International Conference on Automation, Control, Engineering and Computer Science (ACECS'14)
Proceedings - Copyright IPCO-2014, pp.192-104
ISSN 2356-5608

A Chaotic secure communication scheme using Time delay Chua's circuit: application to digital Image Encryption

Trabelsi Karim[1] and Belghith Safya[2]

Ecole Nationale d'Ingénieurs de Tunis/Laboratoire 6'com, université Tunis El Manar
1002 Tunis , Tunisia
Trabelsi Karim, karim_enit@yahoo.fr

ABSTRACT

In the past few years, a number of image cryptosystems have been proposed; however, many of them have been shown to be insecure. In this paper we present a robust and efficient cryptosystem based on the synchronization of a chaotic time delay system to transmit a digital image in a secure way. The transmitter module consists of a chaotic generator which is the time delay feedback Chua circuit and an encryption mechanism (chaotic masking), in which the secret spreading message (digital image) is added to the output of the chaotic generator. The receiver module consists of a non linear state observer design, driven by only one of the states of the time delay feedback Chua circuit; and a decryption mechanism. A secure analysis proves that this cryptosystem is robust to some best-known attacks; this efficiency relies to the properties of the chosen chaotic generator and the efficiency of the nonlinear observer.

Keywords: Cryptosystem, Chaos, Time delay Chua Circuit

INTRODUCTION

The security of digital images has become increasingly more important in today's highly computerized and interconnected world. The media content must be protected in applications such as confidential video conferencing, medical imaging, and in industrial or military imaging systems. Image encryption is somehow different from text encryption due to some inherent features of image, such as bulk data capacity and high correlation among pixels. Therefore, traditional cryptographic techniques such as DES, AES and RSA are no longer suitable for practical image encryption, especially for an online communication scenario [1-2]. In order to overcame this problem, many fast encryption algorithms specially designed for digital images have been proposed such as selective encryption (or partial encryption)[5]. However, many works have been presented some limitations of this type of algorithms, such as [4].

On the other hand, since 1990s, many researchers have noticed that there exists an interesting relationship between chaos and cryptography [6], as a result of investigating this above relationship, a rich variety of chaos-based cryptosystems for end-to- end communications have been put forward [7-12]. There exist two main approaches of designing chaos-based cryptosystems: analog and digital. In this paper, only the analog chaotic cryptosystem is taken into consideration.

These types of cryptosystems rely on synchronization approach of chaotic systems. The basic idea of these cryptosystems is based on using a chaotic nonlinear oscillator as a broad band pseudo-random signal generator. This signal is combined with the message using an encryption mechanism to produce an unintelligible signal, which is transmitted through the communication channel. At the reception side, ones synchronization is achieved, the pseudo-random signal is regenerated, so that by combining it with the received signal the original message will be recovered [7, 8, 10].

Though a large number of chaos-based cryptosystems have been proposed, many of them were not designed in a secure way and have been found insecure. In fact, it has been noticed that a systematic approach to the design and security evaluation of chaos-based cryptosystems is lacking.

In this work, we propose a robust and efficient cryptosystem based on the chaotic time delay feedback Chua circuit to transmit a digital image in a secure way. It consists of two steps: the first one assures the transmitter/receiver synchronization while the second step focuses on the encryption/decryption procedure. The synchronization is performed through a non linear state observer design, driven by the transmitted signal, and the encryption/decryption procedure is ensured by using the chaotic masking method [7,8].

The rest of the paper is organized as follows. In Section 2, we describe the characteristics of chaotic generator. The Section 3 is devoted to the observer design used in the receiver module. The proposed cryptosystem, the transmission and the recovery of the digital image are presented in section 4. In section 5 the security of the proposed scheme is analyzed. Finally, Section 6 concludes the paper.

CHAOTIC GENERATOR: TIME DELAY FEEDBACK CHUA CIRCUIT

Electrical scheme and mathematical model:

The chaotic generator consists of the time delay feedback Chua circuit [16] which is shown in figure (1)

