Optics and Lasers in Engineering 50 (2012) 1352–1358

Contents lists available at SciVerse ScienceDirect

Optics and Lasers in Engineering

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

Image encryption based on the random rotation operation in the fractional Fourier transform domains

Zhengjun Liu [a,b,*], She Li [c], Meng Yang [a], Wanyu Liu [a], Shutian Liu [d]

[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] School of Science, Heilongjiang Institute of Science and Technology, Harbin 150027, China
[d] Department of Physics, Harbin Institute of Technology, Harbin 150001, China

ARTICLE INFO

Article history:
Received 8 April 2012
Received in revised form
29 May 2012
Accepted 29 May 2012
Available online 19 June 2012

Keywords:
Random rotation operation
Pixel scrambling
Amplitude encoding
Phase encoding

ABSTRACT

A kind of image encryption scheme is presented by using a rotation operation being regarded as the scrambling scheme of the pixels. The rotation operation is composed of rotation center, radii and angle. For the data of phase and amplitude of complex number, the rotation operation is performed with random controlling parameters iteratively. The parameters are random and serve as the key of this encryption method. Subsequently, the fractional Fourier transform is introduced to alter the values of image pixel. The process mentioned above will be achieved many times for enhancing the security of the proposed algorithm. Numerical simulation is given to demonstrate the validity and performance of the image hiding procedure.

1. Introduction

The information security technique is to protect secret data for private benefit or organizational benefit in the application of transmission and storage of message. Some algorithms have been reported based on optical system and mathematical transforms, such as random phase encoding [1] and discrete fractional random transform [2–4]. Lang has proposed an image encryption scheme based on multiple parameter fractional Fourier transform and chaotic mapping [5,6]. Three encryption algorithms [7–9] have been represented by using interference and digital holography. Gyrator transform and radial Hilbert transform have been introduced for encrypting secret image [10,11]. As a special example of non-uniform illumination, an image encoding method with optical beam has been presented [12]. As an expanded version of random phase encoding, affine transform has been considered to encrypt two images [13]. The rotation of color vector [14] can be considered as a kind of random phase encoding in three-dimensional space. In the most of algorithms mentioned above, the value of the image is changed by random phase function for hiding the secret information.

Other encryption methods have been designed by using pixel scrambling operation to obtain a random pattern. The jigsaw transform is a random shift, in which many divided sub-images with same shape (square or rectangle) are moved randomly in the horizontal direction and vertical direction. The jigsaw transform has been utilized for encrypting secret image [15,16]. For jigsaw transform, the pixel sequence is not changed in every sub-image. Arnold transform [17], which is also called as cat mapping, is another scrambling transform. The Arnold transform has been employed for hiding one image or two images [18–22]. However, the Arnold transform has a property of limited period, which is vulnerable in the application of information security when this transform is employed directly in encryption algorithm.

In this paper, a pixel scrambling operation is introduced for hiding the secret image. In the original secret image, a circled area is selected and rotated at an angle θ. The rotation operation is reverse by taking $-\theta$ or $2\pi-\theta$. The operation will be controlled by rotating center, radii and angle θ. The parameters can be regarded as the key in the proposed encryption algorithm. To obtain a random pattern, the rotation operation is performed many times in practical application. The fractional Fourier transform is employed for changing the value of complex function after the rotation processing. For designing more random data serving as a key in this encryption approach, the procedures mentioned above will be implemented iteratively. Some numerical simulations have been shown for validating the performance of this encryption scheme.

* Corresponding author at: HIT-INSA Sino French Research Center for Biomedical Imaging, Department of Automatic Measurement and Control, Harbin Institute of Technology, Harbin 150001, China. Fax: +86 45186415146.
E-mail addresses: zjliu@hit.edu.cn, zjliuv@gmail.com (Z. Liu).

0143-8166/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlaseng.2012.05.021

The rest of this article is organized as follows. In Section 2, the rotation operation is defined and analyzed. The encryption algorithm is also presented. In Section 3, numerical simulation is provided to test the validity of the image encryption method. In Section 4, the conclusion is given briefly.

2. Rotation operation and image encryption scheme

Before introducing the proposed image encryption algorithm, the rotation operation is expressed in detail. The fractional Fourier transform is also presented in brief for constructing the hiding method of the secret information.

