Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

Robust Chaotic Cryptosystems Based on T-S Fuzzy Model

Gwo-Ruey Yu

Department of Electrical Engineering, National Ilan University
Ilan City, Taiwan (e-mail: gwoyu@niu.edu.tw).

Abstract: This paper presents the robust design for chaotic cryptosystems. The cryptosystem combines cryptograph with chaotic synchronization. The hyperchaotic signals are synchronized between the encrypter and the decrypter based on observer gains. The technique of linear matrix inequality (LMI) is applied to determine the observer gains. A theorem has been proposed to guarantee the robust stabilization for the chaotic synchronization system with external disturbance. Furthermore, the disturbance attenuation level is minimized such that the cryptosystems are optimally robust. Computer simulation demonstrates that the effectiveness of the robust design.

1. INTRODUCTION

Since the internet and mobile phone are worldwide, the synchronization of chaotic system and its application to secure communication have received considerable attentions (Duan *et al*., 1997, Yang *et al*., 1997, Liao *et al*., 1999, Lian *et al*., 2000, Lian *et al*., 2001). Chaotic systems are situated between deterministic systems and stochastic systems. The pioneering work of Pecora *et al*. (1990) and Carroll *et al*. (1991) have led to many studies regarding the synchronization of two chaotic systems (Chen *et al*., 1998, Lakshmanan *et al*., 1996). There are a lot of researches in investigating chaos-based secure communications.

Various methods have been developed to hide the plain texts of the message using chaotic signals, for instance, chaotic switching (Kilic *et al*., 2001, Tada *et al*., 2006)**,** chaotic modulation (Chen *et al*., 2005, Sathyan *et al*., 2006) and chaotic masking (Alvarez *et al*., 2004, Murali *et al*., 2003). To improve the problems of chaos-based secure communication systems, the cryptography are introduced to the encrypter. In this paper, the plain text is first encrypted by cryptography and then it is masked with a chaotic signal such that the level of security is enhanced.

Fuzzy controller has been widely used in industry for its easy realization and good robustness. Takagi and Sugeno (2001) proposed a fuzzy model to represent a nonlinear system. There are two ways for establishing fuzzy models. One is represented by fuzzy IF-THEN rules that describe input-output relations of a nonlinear system. The other is derived from given dynamic equations. In this paper, the T-S fuzzy model is obtained by using local approximation in fuzzy partition spaces. Herein, the Lorenz's equation is represented as the T-S fuzzy model via choosing linear terms.

An observer is designed to achieve the chaos synchronization between the transmitter and the receiver. In the observer scheme, each control rule is designed from the corresponding rule of the T-S fuzzy model (El Hajjaji *et al*., 2006). The observer shares the same fuzzy sets with the fuzzy model in the premise parts. By the way, the stability criterion is derived for the chaos-based cryptosystem under external disturbance. In this paper, the robust observer gains are designed via LMI techniques.

The remainder of this paper is organized as follows. Section 2 discusses the synchronization cryptosystem based on T-S fuzzy model. Section 3 provides computer simulation to demonstrate the effectiveness of the design. Section 4 gives the conclusions.

2. DESIGN OF CHAOTIC CRYPTOSYSTEMS BASED ON T-S FUZZY MODEL

First, we represent chaotic systems using T-S fuzzy model. The main feature of a T-S fuzzy model is to express the local dynamics of each fuzzy implication by linear subsystems. The T-S fuzzy model is achieved by fuzzy blending of the linear subsystem. Fig. 1 shows the structure of chaos-based cryptosystem. It consists of the encrypter (the drive chaotic system and an encryption function) and decrypter (the response chaotic system and a decryption function). The proposed design framework includes five parts.

Part 1: The drive chaotic systems with external disturbances are considered.