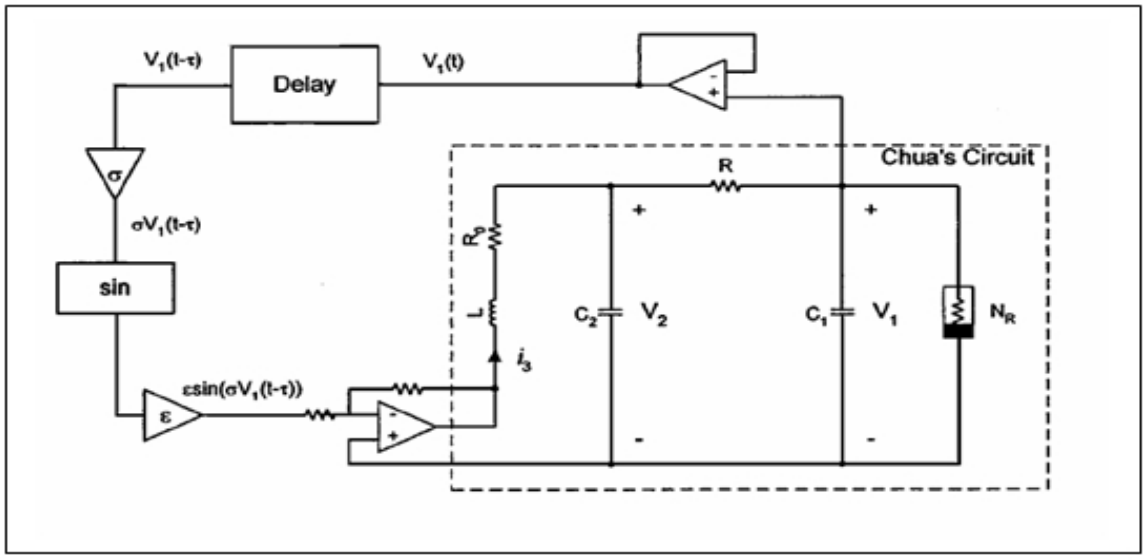

Figure 1. Time delay feedback Chua circuit

A time delay voltage feedback is added to the nominal Chua circuit. This system is described by the following system:

$$\begin{aligned} \dot{v}_1 &= \frac{1}{c_1}(G(v_2 - v_1) - h(v_1)) \\ \dot{v}_2 &= \frac{1}{c_2}(i_3 + G(v_1 - v_2)) \\ \dot{i}_3 &= -\frac{1}{L}(v_2 + r_0 i_3 + w(v_1(t-\tau))) \end{aligned} \quad (1)$$

Where v_1, v_2 and i_3 are the voltage across c_1, the voltage across c_2 and the current through L, respectively. $G = \frac{1}{R}$ and

$$h(v_1) = G_b v_1 + \frac{1}{2}(G_a - G_b)(|v_1 + E| - |v_1 - E|) \quad (2)$$

is the $v-i$ characteristic of the non linear resistor.

The time-delay function input is :

$$w(v_1(t-\tau)) = \varepsilon \sin(\sigma v_1(t-\tau)) \quad (3)$$

Where ε and σ are tow positive constants and τ represents the time delay.

Transmitter key definition

The parameter r_0 is taken as the cryptosystem secret key. The value of this key is chosen in a way that makes the output behaviour of the circuit be chaotic. To do so, we plotted the bifurcation diagram which is used to study the changes in the evolution of the solution's system with respect to changes in a chosen parameter. In this case, we plotted v_1 with the control parameter r_0, so by varying its value from 1 to 50, keeping the other parameter fixed as following:

$R = 1950; c_1 = 10^{-8}; c_2 = 10^{-7}; L = 18{,}68.10^{-3}; \sigma = 0{,}5; \varepsilon = 0{,}2$ and $\tau = 0{,}001$

The bifurcation diagram is illustrated in figure(2)

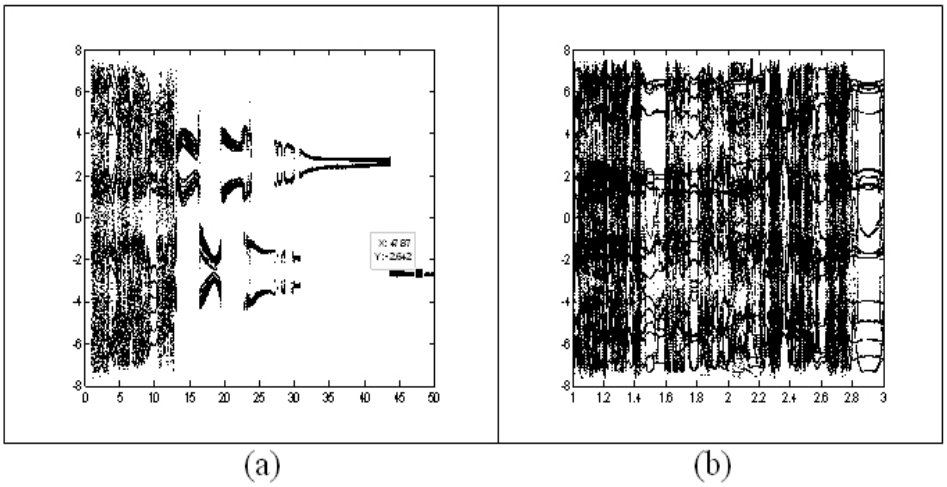

Figure 2. Bifurcation diagram (a) For $1 < r_0 < 50$, (b) Zoom for $1 < r_0 < 3$

As can be seen from the figure (2a), the state variable v_1 is stable if r_0 is superior to 47.87, and then, if r_0 is inferior to this value the system dynamics follows usual period doubling rout

to chaos. From the bifurcation diagram we can deduce that the key space is so large, since there an infinity of values corresponding to the chaotic behaviour of the chaotic generator.

Since, for all $r_0 < 3$ the behaviour of the chaotic generator is chaotic, we define and fix $r_0 = 1.2$ as the transmitter secret key.

