23

# Robust Designs of Chaos-Based Secure Communication Systems

Ashraf A. Zaher
*Kuwait University – Science College – Physics Department*
*P. O. Box 5969 – Safat 13060 - Kuwait*

## 1. Introduction

Chaos and its applications in the field of secure communication have attracted a lot of attention in various domains of science and engineering during the last two decades. This was partially motivated by the extensive work done in the synchronization of chaotic systems that was initiated by (Pecora & Carroll, 1990) and by the fact that power spectrums of chaotic systems resemble white noise; thus making them an ideal choice for carrying and hiding signals over the communication channel. Drive-response synchronization techniques found typical applications in designing secure communication systems, as they are typically similar to their transmitter-receiver structure. Starting in the early nineties and since the early work of many researchers, e.g. (Cuomo et al., 1993; Dedieu et al., 1993; Wu & Chua, 1993) chaos-based secure communication systems rapidly evolved in many different forms and can now be categorized into four different generations (Yang, 2004).

The major problem in designing chaos-based secure communication systems can be stated as how to send a secret message from the transmitter (drive system) to the receiver (response system) over a public channel while achieving security, maintaining privacy, and providing good noise rejection. These goals should be achieved, in practice, using either analog or digital hardware (Kocarev et al., 1992; Pehlivan & Uyaroğlu, 2007) in a robust form that can guarantee, to some degree, perfect reconstruction of the transmitted signal at the receiver end, while overcoming the problems of the possibility of parameters mismatch between the transmitter and the receiver, limited channel bandwidth, and intruders attacks to the public channel. Several attempts were made, by many researchers to robustify the design of chaos-based secure communication systems and many techniques were developed. In the following, a brief chronological history of the work done is presented; however, for a recent survey the reader is referred to (Yang, 2004) and the references herein.

One of the early methods, called additive masking, used in constructing chaos-based secure communication systems, was based on simply adding the secret message to one of the chaotic states of the transmitter provided that the strength of the former is much weaker than that of the later (Cuomo & Oppenheim, 1993). Although the secret message was perfectly hidden, this technique was impractical because of its sensitivity to channel noise and parameters mismatch between both the transmitter and the receiver. In addition, this method proved to have poor security (Short, 1994). Another method that was aimed at digital signals, called chaos shift keying, was developed in which the transmitter is made to alternate

between two different chaotic attractors, implemented via changing the parameters of the chaotic system, based on whether the secret message corresponds to either its high or low value (Parlitz et al., 1992). This method proved to be easy to implement and, at the receiver side, the message can be efficiently reconstructed using a two-stage process consisting of low-pass filtering followed by thresholding. Once again, this method shares, with the additive masking method, the disadvantage of having poor security, especially if the two attractors at the transmitter side are widely separated (Yang, 1995). However, it proved to be more robust in terms of handling noise and parameters mismatch between the transmitter and the receiver, as it was only required to extract binary information.

Extending conventional modulation theory, in communication systems, to chaotic signals was then attempted such that the message signal is used to modulate one of the parameters of the chaotic transmitter (Yang & Chua, 1996). This method was called chaotic modulation and it employed some form of adaptive control at the receiver end to recover the original message via forcing the synchronization error to zero (Zhou & Lai, 1999). The recovered signal, using this technique, was shown to suffer from negligible time delays and minor noise distortion (d'Anjou et al., 2001). Another variant to this method that relied on changing the trajectory of the chaotic transmitter attractor, in the phase space, was also explored in (Wu & Chua, 1993). This method was distinguished by the fact that only one chaotic attractor in the transmitter side was used, in contrast to many attractors in the case of parameter modulation. Although these two techniques (second generation) had a relatively higher security, compared to the previously discussed methods, they still lack robustness against intruder attacks using frequency-based filtering techniques, as exemplified by (Zaher, 2009), especially in the case when the dominant frequency of the secret message is far away from that of the chaotic system.

Motivated by the generation of cipher keys for the use of pseudo-chaotic systems in cryptography (Dachselt & Schwarz, 2001; Stinson, 2005) and the poor security level of the second generation of chaos-based communication systems, a third generation emerged called chaotic cryptosystems. In these systems, various nonlinear encryption methods are used to scramble the secure message at the transmitter side, while using an inverse operation at the receiver side that can effectively recover the original message, provided that synchronization is achieved (Yang et al., 1997). Encryption functions depend on a combination of the chaotic transmitter state(s), excluding the synchronization signal, and one or more of the parameters so that the secret message is effectively hidden. The degree of complexity of the encryption function and the insertion of ciphers (secret keys) led to having more robust techniques with applications to both analog and digital communication (Sobhy & Shehata, 2000; Jiang, 2002; Solak, 2004).

Recently, new techniques, based on impulsive synchronization, were introduced (Yang & Chua, 1997). These systems have better utilization of channel bandwidth as they reduce the information redundancy in the transmitted signal via sending only synchronization impulses to the driven system. Other methods for enhancing security in chaos-based secure communication systems that are currently reported in the literature include employing pseudorandom numbers generators for encoding messages (Zang et al., 2005) and using high-dimension hyperchaotic systems that have multiple positive Lyapunov exponents (Yaowen et al., 2000).

The main purpose of this chapter is to provide a versatile combination of the parameter modulation technique, which belongs to the second generation of chaos-based secure com-

munication systems, and cryptography, which belongs to the third generation, such that the resulting system has the advantages of both of them and, in addition, exhibits more robustness in terms of improved security. The two main topics of chaos synchronization and parameter identification are covered in the next sections to provide the foundation of constructing chaos-based secure communication systems. This is being achieved via using the Lorenz system to build the transmitter/receiver mechanism. The reason for this choice is to provide simple means of comparison with the current research work reported in the literature; however, other chaotic or hyperchaotic systems could have been used as well. The examples illustrated in this chapter cover both analog and digital signals to provide a wider scope of applications. Moreover, most of the simulations were carried out using Simulink while stating all involved signals including initial conditions to provide a consistent reference when verifying the reported results and/or trying to extend the work done to other scenarios or applications. The mathematical analysis is done in a step-by-step method to facilitate understanding the effects of the individual parameters/variables and the results were illustrated in both the time domain and the frequency domain, whenever applicable. Some practical implementations using either analog or digital hardware are also explored.
The rest of this chapter is organized as follows. Section 2 gives a brief description of the famous Lorenz system and its chaotic behaviour that makes it a perfect candidate for implementing chaos-based secure communication systems. Section 3 discusses the topic of synchronizing chaotic systems with emphasis to complete synchronization of identical chaotic systems as an introductory step when constructing the communication systems discussed in this chapter. Section 4 addresses the problem of parameter identification of chaotic systems and focuses on partial identification as a tool for implementing both the encryption and decryption functions at the transmitter and the receiver respectively. Section 5 combines the results of the previous two sections and proposes a robust technique that is demonstrated to have superior security than most of the work currently reported in the literature. Section 6 concludes this chapter and discusses the advantages and limitations of the systems discussed along with proposing future extensions and suggestions that are thought to further improve the performance of chaos-based secure communication systems.

## 2. The Lorenz System

The Lorenz system is considered a benchmark model when referring to chaos and its synchronization-based applications. Although the Lorenz "strange attractor" was originally noticed in weather patterns (Lorenz, 1963), other practical applications exhibit such strange behaviour, e.g. single-mode lasers (Weiss & Vilaseca, 1991), thermal convection (Schuster & Wolfram, 2005), and permanent magnet synchronous machines (Zaher, 2007). Many researchers used the Lorenz model to exemplify different techniques in the field of chaos synchronization and both complete and partial identification of the unknown or uncertain parameters of chaotic systems. In addition, The Lorenz system is often used to exemplify the performance of newly proposed secure communication systems as illustrated in the references herein. The mathematical model of the Lorenz system takes the form

$$\begin{aligned}\dot{x}_1 &= -\sigma x_1 + \sigma x_2 \\ \dot{x}_2 &= \rho x_1 - x_2 - x_1 x_3 \\ \dot{x}_3 &= -\beta x_3 + x_1 x_2\end{aligned} \tag{1}$$

where $X = [x_1\ x_2\ x_3]^T$ is the state vector and $\sigma$, $\rho$, and $\beta$ are constant parameters. Notice that each differential equation contains only one parameter. The nominal values of the parameters are 10.0, 28.0, and 8/3 respectively. Using linear analysis techniques, it can be demonstrated that the free-running case corresponds to the following unstable equilibrium points

$$(0\,,0\,,0) \text{ and } \left[\pm\sqrt{\beta(\rho-1)} \quad \pm\sqrt{\beta(\rho-1)} \quad (\rho-1)\right]^T \tag{2}$$

Starting from any initial conditions the Lorenz system will exhibit a chaotic behavior that is characterized by the typical response illustrated in Fig. (1), for which the initial conditions were assumed (1 , 0 , 0).

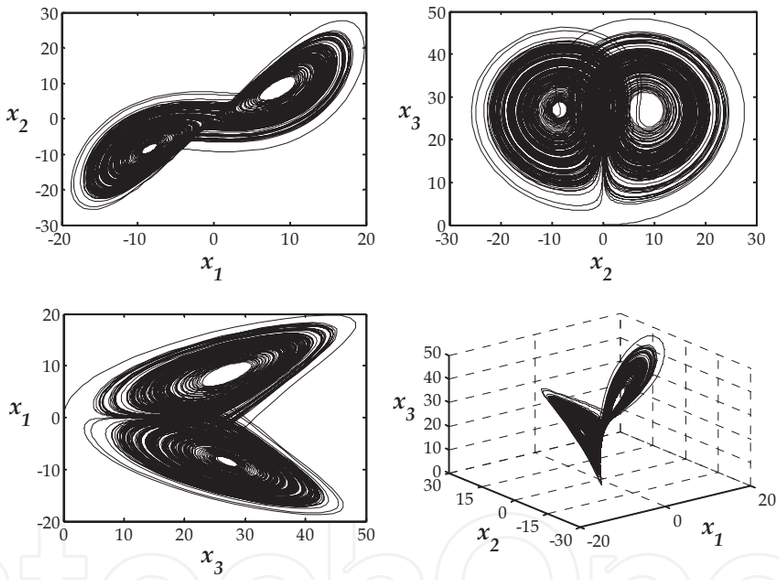



Fig. 1. Illustration of the chaotic performance of the Lorenz system for the nominal values of the parameters.

Throughout this chapter, it will be assumed that both $\rho$ and $\beta$ are kept constants and that only $\sigma$ is allowed to change in the interval $8 \le \sigma \le 12$. For this specified interval of $\sigma$, it can be proven that the system will still exhibit a chaotic performance; however, the chaotic attractor will change.

## 3. Synchronization of Chaotic Systems

Synchronization of chaos refers to a process wherein two (or many) chaotic systems (either equivalent or nonequivalent) adjust a given property of their motion to a common behav-

iour due to a coupling or to a forcing (periodical or noisy) (Boccaletti, 2002). Because of sensitivity to initial conditions, two trajectories emerging from two different closely initial conditions separate exponentially in the course of the time. As a result, chaotic systems defy synchronization. There exist several types of synchronization including complete synchronization, lag synchronization, generalized synchronization, frequency synchronization, phase synchronization, Q-S synchronization, time scale synchronization, and impulsive synchronization. The reader is referred to (Zaher, 2008a) for a list of references that cover these different techniques

Synchronization for two identical, possibly chaotic, dynamical systems can be achieved such that the solution of one always converges to the solution of the other independently of the initial conditions (Balmforth, 1997). This type of synchronization is called drive-response (master-slave) coupling, where there is an interaction between one system and the other, but not vice versa, and synchronization can be achieved provided that all real parts of the Lyapunov exponents of the response system, under the influence of the driver, are negative (Pecora & Carroll, 1991). In the drive-response synchronization scheme it is usually assumed that the complete state vector of the drive system is not available and that only a single scalar output is used in unidirectional coupling between the drive and the response systems. This configuration found useful applications in both secure communication applications (Liao & Huang, 1999) and the construction of parameter identification algorithms (Carroll, 2004; Chen & Kurths, 2007).

