Optics and Lasers in Engineering 91 (2017) 106–114

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Optical noise-free image encryption based on quick response code and high dimension chaotic system in gyrator transform domain

Liansheng Sui[a,*], Minjie Xu[a], Ailing Tian[b]

[a] School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China
[b] Shannxi Province Key Lab of Thin Film Technology and Optical Test, Xi'an Technological University, Xi'an 710048, China

ARTICLE INFO

Keywords:
Double random phase encoding
Image encryption
Phase retrieval algorithm
Gyrator transform

ABSTRACT

A novel optical image encryption scheme is proposed based on quick response code and high dimension chaotic system, where only the intensity distribution of encoded information is recorded as ciphertext. Initially, the quick response code is engendered from the plain image and placed in the input plane of the double random phase encoding architecture. Then, the code is encrypted to the ciphertext with noise-like distribution by using two cascaded gyrator transforms. In the process of encryption, the parameters such as rotation angles and random phase masks are generated as interim variables and functions based on Chen system. A new phase retrieval algorithm is designed to reconstruct the initial quick response code in the process of decryption, in which a priori information such as three position detection patterns is used as the support constraint. The original image can be obtained without any energy loss by scanning the decrypted code with mobile devices. The ciphertext image is the real-valued function which is more convenient for storing and transmitting. Meanwhile, the security of the proposed scheme is enhanced greatly due to high sensitivity of initial values of Chen system. Extensive cryptanalysis and simulation have performed to demonstrate the feasibility and effectiveness of the proposed scheme.

1. Introduction

As we know, image security that utilizes optical techniques has become an important research topic during the past decades. Since Refregier and Javidi proposed the famous image encryption architecture based on double random phase encoding (DRPE) in Fourier transform domain [1], a large number of schemes which make use of different optical techniques such as diffractive imaging [2,3], integral imaging [4,5], ghost imaging [6–8], photon-counting [9,10], polarized light encoding [11], interferometer [12,13], compressive sensing [14–16] and ptychography [17] have been suggested. It is worth noting that the plain image can be encrypted and compressed simultaneously by using special optical schemes which are introduced by Alfalou and Brosseau [18]. Numerous kinds of optical image encryption techniques are analyzed [19,20], which provide potential solutions to purely optical cryptosystem. Recently, Javidi et al. [21] present an overview of the potential, recent advances and challenges of optical security and encryption using free space optics in different aspects such as novel encryption approaches, compression for compressed data, phase retrieval algorithms, implementation at nano- or micro-scale, ghost imaging and quantum imaging.

Due to intrinsic linearity, image encryption schemes based on DRPE architecture have serious security risks, namely they are vulnerable to several forms of attack such as known plaintext attack [22–24]. In order to enhance security, the DRPE-based architecture has been extended into various transform domains such as fractional Fourier transform domain [25,26], Fresnel transform domain [27–29], gyrator transform (GT) domain [30–32], fractional angular transform domain [33,34], fractional random transform domain [35], fractional Mellin transform domain [36], gyrator wavelet transform domain [37] and lifting-wavelet transform frequency domain [38] in which additional parameters can be employed as the private keys. The output of these schemes usually is the complex amplitude distribution, which is not convenient to store and transmit because optical elements such as spatial light modulator cannot record the phase and amplitude data simultaneously. To avoid considering the complex data as ciphertext, a plenty of schemes based on interference is suggested since Zhang and Wang [39] originally proposed to encrypt a plain image into two phase-only masks (POMs) without using iterative calculations. However, an inherent problem among these optical cryptosystems cannot be resolved efficiently, where the silhouette information of the plain image can be detected presumably when any one of resultant masks is deployed in the process of decryption [40–45]. Additionally, a plenty of image encryption schemes based on different chaotic maps are

* Corresponding author.

http://dx.doi.org/10.1016/j.optlaseng.2016.11.017
Received 5 August 2016; Received in revised form 17 November 2016; Accepted 17 November 2016

presented [46–49], in which the plain image can be encoded as the real-valued function.

Recently, approaches have been reported to solve the silhouette problem by making use of additional techniques such as time-consuming transformation, encoding with larger number of POMs and phase retrieval algorithms. In the scheme suggested by Kumar et al. [50], this shortcoming is surmounted by employing the jigsaw transformation in a single step. Wang and Zhao [51] generalized earlier interference-based encryption scheme with two POMs and suggested to hide the information of plain image into three POMs, in which it is still possible that the remnant information can be intercepted by an unauthorized user when two of POMs are known simultaneously. Wang et al. [52] encrypted the plain image into two complex ciphertexts, in which it makes the decryption process complicated that the random POM and related complex field distribution should be modulated by two predesigned phase-only factors. Wang et al. [53] presented an image hiding method to encrypt the plain image into two POMs by using the phase retrieval algorithm under the framework of nonlinear DRPE, which is time-consumed. Due to the property of fast read capacity, Quick response (QR) code has been widely deployed in the field of image encryption. Wang et al. [54] proposed an optical encryption technology by using the known positions of QR code as support constraint, in which the original image can be decrypted with the phase retrieval process. Barrera et al. [55] reported an experimental implementation of a noise-free data recovering based on the joint transform correlator architecture, in which the QR code is used as a container of plain image. Wang et al. [56] designed a secured information retrieval scheme of triple images based on two authenticated phase-only masks, which are calculated with three QR codes of plain images as amplitude constraints.

