Available online at www.sciencedirect.com
ScienceDirect
Communications in Nonlinear Science and Numerical Simulation 13 (2008) 763–781
Communications in Nonlinear Science and Numerical Simulation
www.elsevier.com/locate/cnsns

# An application of Chen system for secure chaotic communication based on extended Kalman filter and multi-shift cipher algorithm

Kia Fallahi *, Reza Raoufi, Hossein Khoshbin

*Electrical Engineering Department, Ferdowsi University of Mashhad, Iran*

Received 26 February 2006; received in revised form 28 June 2006; accepted 7 July 2006
Available online 7 September 2006

**Abstract**

In recent years chaotic secure communication and chaos synchronization have received ever increasing attention. In this paper a chaotic communication method using extended Kalman filter is presented. The chaotic synchronization is implemented by EKF design in the presence of channel additive noise and processing noise. Encoding chaotic communication is used to achieve a satisfactory, typical secure communication scheme. In the proposed system, a multi-shift cipher algorithm is also used to enhance the security and the key cipher is chosen as one of the chaos states. The key estimate is employed to recover the primary data. To illustrate the effectiveness of the proposed scheme, a numerical example based on Chen dynamical system is presented and the results are compared to two other chaotic systems.


*PACS:* 05.45.−a; 05.45.Gg; 05.45.Jn; 05.45.Pq; 05.45.Tp; 05.45.Vx; 05.45.Xt; 87.53.Vb; 87.64.Aa; 89.70.+c; 89.75.−k

*Keywords:* Chaotic cryptosystems; Security; *n*-Shift cipher; Chaotic masking; Encryption; Extended Kalman filter; Chaos states; Synchronization

## 1. Introduction

In the past 20 years, there has been a great deal of interest in the study of non-linear dynamical systems. Deterministic dynamical systems are those whose states changes with time in a deterministic way. The introduction of chaos into communication systems offers several opportunities for improvement. This is because of random nature of chaotic systems. Since a chaotic dynamical system is a deterministic system, its random-like behavior can be very helpful in disguising modulation as noise [1]. A small perturbation eventually causes a large change in the state of the system. In the digital world nowadays, the security of digital signal becomes

* Corresponding author. Address: No. 46, Milad 10, Sajjad Boulevard, Mashhad, Khorasan, 91877, Iran. Tel.: +98 9153 101092; fax: +98 5117 689664.
*E-mail address:* kiafallahi@yahoo.com (K. Fallahi).

1007-5704/$ - see front matter 
doi:10.1016/j.cnsns.2006.07.006

very important since the proliferation of wireless products [2]. Compared to conventional communication systems, there are several unique features of chaotic communication systems [3–5]. Potential benefits of chaotic communications include efficient use of the bandwidth of a communication channel, utilization of the intrinsic nonlinearities in communication devices, large-signal modulation for efficient use of carrier power, reduced number of components in a system, and security of communication by chaotic encryption [6].

Chaotic dynamics with their noise-like broadband power spectra is a good candidate to fight narrow-band effects such as frequency-selective fading or narrow-band disturbances in communication systems. Another attractive feature of chaotic signal is their dependence on initial condition, which makes it difficult to guess the structure of the generator and to predict the signal over longer time interval. This feature is of interesting in cryptography, where highly complex and hard-to-predict signals are employed. Chaotic signals are deterministic so there is no random component in differential equation, but trajectories are noise-like. Also they are bounded and on successive generation of chaos, the states stay in a finite range. Moreover, they are aperiodic, same state never repeated twice. Chaotic output streams will be completely uncorrelated, and the autocorrelation of a chaotic signal has a large peak at zero and decays rapidly. Thus a chaotic system shares many properties of a stochastic process, which are basic requirements of the spread spectrum communications.

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. It is possible to implement a chaotic communication system either with chaos synchronization (coherent) or without chaos synchronization (noncoherent) [7–23]. Most of the research activities in chaotic communication so far address systems based on synchronization of chaos between a transmitter and a receiver linked by a transmission channel. For such systems, chaos synchronization is mandatory, while the quality of communication, measured by the bit-error rate (BER) of a decoded message at the receiver, depends crucially on the accuracy and robustness of synchronization. Following these approaches, different methods have been developed in order to mask the contents of a message using chaotic signals [12–29]. However, it has been shown that most of these methods are not secure or have a low level of security because one can extract the encoded message signal from the transmitted chaotic signal by using different unmasking techniques [24–26]. So to overcome the problem of unmasking the information message from the chaotic carrier, different approaches for designing cryptosystems based on chaos have been recently introduced [22,23]. In these schemes both conventional cryptographic method and synchronization of chaotic systems are combined so that the level of security of transmitted chaotic signal is enhanced. Typically these approaches are based on the synchronization properties of simple chaotic systems. So it is of considerable interest of achieving secure encoding of the digital information signal by considering the fact of masking chaotic encoding signal is as important as masking the information signal. For this purpose combining together the advantages of digital encryption techniques and chaos synchronization methods, the level of security of the transmitted signal can be potentially enhanced.

Extended Kalman filter has been widely used in the state estimation of nonlinear dynamical systems and it is also an important algorithm for the implementation of chaotic synchronization [23]. Many research works demonstrate that EKF can synchronize different chaotic maps for the applications in secure communications. In this work, the Chen dynamical system is used to modulate the sinusoid data via the masking modulation and also for improving the security $n$-shift cipher algorithm is used for security improvement. The modulated signal is transmitted through the additive white Gaussian noise (AWGN) channel. At the receiver, EKF is employed to estimate states of the chaotic systems.

The proposed chaotic communication scheme is totally different from the traditional cryptosystem where both the key and the encrypted signal should be transmitted to the decrypter. It should be pointed out that in this approach, regarding the different employed chaotic states for the objectives of synchronization, masking modulation and multi-shift ciphering algorithm and meanwhile, noting the fact that all chaotic states of a same chaos attractor are inherently absolutely different from each other, there is no requirement for purely transmission of the chaotic key. This in turn, heightens the security level of the system.

In this paper the application of extended Kalman filter for state reconstruction of continuous-time nonlinear systems in a chaotic communication scheme is presented. The proposed scheme uses a Chen dynamical system, Lorenz, and Genesio-Tesi as chaos generators to encrypt data using masking modulation. $n$-Shift cipher algorithm is also used to improve the security. The receiver consists of an extended Kalman filter for state reconstruction, a chaos masking demodulator, and also $n$-shift cipher decryptor. In Section 2, chaotic

masking and $n$-shift cipher algorithm are described. Section 3 shows extended Kalman filter and related equations. In Section 4, the proposed chaotic encryption scheme and numerical examples are presented. Section 5 describes simulation experiments for the proposed system.

## 2. Chaotic cryptosystems

The basic idea of these cryptosystems are based upon consists of using 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 [29].

### 2.1. Chaotic masking

The chaotic signal is added to the information signal and at the receiver the masking is removed. In order for this scheme to properly work, the receiver must synchronize robustly enough as to admit the small perturbation in the driving signal due to the addition of the message. The power level of the information signal must be much lower than that of the chaotic signal to effectively bury it [29].

### 2.2. n-Shift cipher encryption

A chaotic cryptosystem is shown in Fig. 1. In this figure, the encrypter consists of a chaotic system and an encryption function $e(\cdot)$. The key signal $k(t)$ is one of the state variables of a chaotic system. Another state variable is the transmitted signal, which is transmitted through a public channel to the decrypter and used to synchronize the decrypter. $c(t)$ is the encrypted signal which is fed back into the chaotic system. The decrypter consists of a chaotic system and a decryption function $d(\cdot)$. The decrypter can find the key signal when the decrypter and the encrypter are synchronized. The encrypted signal is also recovered via synchronization. Then, $d(\cdot)$ is used to decrypt the encrypted signal. It should be noted that both the key signal and the encrypted signal $c(t)$ are not transmitted to the decrypter. The signal $s_M(t)$ denotes the modulated information signal, $k(t)$ is the key signal, and $c(t)$ is the ciphered transmitted signal. $e(s_M(t))$ is the encrypted signal and $s_R(t)$ is the recovered decrypted signal. We have $d(e(s_M(t))) \to s_M(t)$ when the synchronization is achieved.

We use an $n$-shift cipher to encrypt the plain signal.

