Optics & Laser Technology 50 (2013) 1–7

Contents lists available at SciVerse ScienceDirect

Optics & Laser Technology

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

Color image security system using chaos-based cyclic shift and multiple-order discrete fractional cosine transform

Hong Liu [a,*], Hai Nan [b]

[a] College of Software, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[b] College of Computer Science, Chongqing University, Chongqing 400044, China

ARTICLE INFO

Article history:
Received 18 December 2012
Received in revised form
31 January 2013
Accepted 3 February 2013
Available online 5 March 2013

Keywords:
Color image encryption
Cyclic shift
Multiple-order discrete fractional cosine transform

ABSTRACT

In this paper, a color image encryption algorithm is designed by use of chaos-based cyclic shift and multiple-order discrete fractional cosine transform (MODFrCT). The RGB components of the color image are vertically combined and then simultaneously scrambled by chaos-based cyclic shift to make these three components affect each other. The scrambled RGB components are separately transformed with the MODFrCT, whose orders are determined by the Chirikov standard chaotic map. Based on chaotic inherent properties, the corresponding keys are highly sensitive. At the same time, the transmission of the cipher image is very fast since the DFrCT is a reality preserving transform. Simulation results proved the validity of the proposed algorithm.

1. Introduction

Images contain a large amount of information and are widely used in the Internet. Thus, their security has become a major issue of concern. Image encryption technology based on optics is an effective measure to ensure the information security and has gained great interest with the rapid development of communication technologies. Optical encryption methods own many intrinsic advantages, such as high speed and difficulty of unauthorized access.

Recently, a series of significant works on color image encryption have been researched and reported [1–8]. In [1], a novel method for color image encryption in the Fourier domain has been proposed by converting a color image into an index image format before encoding. The RGB components of color image are scrambled and encoded by the Arnold transform and DRPE [2], respectively. Color image is considered as three homophonous images and is imported into the optical encryption system [3,4]. The color image encryptions, based on the Arnold transform and color-blend operation in discrete cosine transform domains [5], FRFT [6], the rotation of color vector in the discrete Hartley transform [7], and the simultaneous encryption of a color and a gray-scale image using single-channel DRPE in the FRFT domain [8] have been also proposed. In these encryption algorithms, color image is decomposed into the components of red, green and blue (RGB). The same method is used to encrypt RGB components, which means to encrypt three images one after another independently and neglect the correlations between RGB components [9]. Furthermore, Chaos has also been introduced to image security due to its pseudo-randomness and sensitivity to initial conditions and control parameters. These inherent properties make chaotic maps a potential choice for designing cryptosystem [10–16]. There are many optical image encryption schemes combining the chaos theory [2,5,17,18].

In this paper, a novel color image encryption scheme using chaos-based cyclic shift and multiple-order discrete fractional cosine transform (MODFrCT) is proposed. An original color image is scrambled by the chaos-based cyclic shift without neglecting the correlations between RGB components. Subsequently each component (R, G and B) is transformed by the MODFrCT, where the fractional orders are determined by Chirikov standard chaotic map. Therefore, with the help of chaotic characteristics, the sensitivity of the keys is very excellent. In addition, if the input is real, then the output of DFrCT is also real. As a result, the decryption process does not increase the storage or transmission load as in the case of non-reality preserving transform [19].

The rest of this paper is organized in the following sequence. The proposed color image encryption algorithm including the basic theory is addressed in Section 2. In Section 3, some numerical simulations and discussions are given to demonstrate the validity of this algorithm. Concluding remarks are summarized in the final section.

* Corresponding author. Tel.: +86 23 6487 729.
E-mail address: liliary@163.com (H. Liu).

0030-3992/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlastec.2013.02.003

2. Color image encryption scheme

2.1. Basic theory

The Chirikov standard map can be expressed by the following formulas:

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

where $\delta > 0$ is the control parameter, and the ith states x_i and y_i both take real values in $[0,2\pi)$ for all i. The map is an invertible area-preserving chaotic map for two canonical dynamical variables from a square with side 2π onto itself. More on the Chirikov standard map can be found in [20,21].

The discrete fractional cosine transform (DFrCT) [22] of 1D signal $\mathbf{f}$ can be written as matrix multiplications as follows:

$$\Re^p(\mathbf{f}) = \mathbf{R}^p \mathbf{f} \quad (2)$$

where $\mathbf{R}^p$ is the kernel transforms of the DFrCT and p indicates the fractional order.

