Jestr Journal of Engineering Science and Technology Review 8 (2) (2015) 96 - 105
Special Issue on Synchronization and Control of Chaos: Theory, Methods and Applications

JOURNAL OF
**Engineering Science and Technology Review**

www.jestr.org

Research Article

# A Private Secure Communication Scheme Using UKF-based Chaos Synchronization

**Komeil Nosrati[*, 1], Ali Shokouhi Rostami[2], Asad Azemi[3] and Farahnaz Mohanna [2]**

[1] *Research and Development Centre, Great Tehran Electrical Distribution Co, Tehran, Iran.*
[2] *Department of Communication Engineering, University of Sistan and Baluchestan, zahedan,Iran.*
[3] *Department of Electrical Engineering, Penn State University, USA.*

Received 24 September 2014; Revised 26 October 2014; Accepted 18 November 2014

***Abstract***

This paper presents a novel chaotic communication method using an Unscented Kalman Filter (UKF). Applying UKF, the method proposes the estimation of the state variables of the chaotic dynamical system and synchronization. The proposed method is then applied to new private secure communication. The chaotic synchronization is implemented by the UKF in the presence of processing noise and measurement noise. The main highlighted advantages of using UKF are increasing accuracy, efficiency and improvement of synchronization's time. Encoding chaotic communication achieves a satisfactory, typical secure communication scheme. To illustrate the effectiveness of the proposed scheme, a numerical example based on the Lorenz dynamical system and Rössler dynamical system is presented and the results are compared to the Extended Kalman Filter (EKF). The results of simulation have shown the improvement of the function in the case of increasing the accuracy and efficiency of the synchronization, and decreasing its time.

*Keywords:* Chaos Synchronization, Unscented Kalman Filter, Secure Communication, Masking Modulation, Encryption.

## 1. Introduction

In the last three decades chaotic behavior, an attractive phenomenon appearing in nonlinear systems, has been received more attentions to study. A chaotic system is a nonlinear deterministic system and its behavior is complex and unpredictable. Two of the most important characteristics of a chaotic system are the sensitivity to the initial conditions and the variations of the system's parameters that make the chaotic synchronization problems much more important. Pecora and Carroll [1] in their pioneering work addressed the synchronization of chaotic system using a drive-response conception. The idea is to use the output of the driving system to control the response system so that the trajectories of the response's outputs can synchronize those of drive system and they oscillate in a synchronized manner. Heretofore, many synchronization schemes have been developed such as inverse system approach [2], system approach [3], linear and nonlinear feedback control [4-6], and system decomposition approach [1,7]. Recently, many efforts have been made to show that the synchronization problem of chaotic systems could be solved through observer design approach [8-12], in which only the input and output information of drive system are used to construct part or all of the state information of drive system, and many beneficial methods have been developed. For example, several kinds of nonlinear observer design methods are summarized and their adaptations to chaotic synchronizations are discussed in [9] and in [12] a sliding-mode adaptive observer synchronization method for chaotic system is developed.

As a brief introductory and historical background, Extended Kalman Filter (EKF) as an optimal observer is a stochastic estimation scheme for estimating of nonlinear state and tracking applications [13]. In this method, Kalman filtering [14] is used to linearize the nonlinear function. The first order Taylor series expansions are applied to linearization.

Application of EKF to synchronization of chaotic systems is studied in [15] and synchronization is obtained of transmitter and receiver dynamics in case the receiver is given via an extended Kalman filter driven by a noisy drive signal from the transmitter. However, a chief drawback of EKF is the error in function approximation because the EKF uses first order Taylor series for approximating the nonlinearities. So, large errors may be happened when it is used to systems with higher order nonlinearities. For overcoming the drawbacks associated with the approximation errors, many alternatives to EKF have been offered. Unscented Kalman Filter (UKF), as recently proposed by Julier and Uhlman [16], could in theory improve

* E-mail address: komeilnosrati@gmail.com

upon EKF for state estimation since linearization is avoided by an unscented transformation and at least second order accuracy is provided.

This last point is achieved by carefully choosing a set of sigma points, which captures the true mean and covariance of a given distribution and then passing the means and co-variances of estimated states through a nonlinear transformation. As a result, UKF is capable of estimating the posterior mean and co-variances accurately to a high order [17].

In this paper, the UKF is applied for the synchronization of the chaotic system. The chaotic synchronization is implemented by the UKF in the presence of processing noise and measurement noise, and performance according to estimation error is evaluated in comparison with the EKF.

One of the most important applications of chaotic synchronization is that it can be applied to secure communication [11,18]. In chaotic secure communication schemes, a chaotic system is used as a transmitter and the information signal is mixed at the transmitter side to generate a chaotic transmitting signal. Then this signal transmitted to the receiver side. The receiver is also a chaotic dynamic system and it is able to synchronize the transmitter by receiving the transmitting signal and one of states that is passed to the receiver module to improve synchronization. The information signal can be recovered by the receiver, when synchronization is achieved.

This work, inspired by previous works [19-21], develops an UKF-based approach which can reach not only chaotic synchronization but also can be applied to secure communications. For this purpose, the major part of the receiver section consists of an UKF for state reconstruction and chaos masking demodulator. In this work, the Lorenz chaotic system and the Rössler chaotic system are used to modulate sinusoid (analog) data and digital data via masking modulation. Additive White Gaussian Noise (AWGN) channel is used as a medium for transmitting the modulated signal. At the receiver, UKF is employed to estimate states of the chaotic systems. The proposed scheme uses Lorenz and Rössler chaotic system as chaos generators to encrypt data using masking modulation.

This paper is organized as follows: In section 2, a brief review of chaotic systems, Kalman filtering, principles and algorithms of EKF and UKF is presented. The proposed chaotic secure communication scheme is provided in section 3. In section 4, the results of simulation on Lorenz chaotic system and Rössler chaotic system with using of UKF and EKF and their application in proposed chaotic secure communication scheme are presented. Section 5 deals with concluding remarks.

## 2. Chaotic systems and UKF synchronization

In order to understand the proposed system a brief review on the chaotic dynamical systems and their synchronization will be given.

### 2.1. Chaotic Systems

A chaotic system is a nonlinear deterministic system and its behavior is complex and unpredictable. Two of the most important characteristics of a chaotic system are the sensitivity to the initial conditions and the variations of the system's parameters that make the chaotic synchronization problems much more important.

