Observers based synchronization and input recovery for a class of nonlinear chaotic models.

Estelle Cherrier*,†, Mohamed Boutayeb†, and José Ragot*
*CRAN UMR CNRS 7039
INPL 2 Avenue de la Forêt de Haye
F-54516 Vandoeuvre-lès-Nancy Cedex, France
Email : cherrier@eavr.u-strasbg.fr, Jose.Ragot@ensem.inpl-nancy.fr
†LSIIT UMR CNRS 7005
ULP, Pôle API Bd S. Brandt - BP 10413
F-67412 Illkirch, France
Email : mohamed.boutayeb@ipst-ulp.u-strasbg.fr

***Abstract*— In this paper we propose a new cryptosystem, based on a new time-delayed chaotic system. Two chaotic signals are sent by the transmitter: the first one is aimed at synchronizing the receiver, which is proved through the resolution of a Linear Matrix Inequality (LMI). The transmission of a second chaotic signal enables the design of a new way to encrypt a message: we perform a kind of modulation of the frequency of a chaotic signal generated by the transmitter, depending on the message and we propose a method to recover the message. The efficiency of this new cryptosystem is illustrated by the encryption, transmission and recovery of a picture. The security of the proposed cryptosystem is discussed at the end of the article.**

I. Introduction

In this paper, we propose a new way to encrypt, send and decrypt a message, based on the fundamental properties of chaotic signals. This approach uses an observer-based scheme to ensure the synchronization of the receiver with the transmitter: this is performed with a first chaotic signal sent by the transmitter. Then we develop a new encryption method, which consists of a kind of modulation of the frequency of a second chaotic signal generated by the transmitter: the chaotic waveform is sent with a delay which depends on the information to encrypt. At the receiver, the message is recovered by estimating the delay which affects the second chaotic signal, compared with the corresponding signal estimated at the synchronization step.

A standard communication scheme consists of the addition of an information signal to a random carrier at the transmitter. The message is then recovered at the receiver. To realize this process, the receiver needs to know exactly the random carrier to subtract it from the transmitted signal, thus simply obtaining the information signal. In the case of a pseudo-random sequence generated as the carrier, the receiver must know exactly the initial conditions of the transmitter. The security of a standard communication scheme relies on the broadband power spectrum of the random carrier, since the spectral analysis of the transmitted signal does not reveal any information about the message, which is totally hidden in the pseudo-random noise.

Chaotic signals represent an alternative to this issue. Indeed, chaotic systems are particularly characterized by their extreme sensitivity to the initial conditions, they are deterministic but their trajectories look like noise, they have a continuous-like power spectrum [1]. Besides, the work of Pecora and Carroll [2] has opened the field of synchronization of chaotic systems. They showed that two identical chaotic systems, starting with different initial conditions, eventually synchronize, provided that they are coupled according to the *drive-response principle*. This pioneering work inspired the idea of using chaotic systems for communications [3], [4], [5]. The main advantage of using chaotic signals as carrier waveforms to transmit the message instead of classical random or sinusoidal carriers relies on their property of synchronization: two chaotic systems can synchronize without transmitting any information about the initial conditions of the transmitter, which makes them attractive from a security point of view.

The point here is to find an efficient (and secure) way to inject (or hide) the message into the transmitter (see [6], [7] for an overview on digital communications). Several schemes have been established in order to transmit a message in a secure way. The main difference in these designs lies in the methods for hiding or injecting the message at the transmitter, and recovering it at the receiver. Among these schemes, the most important are the following [8], [9].

- *Chaotic masking* [10]: the information signal is added to the output of the transmitter. The transmitted signal consists of this sum, and enables the receiver to synchronize with the transmitter: the reconstructed chaotic signal is then simply subtracted from the transmitted signal to obtain the information signal. However, the information signal has to be sufficiently small in comparison to the chaotic signal, to allow synchronization at the receiver.
- *Chaotic modulation or inverse system approach* [11]: the information signal modulates some parameter(s) of the chaotic encoder. After synchronization is achieved at the receiver, the reconstructed chaotic signal is applied

to the inverse encoder to obtain the information signal. These two schemes are the first that have been implemented, and suffer from a lack of security [12], [13], so some other schemes have been recently designed. To give a few examples, we can mention some new cryptosystems [14], [15], or [16]; a communication scheme based on the detection of parameter mismatch can be found in [17]; a new generation of chaotic synchronization schemes is developed in [18], based on the theory of impulsive differential equations; [19] proposes a modulation method with a nonlinear filter at the receiver; the chaotic carrier is modulated with an appropriately chosen scalar signal in [20]; some observer-based schemes are designed in [21], [22], [23] ... However, these schemes are not often analyzed from a security point of view, thus some attacks are possible, as in [24].

