
Proceedings Paper:
Raoufi, R. and Zinober, A.S.I. (2006) Adaptive sliding mode observers in uncertain chaotic cryptosystems with a relaxed matching condition. In: Proceedings of the International IEEE Workshop on Variable Structure Systems. International Workshop on Variable Structure Systems VSS'06, 05-07 Jun 2006, Alghero, Italy. Institute of Electrical and Electronics Engineers , pp. 220-225. ISBN 1-4244-0208-5

https://doi.org/10.1109/VSS.2006.1644521

Proceedings of the 2006 International Workshop on Variable Structure Systems
Alghero, Italy, June 5-7, 2006

Adaptive Sliding Mode Observers in Uncertain Chaotic Cryptosystems with a Relaxed Matching Condition

R. Raoufi and A.S.I. Zinober

Department of Applied Mathematics, The University of Sheffield
Sheffield, U.K, e-mail: {R.Raoufi, A.Zinober}@shef.ac.uk

Abstract— **We study the performance of adaptive sliding mode observers in chaotic synchronization and communication in the presence of uncertainties. The proposed robust adaptive observer-based synchronization is used for cryptography based on chaotic masking modulation (CM). Uncertainties are intentionally injected into the chaotic dynamical system to achieve higher security and we use robust sliding mode observer design methods for the uncertain nonlinear dynamics. In addition, a relaxed matching condition is introduced to realize the robust observer design. Finally, a Lorenz system is employed as an illustrative example to demonstrate the effectiveness and feasibility of the proposed cryptosystem.**

I. Introduction

Chaos is a behaviour that lies between rigid regularity and randomness. There has been significant interest in using chaotic dynamics to realize secure communications and cryptography during the last two decades. There are several features of chaotic signals, which make them attractive for use in secure communication systems. Chaotic dynamics are noise-like but are deterministic with natural complexity, broad bandwidth and are aperiodic. Another attractive feature of chaotic signals is their high dependence on initial conditions; small changes can lead to dramatically different behaviour over a short time interval. Therefore, long-term prediction is practically impossible due to the sensitivity to the initial conditions. This feature is of interest in cryptography, where highly complex and hard-to-predict signals are employed. Moreover, chaotic signals are aperiodic and have a vanishing autocorrelation function, which makes the signals produced by different generators or even by the same generator with different initial conditions, appear to be uncorrelated. This aspect is important in multi-user communication applications.

Early work on the synchronization of chaotic systems by Pecora and Carroll [1] enforced trajectories of the slave chaos system tracking the same values as those of the master chaotic system. Most of the work in this area focused on synchronization of chaotic systems to recover information signals [2]-[10], [20] . Other methods include, controlling chaotic systems to follow a desired waveform in which a message is encoded [11], and making use of the quick decay of the correlation function for chaotic signals.

In a typical chaotic synchronization communication scheme the information to be transmitted is carried from the transmitter to the receiver by a chaotic signal through an analog channel. The decoding of the information signal in the receiver can be carried out by means of either coherent (synchronization) or non-coherent (without synchronization) demodulation schemes [11]-[14]. It is worthwhile noting that chaotic systems are highly sensitive to trivial perturbations and uncertainties. Mostly, these perturbations or uncertainties happen in the practical electronic realization. Therefore, very often we have an *uncertain* chaotic system. These trivial uncertainties can lead to radically different divergence in the near future behaviour of the chaos states.

This feature of high dependence to any uncertainties motivates the use of them intentionally to create chaotic behaviour much more secure for cryptography. The problem is to design a sufficiently robust synchronization scheme to guarantee the precise mimicry of chaotic systems in a master-slave configuration. A good candidate to achieve this goal is the use of robust sliding mode observer design methods for the uncertain nonlinear dynamics. In essence, the use of variable structure techniques in the state reconstruction of nonlinear systems has some advantages, like allowing the presence of matched uncertain elements in the model and convergence speed over other existing techniques like feedback linearization, extended linearization and traditional Lyapunov-based techniques [15]-[17]. Sliding mode observers (SMO) require the knowledge of a bounding function on the uncertainty but this will not be needed in our approach due to a built-in adaptation mechanism in the sliding mode filter.

