Chaos, Solitons and Fractals 95 (2017) 92–101

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

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

Secure image encryption algorithm design using a novel chaos based S-Box

Ünal Çavuşoğlu[a,*], Sezgin Kaçar[b], Ihsan Pehlivan[b], Ahmet Zengin[a]

[a] Department of Computer Eng., Sakarya University, Sakarya, Turkey
[b] Department of Electrical and Electronics Eng., Sakarya University, Sakarya, Turkey

ARTICLE INFO

Article history:
Received 27 August 2016
Revised 2 December 2016
Accepted 15 December 2016

Keywords:
Image encryption
Chaos based S-BOX
Random number generator
Encryption analysis

ABSTRACT

In this study, an encryption algorithm that uses chaos based S-BOX is developed for secure and speed image encryption. First of all, a new chaotic system is developed for creating S-Box and image encryption algorithm. Chaos based random number generator is designed with the help of the new chaotic system. Then, NIST tests are run on generated random numbers to verify randomness. A new S-Box design algorithm is developed to create the chaos based S-Box to be utilized in encryption algorithm and performance tests are made. As the next step, the new developed S-Box based image encryption algorithm is introduced in detail. Finally, image encryption application is carried out. To show the quality and strong of the encryption process, security analysis are performed. Proposed algorithm is compared with the AES and chaos algorithms. According to tests results, the proposed image encryption algorithm is secure and speed for image encryption application.

© 2016 Elsevier Ltd. All rights reserved.

1. Introduction

Recent years have seen tremendous improvements in image processing and network communication technologies. Maintenance of security in both wired and wireless communication have become of great significance in real time data transfer. Multimedia and visual content has come to be very commonly used in many fields like sharing military, medical personal information. Previously, classical encryption algorithms are tried for image encryption yet these algorithms are able to offer poor performance in encryption of big sized images [1,2]. That is why studies on developing different methods for image encryption have been initiated. One of these fields is chaos based encryption studies.

A close connection between chaotic systems and cryptology have been observed [3,4]. Chaotic systems have certain features like randomness, ergodicity, sensitive dependence to control and initial parameters which meet the fundamental requirements of cryptology. These values generated by chaotic systems are deterministic but highly unpredictable provides an immense advantage for encryption systems [5,6]. New chaos based encryption studies have been carried out with the help of these features [7,8]. Random number generators are used to generate random number series for encryption. The more random the generated numbers are, the better the encryption becomes. Chaos based random number generator designs are one of the common fields where chaotic systems are used for encryption [9,10].

S-Box, which performs confusion, is one of the most important parts used in block encryption algorithms. Therefore, using a strong S-Box structure helps to have a secure encryption. S-Box structures to be used in encryption must be resistant to attacks, have high cryptographic features and be resistant to differential cryptanalysis. Over the last few years, numerous encryption studies have been conducted using chaos based systems. Wang et al. [11] proposed a new chaos based encryption algorithm. An architecture to provide features of confusion and diffusion is presented in the study. In their study, Hassan et al. [12] designed a chaos based encryption algorithm to realize a secure and fast encryption. The comparison with AES algorithm proved that the chaos based system has a higher level of security and a lower calculation load. Chen et al. [13], in their article, developed an asymmetric encryption algorithm to carry out an image encryption with 3-dimensional chaotic map. Liu et al. [14] made use of Chen chaotic map and proposed a chaos based image encryption algorithm. Ginting and Dillak [15] designed a hybrid encryption algorithm which employs RC4 encryption algorithm and logistic chaotic map for encryption of digital images. Bakhache et al. [16], Liu et al. [17] proposed a new chaotic encryption algorithm. Çavuşoğlu et al. [18] performed a chaos based application to be used on TCP protocol. Alireza and Mirghadri [19], in their study, designed an image

* Corresponding author.
E-mail address: unalc@sakarya.edu.tr (Ü. Çavuşoğlu).
URL: http://www.sakarya.edu.tr (Ü. Çavuşoğlu)

http://dx.doi.org/10.1016/j.chaos.2016.12.018
0960-0779/© 2016 Elsevier Ltd. All rights reserved.

encryption algorithm utilizing baker's chaotic map and S-AES block encryption algorithm. The literature has numerous S-Box design algorithms which have been developed with the help of chaotic systems as well as different methods. Jakimoski et al. [4] designed an S-Box design algorithm and a block encryption algorithm in which logistic map chaotic map is used and made its cryptanalysis. Tang et al. [20,21] proposed a method to produce chaos based S-Box to be used in block encryption algorithms like DES, AES, IDEA and so on. Utilizing different approaches, Ozkaynak et al. [22] and Wang et al. [23,24] created S-Box designs.

In image encryption, complex structures of modern encryption algorithms that require high processing power have negative influence on performance of encryption processes. In addition, processing sources are limited and employing them in real time environments cause disadvantages. Chaotic system based encryption studies are very common in the literature but it is observable that the encryption studies in which only chaotic systems are used bear some weaknesses [25,26]. An encryption algorithm to overcome such weaknesses using chaos based S-BOX and has low process load and high level of security is designed. Examining the chaos based S-BOX design algorithms in the literature, one can see that they include mathematically complex row column transform processes. To create S-Box structures used in block encryption algorithms, on the other hand, operations that require so much load are carried out.