In contrast to these approaches, we propose a completely new (to our knowledge) method to transmit the message by sending two chaotic signals: one for the synchronization, and the second for the encryption. The chaotic transmitter is a new chaotic system, chosen for its noise-like trajectories. Furthermore, a parameter of the transmitter can be chosen as the key of our cryptosystem, which can guarantee a good level of security.

This paper is organized as follows. Section II details the different parts in the design of a cryptosystem: choice of the chaotic transmitter (section II-A), the synchronization problem (section II-B) and the encryption-decryption method (section II-C). The efficiency of our cryptosystem is tested in section III through the encryption, the transmission and the recovery of a picture, in simulations using Matlab. Section IV ends this paper with a study of the security of the proposed cryptosystem.

II. Design of a new cryptosystem

A. The transmitter: a new chaotic system

In [25], [26] we chose a modified Chua's circuit as the transmitter in our observer-based synchronization scheme. This system differs from the standard Chua's circuit in the sense that a time-delayed feedback has been added (see details in [27]). This process belongs to the recent technics of "anticontrol" of chaos: in [28] it is shown that a finite-dimensional, continuous-time, autonomous system can be driven from nonchaotic to chaotic, or that the chaos of an initially chaotic system can be enhanced. However, Chua's circuit has a piecewise-linear nonlinearity, which may not be desirable from a mathematical point of view. In [29] the piecewise-linear nonlinearity has been replaced by a polynomial of degree three, but it is said in this paper that the nonlinearity of Chua's circuit can be any scalar nonlinearity, provided that it is an odd function. So we propose a new chaotic system based on the dimensionless form of Chua's circuit (concerning the linear part), and the nonlinearity consists of an hyperbolic tangent and a time-delayed feedback:

$$\dot{x}(t) = Ax(t) + F\left(x(t)\right) + H\left(x(t-\tau)\right) \tag{1}$$

where

$$A = \begin{pmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix} \tag{2}$$

$$F(x(t)) = \begin{pmatrix} -\alpha\delta\tanh(x_1(t)) \\ 0 \\ 0 \end{pmatrix} \tag{3}$$

$$H(x(t-\tau)) = \begin{pmatrix} 0 \\ 0 \\ \varepsilon\sin(\sigma x_1(t-\tau)) \end{pmatrix} \tag{4}$$

We have chosen to keep the structure of the chaotic transmitter chosen in [25]. The system (1) is chaotic thanks to the presence of the time-delay feedback: if ε is chosen equal to zero, no chaotic behavior can be observed. The computation of the Lyapunov exponents [1] of (1) can ensure that this system is chaotic: this is beyond the scope of this paper, and will be discussed elsewhere (the smooth nonlinearity of the system enables the computation of these exponents).
The values of the parameters of (1) are chosen to ensure a chaotic behavior: $\alpha = 9$, $\beta = 14$, $\gamma = 5$, $\delta = 0.5$, $\varepsilon = 1000$, $\sigma = 10^5$, $\tau = 1$.

We provide the phase portrait of (1) in the plane $(x_1 - x_2)$ in Fig. 1, and Fig. 2 shows the chaotic attractor.

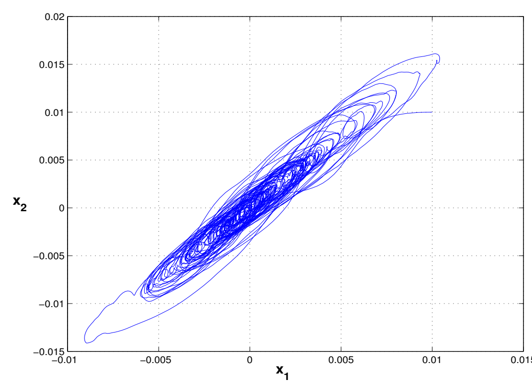

Fig. 1. Phase portrait in the plane $x_1 - x_2$

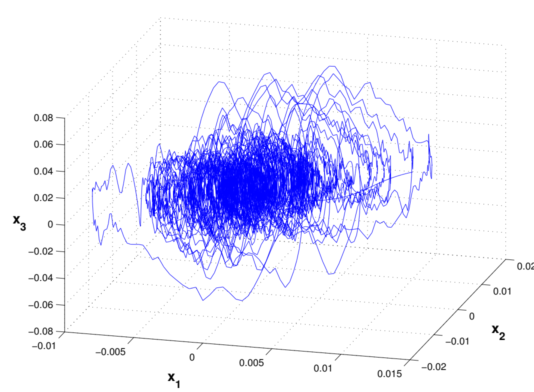

Fig. 2. A new chaotic attractor

Remark 1: We recall that a function f satisfies the Lipschitz property with constant k if there exists $k > 0$ such that

$$\|f(x) - f(y)\| \leq k\|x - y\| \ \forall \ x, y \tag{5}$$

(3) and (4) show that the nonlinear functions F and H satisfy the Lipschitz condition with respective constants $k_F = |\alpha\delta|$ and $k_H = |\varepsilon\sigma|$.

