Optics and Lasers in Engineering 51 (2013) 1327–1331

Contents lists available at SciVerse ScienceDirect

Optics and Lasers in Engineering

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

Double-image encryption by using chaos-based local pixel scrambling technique and gyrator transform

Huijuan Li [a,*], Yurong Wang [b], Haitao Yan [a], Liben Li [a], Qiuze Li [a], Xiaoyan Zhao [a]

[a] School of Physics and Engineering, Henan University of Science and Technology, Luoyang, Henan 471023, PR China
[b] School of Information Science and Engineering, Shandong University, Jinan, Shandong 250100, PR China

ARTICLE INFO

Article history:
Received 31 July 2012
Received in revised form
9 May 2013
Accepted 10 May 2013
Available online 10 June 2013

Keywords:
Image encryption
Arnold transform
Gyrator transform
Chaotic map

ABSTRACT

A novel double-image encryption algorithm is proposed by using chaos-based local pixel scrambling technique and gyrator transform. Two original images are first regarded as the amplitude and phase of a complex function. Arnold transform is used to scramble pixels at a local area of the complex function, where the position of the scrambled area and the Arnold transform frequency are generated by the standard map and logistic map respectively. Then the changed complex function is converted by gyrator transform. The two operations mentioned will be implemented iteratively. The system parameters in local pixel scrambling and gyrator transform serve as the keys of this encryption algorithm. Numerical simulation has been performed to test the validity and the security of the proposed encryption algorithm.

1. Introduction

With the rapid development of modern communication and propagation techniques, information security is becoming a serious problem in the processes of transmission and storage, especially in the image copying and downloading from Internet. Encryption is one way to ensure the security. Since Réfrégier and Javidi [1] proposed the double-random phase encoding technique, many optical techniques, such as digital holography [2,3], Fresnel transform [4,5], fractional Fourier transform [6,7], gyrator transform [8–10], and Hartley transform [11–13], have been used for image encryption.

The pixel scrambling operation, which can change the position of image pixel randomly, is another encryption method that has been considered for hiding the secret information to enhance image security [7,9,14–25]. At the same time, with the properties of sensitivity to initial conditions and control parameters, pseudo-randomness and ergodicity, chaotic maps have been widely used for constructing encryption scheme in pure digital image encryption [21,26–32].

In recent years, as a new information security technology, multiple-image encryption has attracted much attention owing to economic memory occupation and efficient transmission via a network. Situ and Zhang [33] first proposed a multiple-image encryption by using wavelength multiplexing. Subsequently various multiple image encryption schemes have been designed and reported [15,20,24,31,34–44].

In this paper, we present a new double-image encryption algorithm by using chaos-based local pixel scrambling technique and gyrator transform. Two original images are first regarded as the amplitude and phase of a complex function. Arnold transform is used to scramble pixels at a local area of the complex function. Then the changed complex function is converted by gyrator transform. The two operations mentioned will be implemented iteratively. Numerical simulation has been performed to test the validity and the security of the proposed encryption algorithm.

The rest of this paper is organized in the following sequence. In Section 2, the proposed double-image encryption algorithm is addressed. In Section 3, some numerical simulations are given to demonstrate the performance of the algorithm. Concluding remarks are summarized in the final section.

2. Double image encryption algorithm

Before introducing the double image encryption algorithm, we first recall the gyrator transform, Arnold transform and chaotic maps, which are used in the encryption scheme.

The gyrator transform (GT) belongs to a kind of the linear canonical integral transforms [45,46]. For a two-dimensional function $f(x,y)$, the mathematical definition of the transform is written as

$$F(u,v) = \mathcal{G}^{\alpha}[f(x,y)](u,v)$$

* Corresponding author. Tel.: +86 15824982317.
E-mail address: hjliding@gmail.com (H. Li).

0143-8166/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlaseng.2013.05.011

$$= \frac{1}{|\sin\ \alpha|}\iint f(x,y)\exp\left[\mathrm{i}2\pi\frac{(xy+uv)\cos\ \alpha-(xv+yu)}{\sin\ \alpha}\right]\mathrm{d}x\,\mathrm{d}y, \quad (1)$$

where α is called the rotation angle. The function $F(u,v)$ is the output of the transform. The symbol $\mathcal{G}^{\alpha}$ denotes the gyrator operator at angle α. The GT is additive and periodic with respect to α. The inverse GT corresponds to the GT at angle $-\alpha$. The transform can be implemented by an optical system composed of six thin cylinder lenses [46], and can be numerically implemented by using the fast Fourier transform algorithm [47]. This transform will be utilized in the implementation of the double image encryption scheme.

The classical Arnold transform (AT) is an area-preserving, invertible chaotic map [48] in the unit square described by

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \mathrm{mod}\left(\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}, 1\right), \quad (2)$$

where operator "mod" denotes the modulus after division, $(x,y)^{\mathrm{T}}$ and $(x',y')^{\mathrm{T}}$ are pixel positions before and after AT. In order to incorporate (2) into digital image encryption, one can discretize it as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \mathrm{mod}\left(\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}, M\right), \quad (3)$$

where M is the size of a square matrix, $x,\ y,\ x',\ y' \in \{0,1,\ldots,M-1\}$. Executing the transform in (3) some times, one will make a digital image sized $M \times M$ like white noise through pixel scrambling.

