Optics and Laser Technology 108 (2018) 162–169

Contents lists available at ScienceDirect

Optics and Laser Technology

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

Research Note

Novel encryption method based on optical time-delay chaotic system and a wavelet for data transmission

Adil Bouhous, Karim Kemih *

L2EI Laboratory, Jijel University, Algeria

ARTICLE INFO

Article history:
Received 16 April 2018
Received in revised form 9 May 2018
Accepted 25 June 2018

Keywords:
Novel encryption method
Optical time-delay chaotic system
Descriptor observer design
Discrete wavelet transform
Watermarking

ABSTRACT

In this paper, a new encryption approach based on optical time-delay chaotic system and a wavelet is proposed for date transmission. The general principle of this method is to drown the image in the chaos before inserting it into the approximation of another image (watermarking) obtained using the discrete wavelet transform (DWT). At the receiver, we use a descriptor observer with an unknown input design to establish synchronization between the transmitter and the receiver and to recover the transmitted encrypted image. The received image is decrypted after being extracted the encrypted image by using the discrete wavelet transform (DWT) and a decryption function. The got results plainly show the effectiveness of the proposed method which can be used to secure transmission of medical images.

1. Introduction

Cryptography is a means of storing and transmitting information in a private way so that only intended audiences can access it. This means is highly efficient for conserving and protecting sensitive messages stored on a medium or transmitted on unsecured networks. The purpose of cryptography is to hide information with unauthorized people, it has sustained various changes that closely follow the progress of technology. Many researchers have been drawn to the founding work of Pecora and Caroll [1], so they have studied complex nonlinear systems and added a whole new dimension to cryptography [2–11]. One of the most used techniques by researchers is encryption by chaotic systems. Chaos is defined by the behaviour related to instability and non-linearity in deterministic dynamic systems, the relation between instability and chaoticity is then that the system is highly sensitive to changes in initial conditions. These characteristics are the desired criteria in the application of encryption. Another technique broadly used in encryption is digital watermarking. This technique makes it possible to add and integrate secret information in images such as medical images, videos or other digital documents, and thanks to the wide application of this technique in cryptography, many studies have been conducted recently [12–16].

On the other hand, the synchronization of chaotic systems is not obvious. The possibility of having two identical oscillating systems is not easy. As we have already mentioned, chaos is characterized by a strong dependence on initial conditions, two initial conditions almost similar can lead to very different states of the system, it can be seen that synchronization is not possible. To overcome this problem, there are two approaches. The first approach is the drive-response technique proposed by Carroll and Pecora in 1990 [1]. The transmitter in this scheme is known as the drive system while at the receiver, the system is called the response system. The principal limitation of this concept is the lack of a systematic procedure to find a good decomposition of the drive system in order to guarantee negative conditional Lyapunov exponents. This approach is considered a self-synchronization and can be opposed to the other approach which is observer-based synchronization [17–22]. The problem of synchronization can be considered as a problem of state estimation, by giving the transmitter chaotic, the observer of this system could be considered as the receiver of the system [21]. Many papers in literature have studied this problem, such as in [23], the authors proposed s a new approach to design an observer for chaotic system reconstruction using chaotic T–S model. An unknown input observer for a class of nonlinear systems in the presence of uncertainties that appears on both the state and output matrices in developed in [24]. In [25], the authors proposed a new approach to synchronize chaotic system using unknown inputs Takagi–Sugeno fuzzy observer.

In this work, we propose a novel encryption method based on optical time-delay chaotic system and watermarking using wavelets to transmit a secure image through a communication channel. Our algorithm is composed of three steps: (1) encryption- alpha

* Corresponding author.
E-mail address: karim.kemih@ensea.fr (K. Kemih).

https://doi.org/10.1016/j.optlastec.2018.06.052
0030-3992/© 2018 Elsevier Ltd. All rights reserved.

blending embedding, (2) synchronization, and (3) alpha blending extraction-decryption. We use a chaotic hybrid optical bistable system with a time delay as a chaotic transmitter. The Synchronization is ensured using a descriptor observer with an unknown input.

The layout of this paper is as follows: Section 2 presents and bestows details of the different parts of the proposed method. Simulations results obtained in Section 3 validate our encryption method. Finally, Section 4 concludes the paper.

2. The novel image encryption algorithm

2.1. Related work

Several methods of image encryption have been proposed in the literature, Ratnavelu et al. [2] used fuzzy cellular neural networks that have chaotic behaviour to encrypt images. Zahmoul et al. created a new map to generate chaotic sequences, this map is based on the Beta function and is used for image encryption [6]. Parvaz and Zarebnia defined a combined chaotic system based on logistic, Sine and Tent systems. This combined chaotic system is utilised to introduce an algorithm for encrypting images [7]. Kadir et al. injected impulse signals randomly into the Lorenz system to improve the complexity of the trajectory and to encrypt color images [9]. Mao et al. proposed a new image encryption method based on the chaotic Baker map [10]. Gulshan et al. used the discrete wavelet transformation (DWT) and the international data encryption algorithm (IDEA) for developed a new technique chaotic image encryption [11].