Remark 2: In a chaotic secure communication scheme, the chaotic system parameters play the key role in secure transmissions. The presence of the time-delay feedback adds further parameters that need to be known to recover the message, and thus enhances the security not only by enhancing the complexity of the chaos in the transmitter. We will see in section IV that the parameter σ can be considered as the key of our cryptosystem.

B. Observer-based synchronization

There are two main approaches to ensure the synchronization of a chaotic system. First, the *drive-response* principle was found by Pecora and Carroll in 1990 [2]. In this scheme, the transmitter is called the *drive system*, and the receiver is called the *response system*. The driving signal is usually some of the transmitter's state variables, and the response system is chosen as a part of the drive system. It has been shown that, if the conditional Lyapunov exponents [1] of the response system are all negative, synchronization occurs: the response system is forced by the drive signal, and it forgets its own initial conditions. The main limitation of this concept, is that the drive signal and the response system are obtained from the drive system, but there is no systematic procedure available to find a good decomposition of the drive system to ensure negative conditional Lyapunov exponents.

This approach is a kind of self-synchronization, and can be opposed to the second approach : the *observer-based synchronization* (see [30], [31]). Indeed, the problem of synchronization can be seen as a state estimation problem: given the chaotic transmitter, the receiver can be designed as an observer of this system. Then the receiver and the drive signal must check a property of detectability to ensure synchronization. Since this is a well-studied problem, several procedures are available to design the observer. Some observer-based concept to design synchronization schemes for chaotic systems can be found in the following papers: [32], [33], [21], [22], [23]. We have chosen an observer-based communication scheme, so we must determine an observer which synchronizes with (1).

Classically, to ensure the synchronization of the observer, the transmitter sends a chaotic signal, of the form:

$$y_1(t) = Cx(t) \tag{6}$$

We underline the fact that the synchronization step is completely separated from the encryption step (which will be detailed in section II-C), in particular the chaotic signal y_1 does not contain any information about the message.

In [25] and in [26] we have designed two observer-based synchronization schemes for a delayed Chua's circuit. Here we propose another observer-based approach, to deal with a large Lipschitz constant (*Remark 1* implies $k_H = 10^8$). For this purpose, we choose $C = \begin{pmatrix} 1 & \zeta & 0 \end{pmatrix}$ with $\zeta \ll 1$. We obtain

$$y_1(t) = x_1(t) + \zeta x_2(t) \tag{7}$$

The dynamic model of the transmitter (1) can be rewritten as:

$$\left\{ \begin{array}{rcl} \dot{x}(t) & = & \tilde{A}x(t) + \tilde{B}y_1(t) \\ & & +\tilde{F}(y_1(t), x_2(t)) + \tilde{H}(y_1(t-\tau), x_2(t-\tau)) \\ y_1(t) & = & Cx(t) \end{array} \right. \tag{8}$$

where

$$\tilde{A} = \begin{pmatrix} 0 & \alpha - \zeta & 0 \\ 0 & -(1+\zeta) & 1 \\ 0 & -\beta & -\gamma \end{pmatrix} \tag{9}$$

$$\tilde{B} = \begin{pmatrix} -\alpha \\ 1 \\ 0 \end{pmatrix} \tag{10}$$

$$\tilde{F}(y_1(t), x_2(t)) = \begin{pmatrix} \alpha\delta \tanh(y_1(t) - \zeta x_2(t)) \\ 0 \\ 0 \end{pmatrix} \tag{11}$$

$$\tilde{H}(y_1(t-\tau), x_2(t-\tau)) = \begin{pmatrix} 0 \\ 0 \\ \varepsilon \sin\left(\sigma(y_1(t-\tau) - \zeta x_2(t-\tau))\right) \end{pmatrix} \tag{12}$$

The dynamic model of the receiver is chosen of the following form:

$$\begin{array}{rl} \dot{\hat{x}}(t) = & \tilde{A}\hat{x}(t) + \tilde{B}y_1(t) + \tilde{F}(y_1(t), \hat{x}_2(t)) \\ & +\tilde{H}(y_1(t-\tau), \hat{x}_2(t-\tau)) + K(y_1(t) - C\hat{x}(t)) \end{array} \tag{13}$$

We define the synchronization error vector $e(t) = x(t) - \hat{x}(t)$, and its derivative is given by

$$\dot{e}(t) = A_K e + \tilde{F} - \hat{\tilde{F}} + \tilde{H} - \hat{\tilde{H}} \tag{14}$$

with the notations

$$\begin{array}{l} A_K = \tilde{A} - KC \\ \tilde{F} = \tilde{F}(y_1(t), x_2(t)) \\ \hat{\tilde{F}} = \tilde{F}(y_1(t), \hat{x}_2(t)) \\ \tilde{H} = \tilde{H}(y_1(t-\tau), x_2(t-\tau)) \\ \hat{\tilde{H}} = \tilde{H}(y_1(t-\tau), \hat{x}_2(t-\tau)) \end{array}$$

The following theorem provides a sufficient condition for the synchronization of the observer (13) with the transmitter (8).