This drive-response synchronization scheme is essentially a control problem as the drive signal is used as a feedback signal for the response system such that the synchronization error is continuously attenuated. Due to the nonlinear nature of the dynamics involved in chaos synchronization, Lyapunov functions proved to be successful for the purpose of achieving global stability for this type of synchronization via forcing the error dynamics to approach a zero steady state. In this section, a recursive algorithm, inspired from backstepping control, is proposed such that both fast and stable operation of the synchronization process is obtained. Backstepping is basically a recursive design procedure that can extend the applicability of Lyapunov-based designs to nonlinear systems via introducing virtual reference models to prescribe target behaviour for some or all of the original system states and then use some of them as virtual controls to the output (Krstic, 1995). This idea seems to be very appealing, especially when combined with Lyapunov-energy-like functions to design the control law. Using the Lorenz system, described by Eq. (1), and assuming identical dynamics for both the transmitter (drive system) and the receiver (response system), the following virtual (intermediate) functions are introduced

$$f_i = x_i - k_{i1}x_1 \text{ , } i = 2,3 \tag{3}$$

where $k_{21}$ and $k_{32}$ are control parameters to be found later, $x_1$ is the drive signal, and both $f_2$ and $f_3$ are used implicitly to observe $x_2$ and $x_3$ of the transmitter.

Subsituting Eq. (1) in the derivative of Eq. (3) yields

$$\begin{aligned} \dot{f}_2 &= [\rho x_1 - (f_2 + k_{21}x_1) - x_1(f_3 + k_{31}x_1)] - k_{21}[-\sigma x_1 + \sigma(f_2 + k_{21}x_1)] \\ &= -f_2 - x_1 f_3 - \sigma k_{21} f_2 + \varphi_2(x_1) \end{aligned} \tag{4}$$

where

$$\varphi_2(x_1) = x_1\left[\rho - k_{21} + \sigma k_{21}(1-k_{21})\right] - k_{31}x_1^2 \tag{5}$$

and

$$\begin{aligned}\dot{f}_3 &= [-\beta(f_3 + k_{31}x_1 + x_1(f_2 + k_{21}x_1)] - k_{31}[-\sigma x_1 + \sigma(f_2 + k_{21}x_1)] \\ &= x_1 f_2 - \beta f_3 - \sigma k_{31} f_2 + \varphi_3(x_1)\end{aligned} \tag{6}$$

where

$$\varphi_3(x_1) = x_1\left[-\beta k_{31} + \sigma k_{31}(1-k_{21})\right] + k_{21}x_1^2 \tag{7}$$

Now, introducing the following synchronization errors

$$e_i = x_i - \hat{x}_i = f_i - \hat{f}_i \text{ , } i = 2,3 \tag{8}$$

results in

$$\begin{aligned}\dot{e}_2 &= -(1+\sigma k_{21})e_2 - x_1 e_3 \\ \dot{e}_3 &= x_1 e_2 - \beta e_3 - \sigma k_{31} e_2\end{aligned} \tag{9}$$

The following simple Lyapunov function is now proposed

$$L = 0.5(e_2^2 + e_3^2) \tag{10}$$

leading to

$$\begin{aligned}\dot{L} &= e_2\dot{e}_2 + e_3\dot{e}_3 \\ &= -[(1+\sigma k_{21})e_2^2 + \sigma k_{31}e_2e_3 + \beta e_3^2]\end{aligned} \tag{11}$$

which can be made negative definite via the following choice of the control parameters

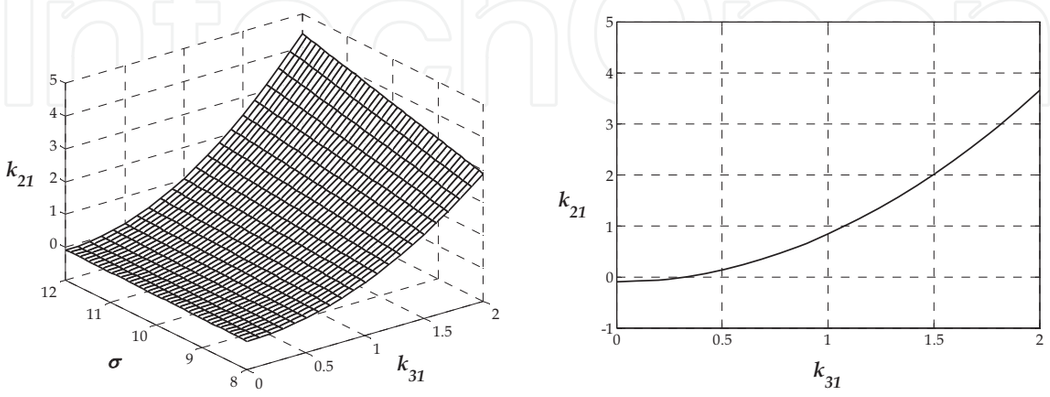
$$k_{21} \geq \frac{\sigma k_{31}^2}{4\beta} - \frac{1}{\sigma} \tag{12}$$

From which global stability is assured as illustrated by Eq. (13)

$$\dot{L} = -(1 + \sigma k_{21} - \frac{\sigma^2 k_{31}^2}{4\beta})e_2^2 - (\frac{\sigma k_{31}}{2\sqrt{\beta}}e_2 + \sqrt{\beta}e_3)^2 \leq 0 \tag{13}$$

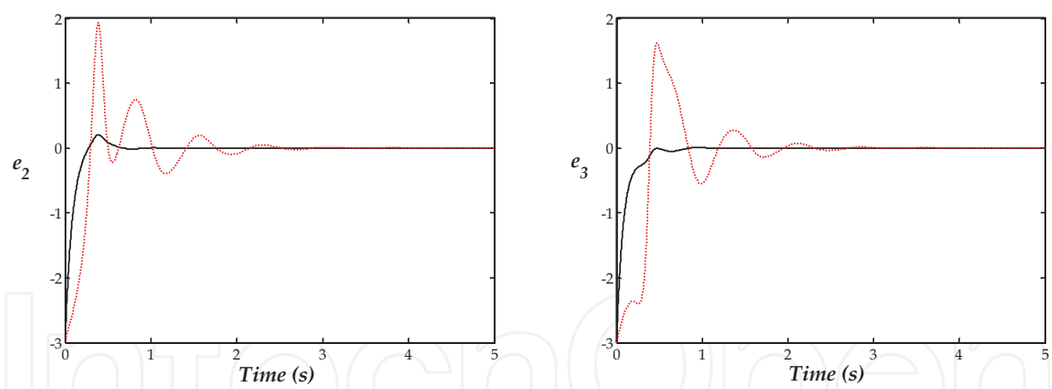
Figure (2) represents a graphical interpretation of the result obtained in Eq. (12), where it is shown that a wide range of values exist to implement the suggested technique. This offers

flexibility, when implementing this synchronization method, in meeting any physical constraints imposed by the chosen analog or digital hardware. In addition, it should be emphasized that when both $k_{21}$ and $k_{31}$ are put equal to zero, the conventional method of synchronization, developed in (Pecora & Carroll, 1990), is obtained. This fact is taken an advantage of when comparing the speed of response of the suggested technique to other methods reported in the literature, as illustrated in Fig. (3).




(a) (b)

Fig. 2. Stable range of the control parameters, showing $k_{21}$ as a function of both $\sigma$ and $k_{31}$ corresponding to the ranges $8 \leq \sigma \leq 12$ and $0 \leq k_{31} \leq 2$ as illustrated in (a). The relationship between $k_{21}$ and $k_{31}$ for the nominal value of $\sigma = 10$ is shown in (b).




(a) (b)

Fig. 3. Comparison between the fast recursive synchronization method for the special case $k_{21} = k_{31} = 1$ (solid line) and the conventional synchronization when $k_{21} = k_{31} = 0$ (dotted line) for both $e_2$ and $e_3$ in (a) and (b) respectively.

### 3.1 A detailed example

The designed receiver acts as a state observer that uses one scalar time series ($x_1$) to estimate the remaining states of the transmitter ($x_2$ and $x_3$). Because of the nonlinear structure of the overall system comprising both the transmitter and the receiver, it will be difficult to draw general conclusions about the best values of the control parameters that result in the fastest response while avoiding too much control effort that might lead to saturation and conse-

quently adding more nonlinearities into the system. To investigate the practicality of the design, a simple version of the design is now implemented in analog hardware using $k_{21} = 1$ and $k_{31} = 0$. The resulting system is governed by Eq. (14) and is illustrated by the Simulink block diagram, shown in Fig. (4).

$$\begin{aligned}
\dot{x}_1 &= -\sigma x_1 + \sigma x_2 \\
\dot{x}_2 &= \rho x_1 - x_2 - x_1 x_3 \\
\dot{x}_3 &= -\beta x_3 + x_1 x_2 \\
\dot{\hat{f}}_2 &= -(\sigma+1)\hat{f}_2 - x_1 \hat{f}_3 + (\rho-1)x_1 \\
\dot{\hat{f}}_3 &= x_1 \hat{f}_2 - \beta \hat{f}_3 + x_1^2 \\
\hat{x}_2 &= \hat{f}_2 + x_1 \\
\hat{x}_3 &= \hat{f}_3
\end{aligned} \tag{14}$$

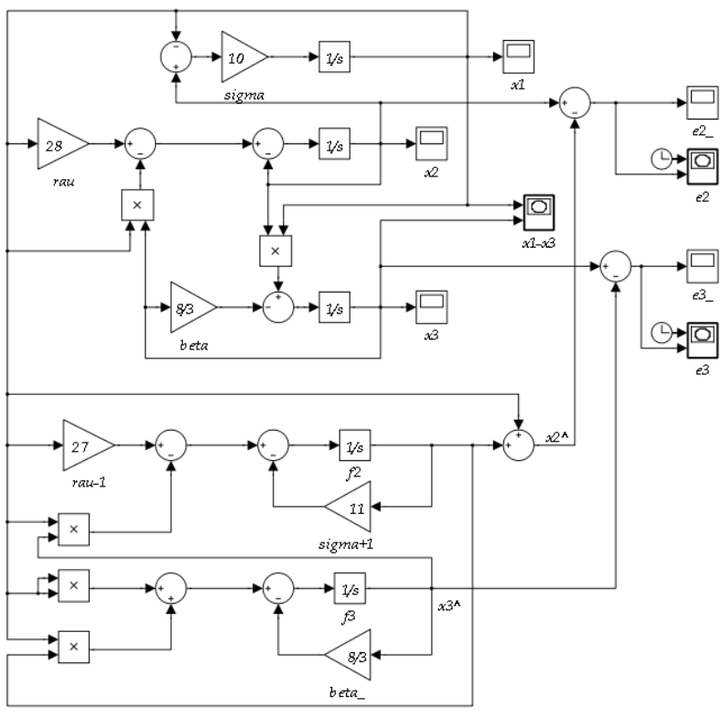



Fig. 4. A Simulink model for the simulation and implementation of Eq. (14) for the special case when $k_{21} = 1$ and $k_{31} = 0$.