The $n$-shift cipher is defined by

$$e(s_M(t)) = \underbrace{f_1(\ldots f_1(f_1}_{n}(s_M(t), \underbrace{k(t)), k(t)), \ldots, k(t)}_{n}) = c(t) \tag{1}$$

where the parameter $h$ is chosen such that $s_M(t)$ and $k(t)$ lie within $(-h,h)$, and $f_1(x,k)$ is the following nonlinear function:

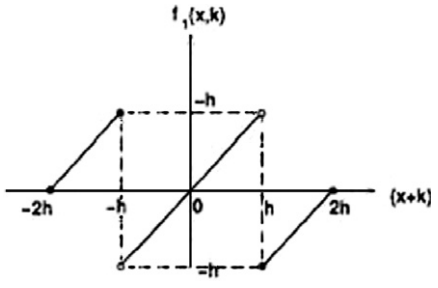


Fig. 1. Nonlinear function used in continuous shift cipher.

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

This function is shown in Fig. 1.

The corresponding decryption rule is the same as the encryption rule

$$s_{\mathrm{R}}(t)=d(c(t))=\underbrace{f_1(\ldots f_1(f_1}_{n}(c(t),\underbrace{-\hat{k}(t)),-\hat{k}(t)),\ldots,-\hat{k}(t)}_{n}) \tag{3}$$

where $\hat{k}(t)$ is estimated key in the receiver circuit and should precisely approximate $k(t)$.

In the $n$-shift cipher, the key signal is used $n$ times to encrypt the plain signal. Since the encrypted signal is a function of $k(t)$ and $s_{\mathrm{M}}(t)$, and since the encrypted signal is used to derive the circuit, it hides both the dynamical and the statistical characteristic of both $k(t)$ and $s_{\mathrm{M}}(t)$ [22].

## 3. Extended Kalman filter

EKF is an important and fascinating algorithm in the nonlinear filter theory and state estimation. In order to present a picture for design process, a brief discussion of stochastic state estimation design will follow [23]. The EKF based synchronization approach employs extended Kalman filter at the receiver section and generates the state estimates based on the noisy output measurement. Meanwhile, this method can render the processing noise as well. When the states of a chaotic system are estimated using an EKF, the process within the filter synchronizes to the transmitter as the estimates converge, and no decomposition is required. This synchronization is insensitive to additive noise.

Consider the provided nonlinear system and measurement model

$$\dot{x}(t)=A(x(t))x(t)+\Gamma v(t) \tag{4}$$

$$y(t)=h(x(t))+\Lambda w(t) \tag{5}$$

where $A\in R^{n\times n}$, $x(t)\in R^{n\times 1}$ is the state, $\Gamma$ is a column vector, $v(t)\in R^{n\times 1}$ is the process noise, $y(t)\in R^{p\times 1}$ is the measurement, $h\in R^{p\times 1}$, $\Lambda$ is a column vector and $w(t)\in R^{p\times 1}$.

Noise is white Gaussian and has characteristics as follows:

$$\begin{cases}E\{v\}=0\\ E\{w\}=0\\ E\{vv^{\mathrm{T}}\}=V\\ E\{ww^{\mathrm{T}}\}=W\end{cases} \tag{6}$$

and

$$h(x(t))=Cx(t) \tag{7}$$

in which $C$ is the measurement vector.

The EKF equation, is as follows:

$$\dot{\hat{x}}=f(\hat{x}(t))+L(t)(h(x(t))-C\hat{x}(t)) \tag{8}$$

where $L(t)$ is the Kalman filter gain satisfying

$$L(t)=\widehat{A}(t)P(t)C^{\mathrm{T}}+CP(t)C^{\mathrm{T}}+\Lambda W\Lambda^{\mathrm{T}} \tag{9}$$

and $P(t)$ is the solution to the Reccati equation

$$\begin{aligned}&\dot{P}(t)=\widehat{A}(t)P(t)\widehat{A}(t)^{\mathrm{T}}-L(t)(CP(t)\widehat{A}(t))+\Gamma^{\mathrm{T}}V\Gamma\\ &P(0)=P_0\end{aligned} \tag{10}$$

In the above equations, $V\geqslant 0$ and $W>0$, are noise covariance and are chosen to improve the convergence.

## 4. Proposed chaotic encryption scheme and numerical example

We have enhanced the security of the transmitted signal by using multi-shift cipher encryption algorithm. The synchronization is achieved by extended Kaman filter (EKF) as the state estimator in the presence of noise. The block diagram of the proposed scheme is shown in Fig. 2. The proposed scheme does not need to know the initial condition of the chaotic signals between the receiver and the transmitter. The system consists of a transmitter module, a communication channel and a receiver module. The transmitter module consists of a chaotic system, and an encryption mechanism. In this system the chaotic signal is generated by using Chen dynamical system. Chen dynamical system is described by the following system model of differential equations:

$$\begin{bmatrix}\dot{x}_1(t)\\ \dot{x}_2(t)\\ \dot{x}_3(t)\end{bmatrix} \equiv \begin{bmatrix}-a & a & 0\\ c-a & c & 0\\ 0 & 0 & -b\end{bmatrix}\begin{bmatrix}x_1(t)\\ x_2(t)\\ x_3(t)\end{bmatrix} + \begin{bmatrix}0\\ -x_1(t)x_3(t)\\ x_1(t)x_2(t)\end{bmatrix} \tag{11}$$

where $x_1(t)$, $x_2(t)$ and $x_3(t)$ are the state variables and $a$, $b$ and $c$ are three positive real constants.

Obviously, the Chen nonlinear model can also be presented as

$$\begin{bmatrix}\dot{x}_1(t)\\ \dot{x}_2(t)\\ \dot{x}_3(t)\end{bmatrix} \equiv \begin{bmatrix}-a & a & 0\\ c-a & c & -x_1(t)\\ 0 & x_1(t) & -b\end{bmatrix}\begin{bmatrix}x_1(t)\\ x_2(t)\\ x_3(t)\end{bmatrix} = A(x(t))x(t) \tag{12}$$

We assume that all the states are available and divergence of the above model is given by

$$\nabla \cdot \vec{F} = \frac{\partial F_1}{\partial x_1} + \frac{\partial F_2}{\partial x_2} + \frac{\partial F_3}{\partial x_3} = -a + c - b < 0 \tag{13}$$

when

$$a + b > c$$

where

$$\vec{F} = (F_1, F_2, F_3) = \vec{F} = (F_1, F_2, F_3) = (a(x_2 - x_1), (c-a)x_1 - x_1x_3 + cx_2, x_1x_2 - bx_3) \tag{14}$$

Thus, system (11) is a forced dissipative system similar to a Lorenz system. Therefore, the solutions of system (11) are bounded as time goes to infinity. Chen shows that system (11) exhibits Chaos for specified values of the parameters [30]. It is worthy noting that it is assumed that all the chaotic states are available for measurement. Process noise is considered in chaos states. The encryption mechanism is described as follows: First, a chaotic digital key is selected from one of the chaotic states.

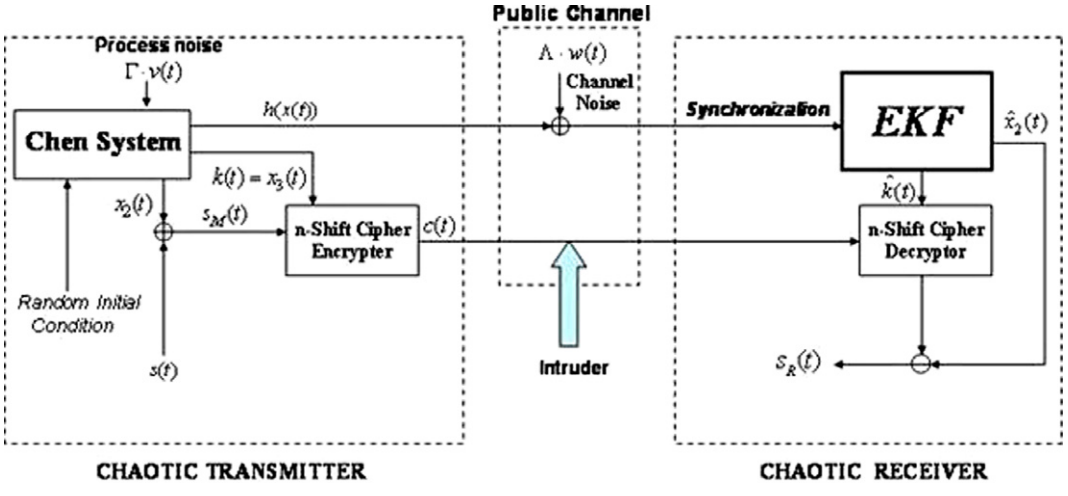


Fig. 2. Block diagram of proposed chaotic communication scheme.

