OBSERVERS BASED SYNCHRONIZATION AND INPUT RECOVERY FOR A CLASS OF CHAOTIC SYSTEMS. APPLICATION TO IMAGE TRANSMISSION

Estelle Cherrier[†,‡]*, José Ragot*[†]*,*

[†] CRAN UMR 7039 / Nancy-Université, CNRS
2 Avenue de la Forêt de Haye
54516 Vandoeuvre-lès-Nancy Cedex FRANCE

Mohamed Boutayeb[‡]

[‡] LSIIT-UMR CNRS 7005
ENSPS, Bd Sébastien Brandt - BP 10413
67412 Illkirch FRANCE

ABSTRACT

This paper presents an image transmission as an application of a chaotic cryptosystem. The underlying problem concerns nonlinear state estimation and unknown input recovery. The proposed communication scheme 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 nonlinear state observer design, driven by the transmitted signal. The encryption is realized through phase modulation of a second chaotic signal, depending on the message. Efficiency of the proposed approach is shown through an image transmission.

1. INTRODUCTION

Chaotic systems belong to a particular class of nonlinear systems, known for its high complexity. The American mathematician Edward Lorenz discovered in 1970 that some nonlinear phenomena are so sensible to initial conditions -even if they are governed by deterministic rules- that their behavior is simply unpredictable. Chaotic systems are characterized by some properties:
▷ they are *deterministic* systems ;
▷ they have an extreme sensibility to initial conditions (also known as the *butterfly effect*) ;
▷ their asymptotic behavior is *aperiodic*.

Besides, synchronization phenomena have been reported since the XVIth century, when the Dutch mathematician Huygens observed the synchronization of two pendulum clocks placed against the same wall. In spite of this intrinsic long-term unpredictability which seems *a priori* very far from the definition of synchronization, Pecora and Carroll addressed the synchronization of chaotic systems in their pioneering paper [1], and established the *drive-response* principle. Then the issue of synchronization has been linked to a standard nonlinear state estimation problem. For a global view on chaos synchronization, the reader is referred to [2]. Among the potential applications of chaotic synchronization, chaotic cryptosystems seem rather promising, and became an intensive research field. Chaotic cryptosystems, also called secure communication systems, take advantage of intrinsic properties of chaotic systems and their ability to synchronize. A chaotic communication scheme follows the principle below:
▷ at the transmitter side, random-like chaotic signals (*i.e.* the transmitter's states) can be used to drown information ;
▷ an encrypted signal is then sent to the receiver ;
▷ at the receiver side, synchronization is achieved, which means that the receiver has estimated the states of the transmitter ;
▷ the decryption process uses the estimated states to recover the clear message.

Several methods of encryption have been designed, such as chaotic additive masking, chaotic shift keying, chaotic modulation.... Some techniques also use classical cryptography to elaborate more complicated cryptosystems. For an overview on the different methods developed in the literature, see reference [3]. We underline that chaos based encryption/decryption is a special issue belonging to unknown input recovery. In our previous paper [4] we proposed a cryptosystem based on chaotic synchronization and on a new masking method, illustrated by Fig. 1.

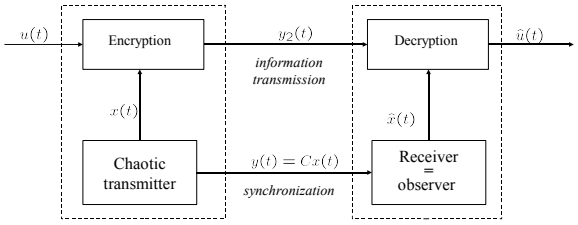

Fig. 1. Proposed cryptosystem

The layout of this paper is as follows. Section 2 is devoted to the description of the transmitter and the design of an observer allowing exponential synchronization. Section 3 details the encryption/decryption process, and section 4 illustrates the efficiency of the proposed cryptosystem through an image transmission.

2. SYNCHRONIZATION SCHEME

2.1. The chaotic transmitter

The transmitter is a chaotic system, whose dynamics involves a nonlinear delayed feedback:

$$\left\{\begin{array}{lcl} \dot{x}_1(t) &=& -\alpha x_1(t) + \alpha x_2(t) - \alpha\delta\tanh(x_1(t)) \\ \dot{x}_2(t) &=& x_1(t) - x_2(t) + x_3(t) \\ \dot{x}_3(t) &=& -\beta x_2(t) - \gamma x_3(t) + \varepsilon\sin(\sigma x_{1\tau}(t)) \end{array}\right. \quad (1)$$

This model can be rewritten in a more compact form as

$$\dot{x}(t) = Ax(t) + F(x(t)) + H(x(t-\tau) \quad (2)$$

where

$$A = \begin{pmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix} \quad (3)$$

$$F(x(t)) = \begin{pmatrix} -\alpha\delta\tanh(x_1(t)) \\ 0 \\ 0 \end{pmatrix} \quad (4)$$

$$H(x_\tau(t)) = \begin{pmatrix} 0 \\ 0 \\ \varepsilon\sin(\sigma x_1(t-\tau)) \end{pmatrix} \quad (5)$$

The presence of the time delay ensures a very complex chaotic behavior [5], which is highly desirable from a security point of view. The figure 2 shows one particular attractor of system (1), corresponding to the parameters values given in table 1.