2.2. The proposed method

A schematic description of the method proposed in this article is shown in Fig. 1. As we can show, the novel encryption method to secure communication is structured in three steps:

(1) encryption- alpha blending embedding; (2) synchronization; (3) alpha blending extraction-decryption. In the first step, we use a highly nonlinear function $\varnothing$ to encrypt the original image S_T with the chaotic state signals $x_t(t)$ after, we use the Discrete Wavelet transform (DWT) to add the encrypted image (watermark) in an approximation of a cover image (alpha blending embedding). In the second step, one synchronization is assured between the transmitter and the receiver, Synchronization is ensured by the design of a nonlinear state observer, steer by the transmitted signal, the transmitted signal which carries the transmitted image (watermarked image). In the third step, we use the estimates $x_r(t)$ produced from the synchronizer (state observer), alpha blending extraction and the decryption function (φ) to reproduce an approximate estimate of the transmitted image (recovered image).

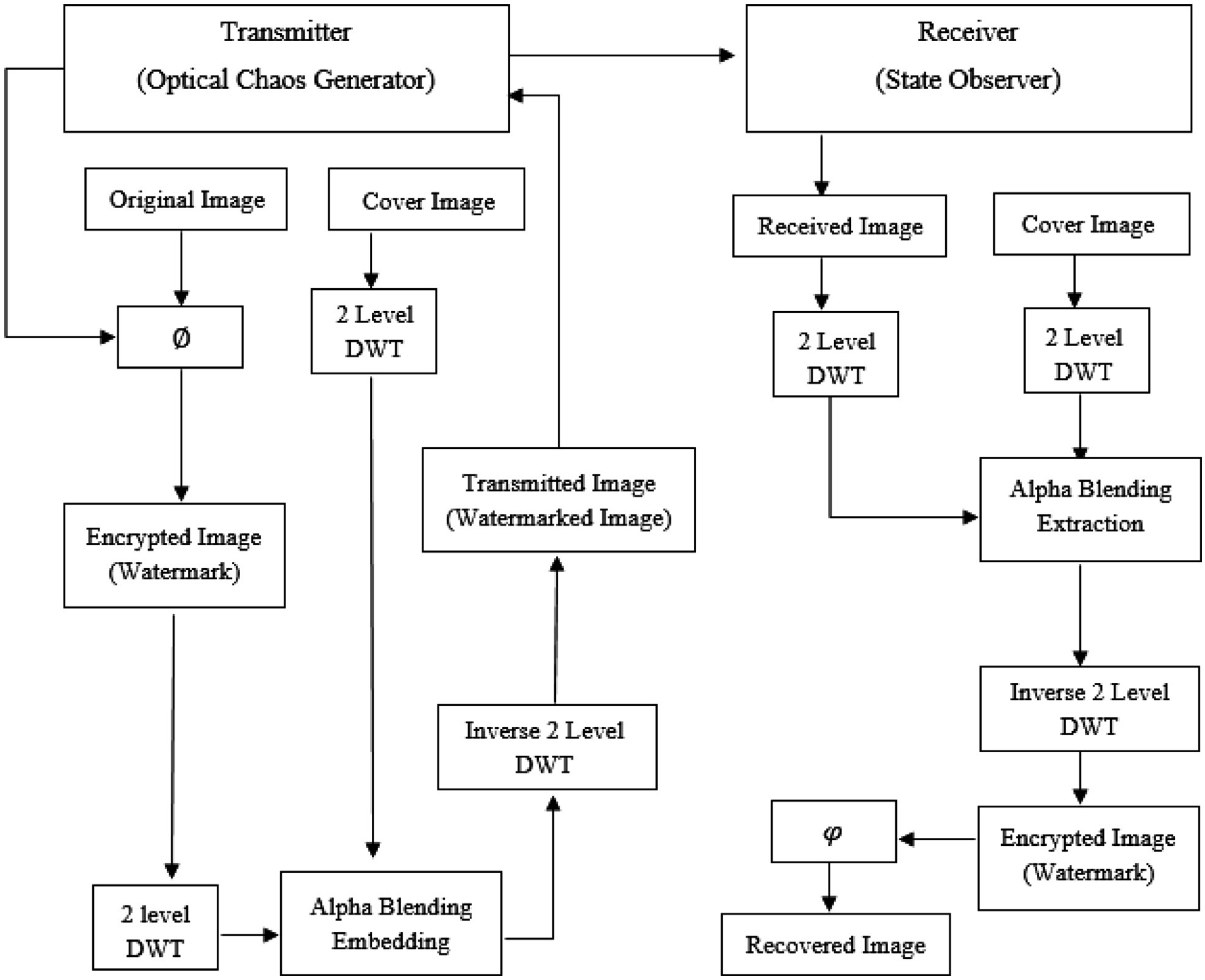

Fig. 1. Proposed method.