**Remark.** The proposed chaotic communication scheme is totally different from the traditional cryptosystem where both the key and the encrypted signal should be transmitted to the decrypter. It should be pointed out that in this approach, regarding the different employed chaotic states for the objectives of synchronization, masking modulation and multi-shift ciphering algorithm and meanwhile, noting the fact that all chaotic states of a same chaos attractor are inherently absolutely different from each other, there is no requirement for purely transmission of the chaotic key. This in turn, heightens the security level of the system.

The information signal $s(t)$ added with second state according to masking modulation. Then the masked signal $s_M(t) = s(t) + x_2(t)$ will be passed to the $n$-shift cipher block.

The key signal for $n$-shift cipher encrypter is the third state of Chen system

$$k(t) = x_3(t)$$

According to Eqs. (1) and (2) the encryption law with $n = 4$ is as follows:

$$c(t) = e(s(t)) = f_1(f_1(f_1(f_1(s_M(t), k(t), k(t), k(t), k(t)))))$$

The encryption law will encrypt the masked signal $S_M(t)$. Then the output signal $c(t)$ will be passed along with the first state for synchronization. Measurement noise, modeled as white Gaussian, is added to the signal. The major part of the receiver section consists of an extended Kalman filter for state reconstruction, $n$-shift cipher decrypter, and chaos masking demodulator. The Chen states will be estimated by EKF. It should be noted that the first state of Chen will be used for chaotic synchronization. In the receiver, first state goes to the EKF and states will be estimated. The estimate of third state is the key for $n$-shift cipher decryption.

$$\hat{k}(t) = \hat{x}_3(t)$$

After cipher decryption, according to the masking demodulation, second state will be subtracted from cipher decryptor output and information signal will be recovered. According to Eqs. (2) and (3) the recovered decrypted data is as follows:

$$s_R(t) = f_1(f_1(f_1(f_1(c(t), -\hat{k}(t), -\hat{k}(t), -\hat{k}(t), -\hat{k}(t))))) - \hat{x}_2(t)$$

The sum of squared errors (SSE) in state estimation is

$$\mathrm{SSE} = \sqrt{\sum_{i-1}^{3}(x_i(t) - \hat{x}_i(t))^2} \tag{15}$$

The parameters and initial values for chaotic system and EKF that used in our simulation are summarized as follows:

Matrix $A(x(t))$ in our proposed scheme is

$$A(x(t)) = \begin{bmatrix} -a & a & \varepsilon \\ c - a & c & -x_1(t) \\ 0 & x_1(t) & -b \end{bmatrix} \tag{16}$$

where $a = 40$, $b = 3$, $c = 31$. $\varepsilon = 0.0001$ is used for ensuring the observability of $A$ and $C$. The parameters for the multi-shift cipher algorithm are $h = 2$ and $n = 4$. The first chaotic state is employed for synchronization. Therefore, the output measurement matrix is

$$C = [1 \quad 0 \quad 0]$$

The initial conditions for chaotic system and the EKF are

$$x(0) = [-1.0032 \quad 2.3545 \quad -0.087]^{\mathrm{T}}, \qquad \hat{x}(0) = [40 \quad 17 \quad 17]^{\mathrm{T}}$$

The characteristics of the process and channel noise used in EKF are

$$\Gamma = [1 \quad 1 \quad 1]^{\mathrm{T}}, \qquad \Lambda = 1, \qquad V = 0.0161, \qquad W = 0.0202$$

In the Reccati differential equation (10) we can use the initial conditions for the covariance matrix as

$$P(0) = 0.1 \times \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The employed information signal for evaluating the performance of the proposed system is

$$s(t) = \sin(2\pi f t), \qquad f = 2 \text{ Hz}$$

The chaotic system is not restricted to Chen and other types of chaotic systems can be used for the proposed scheme. We used two other chaotic systems named: Lorenz and Genesio-Tesi to show the effectiveness of the proposed chaotic encryption scheme. Lorenz system is described by the following differential equations:

$$\begin{aligned} \dot{x}_1(t) &= -\sigma(x_2(t) - x_1(t)) \\ \dot{x}_2(t) &= -x_1(t)x_3(t) + rx_1(t) - x_2(t) \\ \dot{x}_3(t) &= x_1(t)x_2(t) - bx_3(t) \end{aligned} \tag{17}$$

where $\sigma$, $r$, and $b$ are positive parameters. When $\sigma = 10$, $r = 28$, and $b = 1.25$, system (17) behaves chaotically [9].

Genesio-Tesi is described by the following differential equations:

$$\begin{aligned} \dot{x}_1(t) &= x_2(t) \\ \dot{x}_2(t) &= x_3(t) \\ \dot{x}_3(t) &= -c \cdot x_1(t) - b \cdot x_2(t) - ax_3(t) + x_1^2 \end{aligned} \tag{18}$$

where $a$, $b$, and $c$ are positive parameters. When $a = 1.2$, $b = 2.92$, and $c = 6$, system (18) behaves chaotically [31].

The initial conditions for the Lorenz and Genesio-Tesi systems and also EKF values are the same as in the case of Chen system.

## 5. Simulation experiments

In this section, the performance of the proposed scheme will be studied. We have employed Euler method for numerical simulation in MATLAB with the sampling time 0.001. In Fig. 3, the attractor of Chen dynamical

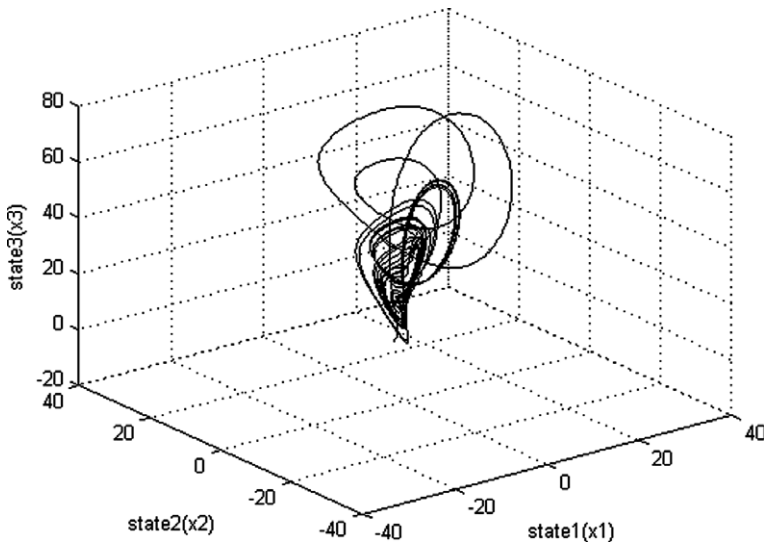


Fig. 3. Attractor of Chen dynamical system.

system can be seen. Figs. 4–6 show the states of Chen system and also their estimates in the same coordinate in the time interval $[0, 5]$ s. The convergence of states is so fast and after a very short time the estimations are synchronized to the original states. We can see the precision of synchronization with EKF in Figs. 4–6. The convergence times of three states of Chen system are shown in Table 1. The maximum of the three values is considered as the convergence time of the system and it is 0.201 s in this case. Fig. 7 shows sum squared

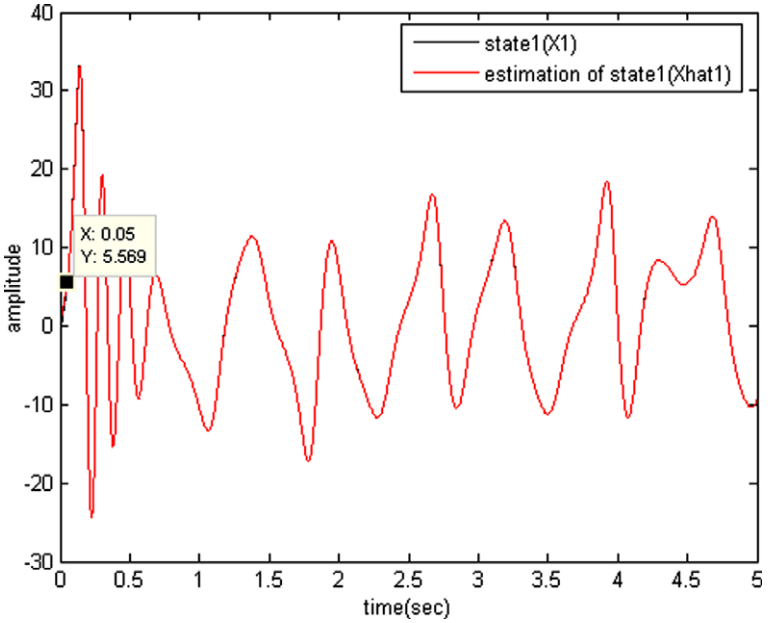


Fig. 4. First state and its estimation (Chen).