The Lorenz system as a chaotic dynamical system can be described by the following differential equations:

$$\begin{cases} \dfrac{dx_1}{dt} = -\sigma(x_1 - x_2) \\ \dfrac{dx_2}{dt} = -x_1 x_3 + \rho x_1 - x_2 \\ \dfrac{dx_3}{dt} = x_1 x_2 - \beta x_3 \end{cases} \quad (1)$$

when $\sigma = 10$, $\beta = 8/3$ and $\rho = 25$ the oscillator behaves chaotically. Rossler system can be described by the following set of differential equations:

$$\begin{cases} \dfrac{dx_1}{dt} = ax_1 + x_2 \\ \dfrac{dx_2}{dt} = -x_1 - x_3 \\ \dfrac{dx_3}{dt} = b - cx_3 + x_2 x_3 \end{cases} \quad (2)$$

when $a = 0.1$, $b = 0.1$ and $c = 14$ system behaves chaotically.

### 2.2. Kalman Filter

The Kalman Filter (KF) is a recursive filtering tool which has been developed for estimating the trajectory of a system from a series of noisy and/or incomplete observations of the system's state. It has the following specifications. First, the estimation process is formulated in the system's state space; second, the solution is obtained by recursive computation; third, it uses an adaptive algorithm, which can be directly applied to stationary and non-stationary environment. In the Kalman filtering algorithm, every new estimate of the state is retrieved from the previous one and the new input so that only the previous estimated result need to be stored. Thus, the Kalman filter is more effective in computation than those which use all or considerable amount of the previous data directly in each estimation [22].

If the system is nonlinear, the Kalman filter cannot be applied directly, but two nonlinear Kalman filtering methods, namely, EKF and UKF are applied for stochastic nonlinear system estimation.

#### 2.2.1. Extended Kalman Filter

The Extended Kalman Filter (EKF) is a set of mathematical equations which uses an underlying process model to make an estimate of the current state of a system and then corrects the estimate using any available sensor measurements. Using this predictor-corrector mechanism, it approximates an optimal estimate due to the linearization of the process and measurement models [23]. The representation of all the details of the EKF is beyond the scope of this paper.

Therefore, we omit some theoretical considerations and present a more algorithmic description.

To illustrate the principle behind the EKF, Let a nonlinear system be represented by the following standard discrete time equations:

$$\begin{aligned} x_{k+1} &= f(x_k) + w_k \\ y_k &= H_k x_k + v_k \end{aligned} \tag{3}$$

where, $k \in N$ is discrete time and $N$ denotes the set of natural numbers. $x_k \in R^{L\times 1}$ is the state, and $y_k \in R^{M\times 1}$ is the measurement. The nonlinear mapping $f(\cdot)$ is assumed to be continuously differentiable with respect to $x_k$ and $H_k$ is a measurement matrix. Moreover, $w_k \in R^{L\times 1}$ and $v_k \in R^{M\times 1}$ are uncorrelated zero-mean Gaussian white sequences and their co variances are as follows:

$$E\left[w_k w_j^T\right] = Q_k \delta_{kj},\ E\left[v_k v_j^T\right] = R_k \delta_{kj},\ E\left[w_k v_j^T\right] = 0 \tag{4}$$

To estimate signal, the error covariance matrix can be expressed as:

$$P(k\,|\,k) = E\left\{\left[x_k - \hat{x}_k\right]\left[x_k - \hat{x}_k\right]^T\right\} \tag{5}$$

where $x_k$, is the true value of the states and $\hat{x}_k$ is its estimation.

Using the method of optimal linearization, the propagation of the error covariance matrix and the Kalman gain $K$ can be expressed as:

$$\begin{aligned} P_{k|k-1} &= F_{k-1} P_{k-1|k-1} F_{k-1}^T + Q_k \\ K &= P_{k|k-1} C^T \left[C P_{k|k-1} C^T + R_k\right]^{-1} \\ \hat{x}_{k|k} &= \hat{x}_{k|k-1} + K\left[y_k - H_k \hat{x}_{k|k-1}\right] \\ P_{k|k} &= (I - KC) P_{k|k-1} \end{aligned} \tag{6}$$

where $F_{k-1} = \left.\dfrac{\partial f(x)}{\partial x}\right|_{x=\hat{x}_{k-1}}$ is the Jacobian matrix and $\hat{x}_{k|k-1} = f(\hat{x}_{k-1|k-1})$.

Fig. 1(a) illustrates that how the Extended Kalman Filter linearizes a nonlinear function around the mean of a Gaussian distribution, and then propagates the mean and covariance through this linearized model.

### 2.2.2. Unscented Kalman Filter

The problem of propagating Gaussian random variables through a nonlinear function can also be approached using another technique, namely the unscented transform (UT). Instead of linearization required by the EKF, a new approximate method UT is used in the UKF [16].

A set of weighted sigma points is deterministically chosen so that the sample mean and sample covariance of these points match those of a priori distribution. The nonlinear function is applied to each of these points in turn to yield transformed samples, and the predicted mean and covariance are calculated from the transformed samples as shown in Fig. 1(b). This strategy typically does both decrease the computational complexity, while at the same time increasing estimate accuracy, yielding faster, more accurate results.

The fundamental difference between EKF and UKF lies in the way that the Gaussian Random Variables (GRV) are represented in the process of propagating through the system dynamics. Basically, the UKF captures the posterior mean and co-variance of the GRV accurately to the third order (in terms of Taylor series expansion) for any form of nonlinearity, whereas the EKF only achieves first-order accuracy. Moreover, since no explicit Jacobian or Hession calculations are necessary in the UKF algorithm, the computational complexity of UKF is comparable to EKF.

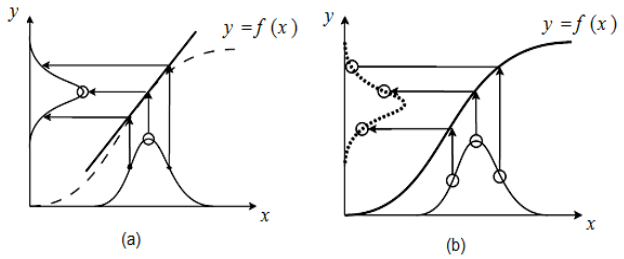


**Fig. 1.** The principle propagating Gaussian random variables through a nonlinear function. (a) Propagating the mean and covariance through this linearized model (EKF). (b) The propagating of sigma points through a nonlinear function (UKF) [24].