In the present work we design an adaptive sliding mode observer (ASMO) for robust chaotic synchronization. It should be pointed out that some other well-known filters such as Extended Kalman Filters (EKF) or state dependent Riccati equation filters (SDRE) are not able to guarantee synchronization with the intentionally injected uncertainties in the chaos model. With this additional security level, we will show that an excellent solution is using robust sliding mode filters.

This paper is organized as follows. Section II briefly presents the application of chaotic behavior in cryptography and secure communication. A new scheme of secure communication, which can also be used as a cryptosystem, based on two identical adaptive sliding mode observers, will be presented in Section III. Section IV is devoted to an example illustrating the effectiveness of proposed configuration via Lorenz system. Section V concludes the paper.

The following notation will be used in the paper. $x \in R^n$

1-4244-0208-5/06/$20 ©2006 IEEE

denotes an n-vector of real elements with the associated norm $\|x\| \equiv \left(x^T x\right)^{1/2}$, $\lambda_{\min}(A)$ $(\lambda_{\max}(A))$ denotes the minimum (maximum) eigenvalue of a symmetric matrix $A(A \in R^{n\times n})$.

II. Chaos and Cryptography

Chaotic cryptosystems use a chaotic non-linear oscillator as a broadband pseudo-random signal generator. This signal is combined with the message to produce an unintelligible signal, transmitted through the insecure communication channel. At reception, the pseudo-random signal is regenerated, so that by combining it with the received signal through the inverse operation, the original message is recovered [18].

In Chaotic Masking Modulation (CM) the chaotic signal is added to the information signal and at the receiver the masking is removed. In order for this scheme to work properly, the receiver must synchronize robustly with a small perturbation in the driving signal due to the addition of the message. The power level of the information signal should be much lower than that of the chaotic signal to bury it effectively [18]. Another technique for chaotic modulation is based on switching which is more suitable for binary communication. Chaotic switching systems or chaos shift keying (CSK) is more robust against noise than chaotic masking. However, its transmission rate is much lower than CM modulation.

In the direct modulation scheme the information signal is multiplied by a chaos-based spread spectrum noise signal. The transmission rate of this method is much higher than the CSK and CM schemes [18]. It is worth noting that this method has a significant higher security level.

III. Proposed Chaotic Cryptosystem via Adaptive Sliding mode Observer Design

A. Robust adaptive sliding mode observers in chaos synchronization

The use of variable structure techniques in the state reconstruction of nonlinear uncertain systems is shown in [19] to have some advantages such as allowing the presence of matched uncertain elements in the model and faster convergence speed over other existing techniques. The security of the chaotic modulation can be significantly enhanced by intentionally adding matched unknown disturbance to the states, which will make it more difficult for a party, intending to intercept the information, to recover the information accurately. Non-adaptive sliding observers require the knowledge of a bounding function on the uncertainty. this not be essential in our approach, due to a built-in adaptation mechanism in the filter for the estimation of the upper bound of the intentionally injected uncertainties.

For the adaptive sliding mode observer we will discuss an uncertain class of chaotic system. This model can be used in CM, direct modulation and CSK schemes. We point out the capability of the robust adaptive observer to handle disturbances, as these have shown to be a challenge for other observers. It should be pointed out that the extra degree of robustness or insensitivity is very useful in chaotic systems applications, as they are super-sensitive to perturbations in the initial conditions and parameters; especially, in our case since we intend to add unknown perturbed signals to the chaotic system to make it much more unpredictable.

B. Uncertain chaos system model and robust adaptive observer design

Consider the following nonlinear chaotic system model in the presence of uncertainty

$$\dot{x} = Ax + f(x,t) + B\xi(y,t) \tag{1}$$

$$y = Cx \tag{2}$$

where $x \in R^n$, $y \in R^r$, $\xi(y,t) \in R^m$ represents the uncertainties and $t \in R^+$. $f(x(t),t)$ is the nonlinear part of the system. The triple (A,B,C) has appropriate dimensions. We make the following assumptions:

(A) (A,C) is assumed to be detectable and observable so that there exists an observer gain $K \in R^{n\times p}$ such that $A_0 = A - KC$ is a strictly Hurwitz matrix.