Sensitivity to parameters:

To quantify the sensitivity to parameters of the time delay Chua's circuit, we analysed the resemblance between two solutions corresponding to two slightly different parameters. This resemblance is measured by computing the intercorrelation between the solutions, to do so , we proceed as following :

(i) we focus our study on the state variable v_1 of the system,

(ii) we vary the parameter $r_0 = 1.2$ (secret key) with a small variation $\pm \Delta r_0 = 10^{-5} r_0$ with 100 steps.

(iii) we computed the inter-correlation:

$$R_{vv1}(0) = \int_{\infty}^{\infty} v(t).v_1(t)dt \qquad (4)$$

Where v and v_1 are variable states of the system for parameters r_0 and $r_0 \pm i.(\Delta r_0)$ $i \in \{0,..,100\}$, respectively.

The figure (3) presented the normalized intercorrelation as a function of mismatch on r_0 of both time delay and standard Chua circuit. This figure shows that the inter-correlation of the time-delay chua system is lower then the inter-correlation of the standard one for all values of mismatch on r_0 $\Delta r_0 \neq 0$. This means that, by introducing a time delay feedback, it is possible to increase the degree of the sensitivity to parameter variation of this system.

So we can conclude that, if we choose correctly the parameters of time delay Chua's circuit, this system can present a high sensitivity to parameters and its can be considered such as an hyperchaotic system, this properties increase the security and performance of cryptosystem using this type of circuit: the deciphering is exact only when the receiver exactly knows the value of r_0 , that is to mismatch is equal to zero.

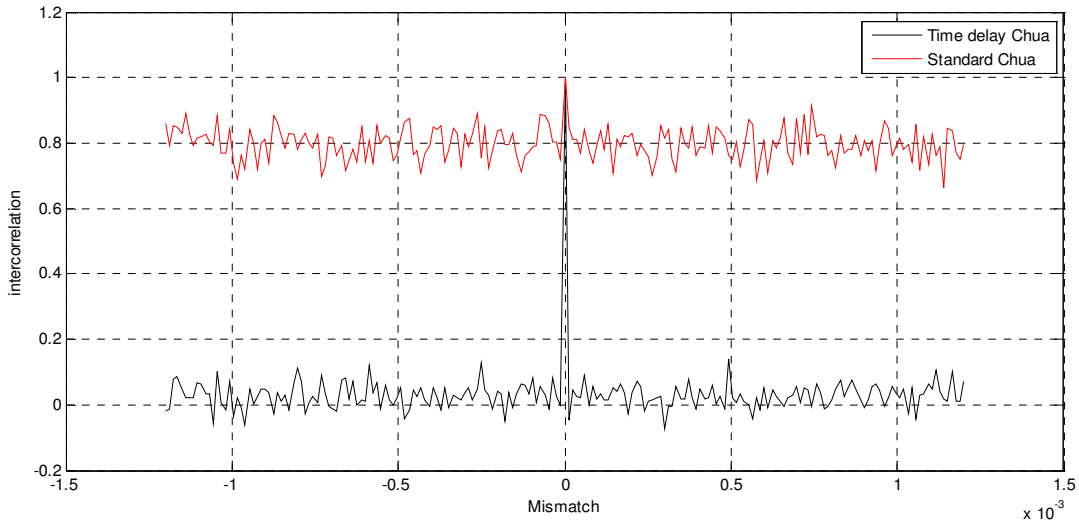

Figure 3. Intercorrelation versus mismatch on r_0.

Power spectrum:

The power spectrum of the state v_1 of both time delay and standard Chua circuit chaotic systems can be found in Figure(4)

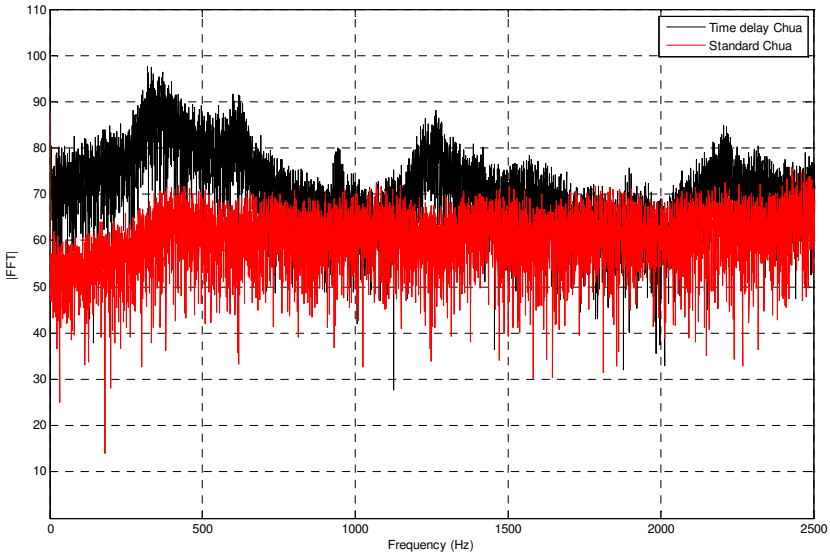

Figure 4. Power spectrum

the power spectrum of the time delay feedback Chua circuit is so high than its standard version power spectrum; this property illustrate the major characteristic of the hyperchaotic system [18]such as time delay chaotic system.
We can conclude that one of the most significant advantages of using time delay Chua's circuit is spreading the power spectrum. By increasing the complexity of power spectrum, the traditional cracking algorithms of chaotic masking will be unusable, thus enhancing the security.

