Optics and Lasers in Engineering 66 (2015) 1–9

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Analysis and improvement of a double-image encryption scheme using pixel scrambling technique in gyrator domains

Jun-xin Chen[a], Zhi-liang Zhu[b,1], Chong Fu[a], Li-bo Zhang[b], Hai Yu[b]

[a] School of Information Science and Engineering, Northeastern University, Shenyang 110004, China
[b] Software College, Northeastern University, Shenyang 110004, China

ARTICLE INFO

Article history:
Received 28 December 2013
Received in revised form
26 July 2014
Accepted 11 August 2014
Available online 15 September 2014

Keywords:
Double-image encryption
Cross-talk disturbance
Lightweight pixel confusion
Gyrator transform

ABSTRACT

Recently, a double-image encryption scheme using local pixel scrambling technique and gyrator transform has been proposed [Opt Lasers Eng 2013; 51: 1327–31]. Through our simulations, there is serious cross-talk disturbance in the phase-based image when the encrypted data undergoes noise perturbation or occlusion attack. The disturbance will cause serious deterioration in the retrieved phase-based image and bring about visibility ambiguities to the receiver, and hence downgrades the practicability of the cryptosystem. In this paper, detailed analysis of the cross-talk disturbance in the original scheme will be firstly given out, and then the corresponding improvement is subsequently proposed. Numerical simulations results indicate that the improved scheme well address the cross-talk disturbance and further enhance the security of the original cryptosystem.

1. Introduction

With the dramatic development of modern communication technologies, the security of information has become an important issue when it is transmitted or stored over open channels. Optical systems are of growing attraction in image encryption area for their high speed and parallel processing advantages. Since Refregier and Javidi proposed the double random phase encoding (DRPE) [1], optical image encryption schemes have been extensively researched during the past decades [2–32]. In [2], Unnikrishnan and Singh implemented DRPE in fractional Fourier transform (FRFT) domain [2], and then FRFT has shown its advantages in the optical security field and a variety of image encryption algorithms are subsequently proposed [3–10]. In recent years, researchers also developed optical image encryption schemes in gyrator transform (GT) domains [11–17,32], especially after Liu et al. addressed the numerical simulation difficulties of GT [18]. Researchers rewrote the GT using convolution operations in [18], and hence the GT can be simulated by using phase-only filtering, Fourier transform and inverse Fourier transform. Some other techniques, such as Hartley transform [19–22], digital holography [23–25], watermarking [26,27], discrete fractional cosine transform [28] and image sharing [29–31] mechanisms are also employed to build secure image encryption schemes.

Recently, Li et al. proposed a novel double-image encryption scheme using chaos-based local pixel scrambling (LPS) technique in GT domains [32]. The two plain images are regarded as the amplitude and phase of a complex function, then pixel scrambling operation are performed using LPS, and the shuffled complex function is transformed by GT at last. The two operations above-mentioned can be implemented iteratively to satisfy the security requirements. Numerical simulations and security analyzes have proved that the scheme has a high level of security and large key space. However, we found that there will be serious cross-talk disturbance in the recovered phase-based image when the cipher data undergoes noise perturbation or occlusion attack. In these scenarios, the outline of the amplitude-based image will cross into the decrypted phase-based image. The more severe the attacks are, the more cross-talk disturbance generated. The crossed information will cause serious deterioration in the recovered phase-based image and bring about visibility ambiguities to the receiver. The practicability of the cryptosystem is consequently downgraded. In this paper, we will present the cross-talk weakness of the original scheme at first, and then an improvement is suggested by adding a pre-processing pixel confusion layer to the amplitude-based image. The purpose of introducing such an operation is to shuffle the amplitude-based image before it enters into the original cryptosystem. Therefore, the cross-talk disturbance will be the shuffled version of the original amplitude-based image, which is completely unrecognizable and hence bring about less influence to the decrypted phase-based image. The quality of the decrypted phase-based image is thus improved. Besides, as a

E-mail address: zhuzhiliang.sc@gmail.com (Z.-l. Zhu).
[1] Tel.: +86 24 86581232.

http://dx.doi.org/10.1016/j.optlaseng.2014.08.010
0143-8166/© 2014 Elsevier Ltd. All rights reserved.

type of image permutation approach, the pre-processing pixel confusion operation can provide additional protection to the amplitude-based image, and hence strengthen the security of the whole cryptosystem. Numerical simulations results prove the security enhancements.

The remaining of this paper is organized as follows. In the next section, a review of the double-image encryption scheme in [32] is firstly given out. Then the cross-talk disturbance analysis and the improvement of the scheme will be reported in Section 3. Numerical simulations and discussions are addressed in Section 4. Finally, conclusions will be drawn in the last section.

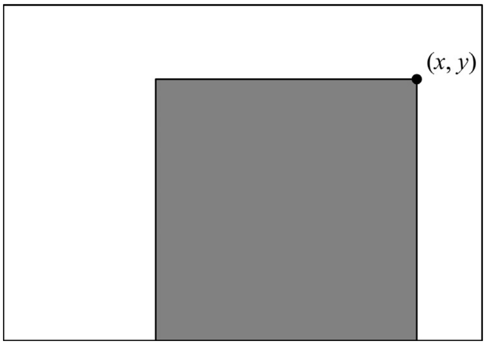

Fig. 1. The selected scrambled area of LPS.