(B) The unknown disturbance $\xi(y,t)$ is bounded (but unknown)

$$\|\xi(y,t)\| < \rho \tag{3}$$

(C) The following Lyapunov equation has a positive solution P for a positive definite matrix $Q = Q^T > 0$

$$A_0^T P + PA_0 = -Q \tag{4}$$

(D) The known nonlinearity $f(x,t)$ satisfies a Lipshitz condition

$$\|f(x_1,t) - f(x_2,t)\| \le \gamma \|x_1 - x_2\| \tag{5}$$

where $x_1, x_2 \in R^n, \gamma \in R^+$ is a known positive constant.

(E) *Matching condition with unmatched uncertainty distance* [21]: In many applications, satisfying the classical matching condition $B = P^{-1}C^T$ by finding appropriate matrices K and Q to satisfy simultaneously the LE equation (4) and the classical matching condition is very restrictive. Therefore, introducing the matching condition with unmatched uncertainty distance is a more relaxed condition to design the adaptive robust observer. So, we assume that

$$\Gamma = B - \beta P^{-1}C^T, \|\Gamma\| \le \varepsilon \tag{6}$$

where β is a positive parameter. The unmatched distance is $\|\Gamma\| \le \varepsilon$ and if ε is very small, the stability of the system can be ultimately achieved. We will use the following robust ASMO to reconstruct the system states from the measurement $y(t)$

$$\dot{\hat{x}}(t) = A\hat{x}(t) + f(\hat{x}) + Ke(t) + S(\hat{x}(t), y(t), \hat{\rho}(t)) \tag{7}$$

where $e(t)$ is the estimation error defined as

$$e(t) = x(t) - \hat{x}(t)$$

$S(\hat{x}(t), y(t))$ is the sliding mode adaptive gain of the observer which is calculated from

$$S(\hat{x}(t), y(t), \hat{\rho}(t)) = \hat{\rho}(t)\beta P^{-1}C^T \frac{Ce}{\|Ce\|} \tag{8}$$

for $\|Ce\| \neq 0$, our improved adaptive algorithm can be chosen as

$$\dot{\hat{\rho}}(t) = \eta(\|Ce(t)\| - \eta_0\hat{\rho}(t)),\ \eta, \eta_0 \geq 0 \tag{9}$$

To prove the stability of the adaptive sliding mode observer (7)-(9), consider the following Lyapunov function candidate

$$V(e(t), \bar{\rho}(t)) = e^T Pe + \eta^{-1}\beta\bar{\rho}^2(t) \tag{10}$$

where

$$\bar{\rho}(t) = \rho - \hat{\rho}(t)$$

The evolution of the estimation error is

$$\dot{e}(t) = A_0 e - S(\hat{x}, y, \rho(t)) + B\xi(y,t) + f(x,t) - f(\hat{x},t)$$

the derivative of $V(e(t), \bar{\rho}(t))$ is evaluated along the $e(t)$ and $\bar{\rho}(t)$

$$\begin{aligned}
\dot{V} &= e^T(A_0^T P + PA_0)e + 2e^T P(B\xi(y,t) \\
&\quad -S(\hat{x}, y, \rho(t))) + 2e^T P(f(x,t) - f(\hat{x},t)) \\
&\quad + 2\eta^{-1}\beta\bar{\rho}(t)(-\dot{\hat{\rho}}(t) \\
&= -e^T Qe + 2e^T P(f(x,t) - f(\hat{x},t)) + 2e^T P\Gamma\xi(y,t) \\
&\quad + 2e^T C^T\beta\xi(y,t) - 2\hat{\rho}(t)\beta\frac{e^T C^T Ce}{\|Ce\|} \\
&\quad + 2\eta^{-1}\beta\bar{\rho}(t)(-\dot{\hat{\rho}}(t)) \\
&< -(\lambda_{\min}(Q) - 2\gamma\lambda_{\max}(P))\|e\|^2 \\
&\quad + 2\beta\|Ce\|(\rho - \hat{\rho}(t)) \\
&\quad + 2\|e\|\|P\|\varepsilon\rho + 2\eta^{-1}\beta\bar{\rho}(t)(-\dot{\hat{\rho}}(t))
\end{aligned}$$

