International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:6, No:7, 2012

Digital Image Encryption Scheme using Chaotic Sequences with a Nonlinear Function

H. Ogras, M. Turk

***Abstract*—**In this study, a system of encryption based on chaotic sequences is described. The system is used for encrypting digital image data for the purpose of secure image transmission. An image secure communication scheme based on Logistic map chaotic sequences with a nonlinear function is proposed in this paper.

Encryption and decryption keys are obtained by one-dimensional Logistic map that generates secret key for the input of the nonlinear function. Receiver can recover the information using the received signal and identical key sequences through the inverse system technique. The results of computer simulations indicate that the transmitted source image can be correctly and reliably recovered by using proposed scheme even under the noisy channel. The performance of the system will be discussed through evaluating the quality of recovered image with and without channel noise.

***Keywords*—**Digital image**,** Image encryption, Secure communication

I. Introduction

The study of chaotic dynamics in deterministic systems has become very popular in the past few decades, emerging from the study of non-linear dynamics. Deterministic dynamical system can exhibit different steady-state behaviors including DC, periodic and chaotic. DC is a non-oscillatory state and periodic behavior is the simplest type of steady-state oscillatory motion. Sinusoidal signals, which are used as carriers for conventional communication systems, are periodic solutions of the continuous time deterministic dynamical systems [1]. These systems also admit complex behavior, non-periodic and characterized by random-like in time domain and appear wide noise-like power spectra in frequency domain; this is chaotic state.

In recent years, digital communication techniques based on chaotic systems gains more and more concern on its research and application in the communication areas with the increasing development of nonlinear systems [2]. It is well known that chaotic signals are random-like, aperiodic, broadband and having low power spectrum density. These are major properties that coincide with requirements for signals applied in secure communication systems which provide robustness in multipath environment, ease of spectrum spreading, added security etc.

Chaos is one type of complex dynamic behaviors generated by deterministic nonlinear dynamical systems and widely used in image encryption systems motivated by the chaotic properties such as non-periodic, extreme sensitivity to initial conditions, system parameters etc [3,4]. The chaos-based encryption was first proposed in 1989. Since then, researches have proposed a lot of encryption algorithms based on chaotic system [5].

Chaotic map with some dynamics of its own characteristics and high sensitivity to the initial condition and parameters are very suitable for constructing encryption algorithms. Chaotic encryption algorithm has advantages of a large space, simple implement, robustness and faster encryption over the traditional method [6]. A cryptosystem is one of the basic approaches that has been proposed to enhance the safety of chaotic communication systems [7]. A cryptosystem is simply a cipher algorithm that converts the original message into apparently random non-sense message.

In this paper, a stream cipher algorithm where the message is encrypted bit-by-bit with the application of a secret key generator is used. Decryption process will be achieved by using the same algorithm as in encryption and with the same secret key generator. The proposed encryption scheme includes one-dimensional Logistic map and a nonlinear function. Logistic system has an iterative equation that uses chaotic iteration to generate secret key.

The rest of this paper is organized as follows. Section II presents the proposed encryption scheme through the combination of discrete time chaotic map and nonlinear function. Section III describes computer-based simulation results with discussions of security analyses. Finally, some conclusions will be given in Section IV.

II. Description of The Image Encryption Algorithm

An encryption algorithm can be regarded as a mathematical transformation and generates ciphered message. At the receiving end, the ciphered message is decrypted by a decryption module which essentially applies an inverse transformation.

The encryption algorithm employs one-dimensional Logistic map which is a simple but very popular system having only one degree of *x* and one system parameter *r* and defined as

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

Here, $0 \le r \le 4$ is bifurcation parameter and $x_n \in (0,1)$. If $3.57 \le r \le 4$ then Logistic map is in the state of chaos. In this paper, we use discrete-time Logistic map as a key generator due to the having simple structure and one kind of easy chaotic system that can be modeled in computer environment. The behaviors of Logistic map according to *r*, can be observed from the bifurcation diagram shown in Fig. 1.

