is an effective technique, which can also be used for multispectral image encryption. Apart from multispectral image encryption, the proposed scheme can be further extended for simultaneous compression and encryption of multiple images [15,16].

2. Fusion technique for high quality colored image

In this section, color image components corresponding to different wavelengths are decomposed into wavelet coefficients using discrete WT [8]. In a one-dimensional (1-D) discrete WT, an input function \( f(x) \) is decomposed into coefficients with starting scale \( m_o \), as:

\[
W_\phi(m_o,k) = \left( \frac{1}{\sqrt{L'}} \right) \sum_k f(x) \phi_{m_o,k} \tag{1}
\]

\[
W_\psi(m,k) = \left( \frac{1}{\sqrt{L'}} \right) \sum_k f(x) \psi_{m,k} \tag{2}
\]

Here, \( L' \) scaling parameter of wavelet. \( W_\phi(m_o,k) \) and \( W_\psi(m,k) \) are called as approximation and detailed coefficients respectively. In a two-dimensional (2D) discrete WT, a 1-D discrete WT is first performed on the rows and on the columns of data. This results in one set of approximation coefficients \( W_\phi(m,r,s) \) and three sets of detailed coefficients \( W_\psi(m,r,s) \) where \( \eta = \{H,V,D\} \) represents horizontal, vertical and diagonal components.

Let \( f(x,y) \) be a 2D color image to be encrypted. Here, \( f_r(x,y), f_g(x,y), \) and \( f_b(x,y) \) represent their red, green, and blue components, respectively. Suppose, the recovered images corresponding to wavelengths \( \lambda_r \) and \( \lambda_r + \delta \lambda_r \) are given as \( f'_r(x,y) \) and \( f''_r(x,y) \) respectively. Similarly, the recovered images corresponding to wavelengths \( \lambda_g \) and \( \lambda_g + \delta \lambda_g \) are given as \( f'_g(x,y) \) and \( f''_g(x,y) \) respectively. Similarly, the recovered images corresponding to wavelengths \( \lambda_b \) and \( \lambda_b + \delta \lambda_b \) are given as \( f'_b(x,y) \) and \( f''_b(x,y) \) respectively. Now, discrete WT is performed for fusion in order to reconstruct better quality color image [8].

\[
W_{fLL} = \text{AVG} (W_{LL11}, W_{LL22}) \tag{3}
\]
The combination of all four components is given as
\[ g'_r (\psi, \phi) = \{ W_{FLr}, W_{FHLr}, W_{FHLr}, W_{FHHr} \} \] (7)

Similarly for green and blue components, the combinations of coefficients are
\[ g'_g (\psi, \phi) = \{ W_{FLg}, W_{FHLg}, W_{FHLg}, W_{FHHg} \} \] (8)
\[ g'_b (\psi, \phi) = \{ W_{FLb}, W_{FHLb}, W_{FHLb}, W_{FHHb} \} \] (9)

Hence, individual fused components of color image are obtained using WT in order to retrieve better quality of a color image.

3. Encryption of fused color components using phase-truncation approach

In order to encrypt all fused color components, amplitude- and phase truncation based asymmetric encryption scheme has been carried out. The principle of encryption has been depicted in Fig. 1(a) for red component only. Fused red component, \( g'_r (\psi, \phi) \) is bonded with an RPM, \( R_1(\psi, \phi) \) and its Fresnel transformation (FrT) is obtained at some distance \( z_1 \). The obtained spectrum is phase-truncated (PT) and we get, \( H_{r}(u,v) \).

\[ H_{r}(u,v) = PT \left[ FrT_{z_1} \left[ g'_r (\psi, \phi) \times R_{1}(\psi, \phi) \right] \right] \] (10)

Here, \( R_1(\psi, \phi) \) is the random white sequence uniformly distributed in the interval [0,2\( \pi \)]. For successful retrieval of the red component, the decryption key; \( k_r(u,v) \) is generated after amplitude-truncation (AT), as defined in the following Equation,

\[ k_r(u,v) = AT \left[ FrT_{z_1} \left[ g'_r (\psi, \phi) \times R_{1}(\psi, \phi) \right] \right] \] (11)

Similarly, fused green and blue components are encrypted using different RPMs and corresponding PT operated and AT operated values are obtained.

\[ H_{g}(u,v) = PT \left[ FrT_{z_2} \left[ g'_g (\psi, \phi) \times R_{2}(\psi, \phi) \right] \right] \] (12)

For successful retrieval of the green component, the decryption key; \( k_g(u,v) \) is generated.