Drive model rule i:

IF y(t) is M_i, THEN

$$\dot{x}_d(t) = A_i x_d(t) + D_i v(t)$$

$$y_d(t) = C x_d(t), \qquad i = 1, 2, \ldots, r \tag{1}$$

where M_i are fuzzy sets, r is the number of fuzzy rules, $x_d \in \Re^{n\times 1}$ is the state vector of the drive chaotic system, and $y_d(t)$ is a scalar signal, which transmitted through a public channel.

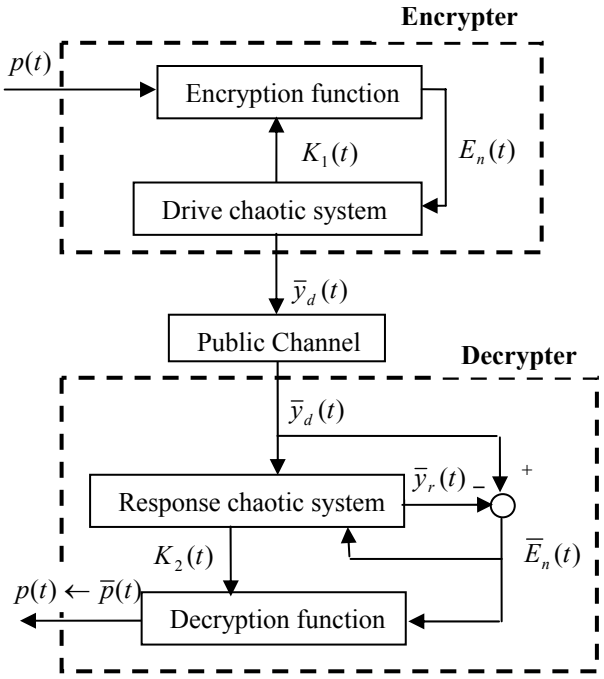

Fig.1. Chaos-based cryptosystem.

$A_i \in \Re^{n\times n}$ and $C \in \Re^{1\times n}$ are system matrices and output matrices; $v \in \Re^{n\times p}$ denotes the external disturbance with an upper bound; and $D_i \in \Re^{n\times m}$ is the disturbance injection matrix.

By utilizing the singleton fuzzifier, product fuzzy inference, and weighted average defuzzifier, the defuzzified output of the T-S fuzzy model (1) is inferred as follows:

$$\begin{aligned} x_d(t) &= \sum_{i=1}^{r} h_i(y(t))(A_i x_d(t) + D_i v(t)) \\ y_d(t) &= C x_d(t) \end{aligned} \tag{2}$$

where

$$\begin{aligned} &h_i(y_d(t)) = w_i(y_d(t)) \Big/ \textstyle\sum_{i=1}^{r} w_i(y_d(t)) \\ &h_i(y_d(t)) \geq 0 \\ &\sum_{i=1}^{r} h_i(y_d(t)) = 1 \end{aligned}$$

with $w_i(y_d(t)) = M_i(y_d(t))$ for all t.

Part 2: Given the drive chaotic system (1), we have obtained the response system as follow:

Response model rule i:

IF $y_d(t)$ is M_i, THEN

$$\begin{aligned} \dot{x}_r(t) &= A_i x_r(t) + L_i(y_d(t) - y_r(t)) \\ y_r(t) &= C x_r(t), \qquad i = 1, 2, \ldots, r \end{aligned} \tag{3}$$

where $x_r \in \Re^{n\times 1}$ is the state vector of the response chaotic system, y_d is the output of the response chaotic system, $L_i \in \Re^{n\times 1}$ are the observer gains to be designed later. The defuzzification process is given as

$$\begin{aligned} \dot{x}_r(t) &= \sum_{i=1}^{r} h_i(y_d(t))(A_i x_r(t) + L_i(y_d(t) - y_r(t))) \\ y_r(t) &= C x_r(t) \end{aligned} \tag{4}$$