Theorem 3: If the following conditions are verified:

1) the pair (A, C) is detectable;
2) there exist $k_1, k_2 > 0$, a matrix K and a symmetric, positive-definite matrix P solution of the following LMI (where I_3 denotes the identity matrix of dimension 3 and $A_K = A - KC$):

$$\zeta^2 k_H^2 - k_1 + 1 < 0 \tag{15}$$

$$\begin{pmatrix} A_K^T P + PA_K + k_1 I_3 & P \\ P & -\frac{1}{k_2} I_3 \end{pmatrix} < 0 \tag{16}$$

then (13) is an observer for (1): $\hat{x}(t) \to x(t)$ when $t \to \infty$.

Proof: The transmitter is a time-delay system, so it is classical to define a Lyapunov-Krasovskii functional

$$V = e^T P e + \xi \int_{-\tau}^{0} e(t+\theta)^T e(t+\theta) d\theta \quad (17)$$

where P is a symmetric, positive-definite matrix, and ξ is a positive scalar. It is easy to show that V is positive and upper bounded.

We compute the derivative of V along the trajectories of (14):

$$\begin{aligned} \dot{V} &= e^T \left(A_K^T P + P A_K\right) e + 2e^T P(\tilde{F} - \hat{\tilde{F}}) \\ &\quad +2e^T P(\tilde{H} - \hat{\tilde{H}}) + \xi e^T e - \xi e_\tau^T e_\tau \end{aligned} \quad (18)$$

with $e_\tau(t) = e(t-\tau)$.

The Cauchy-Schwarz and the Young inequalities applied successively, and the Lipschitz property of $\tilde{F}$ and $\tilde{H}$ lead to:

$$2e^T P(\tilde{F} - \hat{\tilde{F}}) \leq \zeta^2 k_F^2 e^T P P e + e^T e \quad (19)$$

and

$$2e^T P(\tilde{H} - \hat{\tilde{H}}) \leq e^T P P e + \zeta^2 k_H^2 e_\tau^T e_\tau \quad (20)$$

With (19) and (20), (18) leads to:

$$\begin{aligned} \dot{V} &\leq e^T \left(A_K^T P + P A_K + (1+\xi) I_3 + (1+\zeta^2 k_F^2) P^2\right) e \\ &\quad +(\zeta^2 k_H^2 - \xi) \|e_\tau\|^2 \end{aligned} \quad (21)$$

We set $k_1 = 1 + \xi$ and $k_2 = 1 + \zeta^2 k_F^2$. Then condition (15) implies $\zeta^2 k_H^2 - \xi < 0$, and (22) yields:

$$\dot{V} \leq e^T \left(A_K^T P + P A_K + k_1 I_3 + k_2 P^2\right) e \quad (22)$$

If condition (15) is checked, (22) reduces to

$$\dot{V} \leq -e^T W e \quad (23)$$

with $W = A_K^T P + P A_K + k_1 I_3 + k_2 P^2$.

To apply the Lyapunov theory, the matrix W must be negative-definite. The inequality $W < 0$ can be solved by applying the Schur complement:

$$\begin{aligned} & W < 0 \\ \Leftrightarrow & \left\{ \begin{array}{l} \begin{pmatrix} A_K^T P + P A_K + (1+\xi) I_3 & P \\ P & -\frac{1}{(1+\zeta^2 k_F^2)} I_3 \end{pmatrix} < 0 \\ -(1+\zeta^2 k_F^2) < 0 \end{array} \right. \end{aligned} \quad (24)$$

This demonstrates the condition (16), which can be solved numerically. If it is verified, the synchronization error vector e converges towards zero. ∎

Thus the synchronization step is achieved.

Remark 4:

The detectability of the pair $(\tilde{A}, C)$ is guaranteed by the fact that the matrix W is negative-definite (24).

Remark 5: In practice, to find a solution to the LMI (16), we must impose $\xi \leq 1$. Consequently, to satisfy (15), ζ is chosen such that $\zeta k_H < 1$.

C. A new encryption method

In this part, we detail a new way to encrypt a message. The aim is to transmit a chaotic signal which does not contain explicitly any direct information about the secret message. That is to say we use the most remarkable property of chaotic signals: they look like noise. So we intend to "hide" a message thanks to a chaotic signal, so that it is impossible to detect that a message is transmitted. Some attacks showed that chaotic masking or chaotic modulation are not secure enough [12], [13], [24], so we have designed a method for injecting the message which prevents it from altering the transmitted signal or its power spectral density.

