Optics Communications 341 (2015) 263–270

Contents lists available at ScienceDirect

Optics Communications

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

Optical image encryption scheme using 3-D chaotic map based joint image scrambling and random encoding in gyrator domains

Jun-xin Chen [a], Zhi-liang Zhu [b,*], Chong Fu [a], Hai Yu [b]

[a] School of Information Science and Engineering, Northeastern University, China
[b] Software College, Northeastern University, China

ARTICLE INFO

Article history:
Received 2 November 2014
Received in revised form
1 December 2014
Accepted 13 December 2014
Available online 17 December 2014

Keywords:
Optical encryption
3-D chaotic map
Image scrambling
Random encoding

ABSTRACT

We demonstrate an optical image encryption scheme using 3-D chaotic map based joint image scrambling and random encoding in gyrator domains. A novel image confusion approach that can well address the drawbacks of typical image permutation ciphers is developed to firstly shuffle the plaintext. Then the scrambled image is random phase encoded in the spatial domain and gyrator transform domain. A three-dimensional chaotic map is introduced to generate key stream elements. Simulations demonstrate that the cryptosystem has satisfactory cryptographic features and owns high robustness against noise perturbation as well as occlusion attack.

1. Introduction

Owing to the superior advantages such as high speed, multi-dimensional characteristics and parallel processing, optical information encryption techniques have drawn long-term attention. In 1995, Refregier and Javidi firstly proposed the double random phase encoding (DRPE) architecture based on the 4*f* optical system to encrypt the primary image into stationary white noise [1]. This pioneering achievement has paved the way for numbers of optical security and encryption systems subsequently proposed [2–27]. In [2–5], researchers implemented DRPE in fractional Fourier transform (FrFT) domain, while a number of optical image cryptosystems have also been developed in gyrator transform (GT) domains [6–10], especially after Liu et al. addressed the numerical simulation problems of GT [11]. Some other techniques, such as phase retrieval [12–14], watermarking [15,16] and wavelet transform [17,18] are also employed to build secure image encryption schemes. Meanwhile, the integration of chaos-based image protection approaches with optical techniques has also drawn researchers' concerns. A variety of image scrambling strategies have been developed and employed into optical image encryption schemes [19–27]. Among these techniques, cat map, baker map and standard map are the most adopted permutation ciphers. However, there are several drawbacks in these typical permutation approaches. (1) Operation efficiency. Generally, 3–5 rounds permutation has to be performed in one encryption round so as to achieve a satisfactory image confusion effect. It brings about considerable complexity and efficiency pressure to the cryptosystem. (2) Periodicity. The discretized chaotic maps may become periodic under certain circumstances, which will downgrade the security of the cryptosystem. For example, an image of size 256 × 256 with any parameters in cat map will get back to itself after 192 rounds of permutation. (3) Image size restriction. Most of the traditional image permutation ciphers are originally designed for scrambling a square image. Generally, for shuffling a non-square plain image, extra pixels have to be padded to construct a square image firstly, and that would downgrade the efficiency of the cryptosystem. These drawbacks in such permutation ciphers and the flaws derived from the linearity of DPRE bring about sever threats to optical image encryption schemes. For example, the achievement in [28] demonstrates a chosen-plaintext attack that is suitable for general optical encryption model with the architecture of image scrambling then DRPE.

In this paper, we demonstrate an optical image encryption scheme using three-dimensional (3-D) chaotic map based joint image scrambling and random encoding in gyrator domains. A novel pixel swapping based image permutation (PSBIP) approach is developed so as to firstly shuffle the plain image in the spatial domain. In PSBIP, each pixel will be swapped with another one that is located after it, and the overall permutation procedure is controlled by a serial of key stream elements. Then the confused image will be encrypted into stationary white noise with the help

[*] Corresponding author.
E-mail address: zhuzhiliang.sc@gmail.com (Z.-l. Zhu).

http://dx.doi.org/10.1016/j.optcom.2014.12.045
0030-4018/© 2014 Elsevier B.V. All rights reserved.

of implementing DRPE in GT domain. In traditional DRPE based schemes, the two random phase masks are generated independently, and serve as the secret key. However, the secure storage and transmission of the masks themselves devote considerable workloads to the cryptosystem. In our scheme, the phase masks are generated from the chaotic Chen's system [29]. With the iteration of Chen's map, three serials of pseudorandom state variables are simultaneously produced, with the first one used to control the PSBIP whereas the other two serials are converted to random phase masks. All of the key stream elements are depending on the parameters of Chen's system, which serve as the main key. Amounts of simulations have been carried out, and the results well demonstrate the security performance of the proposed scheme.

The rest of this paper is organized as follows. In the next section, the proposed scheme will be described in detail. Results and security analyses are given out in Section 3, while conclusions will be drawn in the last section.

2. The proposed image encryption scheme

Prior to the description of the proposed scheme, we firstly have to give out some preparative theories.