### 3.2 Practical considerations in the implementation phase

To meet practical considerations when implementing the drive-response system using analog hardware, it will be required to adjust the peak values of the signals to fall within the saturation levels imposed by the power supply and, in addition, to change the frequency

band of the system to conform to that of the signals involved, e.g. the transmitted secret message in the case of secure communication systems. This can be achieved by using the linear transformation in Eq. (15) that results in the modified system depicted by Eq. (16) for which saturation nonlinearity is avoided.

$$\begin{aligned} & t \leftarrow t/\tau \\ & u = 0.2x_1 \text{ , } v = 0.2x_2 \text{ , } w = 0.1x_3 \text{ , } \\ & \hat{g}_2 = 0.2\hat{f}_2 \text{ , and } \hat{g}_3 = 0.1\hat{f}_3 \end{aligned} \tag{15}$$

$$\begin{aligned} \tau\dot{u} &= -\sigma u + \sigma v \\ \tau\dot{v} &= \rho u - v - 10uw \\ \tau\dot{w} &= -\beta w + 2.5uv \\ \tau\dot{\hat{g}}_2 &= -(\sigma+1)\hat{g}_2 - 10u\hat{g}_3 + (\rho-1)u \\ \tau\dot{\hat{g}}_3 &= -\beta\hat{g}_3 + 2.5u\hat{g}_2 + 2.5u^2 \\ \hat{v} &= \hat{g}_2 + u \\ \hat{w} &= \hat{g}_3 \end{aligned} \tag{16}$$

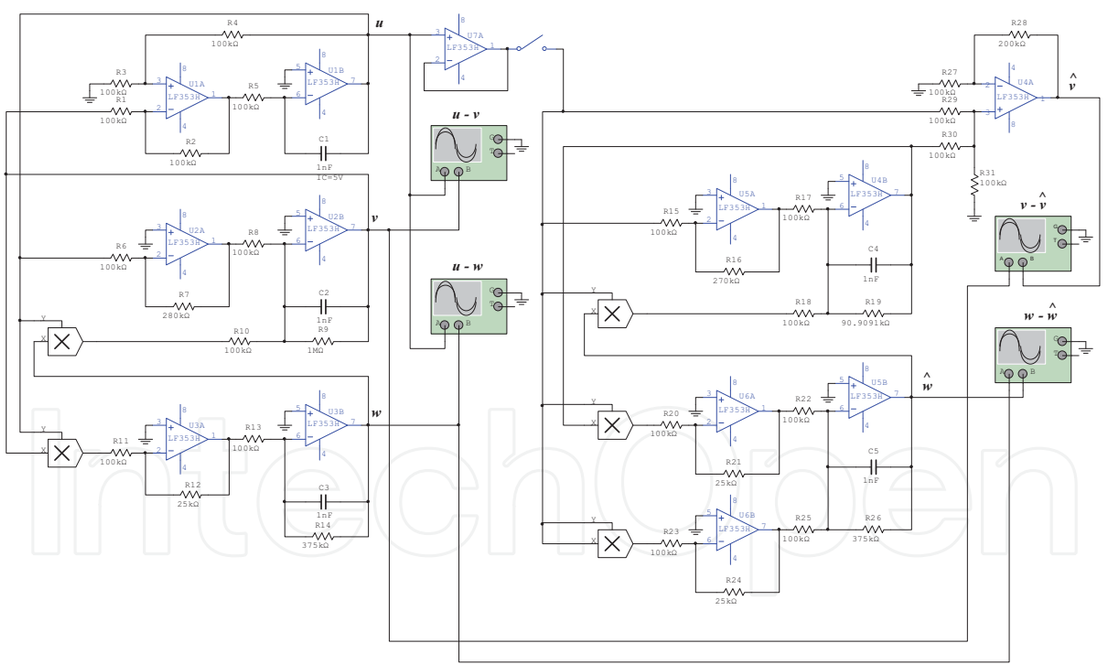
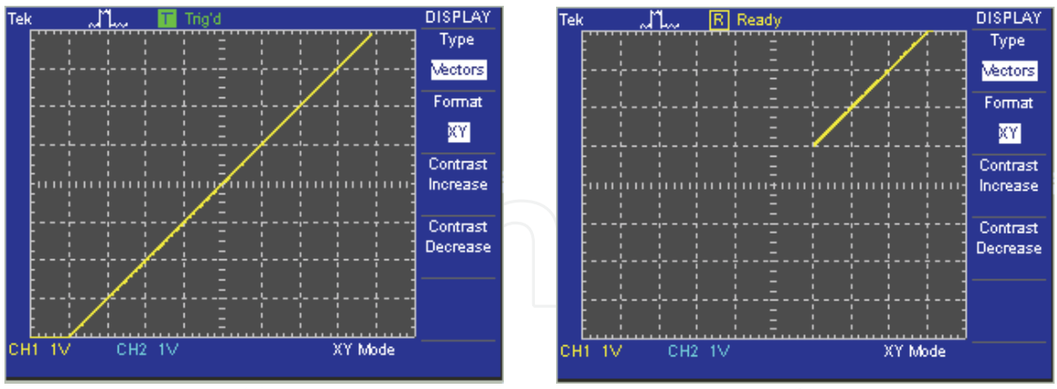



Fig. 5. An analog implementation using the proposed fast recursive drive-response mechanism of the Lorenz system for the special case when using $k_{21}$ = 1 and $k_{31}$ = 0.

The experimental results for the synchronization process are illustrated in Fig. (6), where it evident that the response system is capable of generating faithful estimates of the states of the transmitter with the help of one driving signal.




(a) (b)

Fig. 6. The steady state results of the synchronization, illustrating perfect matching between the states of both the drive and response systems for $x_2$ and $x_3$ in (a) and (b) respectively.

### 3.3 Case study I

Constructing a secure communication system is now investigated where the fast recursive synchronization mechanism is now combined with a nonlinear encryption function, $E$, at the transmitter in order to hide the secret message $s(t)$. At The receiver side, a decryption function, $D$, reverses the scrambling process to reconstruct the original message. Figure (7) illustrates this idea where the frequency band of both the transmitter and the receiver are adjusted using the time scaling factor, $\tau$, and the public channel is used to transmit both $x_1$ (the driving signal necessary for synchronization), and $E$, the encrypted secret message, which is similar to the work done in (Jiang, 2002; Solak, 2004; Zaher, 2009). Figure (8) illustrate the power spectrum analysis for both the secret message and the chaotic transmitter.

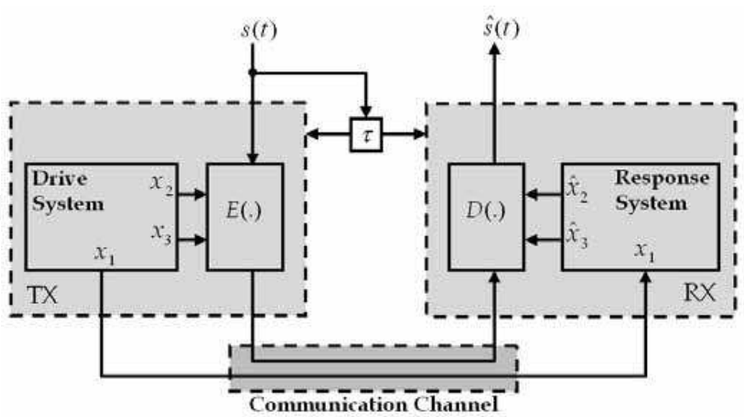



Fig. 7. A block diagram representation of the chaos-based secure communication system.

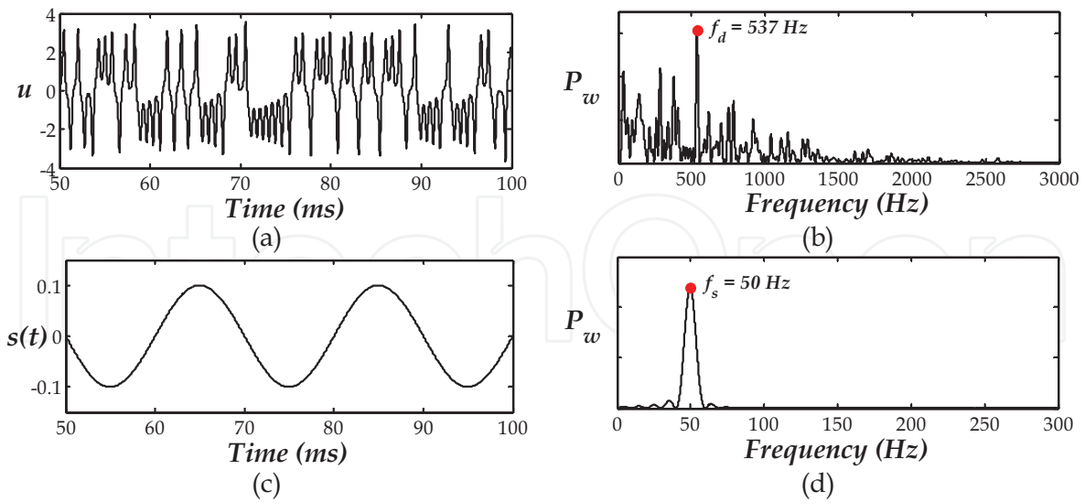



Fig. 8. The driving signal, $u = 0.2x_1$ and its power spectrum for the case when $\tau = 1$ ms are shown in (a) and (b) respectively. The sample transmitted secret message and its power spectrum are illustrated in (c) and (d) respectively.

Both the encryption and decryption functions are given in Eq. (17), where only $x_2$ was used to construct the nonlinear scrambling. The decryption function should settle very fast to the inverse of the encryption function, once synchronization is achieved.

$$\begin{aligned} E(X,s,t) &= x_2^2 + (1+x_2^2)s(t) \\ \hat{s}(t) &= D(\hat{X},s,t) = (E(X,s,t) - \hat{x}_2^2)/(1+\hat{x}_2^2) \end{aligned} \tag{17}$$

For improved security, the amplitude of the secret message should be much smaller than that of $x_2$. For simplicity and without loss of generality, a sinusoidal signal is chosen for illustration purposes with the form $s(t) = A_s \sin(2\pi f_s t)$, $f_s << f_d$, for which the frequency, $f_s$, is chosen to be much less than the dominant frequency of the chaotic attractor of the transmitter, $f_d$, to ensure minimum effects of transients. Figure (9) illustrate the improvements in the decryption error, $e(t) = D(t) - s(t)$, when using the conventional and the fast recursive methods for synchronization, where the absolute value of $e(t)$ over five periods of the transmitted signal was found to reduce from 4.2% to 1.7% respectively.

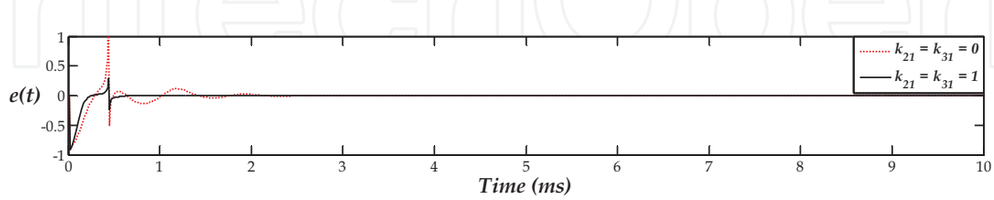



Fig. 9. A comparative study of the transient effects on the decryption error.

Figure (10) illustrate the complete response of the communication system, demonstrating the satisfactory performance of the proposed technique.