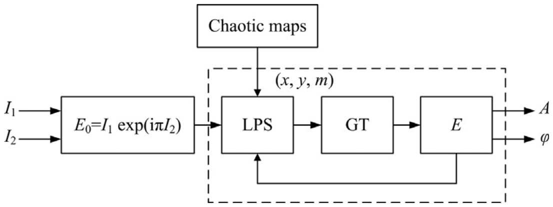

Fig. 2. The schematic of the original cryptosystem.

2. Review of the double-image encryption scheme

Prior to the double-image encryption algorithm in [32], we firstly recall GT and LPS, which are applied in that scheme.

2.1. Gyrator transform

The GT is mathematically defined as a linear canonical transform which produces the rotation in position-spatial frequency planes [33,34]. 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

$$F(u,v)=\mathcal{G}^{\alpha}[f(x,y)](u,v)=\frac{1}{|\sin\ \alpha|}\iint f(x,y)\exp\left[i2\pi\frac{(xy+uv)\cos\ \alpha-(xv+yu)}{\sin\ \alpha}\right]dxdy. \tag{1}$$

The GT has some properties similar to FRFT, and is additive and periodic with respect to the angle α. The transform can be achieved by using an optimized flexible optical system which contains only three generalized lenses with fixed distance between them, and the angle α is changed by rotation of the cylindrical lenses which form the generalized lenses [34]. The GT can also be computer simulated using phase-only filtering, Fourier transform and inverse Fourier transform [18]. The inverse GT corresponds to the GT at angle $-\alpha$.

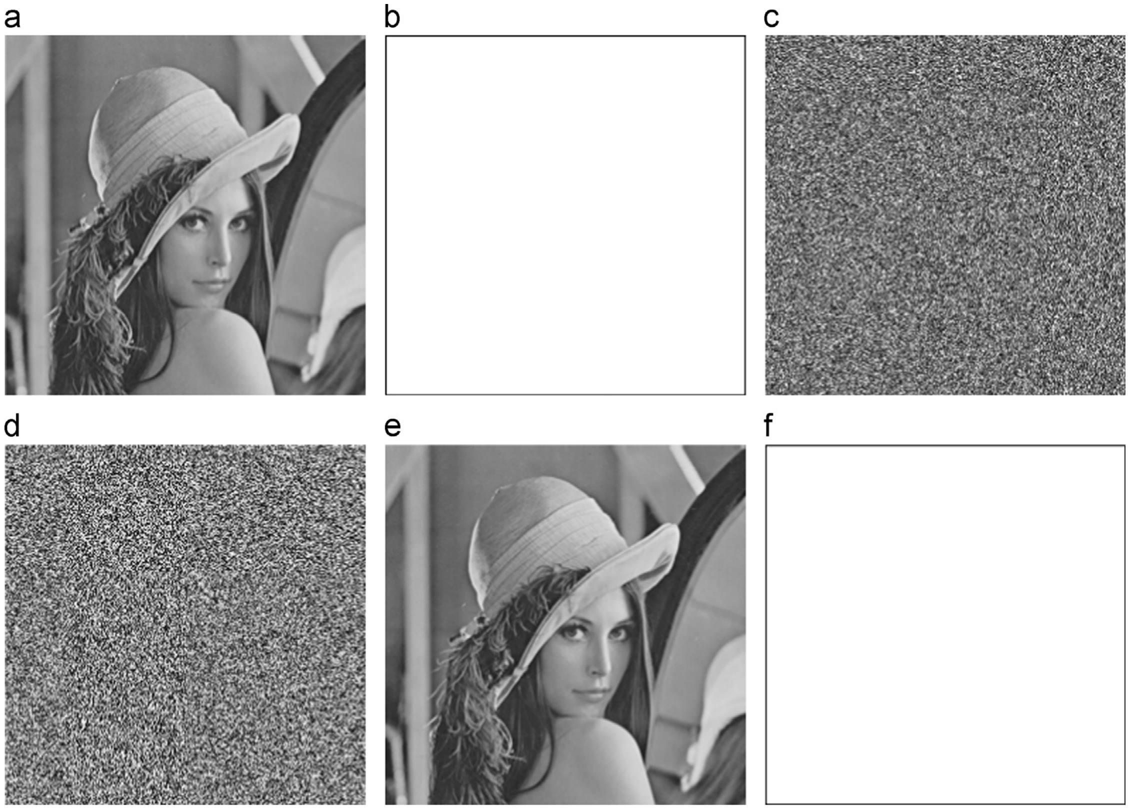

Fig. 3. The simulation results of the original encryption scheme. (a) Lena image regarded as I_1; (b) white image as I_2; (c) amplitude of the encrypted image; (d) phase of the encrypted image; (e) decrypted image of Lena; and (f) decrypted image of the white image.