The algorithm for implementing the UKF can be summarized as follows [25]. Consider the nonlinear discrete-time system represented by

$$\begin{aligned} x_{k+1} &= f(x_k) + w_k \\ y_k &= H_k x_k + v_k \end{aligned} \tag{7}$$

Similar to previous part, $k \in N$ is discrete time and $N$ denotes the set of natural numbers. $x_k \in R^{L\times 1}$ is the state, and $y_k \in R^{M\times 1}$ is the measurement. The nonlinear mapping $f(\cdot)$ is assumed to be continuously differentiable with respect to $x_k$ and $H_k$ is a measurement matrix. Moreover, $w_k \in R^{L\times 1}$ and $v_k \in R^{M\times 1}$ are uncorrelated zero-mean Gaussian white sequences and have the following characteristics:

$$E\left[w_k w_j^T\right] = Q_k \delta_{kj},\ E\left[v_k v_j^T\right] = R_k \delta_{kj},\ E\left[w_k v_j^T\right] = 0 \tag{8}$$

*Step 1:* The L-dimensional random variable $x_{k-1}$ with mean $\hat{x}_{k-1}$ and covariance $\hat{P}_{k-1}$ is approximated by sigma points which are computed with the following equations:

$$\begin{cases} \chi_{i,k-1} = \hat{x}_{k-1}, & i = 0 \\ \chi_{i,k-1} = \hat{x}_{k-1} + \left(a\sqrt{L\hat{P}_{k-1}}\right)_i, & i = 1,2,...,L \\ \chi_{i,k-1} = \hat{x}_{k-1} - \left(a\sqrt{L\hat{P}_{k-1}}\right)_{i-L}, & i = L+1,...,2L \end{cases} \tag{9}$$

where $a \in R$ is a tuning parameter denoting the spread of the sigma points around $\hat{x}_{k-1}$ and $(a\sqrt{L\hat{P}_{k-1}})_i$ is the $i^{th}$ column of the matrix square root of $L\hat{P}_{k-1}$. The parameter is often set to a small positive value.

Step 2: Prediction. Each point is instantiated through the process model to yield a set of transformed samples as (10).

$$\chi_{i,k|k-1} = f(\chi_{i,k-1}), \quad i = 0,\ 1,\ ...,\ 2L \tag{10}$$

The predicted mean and covariance are computed as:

$$\hat{x}_{k|k-1} = \sum_{i=0}^{2L} w_i \chi_{i,k|k-1} \tag{11}$$

$$\hat{P}_{k|k-1} = \sum_{i=0}^{2L} \left[ w_i (\chi_{i,k|k-1} - \hat{x}_{k|k-1})(\chi_{i,k|k-1} - \hat{x}_{k|k-1})^T \right] + Q_k \tag{12}$$

where

$$\begin{cases} w_i = 1 - \dfrac{1}{a^2}, & i = 0 \\ w_i = \dfrac{1}{2La^2}, & i = 1,...,2L \end{cases} \tag{13}$$

*Step 3:* Update. As the measurement equation is linear, measurement update can be performed with the same equations as the classical Kalman filter as (14).

$$\begin{aligned} &\hat{y}_k = H_k \hat{x}_{k|k-1} \\ &\hat{P}_{yy} = H_k \hat{P}_{k|k-1} H_k^T + R_k \\ &\hat{P}_{xy} = \hat{P}_{k|k-1} H_k^T \\ &K = \hat{P}_{xy} \hat{P}_{yy}^{-1} \\ &\hat{x}_k = \hat{x}_{k|k-1} + K(y_k - \hat{y}_k) \\ &\hat{P}_k = \hat{P}_{k|k-1} - K\hat{P}_{xy}^T \end{aligned} \tag{14}$$

*Step 4:* Repeat steps 1 to 3 for the next sample. Clearly, the implementation of the UKF is extremely convenient, because Jacobian matrix is not needed to be evaluated which is necessary in the EKF.

## 3. Proposed Chaotic Secure Communication Scheme

By using a chaotic oscillator as a broadband pseudo-random signal generator and masking the message with this signal, to produce an unintelligible signal, the encrypted data can be transmitted through the unsecure communication noisy channel. At receiver, by regenerating the pseudo-random signal using of synchronization and combining it with the received signal (encrypted data) through the inverse operation, the original message is recovered [21].

In proposed scheme, the synchronization is achieved by the UKF acting as the state estimator in the presence of noise and we have enhanced the accuracy of the recovered signal by using the UKF instead of the EKF. The block diagram of the proposed scheme for secure communication is shown in Fig. 2. This 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 (consists of a chaotic system and an encryption mechanism), a communication channel, and a receiver module. In this system, the chaotic signal is generated by using the Lorenz chaotic system that is described by (1) and process noise is considered in chaos states.

The mechanism of encryption is based on masking modulator. The algorithm of encryption process can be described as follows [20]:

The information signal $s(t)$ is added to the second state and then the encrypted signal $s_M(t)$ that is the sum of $s(t)$ and $x_2(t)$, passes through an AWGN channel. The first state of Lorenz chaotic system, $x_1(t)$, is also passed to the receiver module to synchronization. The major part of the receiver side consists of an UKF for state reconstruction and chaos masking demodulator. The Lorenz chaotic states are estimated by the UKF. It should be noted that the first state of the Lorenz is used for chaotic synchronization. In the receiver, the $x_1(t)$ goes to the UKF and other states are estimated.