By using the adaptive law (9) one obtains

$$\begin{aligned}
\dot{V} &< -(\lambda_{\min}(Q) - 2\gamma\lambda_{\max}(P))\|e\|^2 \\
&\quad + 2\|P\|\varepsilon\rho\|e\| + 2\beta\eta_0(\rho - \hat{\rho}(t))\hat{\rho}(t) \\
&< -(\lambda_{\min}(Q) - 2\gamma\lambda_{\max}(P))\|e\|^2 \\
&\quad + 2\|P\|\varepsilon\rho\|e\| - 2\beta\eta_0(\frac{1}{2}\rho - \hat{\rho}(t))^2 + \frac{2\beta}{4}\eta_0\rho^2 \\
&< -(\lambda_{\min}(Q) - 2\gamma\lambda_{\max}(P))\|e\|^2 \\
&\quad + 2\|P\|\varepsilon\rho\|e\| + \frac{2\beta}{4}\eta_0\rho^2 \\
&< -(\lambda_{\min}(Q) - 2\gamma\lambda_{\max}(P) - 1)\|e\|^2 \\
&\quad + (\|P\|\varepsilon\rho)^2 + \frac{1}{4}\eta_0\rho^2
\end{aligned}$$

Negative definiteness of $\dot{V}$ is obtained for

$$\|e(t)\| \geq \kappa = \sqrt{\frac{(\|P\|\varepsilon\rho)^2 + \frac{\beta}{2}\eta_0\rho^2}{\lambda_{\min}(Q) - 2\gamma\lambda_{\max}(P) - 1}} \tag{11}$$

if the following design condition

$$\lambda_{\min}(Q) \geq 2\gamma\lambda_{\max}(P) + 1 \tag{12}$$

is satisfied. Therefore, the state error trajectory enters the closed ellipsoid and remain there

$$\Omega = \{e \in R^n | V(e(t)),\ \hat{\rho}(t)) \leq \lambda_{\max}(P)\kappa^2\} \tag{13}$$

the ultimate stability of the designed ASMO is guaranteed.

Remark 1. Practically, we can use the following continuous sliding control instead of equation (8)

$$S(\hat{x}(t), y(t), \hat{\rho}(t)) = \hat{\rho}(t)P^{-1}C^T\beta\frac{Ce}{\|Ce\| + \delta} \tag{14}$$

with

$$0 < \delta \ll 1$$

This yields a continuous approximation of the signum function to eliminate high frequency chattering.

Remark 2. In the modified adaptation law (9), the parameter η_0 should be chosen suitably small $0 \leq \eta_0 \ll 1$ by the designer. η_0 prevents $\hat{\rho}(t)$ from becoming too large and quarantees suitable magnitude of the adaptive gain.

C. The proposed chaos communication scheme

We, now propose a new chaotic communication scheme based on adaptive sliding mode observers in the presence of uncertainties. In the transmitter module a chaotic system is employed as the master to generate a chaotic driver signal for synchronization via the output measurement signal. To enhance significantly the security level of the new scheme, an unknown perturbation signal $\xi(y,t)$ is constructed from the output measurement is intentionally injected into the chaotic dynamics. Practically, all the states of a chaotic system can not be measured. To remedy this problem, an ASMO is used in the transmitter section to generate all the states of the main chaotic encrypter. It should be pointed out that the ASMO (7)-(9) is sufficiently robust to estimate all the states despite the uncertainties. Subsequently, modulation schemes such as CM, CSK, etc can be easily designed based on the state estimate. In this paper, we consider only chaotic masking modulation (CM). The proposed scheme is illustrated in Figure 1. The information signal $s(t)$ is masked with the second state estimate in the transmitter section. The actual first state of the chaotic system, the output measurement $y(t)$, is transmitted through a communication channel, which may be not secure, to the receiver section. The hidden information signal $c(t)$ is transmitted through another insecure channel to the receiver section as well. The ASMO is employed in the receiver module to estimate the states of the master chaotic system via the received measurement signal. It should be emphasized that the receiver observer is identical to the one designed in the transmitter module. When synchronization is achieved, the masking modulation can be removed precisely using the second state estimate in the receiver section.