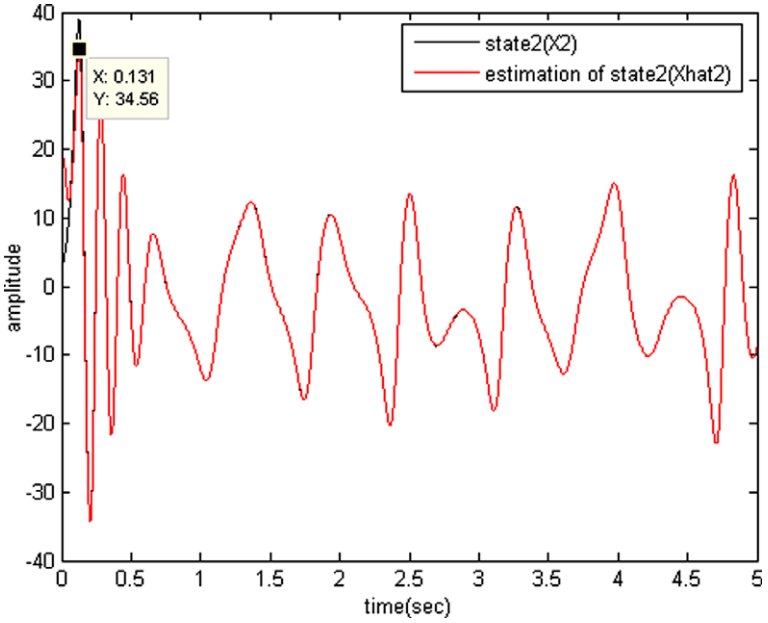


Fig. 5. Second state and its estimation (Chen).

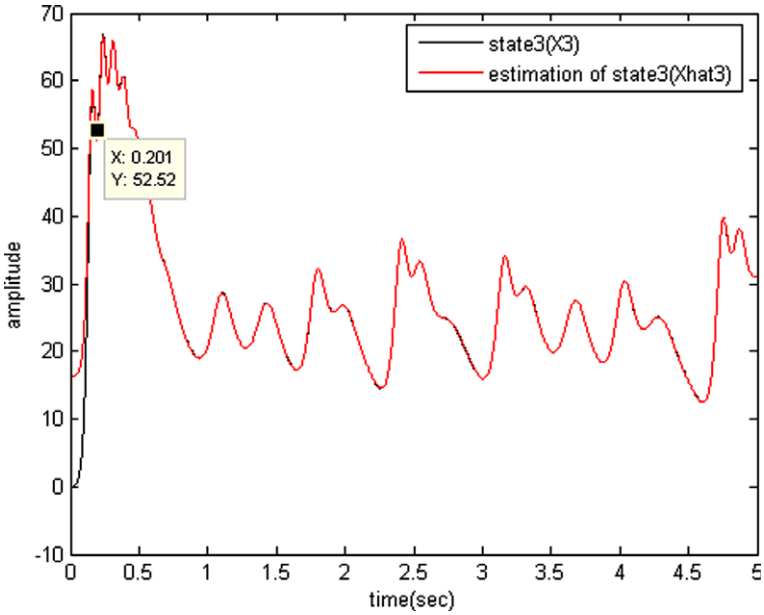


Fig. 6. Third state and its estimation (Chen).

Table 1
Convergence time in state estimation

| Synchronization time | State1 (s) | State2 (s) | State3 (s) | Maximum (s) |
|---|---|---|---|---|
| Chen system | 0.05 | 0.131 | 0.201 | 0.201 |
| Lorenz system | 0.162 | 1.034 | 1.566 | 1.566 |
| Genesio-Tesi | 1.33 | 5.12 | 5.11 | 5.12 |

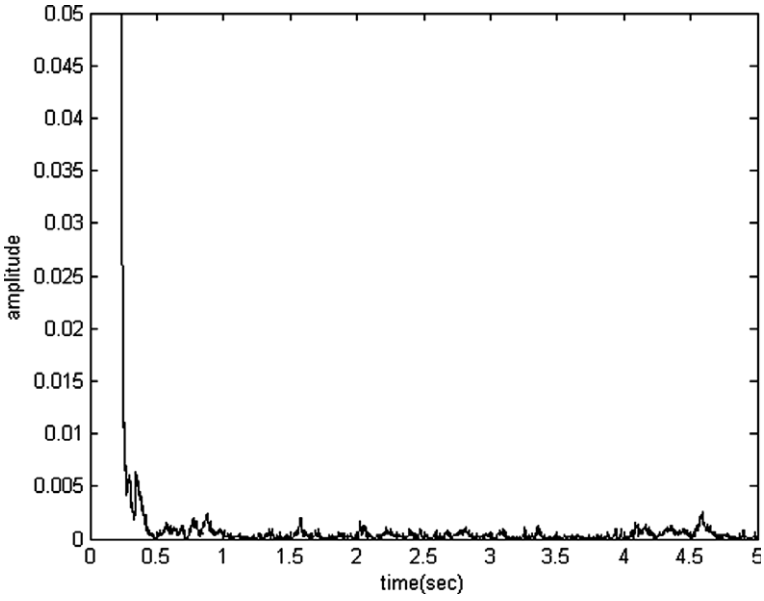


Fig. 7. Sum squared error in state estimation (Chen).

error in state estimation of three states at each point and obviously, it is very low and satisfactory. In Fig. 8, the data that is encrypted by masking can be seen. By looking to this signal we can not understand the message. After that, the encrypted data is ciphered with n-cipher algorithm to enhance the security and as a result, it is more difficult to break the encryption. Fig. 9 shows the masked-ciphered data and from it we can see the signal is unintelligible. Fig. 10 shows the original sinusoid data and the recovered data in the same coordinate. We can see that the recovered data is nearly the same as the original data. As indicated in Table 2, after 0.206 s the data is recovered and converged nearly to the original data. By using our proposed secure chaotic communication

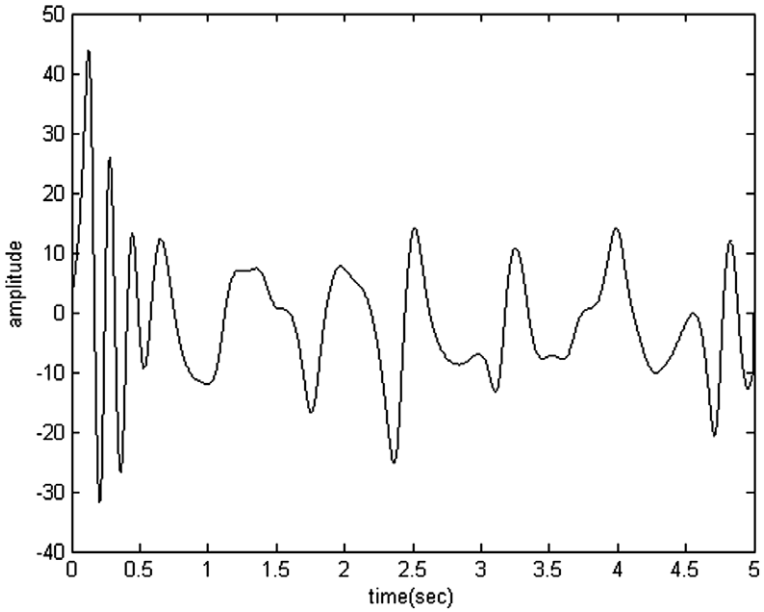


Fig. 8. Data encrypted with masking (Chen).