OBSERVER DESIGN

In this section, we are interested in the design of a nonlinear observer which ensures synchronization with the chaotic generator. In this work we consider the observer described in [17].

This observer possesses the following advantages:

- It is simple to be implemented
- it does not require the computation of any Lyapunov Exponent and
- it does not require initial conditions belonging to the same basin of attraction.

The dynamic model of the chaotic generator can be rewritten as:

$$\dot{x} = A.x + B.f(x, x_\tau) \tag{6}$$

With $\dot{x} = (\dot{v}_1, \dot{v}_2, \dot{i}_3)^T$, $A = \begin{pmatrix} \frac{-G}{c_1} & \frac{G}{c_1} & 0 \\ \frac{G}{c_2} & \frac{-G}{c_2} & \frac{1}{c_1} \\ 0 & -\frac{1}{L} & -\frac{r_0}{L} \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$

and $f(x, x_\tau) = \begin{pmatrix} -\frac{1}{c_1} h(v_1) \\ -\frac{1}{L} \omega(v_1(t-\tau)) \end{pmatrix}$

The dynamic model of the nonlinear observer is the following:

$$\dot{y} = A.y + B.f(y, y_\tau) + g(s(x, x_\tau) - s(y, y_\tau)) \quad (7)$$

Where $g : IR^2 \to IR^3$ is a suitably chosen nonlinear function; and $s : IR^3 \to IR^2$ is the synchronizing signal.

Chaotic generator and observer are said to be synchronizing, if $e(t) = x(t) - y(t) \xrightarrow{t \to \infty} 0$.

Let : $s(x, x_\tau) = f(x, x_\tau) + Kx$

With $K \in IR^{2x3}$, and let : $g(s(x, x_\tau) - s(y, y_\tau)) = B(s(x, x_\tau) - s(y, y_\tau))$

Then the dynamic of the error becomes linear and time-invariant, and can be expressed as:

$$\dot{e} = Ae - BKe = Ae + Bu \quad (8)$$

Where $u = -Ke$ plays the role of a state feedback.

The error dynamic system is controllable if the controllability matrix $m = [B, AB, A^2B]$ is full rank.

In this case, a necessary and sufficient condition for the existence of a feedback gain matrix K such that the error converges to 0 is that all eigenvalues of the matrix $C = [A - BK]$ have negative real parts.

In this work, the chosen matrix m is full rank and we have to sent only one of the states of the time delay feedback Chua circuit to ensure the synchronization of the receiver, if we choose the state v_1 , the structure of the matrix K will be as the following :

$$K = \begin{pmatrix} k_{11} & 0 & 0 \\ k_{21} & 0 & 0 \end{pmatrix}$$

For $k_{11} = -10$ and $k_{21} = -50$,the eigenvalues of the matrix C are $(-45491 \; ; -5487 + 3100\, i ; -5487 - 3100\, i)$; Substitute this matrix K into the observer dynamic and we got the sum of squared errors (SSE) in state estimation as showed in figure (5).

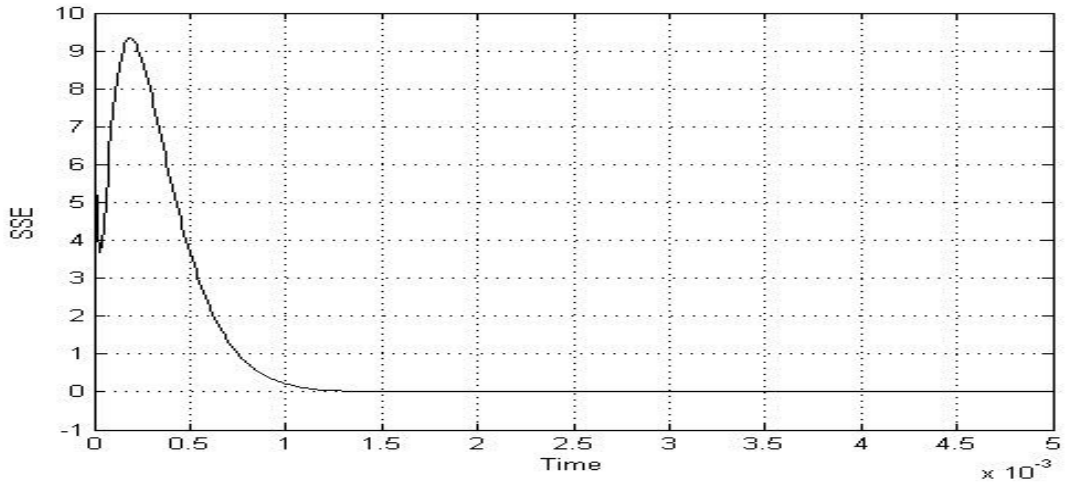

Figure 5. SSE

It's clear that the SSE is very low and satisfactory, the synchronization is achieved after 1,3 ms.