2.1. Rotation operation

A rotation example is shown in Fig. 1. In Fig. 1(b), the data in the white circle is rotated with $\theta=\pi/2$ at clockwise direction. If $\theta<0$, the rotation is achieved along the anti-clockwise direction. When a reverse operation is performed for the image in Fig. 1(b), the recovered image is shown in Fig. 1(c), which is the same result of the original image. The mathematical definition of rotation is written as following steps:

(1) The rotation center is represented by the point (x_0,y_0). A point (x,y) is in the area of the image. The values of the variables (x_0,y_0) and (x,y) are positive integers, because they are the index of pixel position. The distance d from the point (x,y) to the point (x_0,y_0) is expressed as

$$d=\sqrt{(x-x_0)^2+(y-y_0)^2}. \tag{1}$$

(2) The new position (x',y'), which is rotated with an angle θ ($\theta=\pi/2$, π, $3\pi/2$), are calculated as

$$\begin{cases} x'=x_0+\mathrm{real}[C\exp(-\mathrm{i}\theta)], \\ y'=y_0+\mathrm{imag}[C\exp(-\mathrm{i}\theta)], \end{cases} \quad C=(x-x_0)+\mathrm{i}(y-y_0), \tag{2}$$

where the symbol 'i' is the imaginary unit. The functions 'real' and 'imag' are to calculate the real part and imaginary part of a complex number, respectively. Thus the value of (x',y') is an integer to denote a new index in the rotation. When $\theta=0$, 2π, the rotation does not change the input image. If $\theta\neq 0$, $\pi/2$, π, $3\pi/2$, 2π, the rotation defined in Eq. (2) is not reverse because the pixel points are limited in the crosspoints of the grid.

(3) Suppose $I_0(x,y)$ be the image before the rotation, the rotated image $I_0'(x,y)$ is computed as follows:

$$I_0'(x,y)=\begin{cases} I_0(x,y) & \text{if } d\geq r, \\ I_0(x',y') & \text{if } d<r, \end{cases} \tag{3}$$

where the variable 'r' is the radius of the circle.

The rotation operations mentioned above can be illustrated with a function expression $I_0'=\mathcal{R}(I_0;x_0,y_0,r,\theta)$. The symbol '$\mathcal{R}$' is the rotating operator. The corresponding reverse operation is

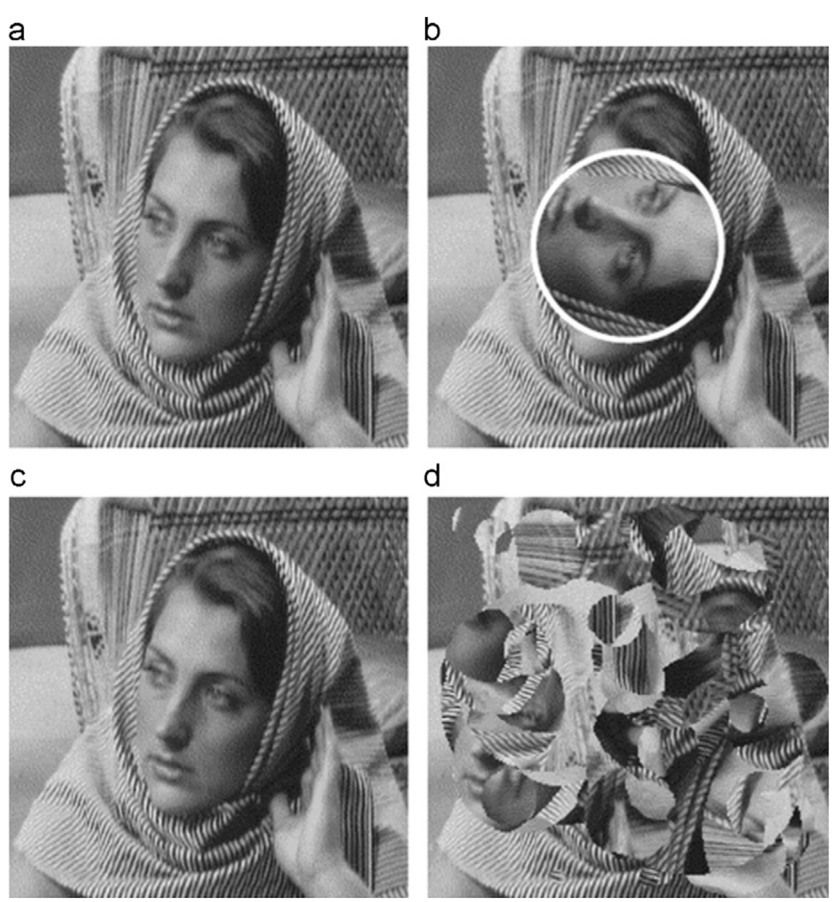

Fig. 1. An example of the rotation operation: (a) original image, (b) the image rotated with $\theta=\pi/2$, (c) the recovered image and (d) the image rotated with 40 operations.