Commun Nonlinear Sci Numer Simulat 19 (2014) 3106–3118

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

Chaotic substitution for highly autocorrelated data in encryption algorithm

Amir Anees [a,*], Adil Masood Siddiqui [b], Fawad Ahmed [a]

[a] Department of Electrical Engineering, HITEC University, Taxila, Pakistan
[b] Department of Electrical Engineering, Military College of Signals, National University of Science and Technology, Rawalpindi, Pakistan

ARTICLE INFO

Article history:
Received 3 January 2013
Received in revised form 5 February 2014
Accepted 10 February 2014
Available online 20 February 2014

Keywords:
Substitution box (S-box)
Chaos
Encryption

ABSTRACT

This paper addresses the major drawback of substitution-box in highly auto-correlated data and proposes a novel chaotic substitution technique for encryption algorithm to sort the problem. Simulation results reveal that the overall strength of the proposed technique for encryption is much stronger than most of the existing encryption techniques. Furthermore, few statistical security analyses have also been done to show the strength of anticipated algorithm.

1. Introduction

Substitution boxes (S-boxes) are the vector Boolean functions used commonly in cryptographic applications. A function of the form $S : GF(2)^n \rightarrow GF(2)^m$ is called an $n \times m$ S-box which takes n bits as the input and gives m bits as the output. If each output bit is called the n-variable Boolean function f_i, then $S(x) = (f_1(x), \ldots, f_m(x))$, where $xGF(2)^n$ [1]. S-box is the only non-linear part of the block cipher and is a source to create confusion. There are many S-box construction methods available in the literature [2–5]. In cryptographic applications, the performance of different S-boxes can vary from one another and depends upon nature of data and their application. A major performing criterion of the S-box in encryption techniques is its non-linearity. A foremost research development in the past few years for the construction of S-boxes has been done mainly to increase the non-linearity of these S-boxes [6–8]. However, in case of highly auto-correlated message data, the S-box exhibits poor substitution results despite its high non-linearity.

Chaotic dynamics are the behavior exhibit by some nonlinear dynamical system and can be used as a source of diffusion in substitution techniques. It has been observed by many researchers that there exists the close relationship between chaos and cryptography; many properties of chaotic systems have their corresponding in traditional cryptosystems. Chaotic systems have several compelling features favorable to secure communications, such as sensitivity to initial condition, ergodicity, control parameters and random like behavior, which can be correlated with some conventional cryptographic properties of good ciphers, such as confusion and diffusion proposed by Shanon. In the proposed substitution algorithm, chaos is being used with the S-box to strengthen the projected algorithm via applying the Shannon idea of sequential application by combining the confusion and diffusion properties.

Most of the number theory or algebraic concepts based traditional ciphers such as Advanced Encryption Standard (AES), Data Encryption Standard (DES) and so on not appear to be ideal for multimedia applications due to certain and justified

* Corresponding author. Tel.: +92 3435859172.
E-mail addresses: amiranees@yahoo.com (A. Anees), dradil@mcs.edu.pk (A.M. Siddiqui), fawad@hitecuni.edu.pk (F. Ahmed).

http://dx.doi.org/10.1016/j.cnsns.2014.02.011
1007-5704/

reasons described in [9]. In modern years, chaotic encryption technology has been developed rapidly and has commended several advantages over the traditional encryption algorithms such as speed, high security, reasonable computational overheads and computational power. Chaotic encryption makes use of chaotic system properties such as loss of information and sensitive to initial conditions that makes it less vulnerable to security attacks. According to the classification of chaotic systems, the chaotic encryption schemes, which have been proposed, can be divided into analog chaotic cryptosystems utilizing continuous dynamical systems [10] and digital chaotic cryptosystems utilizing discrete dynamical systems [11]. In 1997, a new chaos-based secure communication scheme was proposed by Tao Yang, Chai Wu and Leon O. Chua [12] to encounter the attacks proposed recently. In 2003, Zhang Han et al. [13] proposed a new image chaotic encryption algorithm based on two dimensional chaotic map. The presented technique deals the problem of self-similarity and visional physiological characteristic of image existed in previous traditional encryption techniques. The performance analyses of cryptosystems based on chaotic dynamical systems were done by G. Alvarez et al. [14] to show the strength of chaotic encryption systems. V. Guglielmi et al. [15] also presented the security analyses of a chaotic cryptosystem implemented on DSP in 2004. The hardware realization of chaotic cryptographic system with minimum complexity and fast throughput is presented by H. S. Kwok and Wallace K. S. Tang [16] in 2005. Although there has been exceptional growth in chaotic cryptography in last two decades but at the same time this leads to the publication of those chaotic cryptographic papers which shows certain flaws.

2. Problem statement

The S-box mapping for digital data is shown in Fig. 1. It is a bijective mapping relation which holds one to one and onto relations, in which a message symbol is replaced with only one unique symbol/element of S-box. Substitution-box can be thought of as a bijective function, $f(x)$ such that,

$$S : GF(2)^n \rightarrow GF(2)^m \tag{1}$$

$$\text{if } x_1 = x_2 \tag{2}$$

$$\text{then } f(x_1) = f(x_2) \tag{3}$$

Two different symbols of message neither can be replaced with single element of S-box, nor can the two elements of S-box take place of single message symbol. If the same symbols of the message come, they are all replaced with single S-box element. So the histogram peaks remain the same in both message and encrypted data; only their distribution will be interchanged.

The traditional S-box substitution algorithm for digital 2-dimensional (gray scale) image is described in Fig. 2. The substitution function is based upon one to one and onto relation (bijective), i.e. an image pixel is encrypted with only one element of S-box. If same pixels of an image exist, they are all encrypted with one unique element of S-box. So, if there is a region/portion which has pixels with the same value (perfect correlation with itself) then whole portion will be replaced with another portion having same value pixels. The eavesdropper can then deduce information about the message image from the encrypted image.

This effect can be seen in the Figs. 3–6 for 256, 128, 64 and 2 (binary) gray scales images, respectively. In Fig. 3, there are few patterns in substituted image which resemble with the message image due to the same problem discussed earlier. Figs. 4

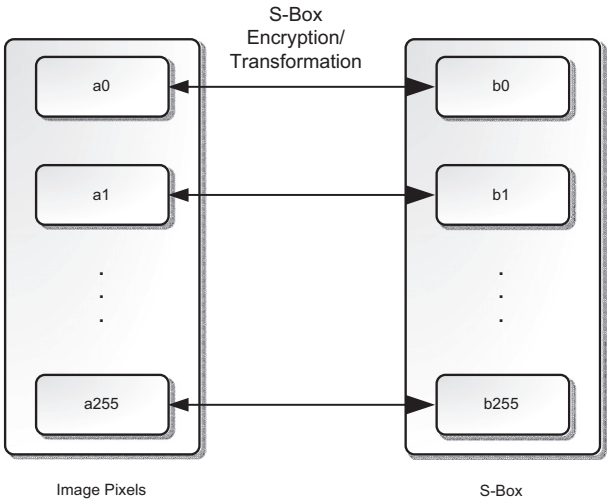

Fig. 1. S-box bijective (one to one and onto) substitution function.