PROPOSED CRYPTOSYSTEM: DIGITAL IMAGE ENCRYPTION

The proposed cryptosystem is based on the nonlinear observer synchronization method of the chaotic time delay feedback Chua circuit.

Selected communication scheme

In this work, we considered the scheme illustrated in figure(6)

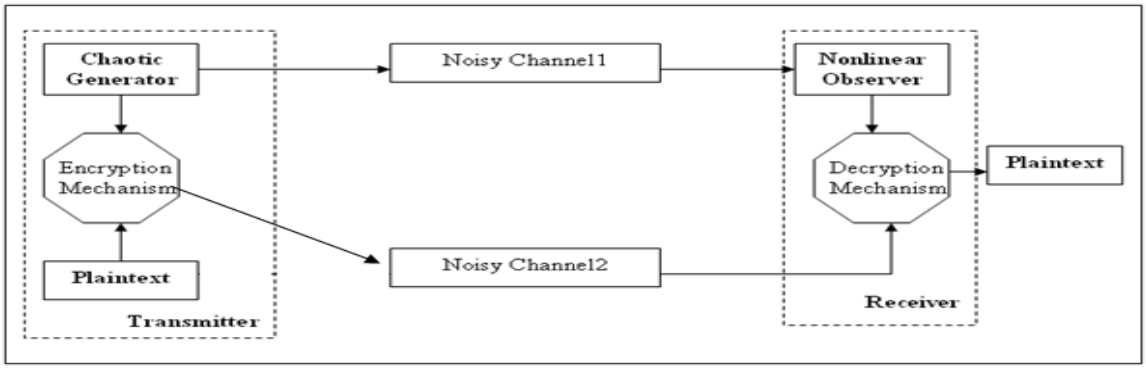

Figure 6. Proposed communication scheme

In this scheme, the synchronization and the encoding are independent, indeed, two chaotic signals are sent by the transmitter. On the one hand, a first signal is aimed to the synchronization of the receiver.
On the other hand, a second signal is used to encrypt the message: the information signal is injected in the second chaotic signal by the encryption mechanism to create masked message.

Image encryption/Decryption

The aim of this work consists to transmit a digital image in a secure way. In this work, we will consider a gray-level image. However, in discrete signal encryption, the signal should be converted into one-dimensional array, and hence image files have to be redimensioned as a one-dimensional signal array before processing, in this work, we transform the images file on NRZ signal written as:

$$m(t) = \sum_k a_k \, g(t - kT_b) \qquad (10)$$

where $a_k \in \{-1,1\}$ are symbols, $g(t) = 1 \ \forall t \in [(k-1)T_b, kT_b]$ and T_b is the symbol period.

In order to recover the original signal and enhancing the security of the cryptosystem, we choose the chaotic signal as following:

$$s(t) = \alpha . a \sin\left(m(t) + \beta v_2\right) \qquad (11)$$

where $m(t)$ is the original message,

After the synchronization step, the receiver recovers the message using the decryption mechanism ensured by the function:

$$\tilde{m}(t) = \sin\left(\frac{s(t)}{\alpha}\right) - \beta(\tilde{v}_2(t)) \quad (12)$$

Where $\tilde{v}_1$ and $\tilde{v}_2$ are given by the dynamic model of the observer.

The result of the encryption using the proposed chaos cryptosystem is illustrated in Figure(7). Figure(7.a) shows the original image of Lena, Figure(7.b) is the encrypted image and in Figure(7.c) the recovered image is successfully obtained.

Figure7. Image secure Transmission :(a) the original image,(b) the encrypted image, (c) the recovered image

CRYPTOSYSTEM SECURITY ANALYSIS

This section is devoted to some security questions: test of diffusion and confusion properties and robustness study of the proposed cryptosystem to some best-known attacks.

Diffusion and confusion properties

To resist common attacks, the designed cryptosystem should have the following two basic cryptographic properties: confusion and diffusion [6]. The first property is intended to make statistical properties of the ciphertext, such as distribution, correlation and differential probability, should be independent of the exact value of the key and of the plaintext. The second property consists to the high sensitivity of the system to key or to the plaintext, that for two keys (or two plaintexts) with the slight difference, we obtained two deferent ciphertexts.

Cryptosystem diffusion properties:

We would like to prove here that the proposed cryptosystem possesses the diffusion property, thus we encrypt the same image twice with two different values of key and we show these histograms which will be illustrated in the figure(8). The histograms (8a-8b) show that the

images obtained by subtraction of tow encryptions of the same image for a simple change of keys are different, thus we can deduce that this cryptosystem possesses the property of diffusion.