2.1. Chaotic Chen's system

The Chen's system is a well-known chaotic map, whose mathematic formula is given in Eq. (1).

$$\begin{cases} \dfrac{dx}{dt} = a(y - x) \\ \dfrac{dy}{dt} = (c - a)x - xz + cy. \\ \dfrac{dz}{dt} = xy - bz \end{cases} \tag{1}$$

In this equation, a, b, and c are control parameters, when $a=35$, $b=3$, $c\in[20,28.4]$ the system is chaotic. The initial system states x_0, y_0, z_0 and the control parameter c can be combined as the secret key. The attractors of Chen's system are shown in Fig. 1 with control parameters $a=35$, $b=3$, $c=28$ and the initial values $x_0=3.3$, $y_0=-2.1$, $z_0=6.8$.

With each iteration of Chen's map, three chaotic state variables x, y and z will be generated simultaneously. Suppose that the plain image is with size $M\times N$, the Chen's map will be iterated $M\times N$ times, and hence a series of x, y and z are generated. Without loss of generality, we denote $x=\{x(1), x(2), \dots, x(M\times N)\}$, $y=\{y(1), y(2), \dots, y(M\times N)\}$ and $z=\{z(1), z(2), \dots, z(M\times N)\}$ for the series of x, y and z, respectively. All the series will be quantized to the required key stream elements and further be used in the encryption/decryption process of the cryptosystem.

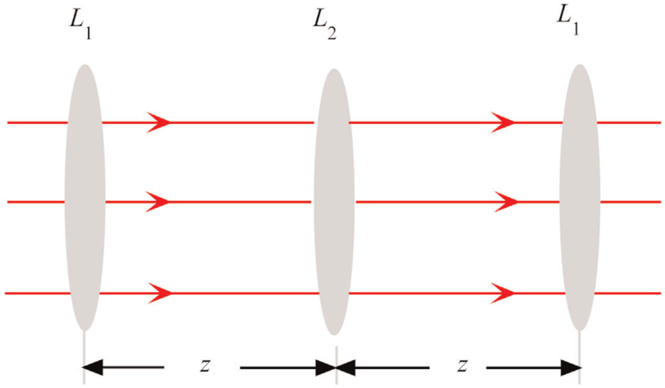

Fig. 2. Optical implementation of GT.

Table 1
Results of the PSBIP and traditional permutation techniques.

Permutation approach	Rounds	Pixel correlation			Time (ms)
		Horizontal	Vertical	Diagonal	
Plain-image		0.9703	0.9425	0.9188	–
PSBIP	1	0.0129	−0.0194	−0.0163	13.9
Cat map	3	−0.0273	−0.0626	−0.0106	14.2
Baker map	3	0.0062	0.1687	0.0438	138.6
Standard map	3	0.0477	0.1187	0.0482	187.1

2.2. Gyrator transform

The GT is mathematically defined as a linear canonical transform which produces the rotation in position-spatial frequency planes [30,31]. The GT at parameter α, which will be called below as a rotation angle, of a two dimensional function $f(x, y)$ is calculated as

$$\begin{aligned} F(u, v) &= \mathcal{G}^{\alpha}[f(x, y)](u, v) \\ &= \frac{1}{|\sin\alpha|}\iint f(x, y)\exp\left[i2\pi\frac{(xy + uv)\cos\alpha - (xv + yu)}{\sin\alpha}\right] \\ &\quad dx\, dy \end{aligned} \tag{2}$$

The GT has some properties similar to FrFT, and is additive and periodic with respect to the angle α. The transform can be

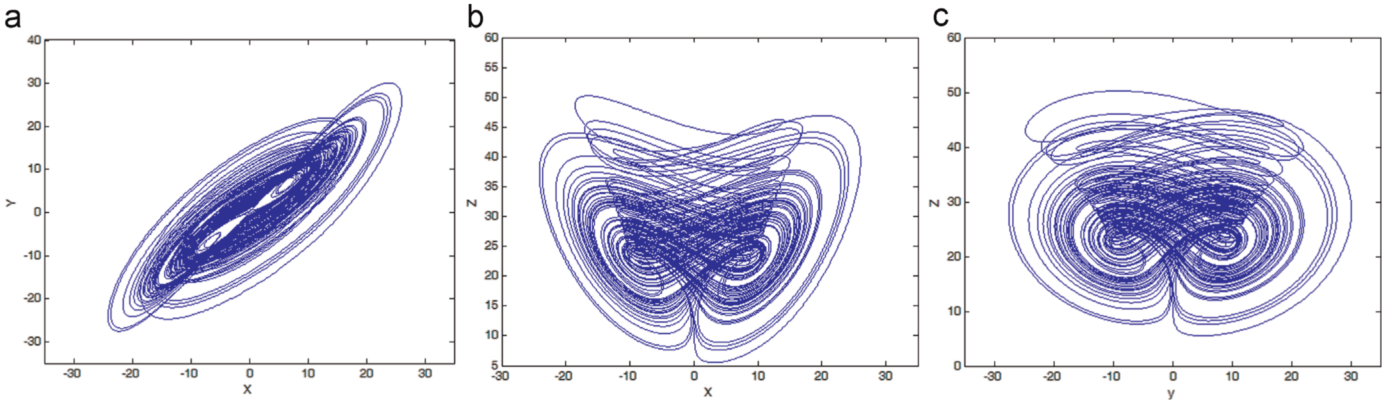

Fig. 1. Attractors of Chen's system. (a) x–y plane; (b) x–z plane; and (c) y–z plane.