Hidayet Ogras is with Batman University, Turkey e-mail:hidayet.ogras@batman.edu.tr

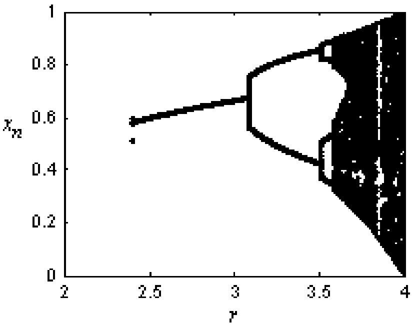

Fig. 1 Bifurcation diagram

We also use a nonlinear function in order to improve the security of the encryption algorithm. The nonlinear function has two inputs of image data in the form of binary and key sequences generated by Logistic map. It is defined as

$$f(x,m)=\frac{(x+a)^3+x^2(1-m)+xm}{b} \tag{2}$$

where *a* and *b* are constants of the nonlinear functions. Chaotic key sequence is denoted as *x* and *m* shows the image data as binary form which refers 0 or 1. When *a*=0.8 and *b*=7 are selected as the parameters of the nonlinear function, $f(x)$ maps the area of [0,1] to ensure that the next iterative point is located in chaotic area. So, the $f(x)$ will be

$$f(x,m)=\frac{(x+0.8)^3+x^2(1-m)+xm}{7} \tag{3}$$

Before the encryption process, image source is converted to serial binary codes in Matlab environment. Therefore, the transmitted signal $s(x)$, according to the $f(x)$, will be given by,

$$s(x)=\begin{cases}\dfrac{(x+0.8)^3+x}{7} & when\ bit\ '1'\ is\ transmitted\\ \dfrac{(x+0.8)^3+x^2}{7} & when\ bit\ '0'\ is\ transmitted\end{cases} \tag{4}$$

The algorithm uses chaotic iteration to generate the secret key. General structure of the proposed encryption scheme is shown in Fig. 2.

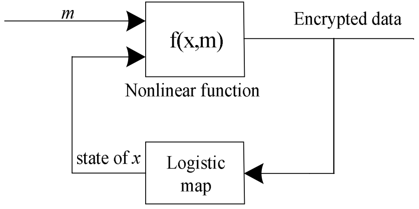

Fig. 2 Block diagram of encryption scheme

After the encryption process of the proposed scheme, a part of the encrypted information with respect to the some bits of the source image is shown in Fig. 3.

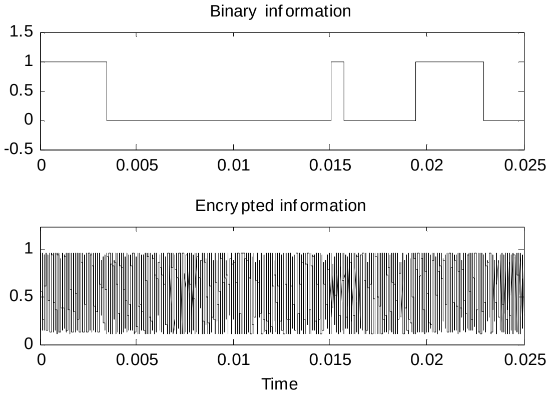

Fig. 3 Binary and Encrypted information

The encryption algorithm should use a map with multi-parameter and a wide range and increase the number of parameters in order to enhance the security of the system for the exhaustion attack. In this situation, the parameters of the $f(x)$ can also be considered as secret key for the proposed encryption algorithm.

The nonlinear function, which is used as a mathematical transformation, is selected as the output of the function will not diverge during the encryption process so as the transmitted signal. Furthermore, using this function helps the whole system for becoming more complex structure because of utilizing additional possibility for the secret keys.

Receiver can recover the information according to the received signal and identical key sequences by using inverse system technique. Identical key sequences are generated by the same logistic map in the receiver side. Decryption algorithm scheme in receiver side is shown in Fig. 4.

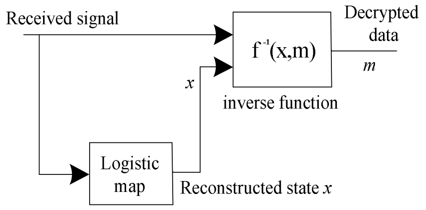

Fig. 4 Block diagram of decryption scheme

The important feature of this scheme is that transmitted signal contains self-synchronization and does not require additional synchronization.

III. The Results And Analysis Of The Simulations

As a binary source, Lena image of 256x256 is used in our computer-based simulations. First of all, Lena image is converted to a binary image by thresholding of 0.5 as shown in Fig. 5 with its histogram.

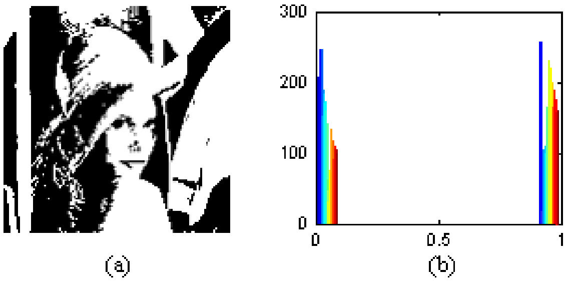

Fig. 5 Binary image and its histogram

Then, the image is encrypted by using the proposed algorithm with r=4. The encrypted image and its histogram are shown in Fig. 6.