Remark 3. In practical applications it may be unrealistic to implement the exact identical sliding mode coupled observer in a transmitter-receiver configuration. Therefore there could be an undesired error between the states estimates of the robust observers. The mismatched error can be modelled by an additive perturbation ΔK on one of the observers gain. It should be noticed that the additive gain perturbation simultaneously influences the matching condition (refer to assumptions (C) and (E)). On the other hand, in spite of the hardware perturbation, it is obvious that both implemented

observers obey the ultimate error upper bound (11) if the conditions (4) and (12) are satisfied. Consequently

$$\sup\left(\|\hat{x}_{\text{Transmitter}} - \hat{x}_{\text{Receiver}}\|\right) = 2\kappa$$

Subsequently, one can obtain the following ultimate recovery data error

$$\sup\left(|s_R(t) - s(t)|\right) \leq 2\kappa \tag{15}$$

Remark 4. In should be emphasized that the state adaptive robust observers can be synchronized to the master chaotic driver system in spite of different initial conditions. Furthermore, the difference due to the initial values of the observers practically imposes transient error in the data recovery until the synchronization is achieved.

IV. Simulation Example

As an example consider the following chaotic model is called the Lorenz attractor

$$\dot{x}(t) = \begin{bmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ -x_1 x_3 \\ x_1 x_2 \end{bmatrix} + B\xi(y,t)$$
$$y = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} x$$

where σ, r, b are positive parameters. When $\sigma = 10, r = 28$ and $b = 1.25$, the above system behaves chaotically [1]. The available output is chosen to be the first state x_1. The structure of the intentional injected uncertainty (which is completely unknown in receiver section) is chosen as

$$B = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \ \xi(y,t) = \sin(y)\cos(5t)$$

By choosing the matrices

$$Q = 100 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \ K = \begin{bmatrix} 10 \\ 100 \\ 1 \end{bmatrix}$$

the solution of LE equation (4) yields

$$P = \begin{bmatrix} 2.7059 & 0.4118 & -0.0133 \\ 0.4118 & 20.3475 & 0.2423 \\ -0.0133 & 0.2423 & 40.0106 \end{bmatrix}$$

and the eigenvalues of $A_0 = A - KC$ are -1.2500, -10.5000 ± 25.0948i. If we select $\beta = 2.7$, then according to the relaxed matching condition (6)

$$\Gamma = \begin{bmatrix} -0.0009 \\ 0.0203 \\ -0.0005 \end{bmatrix}$$

Therefore the unmatched distance is $\varepsilon = 0.0203$ which is sufficiently small to achieve acceptable ultimate stability. The above design procedure is valid since the Lipshitz constant γ satisfies the inequality (12)

$$\gamma \leq 1.2371$$

Finally, using the above parameters and equations (7)-(9) with $\eta = 5$, the ASMO can be properly designed to achieve the robust adaptive synchronization in the presence of intentional injected uncertainty signal. It is assumed that $\Delta K = 0$, $\eta_0 = 0.001$. It should be pointed out that the encryption rule has been chosen as

$$c(t) = s(t) + \hat{x}_2(t)$$

where $s(t) = 2\sin(2\pi 5t)$ is the actual data (message) and $c(t)$ is the encrypted data. Figure 2 depicts the three dimensional plot of the Lorenz attractor. The actual states and their estimates are shown in Figure 3. Figure 4 illustrates the adaptive gain of the employed sliding mode state estimators. The actual data is plotted in Figure 4. Figure 5 shows the encrypted signal. The recovered data and the error of data recovery are depicted in Figures 6 and 7 respectively. Obviously, the recovered data implies the effectiveness of the proposed scheme.