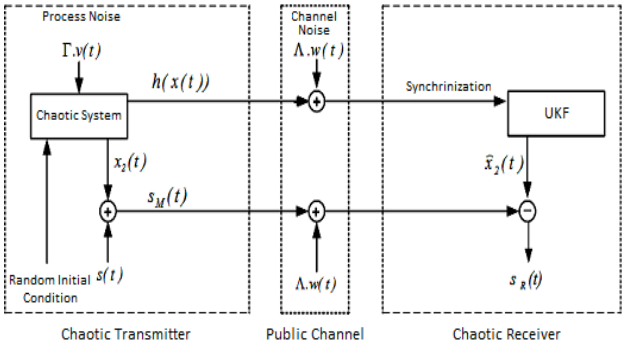


**Fig. 2.** Block diagram of the proposed chaotic secure communication scheme.

The performance of synchronization method and the proposed scheme will be studied. The Lorenz chaotic system is used to illustrate the effectiveness of the proposed methods. The initial conditions for this chaotic system, the EKF and UKF are as follows:

$$\begin{cases} x(0) = \begin{pmatrix} -1.0032 & 2.3545 & -0.087 \end{pmatrix}^T \\ \hat{x}(0) = \begin{pmatrix} 20 & 15 & 15 \end{pmatrix}^T \end{cases} \tag{15}$$

The characteristics of the process and channel noise used in the EKF and UKF are as follows:

$$\Gamma = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}^T, \quad \Lambda = 1, \quad R_k = 0.2, \quad Q_k = 0.18 \tag{16}$$

The employed analog information signal for evaluating the performance of the proposed system is cited underneath:

$$s(t) = 5 \cdot Sin(2\pi ft), \quad f = 2Hz \tag{17}$$

The chaotic system is not restricted to Lorenz and other types of chaotic dynamics in order to be used for the proposed scheme. Another chaos generator which can be used in the proposed system is Rössler dynamical system which has been described by the system model of differential Eq. (2). The initial conditions for the Rössler dynamical

system and also EKF and UKF values are the same as those for the Lorenz system.

## 4. Simulation Results

In this section, the performance of synchronization method and the proposed communication scheme will be analyzed. The Euler method for numerical simulation in MATLAB is used by 0.001 as the sampling time. In Fig. 3, the attractor of the chaotic Lorenz system is illustrated, Fig. 4-6 show the three states of the Lorenz system and their estimations in the time interval between 0 and 50 by the use of the UKF. The estimations have been synchronized to the original states after a short while. The convergence times of the three states of Lorenz system by the use of the UKF and the EKF have been shown in Table 1. The maximum of the three values by the UKF is considered as the convergence time of the system which is 0.899 second. This value for the EKF is 0.979 second. For comparing the UKF and the EKF, we have included plots of absolute estimation errors for the three states using these methods in Fig. 7-9. The results show absolute estimation errors of the three states in the UKF are clearly less than the EKF. To illustrate this more, we have calculated the mean squared error (MSE) for the three states by the use of the UKF and the EKF. The MSE in state estimation is as follows:

$$MSE = \frac{1}{N}\sum_{i=0}^{N}\left(x_k(i)-\hat{x}_k(i)\right)^2, \quad k=1,\ 2,\ 3 \tag{18}$$

where $x_k(i)$ and $\hat{x}_k(i)$ are the $k^{th}$ state variable and its estimate at instant of $i$ respectively. As it can be observed in Table 2, the UKF method has more accuracy than the EKF.

