DYNAMICS DAYS SOUTH AMERICA 2010
International Conference on Chaos and Nonlinear Dynamics

INPE – National Institute for Space Research
São José dos Campos – SP – Brazil – July 26-30, 2010

CRYPTOGRAPHY WITH CHAOS USING CHUA'S ATTRACTOR

Cleber Henrique Oliveira 1, José Carlos Pizolato Junior 2

1UEL, Londrina-PR, Brazil, cleberho@hotmail.com
2UEL, Londrina-PR, Brazil, jcpizolato@yahoo.com.br

Keywords: Control of Chaos and applications, Chaotic Dynamics, Stochastic Dynamics.

1- INTRODUCTION

Experts in nonlinear dynamics use the word "chaos" as a technical term to refer to the irregularity and unpredictable behavior of nonlinear deterministic systems [1-2]. For thereabout two decades, researchers have been studying the chaotic system characteristics and their use in information cryptography. In the work proposed by Rong He and P.G. Vaidya [3], the chaotic system synchronization is used for the cryptography key generation. The modified Chua's circuit was used to transfer audio and image information in a chaotic synchronization scheme [4]. In these two ultimate results published [3-4], there is a requirement of systems synchronization between transmitter and receiver.

Nevertheless, there are proposals for cryptographic systems with no requirement of synchronization between transmitter and receiver. The algorithm proposed by Batista [5] suggests a cryptographic system based on a unidimensional chaotic system, the logistic map [1], mathematically molded by $f_\mu(x) = \mu x(1-x)$. In it, the chaotic behavior is used for data ciphering.

This paper proposes a new algorithm of data cryptography based on the contributions from the cryptographic method presented in [3]. The chaotic system cipher uses Chua's attractor presented in [4], in order to cause a chaotic behavior. The proposed algorithm uses chaotic signals with no requirement of systems' synchronization between transmitter and receiver. Results reveal that this algorithm does not demand high capacity of computational processing.

2- PROPOSED ALGORITHM

The algorithm assumes the principle that for each unit of plaintext, there must be a key k to make it unrecognizable. During the execution of the algorithm each key k is used only once in the process.

The proposed cipher uses Chua's chaotic system behavior [4] to generate keys k in a non-periodic orbit, by using the iterations $f_p : I \to I$, with interval I necessary to cipher the information and parameter P, which were adjusted to generate the chaotic attractor in Chua's circuit [6-7]. The interval I is divided in N sub-intervals Ik, $(k = 1,2,3,...,N)$ called sites. Each site is used to generate keys k, defined by $x_1(t)$, $x_2(t)$ and $x_3(t)$, so that key $k = x_1(t) + x_2(t) + x_3(t)$.

The state equations system normalized for Chua's circuit is described as follows:

$$\dot{x}_1 = \alpha\left(x_2 - f(x_1)\right) \quad (1)$$

$$\dot{x}_2 = x_1 - x_2 + x_3 \quad (2)$$

$$\dot{x}_3 = -\beta x_2 \quad (3)$$

The nonlinear function $f(x_1)$ is mathematically described by:

$$f(x_1) = bx_1 + 0.5(a-b)(|x_1 + c| - |x_1 - c|) \quad (4)$$

The system parameters ($b = -\frac{1}{7}$, $a = \frac{2}{7}$, $\alpha = 9$, $\beta = 14.28$ and $c = 1$) were adjusted to allow the generation of the chaotic attractor in Chua's circuit. [6-7].

The original information is called information unit p, the unrecognizable information is called ciphered information unit c and the key is called k. The process to transform an information unit p in ciphered information c is called ciphering and the opposite process is called deciphering. Since only one information unit is deciphered at a time, the proposed algorithm is assorted as a flow ciphering [8].

The ciphering process of p_j consists of iterating f_p consecutively, starting from the initial condition (key) $x_0 \in I$, computing the number of iterations and associating each site Ik for the ciphering of one information unit p, by using the cryptographic method $c = (p + k) \bmod(256)$.

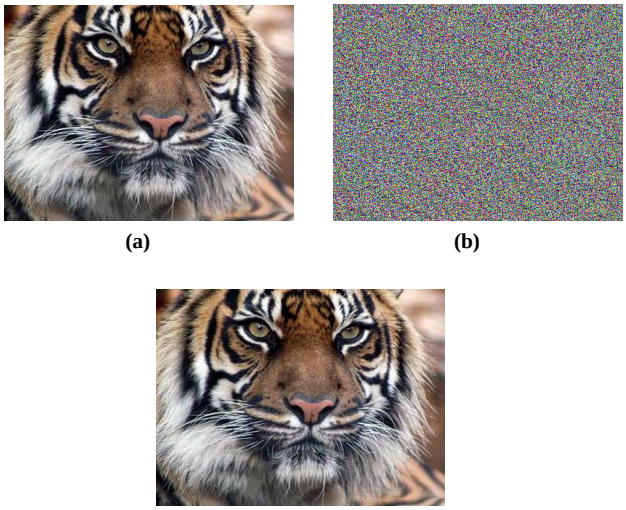
The deciphering of c_j is made by using the same key k, that is, associating the same subinterval ik with the ciphered information unit c_j, considering $p = c - (k \bmod(256))$.