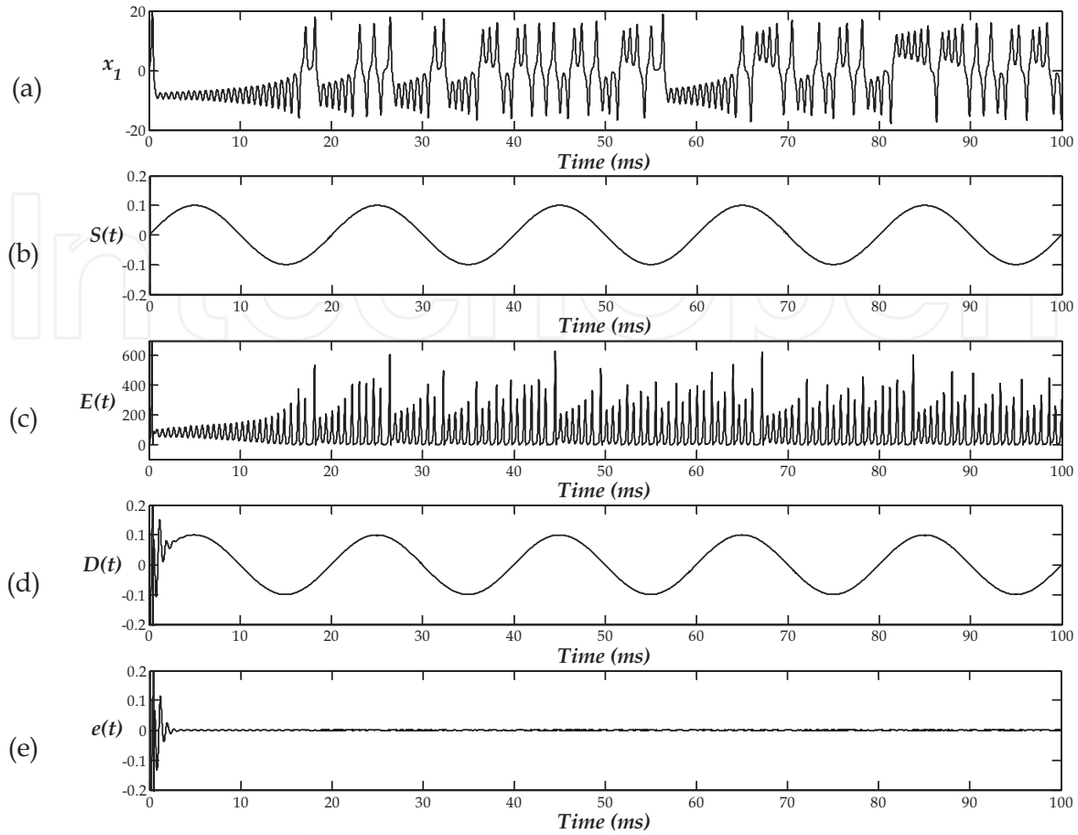



Fig. 10. Signals profile of the secure communication system. The synchronization signal, $x_1$, is shown in (a), the secret message, $s(t)$, in (b), the encrypted signal, $E(t)$, in (c), the decrypted signal, $D(t)$, in (d), and finally the decryption error, $e(t)$, in (e).

### 3.4 Sensitivity and security analysis for case study I

The encryption function considered in the previous section depends only on $x_2$ and consequently the decryption error is sensitive to synchronization errors. To investigate this problem, two cases will be considered that include both multiplicative and additive errors. These errors can result from channel noise, modelling errors, or both. The mathematical representation of this problem is described in Eq. (18).

$$\begin{aligned} &\text{Multiplicative error}: \hat{x}_2 = x_2(1+\Delta) \\ &\text{Additive error}: \hat{x}_2 = x_2 + \delta \end{aligned} \tag{18}$$

Figure (11) shows the synchronization error problem for the case when the transmitted message is an analog sinusoidal signal for different values of $\Delta$ and $\delta$, illustrating the strong dependence of the decryption error on the synchronization errors. Figures (12) and (13) confirm the same result when the frequency of the transmitted message is comparable to and much greater than the dominant frequency of the chaotic attractor of the transmitter, corresponding to 500 Hz and 5 kHz respectively.

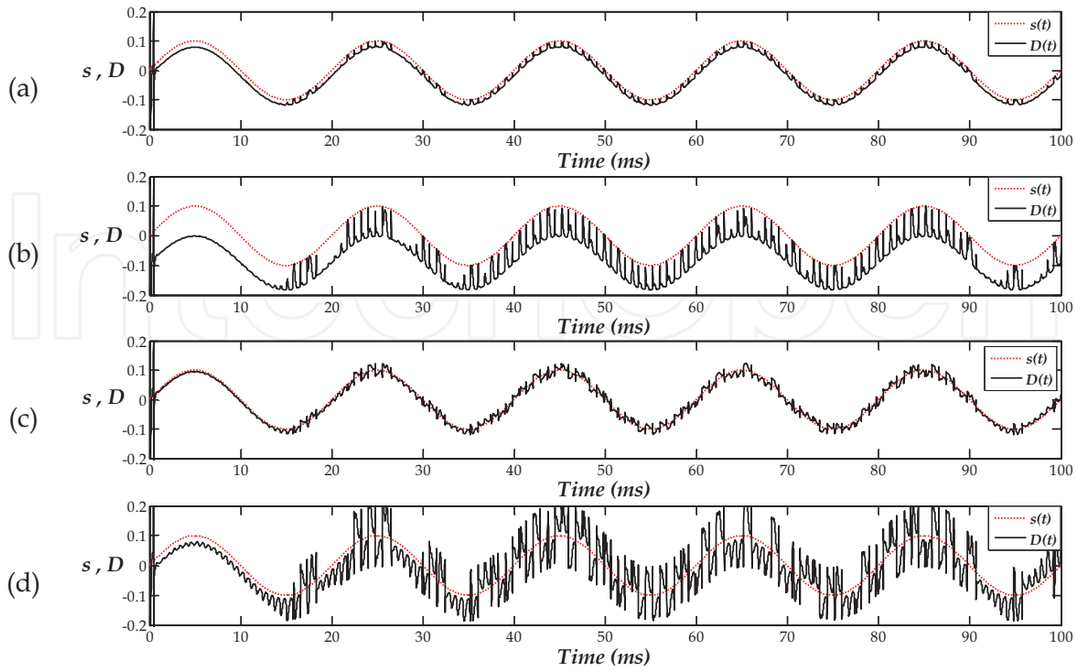



Fig. 11. The sensitivity to synchronization multiplicative errors is exemplified in (a) and (b), corresponding to $\Delta = 0.01$ and 0.05 respectively and to synchronization additive errors in (c) and (d), corresponding to $\delta = 0.02$ and 0.1 respectively ($f_s = 50$ Hz).

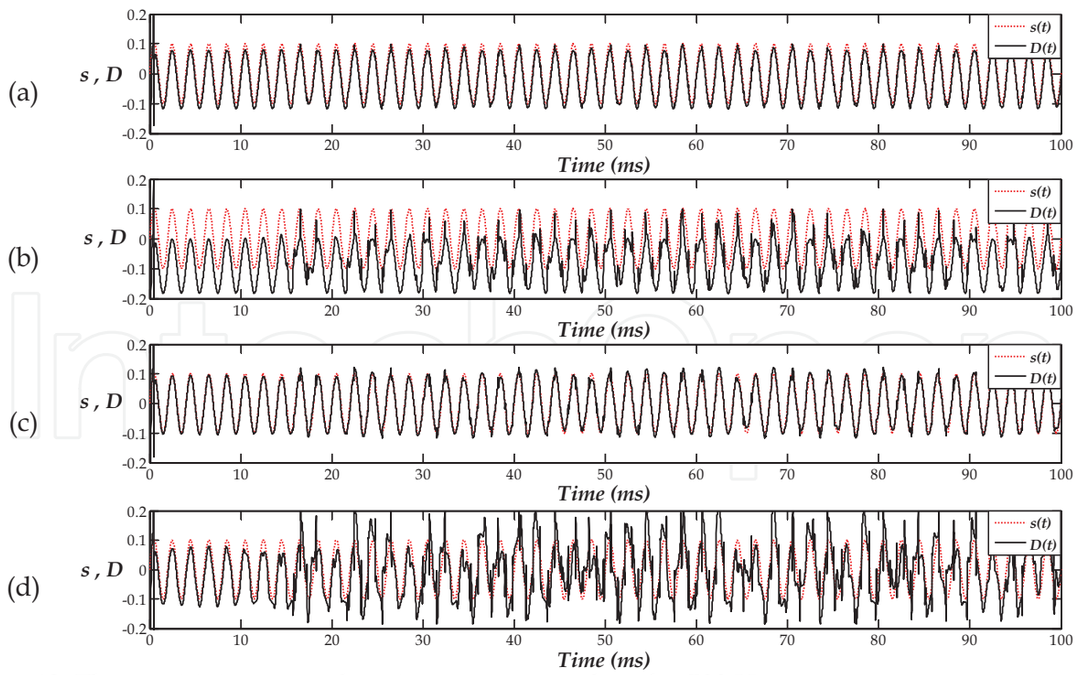



Fig. 12. The sensitivity to synchronization errors, when $f_s = 500$ Hz.

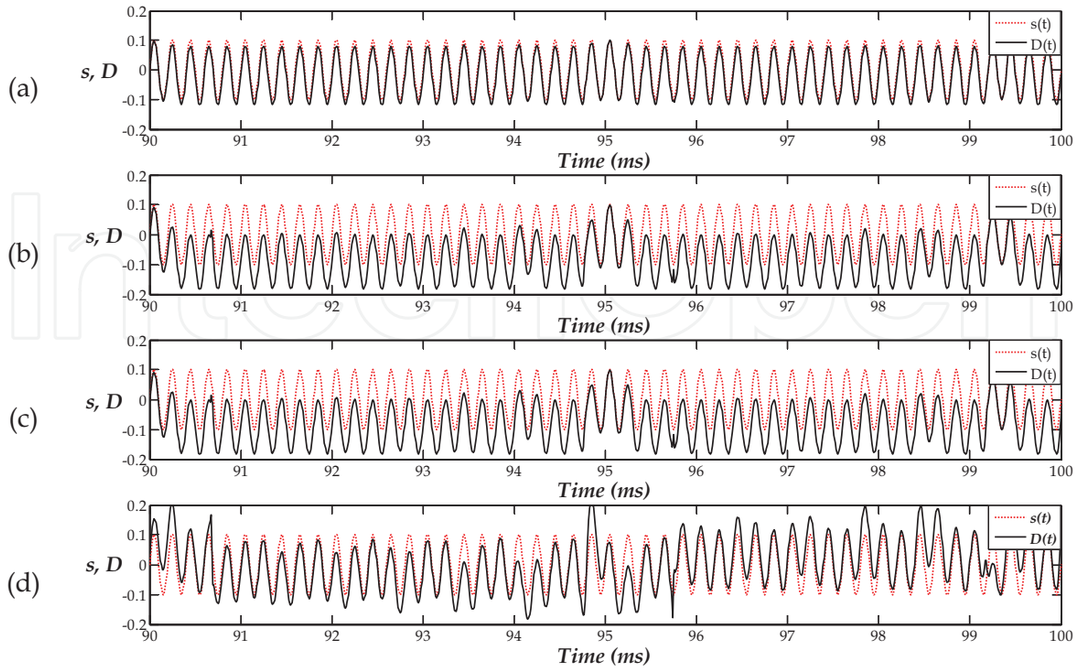



Fig. 13. The sensitivity to synchronization errors, when $f_s$ = 5 kHz.

Figures (11-13) show that the effect of additive error is more critical than multiplicative error. In addition, as the frequency of the transmitted signal increases the decrypted signal deteriorates, as transient effects will persist. Although the envelope of the transmitted signal can be clearly seen from the distorted decrypted signal, for the transmission of digital signals this is not the case. To complete the analysis of the communication system, its security is investigated by assuming that an intruder picks up the encrypted message from the communication channel and then tries to isolate the digital secret message by employing a two-stage process consisting of low-pass filtering and thresholding. This is illustrated in Fig. (14).

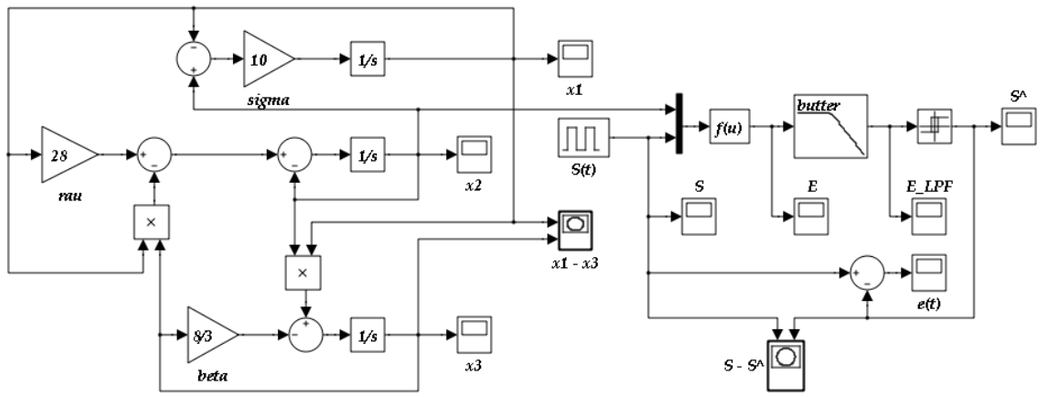



Fig. 14. A Simulink model illustrating the possibility of breaking the security of the communication system via utilizing simple filtering techniques.