α	β	γ	δ	ε	σ	τ
9	14	5	-0.5	100	10^4	1

Table 1. Transmitter's parameters

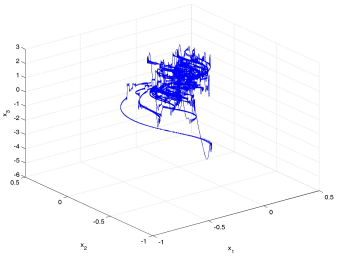

Fig. 2. Chaotic attractor

Once the transmitter has been chosen, the receiver has to be designed, so as to synchronize with it. We propose now an observer-based synchronization scheme, relying on nonlinear control theory. Before focusing on the observer synthesis, we need to transform the transmitter dynamic model. We precise that the transmitted signal is expressed as:

$$y(t) = Cx(t) \quad (6)$$

2.2. Transmitter model transformation

Owing to the fact that both nonlinear functions F and H, respectively defined in eq. (4) and (5), satisfy the Lipschitz condition with respective constants k_F and k_H, we intend to manage big values of these constants.
We propose to choose the following matrix C:

$$C = \begin{pmatrix} 1 & \zeta & 0 \end{pmatrix} \quad (7)$$

ζ being an arbitrary parameter. Then we deduce from (7):

$$x_1(t) = y(t) - \zeta x_2(t) \quad (8)$$

If we replace x_1 by its expression (8) in (**??**), we obtain the equivalent dynamic model of the transmitter:

$$\left\{\begin{array}{l} \dot{x}(t) = \tilde{A}x(t) + \tilde{B}y(t) + \tilde{F}(x(t), y(t)) + \tilde{H}(x_\tau(t), y_\tau(t)) \\ y(t) = Cx(t) \end{array}\right. \quad (9)$$

where

$$\tilde{A} = \begin{pmatrix} 0 & \alpha(1+\zeta) & 0 \\ 0 & -(1+\zeta) & 1 \\ 0 & -\beta & -\gamma \end{pmatrix} \quad (10)$$

$$\tilde{B} = \begin{pmatrix} -\alpha \\ 1 \\ 0 \end{pmatrix} \quad (11)$$

$$\tilde{F}(x(t), y(t)) = \tilde{F} = \begin{pmatrix} \alpha\delta\tanh(y(t) - \zeta x_2(t)) \\ 0 \\ 0 \end{pmatrix} \quad (12)$$

$$\tilde{H}(x_\tau(t), y_\tau(t)) = \tilde{H} = \begin{pmatrix} 0 \\ 0 \\ \varepsilon\sin\left(\sigma(y(t-\tau) - \zeta x_2(t-\tau))\right) \end{pmatrix} \quad (13)$$

Then we obtain upper bounds on Lipschitz constants $k_{\tilde{F}}$ and $k_{\tilde{H}}$ of new nonlinear function $\tilde{F}$ and $\tilde{H}$: $k_{\tilde{F}} \leq |\zeta| k_F$ and $k_{\tilde{H}} \leq |\zeta| k_H$.

In the rest of the paper, we omit the time variable t when unnecessary.

2.3. Nonlinear observer design

We choose a type of high-gain observer, whose dynamics is given by:

$$\dot{\hat{x}} = \tilde{A}\hat{x} + \tilde{B}y + \tilde{F}(\hat{x}, y) + \tilde{H}(\hat{x}_\tau, y_\tau) + K(y - C\hat{x}) \quad (14)$$

It can be rewritten as:

$$\dot{\hat{x}} = \tilde{A}\hat{x} + \tilde{B}y + \hat{\tilde{F}} + \hat{\tilde{H}} + K(y - C\hat{x}) \quad (15)$$

where we have noted $\hat{\tilde{F}} = F - \tilde{F}$ and $\hat{\tilde{H}} = H - \tilde{H}$. Now, it is aimed at finding a convenient gain K such that $\hat{x}$ converges towards x.
The synchronization error vector is defined by $e = x - \hat{x}$. Using (9) and (15), its dynamics is expressed as:

$$\dot{e} = A_K e + \tilde{F} - \hat{\tilde{F}} + \tilde{H} - \hat{\tilde{H}} \quad (16)$$

where

$$A_K = \tilde{A} - KC \tag{17}$$

The following theorem gives a sufficient condition of exponential synchronization of receiver (14) with transmitter (9).

