Optics and Lasers in Engineering 88 (2017) 37–50

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms

Akram Belazi [a,*], Ahmed A. Abd El-Latif [b], Adrian-Viorel Diaconu [c], Rhouma Rhouma [a], Safya Belghith [a]

[a] National Engineering School of Tunis, Tunisia
[b] Mathematics Department, computer science laboratory, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
[c] Lumina-The University of South-East Europe, IT&C Department, Bucharest 021187, Romania

ARTICLE INFO

Article history:
Received 26 April 2016
Received in revised form
9 June 2016
Accepted 21 July 2016

Keywords:
Cryptography
S-box
Chaos
Linear fractional transform
Partial encryption
Lifting-Wavelet Transform

ABSTRACT

In this paper, a new chaos-based partial image encryption scheme based on Substitution-boxes (S-box) constructed by chaotic system and Linear Fractional Transform (LFT) is proposed. It encrypts only the requisite parts of the sensitive information in Lifting-Wavelet Transform (LWT) frequency domain based on hybrid of chaotic maps and a new S-box. In the proposed encryption scheme, the characteristics of confusion and diffusion are accomplished in three phases: block permutation, substitution, and diffusion. Then, we used dynamic keys instead of fixed keys used in other approaches, to control the encryption process and make any attack impossible. The new S-box was constructed by mixing of chaotic map and LFT to insure the high confidentiality in the inner encryption of the proposed approach. In addition, the hybrid compound of S-box and chaotic systems strengthened the whole encryption performance and enlarged the key space required to resist the brute force attacks. Extensive experiments were conducted to evaluate the security and efficiency of the proposed approach. In comparison with previous schemes, the proposed cryptosystem scheme showed high performances and great potential for prominent prevalence in cryptographic applications.

1. Introduction

Recently, encryption of sensitive information has become a hot problem studied by many experts and researchers. With respect to the amount of encrypted data, the encryption can be divided into full encryption and partial encryption (also called selective encryption) according to the amount of the data encrypted [1–8]. Full encryption is mainly used for application areas that have requirements for high levels of security, such as privacy protection, secure communications, information security, and military applications. There are many different schemes for full encryption approaches for multimedia data, among which image scrambling which is to randomly change the positions of image pixels in spatial domain or frequency domain. Full encryption can also be achieved using different compression or encryption methods [3,5].

On the other hand, partial encryption can save the encryption time to meet the requirement of real-time applications since it can reduce the huge computation requirements for multimedia encryption [5,6,8,21–23,46]. Selective scrambling is one of the partial encryption schemes. Efficiently protecting copyright and encrypting color images or videos in real time applications are usually based on the principle of partial encryption (encrypting only a portion of the data). Partial encryption consists in encrypting information with different levels of security for different users according to their needs. Pay television is a good example of applications of partial encryption. The service providers want to show the customers what types of programs they are going to sell them. They partially encrypt their programs. Unauthorized customers who do not pay for the service can only watch the encrypted TV programs with a very low quality. Only a customer who purchased the programs can watch high quality unencrypted TV programs.

Over the last few years, thanks to chaotic systems which play a vital role in cryptography, chaotic maps have various ultimate features such as ergodicity and sensitivity to preliminary condition. They also exhibit random behavior, which can be applied to the field of cryptography [9,10]. The behavior of the system is predictable if the initial conditions are available to the observer, whereas in the absence of this knowledge, the system appears to be random [10]. The random behavior can be used to induce confusion and diffusion in the plaintext, thus enabling the data owner to safely transmit over insecure communication channels.

* Corresponding author.
E-mail address: belazi.akram@gmail.com (A. Belazi).

http://dx.doi.org/10.1016/j.optlaseng.2016.07.010
0143-8166/

Therefore, the use of chaos to enhance the strategy of novel cryptosystems is a standard indication. Additionally, substitution-boxes, or simply S-boxes, are used to increase confidentiality in substitution stage of some encryption approaches [11–13].

In the literature, several selective encryption schemes have been proposed. In what follows, we review most of them. Lian et al. suggested a JPEG2000 based image encryption scheme [5], which encrypts some wavelet coefficients selectively. Bhatnagar and Wu et al. [46] proposed a selective encryption scheme to scramble the pixel positions by means of Saw-Tooth space filling curve followed by the diffusion of interest pixels using non-linear chaotic map and singular value decomposition. An embedded partial encryption method of compressed color images based on chaos was presented in [22]. It presented an encryption method for encrypting only the significant bits obtained by Color-SPIHT (CSPIHT) compression algorithm. In [23], Reham et al. proposed a combined method of chaotic map and DNA complementary rules to generate key stream sequences used to encrypt the selected parts of images. Recently, Wen et al. [6] presented an infrared target-based selective encryption by chaotic maps. The previous works bring good contribution to selective encryption field; however, they are not enough to promote in potential image applications.

