Optics & Laser Technology 47 (2013) 152–158

Contents lists available at SciVerse ScienceDirect

Optics & Laser Technology

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

Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains

Zhengjun Liu [a,b,*], Yu Zhang [a], She Li [c], Wei Liu [c], Wanyu Liu [a], Yanhua Wang [d], Shutian Liu [c]

[a] HIT-INSA Sino French Research Center for Biomedical Imaging, Department of Automatic Measurement and Control, Harbin Institute of Technology, Harbin 150001, China
[b] State Key Laboratory of Transient Optics and Photonics, Chinese Academy of Sciences, Xi'an 710119, China
[c] Department of Physics, Harbin Institute of Technology, Harbin 150001, China
[d] Kunshan Branch, Institute of Microelectronics of Chinese Academy of Science, Kunshan 215347, China

ARTICLE INFO

Article history:
Received 22 July 2012
Received in revised form
4 September 2012
Accepted 6 September 2012
Available online 12 October 2012

Keywords:
Image hiding
Cryptography
Scrambling

ABSTRACT

We present a double image encryption scheme by using random pixel exchanging and phase encoding in gyrator domains. Two original images are regarded as the amplitude and phase of a function in the encryption algorithm. The pixels of the two images are exchanged randomly by controlling of a matrix. The same random matrix is used in the process of pixel exchanging and phase encoding for saving space in the application of transmission and storage of key. Some numerical simulation results are made for demonstrating the performance and security of the double image encryption.

1. Introduction

Optical information security technology has been researched and developed for protecting the secret data during storage and transmission in practical application. Double random phase encoding is a classical method of optical encryption [1]. The phase encoding has been developed and employed in some encryption schemes [2–6]. The encoding method has also been applied for information authentication [7], multiple-encryption [8] and color encryption [9]. As an expanded version, random intensity encoding has been designed for image encryption [10,11]. Several transforms being regarding as a tool converting pixel value have been utilized in image hiding scheme, such as fractional Mellin transform [12], fractional Hadamard transform [13], multiple-parameter fractional Fourier transform [14], Fourier transform [1,15] and discrete cosine transform [16,17]. The optical stream cipher composed of cellular automata has been reported by Zhang and Karim [18]. In recent years, the security of encryption algorithm [1] has been considered and analyzed at various aspects. Chosen-plaintext attack [19] and known-plaintext attack [20] have been introduced for testing the security of the random phase encoding [1], which is vulnerable because of the linearity of encryption process. Moreover, the key space of random phase encoding [1] has been analyzed numerically [21,22]. Recently Alfalou and Brosseau have reported a complete discussion and comparison on optical encryption methods [23].

Multiple-image encryption is a new information security technology. Since Situ and Zhang have proposed a wavelength multiplexing scheme to hide many secret images [24], several multiple-encryption algorithms [25–32] have been reported by use of different optical structure. Compare to conventional image encryption, which can be called as single image hiding, multiple-encryption have an obvious advantage at the aspect of data space in the application of storage and transmission of the encrypted data and key. Regarding as a special case of multiple-encryption, double image encryption has been developed by using amplitude and phase (or the real part and imaginary part of complex function) to represent two images during the performance of the algorithms [33–40] based on gyrator transform, fractional transform and a kind of asymmetric algorithm. Moreover, the color image encryption algorithms [41,42] can be regarded as triple-image encryption [39].

In this paper, a random pixel exchanging operation regarding a scrambling method [28,43], is defined for scrambling pixel sequence of image in encryption scheme. Two secret images serve as the real part and imaginary part of complex function and are imported into encryption system. At the same time, the pixels of the two images are exchanged with self (or each other) randomly under the control of a random matrix, which is also employed for generating random phase data in random phase encoding. The scrambled data is converted into gyrator domain.

* Corresponding author at: Harbin Institute of Technology, Department of Automatic Measurement and Control, HIT-INSA Sino French Research Center for Biomedical Imaging, Harbin 150001, China
E-mail addresses: zjliu@hit.edu.cn, zjliuv@gmail.com (Z. Liu).

0030-3992/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlastec.2012.09.007

The real part and imaginary part of gyrator spectrum are scrambled by exchanging pixel again. Subsequently the scrambled gyrator spectrum is encoded with random phase and is changed by gyrator transform, after which the encrypted data is received finally. The random matrix mentioned above is the main key of the algorithm. Compare to conventional encryption methods [1–4], the random matrix is used for generating random phase and controlling random, which will enhance the security of the algorithm. The fractional order of gyrator transform is an additional key. Some numerical simulations have been performed to test the validity of the proposed method.

The rest of this article is organized as follows. In Section 2, the random pixel exchanging operation is defined and illustrated. In Section 3, the double image encryption scheme is shown and explained. In Section 4, numerical simulation has been achieved to check the performance of the encryption algorithm. In Section 5 the conclusion remark is given briefly.