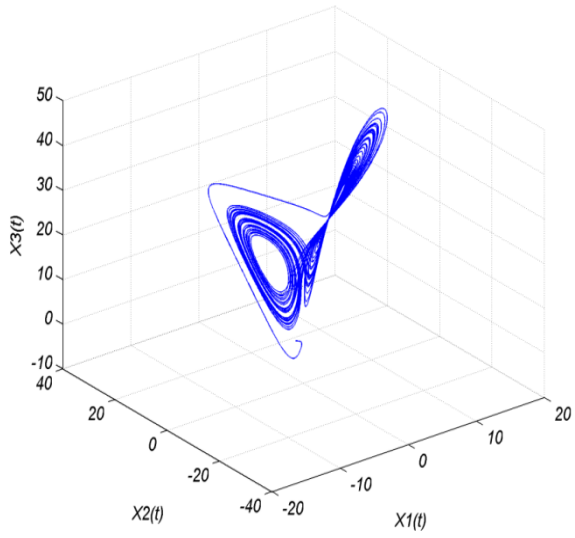


**Fig. 3.** Attractor of Lorenz dynamical system.

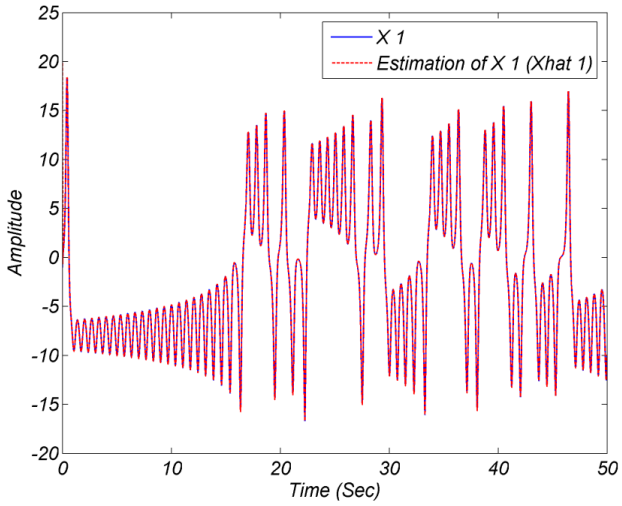


**Fig. 4.** First state of Lorenz system and its estimate.

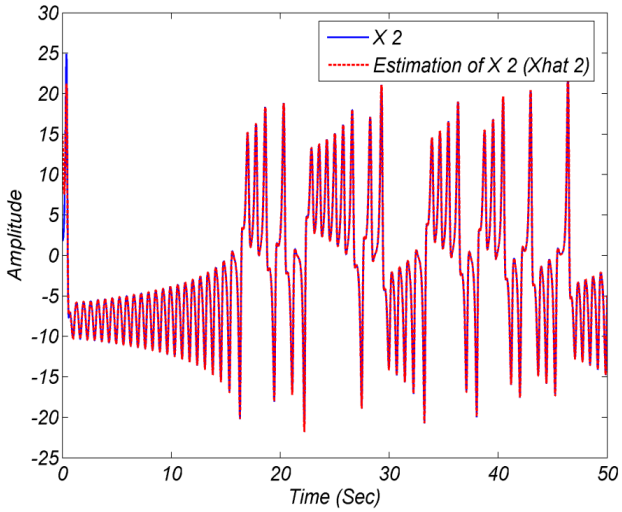


**Fig. 5.** Second state of Lorenz system and its estimate.

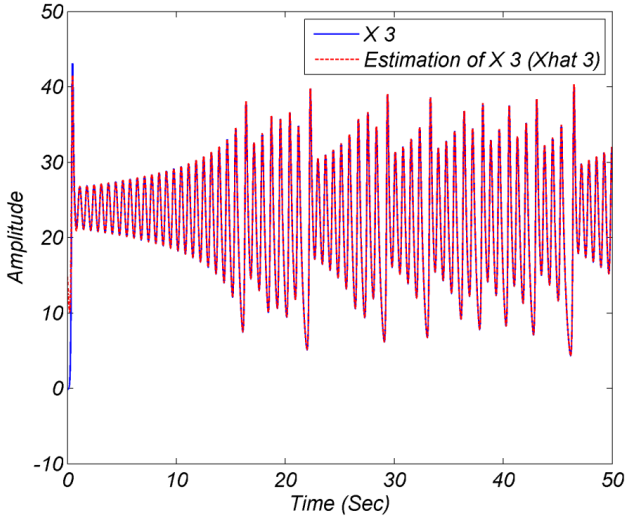


**Fig. 6.** Third state of Lorenz system and its estimate.

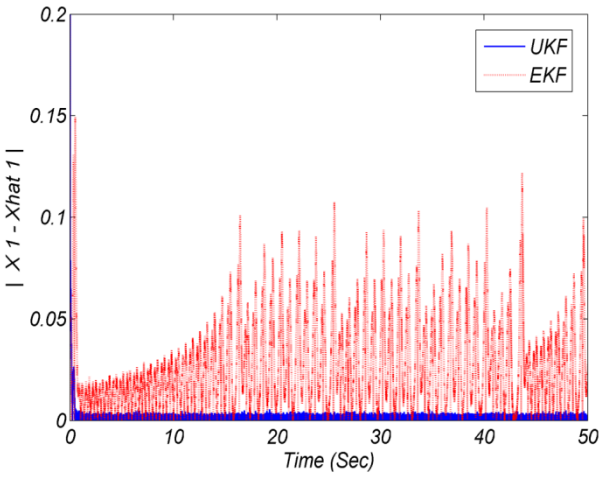


**Fig. 7.** Absolute error in estimation of the first state (Lorenz).

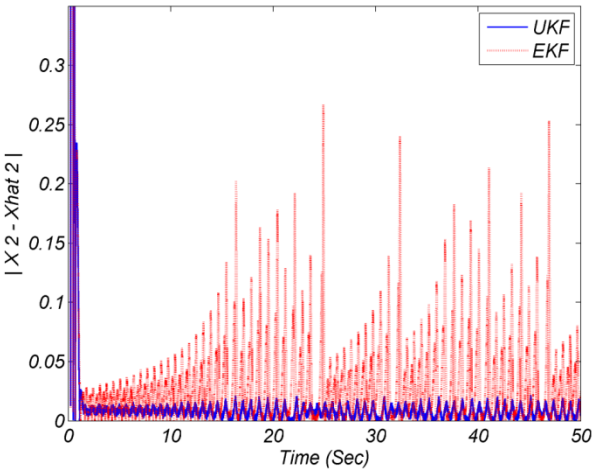


**Fig. 8.** Absolute error in estimation of the second state (Lorenz).

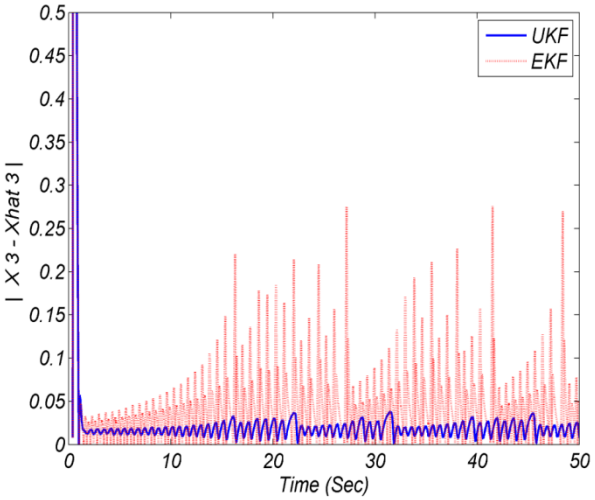


**Fig. 9.** Absolute error in estimation of the third state (Lorenz).

| | Synchronization Method | |
|---|---|---|
| | **EKF** | **UKF** |
| $x_1$ | 0.006 | 0.006 |
| $x_2$ | 0.979 | 0.650 |
| $x_3$ | 0.966 | 0.899 |
| **Maximum (sec)** | 0.979 | 0.899 |

**Tab. 1.** Convergence time (sec) in state estimation of Lorenz system.

| | Synchronization Method | |
|---|---|---|
| | **EKF** | **UKF** |
| $x_1$ | 0.0107 | 0.0097 |
| $x_2$ | 0.2905 | 0.2891 |
| $x_3$ | 0.7974 | 0.7528 |

**Tab. 2.** MSE (0 – 50 sec) for three state variables of Lorenz system.

In Fig. 10, the data that is encrypted by masking modulation can be seen in the case of using Lorenz system in time domain. In this case, the data is masked by the first state of Lorenz system for encryption. This makes the signal complicated and secure that we cannot understand the content of the message when looking at this signal. It is obvious that the analog data is completely hidden in the frequency content of the chaotic state and filtering techniques cannot recover the information which is modulated by masking modulation. Figure 11 presents the original sinusoid data and the recovered data that are simulated in the same coordinate. We can see that the recovered data is nearly the same as the original data. As indicated in Fig. 11 and Table 5 after 1.071 seconds, the data is recovered and converged nearly to the original data. By using our proposed secure chaotic communication scheme in the presence of channel noise and processing noise, the data can be precisely recovered. The noise performance of this system is related to the use of the UKF for state synchronization.

For evaluating the performance of the proposed system in a digital case, a pulse input is also used. Figure 12 shows the digital data encrypted with masking modulation. Figure 13 shows the original digital data and the recovered digital data in the same coordination. As indicated in Table 5, after 1.099 seconds the digital data is recovered and converged to the original digital data.

