Signal Processing 128 (2016) 155–170

Contents lists available at ScienceDirect

Signal Processing

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

A novel image encryption scheme based on substitution-permutation network and chaos

Akram Belazi [a], Ahmed A. Abd El-Latif [b,*], 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

ARTICLE INFO

Article history:
Received 29 July 2015
Received in revised form
26 March 2016
Accepted 29 March 2016
Available online 6 April 2016

Keywords:
Image encryption
S-box
Permutation-substitution (SP) network
Chaotic systems

ABSTRACT

In this paper, a novel image encryption approach based on permutation-substitution (SP) network and chaotic systems is proposed. It consists of four cryptographic phases: diffusion, substitution, diffusion and permutation. Firstly, a diffusion phase is proposed based on new chaotic map. Then, a substitution phase based on strong S-boxes followed by a diffusion phase based on chaotic logistic map are presented which will, in turn, significantly increase the encryption performance. Finally, a block permutation phase is accomplished by a permutation function to enhance the statistical performance of the proposed encryption approach. Conducted experiments based on various types of differential and statistical analyses show that the proposed encryption approach has high security, sensitivity and speed compared to previous approaches

1. Introduction

1.1. Background

The close relationship between chaotic dynamical systems and cryptosystems has opened the door for several chaos-based cryptosystem schemes, especially image encryption. Indeed, chaotic system exhibits random behavior and has a lot of inherent features, such as unpredictability, ergodicity, and sensitivity to their parameter(s) and initial value(s), which make them a good candidate to design secure cryptosystems. 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. The random behavior can be used to induce confusion and diffusion in the plain image, thus enabling the data owner to safely transmit over insecure communication channel.

1.2. Review of the previous chaos-based encryption schemes

The literature is rich of chaos-based image encryption designs. In what follows, we review some of those relevant to the present work. Wang et al. proposed an image encryption for color images based on chaotic system [1]. Liu and Wang [2] proposed an encryption scheme for color images using spatial bit-level permutation and a high-dimension chaotic system. In [3] Liu et al. proposed an image encryption using Choquet fuzzy integral and hyper chaotic system for color images. Zhou et al. [4] proposed 1D chaotic map by coupling the tent and the sine maps, which is then adapted to encipher the plain image. In [5] Liu et al., proposed a chaos-based color image block encryption scheme using S-box. Ping et al. proposed an image encryption based on non-affine and balanced cellular automata [6]. Wang et al. [7] proposed a chaotic block image encryption algorithm based on dynamic random growth technique. An image encryption scheme based on 2D sine logistic modulation map was proposed by Hua et al. [8]. Liu and Wang [9] proposed a stream cipher scheme for color images based on one-time keys and piecewise linear chaotic map. Murillo-Escobar et al. proposed an image encryption scheme for color images in RGB format based on total plain image characteristics and chaos [10]. Chen et al. [11] proposed an encryption scheme with dynamic diffusion key stream obtained from the permutation matrix.

1.3. Limitations of encryption schemes

On the other hand, the cryptanalysts play a vital role in the cryptanalysis of encryption schemes and study the performance analysis [12–17]. Qualitatively speaking, the security of most designed chaos-based schemes is groundless and most of them are slow. This is due to the small key space, the considerable iteration steps to comply the encryption process (the tradeoff between security and the overall performance) and the inappropriate key streams generation for the internal structure of encryption/decryption, which helps the cryptanalysts to break the schemes. The need for new encryption schemes taking into account the

[*] Corresponding author.
E-mail address: ahmed_rahiem@yahoo.com (A.A. Abd El-Latif).

http://dx.doi.org/10.1016/j.sigpro.2016.03.021
0165-1684/© 2016 Elsevier B.V. All rights reserved.

performance analysis of previous approaches by the cryptanalysts is essential in image encryption applications.

1.4. Contribution and organization of this work

In this paper, we propose a new image encryption approach for secure digital images. It is composed of four cryptographic phases and uses two chaotic systems to control the structure of the encryption scheme so that it achieves high encryption performance. Firstly, a diffusion phase based on bitwise XOR operation and a new chaotic map is proposed. Then, a substitution phase based on strong S-boxes, proposed in [18], followed by a diffusion phase based on chaotic logistic map are introduced to enhance the encryption performance. Finally, a block permutation phase is accomplished by a permutation function, MAP function, to reinforce the statistical performance of the proposed encryption approach.

Conducted experiments based on differential and statistical analyses show that the proposed cryptosystem approach is efficient and has good cryptographic properties. The superior results of numerical analysis demonstrate that the proposed encryption scheme outperforms current image encryption schemes in terms of encryption performance.

