Optics and Lasers in Engineering ∎ (∎∎∎∎) ∎∎∎–∎∎∎

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Asymmetric color image encryption based on singular value decomposition

Lili Yao, Caojin Yuan *, Junjie Qiang, Shaotong Feng, Shouping Nie

Key Laboratory for Opto-Electronic Technology of Jiangsu Province, Nanjing Normal University, WenYuan Road 1, 210023 Nanjing, China

ARTICLE INFO

Article history:
Received 21 January 2016
Received in revised form
5 June 2016
Accepted 6 June 2016

Keywords:
Color image encryption
Asymmetric
Singular value decomposition
Indexed image

ABSTRACT

A novel asymmetric color image encryption approach by using singular value decomposition (SVD) is proposed. The original color image is encrypted into a ciphertext shown as an indexed image by using the proposed method. The red, green and blue components of the color image are subsequently encoded into a complex function which is then separated into U, S and V parts by SVD. The data matrix of the ciphertext is obtained by multiplying orthogonal matrices U and V while implementing phase-truncation. Diagonal entries of the three diagonal matrices of the SVD results are abstracted and scrambling combined to construct the colormap of the ciphertext. Thus, the encrypted indexed image covers less space than the original image. For decryption, the original color image cannot be recovered without private keys which are obtained from phase-truncation and the orthogonality of V. Computer simulations are presented to evaluate the performance of the proposed algorithm. We also analyze the security of the proposed system.

1. Introduction

With the rapid development of computer network technology, distribution and exchange information become more quickly and easily. The ensuing question is how to ensure the security of important information. Since Refregier and Javidi [1] proposed the double random phase encryption, optical encryption techniques, such as the use of optical transform [2–6], interference [7,8], and polarized light encoding [9], have attracted increasing attention. Although the optical encryption techniques show a variety of advantages such as multi-dimensional operation and parallel processing capability, recent works have demonstrated that traditional optical encryption techniques are vulnerable to different types of attacks due to the inherent linearity of the overall system. To overcome this shortcoming, nonlinear phase-truncation techniques [10,11] and nonlinear encryption methods based on phase retrieval algorithm [12,13] have been proposed. Besides aforementioned methods, the invisibility of decoded images [14,15] has also been proposed to guarantee the security of symmetric cryptosystem. Mathematical techniques such as vector operation [16], natural logarithm operation [17], log-polar transform [18], chaos [19,20] and singular value decomposition (SVD) [21,22] have also been used in encryption systems to overcome the issue of linearity.

Singular value decomposition (SVD) [23] is an important factorization of a rectangular real or complex matrix with many applications in image processing. SVD-based watermarking techniques [24,25] have been mostly considered in recent years mainly as larger variation of the singular values does not occur when a small perturbation is added to an image. As SVD gives a one-way asymmetrical decomposition algorithm [21], SVD-based image encryption techniques have been further proposed in recent years. In these methods, three segments of the results of SVD are always used as three gray-scale ciphertexts after individually encoded. For instance, Chen et al. presented image encryption based on SVD and Arnold transform in fractional domain [22]. In this technique, the fractional Fourier spectrum of the original gray-scale image is decomposed into three segments by SVD. All the three parts are Arnold transformed to obtain three encrypted images and assigned to different authorized users for security. Abuturab proposed color information verification system based on SVD in gyrator transform domains [21]. In this technique, each channel of the original color image is independently modulated by random phase masks and then separately gyrator transformed. The three gyrator spectra are multiplied to get one encoded image. The image is then separated into three segments by SVD. All the three parts are individually gyrator transformed and assigned to different authorized users for security.

In this paper, we propose a new asymmetric color image encoding technique based on SVD. The red, green and blue components of the color image are subsequently encoded into a complex function which is then separated into U, S and V parts by SVD. The obtained orthogonal matrices U and V are multiplied and phase-truncated to obtain the data matrix of the ciphertext image, while the diagonal

* Corresponding author.
E-mail address: optyuan@163.com (C. Yuan).

http://dx.doi.org/10.1016/j.optlaseng.2016.06.007
0143-8166/

entries in three matrices S are abstracted to form the colormap of the ciphertext image. In this way, the original color image with $3 \times N \times N$ pixels is encrypted into an indexed image with $N \times N + N \times 3$ pixels, which decreases the burden of storage and transmission as compared with aforementioned SVD-based image encryption methods [21,22]. Moreover, in the proposed method, private keys obtained from phase-truncation guarantee the safety, and private keys obtained from the orthogonality of V establish an additional security layer. Numerical simulation results have been shown to demonstrate the efficiency and security of the proposed cryptosystem.

The rest of the paper is organized as follows. In Section 2, the principle of SVD is briefly introduced and the processes of encryption and decryption are described in detail. In Section 3, numerical simulations are presented to demonstrate the performance of the proposed algorithm. In Section 4, security analysis of the algorithm are presented. Some conclusions are drawn in Section 5.