Based on the previous review and analysis, we propose an efficient partial encryption scheme, in which the permutation-substitution-diffusion (PSD) network was adapted firstly in the approximation coefficients based on lifting wavelet transform (LWT) domain. Here, LWT was applied to the original image in order to get the approximation coefficients (CA) to be encrypted by the block permutation based on chaotic tent map. Then, a new S-box method based on chaotic system and linear fractional transform (LFT) is presented to substitute the permuted image. This will increase the nonlinearity of the resulted image. Finally, a diffusion scheme based on chaotic logistic map is presented to enhance the security of the final encrypted image. Thorough cryptographic performance and security analysis ascertain the efficacy of the proposed encryption scheme.

The rest of this paper is organized as follows: Section 2 gives an account of the preliminary work for the proposed approaches. In Section 3, the proposed S-box is introduced. The proposed partial image encryption approach is given in Section 4. Section 5 is devoted to the experimental results and cryptographic analysis. Finally, Section 6 concludes the paper.

2. The preliminary work

2.1. Chaotic systems

The proposed cryptosystem approaches were constructed based on three of the most frequently used chaotic maps: the logistic map, the Chebyshev map, and the asymmetric tent map. The three chaotic maps are presented as follows:

2.1.1. Logistic map

The logistic map is a well-known 1D nonlinear chaotic map and is defined as:

$$y_{n+1} = \alpha\, y_n(1 - y_n) \tag{1}$$

where $\alpha \in [0, 4]$ is the control parameter and $y_0 \in [0, 1]$ is the initial condition. The logistic map shows good behavior and is frequently used in many applications [4,9]. The dynamics of the logistic map is validated using Hopf bifurcation diagrams. The logistic map is chaotic for $\alpha \in [3.57, 4]$ and slight variations of the initial value produce major differences in the random generated values, which are a non-periodic and non-converging sequence.

2.1.2. Chebyshev map

The Chebyshev map is a dynamical system defined as [14]:

$$y_{n+1} = \tau(y_n) = \cos(k.\arccos(y_n))n = 0, 1, 2, \ldots \tag{2}$$

Where $y_n = \tau^n(y_0)$, y_0 is an initial seed, and $k \in N$ denotes the degree of the Chebyshev map. When the seed $y_0 \in [0, 1]$ and $k > 1$, Eq. (2) is a nonlinear ergodic map.

The reason for choosing Chebyshev map is its simplicity and higher security level compared to some other chaotic systems.

2.1.3. The asymmetric tent map

The asymmetric tent map is one-dimensional dynamical system and is essentially a distorted version of the tent map. It is defined by Eq. (3):

$$z_{n+1} = \begin{cases} \dfrac{z_n}{\mu} & \text{if } 0 \le z_n < \mu \\ \dfrac{(1 - z_n)}{(1 - \mu)} & \text{if } \mu \le z_n \le 1 \end{cases} \tag{3}$$

where z_0 and $\mu \in [0, 1]$ are the initial condition and the control parameter, respectively. More details of this chaos map can be found in [15].

2.2. Lifting-Wavelet Transform

Introduced in 1998, by Sweldens [16], the Lifting-Wavelet Transform (LWT) represents a faster and more efficient (in terms of computational complexity) implementation of traditional wavelet transform. It is described as comprehensively possible (i.e., reasoning and proofs) in [16,17].

LWT's unique properties such as integer coefficients with error free quantization, resp, and time-frequency localization capability [18] have increased its usage in the field of image processing, e.g., [19,20]. Indeed, the reconstruction of LWT is an inverse process of decomposition.

The lifting scheme is composed of three phases: Split/Merge, Prediction and Update as shown in Fig. 1.

(1) Split/Merge (S/M): means split the input signals into odd (x_{odd}) and even (x_{even}) samples.
(2) Prediction (P): is used to keep the even samples changeless and use x_{odd} predicts x_{even} using the predict operator P[.].
(3) Update (U): is used to update the even samples based on the update operator U[.]

2.2.1. Superiority of LWT

LWT has several unique properties in comparison with the traditional wavelets [18]:

1. It can be calculated more efficiently and needs less memory space.
2. It is particularly easy to build non-linear wavelet transforms and

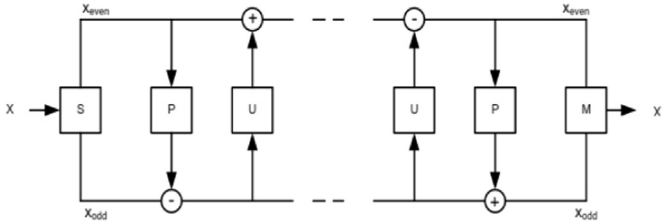

Fig. 1. An illustration of decomposition and reconstruction of lifting wavelet.