Cryptography with chaos using Chua’s system

C H Oliveira 1 and J C Pizolato Jr 2

1 State University of Londrina (UEL-PR), Brazil
2 Federal University of São Carlos (UFSCAR-SP), Brazil

E-mail: cleberho@hotmail.com

Abstract: In the last years, chaotic systems have been applied in information security. These systems have a complex and unpredictable behavior, what makes them more attractive for data cryptography applications. In this work, the chaotic behavior of signals generated by Chua’s system is combined with the original information in order to obtain a safe cryptographic method. The experimental results demonstrate that the proposed scheme can be used in data cryptography applications.
1. Introduction
Experts in nonlinear dynamics use the word “chaos” as a technical term to refer to the irregularity and unpredictable behaviour of nonlinear deterministic system [1-2]. These systems, although having only one or two degrees-of-freedom, can display an amazing random behaviour, from periodic up to chaotic.

For thereabout two decades, researchers have been studying the chaotic system characteristics and their use in information cryptography. In Rong He and P.G. Vaidya’s work [3], the chaotic synchronization system is used in the cryptography key generation. The modified Chua’s circuit was used to send 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]. 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], in which the algorithm utilizes the Chua’s system in order to cause a chaotic behaviour. The proposed chaotic cipher 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.

This paper will be presented as it follows. The mathematical model of Chua’s system is analyzed in section 2. The algorithm proposed is presented in section 3. Section 4 presents qualitative results through the application of the proposed cryptographic process on two pieces of information, being the first a sort of image information and the second a sort of text information. Furthermore, it displays the frequency analysis on a sort of text information. In section 5, some considerations are made on the algorithm proposed. The conclusions concerning the cryptography scheme proposed are in section 6.

2. The Chua’s system
The mathematical model of Chua’s system [4], is described by the system of state equations that follows:

\[
\begin{align*}
C_1 \frac{d v_{c1}}{dt} & = \frac{1}{R} (v_{c2} - v_{c1}) - g_{NR}(v_{c1}) \\
C_2 \frac{d v_{c2}}{dt} & = \frac{1}{R} (v_{c1}) + i_L \\
L \frac{di_L}{dt} & = -v_{c2}
\end{align*}
\]

(1) (2) (3)

Where: \(v_{c1}\) e \(v_{c2}\) correspond to the tensions through the capacitors \(C_1\) and \(C_2\) respectively, \(i_L\) is the current whereby the inductor \(L\) and \(g_{NR}(v_{c1})\) represent a nonlinear function which defines the characteristics \(v - i\) of Chua’s diode, mathematically described in (4).

\[
g_{NR}(v_{c1}) = G_a v_{c1} + \frac{1}{2} (G_a - G_b)(|v_{c1} + E| - |v_{c1} - E|)
\]

(4)
The application of the transformations \( x_1 = \frac{v_{c_1}}{E}, x_2 = \frac{v_{c_2}}{E}, x_3 = \frac{i_L}{EG}, \tau = \frac{Gt}{C_2} \) where \( E = 1 \text{ V} \) and \( G = 1/R \), it is possible to get the system of state equations of Chua’s system normalized, as follows:

\[
\begin{align*}
\dot{x}_1 &= \alpha(x_2 - f(x_1)) \\
\dot{x}_2 &= x_1 - x_2 + x_3 \\
\dot{x}_3 &= -\beta x_2
\end{align*}
\]

Where: \( \dot{x} = dx/d\tau, \alpha = C_2/C_1 > 0 \) and \( \beta = C_2/G^2 L > 0 \) are the system bifurcation parameters.

The nonlinear function \( f(x_1) \) is mathematically described by (8):

\[
f(x_1) = bx_1 + \frac{1}{2}(a-b)(|x_1 + c| - |x_1 - c|)
\]

Where: \( a = G_u/G < 0 \) e \( b = G_u/G < 0 \).

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

3. The proposed algorithm

The original message is called plain text, the unreadable message is called ciphered and the key is called \( k \). The process of turning a plaintext into a ciphered text is called ciphering and the inverse process is called deciphering. Since only one plaintext is ciphered at a time, the proposed algorithm is a flow ciphering system [8]. The algorithm assumes that for each unit of plaintext, there must be a key \( k \) to make it unrecognizable. In this algorithm each key \( k \) is used only once in the encoding process.