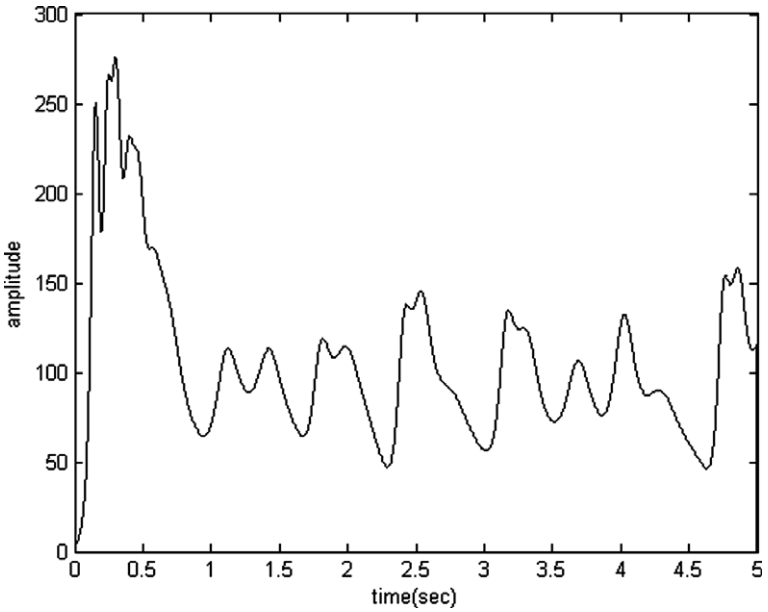


Fig. 9. Data encrypted with masking and *n*-shift cipher (Chen).

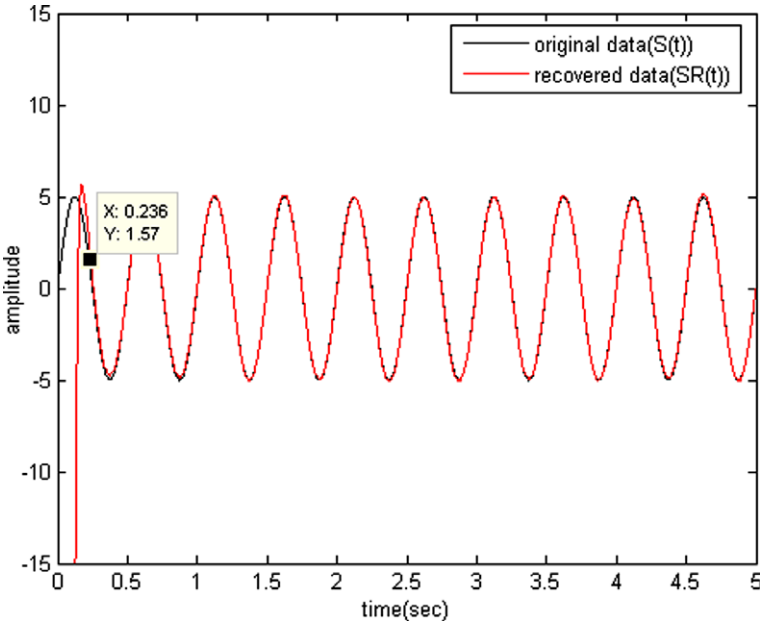


Fig. 10. Original data $S(t)$ and recovered data $\mathrm{SR}(t)$ (Chen).

Table 2
Convergence time of recovered data to the original data

| Type of chaotic system | Time of data convergence (s) |
|---|---|
| Chen system | 0.26 |
| Lorenz system | 1.623 |
| Genesio-Tesi system | 5.66 |

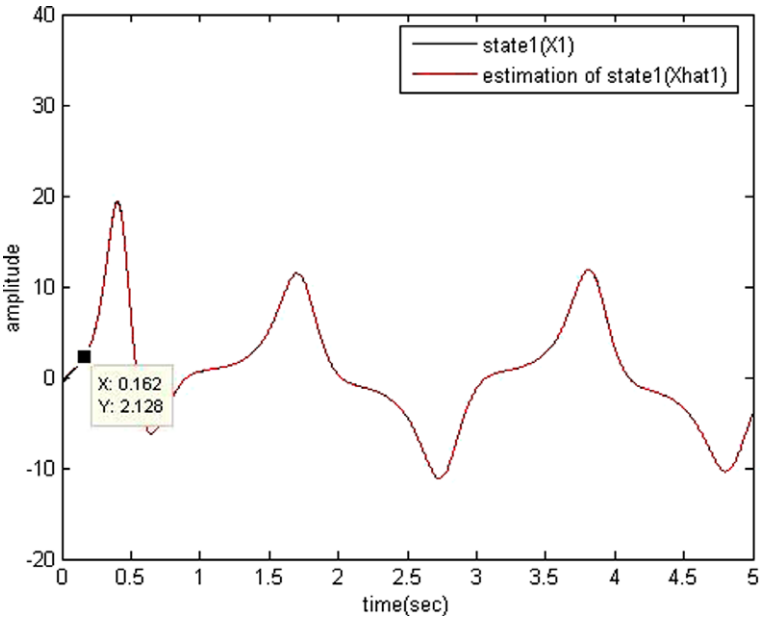


Fig. 11. First state and its estimation (Lorenz).

scheme in the presence of channel noise and processing noise, the data can be recovered precisely. The noise performance of this system is related to the use of EKF for state synchronization.

The results of simulations show that the proposed method work also well with other types of chaotic systems. In Figs. 11–13 Lorenz chaotic states and their estimations can be seen in the time interval of $[0, 5]$ s. It is obvious that all states are regenerated with good accuracy as well as the Chen system. The convergence times of three states of Lorenz system are shown in Table 1. The maximum of the three values

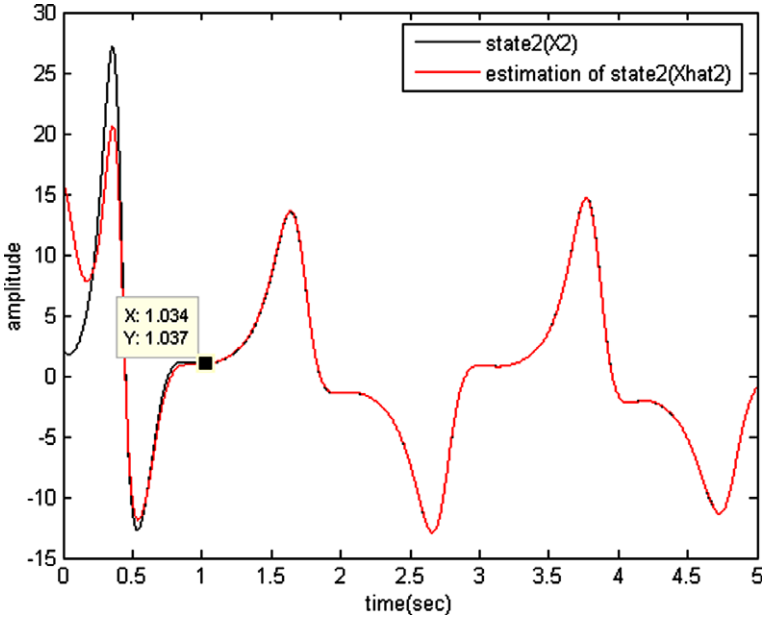


Fig. 12. Second state and its estimation (Lorenz).

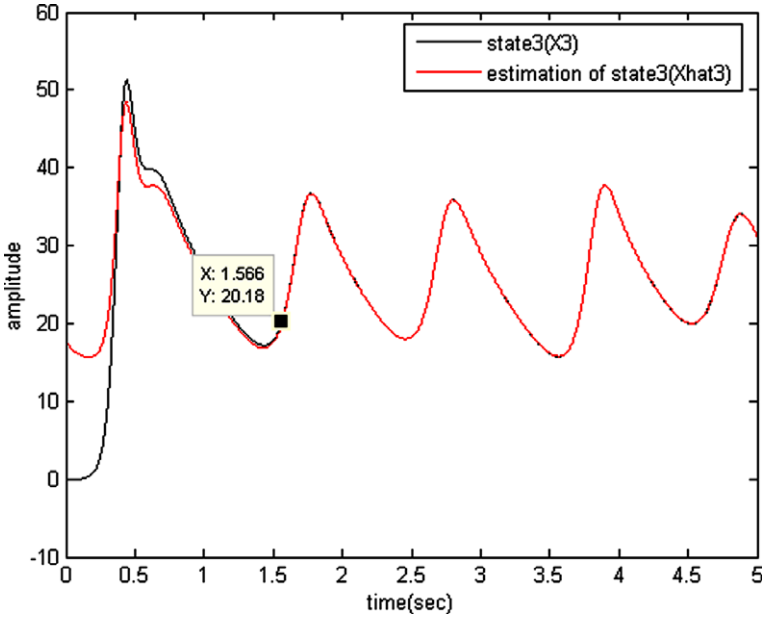


Fig. 13. Third state and its estimation (Lorenz).

