Synthesis of a nonlinear cryptosystem based on the synchronization of chaotic circuits via a one-dimensional signal

DONATO CAFAGNA, LEONARDA CARNIMEO
Dipartimento di Elettrotecnica ed Elettronica
Politecnico di Bari
via E. Orabona, 4 - 70125 Bari
ITALY
cafagna@poliba.it, carmineo@poliba.it

Abstract: – In this paper a method to synchronize chaotic cryptosystems via a scalar transmitted signal is proposed with the aim of enhancing the security of communication systems. The scalar signal is obtained as a suitable linear combination of state variables of the transmitter and encrypted signals. The suggested method is applied to bidirectionally coupled Chua's oscillators. Moreover, the performance of the proposed cryptosystem is investigated in the presence of channel noise. Simulation results are reported to confirm the validity of the suggested method.

Key-Words: – Circuits, Nonlinear systems, chaotic synchronization, secure communications.

1 Introduction

During the last decade synchronization of chaotic systems has received a considerable attention due to the possibility of exploiting the broad-band spectrum and noise-like properties of chaotic signals [1–3]. In fact, these properties can be utilized for transmitting messages by means of synchronized chaotic circuits in secure communications [4–5]. However, as it is widely demonstrated, chaos strongly depends on the values of parameters and initial conditions, which can cause the divergence even of nearby starting orbits. In order to overcome this serious drawback, several methods have been proposed to implement two real chaotic circuits oscillating in a synchronized way. Some of these approaches include the Pecora-Carroll drive-response method [1], the continuous error-feedback method [2] and the impulsive synchronization method [3]. It should be noted that most of these techniques concern with the synchronization of low dimension systems characterized by only one positive Lyapunov exponent. Difficulties arising from the use of low dimension systems [6] have been recently overcome by adopting chaotic systems with multiple positive Lyapunov exponents, which can assure higher levels of security in communication systems [7–9]. In these works an increased level of security has been obtained for the considered systems, by applying proper cryptographic techniques to the information-bearing signals to be transmitted [10–13]. Concerning with the synchronization of high dimension chaotic circuits using a scalar signal, in [13] a cryptosystem has been proposed, which involves a traditional cryptographic technique to increase the randomness and unpredictability of the communications scheme. In particular, in [13] the transmitted scalar signal was obtained as a combination of proper nonlinear functions and encrypted signals. However, the use of nonlinear functions, both in the transmitting system and in the receiving one makes the whole system difficult to realize. Under the above considerations, in this paper a simpler technique to implement a cryptosystem based on the synchronization of chaotic circuits via a one-dimensional feedback signal is proposed. In particular, the transmitted signal is obtained as a linear combination of selected state variables of the transmitter and of encrypted signals via a squarewave characterized by a period $T$. At the transmitter, an alternating transmission of two different state variables and suitably encrypted signals is achieved. Then, at the receiver a proper linear feedback signal given by the difference between the transmitted signals and the corresponding state variables of the receiving...
system provides the proposed control action. The achieved chaotic synchronization via an “ad hoc” scalar transmitted signal enables a satisfactory recovering of the properly encrypted information-bearing signal. More in detail, chaotic circuits constituted by two bidirectionally coupled Chua’s oscillators are considered which are synchronized by means of the impulsive synchronization method proposed in [11]. Furthermore, the performance of the proposed chaotic cryptosystem is investigated in the presence of channel noise, by carrying out several simulations.

2 Synthesis of a nonlinear cryptosystem based on chaotic synchronization

2.1 Chaotic synchronization

In this section, a method for synchronizing two identical high dimension chaotic circuits via a scalar signal is developed. In particular, a unidirectional synchronization is considered in which one of the chaotic circuits, defined as the driving system, sends synchronization impulses to the other chaotic circuit, defined as the driven one. The basic chaotic circuit considered in this work is formed by a pair of bidirectionally coupled Chua’s oscillators. This circuit is characterized by the existence of a rich variety of dynamical behaviours, such as chaotic attractors [14]. The state equations of the two coupled Chua’s oscillators, constituting the driving system, can be written in dimensionless form as [9]:

\[
x(t) = Ax(t) + g(x)
\]

where

\[
x = [x_1, x_2, ..., x_6]^T \in \mathbb{R}^6
\]

\[
g(x) = [-\alpha g(x_1), 0, 0, -\alpha g(x_4), 0, 0]^T
\]

with \( g(x_i) = bx_i + (a-b)(|x_i+1|-|x_i-1|)/2, \) \( i = 1,4 \)

\[
A = \begin{bmatrix}
-\alpha & \alpha & 0 & 0 & 0 & 0 \\
1 & (-1-K) & 1 & 0 & K & 0 \\
0 & -\beta & -\gamma & 0 & 0 & 0 \\
0 & 0 & 0 & -\alpha & \alpha & 0 \\
0 & H & 0 & 1 & (-1-H) & 1 \\
0 & 0 & 0 & 0 & -\beta & -\gamma \\
\end{bmatrix}
\]

and \( \alpha, \beta, \gamma, a, \) and \( b \) are constants. The parameters \( K \) and \( H \), which characterize the bidirectional coupling between the two Chua’s oscillators, are chosen as \( K = H \) to obtain a symmetrical coupling.

In order to achieve the identical synchronization between the driving system and the driven one, a proper impulsive scalar signal has to be considered. In particular, the proposed impulsive synchronization signal, indicated with \( r(t) \in \mathbb{R} \), consists of two terms and is given by:

\[
r(t) = u(t)x_i(t) + u(t-T/2)x_d(t) \quad \forall t
\]

where \( u(t) \) is a squarewave characterized by peak values 0 and 1, and period \( T \) as reported in Fig.1.

![Time waveforms of the squarewaves](image)

Fig.1. Time waveforms of the squarewaves \( u(t) \) and \( u(t-T/2) \) and of the transmitted signal \( r(t) \).

The first half of each period \( T \) is devoted to the transmission of a sample of the chaotic signal \( x_i(t) \) of the driving system, whereas the second half of each \( T \) is devoted to the transmission of a sample of the chaotic signal \( x_d(t) \). In this way, samples of the signals \( x_i(t) \) and \( x_d(t) \) are alternatively transmitted to the driven system for \( T/2 \) time units. It should be noted that, by considering samples of the chaotic signals for \( T/2 \) time units, the length \( T \) of each time frame is fully utilized and a discontinuous synchronization signal is obtained, rather than a really impulsive one. This choice is optimal from a synchronization point of view when a scalar signal via a single transmission channel has to be transmitted.

By introducing a proper linear feedback control at the receiver, the state equations of the driven system can be written as:

\[
\dot{y}(t) = Ay(t) + g(y(t)) + M[U(Nr(t) - y(t))]
\]

(3)
where

\[ y = [y_1, y_2, ..., y_6]^T, \quad M = \text{diag}[M_{11}, 0, 0, M_{44}, 0, 0] \]

\[ U = \text{diag}[u(t), 0, 0, u(t-T/2), 0, 0], \quad N = [1, 0, 0, 1, 0, 0]^T \]

Being \( K = H \), a suitable choice for the elements of the feedback gain matrix \( M \) has been found to be \( M_{11} = M_{44} = M \). It should be noted that this scheme enables the application of two impulsive linear feedback signals to the driven system. In particular, given a generic period \( T \), the feedback signals are characterized by the following expressions:

- the signal applied to the first equation of the driven system is equal to \( M(x_1(t) - y_1(t)) \) and is different from zero only during the first half of \( T \);
- the signal applied to the fourth equation of the driven system is equal to \( M(x_4(t) - y_4(t)) \) and is different from zero only during the second half of \( T \).

By analyzing eqns.(3), it is worth noting that the stability of the driven system depends on the choice of the values of the feedback gain \( M \) and of the period \( T \). In order to assure the asymptotic stability of the driven system, after settling the values of the feedback gain \( M \), suitable values of \( T \in [0, +\infty[ \) have to be considered.