We propose to send one of the chaotic signals generated at the transmitter (we do not use the signal y_1 that is sent for the synchronization of the receiver), with a delay depending on the message:

$$y_2(t) = x_3(t - \nu(u(t))) \quad (25)$$

$y_2(t)$ is obtained from the signal $x_3(t)$, deformed by a frequency modulation. So y_2 looks like noise too. In practice, we assume that $u(t) \in [0,1]$, and the function ν will be chosen as $\nu(u(t)) = T_u u(t)$, with $0 < T_u \leq T_e$ (where T_e will be the discretization step of the numerical integration of the differential equations) to enable the recovery of u.

The Taylor-Lagrange formula applied to x_3 is expressed as (all the functions involved are sufficiently smooth to apply this theorem):

Proposition 6 (Taylor-Lagrange):

$$\exists t_1 / x_3(t) - x_3(t - T_u u(t)) = \dot{x}_3(t) T_u u(t) - \frac{\ddot{x}_3(t_1)}{2} (T_u u(t))^2 \quad (26)$$

In practice $T_u \leq T_e \leq 10^{-2} \Rightarrow T_u^2 \leq 10^{-4}$. So, if we use the fact that a chaotic system has bounded trajectories, we can make the following first-order approximation:

$$x_3(t) - x_3(t - T_u u(t)) = x_3(t) - y_2(t) = \dot{x}_3(t) T_u u(t) \quad (27)$$

If we take a sufficiently small integration step $T_e \leq 10^{-2}$, since x_3 is chaotic, we assume that this signal is never constant (if this case would happen, it would be impossible to recover the delay between x_3 and y_2). That is why our encryption method well fits to chaotic signals. The inversion of equation (27) leads to (under the condition $\dot{x}_3(t) \neq 0$):

$$u(t) = \frac{x_3(t) - y_2(t)}{T_u \dot{x}_3(t)} \quad (28)$$

Now we use the fact that the synchronization step is completely separated from the encryption step: the recovery of the message u relies on the relation (28) and the dynamics of the receiver (13) (we note $K = (\kappa_1\ \kappa_2\ \kappa_3)$):

$$\begin{aligned} \hat{u}(t) &= \frac{\hat{x}_3(t) - y_2(t)}{T_u \dot{\hat{x}}_3(t)} \\ &= \frac{\hat{x}_3(t) - y_2(t)}{T_u(-\beta \hat{x}_2(t) - \gamma \hat{x}_3(t) + \varepsilon \sin(\sigma \hat{x}_1(t-\tau)) + \kappa_3(y_1(t) - \hat{x}_1(t) - \zeta \hat{x}_2(t)))} \end{aligned} \quad (29)$$

Remark 7: If it happens that $\dot{\hat{x}}_3(t) = 0$, then we use the Taylor-Lagrange formula (26) for an approximation at the second order, since the first and the second-order derivatives cannot be null at the same instant.

This second signal y_2 represents a new way to encrypt a signal, it performs a kind a modulation of the frequency of the chaotic signal x_3, so y_2 looks like noise too. We underline that there is no direct information sent through the channel from the transmitter to the receiver, so the security seems to be optimal. In short, the transmitter is used to synchronize the receiver and to encrypt the information signal, and these two processes can be treated in two separated steps. The efficiency of the decryption process relies on the efficiency of the synchronization. This will be illustrated on the example of section III.

III. Simulations

A. Synchronization

We propose here to test our cryptosystem with the famous "Lenna picture":

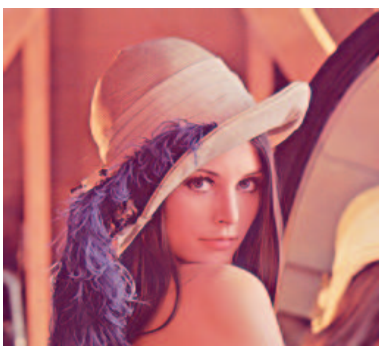

Fig. 3. Original Lenna picture

The synchronization error of each state component is plotted on Fig. 4 with a zoom on [0,1] seconds. The initial conditions chosen for the transmitter are $\begin{pmatrix} 0.01 & 0.01 & 0 \end{pmatrix}^T$ and for the receiver $\begin{pmatrix} 0.05 & 0.05 & 0.01 \end{pmatrix}^T$. The LMI (16) is solved with the following parameters and matrices (with rounded values):

$$P \simeq \begin{pmatrix} 4.03 & -1.38 & 0.29 \\ -1.38 & 1.85 & 0.16 \\ 0.29 & 0.16 & 0.41 \end{pmatrix}$$

$$K \simeq \begin{pmatrix} 32.16 \\ 26.91 \\ -28.45 \end{pmatrix}$$

and $\zeta = 10^{-9}$, $\xi = 1$, $k_1 = 2$, $k_2 \simeq 1$.
The signal $y_1(t)$ sent to the receiver for synchronization purpose is shown in Fig. 5.

