Optics and Lasers in Engineering 66 (2015) 285–293

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Opto-digital spectrum encryption by using Baker mapping and gyrator transform

Hang Chen [a,c,*], Jiguang Zhao [b], Zhengjun Liu [c], Xiaoping Du [a]

[a] Department of Space Equipment, The Academy of Equipment, Beijing 101416, China
[b] Department of Scientific Research, The Academy of Equipment, Beijing 101416, China
[c] Department of Automation Measurement and Control, Harbin Institute of Technology, Harbin 150001, China

ARTICLE INFO

Article history:
Received 9 April 2014
Received in revised form
1 October 2014
Accepted 1 October 2014
Available online 24 October 2014

Keywords:
Hyperspectral
Encryption
Cryptography
Optical transform

ABSTRACT

A concept of spectrum information hidden technology is proposed in this paper. We present an optical encryption algorithm for hiding both the spatial and spectrum information by using the Baker mapping in gyrator transform domains. The Baker mapping is introduced for scrambling the every single band of the hyperspectral image before adding the random phase functions. Subsequently, three thin cylinder lenses are controlled by PC for implementing the gyrator transform. The amplitude and phase information in the output plane can be regarded as the encrypted information and main key. Some numerical simulations are made to test the validity and capability of the proposed encryption algorithm.

1. Introduction

The optical information security technology has been deeply researched since Refregier and Javidi proposed double random phase encoding (DRPE) [1–6]. For instance, the DRPE has been developed in the domains of Fresnel transform [2] and fractional Fourier transform [7]. In recent years, many of the proposed optical encryption systems are based on some optical transformation, such as Fourier transform, fractional Fourier transform, gyrator transform (GT), interference and so on [8–13]. Besides, the security of these methods has been demonstrated that is reliable to chosen-plaintext attack and known-plaintext attack. A secret image can be hidden by an encryption algorithm composed of random reversible process. In many encryption schemes, the random phase mask is introduced as the main way to enhance the security. In addition, the storage space of random phase mask is close to the original data [14].

Several kinds of pixel scrambling operations have been introduced in information hidden technology, such as Arnold transform, jigsaw transform and Baker mapping [15–18]. In these pixel scrambling operations [15–21], some parameters generated and used in the transforming process will be regarded as the additional keys to enhancing the security of the encryption algorithms. Some latest color image encryption schemes in gyrator transform domain have been proposed [21–25], the gyrator transform are well used in these schemes and the security, validity and capability of the algorithms are improved.

The hyperspectral image contains rich information both in spatial and spectral domains. The researchers are able to extract plentiful spectral information from hyperspectral image, which makes it possible to identify and discriminate the targets compared with other remotely data, such as multispectral image and ordinary RGB color image [26]. In this paper, an opto-digital spectrum encryption by using Baker mapping and gyrator transform is proposed to encrypt the information both in the spectral and spatial domain. The original hyperspectral image is separated into ever single band before encryption operation. First, the Baker mapping is considered for changing the pixels sequence in each band of the hyperspectral image. Note that the Baker mapping operation only employed in amplitude domain in the input plane of the optical transform system. Subsequently, the randomized data generated by the Baker mapping operation are encoded and converted by gyrator transform twice continuously. To enhance the security of the encryption scheme, an affine transform are introduced and utilized before applying the gyrator transform. Some corresponding numerical simulations are achieved to demonstrate the validity and efficiency of the encryption method.

The rest of the paper is organized in the following sequence. In Section 2, the proposed encryption/decryption algorithm is introduced

* Corresponding author at: Department of Space Equipment, The Academy of Equipment, Beijing 101416, China.
E-mail address: hitchenhang@foxmail.com (H. Chen).

http://dx.doi.org/10.1016/j.optlaseng.2014.10.002
0143-8166/

in detail. In Section 3, numerical simulation results are made and given to demonstrate the validity of the algorithm. Concluding remarks are summarized in the final section.

2. Spectrum encryption algorithm

Both the Baker mapping and gyrator transform are introduced before presenting the encryption in this section. Thereafter, the complete encryption scheme based on the gyrator transform is addressed in detail.

2.1. Baker mapping

Baker mapping is a kind of two-dimensional chaotic process [27], which can scramble the pixel position of the hyperspectral image. The Baker mapping operation is defined as

$$\begin{cases} r' = \frac{N}{n_j}(r-N_j) + \mathrm{mod}\left(s, \frac{N}{n_j}\right), \\ s' = \frac{n_j}{N}\left(s - \mathrm{mod}\left(s, \frac{N}{n_j}\right)\right) + N_j, \quad 0 \le r, s < N. \end{cases} \tag{1}$$

where the vectors (r,s) and (r',s') represents the index of image matrix before and after employing the mapping operation, respectively. The integer n_j is the input parameter of Baker mapping and N/n_j is also an integer. Besides, the parameter n_j should satisfy the equation $n_1+n_2+...n_j+...+n_{J-1}+n_J=N$, $j=1,2,...,J$. Moreover, the parameter N denotes the size of the square image, which obeys the relationship as $N_j = n_1+n_2+\cdots+n_j$, which is an accumulated value of the first j elements of all the parameters n_j in the mapping, $N_0=0$.