V. Conclusion

This paper proposes a new practical secure communication scheme using the concept of adaptive sliding mode observer design. An uncertain signal is intentionally injected into the chaotic driver to enhance the security level of the overall system. The robust synchronization is based on an ASMO. A relaxed matching condition is used to make the design procedure more realizable.

References

[1] L.M. Peccora and T.L. Carroll, Synchronization in Chaotic Systems, Phys. Rev. Lett., vol.64,pp. 821–824, Feb. 1990.

[2] Tao Yang and L.O. Chua, L.O, Impulsive stabilization for control and synchronization of chaotic systems: theory and application to secure communication, IEEE Transaction on Circuit and Systems, I–Fundamental Theory and Applications, vol. 44, pp.976–988, 1997.

[3] L. Kocarev, K.S. Halle, K. Eckert and L.O. Chua, Experimental demonstration of secure communication via chaotic synchronization, Int. J. Bifurcation & Chaos, vol. 2, pp.709–713, 1992.

[4] M. Hasler and Y. Maistrenko, An Introduction to the Synchronization of Chaotic Systems: Coupled Skew Tent Maps, IEEE Trans. Circuits and Sys., vol. 44, pp. 856–866, Oct. 1997.

[5] H. Nijmeijer, and I.M.Y. Mareels, An observer looks at synchronization, Circuits and Systems I: Fundamental Theory and Applications, vol. 44, pp. 882–890, Oct. 1997.

[6] G. Kolumban, M. P. Kennedy and L. Chua, The Role of Synchronization in Digital Communications Using Chaos–Part II: Chaotic Modulation and Chaotic Synchronization, IEEE Trans. Circuits and Sys., vol. 45, pp. 1129–1139, Nov. 1998.

[7] V. Rubezic and R. Ostojic, Synchronization of chaotic Colpitts oscillators with applications to binary communications, Proceedings of ICECS '99. vol. 1, pp. 153-156, Sept. 1999.

[8] Teh-Lu Liao and Nan-Sheng Huang, An observer-based approach for chaotic synchronization with applications to secure communications, Circuits and Systems I: Fundamental Theory and Applications, vol. 46, pp. 1144–1150, Sept. 1999.

[9] Amirazodi, J., E.E. Yaz, A. Azemi and Y.I. Yaz, Nonlinear observer performance in chaotic synchronization with application to secure communication, Proceedings of the 2002 International Conference on Control Applications, vol. 1, pp. 76–81, Sept. 2002.

[10] K.M. Cuomo and A.V. Oppenheim, Circuit implementation of synchronized chaos with applications to communication, Phys. Rev. Lett., vol. 71, pp. 65–68, 1993.

[11] S. Hayes, C. Grebogi and E. Ott, Communicating with chaos, Phys. Rev. Lett., vol. 70, pp. 30313034, 1993.

[12] K. Murali and M. Lakshmanan, Transmission of signals by synchronization in a chaotic Van der Pol-Duffing oscillator, Phys. Rev. E, vol. 48, pp. 271–350, 1993.

[13] K. Murali, Digital signal transmission with cascaded heterogeneous chaotic systems, Phys. Rev. Letter, vol. 63, pp. 217–223, 2001.

[14] M.P. Kennedy and G. Kolumban, Digital communications using chaos, Signal Processing, vol. 80, pp. 1307–1320, 2000.

[15] W. Baumann, and W. Rugh, Feedback control of non-linear systems by extended linearization, IEEE Trans. Autom. Control, vol. 31, pp. 40-47, 1986.

[16] D. Bestle and M. Zeitz, Canonical form observer design for nonlinear time-variable systems, Int. J. Cont., vol. 38, pp. 419-431, 1983.

[17] A.J. Krener, and W. Respondek, Nonlinear observer with linearizable error dynamics, SIAM J. Control Optim., vol. 23, pp. 197-216, 1985.