is 1.566 s in this case. Fig. 14 shows sum squared error in state estimation of three states at each point and it is very low as the case of Chen system. Fig. 15 shows the sinusoid data that is encrypted with masking. By looking to this signal we could not understand the message as in the pervious case. In Fig. 16 the masked-ciphered signal is shown. The resultant signal is also unintelligible as the case of Chen system. Fig. 17 shows the original sinusoid data and also the recovered data in the case of Lorenz system. As indicated in Table 2, after 1.623 s

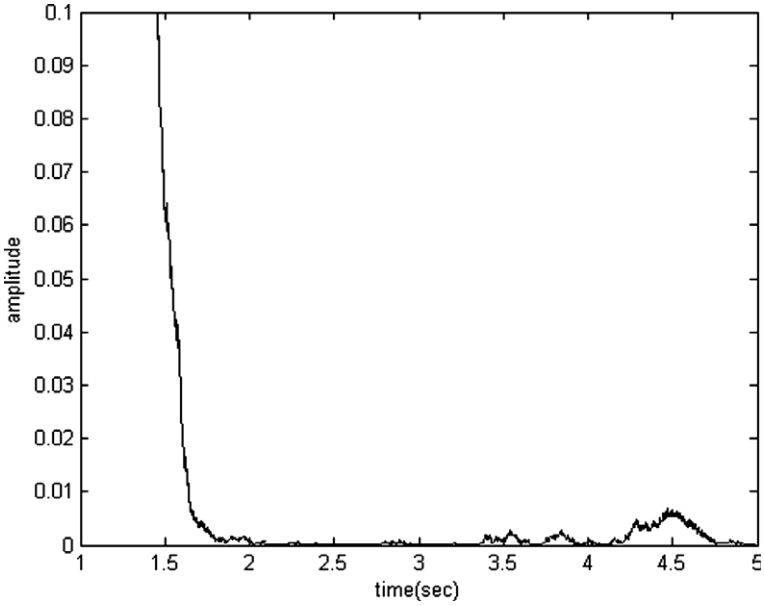


Fig. 14. Sum squared error in state estimation (Lorenz).

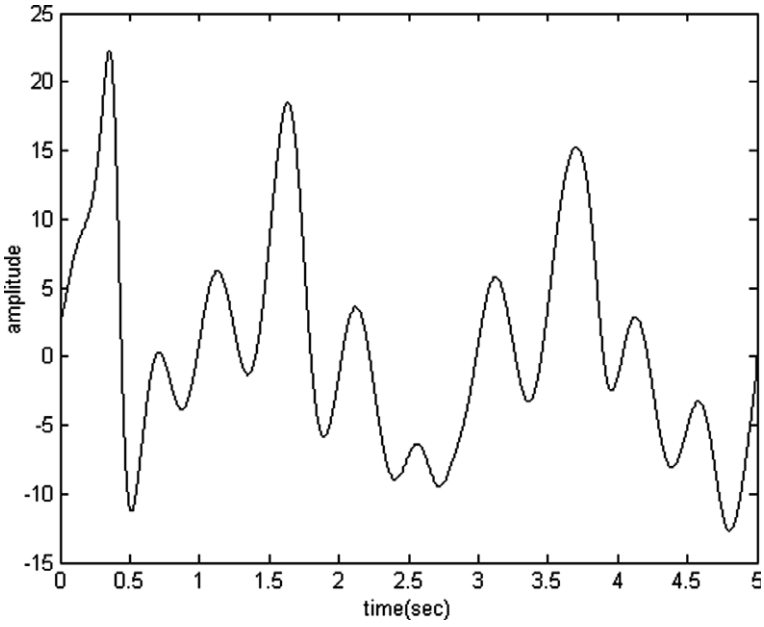


Fig. 15. Data encrypted with masking (Lorenz).

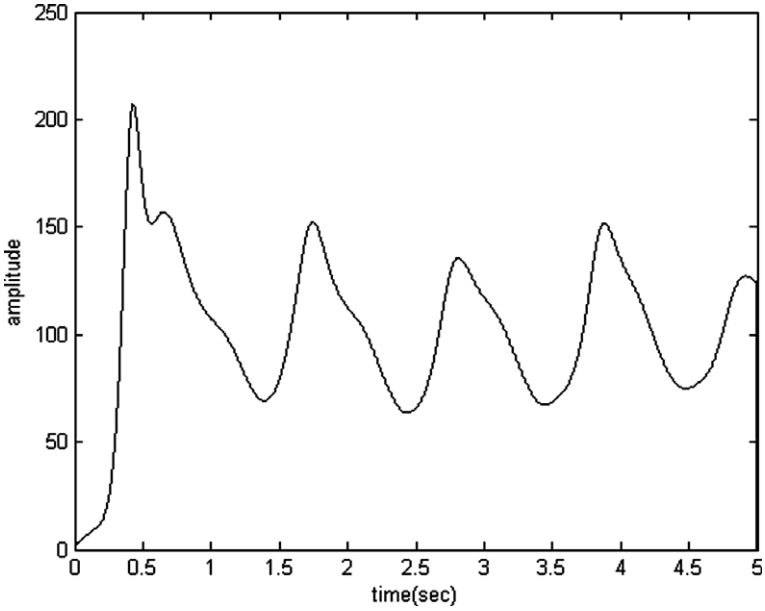


Fig. 16. Data encrypted with masking and $n$-shift cipher (Lorenz).

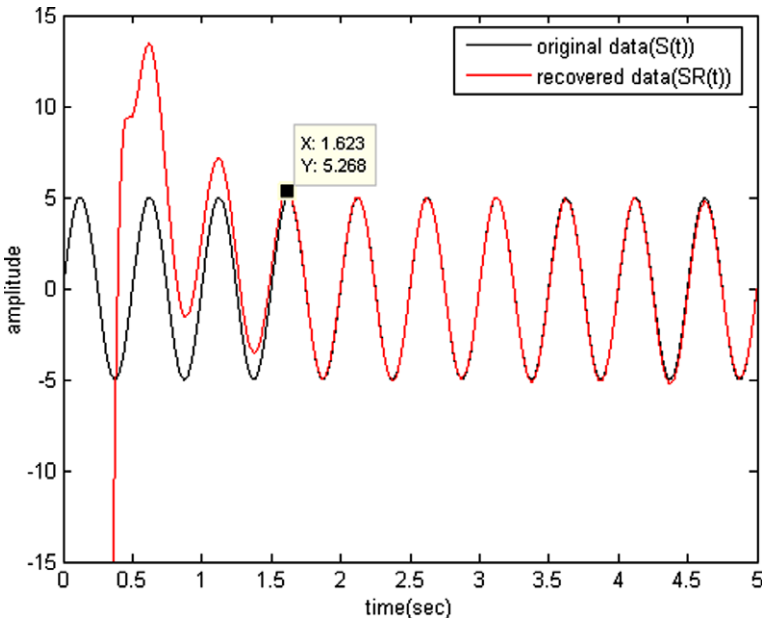


Fig. 17. Original data $S(t)$ and recovered data $\mathrm{SR}(t)$ (Lorenz).

the data is recovered and converged nearly to the original data. This value is 1.5 s more than the previous case. From observing Fig. 17, it is obvious that the data recovery error is very low as before.

Finally, the third system, Genesio-Tesi system, is also implemented to check the performance of the proposed scheme. In Figs. 18–20 Genesio-Tesi chaotic states and their estimations are shown in the time interval of $[0, 20]$ s. All of the states are regenerated with good accuracy as well as the Chen system. The convergence

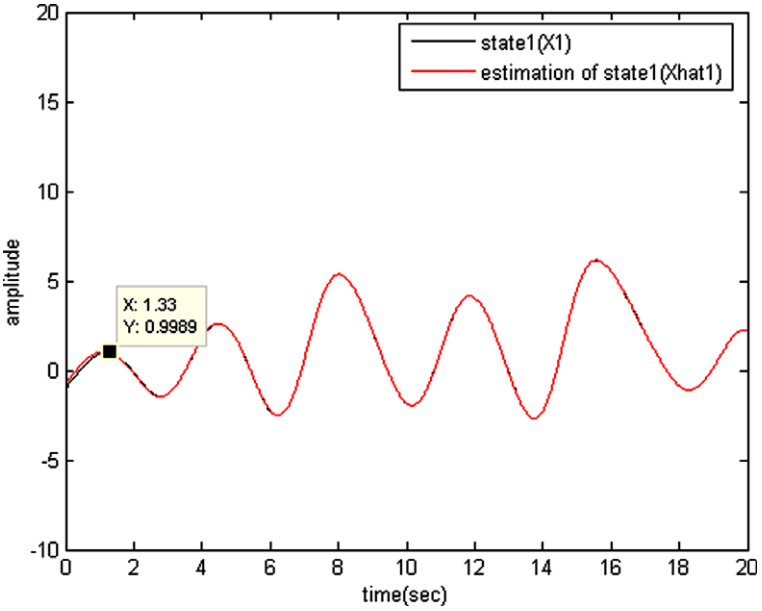


Fig. 18. First state and its estimation (Genesio-Tesi).