The key generator \( k \) uses a non-periodic orbit, in which \( f_p : I \mapsto I \), through Chua’s chaotic system behaviour, with the interval \( I \) and parameter \( P \) [6-7]. The interval \( I \) is divided in \( N \) sub-intervals \( I_k, (k = 1,2,3,...,N) \) used to generate keys \( k \), defined by \( x_i[r], x_{i+1}[r] \) e \( x_{i+2}[r] \).

The ciphering process 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 \( I_k \) for a plaintext unit ciphering \( p \), by using \( c = (p + k) \text{ mod}(256) \). The \( c \) deciphering is made by using the same key \( k \), that is, associating the same sub-interval \( I_k \) with the text unit ciphered \( c_j \), using \( p = c \text{ mod}(256) \). These processes use an alphabet compounded of symbols based on the ASCII table in which the equivalence used is 0,1,...,255.

For both the plain text \( p \) and the ciphered text \( c \in \{0,1,...,255\} \). In order to cipher a plaintext unit, \( c = (p + k) \text{ mod } 256 \) is used and to decipher a ciphertext unit \( p = c \text{ mod}(256) \). This way, this method is especially characterized by the simplicity of the algebraic functions involved. Security is increased through the generation of the keys \( k \), where each key is used only once either to cipher a plaintext unit or to decipher a ciphertext unit.
3.1. Key generator
In the proposed algorithm, the key generator $k$ for ciphering data uses the Chua’s chaotic system characteristics, presented in the reference [4]. The key $k$, is generated from each sub-interval $I_k$ of $x_1[t], x_2[t]$ and $x_3[t]$ in which, $k = x_1[t] + x_2[t] + x_3[t]$. Through the algebraic functions involved, a complex and unpredictable behavior is obtained. Therefore, the normalized version of Chua’s system is given by the equations (9-11):

$$
\begin{align*}
\dot{x}_1 &= \alpha(x_2 - f(x_1)) \\
\dot{x}_2 &= x_1 - x_2 + x_3 \\
\dot{x}_3 &= -\beta x_2
\end{align*}
$$

and by the nonlinear function (12):

$$
f(x_1) = bx_1 + \frac{1}{2}(a-b)(|x_1 + c| - |x_1 - c|)
$$

However, the parameters presented in [6-7] $b = -\frac{1}{7}, a = \frac{2}{7}, \alpha = 9, \beta = 14, 28$ are used, and $c = 1$, in which the integration algorithm used is Euler.

Figure (1) shows a three-dimensional chaotic system $\dot{x}_1, \dot{x}_2$ and $\dot{x}_3$, which represents and attractor generated by Chua’s chaotic system.

![Attractor generated by Chua’s chaotic system simulation with parameters [6-7] (b = -\frac{1}{7}, a = \frac{2}{7}, \alpha = 9, \beta = 14, 28 and c = 1) and initial conditions (x_1[0] = 0.2, x_2[0] = 0.6 and x_3[0] = 0.7001).](attachment:attractor.png)

Nevertheless, the attractor generated based on Chua’s chaotic system, used to generate the keys $k$, which are defined by $x_1[t], x_2[t]$ and $x_3[t]$ are dependent on the initial conditions. Each key $k$ is
used only once, that is, exclusively by one text unit. Yet, for \( x_1[t], x_2[t] \) e \( x_3[t] \) it is determined the interval, which becomes dependent on the amount of text units of the information. Thus, the sub-intervals \( I_k \) of \( x_1[t], x_2[t] \) and \( x_3[t] \) are used to create the keys \( \{ k_1, k_2, k_3, ..., k_n \} \).

