Optik 125 (2014) 4474–4479

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Triple color images encryption algorithm based on scrambling and the reality-preserving fractional discrete cosine transform

Jianhua Wu[a,*], Fangfang Guo[a], Yaru Liang[b], Nanrun Zhou[a]

[a] Department of Electronic Information Engineering, Nanchang University, China
[b] School of Mechatronic Engineering, Nanchang University, China

ARTICLE INFO

Article history:
Received 8 August 2013
Accepted 12 February 2014

Keywords:
Image encryption
Cyclic shift
Arnold transform
Reality-preserving fractional discrete cosine transform
Generating sequence

ABSTRACT

An image encryption algorithm to secure three color images simultaneously by combining scrambling with the reality-preserving fractional discrete cosine transform (RPFrDCT) is proposed. The three color images to be encrypted are converted to their indexed formats by extracting their color maps, which can be considered as the three components of a color image. These three components are affected each other by scrambling the interims obtained from vertically and horizontally combining the three indexed formats with the help of the chaos-based cyclic shift. The three scrambled components are separately transformed with the RPFrDCT, in which the generating sequences are determined by the Chirikov standard chaotic map. Arnold transform is used to further enhance the security. Due to the inherent properties of the chaotic maps, the cipher keys are highly sensitive. Additionally, the cipher image is a single color image instead of three color ones, and is convenient for display, storage and transmission due to the reality property of RPFrDCT. Numerical simulations are performed to show the validity of the proposed algorithm.

1. Introduction

The past few decades have witnessed the rapid development of the network multimedia, communication and propagation techniques and the exchange of digital information especially images has also greatly increased. Image encryption has become a major task for information security since the issues about illegal data access on Internet are becoming more and more serious. Since optical image encryption system based on double random phase encoding (DPRE) by the Fourier transform was firstly proposed by Refregier and Javidi [1], it has been extended to other optical transform domains [2–10]. With the emergence of color images, color image encryption [11–16] has become an important issue because of the usefulness of the color information in practical applications. The most common method is the multichannel decomposition based on the RGB model or HSI model, however, the complexity and the cost will be increased since multiple channels must be involved during the encryption and transmission processes. A representative method of single-channel color image encryption is based on the digital transformation of the color image to indexed format [16], which is more compact and reliable than the multichannel ones.

As a new concept in image encryption field, multiple-image encryption has attracted much attention, which encrypts several different images together. Situ and Zhang [17] firstly employed wavelength multiplexing to realize multiple-image encryption. The qualities of the corresponding decrypted images in the algorithm, however, are not perfect due to the cross-talk effects between images. Subsequently, various multiple-image encryption schemes have been designed [18–28]. The most commonly used for two images is based on the complex function, in which two original images are respectively regarded as the real/amplitude and the imaginary/phase of the complex function. Although it can realize multiple-image encryption through the complex function, it may not be implemented in real time since the encrypted images contain both amplitude information and phase information, which makes it difficult to display, store and transfer. Wang and Zhao [27,28] proposed the multiple-image encryption method using the phase-truncation and phase retrieval, which makes the cryptosystem nonlinear and the output real-valued. However, the truncated phases as the cipher keys, whose size is the same as the cipher images, need to be transferred to the receivers for decryption, giving rise to increase of the burden of transmission. Besides, the phase-retrieval process is very time consuming.

* Corresponding author at: Department of Electronic Information Engineering, Nanchang University, 999 Rd. Xuefu, Honggutan New District, Nanchang 330031, P. R. China. Tel.: +86 791 83969336; fax: +86 791 83969338.
E-mail addresses: jhwu@ncu.edu.cn (J. Wu), hellosuger@qq.com (F. Guo), liangyaru@126.com (Y. Liang), nrzhou@ncu.edu.cn (N. Zhou).

http://dx.doi.org/10.1016/j.ijleo.2014.02.026
0030-4026/

To display, store and transfer images conveniently, in this paper, we present a new encryption algorithm to secure three color images simultaneously by use of scrambling and the reality-preserving fractional discrete cosine transform (RPFrDCT). The encrypted image is a single real-valued color image, which is convenient for display, storage and transmission. Firstly, the three color images to be encrypted are separately converted to their indexed formats by extracting their color maps, which can be considered as the three components of a color image. Then two scrambling schemes are implemented to make these three components affect each other by scrambling the interims obtained from vertically and horizontally combining the three indexed formats with the help of the chaos-based cyclic shift. Next, the three scrambled components are separately transformed with the RPFrDCT, in which the generating sequences are determined by the chaotic map. Finally, Arnold transform is used to further enhance the security. Due to the inherent properties of the chaotic maps, the system is highly sensitive to the cipher keys. Numerical simulation results show the feasibility and the validity of the proposed algorithm.

The rest of this paper is organized as follows. Section 2 reviews the principles of the reality-preserving fractional discrete cosine transform, the concept of true color and indexed color images, the Chirikov standard chaotic map, and the Arnold transform. The proposed encryption algorithm is also described in Section 2. Simulations and discussion are given in Section 3. Finally, a brief conclusion is drawn in last section.

2. Principles

2.1. Definition of the reality-preserving fractional discrete cosine transform

The fractional discrete cosine transform (FrDCT) is a generalization of the DCT. In current documents, even though several versions of fractional cosine transform have been derived, the FrDCT [31] different from those defined in [29,30] possesses the mathematical properties of reality in addition to the fundamental properties such as linearity, unitarity and additivity. And the reality is of importance for image encryption, which ensures the outputs are real for real inputs.