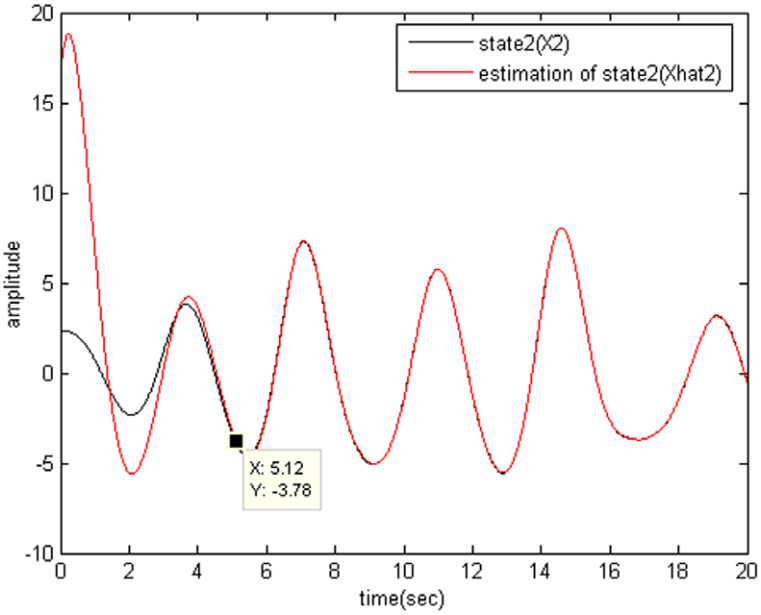


Fig. 19. Second state and its estimation (Genesio-Tesi).

times of three states of Genesio-Tesi system are shown in Table 1. The maximum of the three values is 5.12 s in this case. This value is more than other two cases. Fig. 21 shows sum squared error in state estimation of three states at each point and they are very low as previous cases. Fig. 22 shows the sinusoid data that is encrypted with masking. In Fig. 23, masked data which is ciphered by *n*-shift cipher algorithm is demonstrated. Fig. 24 shows the original sinusoid data and also the recovered data in the case of Genesio-Tesi system. As indicated

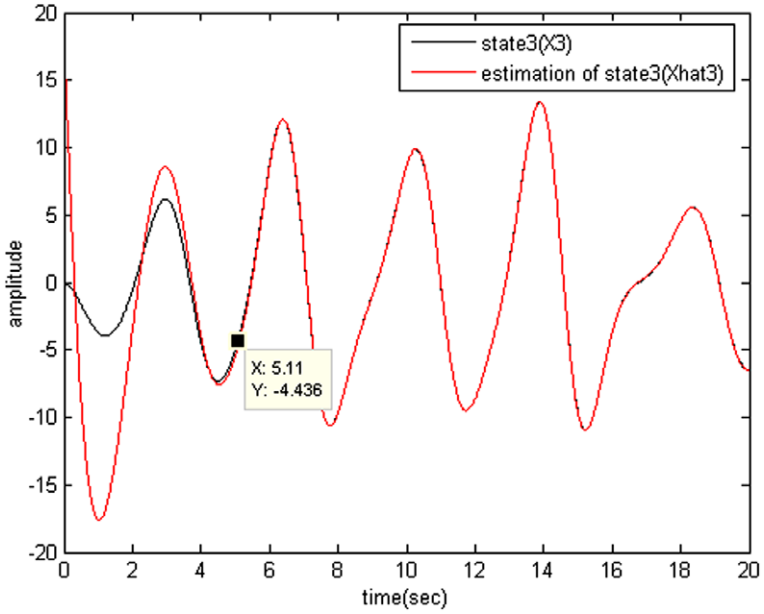


Fig. 20. Third state and its estimation (Genesio-Tesi).

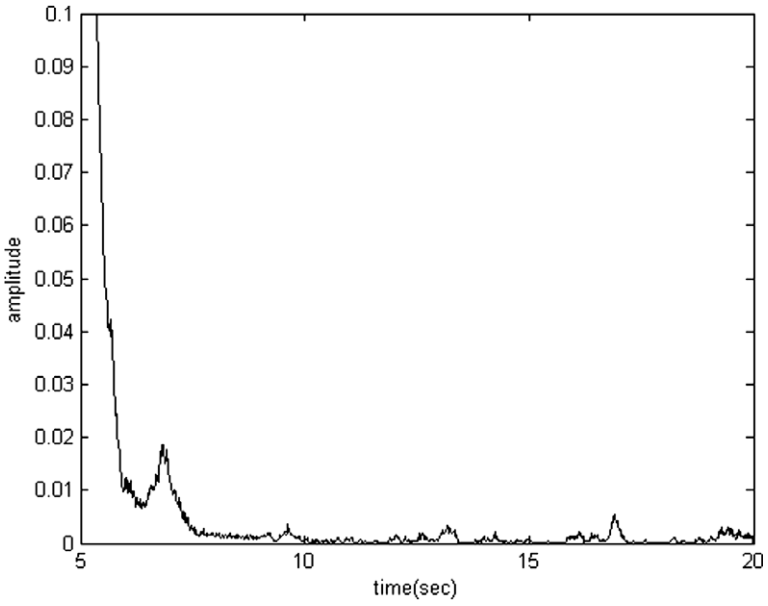


Fig. 21. Sum squared error in state estimation (Genesio-Tesi).

in Table 2, after 5.66 s the data is recovered and converged nearly to the original data. This value is more than as the cases of other two systems. Data recovery error is also very low as before.

## 6. Conclusion

In order to improve the security of data transmission, a chaotic communication method based on multi-shift ciphering is presented. The stochastic extended Kalman filter is used for state reconstruction in noisy

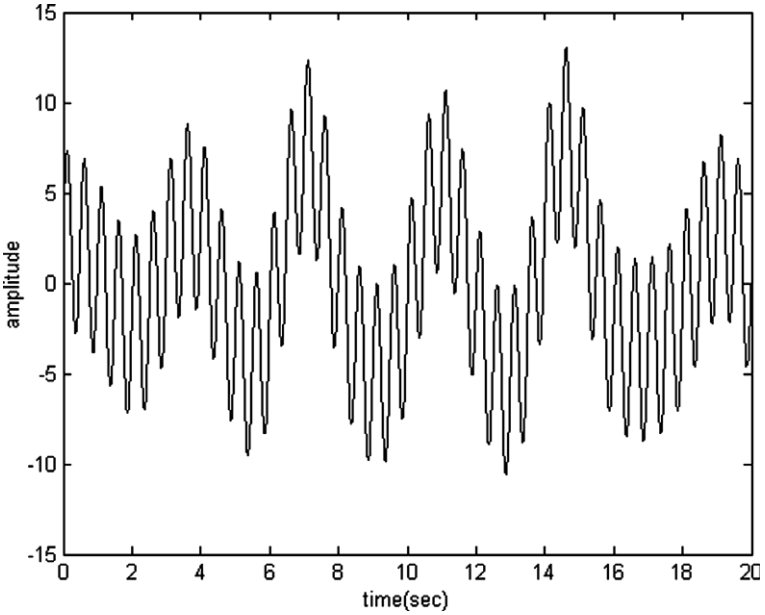


Fig. 22. Data encrypted with masking (Genesio-Tesi).