Part 3: Assumed a signal of plain text $p(t)$, the cipher signal is defined by

$$E_n(t) = E_n(p(t), K_1(t)) \tag{5}$$

where $K_1(t)$ is a key signal that recovered in the response chaotic system. $E_n(.)$ is a generic encryption function that makes use of a key signal $K_1(t)$ (Yang *et al.*, 1997). According to symmetric algorithms, that is, using the same key signal for encryption and decryption functions, we could retrieve the plaintext signal from the cipher signal $E_n(t)$

$$p(t) = D_e(E_n(t), K_2(t)) \tag{6}$$

where $K_2(t)$ is a key signal that recovered in the response chaotic system. $D_e(.)$ is a generic decryption function. Since the key signals are recovered from the chaotic systems, they are assumed that

$$K_1(t) = K_1(x_d(t)) \tag{7}$$

$$K_2(t) = K_2(x_r(t)) \tag{8}$$

Part 4: By taking the drive chaotic system (1), the cipher signal (5), and the key signal (7), we have obtained the fuzzy encrypter by the following rules:

Encrypter model rule i:

IF $\bar{y}_d(t)$ is M_i, THEN

$$\begin{aligned} \dot{\bar{x}}_d(t) &= (A_i \bar{x}_d(t) + D_i v(t) + L_i E_n(t)) \\ \bar{y}_d(t) &= C\bar{x}_d(t) + E_n(t), \qquad i = 1, 2, \ldots, r \end{aligned} \tag{9}$$

where $\bar{y}_d(t)$ is the transmitted signal which embedded in the cipher signal $E_n(t)$. The overall fuzzy encrypter can be inferred as

$$\dot{\bar{x}}_d(t) = \sum_{i=1}^{r} h_i(\bar{y}_d(t))(A_i \bar{x}_d(t) + D_i v(t) + L_i E_n(t)) \tag{10}$$

$$\bar{y}_d(t) = C\bar{x}_d(t) + E_n(t) \tag{11}$$

It is necessary to generate the key signal at the response chaotic system for retrieving the plaint signal. Therefore, the

chaos synchronization between encrypter and decrypter must be guaranteed. The decrypter is derived using the technique of fuzzy observer design.

Part 5: Given the response chaotic system (3) and the encrypter (9), the fuzzy decrypter can be obtained by the following rules

Decrypter model rule i:

IF $\bar{y}_d(t)$ is M_i, THEN

$$\begin{aligned}\dot{\bar{x}}_r(t) &= A_i\bar{x}_r(t) + L_i(\bar{y}_d(t) - \bar{y}_r(t))\\ \bar{y}_r(t) &= C\bar{x}_r(t), \qquad i = 1, 2, \ldots, r\end{aligned} \tag{12}$$

The overall fuzzy decrypter is inferred as

$$\dot{\bar{x}}_r(t) = \sum_{i=1}^{r} h_i(\bar{y}_d(t))(A_i\bar{x}_r(t) + L_i(\bar{y}_d(t) - \bar{y}_r(t))) \tag{13}$$

$$\bar{y}_r(t) = C\bar{x}_r(t) \tag{14}$$

Hence, the recovered cipher signal is

$$\bar{E}_n(t) = \bar{y}_d(t) - \bar{y}_r(t). \tag{15}$$

Let the error signal be $e_x(t) = \bar{x}_d(t) - \bar{x}_r(t)$. Taking the previous considerations into account, (12) has to be designed such that $\bar{x}_r(t)$ converges to state $\bar{x}_d(t)$ as $t \to \infty$. These two chaotic systems are synchronized between the encrypter and decrypter, that is, $e_x(t) \to 0$ as $t \to \infty$. The decrypter (12) could be treated as an observer of encrypter (9). Since $e_x(t) = \bar{x}_d(t) - \bar{x}_r(t)$ and from (10) and (13), the following equation can be obtained:

$$\dot{e}_x(t) = \sum_{i=1}^{r} h_i(\bar{y}_d(t))(A_i - L_iC)e_x(t) + D_iv(t) \tag{16}$$

Then, the error of the cipher signal can be described as

$$e_{En}(t) = \bar{E}_n(t) - E_n(t) = Ce_x(t) \tag{17}$$

Lemma: The chaotic control system will be globally asymptotically stable if there exists a common positive definite matrix P such that

$$G_{ii}^{\ T}P + PG_{ii} \le 0 \tag{18}$$

$$\left(\frac{G_{ij}+G_{ji}}{2}\right)^T P + P\left(\frac{G_{ij}+G_{ji}}{2}\right) \le 0, \tag{19}$$

By exploiting Lyapunov stability criterion and LMI theory, the following theorem presents a fuzzy observer design for disturbance attenuation of the Takagi-Sugeno fuzzy model.