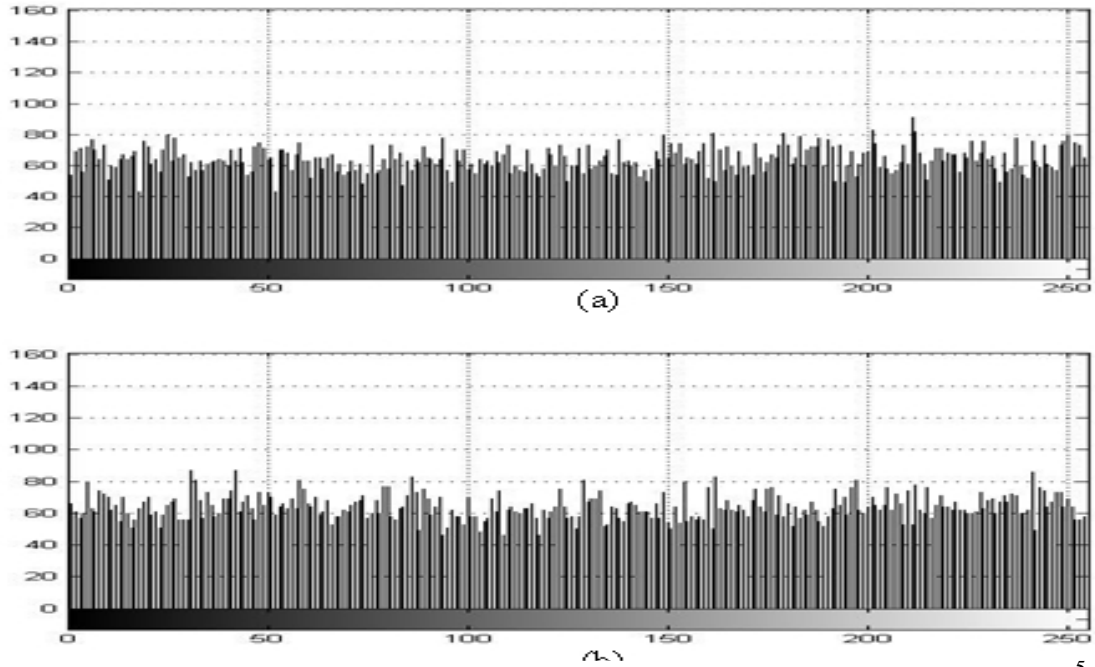

Figure 8. Histogram of the encrypted image: (a) key = 1.2, (b) key=$1.2+10^{-5}$

Cryptosystem confusion properties:

The confusion of this cryptosystem is tested by the sending of the same figure twice, but in this case without changing the key, the images obtained is shown in figure(9) : it proves that the two ciphertext with the same key corresponding to the same plaintext, are completely different. This proves that the proposed cryptosystem possesses the property of confusion.

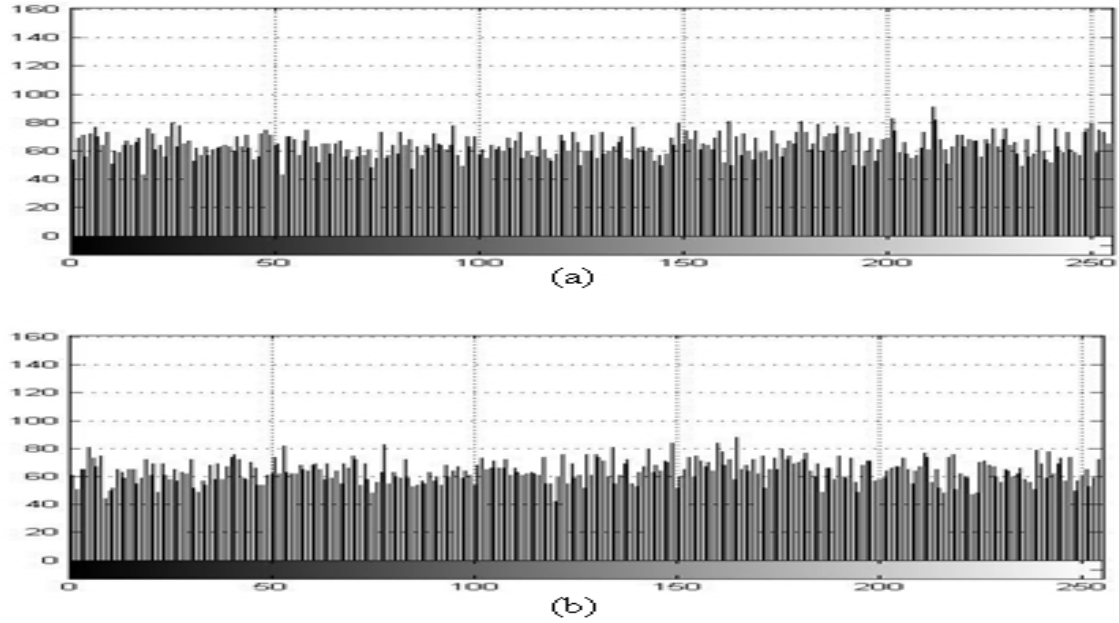

Figure 9. Encrypted image histogram :(a) first sent,(b) second sent

Remark: This result is due to the process of synchronization, with each sending of message, the state of the transmitter (which corresponds at the initial state) changes. That means that the proposed cryptosystem exploits the properties of the chaotic systems and their synchronization: we exploit here the extreme sensitivity to the initial conditions, and the capacity of the receiver to be synchronized without knowing the initial state of the transmitter.