The FrDCT is derived based on the eigen-decomposition and eigenvalue substitution of the DCT-II kernel, which is denoted as:

$$\mathbf{C} = \left\| \frac{1}{\sqrt{N}} \varepsilon_k \cos\left(2\pi \frac{(2n+1)k}{4N}\right) \right\| \tag{1}$$

where $n, k = 0, 1, \ldots, N-1$ and $\varepsilon_0 = 1$, $\varepsilon_k = \sqrt{2}$ for $k > 1$.

The eigen decomposition of an $N \times N$ DCT-II matrix $\mathbf{C}$ can be expressed by:

$$\mathbf{C} = \mathbf{U}\Lambda\mathbf{U}^* = \sum_n \mathbf{U}_n e^{j\varphi_n} \tag{2}$$

where $\mathbf{U}$ is a unitary matrix, composed of columns (eigenvectors) $\mathbf{u}_n, \mathbf{u}_m^*\mathbf{u}_n = \delta_{mn}$, $\mathbf{U}_n = \mathbf{u}_n\mathbf{u}_n^*$, and $\mathbf{\Lambda}$ is the diagonal matrix with diagonal entries, i.e. eigenvalues λ_n, $\lambda_n = e^{j\varphi_n}$ with $0 < \varphi_n < \pi$.

The fractional discrete cosine transform matrix $\mathbf{C}_\alpha$ can be written by substituting the eigenvalues λ_n with their αth powers λ_n^α as follows:

$$\mathbf{C}_\alpha = \mathbf{U}\Lambda^\alpha\mathbf{U}^* \tag{3}$$

The matrix $\mathbf{C}_\alpha$ given by (3) can be rewritten in an alternative form in accordance with the eigenstructure of matrix $\mathbf{C}$:

$$C_\alpha = 2\mathrm{Re}\left[\sum_{n=1}^{K} \mathbf{U}_n \lambda_n^\alpha\right] + \mathbf{V}_1(1)^\alpha + \mathbf{V}_{-1}(-1)^\alpha \tag{4}$$

where $\mathbf{U}_n = \mathbf{u}_n\mathbf{u}_n^*$, $K = (N - \mu_1 - \mu_{-1})/2$, μ_1 and μ_{-1} represent the multiplicities of the eigenvalues 1 and -1, respectively. $\mathbf{V}_1$ collects the μ_1 matrices $\mathbf{U}_n$ corresponding to the eigenvalue 1 and similarly for $\mathbf{V}_{-1}$.

If $N = 4N_0$, N_0 is an integer, the absence of the $(\pm 1)^\alpha$ in (4) guarantees that $\mathbf{C}_\alpha$ becomes a real-valued matrix and can be written as:

$$\mathbf{C}_\alpha = 2\mathrm{Re}\left[\sum_{n=1}^{N/2} \mathbf{U}_n \, e^{j\omega_n\alpha}\right] = \sum_{n=1}^{N/2} (\mathbf{A}_n \cos\omega_n\alpha + \mathbf{B}_n \sin\omega_n\alpha) \tag{5}$$

$$\omega_n = \varphi_n + 2\pi q_n, n = 1, 2, \ldots, \frac{N}{2}, \quad 0 < \varphi_n < \pi, \tag{6}$$

where $\mathbf{A}_n = 2\mathrm{Re}[\mathbf{U}_n]$, $\mathbf{B}_n = -2\mathrm{Im}[\mathbf{U}_n]$, q_n is an arbitrary sequence of integers, and we call the sequence $\mathbf{q} = (q_1, q_2, \ldots, q_{N/2})$ the generating sequence (GS) of the FrDCT, which is introduced due to the multiplicity of the roots of the αth power of λ_n. Different choices of q_n lead to different matrices $\mathbf{C}_\alpha$ and, hence, to different FrDCT definitions. So taking the GS $\mathbf{q}$ as secret key can provide a huge key space. Readers can refer to [31] for more information about $\mathbf{q}$. The expansion of the FrDCT for a two-dimensional signal is straightforward and simple through two FrDCTs successively by rows and by columns.

2.2. Concept of true and indexed color images

A true color image can be treated as a three-dimensional (3-D) matrix with each pixel as a triplet corresponding to the values of the primary color components in RGB model, while an indexed color image consists of two 2-D matrices, i.e. an image matrix and a color map matrix. The color map is an $M \times 3$ array of class double containing floating-point values in the range [0, 1], whose length M is equal to the numbers of colors it defines. For example, M is 256 for an 8-bit color system. Each row of the color map specifies the red, green and blue components of a single color. An indexed image directly maps the pixel intensity values to the color map values. The color of each image pixel is determined by using the corresponding value of the image matrix as a pointer into color map [24]. After representing an RGB color image with its indexed format, the encryption of the color image can be simplified. Since the color map is uniquely defined for all color images in the same color system and only an indexed image needs to be encrypted, which is straightforward compared with the multichannel encryption. The color image can be retrieved after adding the color map to the decrypted indexed image [16].

2.3. Chirikov standard map

Chirikov standard map (CSM) [26] is an invertible area-preserving chaotic map for two canonical dynamical variables from a square with side 2π onto itself, i.e.:

$$\begin{cases} x_{i+1} = (x_i + y_i) \bmod 2\pi \\ y_{i+1} = (x_i + \delta \sin(x_i + y_i)) \bmod 2\pi \end{cases} \tag{7}$$

where $\delta > 0$ is the control parameter, and x_i and y_i both take real values in the range $[0, 2\pi)$ for all i. In this paper, the Chirikov standard map will be used twice, which respectively generates the random sequences to be applied to the cyclic shift and the generating sequences.

2.4. Arnold transform

As a simple scrambling method, Arnold transform (AT) commonly known as cat face transform is widely used. The transform is a process of clipping and splicing that realigns the pixel matrix of