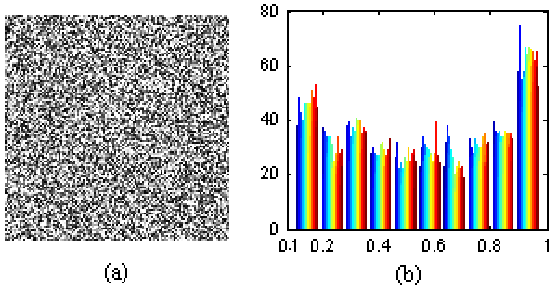

Fig. 6 Encrypted image and its histogram

The encoded message has a very good statistical characteristic, where the pixels of the digital image are changed and uniformly scrambled as shown in its histogram.

The recovered image is analyzed and observed under the different conditions such as distinct channel noise effects in signal to noise ratio (SNR) mode, bifurcation parameter which shows the behavior of the key generator system and also the parameters of the nonlinear function.

Fig.7 shows encrypted image and decrypted image under the situation of noise free.

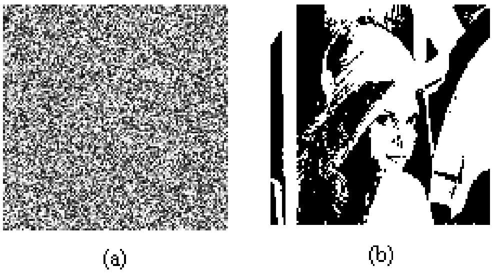

Fig. 7 Encrypted image and decrypted image

When the dynamic behavior of the Logistic map changes by the different value of *r*, the encryption algorithm also changes because the key sequence, *x* depends on the bifurcation parameter *r* of the system. Encrypted and recovered images with different *r* parameters of the system are shown in Fig. 8.

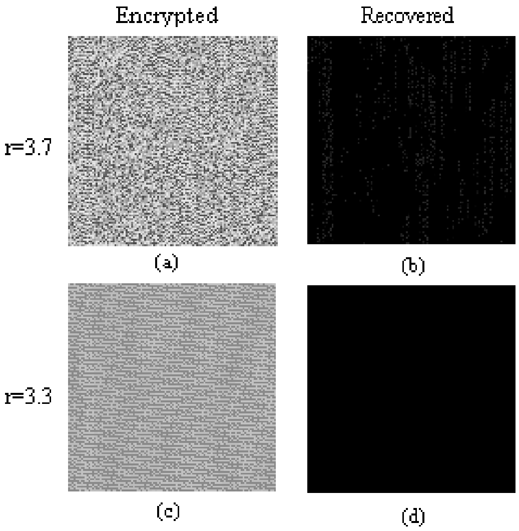

Fig. 8 Encrypted and Recovered images with different *r*

In transmitter side, if the parameter of *r* is changed to a different value, for instance r=3.7, then the recovered image is not decrypted correctly when it is compared to original image, even the state is still in chaotic region. Fig. 9 shows that the histograms of the encrypted images are completely different when the different *r* values are used for the encryption. When r=3.3 is selected, then the Logistic map is in state of periodic.

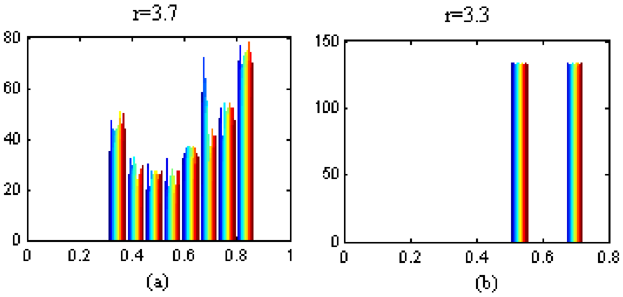

Fig. 9 Histograms of encrypted images when r=3.7 and r=3.3

The parameter of *r* can be considered as a key for decryption process. The image can not be fully decrypted unless the r values for both transmitter and receiver systems are same.

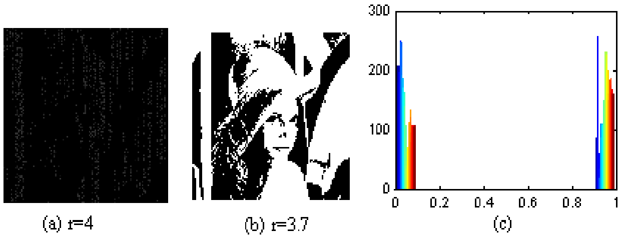

Fig. 10 Decrypted images when receiver has different *r* values

The recovered images are shown in Fig. 10, when the receiver system has r=4 and r=3.7 respectively, while transmitter has r=3.7.