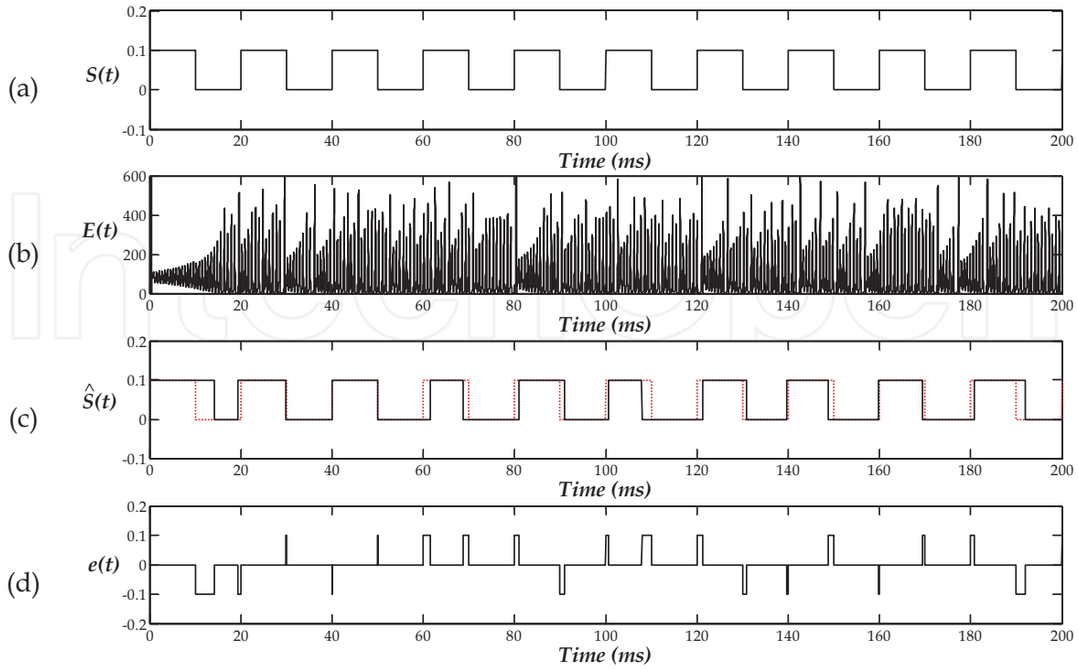



Fig. 15. The response of the intruder system showing the original secret message; $s(t)$, its encryption using only $x_2$; $E(t)$, the decrypted signal; $D(t)$ superimposed on $s(t)$, and the decryption error; $e(t)$, in (a), (b), (c), and (d) respectively.

Figure (15) shows a successful attack of an intruder for the case when the frequency of the digital secret message, $f_s$, was much less than that of the chaotic transmitter, $f_d$. The same argument applies when $f_s$ is much higher than $f_d$ as using a high-pass filter can isolate the digital message; however, the effect of time delays and channel noise will be more obvious. When $f_s$ and $f_d$ occupy the same frequency interval, it will not be possible to use filtering techniques to separate them from each other. This fact will be used later in this chapter to robustify the design of the secure communication system. It can be also demonstrated that it is easier to break into the system and recover digital message rather than analog messages because of the sensitivity of the later to noise.

### 3.5 Case study II

The aforementioned discussion requires modifying the encryption function at the transmitter, depicted by Fig. (7) and Eq. (17), to make it more difficult for the intruder to break the security of the communication system. This will be the topic of the next section; but first the parameter modulation technique is now investigated as a possible replacement to encryption. Figure (16) shows a Simulink model for such purpose, where the secret message is used directly to modulate the value of $\sigma$. The analysis carried out in (Álvarez, 2004; Zaher, 2009) is now used to prove that it is easy to recover the original digital signal using low-pass filtering followed by thresholding, without having to know the structure of the transmitter or to synchronizer a receiver model with that of the transmitter. Figure (17) illustrate the results of such system.

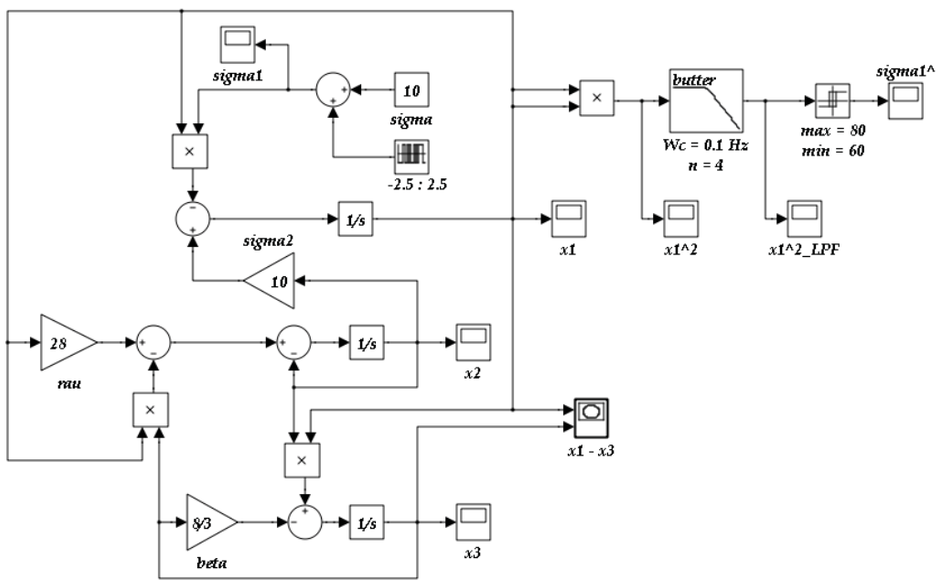



Fig. 16. A Simulink block diagram illustration of using simple filtering techniques to break into a chaos-based communication system that relies on parameter modulation.

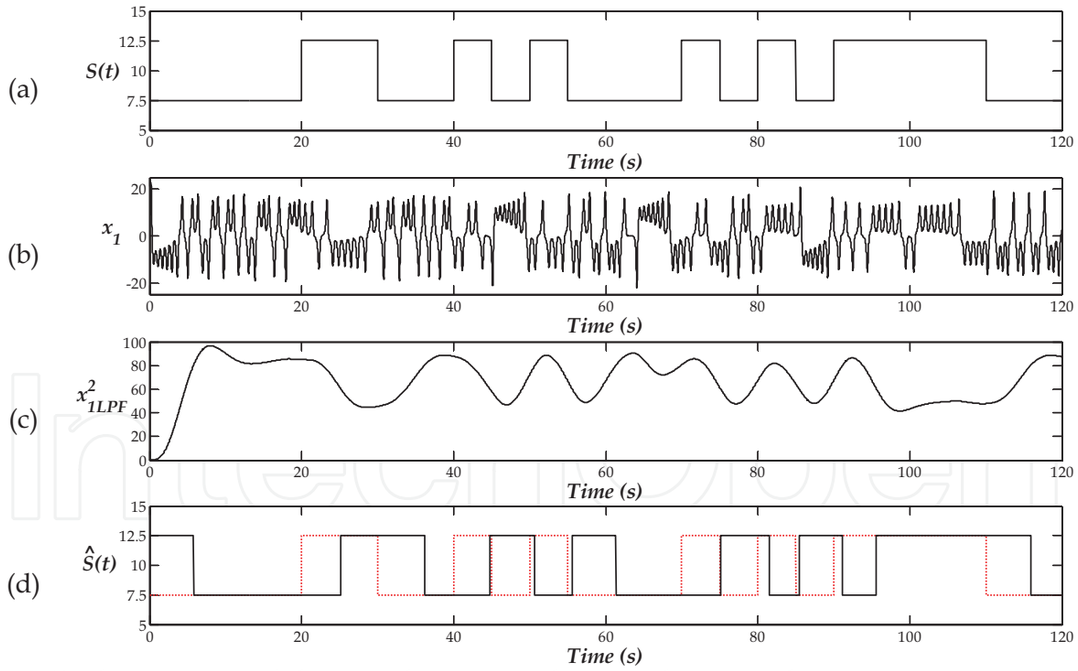



Fig. 17. The response of the intruder system showing the original secret message; $s(t)$, its encryption; $E(t)$, the output of the low-pass filter, and the reconstructed message, superimposed on $s(t)$, in (a), (b), (c), and (d) respectively.

## 4. Identifying the Parameters of Chaotic Systems

A feasible improvement to chaos-based cryptosystems can be made via making the encryption process a function of one or more of the parameters of the chaotic transmitter and not only the states. A possible candidate is given in Eq. (19) and is illustrated in Fig. (18).

$$\begin{aligned} E(X,\sigma,s,t) &= x_2^2 + (\sigma^2 + x_2^2)s(t) \\ \hat{s}(t) = D(\hat{X},\sigma,s,t) &= (E(X,\sigma,s,t) - \hat{x}_2^2)/(\sigma^2 + \hat{x}_2^2) \end{aligned} \tag{19}$$

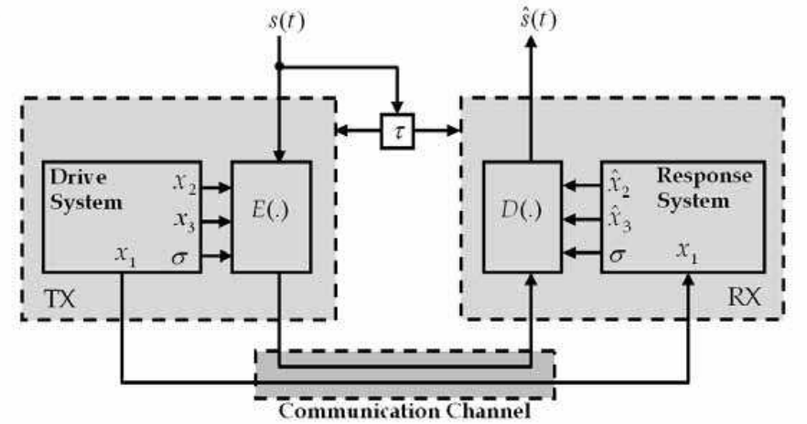



Fig. 18. A block diagram representation of the modified chaos-based secure communication system for which the encryption function depends on $\sigma$.

Although the scrambling of the message is improved, this has the effect of increasing the message strength; thus making it more vulnerable to be digged out of the encrypted signal using simple filtering techniques. This is illustrated in Fig. (19) using the same filtering technique discussed in Sec. (3.5). Figure (20) shows a Simulink model for implementing Eq. (19), while Figs. (21) and (22) show the effect of guessing $\sigma$ by the intruder, assuming that only the model of the transmitter and the structure of the encryption function are known.