Proposition: Consider the error dynamics system (16) and (17), the disturbance rejection can be realized by minimizing γ subject to

$$\sup_{\|v(t)\|_2 \ne 0} \|e_{En}(t)\|_2 / \|v(t)\|_2 \le \gamma \tag{20}$$

Theorem: The error dynamics system described by (16) and (17) is globally asymptotically stable if there exist a common positive definite matrix P, observer gains L_i such that

$$\begin{aligned}&\underset{S_i,P}{\text{minimize}}\ \gamma^2\\ &\begin{bmatrix} A_i^TP - C^TS_i^T + PA_i - S_iC + C^TC & PD_i \\ D_i^TP & -\gamma^2 I \end{bmatrix} \le 0,\end{aligned} \tag{21}$$

where $S_i = PL_i$.

Thus, the observer gains and the minimization γ can be determined by solving (21) based on LMI technology.

3. SIMULATION RESULTS

This paper uses Lorenz's equations for the chaos-based cryptosystem. The nonlinear Lorenz's mathematical equations are defined as follows:

$$\begin{cases}\dot{x}_1(t) = a(x_2(t) - x_1(t)) + u(t)\\ \dot{x}_2(t) = cx_1(t) - x_2(t) - x_1(t)x_3(t)\\ \dot{x}_3(t) = x_1(t)x_2(t) - bx_3(t)\end{cases} \tag{22}$$

where a, b, and c are constants.

Let the Lorenz's equations be represented as T-S fuzzy model (9). The premise variable of fuzzy set rules is chosen as $\bar{y}_d(t)$, which satisfies $\bar{y}_d(t) \in [-d \quad d]$ and $d > 0$. The two membership functions of fuzzy sets are designed as $M_1(\bar{y}_d(t)) = \frac{(1 + \bar{y}_d(t)/d)}{2}$ and $M_2(\bar{y}_d(t)) = \frac{(1 - \bar{y}_d(t)/d)}{2}$, respectively. Fig. 2 show the membership functions of fuzzy sets. The state vector of the encrypter is defined as $\bar{x}_d = [\bar{x}_{d1}(t) \quad \bar{x}_{d2}(t) \quad \bar{x}_{d3}(t)]^T$. The system matrices are

$$A_1 = \begin{bmatrix} -a & a & 0 \\ c & -1 & -d \\ 0 & d & -b \end{bmatrix},$$

$$A_2 = \begin{bmatrix} -a & a & 0 \\ c & -1 & -d \\ 0 & -d & -b \end{bmatrix}.$$

The output matrix is $C = [1 \quad 0 \quad 0]^T$, the disturbance injection matrices are $D_1 = D_2 = [1 \quad 0 \quad 0]^T$. Moreover, the decrypter can be described as (12), the state vector of the decrypter is $\bar{x}_r = [\bar{x}_{r1}(t) \quad \bar{x}_{r2}(t) \quad \bar{x}_{r3}(t)]^T$.