The performance of the system is discussed through evaluating the quality of decrypted image under AWGN channel. Recovered images are shown in Fig. 11 under the different values of SNR.

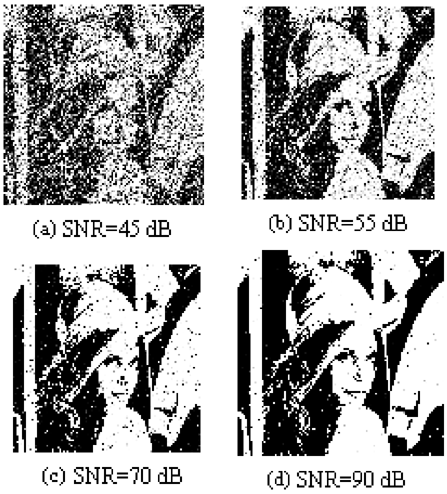

Fig. 11 Recovered images under the different SNR

The quality of the recovered images under AWGN channel depends on the signal to noise ratio in the transmission channel. However, the proposed scheme is not resistant to noise enough due to the synchronization error will propagate in a low-SNR channel as expected.

Decryption algorithm is also sensitive for the parameters of the nonlinear function. If there is a change for the both parameters *a* and *b,* then the original image will not recovered as shown in Fig. 12.

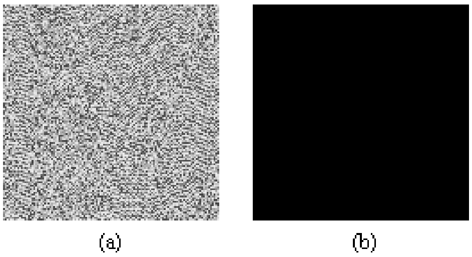

Fig. 12 a) Encrypted image when a=0.7 b) Decryption result

IV. Conclusion

In this paper, an encryption algorithm based on chaotic sequences is proposed for the system having ability to encrypt digital image for secure image transmission. The results of computer simulations indicate that the transmitted source image can be correctly and reliably recovered using proposed scheme.

The proposed encryption scheme can be applied and improved by using other chaotic maps. It can be developed with hyper-chaos based algorithm or any discrete-time chaotic map having more than one dimensional in order to improve security of the system.

The performances of the encryption and decryption process also depend on the dynamic behavior of the chaotic map. Then the sensitivity is compared with respect to arbitrary parameters of the nonlinear function in order to evaluate the system performance. It is observed that decryption algorithm is sensitive to the bifurcation parameter of the Logistic map as well as parameters of the nonlinear function.

As a result, this scheme can be particularly suitable for real time applications with digital hardware and attractive since it provides simple implement, fast image encryption and secure communication.

References

[1] M. P. Kennedy, and G. Kolumban, “Digital communications using chaos,” *Signal processing,* vol. 80, no. 7, pp. 1307-1320, July 2000.

[2] Xunzhang, L. Ying, L. Sun, and Z. Li, “Research on new implementation method of chaotic model based on FPGA,” *ASIC 7th International conference,* pp. 241-244, Oct. 2007.

[3] P. Ying, and L. Min, H. “A color image encryption algorithm based generalized chaos synchronization for bidirectional discrete systems for audio signal communication,” *International Conference on intelligent control and information processing,* pp. 443-447, August 2010.

[4] W. Wei, L. Fen-Lin, G. Xinl, and Y. Yebin, “Color image encryption algorithm based on hyper chaos,” *Information management and engineering, 2010 the 2nd IEEE Int. Conference,* pp. 271-274, April 2010.

[5] T. Gao, Q. Gu, Z. Chen, and R. Cheng, “An improved image encryption algorithm based on hyper-chaos,” *Innovative computing, Information and control 2009 Fourth Int. Conference,* pp. 1281-1284, Dec. 2009.

[6] Z. Yun-peng, L. Wei, C. Shui-ping, Z. Zheng-jun, N. Xuan, and D. Wei-di, “Digital image encryption algorithm based on chaos and improved DES,” *Systems, Man and Cybernetics, 2009 IEEE Int. Conference,* pp. 474-479, Oct. 2009.

[7] T. Chien, and T. Liao, “Design of secure communication systems using chaotic modulation, cryptography and chaotic synchronization,” Chaos, Solitons and Fractals, vol. 24, no. 1, pp. 241-255, 2005.