This process uses an alphabet compounded by symbols based on the ASCII table as a reference, having as equivalence the decimal format (0, 1,..., 255), in which both the information unit p and the ciphered version $c \in (0, 1,..., 255)$.

The cryptographic method proposed is especially characterized by of the algebraic functions involved. Thus, a complex and unpredictable behavior is obtained.

3- RESULTS

The cryptographic method proposed was applied in a piece of image information shown in figure (1). The ciphering/deciphering process uses the system of equations (1-3), with initial conditions ($x(0) = 0.1$, 0.2 e 0.3) to generate the key k.



(a) **(b)**

(c)

Figure 1 – Cryptographic process. (a) Original image (400 x 300 pixels). (b) Ciphered image (400 x 300 pixels). (c) Deciphered image (400 x 300 pixels).

Figure (2) verifies the algorithm security by showing a comparison between the sort of text information composed by information units p_j and its ciphered version c_j. The ciphering process utilizes the system of equations (1-3), with initial conditions ($x(0) = 0.2$, 0.3 and 0.1) to generate the keys k.

Concerning the figure (2), "Y – Byte (Decimal)" represents the information units p_j and their ciphered versions c_j in decimal format (0,1,...,255), according to the ASCII table. In addition, "X – Position of the bytes" represents the positions of the information units p_j and their ciphered version c_j respectively in positions (1,2,...,50). Therefore, for each information unit p, there is a ciphered version c as illustrated in figure (2).

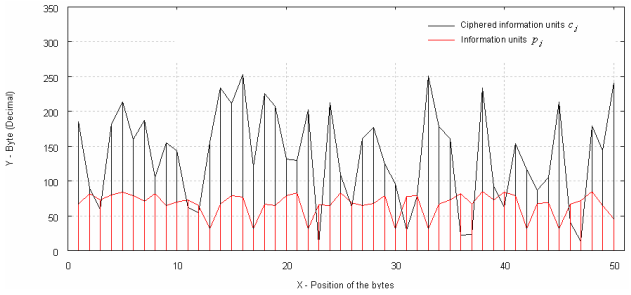


Figure 2 – Graphic of a piece of information composed by information units and their ciphered version.

4- DISCUSSIONS

The proposed algorithm does not require any synchronism between transmitter and receiver in the ciphering/deciphering process. Such cryptographic process does not depend on the alphabet, once it follows the ASCII chart, what implicates in higher levels of security and versatility in several applications.

5- CONCLUSIONS

This paper presents a new cryptographic algorithm by using the chaotic behavior of Chua's circuit to generate cryptographic keys. The proposed algorithm is grounded on the algebraic functions involved and on the complex and unpredictable behavior of the signals used in the cryptographic system. Results obtained and illustrated in figures 1 and 2 reveal that this algorithm can be used for image and text information cryptography.

REFERENCES

[1] Kadanoff, L. P, "Roads to Chaos," Physics Today, pp.46, December, 1983.

[2] Gleick, J. (1990). *Caos: A construção de uma nova ciência*. Rio de Janeiro, Editora Campus, 1990.

[3] Rong He, P. G. Vaidya, "Implementation of chaotic cryptography with chaotic synchronization," Physical Review E, volume 57, number 2, February (1998) 1532-1535.

[4] G. Guzman, C. Cruz-Hernández, R. M. López-Gutierrez, E. E. Garcia-Guerrero, "Synchronization of Chua´s circuits with multi – scroll attractors: Applications to communication," Communication Non-Linear Sci Numer Simulat, October (2008) 2765-2775.

[5] M. S. Baptista, "Cryptography with chaos," Physics Letters A, no. 240, pp. 50-54, 1998.

[6] Madan RN, "Chua's circuit: a paradigm for chaos," Singapore: World Scientific; 1993.

[7] Chua LO, Komuro M, Matsumoto T, "The double scroll family," IEEE Trans Circ Syst I 1986;33(11):1072-118.

[8] Singh, S. *O livro dos códigos*. 7ª Edição. Rio de Janeiro: Editora Record, 2008.

[9] L. P. L. Oliveira and M. Sobottka, "Cryptography with chaotic mixing," Chaos Solitons and Fractals, May 2008.