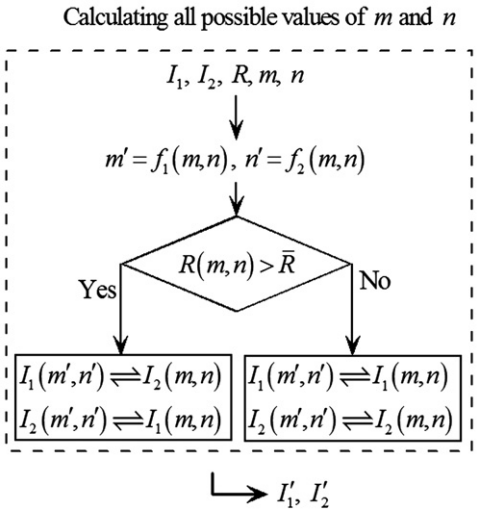

Fig. 1. The random pixel exchanging.

Table 1
A pair of scrambling sequence.

Direction:$I_1,I_2 \rightarrow I'_1,I'_2$	Direction:$I'_1,I'_2 \rightarrow I_1,I_2$
for $m=1:M$ for $n=1:N$ % scrambling end End	for $m=M:-1:1$ for $n=N:-1:1$ % scrambling end End

2. Random pixel exchanging

An illustration of random pixel exchanging process is shown in Fig. 1. The functions I_1 and I_2 represent two images. The variables m and n are the index of the images. The function R is a random matrix, in which all elements are limited in the interval [0,1]. According to certain sequence, all possible values of m and n are utilized for exchanging pixel value. A new position (m',n') is computed as follows

$$m' = f_1(m,n) = 1 + \text{round}\{(M-1) \times \sin[\pi \times R(m,n)]\},$$
$$n' = f_2(m,n) = 1 + \text{round}[(N-1) \times R(m,n)],$$
$$1 \le m \le M, 1 \le n \le N \quad (1)$$

where M and N are the size of the matrix R. The images I_1 and I_2 have $M \times N$ pixels. The function 'round' is to toward nearest integer for input number. The mean value $\overline{R}$ of random matrix R is defined as

$$\overline{R} = \frac{1}{M \times N} \sum_{\forall m,n} R(m,n). \quad (2)$$

When $R(m,n) > \overline{R}$, the pixels at the positions, (m,n) and (m',n'), are exchanged each other for the two images I_1 and I_2. The symbol '$\rightleftharpoons$' in Fig. 1 is to interchange the pixels at the left side and right side. When $R(m,n) \le \overline{R}$, the pixel exchanging is made in the inner pixels of every image as shown in Fig. 1. After all pixel positions are scrambling step by step, two random patterns, I'_1 and I'_2, are received and are regarded as the output of the operation.

The inverse process of the pixel exchanging operation is implemented according to Fig. 1 with an opposite scrambling sequence. A pair of scrambling sequences is given in Table 1, in which the codes of left side and right side are related with pixel exchanging and its reverse operation, respectively. An example of pixel exchanging is shown in Fig. 2. Two input images in Fig. 2(a) and (b) have 256×256 pixels. The two random patterns can be generated (see Fig. 2(c) and (d)). By using the correct value of random matrix R, the two retrieved images are shown in Fig. 2(e) and (f). The pixel exchanging method will be employed in the proposed double image encryption algorithm to enhance security.

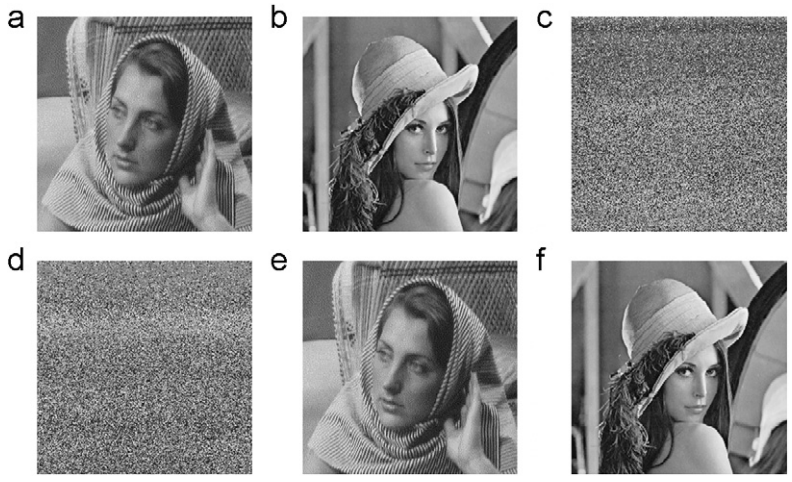

Fig. 2. The result of random pixel exchanging: (a) I_1, (b) I_2, (c) I'_1, (d) I'_2, (e) and (f) are the recovered images.