Simulations show that the proposed method also works well with other types of chaotic systems. Figure 14 shows the attractor of Rössler dynamical system. The convergence times of three states of Rössler system by use of the UKF and the EKF have been shown in Table 3. The maximum of the three values by the UKF is considered as the convergence time of the system which is 5.734 seconds. This value for the EKF is 6.874 seconds. We have calculated the mean squared error (MSE) for the three states by the use of the UKF and the EKF (Table 4). The results, show absolute estimation errors of the three states in the UKF, are clearly less than those in the EKF.

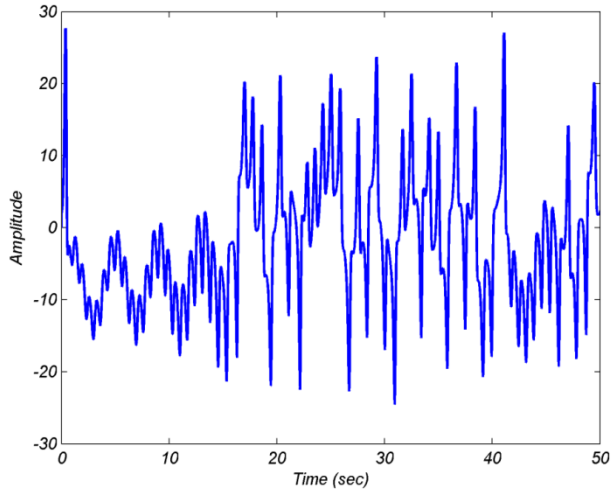


**Fig. 10.** Analog data encrypted with chaos masking modulation (Lorenz).

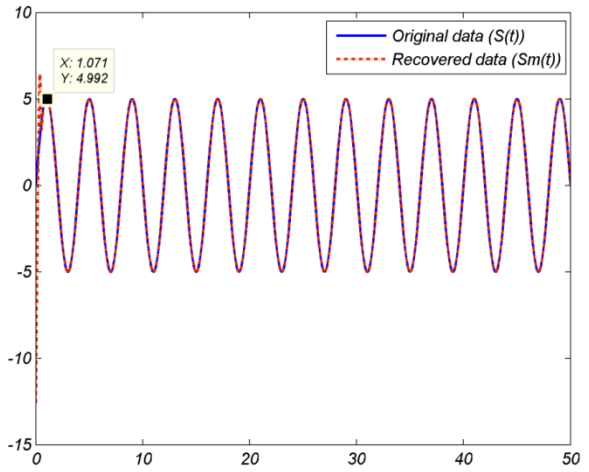


**Fig. 11.** Original sinusoid (analog) data and the recovered data (Lorenz).

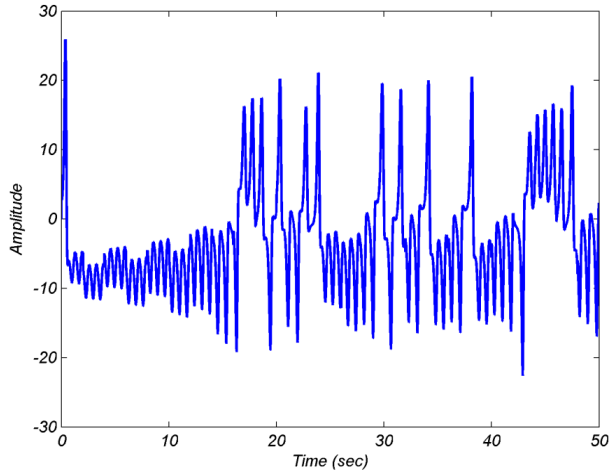


**Fig. 12.** Digital data encrypted with chaos masking modulation (Lorenz).

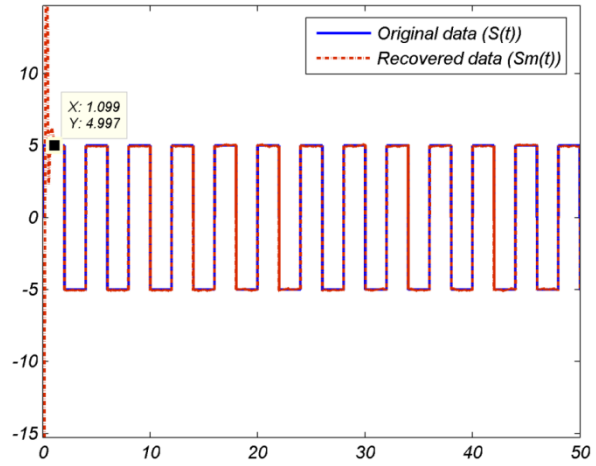


**Fig. 13.** Original digital data and the recovered data (Lorenz).

Figure 15 shows the data encrypted with masking modulation in the case of Rössler system. In this case, the modulated signal is unintelligible and the intruder cannot understand the message as that in the previous case. It is obvious that, in this case also the analog data is completely hidden in the frequency content of the chaos and filtering techniques cannot recover the information. In Fig. 16, the original analog data and the recovered data can be seen in a single plot. It is clear that the data is recovered with such precision. As indicated in Table 5, after 3.868 seconds the data is recovered and converged to the original data.

In the case of digital data, Fig.17 shows the digital data encrypted with masking modulation. The original digital data and the recovered digital data can be seen in Fig. 18 in the same coordinate. As indicated in Table 5, after 5.325 seconds, the digital data is recovered and converged to the original digital data.

In the proposed chaos masking modulation technique, the information signal is masked by the chaotic signal and the information is completely disguised in the chaotic signal and this scheme spreads the signal in frequency domain as well as encrypting the signal in time domain. Some papers have offered some methods in order to break schemes of secure chaotic communication that their application is straightforward if low-dimensional chaos with a simple return map is used in communication. However, the reveal of information is difficult in the more complicated the return map of the transmitted signal [21,26].

In cryptography, infinitely broad and flat spectrum is a fundamental requirement of the pseudo-random noise and the power density much higher than the signal to be concealed. In other words, the plaintext power spectrum should be effectively buried into the pseudo-random noise power spectrum.

On the contrary, the spectrum of the signal generated by the Lorenz or Rössler oscillator is of narrow band, decaying very fast with increasing frequency, showing a power density much lower than the plaintext at plaintext frequencies. The existing methods and high-pass filtering are not able to break the proposed chaos masking method.

