Optics and Laser Technology 111 (2019) 196–204

Contents lists available at ScienceDirect

Optics and Laser Technology

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

Full length article

A secure image encryption method using scan pattern and random key stream derived from laser chaos

T. Sivakumar[c], Pu Li[a,b,*]

[a] Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education of China Taiyuan University of Technology, Taiyuan 030024, China
[b] Institute of Optoelectronic Engineering, Taiyuan University of Technology, Taiyuan 030024, China
[c] Department of Computer Science & Engineering, Dr. Mahalingam College of Engineering & Technology, Coimbatore, Tamil Nadu 642003, India

HIGHLIGHTS

- Our method uses random keys from optical chaos to achieve the image encryption.
- Our method only needs single iteration, but can achieve a significant performance.
- Our method resists the security attacks and takes less time for encryption.

ARTICLE INFO

Keywords:
Laser chaos
True random numbers
Image encryption
Scan pattern
Cryptanalysis

ABSTRACT

Internet allows people in any corner of the world to share instantly all types of information. Secure sharing of sensitive multimedia data necessitates confidentiality service, which is offered by encipherment mechanism. In this paper, a fast and secure image encryption method using scan patterns and true random key streams is proposed. The scan pattern is used to scramble the original image by means of pixel permutation. The random key stream is generated employing a photonics based approach and then used to perform a bitwise XOR operation to get the encrypted image. The proposed method takes very less time for encryption and has substantial resistance with statistical, differential and entropy attacks.

1. Introduction

The amount of digital visual data has increased rapidly today. Image, video and 3D object security becomes increasingly important for many applications such as confidential transmission, video surveillance, military and medical fields. Traditional cryptosystems such as DES, AES and IDEA are often used to encrypt/decrypt textual data. However, these algorithms are not suitable to encrypt multimedia data, due to the large data size and execution time constraints.

In recent years, image encryptions based on permutation are paid great attention because of its fast processing rate. Although there have been many permutation based techniques to achieve image encryption, they can be classified as pixel permutation [1–17], bit permutation [20–23], and block permutation [24–28]. Generally, the performance of block permutation is average and it provides a better result when the block size is very small. Bit permutation methods involve more time for encryption than block and pixel permutation. But, pixel permutation methods offer better results and an acceptable encryption time.

However, some existing encryption methods have already been found insecure among these image encryption methods. Moreover, most of these encryption methods are not secure against all kind of security attacks. Also, the encryption function in several of the image encryption methods is iterated for many times to achieve better results. For instance, the encryption process is repeated for 10 times in Ref. [10]. Random numbers play major role in designing and implementing encryption and decryption methods [29–31,34,37]. Fast random bit sequences can be generated using physical chaos in semiconductor lasers [38]. The chaotic dynamic characteristics of laser diodes are attractive for practical applications such as chaos-based secure communications and random number or bit generation [39,40].

In this paper, a new and secure image encryption method with a scan based pixel permutation and a bitwise XOR operation using true random key streams is proposed. Through generating a large number of wide varieties of scanning paths with continuous diagonal and orthogonal, we utilize the true random key stream derived from a chaotic laser to encrypt the image by the bitwise XOR operation. The proposed method only needs single iteration, but can achieve a significant performance. Moreover, the method resists the security attacks and it will

* Corresponding author.
E-mail address: lipu8603@126.com (P. Li).

https://doi.org/10.1016/j.optlastec.2018.09.048
Received 8 May 2018; Received in revised form 14 July 2018; Accepted 23 September 2018