After several iterations, we obtain the minimized value $\gamma = 0.27$. The positive definite matrix and the observer gains for $\gamma = 0.27$ are

$$P = \begin{bmatrix} 0.3945 & -0.2471 & 0 \\ -0.2471 & 0.6328 & 0 \\ 0 & 0 & 0.4561 \end{bmatrix},$$

$$L_1 = \begin{bmatrix} 36.2714 \\ 23.5081 \\ 11.3492 \end{bmatrix},$$

$$L_2 = \begin{bmatrix} 36.2714 \\ 23.5081 \\ 11.3492 \end{bmatrix}.$$

The values of these parameters are $a = 8$, $b = 5/3$, $c = 21$ and $d = 15$. The initial states of the encrypter and decrypter are $\bar{x}_d(0) = [3 \quad 4 \quad 5]^T$ and $\bar{x}_r(0) = [-3 \quad -4 \quad -5]^T$. In order to encrypt the plain signal, a mod chipper is chosen as

$$E_n(t) = 0.5(p(t) + (30K_1(t)) \bmod (7)) \tag{23}$$

where $p(t) = 2\sin(2\pi t)$. For the sake of simplicity, the key signal $K_1(t) = \bar{x}_{d1}(t)$ has been chosen, although any generic function $K_1(\bar{x}_d(t))$ could be utilized. Then, the decryption function can be written as

$$\bar{p}(t) = 2\bar{E}_n - (30K_2(t) \bmod (7)) \tag{24}$$

where the key signal $K_2(t) = \bar{x}_{r1}(t)$.

The validity of proposed cryptosystem is confirmed by simulation results. In order to analysis the robustness of the fuzzy observer, a disturbance of pulse signal is added to the system during 5th sec to 6th sec. Fig. 3 shows the transmitted signal $\bar{y}_d(t)$. Fig. 4 shows the plain signal $p(t)$ and the recovered plain signal $\bar{p}(t)$. Fig. 5 shows the chaos states $\bar{x}_{d1}(t)$ and $\bar{x}_{r1}(t)$. Fig. 6 shows the tracking error signals $e_{x1}(t) = \bar{x}_{d1}(t) - \bar{x}_{r1}(t)$ for $\gamma = 0.27$ and 20, respectively. Fig. 7 shows the chaos states $\bar{x}_{d2}(t)$ and $\bar{x}_{r2}(t)$. Fig. 8 shows the tracking error signals $e_{x2}(t) = \bar{x}_{d2}(t) - \bar{x}_{r2}(t)$ for $\gamma = 0.27$ and 20, respectively. Fig. 9 shows the chaos states $\bar{x}_{d3}(t)$ and $\bar{x}_{r3}(t)$. Fig. 10 shows the tracking error signals $e_{x3}(t) = \bar{x}_{d3}(t) - \bar{x}_{r3}(t)$ for $\gamma = 0.27$ and 10, respectively.

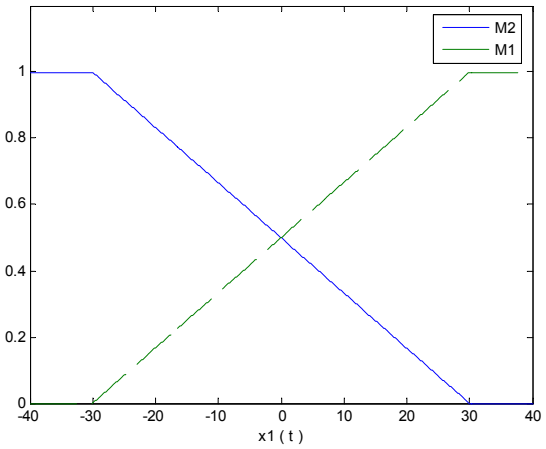

Fig. 2. Membership functions of fuzzy model.

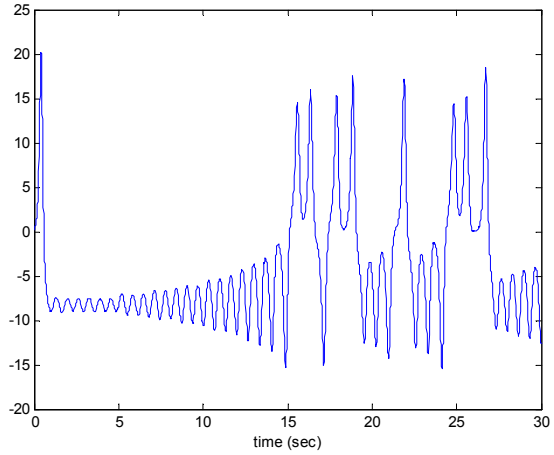

Fig. 3. The transmitted signal.