Figure (2) shows a key generator, which uses chaotic signals with no requirement of system synchronization between transmitter and receiver.

\[
\begin{align*}
\dot{x}_1 &= \alpha (x_2 - x_1) \\
\dot{x}_2 &= x_1 - x_2 + x_3 \\
\dot{x}_3 &= -\beta x_2 \\
\end{align*}
\]

**Key generator**

\[ x(t) \]

**Encryption**

\[ x(t) \]

**Decryption**

\[ x(t) \]

**Figure 2.** Ciphering / deciphering process by using Chua’s chaotic system.

Based on the behavior of Chua’s chaotic system, we will bring forward two examples of key generation \( k \), used in figure (3). From the sub-interval \( I_k \) of \( x_1[t], x_2[t] \) and \( x_3[t] \) in this case, \( t = 1.0 \) we will have \( x_1[t] = 0.610429, \; x_2[t] = 0.231888 \) and \( x_3[t] = 0.609670 \), with \( t = 2.0 \) we will have \( x_1[t] = 0.615602, \; x_2 = 0.241770 \) and \( x_3[t] = 0.576557 \).

Therefore, we use \( n \) decimal places of the sub-interval \( I_k \) to generate a whole part, as the example, \( t = 1.0 \) we will have \( x_1[t] = 0.610429, \; x_2[t] = 0.231888 \) and \( x_3[t] = 0.609670 \), \( t = 2.0 \) we will have \( x_1[t] = 0.615602, \; x_2 = 0.241770 \) and \( x_3[t] = 0.576557 \).

The keys \( k \) are generated from \( x_1[t], x_2[t] \) and \( x_3[t] \) of the sub-interval \( I_k \), in which, \( k = x_1[t] + x_2[t] + x_3[t] \), for instance, \( t = 1.0 \) so \( k = 610429 + 231888 + 609670 \) however, \( k = 1451987 \) and \( t = 2.0, \) so \( k = 615602 + 241770 + 576557 \), however, \( k = 1433929 \).

**3.2. Cryptographic model proposed**

Based on the algorithm proposed, we present the ciphering of two plaintext units used in figure (3), where the characters “C” and “H” are represented respectively in the ASCII table by the numbers: “67” and “72”. However, it is used the cryptographic method \( c = (p + k) \mod(256) \), in which, \( (67 + 1451987) \mod(256) \) and \( (72 + 1433929) \mod(256) \) so the ciphertext units referring to “C” and “H” become “22” and “145”, following the ASCII table.

Figure (3) shows the ciphering process of a piece of information in which each key \( k \) is used only once to cipher a plaintext unit.
Figure 3. Ciphering process using the cryptographic model proposed.

When deciphering, the process is inverse. However, we present the deciphering of two ciphered text units “22” and “145”, used in figure (4). Thus, the cryptographic method is used, $p = c - (k \mod(256))$, in which, “22 = (1451987 mod(256))” and “45 = (1433929 mod(256))”, if resulting of $p < 0$, so, $p + 256$, but the plaintext units referring to “22” and “145”, become “67 = C” and “72 = H”.

Figure (4) shows the deciphering process of a piece of information in which each key $k$ is used only once to decipher a ciphered text unit.

Figure 4. Deciphering process using the cryptographic model proposed.

4. Results
This section presents qualitative results through the application of the proposed cryptographic process on two pieces of information, being the first a sort of image information and the second a sort of text information. Furthermore, it displays the frequency analysis on a sort of text information.

4.1. Appliance of the cryptographic process proposed in a sort of image information
The cryptographic method proposed was applied in a piece of image information (512 x 512 pixels) [9], as shown in figure (5).

In this section, a ciphering /deciphering process is displayed, in which the parameters defined in [6-7] and $x_1[0] = 0.1, x_2[0] = 0.2$ and $x_3[0] = 0.3$ are used to generate the keys $k$. 
Figure 5. Cryptographic process. (a) Original image (512 x 512 pixels) [9]. (b) Ciphered image (512 x 512 pixels). (c) Deciphered image (512 x 512 pixels).

4.2. Appliance of the cryptographic process proposed in a sort of text information

Figure (6) 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 (9-12), with initial conditions $(x[0] = 0.2, 0.3$ and $0.1)$ to generate the keys $k$.

Concerning the figure (6), “Y – ASCII (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 – Character positions” 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 (6).