When employing the Baker mapping, the pixel of every single band image is moved and the pixel value is multiplied by a factor, which can be expressed as [18]

$$I(r',s') = \begin{cases} I(r,s)/t, & \text{if } \phi(r,s) \ge 0, \\ I(r,s) \times t, & \text{otherwise}. \end{cases} \tag{2}$$

where ϕ is the phase function and limited in the interval $[-\pi,\pi)$. The calculated image $I(r',s')$ is randomized in both position and pixel value after the operation expressed as Eq. (2). The inverse process of Baker mapping with pixel value modulation is defined as

$$I(r,s) = \begin{cases} I(r',s') \times t, & \text{if } \phi(r,s) \ge 0, \\ I(r',s')/t, & \text{otherwise}. \end{cases} \tag{3}$$

It is worth noting that (r',s') is calculated by Eq. (1) and the coefficient t in Eq. (2) and Eq. (3) is defined 0.5 in this paper.

2.2. Affine transform

Referring to [21], an affine transform [22] is introduced to enhance the security of the encryption scheme and defined as

$$F(\theta) = \begin{bmatrix} \varphi(\beta1,\beta2)\cos\,\theta & -\varphi(\beta1,\beta2)\sin\,\theta \\ \frac{\sin\,\theta}{\varphi(\beta1,\beta2)} & \frac{\cos\,\theta}{\varphi(\beta1,\beta2)} \end{bmatrix}, \tag{4}$$

where the function $\varphi(\beta1,\beta2)$ satisfying uniform distribution in real number domain. The form of $\varphi(\beta1,\beta2)$ can be defined by many nonlinear types to increase the complexity of the algorithm in practical application. Besides, the function θ is random angle depending on the coordinates pixels x and y. Here, the inverse matrix of $F(\theta)$ is

$$F^{-1}(\theta) = \begin{bmatrix} \frac{\cos\,\theta}{\varphi(\beta1,\beta2)} & \varphi(\beta1,\beta2)\sin\,\theta \\ -\frac{\sin\,\theta}{\varphi(\beta1,\beta2)} & \varphi(\beta1,\beta2)\cos\,\theta \end{bmatrix}. \tag{5}$$

Both the affine transform in Eqs.(4) and (5) will be employed in the proposed algorithm. It is worth noticing that the random angle function $\theta(x,y)$ is regarded as one of the key due to its large scale and strong randomness. In fact, some other affine transform can be introduced for replacing the function $F(\theta)$ [28].

2.3. Gyrator transform

The gyrator transform is a kind of linear canonical transform [29–30] and only has a two-dimensional format [31–32]. For the two-dimensional image$g(x,y)$, the definition of the gyrator transform can be expressed as

$$\begin{aligned} G(u,v) &= \xi^{\alpha}[g(x,y)](u,v) \\ &= \frac{1}{|\sin\,\alpha|}\iint g(x,y)\exp\left[i2\pi\frac{(xy+uv)\cos\,\alpha - xv - yu}{\sin\,\alpha}\right]\mathrm{d}x\mathrm{d}y, \end{aligned} \tag{6}$$

where $G(u,v)$ is the output function of the gyrator transform. The rotation angle α set in the gyrator transform is regarded as the additional key in many encryption algorithms. When $\alpha \in [0,2\pi]$, this transform can be implemented by an optical system composed with six thin cylinder lenses [32]. When $\alpha=\pi/2$, the expression of the transform becomes a Fourier transform with the rotation of the coordinates (u,v) [30,32]. The inverse transform of $\xi^{\alpha}$is$\xi^{-\alpha}$ or $\xi^{2\pi-\alpha}$. The gyrator transform will be adopted in the proposed encryption algorithm.

2.4. Encryption scheme

The flowchart of the encryption scheme is illustrated in Fig. 1. To design this encryption scheme, both the Baker mapping and gyrator transform are considered and utilized. Every single band of the original hyperspectral image is separated to be hidden. First, the divided hyperspectral image is scrambled by employing the Baker mapping with different parameter n_j as depicted in Fig. 1.

Subsequently, the chaotic data and a random function are combined to be calculated by using the affine transform as displayed in the flowchart. Here the process of the affine transform mentioned above can be expressed as

$$\begin{bmatrix} I'_{Baker}(x,y) \\ I'_{random}(x,y) \end{bmatrix} = F(\theta)\begin{bmatrix} I_{Baker}(x,y) \\ I_{random}(x,y) \end{bmatrix}. \tag{7}$$

In the following step, the results from the calculations described above are encoded by using the gyrator transform simultaneously. The image I'_{Baker} and I'_{random} are regarded as the real part and imaginary part of a complex function, respectively. To enhance the security of the encryption scheme, both the affine

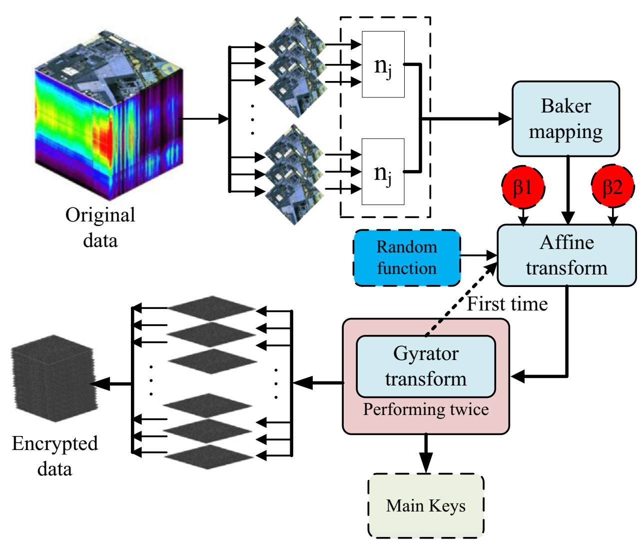

Fig. 1. The flowchart of the encryption algorithm.