The DFrCT is a generalization of the DCT. It uses the eigen decomposition of the DCT kernel. The DFRFT kernel can be written as

$$\mathbf{R}^p = \mathbf{V}\mathbf{D}^p\mathbf{V}^T = \mathbf{V}\mathbf{D}^{2\pi/\alpha}\mathbf{V}^T = \mathbf{V}\mathrm{diag}\{1, e^{-j2\alpha}, \ldots, e^{-j2(N-1)\alpha}\}\mathbf{V}^T \quad (3)$$

where $\mathbf{V} = [\mathbf{v_0}|\mathbf{v}_2|\cdots|\mathbf{v_{2N-2}}]$, $\mathbf{v_k}$ is the kth order DFT Hermite eigenvector, p represents the fractional order and α indicates the rotation angle of transform in the time–frequency plane.

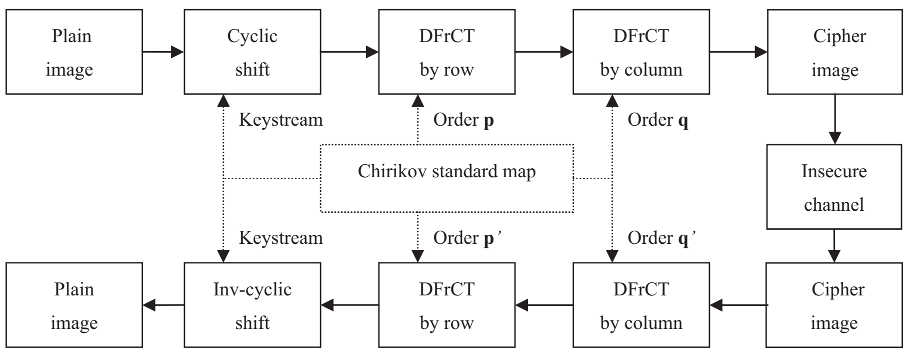

Fig. 1. Encryption and decryption process with the Chirikov standard map and DFrCT.

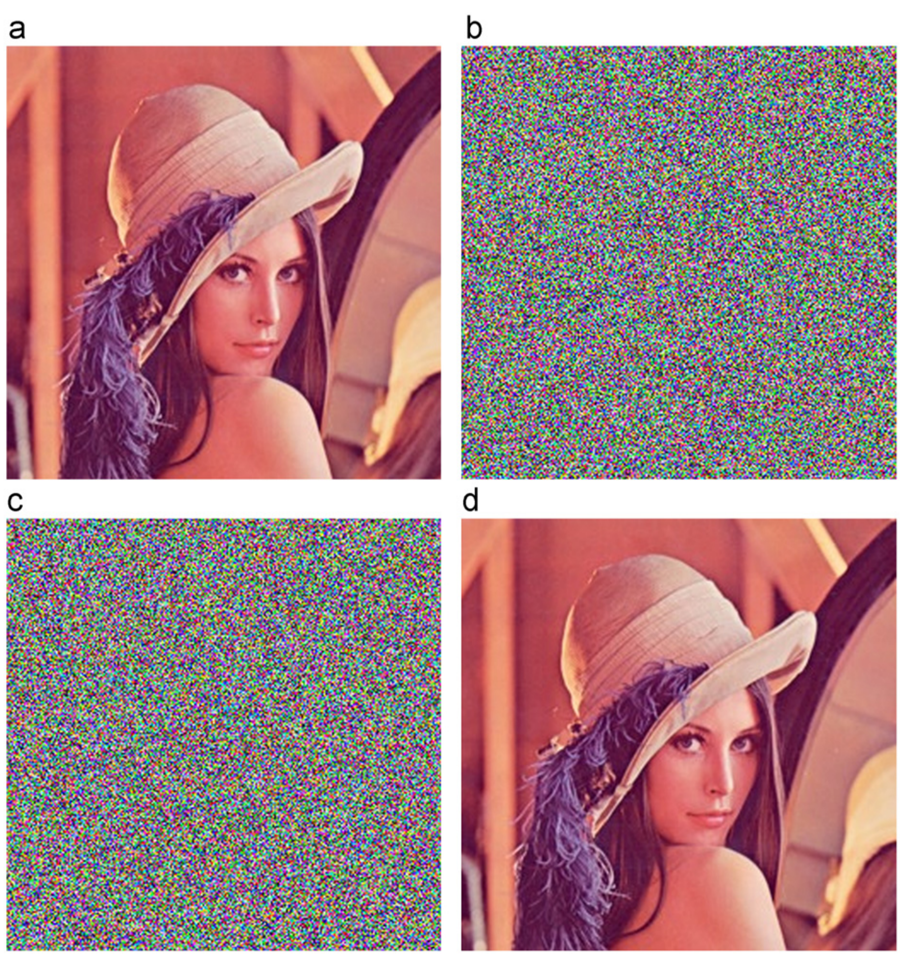

Fig. 2. Encryption and decryption results: (a) the original image, (b) the intermediate image after cyclic shift, (c) the cipher image and (d) the decrypted image.