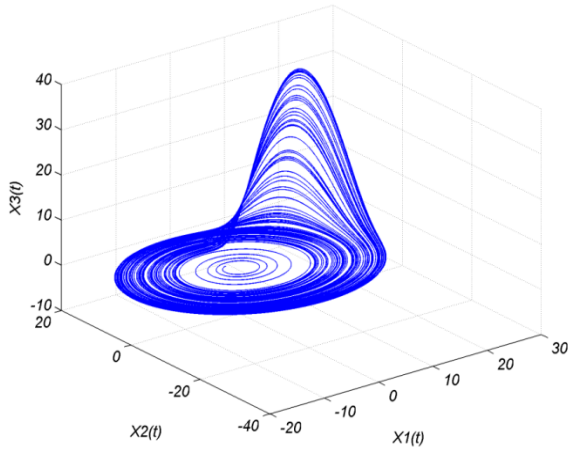


**Fig. 14.** Attractor of Rossler dynamical system.

Chaotic systems are highly dependent on initial condition and also parameters. As it is shown, the dynamical systems which can be used in the proposed scheme are three-dimensional chaotic systems that there are three initial conditions and three parameters. With these three initial conditions and also three parameters, a large key-space can be produced that makes the proposed scheme highly secure.

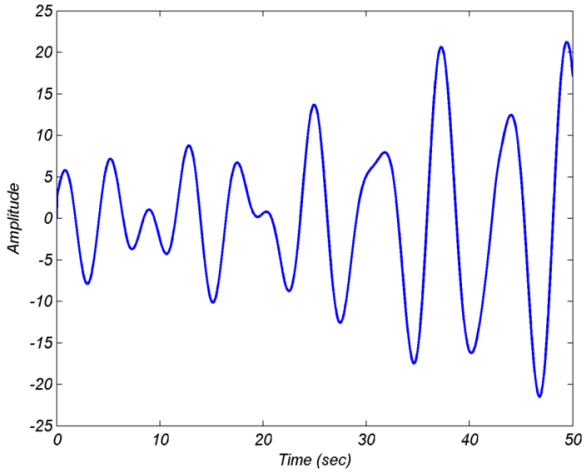


**Fig. 15.** Analog data encrypted with chaos masking modulation (Rossler).

| | Synchronization Method | |
|---|---|---|
| | **EKF** | **UKF** |
| $x_1$ | 0.009 | 0.009 |
| $x_2$ | 6.874 | 5.734 |
| $x_3$ | 5.730 | 2.034 |
| **Maximum (sec)** | 6.874 | 5.734 |

**Tab. 3.** Convergence time (sec) in state estimation of Rössler system.

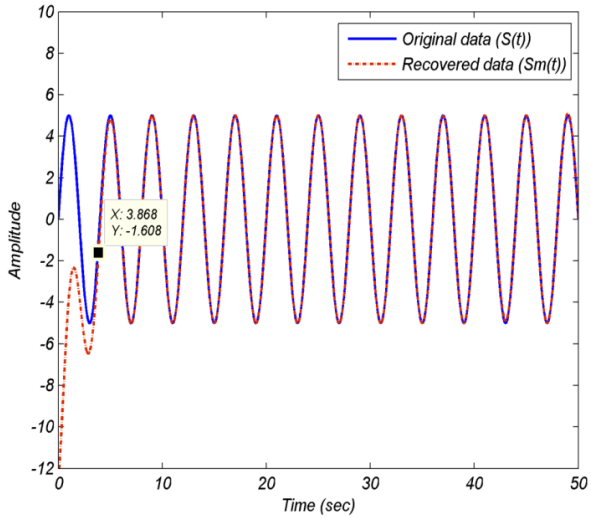


**Fig. 16.** Original sinusoid (analog) data and the recovered data (Rossler).

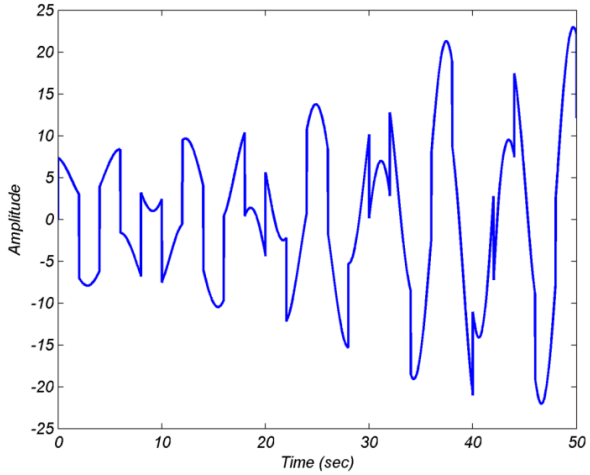


**Fig. 17.** Digital data encrypted with chaos masking modulation (Rossler).

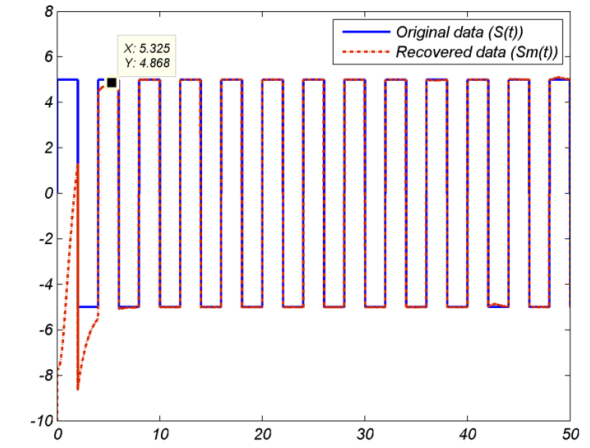


**Fig. 18.** Original digital data and the recovered data (Rossler).

| | Synchronization Method | |
|---|---|---|
| | EKF | UKF |
| $x_1$ | 0.0097 | 0.0094 |
| $x_2$ | 4.2596<br>3.5309 | |
| $x_3$ | 2.0289<br>0.1554 | |

**Tab. 4:** MSE (0 – 50 sec) for three state variables of Rössler system

| Type of chaotic system | Analog data | Digital data |
|---|---|---|
| **Lorenz system** | 1.071 | 1.099 |
| **Rossler System** | 3.868 | 5.325 |

**Tab.. 5.** Convergence time (sec) in data recovery.

## 5. Conclusion

In this paper, we proposed the UKF based synchronization design scheme and its application to secure communications of chaotic systems. The synchronization of the state variables has been done with high accuracy and high speed. The UKF method has been compared with the EKF method to show the improvement of synchronization act and its growth in the performance in regard to accuracy in decreasing state variable estimation error. The calculation of absolute estimation error value for each state variable showed that its value in the UKF method is less than the EKF method. For more comparison, the mean square error (MSE) of two methods has been calculated and compared. Simulation results indicated that the UKF method is more accurate than EKF because of the lower MSE in the UKF method.