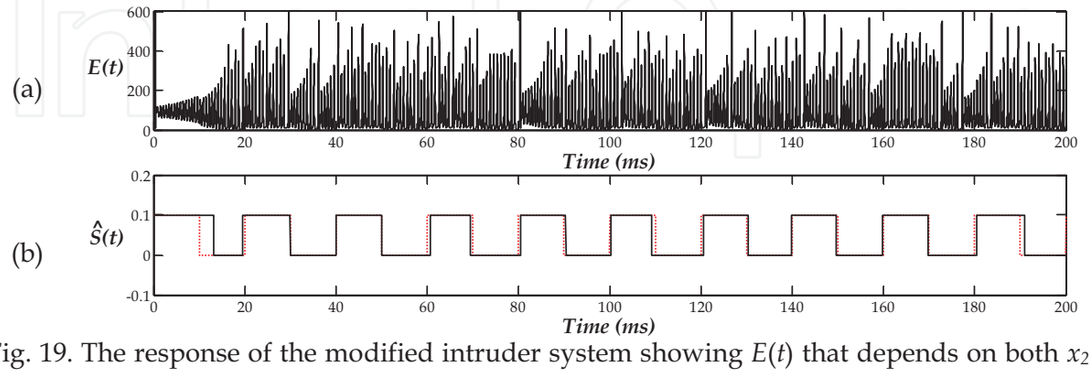



Fig. 19. The response of the modified intruder system showing $E(t)$ that depends on both $x_2$ and $\sigma$; and the decrypted signal, $D(t)$, superimposed on $s(t)$, in (a), (b) respectively.

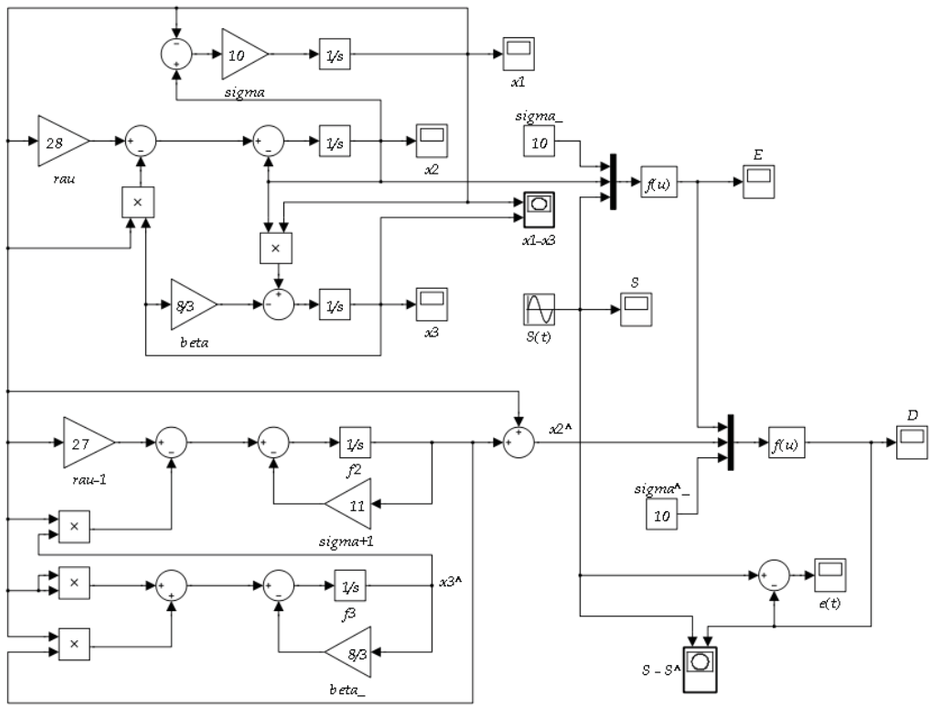
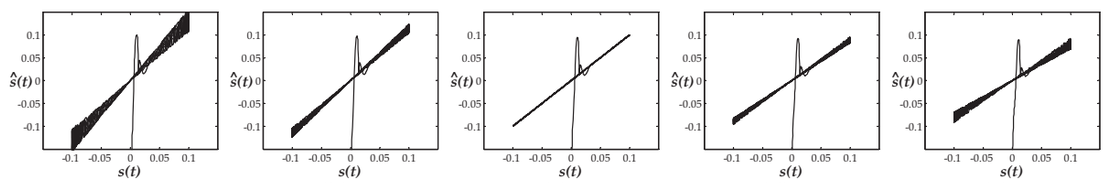
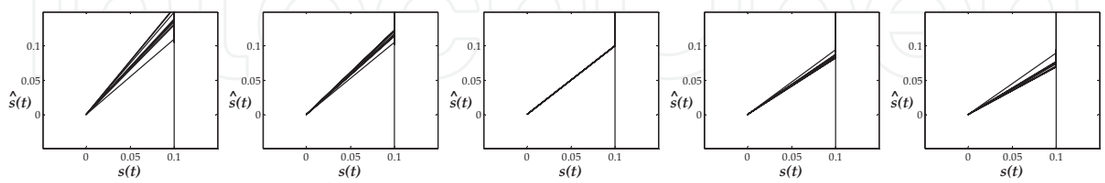



Fig. 20. A Simulink block diagram illustration of using the modified encryption function in Eq. (19) assuming a constant value of $\sigma$.




(a) (b) (c) (d) (e)

Fig. 21. The response of the receiver (or intruder) system assuming complete knowledge of the encryption function and guessing different values for $\sigma$ corresponding to 8, 9, 10, 11, and 12 in (a), (b), (c), (d), and (e) respectively (analog case).




(a) (b) (c) (d) (e)

Fig. 22. The response of the receiver (or intruder) system assuming complete knowledge of the encryption function and guessing different values for $\sigma$ corresponding to 8, 9, 10, 11, and 12 in (a), (b), (c), (d), and (e) respectively (digital case).

### 4.1 Partial identification of the transmitter parameters

Many chaos-based applications require the estimation of some or all of the chaotic system parameters. The degree of complexity of the estimation process depends crucially on many factors; among them the structure and type of nonlinearity of the system at hand, complete or partial availability of the states for direct measurement, and the nature of the application, e.g., whether it is required to control the chaos, or to synchronize two identical or different chaotic systems (Zaher, 2008b). Meanwhile, it is interesting to notice that most, if not all, parameter identification algorithms come together with some form of synchronization, i.e. it is required to identify the unknown parameters in order to achieve synchronization, or synchronization is used as an intermediate step to identify the unknown parameters.

The design procedure for both synchronization and parameter identification usually achieves the desired objectives by constructing a suitable Lyapunov function and forcing its derivative to be negative definite. However, the construction of Lyapunov functions remains to be a difficult task, and is usually considered a bottleneck in the design. Achieving the stability and convergence of the parameter identification algorithms is usually difficult to prove analytically, especially when using synchronization due to the increased order of the overall system (Kocarev & Parlitz, 1995).

Utilizing a single scalar time series for the purpose of parameter identification, synchronization, or both usually puts some constraints on the ability to identify all the parameters of the chaotic system. Many techniques were reported in the literature that only deal with partial identification with application to the Lorenz system (d'Anjou, 2001; Sakaguchi, 2002; Solak, 2004; Zaher, 2007). Motivated by the requirement to improve the security of the encryption function, the parameter $\sigma$ can be considered as a secret key (cipher). Choosing the interval for $\sigma$ should ensure the persistence of chaos; otherwise, the encryption process will fail. For the Lorenz system and considering the nominal values for both $\rho$ and $\beta$ it was found that the chosen range of $8 \le \sigma \le 12$ is satisfactory. In the next section we derive the mathematical foundation for estimating $\sigma$ at the receiver side using only the knowledge of $x_1$ under the assumption that both $\rho$ and $\beta$ are kept constants.

### 4.2 Design of the parameter update law

Under the assumptions in the previous section, the modified receiver dynamics are now described by

$$\begin{aligned} \dot{\hat{x}}_1 &= -\hat{\sigma}\hat{x}_1 + \hat{\sigma}\hat{x}_2 \\ \dot{\hat{x}}_2 &= \rho x_1 - \hat{x}_2 - x_1\hat{x}_3 \\ \dot{\hat{x}}_3 &= -\beta\hat{x}_3 + x_1\hat{x}_2 \end{aligned} \tag{20}$$

where the "^" symbol stands for the estimated value of the unknown state or parameter. Thus, the synchronization and identification errors, respectively, are given by

$$\begin{aligned} e_i &= \hat{x}_i - x_i \,, i = 1,2,3 \\ e_\sigma &= \hat{\sigma} - \sigma \end{aligned} \tag{21}$$

resulting in

$$\begin{aligned}\dot{e}_1 &= \dot{\hat{x}}_1 - \dot{x}_1 \\ &= (-\hat{\sigma}\hat{x}_1 + \hat{\sigma}\hat{x}_2) + (\sigma x_1 - \sigma x_2) \\ &= (-\hat{\sigma}\hat{x}_1 + \hat{\sigma}\hat{x}_2 + \hat{\sigma}x_1 - \hat{\sigma}x_2) + (\sigma x_1 - \sigma x_2 - \hat{\sigma}x_1 + \hat{\sigma}x_2) \\ &= \hat{\sigma}[(\hat{x}_2 - x_2) - (\hat{x}_1 - x_1)] + (\hat{\sigma} - \sigma)(x_2 - x_1) \\ &= \hat{\sigma}(e_2 - e_1) + e_\sigma(x_2 - x_1)\end{aligned} \tag{22}$$

and

$$\begin{aligned}\dot{e}_2 &= \dot{\hat{x}}_2 - \dot{x}_2 \\ &= (\rho x_1 - \hat{x}_2 - x_1\hat{x}_3) - (\rho x_1 - x_2 - x_1 x_3) \\ &= -(\hat{x}_2 - x_2) - x_1(\hat{x}_3 - x_3) \\ &= -e_2 - x_1 e_3\end{aligned} \tag{23}$$

and

$$\begin{aligned}\dot{e}_3 &= \dot{\hat{x}}_3 - \dot{x}_3 \\ &= (-\beta\hat{x}_3 + x_1\hat{x}_2) - (-\beta x_3 + x_1 x_2) \\ &= -\beta(\hat{x}_3 - x_3) - x_1(\hat{x}_2 - x_2) \\ &= -\beta e_3 - x_1 e_2\end{aligned} \tag{24}$$

The goal now is to force the synchronization errors to zero, and, at the same time, to design a parameter update law for $\sigma$ such that the overall system is asymptotically stable. Notice that the receiver has an order of four, compared to the previous one, given by Eqs. (3-9), which has an order of only two. Introducing the following Lyapunov function

$$L = 0.5[e_1^2 + \mu_{23}(e_2^2 + e_3^2) + \mu_\sigma e_\sigma^2] \tag{25}$$

where $\mu_{23}$ and $\mu_\sigma$ are positive constants, leads to

$$\begin{aligned}\dot{L} &= e_1\dot{e}_1 + \mu_{23}e_2\dot{e}_2 + \mu_{23}e_3\dot{e}_3 + \mu_\sigma e_\sigma^2 \\ &= (\hat{\sigma}e_1e_2 - \hat{\sigma}e_1^2 + x_2e_1e_\sigma - x_1e_1e_\sigma) - (\mu_{23}e_2^2 + \mu_{23}x_1e_2e_3) + (\mu_{23}x_1e_2e_3 - \mu_{23}\beta e_3^2) + \mu_\sigma e_\sigma\dot{\hat{\sigma}} \\ &= -(\hat{\sigma}e_1^2 - \hat{\sigma}e_1e_2 + \mu_{23}e_2^2) - \mu_{23}\beta e_3^2 + e_\sigma[e_1(x_2 - x_1) + \mu_\sigma\dot{\hat{\sigma}}]\end{aligned} \tag{26}$$

Proving negative definiteness of Eq. (26) can be greatly simplified by using the assumptions given in Eqs. (27) and (28)

$$\mu_{23} = \frac{\hat{\sigma}}{4}, 0 \le \hat{\sigma} \le \sigma_{\max} \tag{27}$$

$$\dot{\hat{\sigma}} = -\frac{1}{\mu_{23}}(x_2 - x_1)e_1 = -\frac{1}{\sigma\mu_{23}}e_1\dot{x}_1 = k\dot{x}_1(x_1 - \hat{x}_1) \tag{28}$$

where $k = 1/(\sigma\mu_{23})$, as this results in

$$\begin{aligned}\dot{L} &= -[(\sqrt{\hat{\sigma}}e_1)^2 - 2\sqrt{\hat{\sigma}}\frac{\sqrt{\hat{\sigma}}}{2}e_1e_2 + (\frac{\sqrt{\hat{\sigma}}}{2}e_2)^2] - \frac{\hat{\sigma}}{4}\beta e_3^2 \\ &= -(\sqrt{\hat{\sigma}}e_1\frac{\sqrt{\hat{\sigma}}}{2}e_2)^2 - \frac{\hat{\sigma}}{4}\beta e_3^2 \le 0\end{aligned} \tag{29}$$

The parameter update law, given in Eq. (28), and the result, outlined in Eq. (29) completes the design of the modified secure communication system. Thus, at the receiver side, the message can be decrypted provided that the time delay required for synchronization and identification errors is negligible. This can be guaranteed via choosing a large value for $k$. Based on the previous results, using a constant value for $\sigma$ results in poor security, as the intruder can still guess its value. Moreover, if the bandwidths of the transmitted signal and the chaotic transmitter are widely separated, simple filtering techniques can still recover the original message, despite the improved encryption done at the transmitter side. To overcome these problems, another technique will be attempted, in the next section, to achieve improved encryption in both time and frequency domains.