Chaos-specific attacks

Different methods have been proposed to attack chaos-based cryptosystems, for both analog and digital settings, here we are interested to the analog one. There are two best-known possibilities for cryptanalysis [6]: the first is the estimation of the secret parameters from the transmitted ciphertext signal and the second consists to the extraction of the original message signal m (t) directly from the transmitted ciphertext signal.

Parameters estimation

To testing the robustness of the proposed cryptosystem for this attack, we suppose that an intruder obtains the structure of the transmitter, but does not know exactly the value of the key r_0. In the figure (10) the deciphering message appears for $r_0 = 1.2$ in the transmitter and at the intruder system $r_0 = 1.2 + 10^{-10}$.

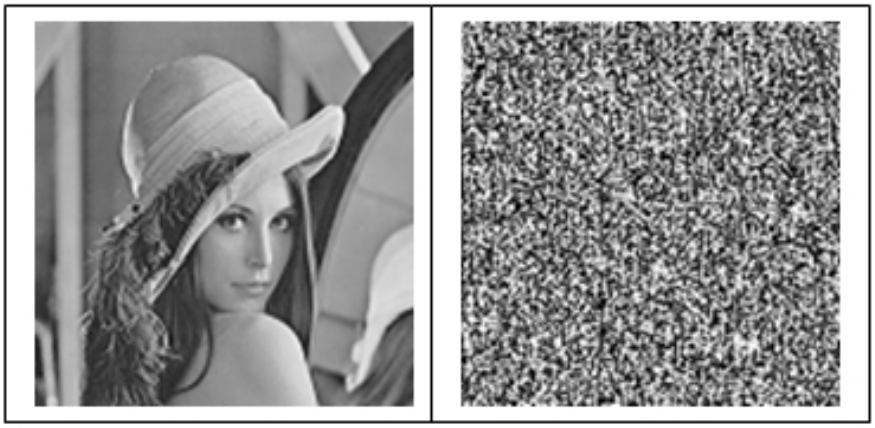

Figure 10. (a) original image (b) deciphering image for $r_0 = 1.2 + 10^{-10}$

It's clear that the intruder can't recover the original image.

So, we can say that the proposed cryptosystem is robust to the parameter estimation attack.

This robustness is achieved since the transmitter having the diffusion property.

Message signal extraction

This can be accomplished using different methods: autocorrelation and cross-correlation analysis, power spectral analysis and filtering technique [6], here we will test the robustness of the proposed cryptosystem to the power spectral attack.

The figure(11) show the power spectral of the plaintext, the pseudorandom noise for time delay feedback Chua circuit and its standard version

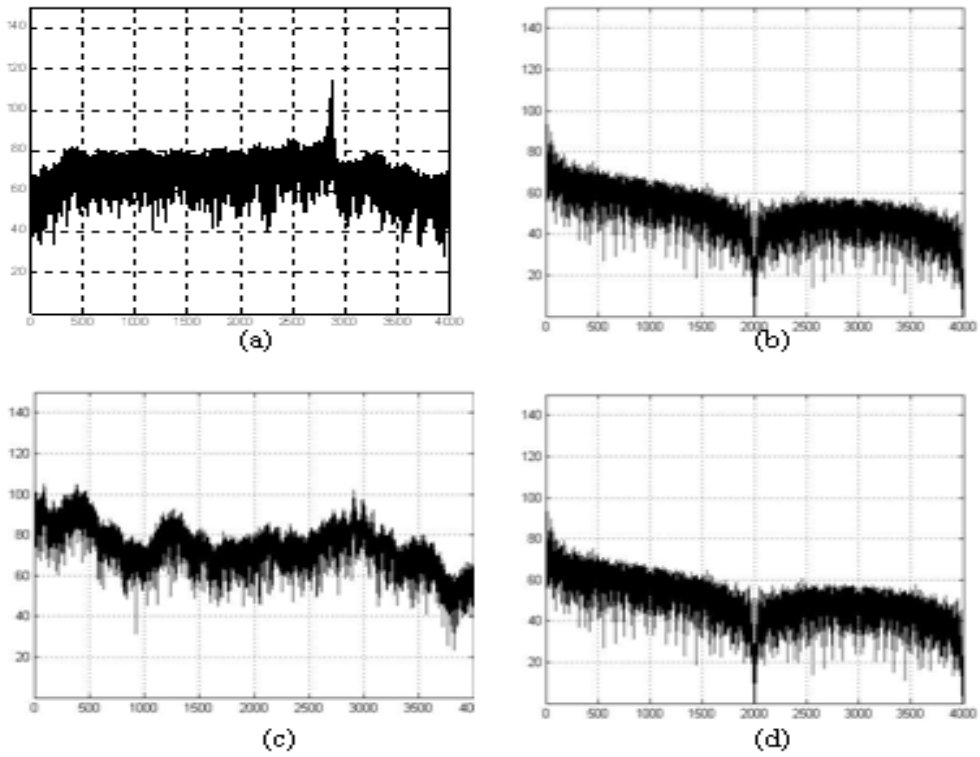

Figure 11. Power spectrum (a) chaotic signal for Standard Chua circuit, (b,d) the spreading signal : NRZ signal with a chip period equal to 0.5 ms, (c) chaotic signal for time delay feedback Chua circuit

The figure(11-c) shows that the spectrum of the pseudorandom noise used in the cryptography is infinitely broad, flat, and of much higher power density than the signal to be concealed. In other words, the plaintext power spectrum is effectively buried into the pseudorandom noise power spectrum.