Different from aforementioned schemes, a novel optical encryption system based on QR code and high dimension chaotic system is proposed under the architecture of DRPE in GT domain in this paper. In the process of encryption, the real-valued ciphertext image can be obtained by only recording the intensity distribution of two cascaded GTs, which are performed on the QR code of the plain image. In the process of decryption, a new phase retrieval algorithm is designed to reconstruct the corresponding QR code from the ciphertext image, in which the known three position detection patterns of QR code are used as the support constraint to achieve high convergence speed. Importantly, although the reconstructed QR code may be destroyed seriously under some kinds of attack, the plain image can be visualized perfectly without any energy loss of information due to high error correction capability of QR code. Finally, numerical simulation results are carried out to demonstrate the feasibility and effectiveness of the proposed scheme.

The rest of this paper is organized as follows. In Section 2, the encryption and decryption processes are introduced in detail. In Section 3, numerical simulation results and security analysis are given. Finally, the conclusion is given in Section 4.

2. Encryption and decryption processes

As an important two-dimensional barcode with many excellent properties such as fast readability with mobile devices such as smart phones, large storage capacity and high error tolerance capability, QR codes have been demonstrated great potential for image encryption. In the proposed scheme, the plain image to be encrypted is first transformed to the corresponding QR code by making use of some generation tools. The consequential QR code as an information container is considered as the input image of the DRPE architecture in the gyrator transform domain. The optical setup is schematically shown in Fig. 1, in which tow chaotic random phase masks (RPMs) are placed in the spatial plane and frequency plane, respectively, and the intensity-sensitive device such as charge-coupled device (CCD) camera in the output plane.

Let the function $f(x, y)$ with size of $M \times N$ pixels denotes the consequential QR code, which is illuminated by a coherent parallel light beam and encrypted by using two chaotic RPMs represented by $r_1(x, y)$ and $r_2(x', y')$, respectively. Initially, $f(x, y)$ is multiplied with the first RPM $r_1(x, y)$, and then the product is optically transformed by using the first GT with the rotation angle α_1. The transformed result is multiplied with the second RPM $r_2(x', y')$, and then the product is optically transformed by using the second GT with the rotation angle α_2. Finally, by superimposing the transformed result on the plane reference beam, the intensity distribution in the output plane is considered as the ciphertext which can be captured in the output plane by recording the holographic interference fringe as an off-axis hologram with CCD camera. The process can be expressed mathematically as

$$C(x'', y'') = |G^{\alpha_2}\{G^{\alpha_1}\{f(x, y) \times r_1(x, y)\} \times r_2(x', y')\}|^2, \tag{1}$$

where $G^{\alpha}\{\cdot\}$ denotes the GT with the rotation angle α and $|\cdot|$ represents the modulus operation. Due to its excellent properties such as the fixed distance between generalized lenses and input-output planes, GT has been widely employed to image encryption [57,58]. Additionally, GT can be implemented optically by utilizing the FT, inverse FT and phase-only filtering with the help of convolution operation [59]. It should be pointed out that the proposed scheme only records the intensity information of the transformed result as the ciphertext with stationary white noise distribution and is different from other encryption schemes under the framework of DRPE where the encrypted results usually are the complex amplitude functions.

As a high-dimension chaos function, Chen system has more complicated dynamical property, which makes it more suitable for practical applications in the fields of optical image encryption [60]. In order to further improve the security of the proposed scheme, two chaotic RPMs $r_1(x, y)$ and $r_2(x', y')$ used in Eq. (1) are generated randomly based on Chen system which is expressed as follows

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy, \\ \dot{z} = xy - bz \end{cases} \tag{2}$$

where a, b and c denote control parameters. Given the initial values x_0, y_0 and z_0, when the control parameters are set to $a = 35$, $b = 3$ and $c \in [20, 28.4]$, three different random value sequences with non-periodic and non-convergent properties can be engendered by iterating this chaotic system with large iterations. In the process of iteration, the fourth order Runge-Kutta algorithm with the small step value such as 0.001 is repeatedly performed. Let three random value sequences are denoted as x_i, y_i and z_i, respectively. According to first two sequence x_i and y_i, only the last $M \times N$ iterative values are preserved to form two new sequences s_1 and s_2 as follows

$$s_1 = 2\pi \times ((abs(x_i) - floor(abs(x_i))) \times 10^{14} \bmod(256))/255, \tag{3}$$

$$s_2 = 2\pi \times ((abs(y_i) - floor(abs(y_i))) \times 10^{14} \bmod(256))/255. \tag{4}$$

where $abs(\cdot)$ is used to compute the absolute value and $floor(\cdot)$ is used to obtain the nearest integer of the argument. Through rearranging the sequence s_1, the two-dimensional matrix denoted as $\{s_1'(i, j)|i = 1, 2, \ldots, M; j = 1, 2, \ldots, N\}$ is obtained, with which the first RPM $r_1(x, y)$ is produced as $\exp(is_1'(i, j))$. Similarly, the second RPM $r_2(x', y')$ is generated as $\exp(is_2'(i, j))$ with the matrix $\{s_2'(i, j)|i = 1, 2, \ldots, M; j = 1, 2, \ldots, N\}$ after rearranging the sequence s_2. Apparently, s_1' and s_2' are two independent random phase functions distributed in the range $[0, 2\pi]$. Obviously, two RPMs $r_1(x, y)$ and $r_2(x', y')$ are used as the interim functions and not considered as the private phase keys directly. Because no random phase masks are used as the private keys, the proposed scheme has high convenience to the management of secret keys in the process of storage and transmission.

Different from other encryption schemes in gyrator transform domain where the rotation angles are predefined as the fixed values, α_1 and α_2 used in Eq. (1) are respectively calculated from the matrices s_1'