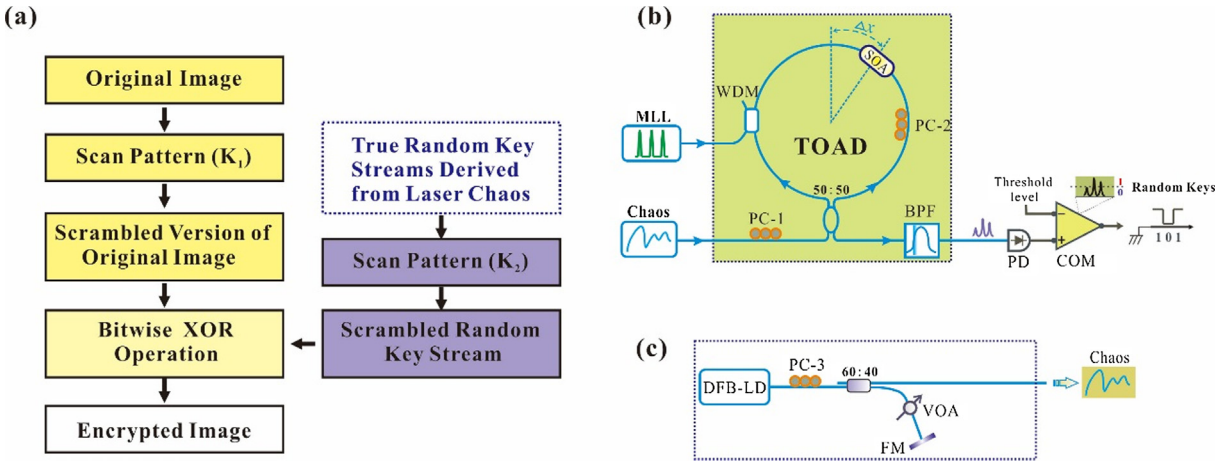
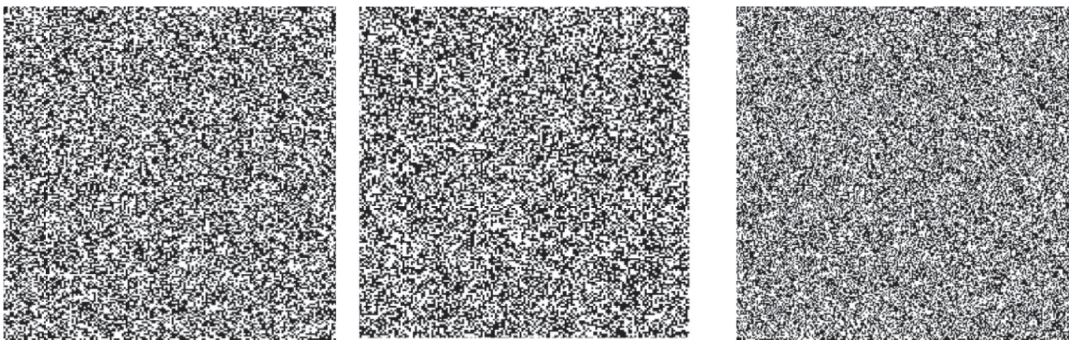
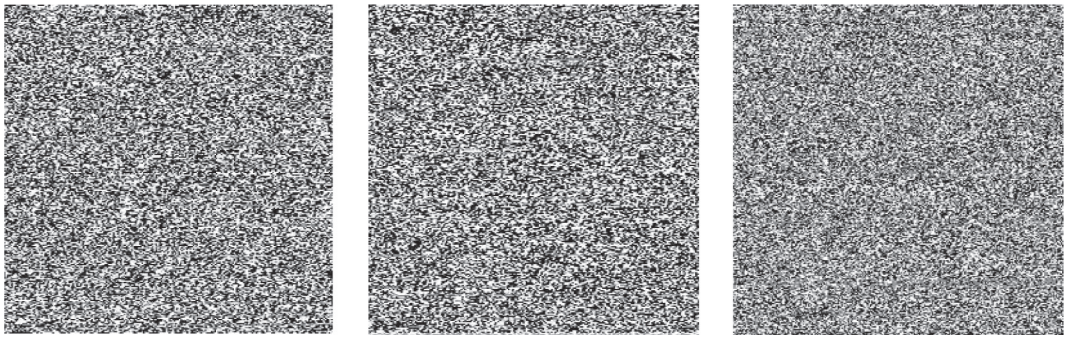


Fig. 1. (a) Block diagram of the proposed image encryption method, (b) Schematic of the fully photonic true random bit generator (TRBG) based on laser chaos and (c) the setup of the chaotic laser used in the experiment. Note: MLL, ultrafast mode-locked laser; Chaos, chaotic laser; WDM, wavelength division multiplexer coupler; SOA, semiconductor optical amplifier; 50:50, 3-dB coupler; PC-1, PC-2 and PC-3, polarization controllers; BPF, optical band-pass filter; PD, photo-detector; COM, comparator; DFB-LD, distributed feedback laser diode; 60:40, 60:40 coupler; VOA, variable optical attenuator; FM, fiber mirror.



(a) Random_1 (R_1) (b) Random_2 (R_2) (c) Random_3 (R_3)

Fig. 2. Sampled random bit streams.



(a) Random_1 (R_1) (b) Random_2 (R_2) (c) Random_3 (R_3)

Fig. 3. Scrambled random bit streams.

take less time for encryption.

The rest of the paper is organized as follows. Section 2 presents our proposed image encryption method. Section 3 deals with the experimental results and analysis. Discussion of results is given in Section 4 and the paper is concluded in Section 5.

2. Proposed image encryption method

Fig. 1(a) presents a block diagram that shows the operation processes of the proposed encryption method. First, the pixels of original image are permuted by using the scan pattern mentioned in key-1 (K_1). Next, the true random key stream is also permuted with the scan pattern mentioned by key-2 (K_2). Both K_1 and K_2 are the basic scan patterns, either continuous diagonal or orthogonal. Finally, the scrambled version of the original image is XOR-ed with the scrambled version of the random key stream to obtain the encrypted image.

2.1. Encryption algorithm

Specifically, the encryption process is executed as the following steps:

Step 1: Start the process.