Theorem 2.1. *If there exist two matrices P and Q, respectively symmetric positive-definite and positive definite, and a strictly positive real η such that the following BMI is feasible:*

$$\begin{pmatrix} \mathcal{R}(P,Q,K) & 0 & P \\ 0 & -e^{-2\eta\tau}Q + \rho I & 0 \\ P & 0 & -\frac{1}{\lambda} I_3 \end{pmatrix} \leq 0 \tag{18}$$

with

$$\mathcal{R}(P,Q,K) = (A-KC)^T P + P(A-KC) + \mu I_3 + Q + 2\eta P \tag{19}$$

and

$$\begin{array}{l} \mu = \zeta k_F \\ \rho = \zeta k_H \\ \lambda = \mu + \rho \end{array} \tag{20}$$

then the synchronization error vector converges exponentially towards zero, according to the formula:

$$\|e(t)\| \leq \sqrt{\frac{\alpha_1}{\alpha_2}} e^{-\eta t} \max_{\theta \in [-\tau, 0]} \|e(\theta)\| \tag{21}$$

with

$$\begin{array}{l} \alpha_1 = \lambda_M(P) + \tau \lambda_M(Q) \\ \alpha_2 = \lambda_m(P) \end{array} \tag{22}$$

Proof. We consider the following Lyapunov-Krasovskii functional:

$$V(e, e_\tau) = e^T P e + \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta \tag{23}$$

where we have chosen P symmetric, positive-definite, Q positive-definite, and $\eta > 0$.
The synchronization error vector norm converges exponentially towards zero if there exists $\phi > 0$ such that:

$$V(e, e_\tau) \geqslant 0 \tag{24a}$$

$$\dot{V}(e, e_\tau) \leq e^{-\phi t} \max_{\theta \in [-\tau, 0]} V'(e(0), e(\theta)) \tag{24b}$$

Since P and Q are positive-definite, condition (24a) is verified on account of the following inequalities:

$$\lambda_m(P)\|e(t)\|^2 \leq V(e, e_\tau) \leq (\lambda_M(P) + \tau\lambda_M(Q)) \max_{\theta \in [-\tau, 0]} \|e(\theta)\|^2 \tag{25}$$

The derivative of the functional V is obtained from (23):

$$\begin{array}{rcl} \dot{V} & = & \dot{e}^T P e + e^T P \dot{e} + e^T Q e - e^{-2\eta\tau} e_\tau^T Q e_\tau \\ & & -2\eta \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta \end{array} \tag{26}$$

Making use of (16), it yields to:

$$\begin{array}{rcl} \dot{e}^T P e + e^T P \dot{e} & = & e^T \left(A_K^T P + P A_K \right) e \\ & & + 2e^T P(\tilde{F} - \hat{\tilde{F}}) + 2e^T P(\tilde{H} - \hat{\tilde{H}}) \end{array} \tag{27}$$

Cauchy-Schwarz' and Young's inequalities lead to the following majoration of $\dot{V}$:

$$\dot{V} \leq \begin{pmatrix} e \\ e_\tau \end{pmatrix}^T \mathcal{M} \begin{pmatrix} e \\ e_\tau \end{pmatrix} - 2\eta \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta \tag{28}$$

where

$$\mathcal{M} = \begin{pmatrix} A_K^T P + P A_K + \lambda P^2 + \mu I + Q & 0 \\ 0 & -e^{-2\eta\tau} Q + \rho I \end{pmatrix} \tag{29}$$

and μ, ρ, λ are defined by eq. (20).
Now, V is rewritten to reveal the same structure as in (28):

$$V = \begin{pmatrix} e \\ e_\tau \end{pmatrix}^T \mathcal{N} \begin{pmatrix} e \\ e_\tau \end{pmatrix} + \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta \tag{30}$$

where

$$\mathcal{N} = \begin{pmatrix} P & 0 \\ 0 & 0 \end{pmatrix} \tag{31}$$

Then (28) and (30) lead to:

$$\dot{V} + 2\eta V \leq \begin{pmatrix} e \\ e_\tau \end{pmatrix}^T (\mathcal{M} + 2\eta\mathcal{N}) \begin{pmatrix} e \\ e_\tau \end{pmatrix} \tag{32}$$

Using the Schur complement, the inequality $\mathcal{M} + 2\eta\mathcal{N} \leq 0$ is equivalent to: (18), with $\mathcal{R}(P,Q,K)$ defined by (19). (18) is a bilinear matrix inequality (we recall that $A_K = A - KC$), owing to the presence of terms PK and $K^T P$. If this BMI is verified, then we deduce from (32):

$$\dot{V} \leq -2\eta V \tag{33}$$

By integration, it comes:

$$V(e, e_\tau) \leq e^{-2\eta t} \max_{\theta \in [-\tau, 0]} V(e(0), e(\theta)) \tag{34}$$