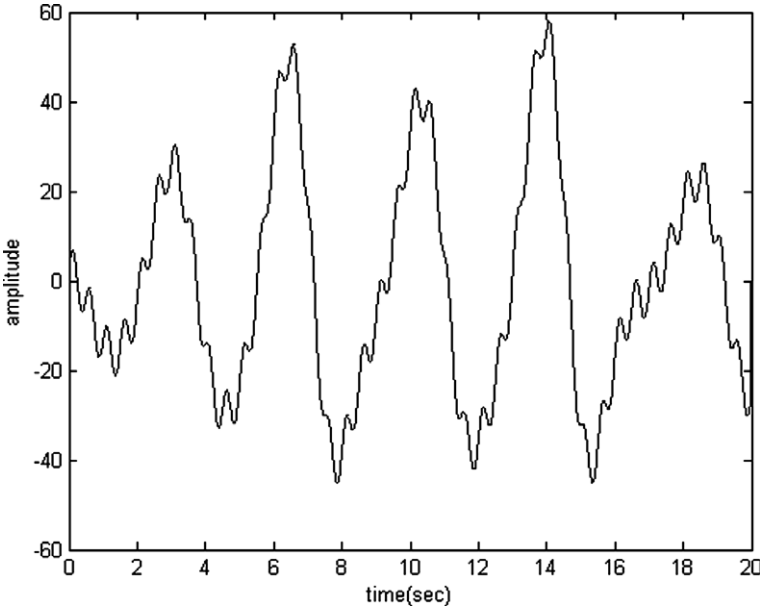


Fig. 23. Data encrypted with masking and *n*-shift cipher (Genesio).

environment. The proposed chaotic communication scheme is totally different from the traditional cryptosystems due to employing different chaos states for the synchronization and the encryption. To inspect the performance of the proposed system, three types of nonlinear dynamics have implemented. From the simulation results, the performance of the proposed systems seems to be satisfactory for secure communication applications. Also, the results are sufficiently acceptable for digital data.

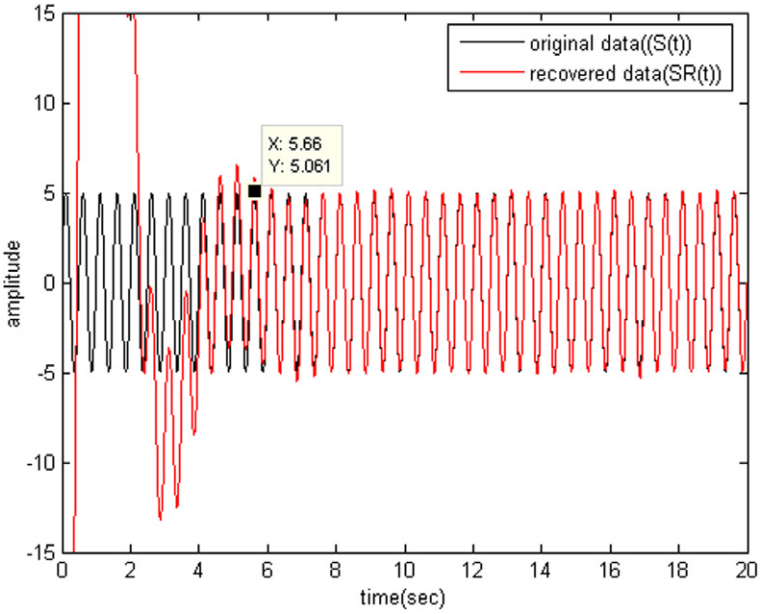


Fig. 24. Original data $S(t)$ and recovered data $SR(t)$ (Genesio).

## References

[1] Heidari-Bateni G, McGillem CD. A chaotic direct-sequence spread spectrum communication system. IEEE Trans Commun 1994;42(2/3/4):1524–7.
[2] Satish K, Jayakar T, Tobin C, Madhavi K, Murali K. Chaos based spread spectrum image steganography. In: Satish K et al., editors. Chaos based spread spectrum image steganography. IEEE; 2005. p. 587–90.
[3] Kolumban G, Kennedy MP, Chua LO. The role of synchronization in digital communications using chaos—Part I: Fundamentals of digital communications. IEEE Trans Circuits Syst I 1997;44(October):927–36.
[4] Kolumban G, Kennedy MP, Chua LO. The role of synchronization in digital communications using chaos—Part II: Chaotic modulation and chaotic synchronization. IEEE Trans Circuits Syst I 1998;45(November):1129–40.
[5] Kolumban G, Kennedy MP. The role of synchronization in digital communications using chaos—Part III: Performance bounds for correlation receivers. IEEE Trans Circuits Syst I 2000;47(December):1673–83.
[6] Dachselt F, Schwatrz W. Chaos and cryptography. IEEE Trans Circuits Syst I 2001;48(Dec.):1498–509.
[7] Azemi A, Raoufi R, Fallahi K, Hosseini-Khayat S. A sliding-mode adaptive observer chaotic communication scheme. In: 13th Iranian Conference on Electrical Engineering (ICEE2005), vol. 2, Zanjan, Iran, May 10–12, 2005.
[8] Peccora LM, Carroll TL. Synchronization in chaotic systems. Phys Rev Lett 1990;64(February):821–4.
[9] Pecora LM, Carroll TL, Johnson GA, Mar DJ. Fundamentals of synchronization in chaotic systems, concepts, and applications. 1997 American Institute of Physics. Chaos 1997;7(4):520–42.
[10] Cuomo KM, Oppenheim AV. Circuit implementation of synchronized chaos with applications to communication. Phys Rev Lett 1993;71:65–8.
[11] Kocarev L, Ha1le KS, Eckert K, Chua LO. Experimental demonstration of secure communication via chaotic synchronization. Int J Bifurcat Chaos 1992;2:709–13.
[12] Murali K. Digital signal transmission with cascaded heterogeneous chaotic systems. Phys Rev E 2001;63:016217–23.
[13] Murali K, Yu H, Varadan V, Leung H. Secure communication using a chaos based signal encryption scheme. In: Murali et al., Secure communication using a chaos based signal encryption scheme, IEEE; 2001. p. 709–14.
[14] Dedieu H, Kennedy MP, Hasler M. Chaos shift keying: modulation and demodulation of a chaotic character using self-synchronizing Chua's circuits. IEEE Trans Circuits Syst II 1993;40:634–42.
[15] Murali K, Lakshmanan M. Transmission of signals by synchronization in a chaotic Van der Pol–Duffing oscillator. Phys Rev E 1993;48:271–350.
[16] Lakshmanan M, Murali K. Chaos in nonlinear oscillators: controlling and synchronization. Singapore: World Scientific; 1996.
[17] Itoh M. Spread spectrum communication via chaos. Int J Bifurcat Chaos 1996;9:155–213.
[18] Hasler M, Maistrenko Y. An introduction to the synchronization of chaotic systems: coupled skew tent maps. IEEE Trans Circuits Syst 1997;44(October):856–66.
[19] Yang T, Chua LO. Impulsive stabilization for control and synchronization of chaotic systems: theory and application to secure communication. Circuits Syst I: Fundam Theory Appl 1997;44(October):976–88.

[20] Nijmeijer H, Mareels IMY. An observer looks at synchronization. Circuits Syst I: Fundam Theory Appl 1997;44(October):882–90.
[21] Hayes S, Grebogi C, Ott E. Communicating with chaos. Phys Rev Lett 1993;70:3031–4.
[22] Yang T, Wu CW, Chua LO. Cryptography based on chaotic systems. IEEE Trans Circuits Syst—I: Fundam Appl 1997;44(5):469–72.
[23] Ruan H, Zhai T, Yaz EE. A chaotic secure chaotic communication scheme with extended Kalman filter based parameter estimation. In: Proceeding of IEEE conference on control applications, vol. 1; 2003. p. 404–8.
[24] Short KM. Unmasking a modulated chaotic communication scheme. Int J Bifurcat Chaos 1996;6:367–75.
[25] Yang T. Recovery of digital signals from chaotic switching. Int J Circuit Theory Appl 1995;23:611–5.
[26] Perez G, Cerdeira HA. Extracting messages masked by chaos. Phys Rev Lett 1995;74:1970–3.
[27] Shannon CE. Communication theory of secrecy systems. In: Jakimoski, BG, Kocarev lj. Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Trans Circuits Syst Technol J. 28:656–715.
[28] Dmitriev AS, Panas Al, Starkov SO, Kuzmin lV. Experiments on RF band communications using chaos. Int J Bifurcat Chaos 1997;7:2511–27.
[29] Alvarez G, Montoya F, Pastor G, Romera M. Chaotic cryptosystems. Int J Bifurcat Chaos 1999:332–8.
[30] Yessen MT. Chaos control of Chen dynamical system. Chaos, Solitons & Fractals 2002;15:271–83.
[31] Chen M, Zhou D, Shang Y. A sliding mode observer based secure communication scheme. Chaos, Solitons & Fractals 2005;25:573–8.