Optics and Laser Technology 103 (2018) 93–98

Contents lists available at ScienceDirect

Optics and Laser Technology

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

Full length article

Binary image encryption in a joint transform correlator scheme by aid of run-length encoding and QR code

Yi Qin [a,*], Zhipeng Wang [b], Hongjuan Wang [a], Qiong Gong [a]

[a] College of Mechanical and Electrical Engineering, Nanyang Normal University, Nanyang 473061, China
[b] College of Physical and Electrical Engineering, Nanyang Normal University, Nanyang 473061, China

ARTICLE INFO

Article history:
Received 28 September 2017
Received in revised form 29 October 2017
Accepted 4 January 2018

Keywords:
Optical encryption
Joint transform correlator
QR code

ABSTRACT

We propose a binary image encryption method in joint transform correlator (JTC) by aid of the run-length encoding (RLE) and Quick Response (QR) code, which enables lossless retrieval of the primary image. The binary image is encoded with RLE to obtain the highly compressed data, and then the compressed binary image is further scrambled using a chaos-based method. The compressed and scrambled binary image is then transformed into one QR code that will be finally encrypted in JTC. The proposed method successfully, for the first time to our best knowledge, encodes a binary image into a QR code with the identical size of it, and therefore may probe a new way for extending the application of QR code in optical security. Moreover, the preprocessing operations, including RLE, chaos scrambling and the QR code translation, append an additional security level on JTC. We present digital results that confirm our approach.

1. Introduction

There has been a growing interest in the use of optical techniques for information security applications [1–7] since Refregier and Javidi proposed their representative work of double random phase encryption (DRPE) [8]. Many other methods based on modern optical principles, such as interference [9], holography [10], diffraction [11], and polarization [12], have been developed for information security. Among these methods, the joint transform correlator (JTC) encryption is of particular importance, as the ciphertext can be directly recorded by intensity-sensitive device and the encryption-decryption procedure is realized in a pure optical manner [13]. Compared to DRPE, alignment and resolution requirements in JTC are relaxed, and spatial filter synthesis is also unnecessary. Consequently, the JTC encryption is extensively investigated for various applications. For example, Amaya et al. proposed to employ wavelength-multiplexing for multiple-image encryption [14]. Lu and Jin further extended the encryption from Fourier domain to fractional Fourier domain [15]. Mela and Iemmi combined the JTC with phase-shifting interferometry to enable the complete encryption–decryption process to be achieved at high speed [16]. Recently, Mosso et al. presented the first experimental technique to encrypt a movie in JTC [17]. Despite the aforesaid merits of JTC, challenges remained. As it is shown in these previous approaches, the decrypted images from JTC architecture degrade severely in quality. Although several efforts are devoted to improve the decryption [18,19], the primary image can still not be completely retrieved. More recently, Zea et al. show the feasibility of complete information retrieval in JTC by aid of the QR code and a customized code, however, the plaintext in their proposal is not an image but a string [20].

Another defect of JTC is its vulnerability against attacks. It has been broken by known-plaintext attack (KPA) [21], chosen-plaintext attack (CPA) [22] and even cipher-only attack (COA) [23]. Consequently, how to enhance its security becomes a significant topic. To do this, Rueda et al. employed another random phase mask as an additional key to reinforce the system security [24]. However, the introduction of the new key obviously complicates the system infrastructure. In this regard, it is hoped to obtain a security-enhanced JTC while maintaining its concise scheme.

Recently, QR code emerges as a data container in optical security and attracts sufficient attention. Barrera et al. show, for the first time, that transforming the primary information into the corresponding QR code before a standard optical encrypting procedure guarantees its perfect retrieval without quality loss, as QR codes are tolerant to speckle noise [25–27].

In this paper, with the help of the QR code, we report a binary image encryption method in JTC that ensures complete retrieval of the plaintext. Before being transformed into the QR code, the binary image is first compressed by run length encoding (RLE) and then permutated with chaos scrambling. The RLE produces

[*] Corresponding author.
E-mail address: 641858757@qq.com (Y. Qin).

https://doi.org/10.1016/j.optlastec.2018.01.018
0030-3992/© 2018 Elsevier Ltd. All rights reserved.

the highly compressed data of the primary image and thus allow it to be encoded into a QR code with the same size as the primary image. Meanwhile, the scrambling appends an additional security level on the cryptosystem.

2. Principle

2.1. Run-length encoding

Run-length encoding (RLE) is known as an important coding approach achieving lossless data compression [28]. In RLE, a string will be divided into several runs, and each run consists of identical letters. Thereafter, the string can be represented by consecutive pairs of the representative letter and the length of the corresponding run. For example, string 'bbcccccddaaaaa' can be compressed into RLE format as b2c6d2a5. Such a run-length encoded string can be significantly shorter than the expanded string representation. In fact, RLE serves as a popular image compression technique, since many classes of images, such a s binary images in facsimile transmission, typically contain large patches of identically valued pixels. It is also easy to know that compression ratio could be further enhanced for binary sequence. For instance, string '111110001111111' can be compressed into RLE format as '5 3 7'. In addition, the run-length decoding (RLD) is a simple inverse of RLE, whose principle is easy to follow.