B. Encryption-decryption

A discrete signal is generated from the Fig. 3: the colored picture is coded as three matrices (one for each basis color red, green, blue), whose coefficients are integers belonging to $[0, 255]$. The rows of the first matrix are concatenated, followed by the rows of the second and the third matrix, so we obtain a one-dimensional vector defining u. We normalize this vector so that all its components are in $[0, 1]$. We choose the integration step $T_e = 10^{-2}$ seconds. The vector u is used to modulate the chaotic signal x_3, and this defines the signal y_2, see Fig. 6.
We give the encrypted picture sent to the receiver in Fig. 7, and the recovered picture in Fig. 8. Some errors appear on

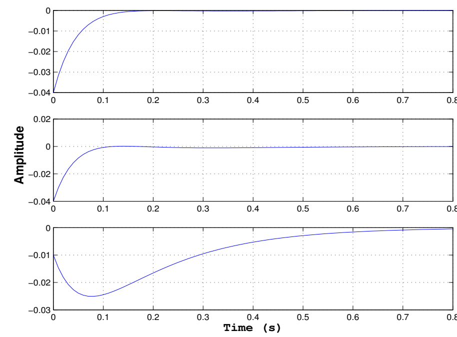

Fig. 4. Plots of the three synchronization errors

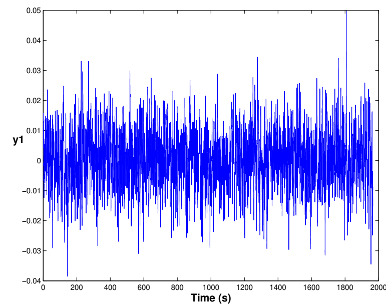

Fig. 5. Signal y_1 transmitted to synchronize the receiver

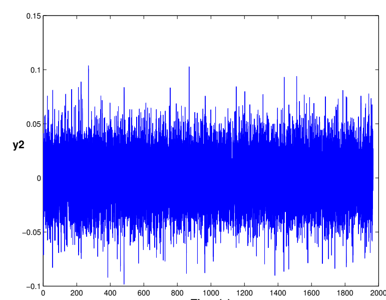

Fig. 6. Signal y_2 transmitted to encrypt and decrypt the message

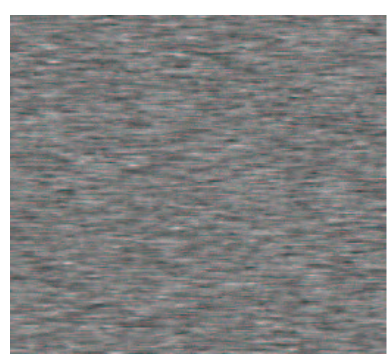

Fig. 7. Encrypted picture of Lenna

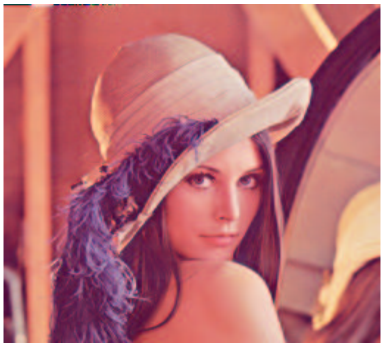

Fig. 8. Recovered picture of Lenna

the first points of the picture, this is due to the time necessary for the receiver to synchronize with the transmitter, which appears on the reconstruction error between u and $\hat{u}$ plotted on Fig. 9. This can be avoided by increasing the speed of

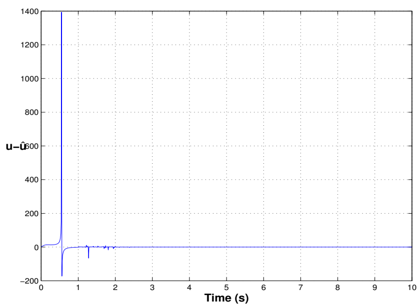

Fig. 9. Reconstruction error

convergence of the receiver, and by concatenating a useless signal before the information signal u, so the synchronization step will be achieved when the useful signal begins to be decrypted.

IV. Some security issues

Some papers [24] regret that the security aspects are not always discussed when a new cryptosystem is designed, so we intend to address this issue in this paragraph. In a chaotic cryptosystem, the security relies on a (the) parameter(s) of the system: it is assumed that, without the exact knowledge of the parameters of the transmitter, it is impossible to recover the encrypted message. However, this is not always the case, and some specific attacks have been designed to break chaotic encryption schemes in certain conditions (mostly concerning chaotic masking or parameter modulation).

The parameter σ can be considered as the key of our cryptosystem. We mentioned in section II-A that the chaotic behavior of the transmitter (1) relies on the presence of the time-delayed feedback (4), whose first and second components are zero, and the third component is defined by $h(x_1(t-\tau)) = \varepsilon \sin(\sigma x_1(t-\tau))$. Since x_1 is a chaotic signal, σ determines the speed of variation of the function h. If σ is sufficiently large, another value $\tilde{\sigma}$ will lead to a completely different behavior of the function h: the larger σ is, the more sensibility there is in that parameter.