Consequently, condition (24b) is fulfilled, with $\phi = 2\eta$.
Besides, the left-hand side of inequality (25) gives:

$$\|e(t)\| \leq \sqrt{\frac{V(e, e_\tau)}{\lambda_m(P)}} \tag{35}$$

Taking (25), (34) and (35) into account, we get:

$$\|e(t)\| \leq \sqrt{\frac{\alpha_1}{\alpha_2}} e^{-\eta t} \max_{\theta \in [-\tau, 0]} \|e(\theta)\| \tag{36}$$

with α_1, α_2 defined by (22), which ends the demonstration of formula (21) and that of theorem 2.1. □

Now we give the observer gain synthesis procedure.

1. First, the parameter η must be chosen arbitrarily in $\mathbb{R}_+^*$.
2. The BMI (18) cannot be solved numerically. We proceed to a variable change, by setting $L = PK$. Then using (19), $\mathcal{R}(P,Q,K)$ can be rewritten as:

$$\begin{array}{l} \mathcal{R}(P,Q,K) = \mathcal{R}'(P,Q,L) = \\ A^T P + P A - C^T L^T - L C + \mu I_3 + Q + 2\eta P \end{array} \tag{37}$$

3. If we replace $\mathcal{R}(P,Q,K)$ by this expression (which is linear in P, Q and L), the BMI (18) is equivalent to the following LMI:

$$\begin{pmatrix} \mathcal{R}'(P,Q,L) & 0 & P \\ 0 & -e^{-2\eta\tau}Q+\rho I & 0 \\ P & 0 & -\frac{1}{\lambda}I_3 \end{pmatrix} \leq 0 \quad (38)$$

4. Standard convex optimization algorithms [6] can now be applied to find convenient matrices P, Q and L. If no solution appears, then η must be reduced, and the process goes back to step 1.

5. The observer gain is simply deduced from $K = P^{-1}L$.

3. ENCRYPTION/DECRYPTION METHOD

We propose a new way to hide the clear message inside a chaotic signal: the transmitter sends a second chaotic signal to the receiver, defined as:

$$y_2(t) = x_3\left(t - \theta(u(t))\right)) \quad (39)$$

The message $u(t)$ is used to modulate the phase of $x_3(t)$. The term $\theta(u(t))$ is equivalent to a variable and unknown delay that must be estimated to recover the clear message. In this paper, we choose

$$\theta(u(t)) = T_u u(t) \quad (40)$$

where T_u is an arbitrary constant, very small w.r.t. the time constant of system (1). After a first-order approximation of the Taylor formula, we obtain the following decryption formula (see [4] for more details):

$$\hat{u}(t) = \frac{\hat{x}_3(t) - y_2(t)}{T_u \dot{\hat{x}}_3(t)} \quad (41)$$

4. APPLICATION TO IMAGE TRANSMISSION

The simulation consists of an image transmission through the proposed cryptosystem. The picture is the famous Lena photography shown in Fig. 3. The images corresponding to the encrypted and the decrypted signals are represented respectively in Fig. 4 and 5.

Fig. 3. Lenna's photography

Fig. 4. Encrypted image

Fig. 5. Decrypted image

5. CONCLUSION

The problem addressed in this paper concerns chaotic cryptosystems. These communication processes use characteristic properties of chaos and synchronization principle. Relying on the transmission of two signals, the proposed cryptosystem efficiency had been illustrated by an image transmission. Further work can deal with the security level of our communication scheme.

6. REFERENCES

[1] L.M. Pecora and T.L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, pp. 821–824, 1990.

[2] S. Boccaletti, J. Kurths, G. Osipov, D.L. Valladares, and C.S. Zhou, "The synchronization of chaotic systems," *Physics Reports*, vol. 366, pp. 1–101, 2002.

[3] T. Yang, "A survey of chaotic secure communication systems," *Int. J. of Comput. Cognition*, vol. 11, no. 6, pp. 81–130, 2004.

[4] E. Cherrier, M. Boutayeb, and J. Ragot, "Observers based synchronization and input recovery for a class of nonlinear systems," *IEEE Transactions on Circuits and Systems I*, vol. 53, no. 9, pp. 1977–1988, 2006.

[5] J.D. Farmer, "Chaotic attractors of an infinite-dimensional dynamical system," *Physica D*, vol. 4, pp. 366–393, 1982.

[6] S. Boyd, L. ElGhaoui, E. Feron, and V. Balakrishnan, *Linear matrix inequalities in systems and control theory*, SIAM, Phildelphia, PA, 1994.