2.2. Chaos scrambling

The chaos is a process of definite pseudo-random sequence generated by nonlinear dynamics system. The dynamical systems can be expressed by various chaos maps that are very sensitive to the initial conditions and parameters. With a chaotic map, large number of random iterative values with the expected properties of non-correlation, pseudo-randomness, ergodicity can be produced. In this paper, the logistic map is used to scramble the compressed sequence by RLE, and its expression is shown as Eq. (1).

$$q_{k+1} = \gamma q_k (1 - q_k) \tag{1}$$

where $\gamma \in (0, 4]$ is the control parameter and $q_k \in [0, 1]$ is the sequence value. When $\gamma \in [3.5699496, 4]$, small variations in the initial value will produce extremely different results over time. For scrambling a sequence with a size of K, the chaos-based sequence scrambling can be achieved by completing the following steps [29]. First of all, a random sequence $S = \{s(k)|k = 1,2,\ldots,K\}$ with K elements is generated by the logistic map, where $s(k)$ and k stand for respectively the element value and its position. Thereafter, sorting the sequence S in ascending order or descending order, a new sequence S' is obtained. Evidently, the rearranged sequence changes only in the positions of the elements. In other words, each element in S has a new position in the new sequence S', as a consequence of which an address map is generated. Therefore, we can reorder the primary sequence by following the same address map.

2.3. The JTC encryption and the proposal

The illustration for implementation of JTC encryption is depicted in Fig. 1. In the encryption procedure of JTC scheme [Fig. 1(a)], the original image $f(x,y)$, bonded to a random phase mask $\alpha(x,y)$, is positioned at coordinate $x = a$. The complex-valued key code $h(x,y)$, which is the inverse Fourier transform of a random-phase mask $H(\mu,\nu)$, is positioned at coordinate $x = -a$. The two random phase masks are statistically independent and have uniform amplitude transmittance. When the input plane is illuminated by a monochromatic plane waves, the joint power spectrum (JPS) can be obtained at the output plane [13]:

$$\begin{aligned} JPS(\mu,\nu) = {} & |A(\mu,\nu) * F(\mu,\nu)|^2 + 1 + [A(\mu,\nu) * F(\mu,\nu)]^c H(\mu,\nu) \\ & \times \exp[-j2\pi(-2a)\mu] + [A(\mu,\nu) * F(\mu,\nu)]^c H^c(\mu,\nu) \\ & \times \exp[-j2\pi(2a)\mu] \end{aligned} \tag{2}$$

In above equations, the centered asterisk and superscript 'c' denote convolution and complex conjugation, $F(\mu,\nu)$ and $A(\mu,\nu)$ represent the Fourier transforms of $f(x,y)$ and $\alpha(x,y)$,respectively. The JPS is saved as the ciphertext.

In the decryption process [Fig. 1(b)], the joint power spectrum is illuminated by a Fourier transform of the key code and then inverse-Fourier-transformed. In the output plane we can obtain:

$$\begin{aligned} d(x,y) = {} & h(x,y) * [\alpha(x,y)f(x,y)] \bullet [\alpha(x,y)f(x,y)] * \delta(x+a,y) \\ & + h(x,y) * \delta(x+a,y) + h(x,y) * h(x,y) \bullet [\alpha(x,y)f(x,y)] \\ & * \delta(x-3a,y) + \alpha(x,y)f(x,y) * \delta(x-a,y) \end{aligned} \tag{3}$$

It can be known that the fourth term on the right side of this equation separates spatially from the other three terms, which are totally noise-like images. In fact, the intensity of it produces the original image, since $\alpha(x,y)$ is a pure phase term that can be removed by an intensity-sensitive device.

The proposed method is a sequential combination of RLE, chaos scrambling, QR code and JTC encryption. The input binary image is firstly transformed into a highly compressed sequence by RLE, and is then rearranged by chaos scrambling. After that, the permuted sequence is encoded into a QR code, which is sent to JTC to complete the encryption. The decryption is a simple inverse process of the encryption. For decryption, the QR code is retrieved from JTC decryption, whose content is subsequently read out and reordered to rover the primary compressed sequence. Then, by aid of Run-length decoding, the primary binary image can be retrieved from this sequence. The whole process of encryption and decryption can be concisely illustrated in the flow charts as shown in Fig. 2.

3. Digital results and discussions

A series of computer simulations have been carried out on the platform of Matlab R2011a to show the feasibility and effectiveness of the proposal. The parameters of the logistic map are set as $q_0 = 0.98$, $\gamma = 3.6$. The wavelength of the illuminating light is 632.8 nm. The primary binary image with a size of 128 × 128 pixels is shown in Fig. 3(a), and the encoded result of it by RLE is shown in Fig. 3(b). Thereafter, the result in Fig. 3(b) is permutated with chaos scrambling, obtaining a reordered sequence [Fig. 3(c)]. The sequence is then encoded into the QR code depicted in Fig. 3 (d). The final encryption result, which is shown in Fig. 3(e), is obtained by putting the QR code into the JTC encryption scheme. The correlation coefficient (CC) is introduced as a criterion for evaluating the similarity between the input and the decrypted image [27]. Fig. 3(f) shows the decrypted QR code from the ciphertext, for which the CC value is 0.2991. Although the QR code suffers from some degradation in quality, a smart phone can read out its content, which is found to be identical with that in Fig. 3(c). Thereafter, by the successive operations of inverse chaos scrambling and RLD, the primary binary image can be exactly retrieved[Fig. 3(g)]. For comparison, we show in Fig. 3(h) the decrypted result of the primary image when the traditional JTC scheme is employed, corresponding to a CC value of 0.0460. It is seen that the recovered plaintext degrades severely in quality and only a blurry silhouette can be observed. From Fig. 3(g) and (h) it is seen that, comparing with the poor decryption quality from the conventional JTC encryption scheme, the output of the proposal is completely a replica of the primary image. Moreover, the improvement in