Optics Communications 335 (2015) 153–160

Contents lists available at ScienceDirect

Optics Communications

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

Wavelet-based image fusion for securing multiple images through asymmetric keys

Isha Mehra, Naveen K. Nishchal *

Department of Physics, Indian Institute of Technology Patna, Patliputra Colony, Patna 800 013, India

ARTICLE INFO

Article history:
Received 12 July 2014
Accepted 14 September 2014
Available online 26 September 2014

Keywords:
Image fusion
Optical asymmetric cryptosystem
Wavelet transforms
Interference
Fractional Fourier transform

ABSTRACT

Image fusion is one of the popular methods which provides better quality fused image for interpreting an image data. Discrete wavelet transform based fusion technique is one such method, in which low and high frequency components are merged together to improve the image content. In this paper, we propose this fusion technique for generating asymmetric keys for securing multiple images. An input image to be encrypted is digitally encoded into two phase-only masks employing the principle of optical interference. This process has been repeated for three different input images; however, it can be extended to *n* images. Now, one of the phase-only masks corresponding to each input image is preserved as a phase key while another set of phase masks are fused together. This fused image is called the encrypted image. Unlike optical asymmetric encryption technique based on amplitude- and phase-truncation approach, here, four asymmetric keys are generated corresponding to each image. Asymmetric keys corresponding to each image, fractional orders, phase-only masks, level of decomposition and type of wavelet, enlarge the key space and hence offer enhanced security. The proposed method is demonstrated through the simulation results.

1. Introduction

In the past few decades, optical information security techniques have been widely studied because of multi-dimensional and parallel processing nature of large storage memories at great speeds [1,2]. The double random phase encoding (DRPE) technique is the basic optical image encryption architecture [3]. Most of the existing encryption schemes deal with binary and gray-scale images. The encryption and decryption are performed with the help of monochromatic light. Thus, the decrypted images do not preserve their color information. Color image encryption has become an important field of research for data security [4], because of presence of all three (red, green, and blue) components. Now-a-days, the multispectral data, which consists of several spectral bands, plays an importance role over the quality and content of the data.

The multispectral data received from satellites and airborne sensors are being increasingly available for further processing and analysis for various applications, including remote sensing [5]. The fused/combined information of various sensors is the source of comprehensive data. The fusion of low and high resolution multispectral images is a widely used technique because the fused images possess complementary information from different sources. Discrete wavelet transform (DWT) based fusion technique is one such method in which low and high frequency components are merged together. Since many of such data are significant from security point of view, therefore, it becomes necessary to develop an optical encryption technique for securing fused data/images.

Any optical cryptosystem is not highly secure until it has enhanced key space with the use of various degrees of freedom. For example, the security of the basic DRPE scheme was improved by employing different optical domains [6,7]. However, due to inherent linearity, such cryptosystems are not highly secure [8–10]. Frauel et al. [11] proved that DRPE resists brute force attack but is susceptible to chosen plain-text and known plain-text attacks. To overcome the problems of linearity in DRPE, amplitude- and phase-truncation based asymmetric cryptosystem has been proposed [12–16]. Recently, an encryption scheme has been proposed in which phase-retrieval algorithm is applied twice for generating two asymmetric keys from intermediate phases [17,18]. However, there are few problems associated with such cryptosystems; one of them is system's complexity for repetitive saving of phase keys in the form of holograms. Secondly, for single step amplitude- and phase-truncation, only one asymmetric key can be generated. For these reasons, the phase-truncation based asymmetric cryptosystem has been proved to be vulnerable against

* Corresponding author. Tel.: +91 612 2552027; fax: +91 612 2277383.
E-mail address: nkn@iitp.ac.in (N.K. Nishchal).

http://dx.doi.org/10.1016/j.optcom.2014.09.040
0030-4018/

specific attack [19]. Thereafter, many modifications have been reported in order to improve its security [20–22].

Wavelet transform (WT) is one of the signal processing tools, which is used for analyzing optical signals [23–27]. Fusion techniques play an important role in the entire multi-wavelength phenomenon [28]. Alfalou and Brosseau [29–31] reported a new spectral multiple image fusion analysis based on the discrete cosine transform. Recently, a wavelet based color image fusion scheme for securing data through phase truncation approach and image hiding has been proposed [32].

In this paper, DWT based fusion technique has been utilized for securing multiple data. Each image to be encrypted is digitally encoded into two phase-only masks (POM) in fractional Fourier transform (FRT) domain using the interference principle [33]. One of the POMs is preserved as a phase key while other one is discrete wavelet transformed. The POMs corresponding to different images are fused together using single level DWT for obtaining the encrypted image. Thus, the interference phenomenon and the WT based fusion plays an important role for securing multiple images. Use of the optical interference helps enhance the security of the scheme. In this case, all four asymmetric keys (approximation, horizontal, vertical, and diagonal coefficients) are necessary for successful decryption. This is because, for decryption through interference principle, exact POMs are required. Also, in the interference based phenomenon, the inherent silhouette problem can be overcome through various existing known schemes [14,34]. Without using the concept of interference only the approximation coefficient (one asymmetric key) is enough to decrypt the input image with acceptable quality. Hence, the scheme becomes less secure.