Figure 6. Graphic of a piece of information composed by information units and their ciphered version.
4.3. System security analysis by using frequency analysis

This section analyses the frequency of the ciphered text units in order to assess the algorithm security against attacks of analysis to the frequency units that emerge in ciphertexts \( c_j \) and then associate plaintext units \( p_j \). Such test verifies a piece of information composed of 18.016 units of plaintexts \( p_j \) with 17.5 KB, in which 4.742 is the highest frequency of a plaintext unit \( p \) and 0 is the lowest frequency, in which 4.742 is the frequency difference between the plaintext units \( p_j \).

Figure (7) shows the analysis of the information frequency composed of plaintext units \( p_j \). Nevertheless, “Y-Frequency” displays the frequency of each plaintext unit \( p \). “X-ASCII (Decimal)” represents the plaintext units \( p_j \), in decimal format, following the ASCII table \( p = \{0,...,255\} \).

![Figure 7](image_url)

**Figure 7.** Illustration of the frequency analysis of a piece of information composed of plaintext units \( p_j \), in decimal format, according to the ASCII table.

Figure (8) shows the frequency analysis of a piece of information composed of 18.016 ciphered text units \( c_j \), with 17.5 KB, referring to the information displayed in figure (7). However, “Y-Frequency” exhibits the frequency of every ciphered text unit \( c \). “X-ASCII (Decimal)” represents the ciphered text units \( c_j \) in decimal format, according to the ASCII table \( p = \{0,...,255\} \).

However, the ciphering was achieved through the proposed algorithm, by using the Chua’s system behavior to generate keys \( k \), with parameters defined in [6-7], and \( x[0] = 0.2, 0.3 \) and 0.1. Since one plaintext unit \( p \) is ciphered at a time, the proposed algorithm is assorted as a flow ciphering system.

The algorithm proposed is classified as a flow ciphering system. But, for every plaintext unit \( p \), there is a ciphertext unit \( c \), that is, the ciphered information will have the same size as the original one. Thus, after the ciphering process, we got 94 to the higher frequency of a ciphertext unit \( c \) and 47 the lowest frequency, being 47 the frequency difference between the ciphertext units \( c_j \).
5. Discussion
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.

6. Conclusions
This paper presents a new cryptographic algorithm by using the chaotic behavior of Chua’s system 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. The results obtained and illustrated in section 4 reveal that this algorithm can be used for data cryptography.

Acknowledgments
The authors thank the Department of Electrical Engineering of Londrina State University and the Department of Electrical Engineering of São Carlos Federal University for their support.

References
[1] Kadanoff L P 1983 Roads to Chaos Physics Today p.46
[2] Gleick J 1990 Caos: A construção de uma nova ciência Editora Campus
[3] Rong He and P G Vaidya 1998 Implementation of chaotic cryptography with chaotic synchronization Physical Review E. volume 57 number 2 p. 1532-1535.
[4] G Guzman, C Cruz-Hernández, R M López-Gutierrez and E E Garcia-Guerrero 2008 Synchronization of Chua’s circuits with multi – scroll attractors: Applications to communications Commun NonLinear Sci Numer Simulat p. 2765-2775
[5] M S Baptista 1998 Cryptography with chaos Physics Letters A. no. 240 p. 50-54
[6] Madan RN 1993 Chua’s circuit: A paradigm for chaos Singapore:World Scientific

Figure 8. Illustration of the frequency analysis of a piece of information consisting of ciphertext units $c_j$, in decimal format, according to the ASCII table.
[7] Chua LO, Komuro M and Matsumoto T 1986 The double scroll family *IEEE Trans Circ Syst I* 33(11):1072-118

[8] Singh S 2008 O livro dos códigos *Editora Record* 7ª Edição

[9] Basso E W Filtros Vetoriais para a Remoção de Ruído em Imagens Coloridas Disponível em: <www.inf.ufrgs.br/~ewbasso/works/fvrric_paper.pdf> Acesso em: 21 mar. 2011.

[10] L P L Oliveira and M Sobottka 2008 Cryptography with chaotic mixing *Chaos Solitons and Fractals*

[11] L M Pecora and Carroll T L 1990 Synchronization in chaotic systems *Phys Rev Lett.* 64:821-824

[12] A Holokx A, Rech P C 2009 A parameter-space of a Chua system with a smooth nonlinearity *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering* v. 19 p. 1351-1355