It is well known that, in the case of synchronization of identical chaotic circuits, for a chosen pair \((M, T)\) and for a chosen set of initial conditions, if all the Conditional Lyapunov Exponents (CLEs) of the driven system are negative, then system (3) is a stable response system and all the variables \( y_i(t) \) will converge asymptotically to all the corresponding variables \( x_i(t) \), or, equivalently,

\[ \lim_{t \to +\infty} \| \varepsilon_i(t) \| = 0 \]

### 2.2 Architecture of the proposed cryptosystem

A block diagram of the proposed chaotic cryptosystem, synchronized as described in the previous subsection, is reported in Fig.2. The state equations (1) of the two bidirectionally coupled Chua’s oscillators constitute the state equation of the driving system for the encrypter. As shown in Fig.2, the chaotic driving system in the encrypter generates the two chaotic keys \( k_1(t) = a_1 x_1(t) \) and \( k_4(t) = a_4 x_4(t) \), where the coefficients \( a_1 \) and \( a_4 \) are constants. The encryption functions \( c_i(m(t), k_i(t)) \) and \( c_d(m(t), k_d(t)) \) are alternatively used to encrypt the information-bearing signal \( m(t) \).
In particular, in order to encrypt the signal \( m(t) \), an \( n \)-shift cipher is chosen [10] to obtain the following two encryption functions:

\[ c_i(m(t), k_i(t)) = q \left( \ldots q \left( q \left( m(t), k_i(t) \right), k_i(t) \right), \ldots, k_i(t) \right) \quad i = 1, 4 \quad (4) \]

where

\[ q(m, k_i) = \begin{cases} 
(m + k_i) + 2h & -2h \leq m + k_i \leq -h \\
(m + k_i) - 2h & h \leq m + k_i \leq 2h \\
m + k_i & h < m + k_i < h
\end{cases} \quad i = 1, 4 \quad (5) \]

The function \( q(m, k_i) \) is the nonlinear function used for the encryption. It should be noted that the coefficient \( a_i \) has to be chosen in such a way that the generic \( k_i \) lies within \((- h, h)\) as shown in [12], where the generic nonlinear function \( q(m, k_i) \) has been plotted. Thus, the signal to be transmitted becomes:

\[ s(t) = u(t)[x_i(t) + c_i(m(t), k_i(t))] + u(t - T/2)[x_i(t) + c_i(m(t), k_i(t))] \quad \forall t \]

In this way, the first half of each time frame is devoted to the transmission of the chaotic signal \( x_i(t) \) generated by the driving system and added to the encrypted signal \( c_i(m(t), k_i(t)) \), whereas the second half of each time frame is devoted to the transmission of the chaotic signal \( x_i(t) \) generated by the driving system and added to the encrypted signal \( c_i(m(t), k_i(t)) \). Then, by transmitting the scalar signal \( s(t) \), the state equations (3) of the driven system in the decrypter can be rewritten as:

\[ \dot{y}(t) = Ay(t) + g(y(t)) + MU(Ns(t) - y(t)) \quad (6) \]

As in the case of chaotic synchronization reported in Section 2.1, this scheme enables the application of two distinct and impulsive feedback signals to the driven system. In particular, the signal appearing in the first equation of the driven system (6) is equal to \( M[x_i(t) + c_i(m(t), k_i(t))] - y_i(t) \) during the first half of each time frame, whereas it equals zero during the second half of each time frame. At the same time, the signal appearing in the fourth equation of the driven system (6) is equal to zero during the first half of each time frame, whereas it equals \( M[x_i(t) + c_i(m(t), k_i(t))] - y_i(t) \) during the second half of each time frame. Assuming that, for a chosen value of \( T \) and for a chosen set of initial conditions, all the conditional Lyapunov exponents of the driven system are negative, then system (6) is a stable response system and the \( y_i(t) \) variables converge asymptotically to the \( x_i(t) \) variables, that is:

\[ y_i(t) \rightarrow x_i(t), \quad i = 1, 4 \text{ when } t \rightarrow \infty \]