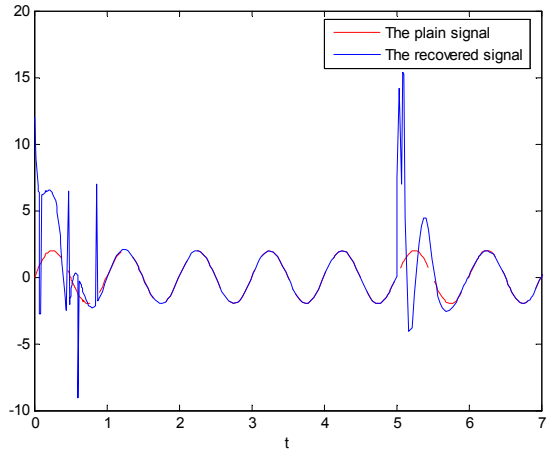

Fig. 4. The plain text and recovered signal.

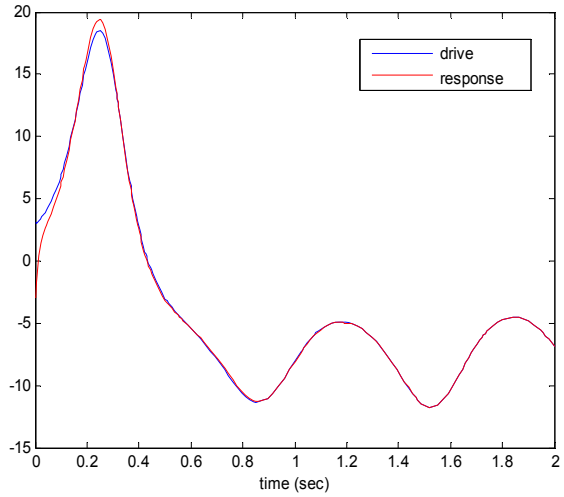

Fig. 5. The chaos states $\bar{x}_{d1}(t)$ and $\bar{x}_{r1}(t)$ for $\gamma = 0.27$.

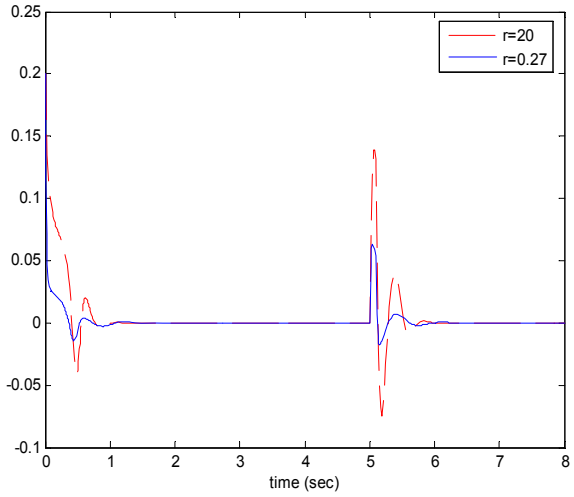

Fig. 6. The tracking error signal $e_{x1}(t)$.