The remainder of this paper is organized as follows: Section 2 gives, as a preliminary work, an overview of the chaotic maps used in the proposed cryptosystem scheme. In Section 3, we present the S-box used in this paper. Section 4 presents, as comprehensively as possible, the design of the cryptosystem approach. The experimental results and security analyses are reported in Section 5. The application of the proposed scheme for color images is presented in Section 6. Finally, Section 7 concludes the paper.

2. Chaotic maps

2.1. The logistic map

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

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

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 [19,20]. The dynamics of the logistic map is validated using Hopf bifurcation diagrams (Fig. 1) It is observed that the logistic map is chaotic for $\alpha \in [3.57, 4]$ and slight variations of the initial value produce major difference in the random generated values which are a non-periodic and non-converging sequence.

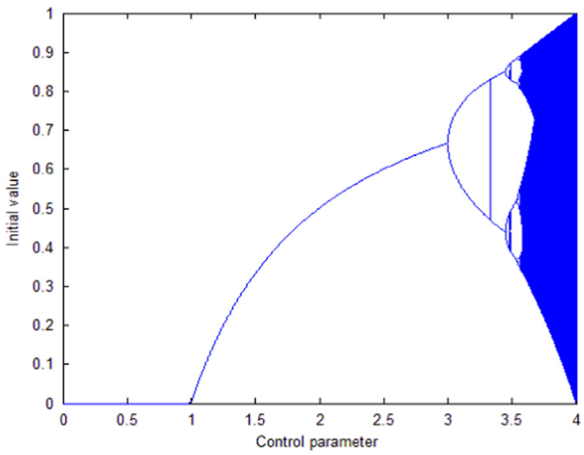

Fig. 1. Bifurcation diagram of the logistic map.

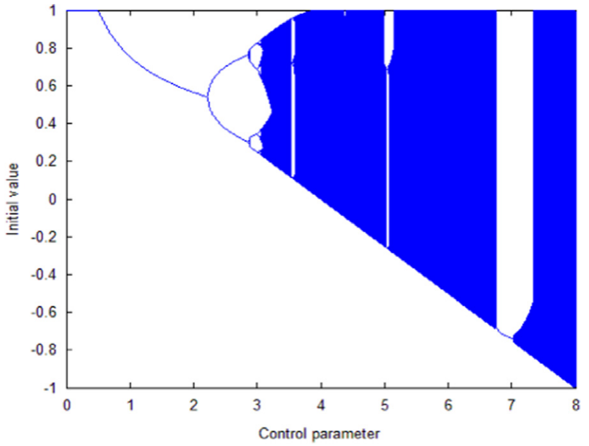

Fig. 2. Bifurcation diagram of the new chaotic map.

2.2. The new chaotic map [21]

The new chaotic map is defined as follows

$$x_{n+1} = \mu\left(x_n^4 - x_n^2\right) + 1 \tag{2}$$

where $\mu \in [3, 8]$ is the control parameter and $x_0 \in [0, 1]$ is the initial value. The hopf bifurcation diagram is shown in Fig. 2. The proof of chaos for the designed map can be found in [21].

2.3. Comparison between logistic map and the new map

In this section, we compare the dynamics analysis of the logistic map and the new chaotic map in terms of Lyapunov exponent and entropy.

2.3.1. Lyapunov exponent

The Lyapunov exponent or Lyapunov characteristic exponent of a dynamical system is a quantity that characterizes the rate of divergence of nearby trajectories. It is used to prove the chaotic behavior of chaotic maps. The Lyapunov exponent is calculated by the following equation:

$$\lambda = \lim_{N \to +\infty} \frac{1}{N} \sum_{n=1}^{N} \log\left|\frac{dx_{n+1}}{dx_n}\right| \tag{3}$$

The computation of Lyapunov exponent between the new map and the logistic map is shown in Tables 1 and 2. In addition, Fig. 3 shows the Lyapunov exponent of the logistic map and new chaotic map. Based on Tables 1 and 2, it is observed that the Lyapunov exponent of the new chaotic map is larger than famous logistic chaotic map.

Table 1
Lyapunov exponent values for logistic map for different pairs of initial conditions (IC) and control parameters (CP).

Pair (IC, PC)	Lyapunov exponent value
(0.3, 4)	0.693141
(0.4, 4)	0.693159
(0.6, 4)	0.693159
(0.7, 4)	0.69313
(0.3, 3.99998)	0.690930
(0.7, 3.99997)	0.690193