2. Encryption and decryption process

2.1. Singular value decomposition (SVD)

Singular value decomposition (SVD) is an important matrix decomposition method used in linear algebra. An image f of size $N \times N$ can be decomposed as:

$$f = USV^T, \tag{1}$$

where T represents transpose.

S is an $N \times N$ diagonal matrix

$$S = \begin{pmatrix} \sigma_1 & 0 & \cdots & 0 \\ 0 & \sigma_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & \sigma_N \end{pmatrix} \tag{2}$$

where σ_i are singular values of $f, \sigma_1 \geq \sigma_2 \geq \sigma_3 \cdots \geq \sigma_r \geq \sigma_{r+1} = \cdots = \sigma_N = 0$, $r = rank(I)$ and U, V^T are $N \times N$ orthogonal matrices, i.e., $UU^T = I$, $VV^T = I$.

2.2. Encryption algorithm

The procedure of the encryption algorithm is shown in Fig. 1(a). The encryption process contains two parts: the formation of the data matrix and the formation of the colormap matrix. Supposing the size of the color image chosen for encryption are of $3 \times N \times N$ pixels, the encryption process is as follows:

2.2.1. Formation of the data matrix

1. The red and green components of the original color image, f_r and f_g, are encoded in a complex function as the real part and the imaginary part. Then, the complex function is singular value decomposed.

$$[U_1 S_1 V_1] = SVD\,(f_r + if_g) \tag{3}$$

2. The obtained orthogonal matrices U_1 and V_1 are multiplied and phase- and amplitude-truncated.

$$c_1 = U_1 \cdot V_1 \tag{4}$$
$$c_{1a} = PT(c_1) \tag{5}$$
$$P_1 = AT(c_1) \tag{6}$$

where the symbol represents dot product and the operators PT and AT stand for phase- and amplitude-truncation, respectively.

3. c_{1a} and the blue component of the original color image, f_b, are encoded in another complex function which is encrypted similarly using (Eqs. (3)-(6).

$$[U_2 S_2 V_2] = SVD(c_{1a} + if_b) \tag{7}$$
$$c_2 = U_2 \cdot V_2 \tag{8}$$
$$c_{2a} = PT(c_2) \tag{9}$$
$$P_2 = AT(c_2) \tag{10}$$

4. c_{2a} is singular value decomposed and the data matrix of the final ciphertext image is obtained after the range of the multiplication result of matrices U_3 and V_3 is adjusted to [0,255].

$$[U_3 S_3 V_3] = SVD(c_{2a}) \tag{11}$$
$$c_3 = U_3 \cdot V_3 \tag{12}$$

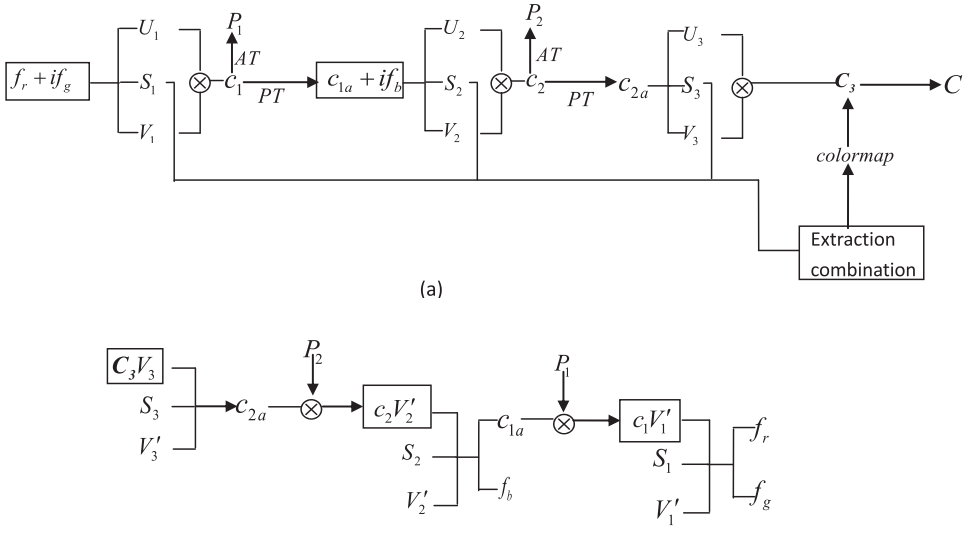

Fig. 1. Flowcharts of proposed (a) encryption and (b) decryption algorithms.

Please cite this article as: Yao L, et al. Asymmetric color image encryption based on singular value decomposition. Opt Laser Eng (2016), http://dx.doi.org/10.1016/j.optlaseng.2016.06.007