Optics and Lasers in Engineering 96 (2017) 39–49

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Image encryption based on new Beta chaotic maps

Rim Zahmoul*, Ridha Ejbali, Mourad Zaied

Research Team in Intelligent Machines, National School of Engineers of Gabes, B.P. W 6072 Gabes, Tunisia

ARTICLE INFO

Keywords:
Beta function
Beta chaotic maps
Image encryption

ABSTRACT

In this paper, we created new chaotic maps based on Beta function. The use of these maps is to generate chaotic sequences. Those sequences were used in the encryption scheme. The proposed process is divided into three stages: Permutation, Diffusion and Substitution. The generation of different pseudo random sequences was carried out to shuffle the position of the image pixels and to confuse the relationship between the encrypted the original image, so that significantly increasing the resistance to attacks. The acquired results of the different types of analysis indicate that the proposed method has high sensitivity and security compared to previous schemes.

1. Introduction

1.1. Research background

As a result of the advanced developments in communications and computer technologies, the Internet has become more and more used for the purpose of supporting client and server services. However, one of the major problems with data transmission over the network is the 'security'. Data security refers to the protection of the information from unauthorized users or attackers. Encryption forms an efficient methodology to make this data secure.

A cryptographic algorithm mechanism leads with the combination of a key a word, number, or expression to encrypt the original data. The identical plaintext encrypts to dissimilar cipher text with unlike keys. Due to its fundamental role in diverse applications, the security of images becomes an important topic for most image and data processing researchers.

Cryptographic algorithm is the mathematical function used for encrypting and decrypting process, this mechanism leads to encrypt the original data using different combination of a key a word, number, or expression. The encrypted data security is completely reliant on two important aspects; the key confidentiality and the cryptographic algorithm strength. A cryptosystem is designate due to the presence of cryptographic algorithm, along with all the working protocols and all potential keys.

Therefore, many encryption techniques have been proposed all over the years [1–10]. They chiefly incorporate optical encryption [1,2], blocks-based [3], permutation and shuffling encryption [4,5], public and secret key encryption [6,7], DNA and genetic encryption [8–10].

One of the most known encryption methods is the chaotic encryption [11]. Cryptography and chaos have some regular peculiarities, which is debated in consequent segment. Chaotic encryption illustrates the use of chaos hypothesis to accomplish diverse cryptographic tasks.

Many researches have used the logistic map [11] in the encryption process because its easier and more effective, but they realize that it has small key space and weak security. Due to its drawbacks [12], they try to create new chaotic maps [5,13] which have more security and better performances.

1.2. Previous research

The similarity between chaotic systems and cryptosystems has led to several chaos-based cryptosystem schemes in which researchers used different methods and features to obtain a secure encryption algorithm. In what follows, some of those works were reviewed. Belazi et al. [5]. proposed a novel image encryption method based on permutation-substitution (SP) network. Wang et al. [14] proposed a color image encryption approach based on chaotic system. Fouda et al. [3] presented a fast chaotic block cipher for image encryption in which they generated a chaotic sequence formed of integer numbers. Wang et al. [15] proposed a novel image encryption algorithm for chaotic block images, using the technique of dynamic random growth. Using chaotic map approach, Rathore et al. [16] presented a proficient image encryption method; they used the logistic map to generate pseudo random sequence which serves to the encryption cryptosystem in which they used Arnold cat map to scramble the positions of image pixels. Then, chaotic map is used to generate pseudorandom key generation. Hua et al. Alkher et al. introduced Securing Images Using Chaotic-based

* Corresponding author.
E-mail addresses: rima.zahmoul@gmail.com (R. Zahmoul), ridha_ejbali@ieee.org (R. Ejbali), mourad.zaied@ieee.org (M. Zaied).

http://dx.doi.org/10.1016/j.optlaseng.2017.04.009
Received 21 January 2017; Received in revised form 6 April 2017; Accepted 19 April 2017
Available online 28 April 2017

image for substitution [17]. Murillo-Escobar et al. presented an image encryption scheme, based chaos and plain image characteristics, for color images [18]. Chen et al. presented an encryption algorithm using a dynamic diffusion key stream generated from the permutation matrix [19]. Li et al. [20] proposed a new image encryption scheme based on hybrid cellular automata (CA) and depth-conversion integral imaging, which have better performances, trying to satisfy the needs of secure image transmission. Guesmi et al. proposed a color image encryption scheme based on chaos, crossover operator and the Secure Hash Algorithm (SHA-2) and used one-time keys [21].

1.3. Our contribution

To further increase the protection of the image encryption schemes based on chaos, we create new chaotic maps based on Beta function. Those created maps have plenty of advantages; like the large range of bifurcation parameter, the strong chaotic behavior, better pseudo random chaotic sequences, and the high number of parameters. We applied a several combinations of these maps in the proposed encryption process in order to generate chaotic pseudo random sequences. Those sequences were used in the key generation; they were used to shuffle the coordinates of the image pixels and to make a confusing relationship between the encrypted and the original image. Therefore, a high resistance against the attacks was noticed. The obtained results show that our method has the advantages of high security analysis.