However, the transform in (3) has a property of limited period, which is vulnerable in the application of information security when it is employed directly in encryption algorithm. On the other hand, when the input image is not square, the transform in (3) cannot deal with whole image directly. To overcome these drawbacks, a local processing scheme is proposed. As shown in Fig. 1, given an $M \times N$ pixel image, for any $x \in \{0,1,\ldots,M-1\}$ and $y \in \{0,1,\ldots,N-1\}$, select the biggest square area with $(x,y)^{\mathrm{T}}$ as its vertex, and then scramble the selected area by AT for m times. As an example, for a 512×768 pixel image, if $x=121$ and $y=612$, then the selected area scrambled by AT is a 391×391 pixel square. We denote this local pixel scrambling (LPS) operation by $\mathcal{J}^{(x,y,m)}$ and its inverse operation by $\mathcal{K}^{(x,y,m)}$. Here the parameters x, y and m will be generated by the following two chaotic maps.

The first chaotic map is the standard map [49]. It is defined as

$$\begin{cases} u_{n+1} = \mathrm{mod}(u_n + \mu \sin v_n, 2\pi), \\ v_{n+1} = \mathrm{mod}(v_n + u_{n+1}, 2\pi), \end{cases} \quad (4)$$

where μ is the control parameter, $n=0, 1,2,\ldots$. All the values of $\{u_n, v_n\}$ appear in the range $[0, 2\pi)$ for the initial values u_0, $v_0 \in [0, 2\pi)$ and control parameter $\mu > 0$. The standard map will be utilized to generate the position parameters x and y by formulas:

$$x_k = \left\lfloor \frac{Mu_{p+k}}{2\pi} \right\rfloor, \quad y_k = \left\lfloor \frac{Nv_{p+k}}{2\pi} \right\rfloor, \quad (5)$$

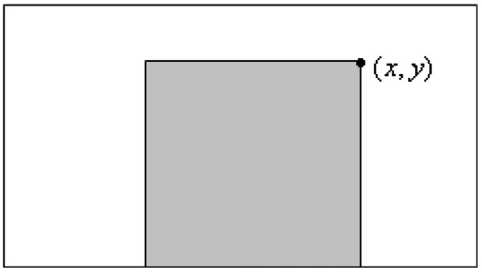

Fig. 1. Selected area scrambled by Arnold transform.

where $\lfloor z \rfloor$ denotes the greatest integer less than z, p is a positive integer, $k=1,2,\ldots$.

The second chaotic map is the logistic map [49]. It is defined as

$$w_{n+1} = \lambda w_n(1-w_n), \quad (6)$$

where λ is the control parameter, $n=0,1,2,\ldots$. All the values of $\{w_n\}$ appear in the range $[0, 1)$ for the initial value $w_0 \in [0, 1)$ and control parameter $\lambda \in (3.57, 4)$. The logistic map will be utilized to generate the Arnold transform frequency m by formula:

$$m_k = \lfloor b w_{q+k} \rfloor + a, \quad (7)$$

where q, a and b are positive integers, $k=1,2,\ldots$.

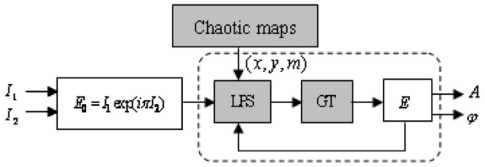

Fig. 2. The schematic of encryption.

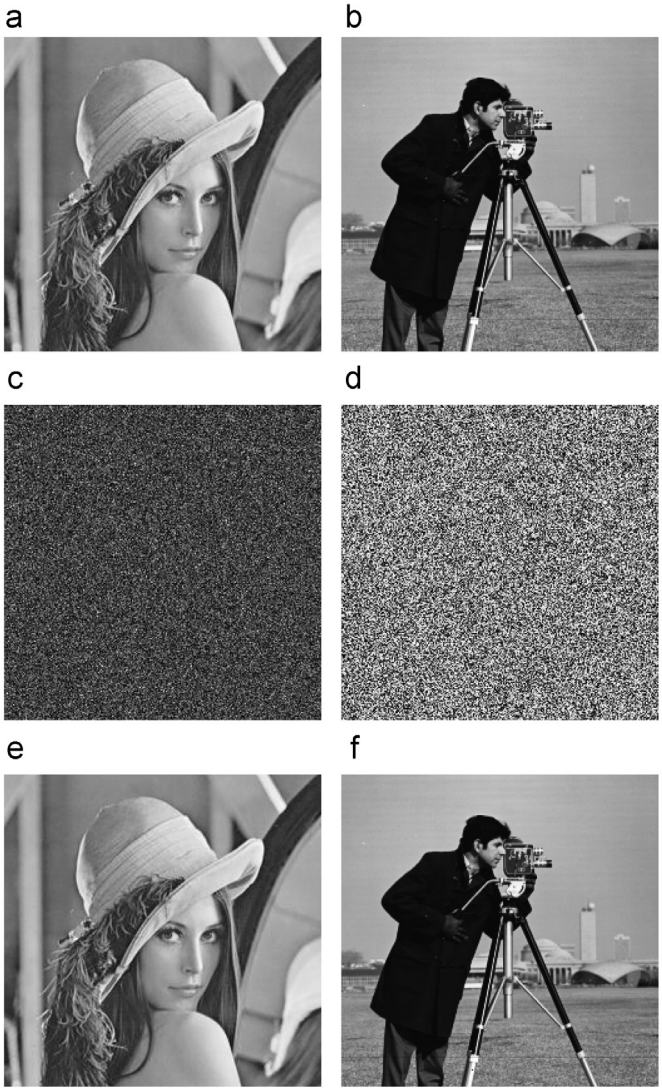

Fig. 3. The result of double image encryption: (a) and (b) original images; (c) the amplitude for the encrypted image; (d) the phase for the encrypted image; (e) and (f) correctly retrieved images.