\[ k_g(u,v) = AT \left[ FrT_{z_2} \left[ g'_g (\psi, \phi) \times R_{2}(\psi, \phi) \right] \right] \] (13)
\[ H_{b}(u,v) = PT \left[ FrT_{z_3} \left[ g'_b (\psi, \phi) \times R_{3}(\psi, \phi) \right] \right] \] (14)

For successful retrieval of the blue component, the decryption key; \( k_b(u,v) \) is generated.

\[ k_b(u,v) = AT \left[ FrT_{z_3} \left[ g'_b (\psi, \phi) \times R_{3}(\psi, \phi) \right] \right] \] (15)

Thus, individual fused components are encrypted using amplitude-and phase truncation approach and the decryption keys corresponding to red, green and blue components are generated.
4. Converting each encrypted color component into different visible cover image

The obtained three different color encrypted images are separately converted to three different cover images to give the disguising information of input image to the attacker. The flowchart is given in Fig. 1(b). A different cover image, \( m_r(\xi, \eta) \) having its size four times larger than the existing encrypted image is considered. The discrete WT is applied to the cover image. Suppose the wavelet coefficients after discrete WT operation are obtained as \( \{ W_{LLr}, W_{HLr}, W_{LHr}, W_{HHr} \} \), so to convert the encrypted red component image into cover image, HH sub-band of the cover image is replaced with encrypted red component with the weighing factor \( \alpha_r \). Here \( \alpha_r \) varies from 1 to 100. Higher the value of \( \alpha_r \), better will be the quality of the reconstructed cover image.

Finally, the inverse discrete WT (IDWT) operation will yield the cover image corresponding to red component.

\[
m'_r(\xi, \eta) = \text{IDWT}(W_{LLr}, W_{HLr}, W_{LHr}, H_r / \alpha_r)
\] (16)

Similarly green and blue encrypted images are converted to corresponding cover images i.e. \( m'_g(\xi, \eta) \) and \( m'_b(\xi, \eta) \), respectively.

For image decryption, use of correct keys and same wavelet are necessary as shown in Fig. 1(c). We used Haar wavelet in this study. All the three cover images are first decomposed into four wavelet sub-bands using Haar wavelet. After being extracted from the HH sub-band, the encrypted images are then applied with the inverse process of the image encryption to reconstruct the original image color components as follows:

For decryption of red color component, the key obtained \( k_r(u,v) \), is bonded with the extracted cipher-text, \( H_r(u,v) \), and its inverse Fresnel transformation is obtained for distance \( z_1 \). The obtained spectrum is phase-truncated, as given by \( f'_r(x,y) \).

\[
g'_r(\psi, \phi) = \text{PT}[\text{FrT}_{-z_1}[H_r(u,v) \times k_r(u,v)]]
\] (17)
\[ g'_g(\psi, \phi) = PT \{ FrT_{-z_{g}} [H_g(u, v) \times k_g(u, v)] \} \]  \hspace{1cm} (18)
\[ g'_b(\psi, \phi) = PT \{ FrT_{-z_{b}} [H_b(u, v) \times k_b(u, v)] \} \]  \hspace{1cm} (19)

Then, IDWT is applied to all three components separately to have a good quality of red component of reconstructed image back.

\[ f'_r(x, y) = IDWT(g'_r(\psi, \phi)) \]  \hspace{1cm} (20)
\[ f'_g(x, y) = IDWT(g'_g(\psi, \phi)) \]  \hspace{1cm} (21)
\[ f'_b(x, y) = IDWT(g'_b(\psi, \phi)) \]  \hspace{1cm} (22)

Finally, better quality colored image is given as

\[ f(x, y) = f'_r(x, y) \otimes f'_g(x, y) \otimes f'_b(x, y) \]  \hspace{1cm} (23)

Thus, use of correct asymmetric keys and same wavelet i.e. Haar wavelet, decrypts a better quality color image.

5. Simulation results

The simulation study was carried out using MATLAB 2010(b). Figure 2(a) shows the input color image of size 256 \times 256 pixels. Figures 2(b) and 2(c) represent the red components corresponding to \( \lambda_r = 632.8 \) nm and \( \lambda_r + \delta \lambda_r = 631.8 \) nm, respectively. Figures 2(d) and 2(e) represent the green components corresponding to \( \lambda_g = 532 \) nm and \( \lambda_g + \delta \lambda_g = 531 \) nm, respectively. Figures 2(f) and 2(g) represent the blue components corresponding to \( \lambda_b = 475 \) nm and \( \lambda_b + \delta \lambda_b = 476 \) nm, respectively.