2. Principle

2.1. Image encoding into two phase-only masks

The proposed encryption process is shown in Fig. 1(a). Let $f'_i(x,y)$ represents one of the input functions to be encrypted. This input image is encoded into two POMs, M_1 and M_2 analytically [33]. The complex function can be obtained using a random phase mask (RPM),

$$f_i(x,y) = f'_i(x,y)\exp[i2\pi\psi(x,y)] \quad (1)$$

where $\psi(x,y)$ is random distribution having between 0 and 1. The FRT of the two POMs consisting of phases, M_1 and M_2, optically interfere at the decryption plane to provide the complex input image $f_i(x,y)$ [33]. This complex distribution can be expressed as,

$$f_i(x,y) = \mathfrak{I}^{\alpha}\{\exp[iM_{1(i)}(\xi,\eta)]\} + \mathfrak{I}^{\alpha}\{\exp[iM_{2(i)}(\xi,\eta)]\} \quad (2)$$

where $\mathfrak{I}^{\alpha}\{.\}$ represents the FRT operation with order α. From Eq. (2) we can write,

$$\exp[iM_{1(i)}(\xi,\eta)] + \exp[iM_{2(i)}(\xi,\eta)] = \mathfrak{I}^{-\alpha}\{f_i(x,y)\} \quad (3)$$

Let us assume that

$$\exp[iM_{1(i)}(\xi,\eta)] + \exp[iM_{2(i)}(\xi,\eta)] = D \quad (4)$$

Then Eq. (4) can be written as

$$\exp[iM_{2(i)}(\xi,\eta)] = D - \exp[iM_{1(i)}(\xi,\eta)] \quad (5)$$

The two phase masks, $\exp[iM_{1(i)}(\xi,\eta)]$ and $\exp[iM_{2(i)}(\xi,\eta)]$ are the phase-only functions. Therefore, we have

$$\left|D - \exp[iM_{1(i)}(\xi,\eta)]\right|^2 = \{D - \exp[iM_{1(i)}(\xi,\eta)]\} \times \{D - \exp[iM_{1(i)}(\xi,\eta)]\}^* = 1 \quad (6)$$

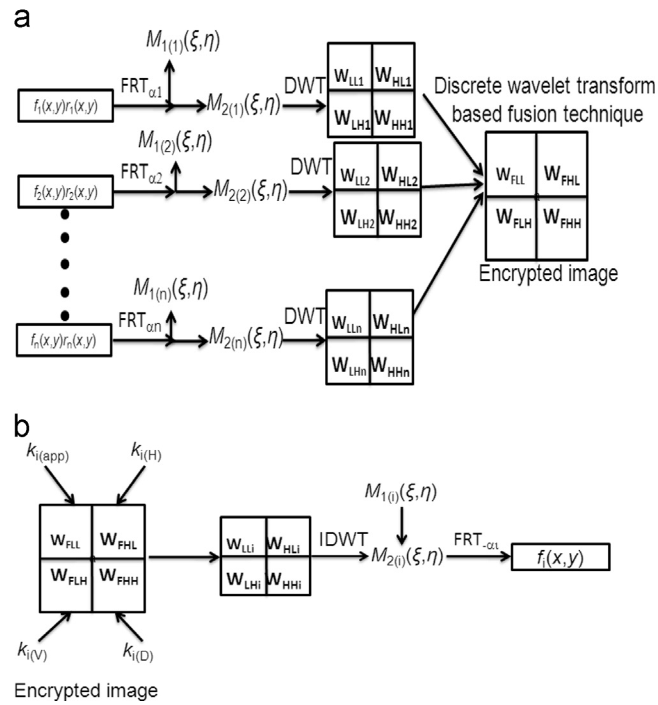

Fig. 1. Block diagram for multiple image encryption scheme using discrete wavelet transform based fusion technique.

Using Eq. (6), we can easily find POMs corresponding to ith image,

$$M_{1(i)}(\xi,\eta) = \arg(D) + \cos^{-1}\left\{\frac{|D|}{2}\right\} \quad (7)$$

$$M_{2(i)}(\xi,\eta) = \arg\{D - \exp(iM_{1(i)}(\xi,\eta))\} \quad (8)$$

where *arg*{.} represents the phase angle.

2.2. DWT based image fusion

In this section, POMs generated corresponding to different images are decomposed into wavelet coefficients using DWT [28]. In a one-dimensional (1-D) DWT, an input function $f(x)$ is decomposed into coefficients with the starting scale m_o as:

$$W_{\phi}(m_o,k) = (1/\sqrt{L'})\sum_k f(x)\psi_{m_o,k} \quad (9)$$

$$W_{\psi}(m,k) = (1/\sqrt{L'})\sum_k f(x)\psi_{m,k} \quad (10)$$

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

The wavelet coefficients obtained corresponding to $M_{1(1)}(\xi.\eta)$ are; $\{W_{LL1}, W_{HL1}, W_{LH1}, W_{HH1}\}$. The DWT operation of $M_{1(2)}(\xi.\eta)$ will yield $\{W_{LL2}, W_{HL2}, W_{LH2}, W_{HH2}\}$, and POM obtained from ith image will yield $\{W_{LLi}, W_{HLi}, W_{LHi}, W_{HHi}\}$, where L and H represent low and high frequency components, respectively. Now, different wavelet coefficients of n number of images are fused together through DWT, in which the high and low frequency components