Then, for the first time, we implemented the UKF in a simple chaotic masking method to illustrate the increasing of security in communication. The chaos masking modulation is used to encrypt data and the receiver is based on the UKF that does not require knowing the initial condition of the transmitter. The proposed method is possible to apply to different kinds of chaotic systems and it can be used for both analog and digital data. The noise performance of the proposed scheme is related to the use of the UKF. Due to employing different chaos states for the synchronization and the encryption, the proposed chaotic communication scheme is totally different from the traditional cryptosystems.

It is also shown that it is difficult to break the proposed secure communication scheme with the existing methods such as high-pass filtering. From the simulation results, the performance of the proposed systems seems to be satisfactory for secure communication applications and therefore be used effectively for ensuring security and privacy in commercial consumer electronics products.

## References


1. L.M. Pecora and T.L. Carroll, Synchronization in chaotic systems, Phys. Rev. Lett., vol. 64(8), pp. 821-824 (1990).
2. M. Hasler, Synchronization of chaotic systems and transmission of information, Int. J. Bifurc. Chaos, vol. 8(4), pp. 647-659 (1998).
3. G. Grassi and S. Mascolo, Nonlinear observer design to synchronize hyperchaotic systems via a scalar signal, IEEE Trans. Circuits Syst. I-Fundamental Theory Appl., vol. 44(10), pp. 1011-1013 (1997).
4. C.-C. Hwang, H. Jin-Yuan, and L. Rong-Syh, A linear continuous feedback control of Chua's circuit, Chaos, Solitons & Fractals, vol. 8(9), pp. 1507-1515 (1997).
5. J. Lü and J. Lu, Controlling uncertain Lü system using linear feedback, Chaos, Solitons & Fractals, vol. 17(1), pp. 127-133 (2003).
6. M. Chen and Z. Han, Controlling and synchronizing chaotic Genesio system via nonlinear feedback control, Chaos, Solitons & Fractals, vol. 17(4), pp. 709-716 (2003).
7. L. Kocarev and U. Parlitz, General approach for chaotic synchronization with applications to communication, Phys. Rev. Lett., vol. 74(25), p. 5028 (1995).
8. T.-L. Liao and S.-H. Tsai, Adaptive synchronization of chaotic systems and its application to secure communications, Chaos, Solitons & Fractals, vol. 11(9), pp. 1387-1396 (2000).
9. H. Nijmeijer and I. M. Y. Mareels, An observer looks at synchronization, IEEE Trans. Circuits Syst. I Fundam. theory Appl., vol. 44(10), pp. 882-890 (1997).
10. M. Feki and B. Robert, Observer-based chaotic synchronization in the presence of unknown inputs, Chaos, Solitons & Fractals, vol. 15(5), pp. 831-840 (2003).
11. S. Bowong, F.M. Moukam Kakmeni, and H. Fotsin, A new adaptive observer-based synchronization scheme for private communication, Phys. Lett. A, vol. 355(3), pp. 193-201 (2006).
12. A. Azemi and E.E. Yaz, Sliding-mode adaptive observer approach to chaotic synchronization, J. Dyn. Syst. Meas. Control, vol. 122(4), pp. 758-765 (2000).
13. M.S. Grewal and A.P. Andrews, Kalman filtering: theory and practice using MATLAB, John Wiley & Sons (2011).
14. R.E. Kalman, A new approach to linear filtering and prediction problems, J. basic Eng., vol. 82(1), pp. 35-45 (1960).
15. C. Cruz and H. Nijmeijer, Synchronization through filtering, Int. J. Bifurc. Chaos, vol. 10(4), pp. 763-775 (2000).
16. S.J. Julier and J.K. Uhlmann, Unscented filtering and nonlinear estimation, Proc. IEEE, vol. 92(3), pp. 401-422 (2004).
17. C.C. Qu and J. Hahn, Process monitoring and parameter estimation via unscented Kalman filtering, J. Loss Prev. Process Ind., vol. 22(6), pp. 703-709 (2009).
18. F. Zhu, Observer-based synchronization of uncertain chaotic system and its application to secure communications, Chaos, Solitons & Fractals, vol. 40(5), pp. 2384-2391 (2009).
19. K. Fallahi, R. Raoufi, and H. Khoshbin, An application of Chen system for secure chaotic communication based on extended Kalman filter and multi-shift cipher algorithm, Commun. Nonlinear Sci. Numer. Simul., vol. 13(4), pp. 763-781 (2008).
20. A. Kiani-B, K. Fallahi, N. Pariz, and H. Leung, A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional Kalman filter, Commun. Nonlinear Sci. Numer. Simul., vol. 14(3), pp. 863-879 (2009).
21. K. Fallahi and H. Leung, A chaos secure communication scheme based on multiplication modulation, Commun. Nonlinear Sci. Numer. Simul., vol. 15(2), pp. 368-383 (2010).
22. J.C. Feng and C.K. Tse, Reconstruction of chaotic signals with applications to chaos-based communications, World Scientific (2008).
23. J.J. Laviola, A comparison of unscented and extended Kalman filtering for estimating quaternion motion, In Proc. of American Control Conference, vol. 3, pp. 2435-2440 (2003).
24. F. Orderud, Comparison of kalman filter estimation approaches for state space models with nonlinear measurements, In Proc. of Scandinavian Conference on Simulation and Modeling, pp. 1-8 (2005).
25. E.A. Wan and R. Van Der Merwe, The unscented Kalman filter for nonlinear estimation, In Proc. of Adaptive Systems for Signal

Processing, Communications, and Control Symposium, AS-SPCC. pp. 153-158 (2000).

26. G. Alvarez, F. Montoya, G. Pastor, and M. Romera, Chaotic cryptosystems, In Proc. of IEEE 33rd Annual International Conference on Carnahan, pp. 332-338 (1999).