## 5. A Proposal for a Robust Communication System

A better scrambling of the secret message can be obtained if the encryption function is made to depend on a continuously changing parameter along with the chaotic states of the transmitter. This parameter can correspond to one of the chaotic transmitter parameters and consequently it can accomplish two tasks:

i. to act as a cipher key that makes the scrambling process of the transmitted message more robust,
ii. to continuously change the chaotic attractor of the transmitter; thus making it harder for an intruder to break into the communication channel

At the receiver, it will be required to accomplish both synchronization with the transmitter and identification of the unknown parameter. Careful examination of Eq. (20) reveals a very important property of the proposed system, which is the decoupling between the states to be synchronized and the parameter to be identified; i.e. the parameter update law has no effect of the synchronization mechanism. In addition, the transmitted signal and the secret key can be made to occupy the same frequency band, thus, retrieving the original message using filtering techniques is impossible. Thus, a new proposal for the robust secure communication system, choosing $x_1$ as the synchronizing signal, and both $x_2$ and $\sigma$ for implementing the encryption function, can take the form

$$\begin{aligned}E(X,\sigma,s,t) &= x_2^2 + (\sigma^2 + x_2^2)s(t) \\ \hat{s}(t) &= D(\hat{X},\hat{\sigma},s,t) = (E(X,\sigma,s,t) - \hat{x}_2^2)/(\hat{\sigma}^2 + \hat{x}_2^2)\end{aligned} \tag{30}$$

With reference to Figs. (7) and (18), Fig. (23) shows a block diagram representation of the robust system, while Fig. (24) illustrates a Simulink model. For both simulation and comparison purposes, $s(t)$ was chosen to correspond to the digital signal considered in (Álvarez,

2004 ), and a piecewise linear profile for $\sigma$ was chosen such that both $s(t)$ and $\sigma$ occupy the same frequency band. No time scaling was necessary in this case and consequently $\tau$ was set to one, while all other parameters are shown in Fig. (24) that is seen to consist of five parts, the transmitter, the encrypter, the synchronization mechanism, the parameter update law, and the dycrypter followed by low pass filtering and thresholding (Zaher, 2009).

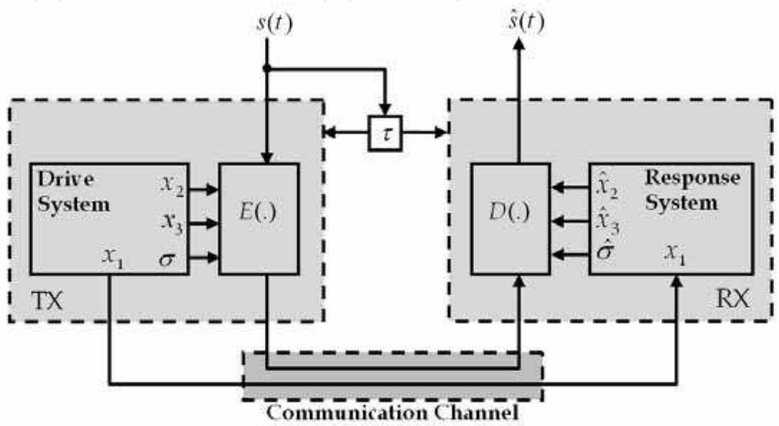



Fig. 23. Block diagram of the robust secure communication system for which both the encryption function and the chaotic transmitter use a piecewise linear profile for $\sigma$.

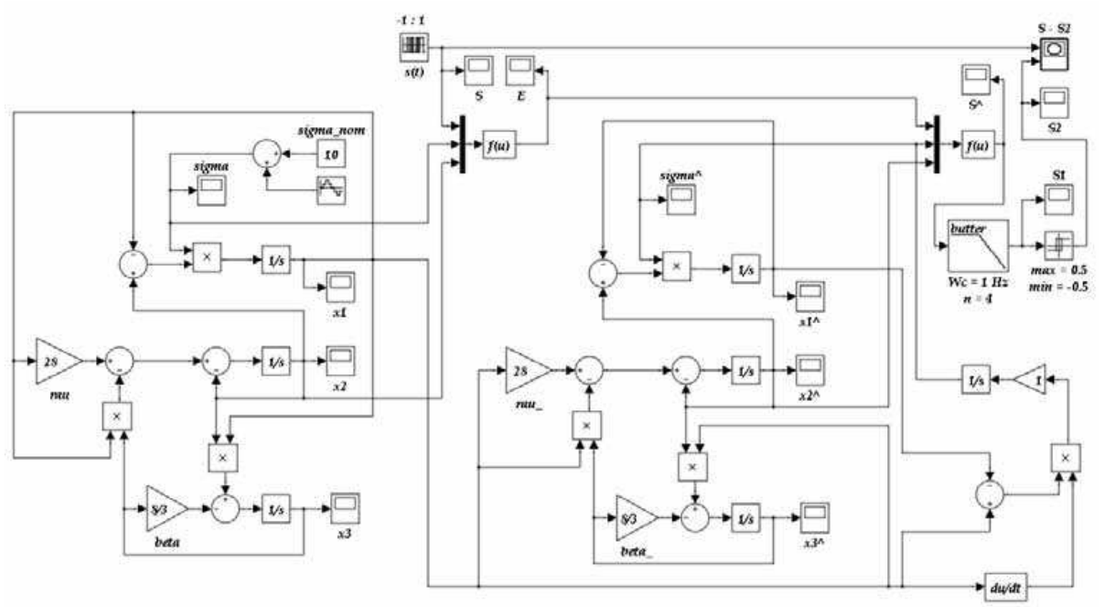



Fig. 24. A Simulink block diagram illustration of the system depicted in Fig. (23).

### 5.1 case study III

Figure (25) shows the simulation results when using the Simulink model, in Fig. (24), after attenuating $s(t)$ by a factor of 100 so that its envelope will be perfectly hidden in the transmitted encrypted signal, $E(t)$, which looks almost like a whit noise. As illustrated in Fig.

(25d), the recovered message is a time-delayed replica of the original message.

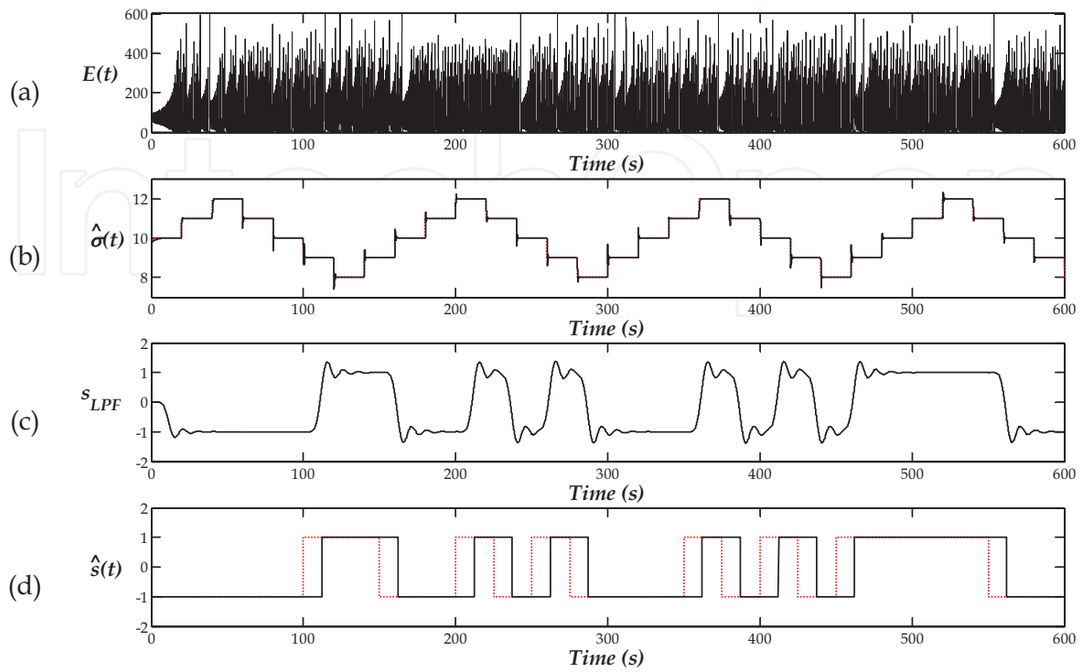



Fig. 25. Simulation results of the robust communication system, when $k$ = 1, showing the encrypted signal, $E$, the estimated value of $\sigma$ superimposed on its original profile, the output after the low-pass filter stage, and the thresholding stages in (a) – (d) respectively.

### 5.2 Security analysis of case study III

Using filtering techniques to break the security of this system is not possible as both $s(t)$ and $\sigma$ are shown to occupy almost the same bandwidth with overlapping frequencies. The time-based decrypter can effectively extract $s(t)$ from the scrambled message provided that $\sigma$ is identified fast enough. This can be achieved by increasing the gain of the parameter update low, $k$, along with attenuating the magnitude of $s(t)$ before using it in the encrypter. To demonstrate this, the Simulink model, shown in Fig. (26), was used to attempt breaking the system security via intercepting the signals available in the public communication channel, namely $E(t)$ and $x_1(t)$, and the results, shown in Fig. (27), verify the robustness of the system. It is also possible to cope with transmitting different messages having different bandwidths via adjusting the time scaling factor, $\tau$, which has the effect of controlling the dominant frequency of the chosen chaotic attractor as well as the time profile for $\sigma$. Other linear and/or nonlinear forms of the encryption functions can be used to promote the security of the system, e.g. using both $x_2$ and $x_3$ in the encryption process. Finally, it can be demonstrated that this system is capable of transmitting both analog and digital signals.

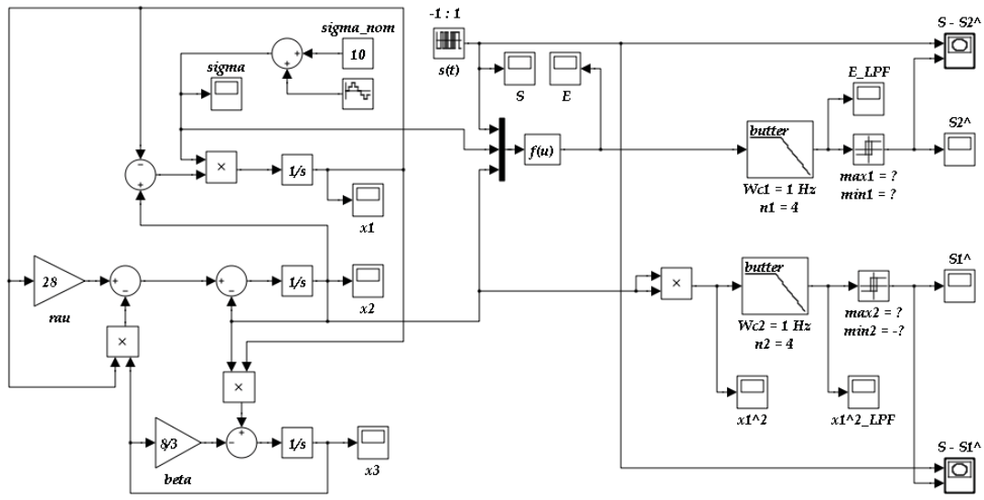



Fig. 26. A Simulink block diagram illustration of the two-filter intruder system.