So, we can conclude that, using this circuit, the traditional cracking algorithms of chaotic masking will be unusable, thus enhancing the security.

CONCLUSION

In this paper, the problem of the secure transmission of a digital image was addressed. We design a chaotic cryptosystem based on the nonlinear observer synchronization method of the chaotic time delay feedback Chua circuit which's chosen for its noise like trajectories, for its extremely broad frequency bandwidth of high magnitude and for its great sensitivity to their parameters, which will be used as secret key. The made security analysis proves that the proposed cryptosystem possesses the properties: confusion and diffusion which make it robust to common attacks. It is interesting to analyse, in further work, the influence of the noise present in the transmission channel on the deciphering quality in the receiver.

REFERENCES

[1] R. Rhouma, S. Meherzi, S. Belghith, *OCML-based colour image encryption,* International Journal of Chaos, Solitons and Fractales 2007.

[2] B. Furht and D.Socek, *Multimedia security : encryption techniques.* IEC Internationnal Engeneering Consortium, Chicago, II, pages 335-349, 2004.

[3] L. Tang, *Methods for encrypting and deciphering MPEG video data efficiently.* Proceeding of the 4th ACM International Multimedia Conference, page 219-230, 1996.

[4] T.Xiang, K.W. Wong, X. Liao, *Selective image encryption using spatiotemporal chaotic system.* Chaos 17, pages 023115.1—023115.12 2007.
[5] H. Cheng and X. Li, *Partial encryption of compressed images and videos.* IEEE Transactions on Signal Processing, volume 48, pages 2439-2451, 2000.
[6] Alvarez G. and Shujun L. *Some Basic Cryptographic Requirements for Chaos-Based Cryptosystem,* International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129-2151, 2006.
[7] A. Kiani-B, K. Fallahi, N. Pariz, H. Leung, *A chaotic secure scheme using fractional chaotic systems based on an extended fractional Kalman filter*, Int. J. Communication in Nonlinear Science and Numerical Simulation, pages 863-879, November 2007.
[8] E. Cherrier, M. Boutayeb, and J. Ragot, *Observers-Based Synchronization and Input Recovery for a Class of Nonlinear Chaotic Models*, IEEE Trans. Circuits Syst. I: Vol. 53, No. 9, pp. 1977-1988. Sept 2006
[9] C. Li, X. Liao, and K. Wong, *Chaotic lag synchronization of coupled time-delayed systems and its applications in secure communications*,*Phys.* D, vol. 194, pp. 187–202, 2004.
[10] T. Yang *A survey o chaotic secure communication systems,* Int. J. of Comp. Cognition 2, 81-130,2004.
[11] G. Kolumbán, M.P. Kennedy, and L. O. Chua, *The role of synchronization in digital communications using chaos-PartI: Fundamentals of digital communications*, IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol.31, no.9, pp.927–936, Sep. 1997.
[12] N. Corron and D. Hahs, *A new approach to communications using chaotic signals*, IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol. 44, no. 5, pp. 373–382, May 1997.
[13] L. Kocarev, K. Halle, K. Eckert, L. Chua, and U. Parlitz, *Experimental demonstration of secure communications via chaotic synchronization,* Int. J. Bifurc. Chaos, vol. 2, pp. 709–713, 1992.
[14] H. Dedieu, M. Kennedy, and M. Hasler, *Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits*, *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl*., vol. 40, no. 10, pp. 634–642, Oct. 1993.
[15] K. Halle, C. Wu, M. Itoh, and L. *Chua, Spread spectrum communication through modulation of chaos, Int. J. Bifurc. Chao*s, vol. 3, no. 2, pp. 469–477, 1993.
[16] Xiao Fan Wang, Guo-Qun Zhong, Kit-Sang Tang, Kim F. Man, and Zhi-Feng Liu, *Generating Chaos in Chua's Circuit via Time-Delay Feedback,* IEEE Trans. Circuits Syst.I. Fundam Theory Appl., Vol. 48, No. 9, September 2001.
[17] Shu yonglu, Tan Bangding,.Lag Synchronization based on Nonlinear observer design for delay system, IEEE ,pp 1396-1400, 2004.
[18] G. Qi, M. A. van Wyk, B. J. van Wyk, G. Chen, *On a new hyperchaotic system,* Physics Letters A 372, pp 124-136, 2007.