As synchronization between encrypter and decrypter is assured and being \( \tilde{k}_i(t) \rightarrow k_i(t), i = 1, 4 \), two decryption functions \( d_i(*, \cdot) \), \( i = 1, 4 \) corresponding to the encryption ones can be considered. Therefore, the information-bearing signal \( m_i(t) \) can be recovered in the following way:

\[ \begin{align*}
    m_i(t) &= d_i([s(t) - y_i(t)], -\tilde{k}_i(t)) u(t) + \\
                &\quad + d_i([s(t) - y_i(t)], -\tilde{k}_i(t)) u(t - T/2) \\
    &\quad + d_i([s(t) - y_i(t)], -\tilde{k}_i(t)) u(t - T/2) \\
    &\quad + d_i([s(t) - y_i(t)], -\tilde{k}_i(t)) u(t - T/2)
\end{align*} \]

where

\[ d_i([s(t) - y_i(t)], -\tilde{k}_i(t)) = q \left( \ldots q \left( q \left( s(t) - y_i(t), -\tilde{k}_i(t) \right), \ldots, -\tilde{k}_i(t) \right) \right) \quad \forall t \]

### 3 Simulation results

Numerical simulations have been carried out to illustrate the capability of the proposed approach. In particular, the following parameter values for both the encrypter and decrypter have been considered:

\[ \alpha = 10, \quad \beta = 14.87, \quad \gamma = 0.0385, \quad a = -1.27, \quad b = -0.68, \quad K = H = 0.25 \]

with the following set of non-null initial conditions:

\[ x_i(0) = 0.2, \quad x_d(0) = 0.25, \quad y_i(0) = -0.05, \quad y_d(0) = 0.1 \]

The above parameter values and initial conditions assure the existence of chaotic behaviour both for the encrypter and the decrypter. By choosing \( M = 25 \) as feedback gain and the value \( T = 0.001 \), the following conditional Lyapunov exponents of the decrypter have been found:

\[ \lambda_1 = -0.451, \quad \lambda_2 = -0.495, \quad \lambda_3 = -3.125 \]

\[ \lambda_4 = -5.015, \quad \lambda_5 = -22.505, \quad \lambda_6 = -32.051. \]

Since all the above exponents are negative, synchronization is assured between the encrypter and the decrypter. In particular, a 50-shift cipher
has been used together with two key signals characterized by the parameters $a_1=0.003$ and $a_4=0.002$ with $h=0.005$. Finally, the sinusoidal waveform $m(t)=A\sin(2\pi ft)$, with $A=0.001$, $f=50$ Hz has been considered as the information-bearing signal. Fig.3 shows the time behaviour of the synchronization errors $e_1(t)=y_1-x_1$ and $e_4(t)=y_4-x_4$, whereas in Fig.4 the time waveform of the recovered signal $m_r(t)$ is reported.

It can be noticed that, also in this case, synchronization is assured which, in its turn, guarantees a satisfactory recovery of the information signal.

Fig.3. Time behaviours of the synchronization errors $e_1(t)$ and $e_4(t)$.

Fig.4. Time waveform of the recovered signal $m_r(t)$

The noise effect on the chaotic cryptosystem has been analyzed by supposing that a zero mean Gaussian noise corrupts the channel. Then the robustness of the synchronization method has been tested by carrying out several simulations. In particular, in Fig.5 the time behaviours of selected variables of the synchronization errors $e_i(t)$ for $i=1,4,5$ with period $T=0.001$, feedback gain $M=25$, in the presence of zero mean Gaussian noise with standard deviation $\sigma=10^{-5}$, are reported.

4. Conclusions

In this paper a method to synthesize a nonlinear cryptosystem based on the synchronization of high dimension chaotic circuits via a one-dimensional signal has been proposed. The transmitted signal has been obtained as a linear combination of state variables and encrypted signals at the transmitter. The behaviour of the proposed cryptosystem has been investigated in the presence of channel noise and applied to bidirectionally coupled Chua's oscillators. Simulation results have shown a satisfactory performance of the proposed cryptosystem.

Acknowledgements

This work was partly supported by the Ministero dell’Università e della Ricerca Scientifica and partly by the Politecnico di Bari.

References:


