Iranian Journal of Fuzzy Systems **Vol. 3, No. 2,** (2006) pp. 21-32

FUZZY OBSERVER DESIGN WITH n-SHIFT MULTIPLE KEY FOR CRYPTOGRAPHY BASED ON 3D HYPERCHAOTIC OSCILLATOR

V. NATARAJAN, P. KANAGASABAPATHY, N. SELVAGANESAN AND R. NATARAJAN

ABSTRACT. A fuzzy observer based scheme for synchronizing two hyperchaotic oscillators via a scalar transmitted signal for cryptographic application is proposed. The Takagi-Sugeno fuzzy model exactly represents chaotic systems. Based on the general fuzzy model, the fuzzy observer of a chaotic system is designed on the basis of the n-shift multiple state based key encryption algorithm. The scalar transmitted signal is designed in such a way that the hyperchaotic carrier masks the encrypted signal, which in turn hides the message signal. Simulation results show that the proposed scheme gives a better performance even when a small additive stochastic noise is present in the channel.

1. Introduction

The use of synchronization of chaotic systems for the purpose of secure communication in cryptography applications was reported by A.Tamasevicius et al [12]. A chaotic signal has a spread-spectrum and can hide a small message signal in the spectral domain. However, a chaotic system can be easily identified in the time domain using one of its state variables. The idea of chaotic masking is to directly add the message in a noise-like chaotic signal at the transmitter, while chaotic modulation is done by injecting the message into a chaotic system as in spread-spectrum transmission [6].

Grassi and Mascolo[5] have proposed a transmitter and receiver, which are based on 3D hyperchaotic oscillator [13], and which are synchronized via a scalar signal by exploiting the concept of the observer from modern control theory. In reference [7] the secure communication of chaotic systems with robust performance via a fuzzy observer based design has been proposed, but these methods do not provide robust performance in the presence of channel noise or parameter changes.

On the other hand, controller and observer design for non-linear systems using T-S Fuzzy models have been reported by several authors[4,8]. The use of a fuzzy observer design helps to achieve the desired objective in a straight forward manner employing the parallel distributed compensation concept.

Received: March 2005; Accepted: April 2006

Key words and phrases: Cryptography, Fuzzy observer, Chaotic systems, n-shift multiple state based key algorithm, T-S fuzzy model.

In this paper, a secure communication scheme, which combines cryptography and the synchronization of hyperchaotic systems based on a fuzzy observer with n-shift multiple state based key algorithms, is proposed. Based on the general T-S fuzzy model, the fuzzy observer of a chaotic system is designed in the receiver. An n-shift cipher with a multiple state based key to encrypt/decrypt the message signal is also proposed. The use of multiple state based keys can increase the complexity of the transmitted signal and is likely to improve the security of communication.

The rest of the paper is organised as follows. Section 2 deals with a secure communication scheme for cryptography. In Section 3, the proposed n-shift multiple key algorithm for cryptography is explained. In Section 4, we establish a T-S fuzzy model that can represent a chaotic system. In Section 5, we construct the fuzzy observer of chaotic systems and derive the conditions via Linear Matrix Inequality (LMI). In Section 6, simulation results for two cases are presented. Section 7 concludes the paper.

2. **The Proposed Communication Scheme**

The proposed communication scheme with possible impovement in the security properties is shown as a block diagram in Figure 1. The transmitter consists of a 3D hyperchaotic oscillator and an encryption function, which is used to encrypt the message signal p(t) by means of the hyperchaotic key k(t). The system states are represented by x(t). The encrypted signal $e_{en}(t)$ is added to the output y(t) of the oscillator circuit and then transmitted on the channel z(t). An n-shift cipher [14] with multiple state based key algorithm which is proposed to encrypt the message signal p(t) is explained in Section 3.

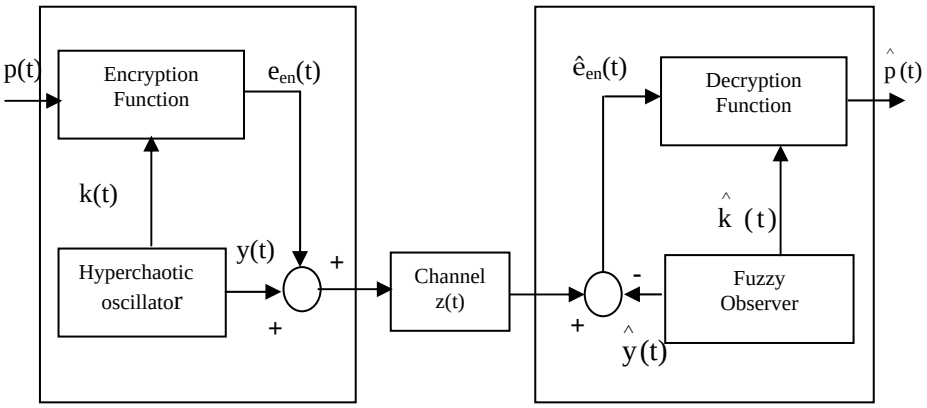

FIGURE 1. The proposed communication scheme

It may be noted that the receiver is a mirror of the transmitter. The difference between the received signal z(t) and the predicted value $\hat{y}(t)$ obtained from

the fuzzy obsever is sent for decryption. As the transmitter and the receiver are synchronised, the predictedvalue of $\hat{x}(t)$ approaches $x(t)$, $\hat{k}(t)$ approaches $k(t)$, and $\hat{e}_{en}(t)$ approaches $e_{en}(t)$ and decryption can be performed, where $k(t)=x_1(t)+x_2(t)+x_3(t)$ and $\hat{k}(t)=\hat{x}_1(t)+\hat{x}_2(t)+\hat{x}_3(t)$ .Consequently $\hat{p}(t)$ approaches $p(t)$.

3. **n-Shift Multiple Key Cipher Algorithm**

The n-shift cipher with multiple state based key algorithm is proposed to encrypt the message signal given in equation (1). In this technique, the message signal is shifted n-times with the key k, which is the combination of states (x_1, x_2, x_3) of the chaotic system considered. The use of the multiple state based key algorithm tends to increase the complexity of the transmitted signal.

$$e_{en}(t)=f_1\left(....f_1\left(f_1\left(p(t),k(t)\right),k(t)\right),....,k(t)\right) \tag{1}$$

The non-linear function $f_1(x,k)$ is defined as follows:

$$f_1(x,k)=\begin{cases}(x+k)+2h, & -2h \le (x+k) \le -h \\ (x+k), & -h < (x+k) < h \\ (x+k)-2h, & h \le (x+k) \le 2h\end{cases} \tag{2}$$

where h is chosen such that p(t) and k(t) lie between –h and h. It may be noted that the decryption technique is similar to the encryption technique (1). The decryption function is defined as

$$\hat{p}(t)=f_1\left(....f_1\left(f_1\left(\hat{e}_{en}(t),-k(t)\right),-k(t)\right),....,-k(t)\right) \tag{3}$$

where $f_1(x, k)$ is given in equation (2).

4. **Design of Fuzzy Model**

In a fuzzy observer design, a chaotic system should be exactly represented by a T–S fuzzy model. Consider a general chaotic system as given below:

$$\begin{aligned} sx(t) &= f(x(t)) \\ y(t) &= h(x(t)) \end{aligned} \tag{4}$$

where $x \in R^n$ is the state vector and $sx(t)$ respectively denotes $\dot{x}(t)$ and $x(t+1)$ in continuous-time and discrete-time systems; $y \in R^m$ is the system

output; f(.) and h(.) are the nonlinear functions with appropriate dimensions. The fuzzy representation of equation (4) is given by of the following rules:
Plant Rule *i*:
If $z_1(t)$ is F_{1i} and … and $z_g(t)$ is F_{gi}, then

$$\begin{aligned} sx(t) &= A_i x(t) + b_i \\ y(t) &= C_i x(t) \qquad \text{for } i=1, 2, \ldots, r \end{aligned} \tag{5}$$

where, $z_1(t), z_2(t), \ldots, z_g(t)$ are the premise variables which represent the states of the system; F_{ji} (j =1, 2,…., g) are the fuzzy sets; r is the number of fuzzy rules; A_i and C_i are the system and output matrices with appropriate dimensions; and $b_i \in R^n$ denotes the constant bias term, which is generated by the exact fuzzy modeling procedure.

Using the singleton fuzzifier, product fuzzy inference and the weighted average defuzzifier, the final output of the fuzzy system is inferred as follows:

$$sx(t) = \sum_{i=1}^{r} \mu_i(z(t))(A_i x(t) + b_i)$$

$$y(t) = \sum_{i=1}^{r} \mu_i(z(t))(C_i x(t))$$

where, $z(t)=[z_1(t) \quad z_2(t) \quad \ldots \quad z_g(t)]^T$ and $\mu_i(z(t)) = \left(w_i(z(t)) \Big/ \sum_{i=1}^{r} w_i(z(t)) \right)$ with $w_i(z(t)) = \prod_{j=1}^{g} F_{ji}(z_j(t))$. It may be noted that $\sum_{i=1}^{r} \mu_i(z(t)) = 1$ for all t, where $\mu_i(z(t)) \geq 0$ for i=1, 2, …, r.

From the equations (4) and (5), it is clear that if we appropriately specify the fuzzy membership functions in the premise parts and associated entries of matrices A_i, C_i and b_i in the consequence parts, the chaotic system can be represented by a fuzzy model. In this paper Lorenz's oscillator system in T–S fuzzy model is considered.
Lorenz's equation:

$$\begin{aligned} \dot{x}_1(t) &= -10x_1(t) + 10x_2(t) \\ \dot{x}_2(t) &= 28x_1(t) - x_2(t) - x_1(t)x_3(t) \\ \dot{x}_3(t) &= x_1(t)x_2(t) - \tfrac{8}{3}x_3(t) \\ y(t) &= x_1(t) \end{aligned} \tag{6}$$

The premise variable of the fuzzy rules is $x_1(t)$, which satisfies $x_1(t) \in [-d \; d]$ with d=30. The fuzzy dynamic model that exactly represents the Lorenz's equation in (6) is derived using this range as follows:

Rule i:
If $x_1(t)$ is F_i then

$$\begin{aligned} sx(t) &= A_i x(t) + b_i \\ y(t) &= C_i x(t) \quad \text{for i=1, 2} \end{aligned} \tag{7}$$

where $x(t) = [x_1(t), x_2(t), x_3(t)]^T$, the fuzzy sets are chosen as

$F_1(x_1(t)) = 1/2\left(1+\left(x_1(t)/d\right)\right)$, and $F_2(x_1(t)) = 1/2\left(1-\left(x_1(t)/d\right)\right)$
and the system matrices are given by

$$A_1 = \begin{bmatrix} -10 & 10 & 0 \\ 28 & -1 & -d \\ 0 & d & -8/3 \end{bmatrix} \quad A_2 = \begin{bmatrix} -10 & 10 & 0 \\ 28 & -1 & d \\ 0 & -d & -8/3 \end{bmatrix}$$

$C_1 = C_2 = [1\ 0\ 0]$, and $b_1 = b_2 = 0$.

5. **Fuzzy Observer of Chaotic Systems**

Consider a chaotic system described by the T–S fuzzy model as given in equation (7) and assume that (A_i, C_i) is a detectable pair for each local linear model. A fuzzy observer can then be derived to estimate the state x(t) from the system output. For simplicity, the premise variable of observer rules and that of fuzzy rules are assumed to be same. Accordingly, a fuzzy observer is given with the following rules:
Observer rule i:
If $y(t)$ is F_i then

$$\begin{aligned} s\hat{x}(t) &= A_i \hat{x}(t) + b_i + L_i(y(t) - \hat{y}(t)) \\ \hat{y}(t) &= C_i \hat{x}(t) \quad \text{for } i = 1, 2, \ldots, r \end{aligned} \tag{8}$$

where, L_i (i=1,2.....r) is the observer gain, determined using LMI approach [9] to ensure the quadratic stability of fuzzy observer dynamics (8). The overall fuzzy observer is inferred in the following equations.

$$\begin{aligned} s\hat{x}(t) &= \sum_{i=1}^{r} \mu_i(y(t)) \left\{ A_i \hat{x}(t) + b_i + L_i(y(t) - \hat{y}(t)) \right\} \\ \hat{y}(t) &= C_i \hat{x}(t) \end{aligned} \tag{9}$$

where, $\mu_i\left(y(t)\right) = \left(w_i\left(y(t)\right) / \sum_{i=1}^{r} w_i\left(y(t)\right)\right)$ with $w_i\left(y(t)\right) = F_i\left(y(t)\right) \geq 0$, r=2 and

$$L_1 = \begin{bmatrix} 0.8054 \\ 0.8947 \\ 0.8945 \end{bmatrix} \qquad L_2 = \begin{bmatrix} 0.9665 \\ 1.0736 \\ 1.0734 \end{bmatrix}$$

The gains L_1, L_2 of the fuzzy observer are determined using the LMI approach [9]. These values are incorporated in the design of fuzzy observer.

6. **Simulation Results**

Simulation results for two different cases are presented to illustrate the performance of the fuzzy observer for a 3D chaotic system in cryptographic application.

Case 1: Channel is assumed to be noise free.

Case 2: Small additive stochastic noise is present in the channel.

The message signal p(t)=0.5 sin(t) and 'h' is chosen as 0.7 for this simulation.

6.1. **Noise Free Channel.** Figures 2 to 7 show the simulation results for the noise free channel. The hyperchaotic transmitted signal (channel output) is shown in Figure 2, whereas the recovered message signal (using equation 3) is shown in Figure 3. It can be seen from this figure that $\hat{p}(t)$ approaches p(t). Figures 5 and 6 show the variation of state variables and their corresponding errors for a given chaotic system and fuzzy observer.

The step change in the message signal from p(t)=0.5 sin(t) to p(t)= sin(0.5*t) is given at the 50th sample instant and the response is shown in Figure 7. It may be observed that the fuzzy observer yields a good tracking performance even for a change in input signal (message signal).

The multiple state based key encryption/decryption technique is used in this work and the corresponding response is shown in Figure 4. This makes the transmitted signal somewhat complex and is likely to improve the effectiveness of the secure communication. In the case of a hyperchaotic system, it seems that it is difficult for any intruder to predict the dynamics of the hyperchaotic carrier y(t) by means of reconstruction of the geometric structure in the phase space [10,11]. Let us assume that the encrypted signal $e_{en}(t)$ is reconstructed by the intruder. If the key k(t) is not transmitted through the channel, it appears to be difficult to recover the original message signal p(t) from $e_{en}(t)$. Therefore, assuming that the key is not transmitted or reconstructed, it may not possible for an intruder to obtain the message, even if the intruder is able to reconstruct the encrypted signal.

Recently, the authors [1-3] have proposed a technique to break the cryptosystem without knowing its parameter values and its transmitter structure using a simple high pass filter. The algorithm proposed is demonstrated when the frequency of the message signal is from 5 Hz to infinity. However for lower freqencies, the noise created by the Lorenz system masks the message signal thus making it difficult to retrieve by nonauthorized means.

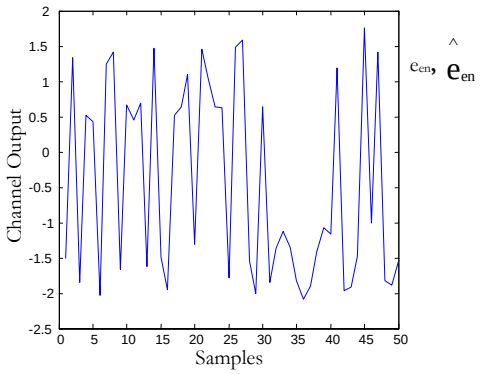

FIGURE 2.Channel output (noise free)

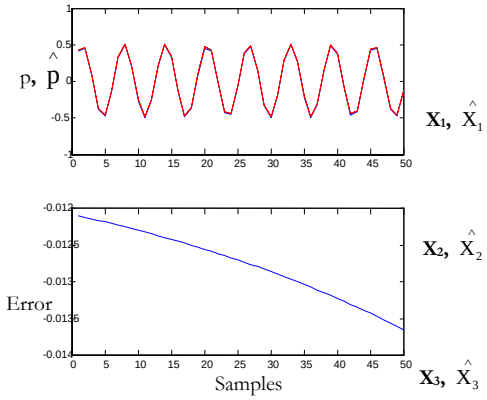

FIGURE 3. Message Vs Recovered signal and the corresponding error

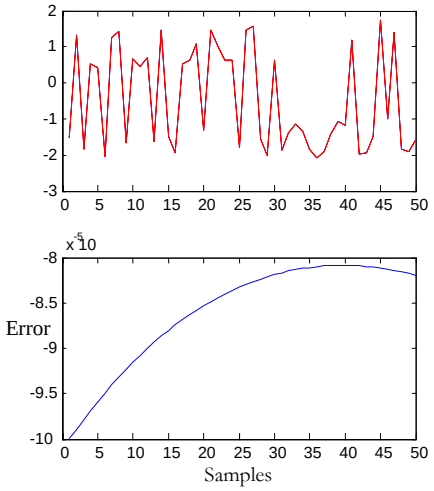

FIGURE 4. Encrypted Vs Decrypted signal and the corresponding error

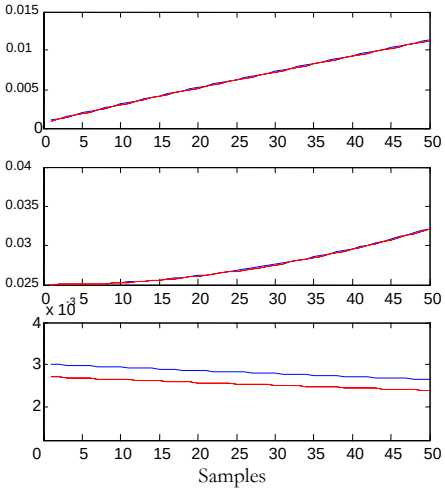

FIGURE 5. System states Vs Observer states

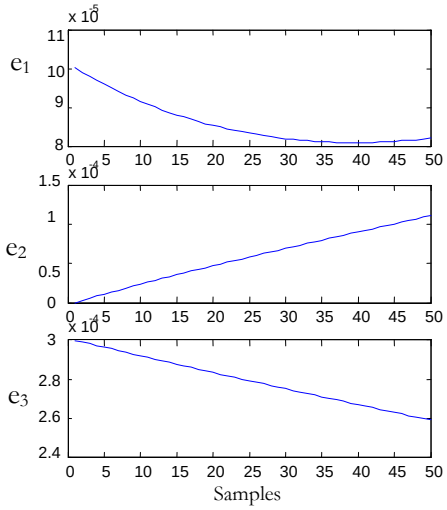

FIGURE 6. Errors in states

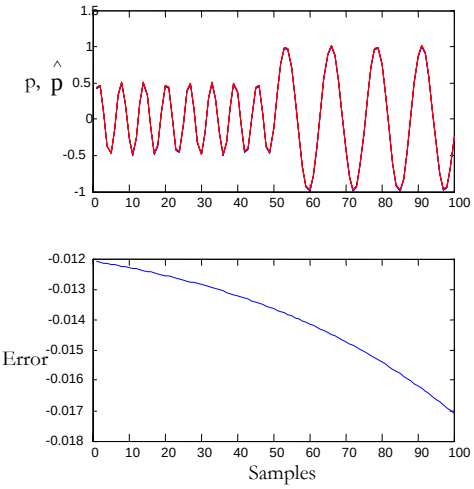

FIGURE 7. Message Vs Recovered signal and the corresponding error with step change at 50th sample time (noise free)

6.2. **Channel with Noise.** Figures 8 to 14 show the simulation results for the channel with small additive stochastic noise. The hyperchaotic transmitted signal (channel output) and the noise signal are shown in Figures 8 and 9, whereas the recovered message signal is shown in Figure 10. It can be seen from this figure that $\hat{p}(t)$ approaches p(t). In particular, the error signal keeps varying between -0.02 and -0.11. Figures 12 and 13 show the variation of the state variables and their corresponding errors for a given chaotic system and fuzzy observer.

The same step change in the message signal is given at the 50th sample instant and the corresponding response is shown in Figure 14. From the responses, it is seen that fuzzy observer yields a good tracking performance even for a change in input signal (message signal). The encrypted /decrypted responses are shown in Figure 11.

The authors [1-3] have presented techniques to break the secure communication only if the system is noise free. In many practical cases, the transmitted signals are disturbed by the noisy signal. These breaking algorithms may not be useful for retrieving the message signal for communication system when noise is present in the channel.

It may be noted that the proposed fuzzy observer yields a good tracking performance even in the presence of noise in channel with adequate security and it

is able to track the change in input with different magnitude and frequency. But conventional observers like reduced order and full order observers are applicable only for noise / disturbance-free-system. As conventional methods are not suitable for noisy systems, a comparative study has not been attempted.

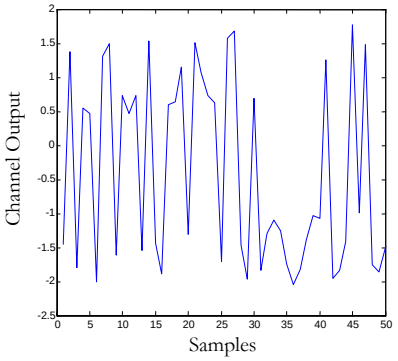

FIGURE 8. Channel output (with noise)

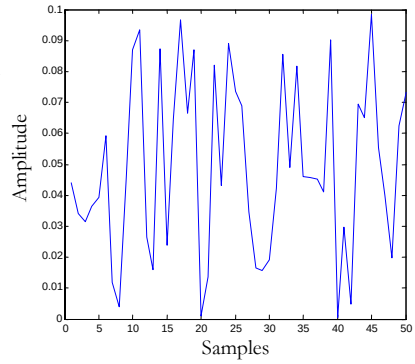

FIGURE 9. Stochastic noise signal

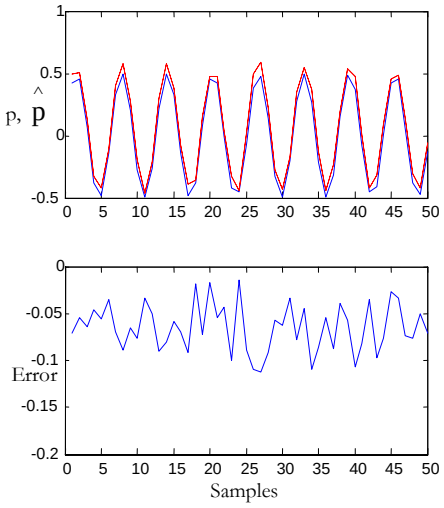

FIGURE 10. Message Vs Recovered signal and the corresponding error

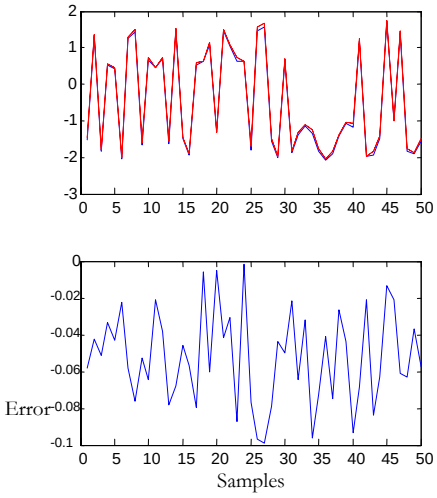

FIGURE 11. Encrypted Vs decrypted signal and the corresponding error

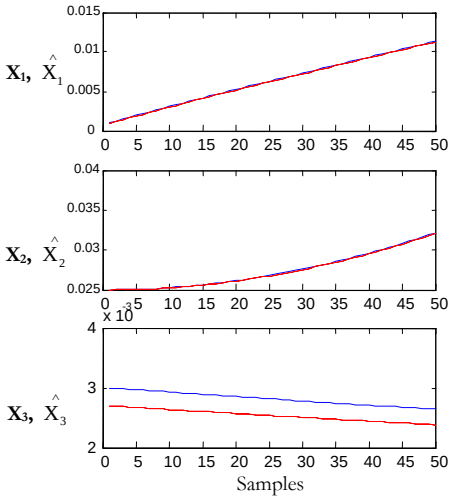

FIGURE 12. System states Vs Observer states

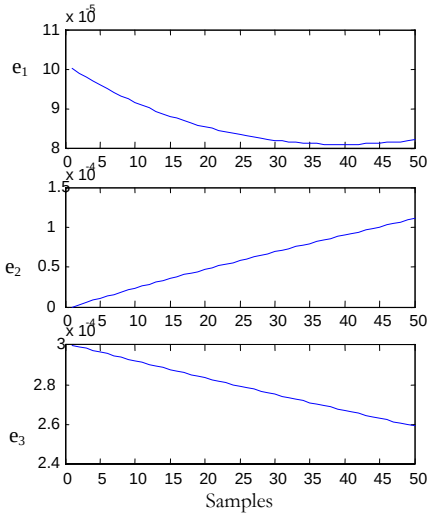

FIGURE 13. Errors in states

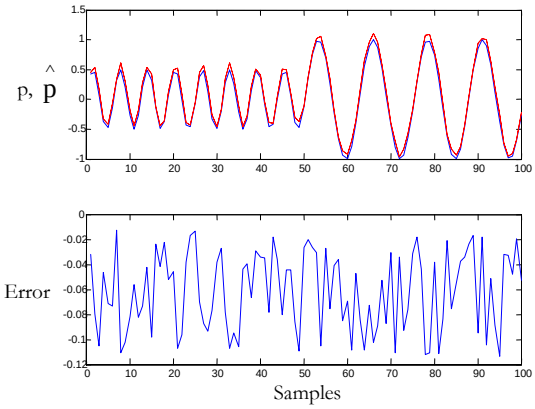

FIGURE 14. Message Vs Recovered signal and the corresponding error with step change at 50th sample time (channel with noise)

7. **Conclusion**

In this paper, a secure communication system based on fuzzy observer design with n-shift multiple state based key algorithm for a 3D chaotic system in cryptographic application is proposed. This approach tries to generate transmitted

signals of adequate complexity, which are used to transmit the message without forging the original message. Simulation results show that the proposed scheme yields a good tracking and robust performance even in the presence of noise in channel and it can track the change in message signal.

Acknowledgments. The authors would like to thank the reviewers and editorial board for their valuable comments and suggestions.

REFERENCES

[1] G. Álvarez and S. Li , *Breaking network security based on synchronized chaos*, Computer Communications, Elsevier , **27** (2004), 1679-1681.

[2] G. Álvarez, S. Li, F. Montoya, M. Romera and G. Pastor, *Breaking projective chaos synchronization secure communication using filtering and generalized synchronization,* Chaos, Solitons & Fractuals, Elsevier, **24** (2005), 775-783.

[3] G. Álvarez, F. Montoya, M. Romera and G. Pastor, *Breaking two secure communication systems based on chaotic masking,* IEEE Transactions on Circuits and Systems-II, **51** (2004), 505-506.

[4] T.-S. Chiang and P. Liu, *Fuzzy model-based discrete-time Chiang type chaotic cryptosystem*, IEEE Int. Fuzzy Systems Conference, 2001.

[5] G. Grassi and S. Mascolo, *Observer design for cryptography based on hyperchaotic oscillators*, Electronics Letters, **34** (1998), 1844 -1846.

[6] K. Halle, C. W. Wu, M. Itoh and L. O. Chua, *Spread spectrum communication through modulation of chaos,* Int. Journal of Bifurcations and Chaos, **3** (1992), 469-477.

[7] K.-Y. Lian, C.-S. Chiu, T.-S. Chiang, and P. Liu, *Secure communications of chaotic systems with robust performance via fuzzy observer-based design,* IEEE Transactions on Fuzzy Systems, **9** (2001), 212-220.

[8] K.-Y. Lian, P. Liu and C.-S. Chiu, *Fuzzy model-based approach to chaotic encryption using synchronization,* Int. Journal of Bifurcation and Chaos, **13** (2003), 215-225.

[9] K.-M. Ma, *Observer design for a class of fuzzy systems*, Proceedings of First International Conference on Machine Learning and Cybernetics, Beijing, (2002), 46-49.

[10] K. M. Short, *Steps towards unmasking secure communication*, Int. Journal of Bifurcation and Chaos, **4** (1994), 959-977.

[11] K. M. Short, *Unmasking a modulated chaotic communications scheme*, Int. Journal of Bifurcation and Chaos, **6** (1996), 367-375.

[12] A. Tamasevicius, G. Mykolaitis, A. Cenys and A. Namajunas, *Synchronisation of 4D hyperchaotic oscillators,* Electronics Letters, **32** (1996), 1536-1538.

[13] A. Tamasevicius, A. Namajunas and A. Cenys, *Simple 4D chaotic oscillator*, Electronics Letters, **32** (1996), 957-958.

[14] T. Yang, C. Wah Wu and L. O. Chua, *Cryptography based on chaotic systems,* IEEE Transactions on Circuits and Systems-I, **44** (1997), 469-472.

V. NATARAJAN*, DEPARTMENT OF INSTRUMENTATION ENGINEERING, MIT CAMPUS, ANNA UNIVERSITY, CHROMEPET, CHENNAL-600044, INDIA
E-mail address: **natraj@mitindia.edu**

P. KANAGASABAPATHY, DEPARTMENT OF INSTRUMENTATION ENGINEERING, MIT CAMPUS, ANNA UNIVERSITY, CHROMEPET, CHENNAL-600044, INDIA

N. SELVAGANESAN, DEPARTMENT OF EEE, PONDICHERRY ENGINEERING COLLEGE, PONDICHERRY-605014, INDIA
E-mail address: **n_selvag@rediffmail.com**

P. NATARAJAN, DEPARTMENT OF INSTRUMENTATION ENGINEERING, MIT CAMPUS, ANNA UNIVERSITY, CHROMEPET, CHENNAL-600044, INDIA

* CORRESPONDING AUTHOR