Even if an intruder obtains the structure of the receiver and intercepts the signals y_1 and y_2 sent by the transmitter, if he does not know the value of σ (here $\sigma = 10000$) shared by the transmitter and the receiver, we can hope that he will not be able to decrypt the message. The Fig. 10 shows the deciphered message with an error of 0.01% on σ. The sensibility increases with the value of σ: if $\sigma = 10^6$, then a 0.001% mismatch produces the same effect.

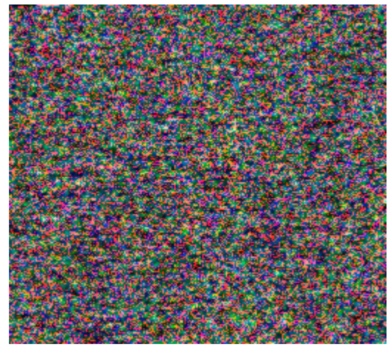

Fig. 10. Deciphering error with a 0.01% mismatch on σ

To quantify the sensibility of the deciphering as a function of the mismatch on σ, Fig. 11 shows the norm of the difference $u - \hat{u}$ divided by the total number of points in u as a function of the mismatch on σ (to cope with the errors due to the synchronization, we start the simulations with the same initial conditions for the transmitter and the receiver). Fig. 12

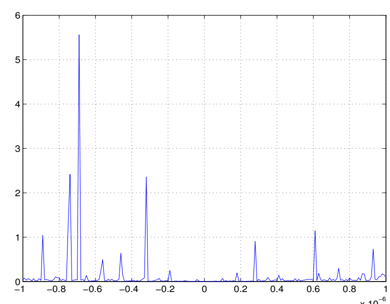

Fig. 11. Error rate of the deciphering vs. error rate of σ

shows a zoom on the amplitude of Fig. 11: the deciphering is exact only when the receiver exactly knows the value of σ.

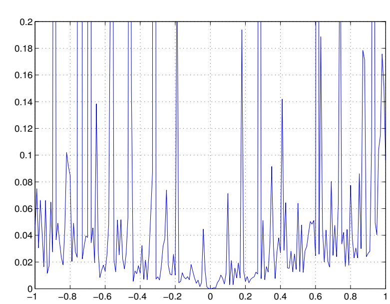

Fig. 12. Zoom in Fig. 11

Since the efficiency of our cryptosystem relies on the efficiency of the synchronization, our future work will be devoted to the analyze of the robustness of the synchronization towards some channel noise or delays, altering each of both transmitted signals y_1 and y_2. Besides, further analyses of the chaotic behavior of the transmitter may lead to an increase of the level of security.

V. Conclusion

In this paper we propose a new cryptosystem to send messages in a secure way. It relies on an observer-based synchronization scheme, and the transmitter is chosen as a new chaotic system. Two chaotic signals are sent to the receiver. The first signal is aimed at ensuring the synchronization of the receiver, and a second chaotic signal is sent by the transmitter, modulated by a variable delay depending on the secret message. We prove the synchronization through the resolution of a LMI, and we detail the encryption method in a discrete case: the message to be transmitted is the famous "Lenna picture". The encrypted and recovered pictures show the efficiency of our method, and we have shown that our cryptosystem possesses a secret key, which guarantees the security.

References

[1] S. Wiggins, *Introduction to applied nonlinear dynamical systems and chaos*. Springer-Verlag, 1990.

[2] L. Pecora and T. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, 1990.

[3] T. Carroll and L. Pecora, "Synchronizing chaotic circuits," *IEEE Trans. Circuit Syst.*, vol. 38, no. 4, pp. 453–456, 1991.

[4] 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.

[5] K. Cuomo, A. Oppenheim, and S. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuit Syst. II*, vol. 40, no. 10, pp. 626–633, 1993.

[6] G. Kolumbán, M. P. Kennedy, and L. O. Chua, "The role of rynchronization in digital communications using chaos - Part I : fundamentals of digital communications," *IEEE Trans. Circuit Syst. I*, vol. 31, pp. 927–936, 1997,

[7] ——, "The role of rynchronization in digital communications using chaos - Part II : chaotic modulation and chaotic synchronization," *IEEE Trans. Circuit Syst. I*, vol. 31, pp. 1129–1140, 1998.

[8] M. Hasler, "Engineering chaos for encryption and broadband communication," *Phil. Trans. R. Soc Lond. A*, vol. 353, pp. 115–126, 1995.

[9] ——, "Recent advances in the transmission of information using a chaotic signal," 1997, http://icwww.epfl.ch/publications/documents/IC-TECH-Report-199729.pdf.