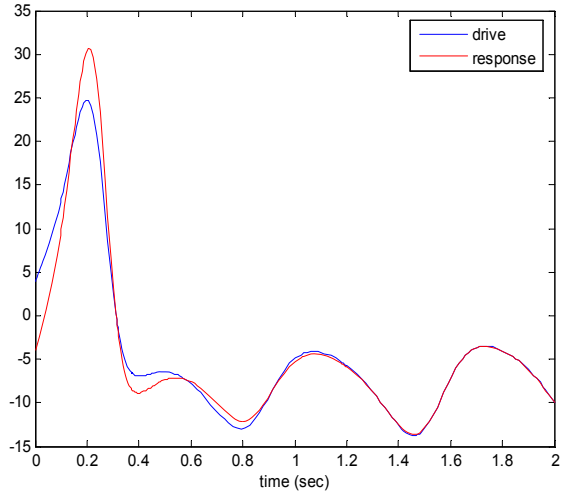

Fig. 7. The chaos states $\bar{x}_{d2}(t)$ and $\bar{x}_{r2}(t)$ for $\gamma = 0.27$ ..

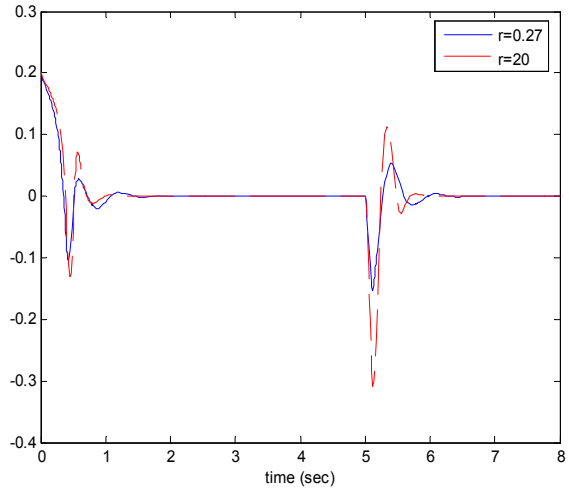

Fig. 8. The tracking error signal $e_{x2}(t)$.

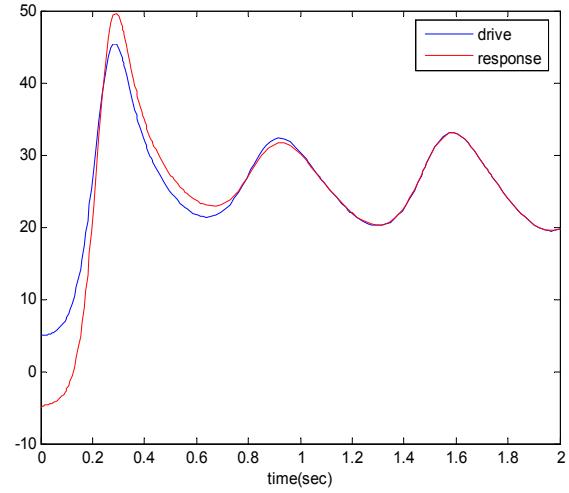

Fig. 9. The chaos states $\bar{x}_{d3}(t)$ and $\bar{x}_{r3}(t)$ for $\gamma = 0.27$.

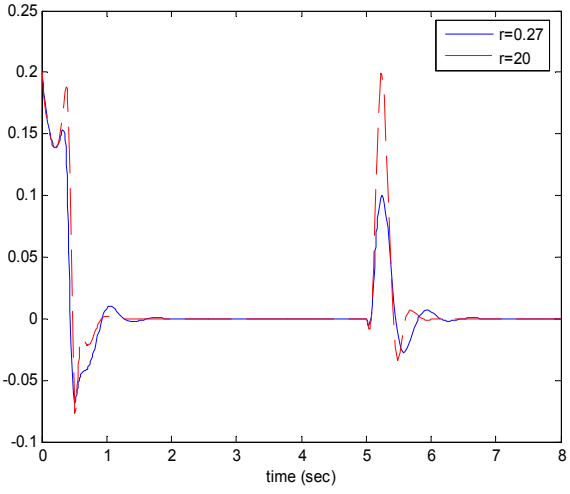

Fig. 10. The tracking error signal $e_{x3}(t)$.

4. CONCLUSIONS

In this paper, the design of robust control for chaos-based cryptosystem has been proposed. The nonlinear chaotic dynamics are represented as the T-S fuzzy model. The decrypter is designed as a global observer of the encrypter. The robust stabilization conditions are derived in the form of LMI. Computer simulations demonstrate that the proposed cryptosystem owns robustness performance against the external disturbance.