The rest of the paper is structured as follow: a preliminary of three gives a description of our new created Beta maps. The fourth section presents in a summary manner the proposed encryption algorithm. In section five, we organized the obtained results. In the end, we conclude the proposed work.

2. Review of the most known chaotic maps

2.1. The logistic map

Proposed by Pierre Verhulst in 1845, the logistic map was one of the simplest and the most famous maps. It was defined by the following equation [22].

$$x_{n+1} = r x_n (1 - x_n) \tag{1}$$

The logistic map depends essentially on two parameters (x_0 and r), it has a random behavior, seems like an irregular jumble of dots, obtained by changing the value of one or both of these parameters. The main idea to create the logistic map was based on an iterations function, where the previous output $x_n - 1$ value influence the current one x_n.

Fig. 1 shows the Bifurcation diagram of logistic map.

The logistic map parameters x_0 (2) and r (3) represent the initial conditions.

$$x_0 \in [0, 1] \tag{2}$$

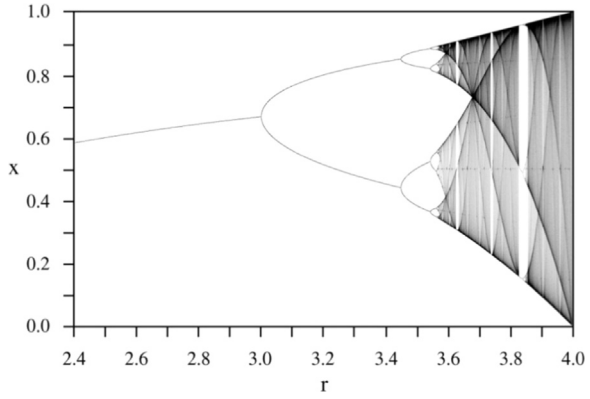

Fig. 1. Bifurcation diagram for the logistic map.

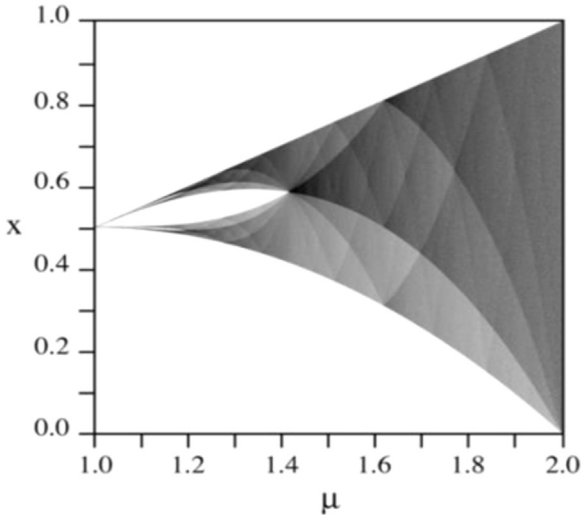

Fig. 2. Bifurcation diagram for the tent map.

and

$$r \in [0, 4] \tag{3}$$

After r exceeds 3.57,The chaotic behavior appears.

2.2. Tent map

A Tent map is defined by an iterated function associated to a dynamical system. It has a chaotic behavior and it is represented by the following equation.

$$T_\mu(x) = \begin{cases} \mu x, & x \le \frac{1}{2} \\ \mu(1 - x), & \frac{1}{2} < x \end{cases} \tag{4}$$

Its diagram is comparable to the logistic map's diagram, but with a corner [23]. It is shown in Fig. 2.

2.3. Piecewise linear chaotic maps (PWLCMs)

The PWLCMs are simple dynamical non-linear systems. Those maps have perfect behavior and high dynamical properties like the invariant distribution, ergodicity, auto-correlation function, mixing property and large positive Lyapunov exponent [24]. The generation of an orbit, which is a real numbers sequence between 0 and 1, was made by the iteration of the PWLCM with control parameters and initial value. It is also called skew tent map due to the similarity of its Eq. (5) with the Tent map's Eq. (4).

3. Our new created chaotic maps

3.1. Beta function

Inspired from the Beta function, which is often found in mathematical statistics and probability theory, we created our new chaotic maps. According to [25–27], the Beta function is defined as follow

$$Beta(x; p, q, x_1, x_2) = \begin{cases} \left(\frac{(x - x_1)}{(x_c - x_1)}\right)^p \left(\frac{(x_2 - x)}{(x_2 - x_c)}\right)^q & \text{if } x \in]x_1, x_2[\\ 0 & \text{else} \end{cases} \tag{5}$$

With p, q, x_1 and $x_2 \in R$, $x_1 < x_2$ and x_c:

$$x_c = \frac{(p x_2 + q x_1)}{(p + q)} \tag{6}$$

The divers shapes of Beta function were given in Fig. 3. We noticed that this function can take similar shapes to that of a trapezoidal,