This study aims to develop a high security and effective image encryption algorithm via simple operations and low process load, with the help of randomness and high dynamic features of chaotic systems, in which S-Box structures are used. For the design of the encryption algorithm, firstly the new chaotic system with high dynamic features and wide key space are developed and the new chaos based RNG is designed and random numbers are generated. NIST randomness tests are run on random bit series. S-BOX generation algorithm, which is supposed to produce the S-BOX to be used in encryption, is designed and then nonlinearity, bit independence criteria (BIC), Strict avalanche criteria (SAC) and Differential approximation probability (DP) performance tests for this S-BOX are done. The encryption algorithm designed here is made cryptologically stronger thanks to the use of S-Box structure. Image encryption application is also carried out with the new proposed, AES and chaos algorithm for comparison results. The encrypted images are put to histogram, correlation, Information Entropy, Liner and Differential attack (NPCR-UACI), Encryption Quality, key length and sensitivity, encryption-decryption time analysis to obtain security and performance level. Experimental results and relative analysis show that the proposed method is secure and efficient for image encryption.

Following the introduction section of the study, the new chaotic system design and its dynamical analysis; the third section contains chaos based RNG design and NIST tests. The fourth section covers the new chaos based S-Box generation algorithm and S-Box performance analysis. The fifth section presents image encryption algorithm design and sixth section covers an image encryption application and security analysis and the last section includes the results and future works.

2. The new chaotic system and its dynamical analysis

In this part, chaotic system to be used in random number generator is introduced and analyses of the chaotic system are made. Once it is observed that the chaotic system has sufficient dynamic features, random number generator is designed. NIST tests are run on random numbers from random number generator. The new chaotic system to be used in RNG design is designed. The fact that the chaotic system has high dynamic features is of great significance in terms of randomness of the numbers to be generated. Eq. (1) shows the equation of the new chaotic system employed in encryption algorithm.

$$\begin{aligned} \dot{x} &= cy - x - bz \\ \dot{y} &= axz - xy - bx \\ \dot{z} &= dxy + b \end{aligned} \tag{1}$$

The value of system parameters: a=1, b=1, c=2, d= −3.

The values of initial conditions: $x_0 = 1,\ y_0 = -1\ ,\ z_0 = 0,01$.

Equilibrium points belonging to the new chaotic system to be used in encryption are calculated. As a result of the chaotic systems equilibrium points analysis; E_1, E_2 equilibrium points are derived given below.

$$\begin{aligned} E_1 &= (0.263763, 1.263763, 2.263763) \\ E_2 &= (-1.263763, -0.263763, 0.736238) \end{aligned} \tag{2}$$

where system parameters are a=1, b=1, c=2, d= −3.

Fig. 1 shows x-y, x-z and y-z phase portrait outputs of the new chaotic system. Time series and key sensitivity graph are seen on Fig. 2. A tiny change in the initial conditions of the system leads to huge changes in the outputs of chaotic system. As can be seen on Fig. 2. 'x' initial condition is assumed '1' and the red curve is found. Then, x is changed by 1/10000, made '0.0001' in other words, and the blue curve is found. An examination of the graph for both values reveals that a small change in the parameter brings about a change in chaotic system output.

Fig. 3 shows the graph of Lyapunov exponents spectrum acquired by changing the 'b' parameter of the new chaotic system between 0 and +3. Lyapunov exponents must be (−, 0, +) for a 3 dimensional chaotic system. In other cases, the system exits chaos. The system has positive Lyapunov exponent at certain intervals and shows chaotic behavior. Fig. 3 exhibits that the new chaotic system has chaotic behaviour feature between values of 0.5 and 2.5. Fig. 4 shows the bifurcation diagram of b parameter between values of 0–3 and the analysis. An examination of Fig. 3 and 4 together proved the existence of chaotic behaviour feature among the same values.

3. RNG design and NIST tests

Chaotic systems are commonly used in random number generator designs. Chaotic systems have features of being random but deterministic. Making use of such features, random number generators that are strong in cryptological terms can be designed. In chaos based random number generator design, sensitive bits of float numbers generated by chaotic system are used and bit series with high randomness are found. RNG design algorithm pseudo code utilized for generation of random bit series is seen on Algorithm 1. After system parameters and initial conditions are entered to chaotic system, appropriate sampling step value is found as 0.0001. Algorithm works up to this value for the generation of 1 million bit which is necessary for NIST tests [27]. Chaotic system is decrypted with RK-4 numerical analysis method and the chosen sampling value is used and float values are taken from time series. The picked float value is transformed to binary (32 bit) value. Following this, an appropriate number of bits are chosen from the sensitive part with the smallest value from 32 bit and they are added to 1 million bit series. After 1 million bit series is formed, it is put through NIST tests. If the series passes all tests, it becomes evident that the system can generate random number series that can be used in encryption cryptologically. Provided that the generated random bit series fails in tests, previous steps are repeated and some changes are made on sampling value or the chosen bits

Download English Version:

https://daneshyari.com/en/article/5499857

Download Persian Version:

https://daneshyari.com/article/5499857

Daneshyari.com