REFERENCES

Alvarez, G., Montoya, F., Romera, M., and Pastor, G. (2004). Breaking two secure communication systems based on chaotic masking. *IEEE Trans. Circuits Syst.,* **vol. 51, no. 10,** pp. 505-506.

Carroll, T. L., and Pecora, L. M. (1991). Synchronizing chaotic circuits. *IEEE Trans. Circuits Syst.* I, **vol. 38,** pp. 453–456.

Chen, C., and Dong, X. (1998). From Chaos to Order Methodologies, Perspectives and Applications. *ser. Nonlinear Science, Singapore: World Scientific.*

Chen, S., and Leung, H. (2005). Ergodic chaotic parameter modulation with application to digital image watermarking. *IEEE Tran. Image Proc.,* **vol.14, no.3,** pp.1590-1602.

Duan, C. K., and Yang, S. S. (1997). Synchronization hyperchaotic with a scalar signal by parameter controlling, *Phys. Rev. Lett. A,* **vol. 229,** pp.151-155.

El Hajjaji, A., Chadli, M., Oudghiri, M., and Pages, O. (2006). Observer-based robust fuzzy control for vehicle lateral dynamics. *American Control Conference, 2006,* pp. 4664-4669, USA.

Kilic, R., and Alci, M. (2001). Chaotic switching system using mixed-mode chaotic circuit. *in Proc. IEEE MW. Symp. Circuits and Systems, MWSCAS'01,* **vol.2,** pp. 584 – 587.

Lakshmanan, M., and Murali, K., (1996). Chaos in Nonlinear Oscillators: Controlling and Synchronization. *Singapore: World Scientific.*

Lian, K. Y., Chiang, T. S., Liu, P., and Chiu, C.-S. (2000). LMI-based fuzzy chaotic synchronization and communication. *FUZZ-IEEE'2000,* **vol.2**

Lian, K. Y., Chiu, C. S., Chiang, T. S., and Liu, P. (2001). Secure communication for chaotic systems with robust performance via fuzzy observer-based design. *IEEE Trans. Fuzzy system,* **vol. 9, no. 1.** pp.212-220.

Liao, T. L., and Huang, N.–S. (1999) An observer-based approach for chaotic synchronization with application to secure cryptosystems. *IEEE Trans. Circuit Syst. I,* **vol. 46, no. 9,** pp. 1144-1150.

Murali, K., Leung, H., and Yu, H. (2003). Design of noncoherent receiver for analog spread-spectrum communication based on chaotic masking. *IEEE Trans. Circuits Syst.,* **vol. 50, no.3,** pp. 432- 441.

Pecora, L. M., and Carroll, T. L. (1990). Synchronization in chaotic systems. *Phys. Rev. Lett,* **vol. 38,** pp. 821-824.

Sathyan, T., and Kirubarajan, T. (2006). Markov-Jump-System-Based Secure Chaotic Communication. *IEEE Trans. Circuits Syst.,* **vol. 53, no. 7,** pp. 1597-1609.

Tada, Y., Uwate, Y., and Nishio, Y. (2006). Performance of chaotic switching noise injected to Hopfield NN for quadratic assignment problem. *in Proc. IEEE Int. Symp. Circuits and Systems, ISCAS'06,* pp. 5519-5522.

Tanaka, K., and Wang, H. O. (2001). *Fuzzy Control Systems Design and Analysis-A Linear Matrix Inequality Approach,* John Wiley & Sons, Inc.

Tanaka, K. and Wang, H. O. (2003). *Fuzzy Control Systems Design and Analysis,* John Wiley and Sons, Inc.

Yang, T., Wu, C. W., and Chua, L. O. (1997). Cryptography based on chaotic systems. *IEEE Trans. Circuit Sys I,* **vol. 44, no.5,** pp.469-472.