[10] K.-Y. Lian and P. Liu, "Synchronization with message embedded for generalized lorenz chaotic circuits and its error analysis," *IEEE Trans. Circuit Syst. I*, vol. 47, no. 9, pp. 1418–1425, 2000.

[11] K. Halle, C. Wu, M. Itoh, and L. Chua, "Spread spectrum communication through modulation of chaos," *Int. J. Bifurc. Chaos*, vol. 3, no. 2, pp. 469–477, 1993.

[12] K. Short, "Steps towards Unmasking Secure Communications," *Int. J. Bifurc. Chaos*, vol. 4, no. 4, pp. 959–977, 1994.

[13] T. Yang, L.-B. Yang, and C.-M. Yang, "Breaking chaotic secure cmmunication using a spectrogram," *Phys. Lett. A*, vol. 247, pp. 105–111, 1998,

[14] T. Yang, C. Wu, and L. Chua, "Cryptography based on chaotic systems," *IEEE Trans. Circuit Syst. I*, vol. 44, no. 5, pp. 469–472, 1997,

[15] Z.-P. Jiang, "A note on chaotic secure communication systems," *IEEE Trans. Circuit Syst. I*, vol. 49, no. 1, pp. 92–96, 2002.

[16] M. Sobhy and A.-E.-D. Shehata, "Secure computer communication using chaotic algorithms," *Int. J. Bifurc. Chaos*, vol. 10, no. 12, pp. 2831–2839, 2000.

[17] T. Carroll and L. Pecora, "Cascading synchronized chaotic systems," *Phys. D*, vol. 67, pp. 126–140, 1993.

[18] T. Yang, "A survey of chaotic secure communication systems," *Int. J. of Comput. Cognition*, vol. 2, no. 2, pp. 81–130, 2004, message cod + code.

[19] N. Corron and D. Hahs, "A new approach to communications using chaotic signals," *IEEE Trans. Circuit Syst. I*, vol. 44, no. 5, pp. 373–382, 1997.

[20] S. Bu and B.-H. Wang, "Improving the security of chaotic encryption by using a simple modulating method," *Chaos, Solitons and Fractals*, vol. 19, pp. 919–924, 2004.

[21] T.-L. Liao and N.-S. Huang, "An observer-based approach for chaotic synchronization with applications to secure communications," *IEEE Trans. Circuit Syst. I*, vol. 46, no. 9, pp. 1144–1150, 1999.

[22] M. Boutayeb, M. Darouach, and H. Rafaralahy, "Generalized state-space observers for chaotic synchronization and secure sommunication," *IEEE Trans. Circuit Syst. I*, vol. 49, no. 3, pp. 345–349, 2002.

[23] G. Millerioux and J. Daafouz, "Global chaos synchronization and robust filtering in noisy context," *IEEE Trans. Circuit Syst. I*, vol. 48, no. 10, pp. 1170–1176, 2001.

[24] G. Alvarez and S. Li, "Cryptographic requirements for chaotic secure communications," 2003, http://arxiv.org/abs/nlin.CD/0311039.

[25] E. Cherrier and M. Boutayeb, "Observer-based approach for synchronization of modified chua's circuit," in *Proceedings of NOLCOS, IFAC Symposium on Nonlinear Control Systems, Stuttgart, Germany*, 2004.

[26] E. Cherrier, M. Boutayeb, and J. Ragot, "Observer-based approach for synchronization of a time-delayed chua's circuit," in *Proceedings of ISCAS, IEEE International Symposium on Circuit and Systems, Kobe, Japan*, 2005.

[27] X. Wang, G.-Q. Zhong, K.-S. Tang, K. Man, and Z.-F. Liu, "Generating chaos in Chua's circuit via time-delay feedback," *IEEE Trans. Circuit Syst. I*, vol. 48, no. 9, pp. 1151–1156, 2001.

[28] X. Wang, G. Chen, and X. Yu, "Anticontrol of chaos in continuous-time systems via time-delay feedback," *Chaos*, vol. 10, no. 4, pp. 771–779, 2000.

[29] M. Franz, "Chua's equation with cubic nonlinearity," *Int. J. Bifurc. Chaos*, vol. 6, pp. 2175–2222, 1996.

[30] H. Nijmeijer and I. Mareels, "An observer looks at synchronization," *IEEE Trans. Circuit Syst. I*, vol. 44, no. 10, pp. 882–890, 1997.

[31] O. Morgül and E. Solak, "Observer based synchronization of chaotic systems," *Physical Review E*, vol. 54, no. 5, pp. 4803–4811, 1996.

[32] G. Grassi and S. Mascolo, "Nonlinear observer design to synchronize systems via a scalar signal," *IEEE Trans. Circuit Syst. I*, vol. 40, no. 10, pp. 640–656, 1997.

[33] M. Feki, "Observer-based exact synchronization of ideal and mismatched chaotic systems," *Phys. Lett. A*, vol. 309, pp. 53–60, 2003.