Optics and Lasers in Engineering 107 (2018) 62–70

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Optical hyperspectral image encryption based on improved Chirikov mapping and gyrator transform

Hang Chen[a,c,*], Camel Tanougast[a], Zhengjun Liu[b], Walter Blondel[c], Boya Hao[d]

[a] *Laboratoire Conception Optimisation et Modélisation des Systèms, University de Lorraine, Metz 57070, France*
[b] *Department of Automation Measurement and Control, Harbin Institute of Technology, Harbin 150001, China*
[c] *Centre de Recherche en Automatique de Nancy (CRAN), UMR 7039, Nancy 54000, France*
[d] *Research Institute of Special Mechanical and Electrical Technology of Beijing, Beijing 100012, China*

ARTICLE INFO

Keywords:
Hyperspectral image encryption
Cryptography
Optical transform

ABSTRACT

We present an optical hyperspectral image cryptosystem using improved Chirikov mapping in the gyrator transform domains. This optical encryption scheme can hide the spatial and spectrum information simultaneously. First, the original hyperspectral image is converted into binary format and then extended into a one dimensional array. Subsequently, improved Chirikov mapping is performed to generate a position array. Here, the binary array of the image can be scrambled by the position sequence. Finally, three thin cylinder lenses are controlled using a PC to implement the gyrator transform, and the amplitude and phase information in the output plane is considered to be the encrypted information. Some numerical simulations verify the validity and capability of the proposed cryptosystem.

1. Introduction

With the rapid development of multimedia applications, data security is becoming an important issue in the transmission and storage of information. An optical image is one of the most commonly used forms of information in modern life. Such images may be two dimensional, such as with a photograph or screen display, or three dimensional, such as with holograms and hyperspectral images. Optical information security techniques haves become increasingly attractive due to their parallel processing and high speed calculation capabilities possible since double random phase encoding (DRPE) was proposed by Refregier and Javidi in 1995 [1]. DRPE was the first optical image encryption algorithm that was developed and studied [2–7]. Optical encryption techniques offer the possibility of high-speed parallel processing of two-dimensional image data and the hiding of information in many different dimensions, which can vastly improve the security level [8]. In fact, one of the motivations for using optics and photonics in information security is the various complex degrees of freedom possessed by optical waveforms, such as amplitude, phase, large bandwidth, nonlinear transformations and polarization. In recent years, many optical encryption schemes have been proposed based on different kinds of optical transformations, such as the fractional Fourier transform, Fresnel transform and the gyrator transform [9–18]. In some of these encryption schemes, the random phase function is utilized to modulate and change the original image, and this is regarded as the operation randomizing the value of the secret information. Then, the image can be decrypted by employing the reverse process. Furthermore, since the hyperspectral image possesses huge information storage capabilities, the idea of simultaneous compression and encryption is desirable for further applications [19].

From the aspect of enhancing security, many pixel scrambling operations have been introduced into cryptosystems, like the Arnold transform, baker mapping and the jigsaw transform [20–22]. Moreover, the parameters generated in the pixel scrambling operations can be regarded as the extra keys in the encryption scheme. The capability of additional keys to protect secret information has also been proven in these encryption algorithms [20,21]. On the other hand, the optical encryption technique has been extended from a single gray image to color images, double images and even multispectral images in the past decades. However, as an important element in military and commercial remote sensing, the hyperspectral image has not been deeply researched within the optical encryption domain. Optical color encryption technology should be extended to the hyperspectral image, which can make a significant contribution to the security of remote sensing. In the previously proposed encryption algorithms for hyperspectral images [23,24], the encryption operation is employed in each single band image separately, which is similar to an ordinary two-dimensional image encryption scheme. We considered applying an improved Chirikov mapping to scramble all of the bands at the same time.

[*] Corresponding author.
E-mail address: hitchenhang@foxmail.com (H. Chen).

https://doi.org/10.1016/j.optlaseng.2018.03.011
Received 24 October 2017; Received in revised form 11 March 2018; Accepted 12 March 2018
0143-8166/© 2018 Elsevier Ltd. All rights reserved.

In this paper, we present a hyperspectral image encryption algorithm using improved Chirikov mapping and the gyrator transform to encrypt the spatial and spectrum information simultaneously. First, the original hyperspectral image is converted into binary format and then extended into a one-dimensional array. Subsequently, an improved Chirikov mapping is employed to create a position array, for which the binary array of the image can be scrambled according to the position sequence. Then the scrambled and exchanged image is transformed using the gyrator transform. The phase data serves as the main key to the encryption algorithm, and the parameters of the gyrator transform and the improved Chirikov mapping are the additional key to increase security. A numerical simulation is performed to validate the performance of the proposed color image encryption.

The rest of the paper is organized as follows. In Section 2, the proposed encryption/decryption algorithm is introduced in detail. In Section 3, the numerical simulation results are arrived at and presented to demonstrate the validity of the algorithm. Concluding remarks are given in the final section.

2. Hyperspectral encryption algorithm

First, both the improved Chirikov mapping and the gyrator transform are introduced in this section. After that, the intact hyperspectral image encryption algorithm based on the gyrator transform is designed and explained in detail.

2.1. Improved Chirikov mapping

Referring to [25], the Chirikov standard map is an area-preserving chaotic map for two canonical dynamical variables from a square with side 2π onto itself. The definition of a standard Chirikov map can expressed as follows

$$\begin{cases} x' = (k \cdot \sin y + x) \bmod 2\pi \\ y' = (y + x') \bmod 2\pi \end{cases} \tag{1}$$

where k is a positive integer which can be regarded as the control parameter. The variables (x, y) and (x', y') represent the image pixel position before and after employing Chirikov mapping.

To enhance the security of the encryption algorithm, improved Chirikov mapping was designed and its mathematical representation can be described as follows

$$\begin{cases} x' = (k \cdot \sin y + x) \bmod 2\pi \\ y' = (h \cdot y + x') \bmod 2\pi \end{cases} \tag{2}$$

where h is a new control parameter which is also a positive integer. The numerical simulations verify that the increased input parameters for chaotic maps enhance the randomness. In addition, the inverse transform for the improved Chirikov mapping can be calculated as

$$\begin{cases} x = (x' - k \cdot \sin y) \bmod 2\pi \\ y = (\frac{y'-x'}{h}) \bmod 2\pi \end{cases} \tag{3}$$

2.2. Gyrator transform

The mathematical definition of a gyrator transform is given briefly in this subsection. The gyrator transform is a kind of linear canonical transform which only has a two-dimensional format [26,27]. In this optical transformation, an angle α exists in the mathematical representation. For the two-dimensional image $I(x, y)$, the definition of the gyrator transform can be expressed as

$$\begin{aligned} G(u, v) &= \xi^{\alpha}[I(x, y)](u, v) \\ &= \frac{1}{|\sin\alpha|} \iint I(x, y) \exp[i2\pi \frac{(xy+uv)\cos\alpha - xv - yu}{\sin\alpha}] \mathrm{d}x\mathrm{d}y, \end{aligned} \tag{4}$$

where $G(u, v)$ is the output function of the gyrator transform. The parameter α defined in the gyrator transform is a rotation angle which is regarded as the extra key in many encryption schemes. When $\alpha = \pi/2$, the expression of the transform becomes a Fourier transform with the rotation of the coordinates (u, v) [27]. When $\alpha \in [0, 2\pi]$, the gyrator transform can be implemented in an optical system composed of six thin cylinder lenses [27]. The inverse transform of ξ^{α} is $\xi^{-\alpha}$ or $\xi^{2\pi-\alpha}$. The gyrator transform will be adopted in the present encryption algorithm. In addition, other transforms, such as the Fourier transform and the Hartley transform [28] can be used in this algorithm instead of the gyrator transform.

2.3. Color image encryption

A flowchart of the intact encryption scheme in this paper is illustrated in Fig. 1. Both the improved Chirikov mapping and gyrator transform mentioned above are considered and utilized to complete this cryptosystem. First, every single band of the hyperspectral image is regarded as an ordinary gray image and encoded into a binary format, respectively, and then extended into a one-dimensional array. Simultaneously, a sufficiently long position sequence is obtained through the improved Chirikov mapping. Then, the binary array of the original hyperspectral image is scrambled according to the position sequence.

In the following step, the scrambled data is converted back into two-dimensional format. Finally, three thin cylinder lenses controlled by a PC to implement the gyrator transform and the results from the calculations described above are encoded in the gyrator transform domain. Every amplitude function of the output from the gyrator transform is composed of cube data which is regarded as the final encrypted image in this paper. The final output function of the gyrator transform can be encoded into the format with amplitude $A(x, y)$ and phase $\phi(x, y)$ which can be expressed as follows

$$A(x, y) \exp[i\phi(x, y)] = I_e(x, y) + i \times I_{key}(x, y) \tag{5}$$

where $I_e(x, y)$ denotes the encrypted image and $I_{key}(x, y)$ represents the main key for decrypting the original image. Due to its large scale and strong randomness, the phase function from the gyrator transform can be regarded as the main key in this encryption algorithm. Furthermore, the size of the encrypted hyperspectral image has the same quality as the original hyperspectral image. All amplitudes and phases will be encoded into the optical encryption system of the gyrator transform by modulation of the spatial light modulator (SLM) [27].

Every step in the flowchart of the encryption algorithm is reversible. Therefore, image decryption can be performed in the reverse direction of the encryption process with inverse transforms. As mentioned above, the parameter α in the gyrator transform can serve as the additional key to increase the security of the encryption scheme. To retrieve the secret hyperspectral image, both the main keys and additional key are necessary in the decryption process. Some simulations will be given to show the result of losing a key in the following section.

The proposed cryptosystem can be implemented using an electro-optical setup as depicted in Fig. 2. The operations in Chirikov mapping and binary array scrambling can be employed by a computer during the decryption/decryption process, while the gyrator transform and its inverse transform can be implemented using an optical system [27]. The optical beams will be utilized for encoding each band of the hyperspectral image. In the output plane, an off-line holography technique is introduced to record the phase information. The other calculation can be performed on a computer. Moreover, the SLM and CCD will accomplish the data communication between the computer and optical system. The algorithm can serve in the hardware-based cryptographic system.

3. Numerical simulation

Some numerical simulations are carried out to demonstrate the validity and capability of the proposed encryption algorithm. To complete the experiments, a hyperspectral image 'Sandiego' from AVIRIS having 189 wavelength bands is considered the original image. The image spatial size for each spectral band is 256 × 256 and the image shows a military airport scene. The false RGB color composites consisting of the