Discrete WT has been carried out for fusion purpose in order to reconstruct better quality color image. Figures 3(a)-3(d) show all four coefficients of discrete WT of reconstructed red component corresponding to wavelength \( \lambda_r \). Figures 3(e)-3(h) show all four coefficients of discrete WT of reconstructed red component corresponding to wavelength \( \lambda_r \). All the three fused color components are shown in Figs. 4(a)-4(c). After fusion of wavelet coefficients, all three color components in WT domain will undergo encryption process through amplitude- and phase truncation approach. Figure 5(a) shows asymmetric (decryption) key, \( k_r(u, v) \) corresponding to red component. Figure 5(b) shows encrypted image, \( H_r(u, v) \) corresponding to red component. Figure 5(c) shows asymmetric (decryption) key, \( k_g(u, v) \) corresponding to green component. Figure 5(d) shows encrypted image, \( H_g(u, v) \) corresponding to green component. Figure 5(e) shows asymmetric (decryption) key, \( k_b(u, v) \) corresponding to blue component. Figure 5(f) shows encrypted image, \( H_b(u, v) \) corresponding to blue component.

The three different colored encrypted images, \( H_r(u, v), H_g(u, v), \) and \( H_b(u, v) \) are separately converted to three different cover images to give the disguising information of input image to the attacker. The three cover images of size 512 \times 512 pixels for all three components have been shown in Figs. 6(a)-6(c). After discrete WT operation of input cover images and replacement of higher frequency component with encrypted images, corresponding results has been shown in Figs. 6(d)-6(f). Thus, The three different colored encrypted images, \( H_r(u, v), H_g(u, v), \) and \( H_b(u, v) \) are separately converted to three different cover images to give the disguising appearance of input image. The final cover images obtained after inverse discrete WT operation has been shown in Figs. 6(g)-6(i). Finally, use of correct asymmetric keys and Haar wavelet decrypts a better quality color image as shown in Fig. 6(j).

To check the security of the proposed scheme, we applied the special attack [18] to the proposed color image encryption scheme. To start with the specific attack algorithm, the exact real valued encrypted image is required. But, this encrypted image is further hidden into cover images using parameters \( a \), type (Haar) and level of wavelets. These parameters are
unknown to the attacker. So, the proposed scheme resists specific attack. The mean square error (MSE) values calculated between input color image and retrieved color image has been plotted against the number of iterations as shown in Fig. 6(k). In this case, we computed the MSE for 100 iterations. It can be observed that the MSE value never converged to zero. Also asymmetric keys, fractional orders, and encryption keys corresponding to three primary color components enhance the security key space in the proposed scheme. Also, Bao et al. [35] have claimed that hiding through such schemes withstand the brute force attack. Hence, it can be inferred that the proposed scheme resists both specific and brute force attack.

Fig. 2. (a) Input color of size 256 × 256 pixels; (b) red component of colored image corresponding to $\lambda = 632.8$nm; (c) red component of colored image corresponding to $\lambda + \delta \lambda = 631.8$nm; (d) green component of colored image corresponding to $\lambda = 532$nm; (e) green component of colored image corresponding to $\lambda + \delta \lambda = 531$nm; (f) blue component of colored image corresponding to $\lambda = 475$nm; and (g) blue component of colored image corresponding to $\lambda + \delta \lambda = 476$nm.

Fig. 3. (a)-(d) Four coefficients of DWT of reconstructed red component corresponding to wavelength, $\lambda_r$. (e)-(h) all four coefficients of DWT of reconstructed red component corresponding to wavelength $\lambda_r + \delta \lambda_r$. 

(C) 2014 OSA 10 March 2014 | Vol. 22, No. 5 | DOI:10.1364/OE.22.005474 | OPTICS EXPRESS 5480
To study the effectiveness of the proposed security scheme, we calculated peak signal to noise ratio (PSNR) [30]. The value of PSNR for the retrieved, color image is 41.5606. With the calculated PSNR value, we infer that when the correct keys are used the PSNR value is extremely high.
6. Conclusion

We proposed color image fusion using wavelet transform for security applications that employs asymmetric encryption scheme and image hiding. Discrete Haar wavelet transform has been used for color image fusion. Further, each fused color components are encrypted using amplitude- and phase-truncation approach. Then, the individual color components are transformed into different cover image or fake image in order to mislead the attacker. Asymmetric keys, Fresnel propagation parameters, weighing factor, and three cover images constitutes the security parameters in the proposed scheme. Apart from this, lens less scheme provides error free environment to the proposed security scheme. The simulation results demonstrate that data fusion is an effective technique, which can be used for multispectral image encryption.

Acknowledgment

The authors acknowledge the funding from the Council of Scientific and Industrial Research, Government of India, under Grant No. 03/(1183)/10/EMR-II.