[18] G. Alvarez, F. Montoya, G. Pastor and M. Romera, Chaotic Cryptosystems, IEEE Transaction, Int. J. Bifurc. Chaos, pp. 332–338,1999.

[19] B.L. Walcott, M.J. Corless and S.H. Zak, Comparative study of nonlinear state-observation technique, Int. J. Control, vol. 45, pp. 2109-2132, 1997.

[20] R. Raoufi and H. Khaloozadeh, A Modified Robust Adaptive Chaos Synchronization, Proc of International Conference on Signal Processing & Communication(SPCOM), pp. 76–80, 2004.

[21] A. J. Koshkouei and A. S. I. Zinober, Sliding mode observation for non-linear systems, Int. J. Control, vol.77, pp. 118–127, 2004.

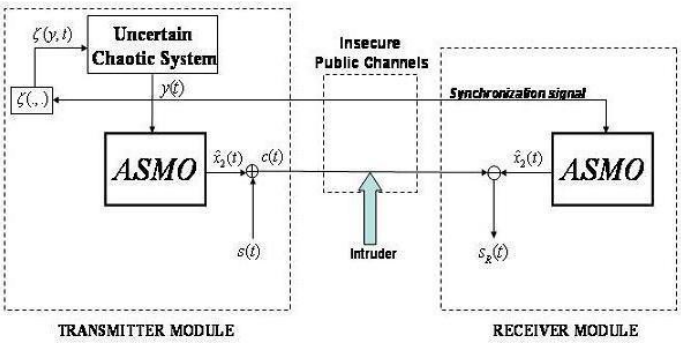

Fig. 1. The proposed chaotic communication scheme based on ASMO

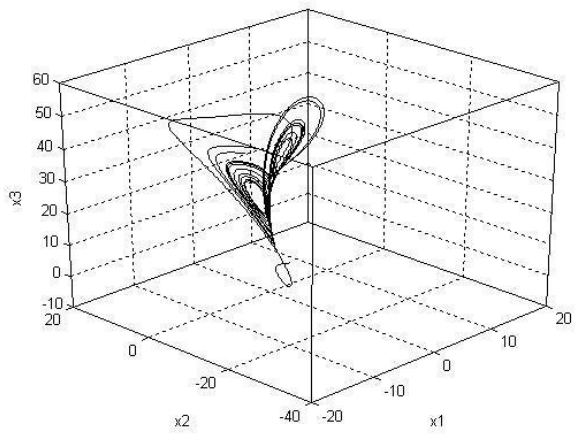

Fig. 2. The Lorenz attractor

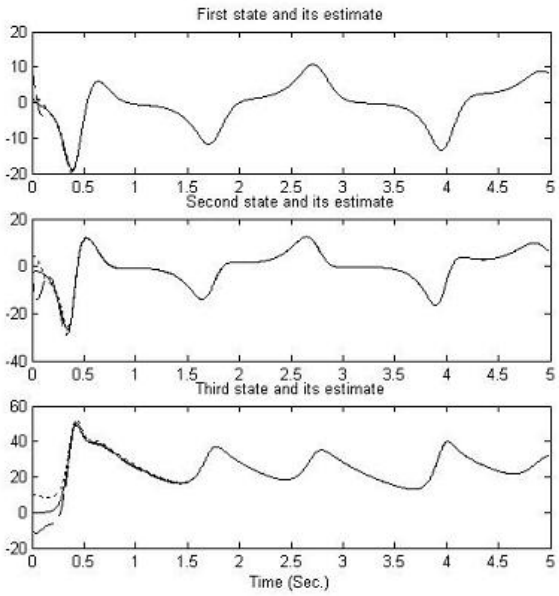

Fig. 3. Actual states and their estimates

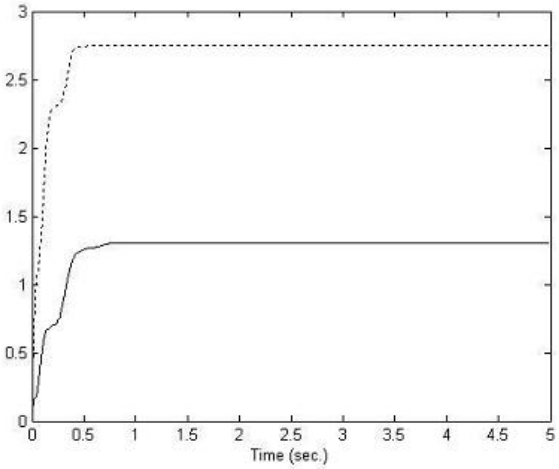

Fig. 4. Adaptive gains

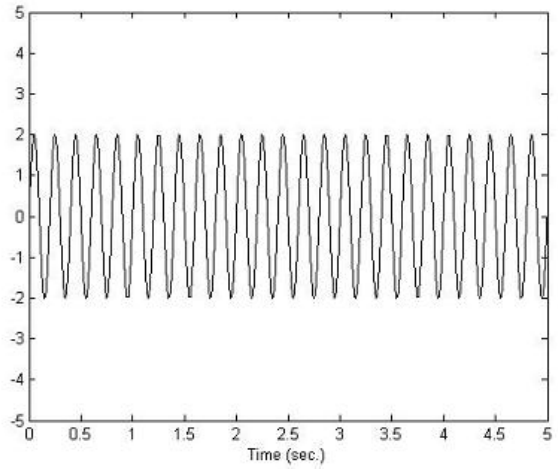

Fig. 5. Actual message

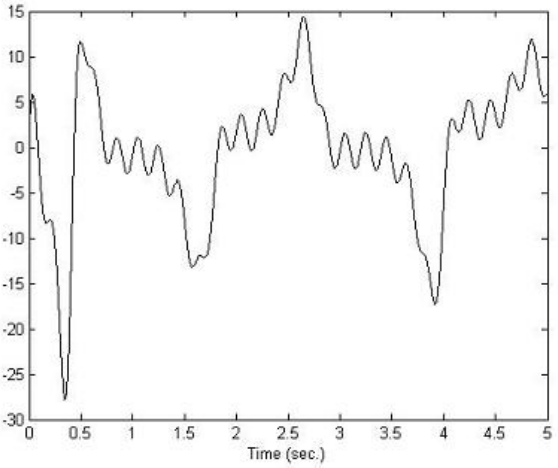

Fig. 6. Encrypted message

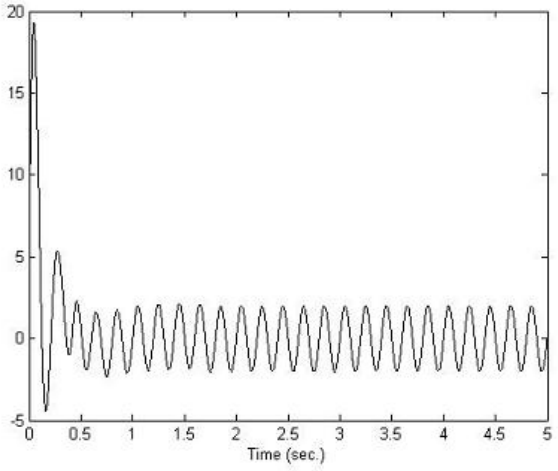

Fig. 7. Recovered message

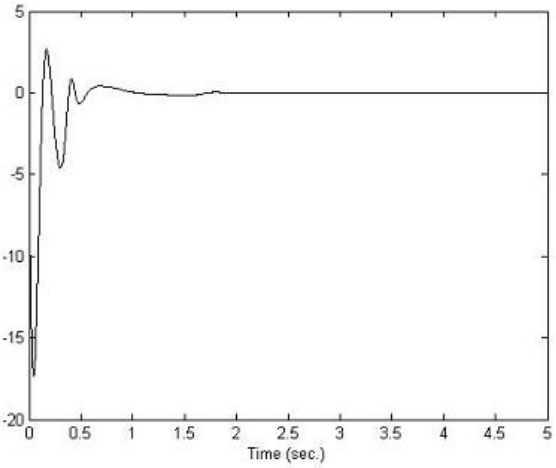

Fig. 8. Data recovery error