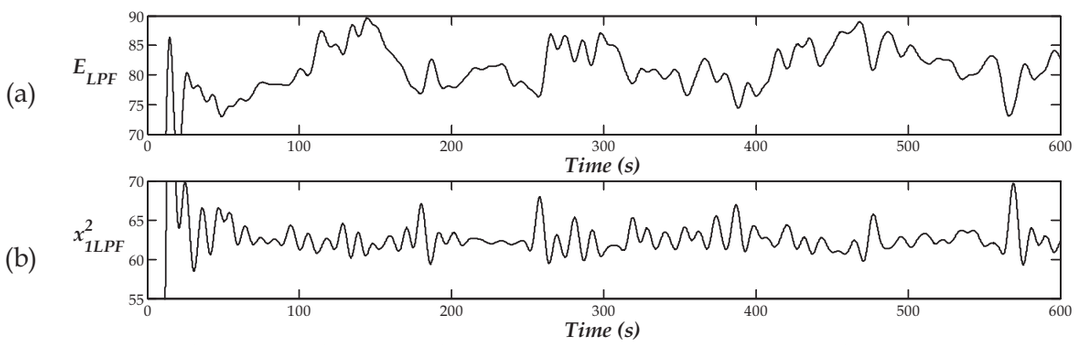



Fig. 27. Results of low-pass filtering of the intruder system, illustrating failure to reconstruct the original message using the encrypted or the driving signals in (a) and (b) respectively.

## 6. Summary and Conclusion

The topic of chaos-based secure communication systems was investigated. The main two processes of chaos synchronization and parameter identification were explored as they represent the corner stone in designing chaos-based cryptosystems. A fast synchronization mechanism was designed using a recursive technique that allows the control of the convergence rate of the synchronization errors. This technique proved to be easy to implement and tune at the same time, compared to other complete synchronization methods reported in the literature. Three case studies were considered that deal with different scenarios involving both analog and digital signals having different bandwidths. Using encryption functions with different forms was attempted, and it was found that some of these forms provide poor security when the frequencies of the transmitted signal and the chaotic attractor are far away in the frequency domain. By augmenting parameter modulation with cryptography, robustness can be improved and the communication system can have a better chance to survive intruder attacks. Although, the Lorenz system was used in this chapter, extensions to other chaotic systems, satisfying the same design characteristics, is straightforward.

## 7. References

Álvarez, G.; Montoya, F.; Romera, M. & Pastor, G. (2004). Breaking parameter modulated chaotic secure communication system. *Chaos Solitons Fractals*, Vol. 21, No. 4, pp. 783-787

Balmforth, N.; Tresser, C.; Worfolk, P. & Wu, C. (1997). Master-slave synchronization and the Lorenz equations. *Chaos*, Vol. 7, No. 3, pp. 392-394

Boccaletti, S.; Kurths, J.; Osipov, G.; Valladares, D. & Zhou, C. (2002). The synchronization of chaotic systems. *Phys Rep*, Vol. 366, No. 1-2, pp. 1-101

Carroll, T. (2004). Chaotic control and synchronization for system identification. *Phys Rev E*, Vol. 69, No. 4, pp. 046202:1-7

Chen, M. & Kurths, J. (2007). Chaos synchronization and parameter estimation from a scalar output signal. *Phys Rev E*, Vol. 76, No. 2, pp. 027203:1-4

Cuomo, K. & Oppenheim, A. (1993). Circuit implementation of synchronized chaos with applications to communications. *Phys Rev Lett*, Vol. 71, No. 1, pp. 65-68

Cuomo, K.; Oppenheim, A. & Strogatz, S. (1993). Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Trans Circ Syst II*, Vol. 40, No. 10, pp. 626-633

d'Anjou, A.; Sarasola, C.; Torrealdea, F.; Orduña, R. & Grana, M. (2001). Parameter-adaptive identical synchronization disclosing Lorenz chaotic masking. *Phys Rev E*, Vol. 63, No. 4, pp. 046213:1-5

Dachselt, F. & Schwarz, W. (2001). Chaos and Cryptography. *IEEE Trans Circ Syst I*, Vol. 48, No. 12, pp. 1498-1508

Dedieu, H.; Kennedy M. & Hasler, M. (1993). Chaos shift keying – modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits. *IEEE Trans Circ Syst II*, Vol. 40, No. 10, pp. 634-642

Jiang, Z. (2002). A note on chaotic secure communication systems. *IEEE Trans Circ Syst I*, Vol. 49, No. 1, pp. 92-96

Kocarev, L. & Parlitz, U. (1995). General approach for chaotic synchronization with application to communication. *Phys Rev Lett*, Vol. 74, No. 25, pp. 5027-5031

Kocarev, L.; Halle, K.; Eckert, K.; Parlitz, U. & Chua, L. (1992). Experimental demonstration of secure communications via chaotic synchronization. *Int J Bifur Chaos*, Vol. 2, No. 3, pp. 709-713

Krstic, M.; Kanellakopoulus, I. & Kokotovic, P. (1995). *Nonlinear and Adaptive Control Design.* John Wiley & sons Inc., ISBN: 978-0471127321

Liao, T. & Huang, N. (1999). An observer-based approach for chaotic synchronization with applications to secure communications. *IEEE Trans Circ Syst I*, Vol. 46, No. 9, pp. 1144-1150

Lorenz, E. (1963). Deterministic nonperiodic flow. *J Atmos Sci*, Vol. 20, No. 2, pp. 130-141

Parlitz, U.; Chua, L.; Kocarev, L.; Halle, K. & Shang, A. (1992). Transmission of digital signals by chaotic synchronization. *Int J Bifurc Chaos*, Vol. 2, No. 4, pp. 973-977

Pecora, L. & Carroll, T. (1990). Synchronization in chaotic systems. *Phys Rev Lett*, Vol. 64, No. 8, pp. 821-825

Pecora, L. & Carroll, T. (1991). Driving systems with chaotic signals. *Phys Rev A*, Vol. 44, No. 4, pp. 2374-2284

Pehlivan, I. & Uyaroğlu, Y. (2007). Rikitake attractor and its synchronization application for secure communication systems. *J Appl Sci*, Vol. 7, No. 2, pp. 232-236

Sakaguchi, H. (2002). Parameter evaluation from time sequences using chaos synchronization, *Phys Rev E*, Vol. 65, No. 2, pp. 027201:1-4

Schuster, H. & Wolfram, J. (2005). *Deterministic Chaos: An Introduction*. Wiley-VCH, ISBN: 978-3527404155

Short, K. (1994). Steps toward unmasking secure communications. *Int J Bifurc Chaos*, Vol. 4, No. 4, pp. 959-977.

Sobhy, M. & Shehata, A. (2000). Secure computer communication using chaotic algorithms. *Int J Bifurc Chaos*, Vol. 10, No. 12, pp. 2831-2839

Solak, E. (2004). Partial identification of Lorenz system & its application to key space reduction of chaotic cryptosystems. *IEEE Trans Circ Syst II*, Vol. 51, No. 10, pp. 557-560

Stinson, D. (2005). *Cryptography: theory and practice*, *3rd ed*. CRC Press, ISBN: 978-1584885085

Weiss, C. & Vilaseca, R. (1991). *Dynamics of Lasers.* VCH, Weinheim, ISBN: 978-0895739667

Wu, C. & Chua, L. (1993). A simple way to synchronize chaotic systems with applications to secure communication systems. *Int J Bifurc Chaos*, Vol. 3, No. 6, pp. 1619-1627

Yang, T. & Chua, L. (1996). Secure communication via chaotic parameter modulation. *IEEE Trans Circ Syst I,* Vol. 43, No. 9, pp. 817-819

Yang, T. & Chua, L. (1997). Impulsive stabilization for control and synchronization of chaotic systems – theory and application to secure communication. *IEEE Trans Circ Syst I*, Vol. 44, No. 10, pp. 976-988

Yang, T. (1995). Recovery of digital signals from chaotic switching. *Int J Circ Theory App*, Vol. 23, No. 6, pp. 611-615

Yang, T. (2004). A survey of chaotic secure communication systems. *Int J Comput Cogn*, Vol. 2, No. 2, pp. 81-130

Yang, T.; Wu, C. & Chua, L. (1997). Cryptography based on chaotic systems. *IEEE Trans Circ Syst I*, Vol. 44, No. 5, pp. 469-472

Yaowen, L.; Guangming, G.; Hong, Z; & Yinghai, W. (2000). Synchronization of hyperchaotic harmonics in time-delay systems and its application to secure communication. *Phys Rev E*, Vol. 62, No. 6, pp. 7898-7904.

Zaher, A. (2007). A nonlinear controller design for permanent magnet motors using a synchronization-based technique inspired from the Lorenz system. *Chaos*, Vol. 18, No. 1, pp. 013111:1-12

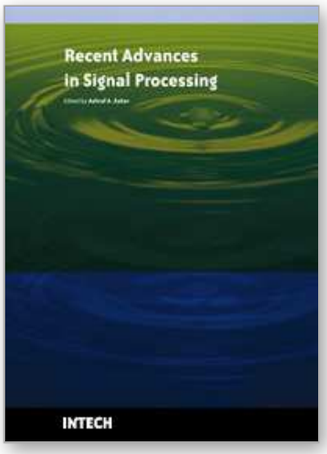
Zaher, A. (2008a). Design of fast state observers using a backstepping-like approach with application to synchronization of chaotic systems. *Chaos*, Vol. 18, No. 2, pp. 023114:1-10

Zaher, A. (2008b). Parameter identification technique for uncertain chaotic systems using state feedback and steady-state analysis. *Phys Rev E*, Vol. 77, No. 3, pp. 036212:1-12

Zaher, A. (2009). An improved chaos-based secure communication technique using a novel encryption function with an embedded cipher key. *Chaos Solitons Fractals*, (in press)

Zhang, Y.; Tao, C.; Du, G. & Jiang, J. (2005). Synchronized pseudorandom systems and their application to speech communication. *Phys Rev E*, Vol. 71, No. 1, pp. 16217290:1-5

Zhou, C. & Lai, C. (1999). Decoding information by following parameter modulation with parameter adaptive control. *Phys Rev E*, Vol. 59, No. 6, pp. 6629-6636




**Recent Advances in Signal Processing**

Edited by Ashraf A Zaher

ISBN 978-953-307-002-5

Hard cover, 544 pages

**Publisher** InTech

**Published online** 01, November, 2009

**Published in print edition** November, 2009

The signal processing task is a very critical issue in the majority of new technological inventions and challenges in a variety of applications in both science and engineering fields. Classical signal processing techniques have largely worked with mathematical models that are linear, local, stationary, and Gaussian. They have always favored closed-form tractability over real-world accuracy. These constraints were imposed by the lack of powerful computing tools. During the last few decades, signal processing theories, developments, and applications have matured rapidly and now include tools from many areas of mathematics, computer science, physics, and engineering. This book is targeted primarily toward both students and researchers who want to be exposed to a wide variety of signal processing techniques and algorithms. It includes 27 chapters that can be categorized into five different areas depending on the application at hand. These five categories are ordered to address image processing, speech processing, communication systems, time-series analysis, and educational packages respectively. The book has the advantage of providing a collection of applications that are completely independent and self-contained; thus, the interested reader can choose any chapter and skip to another without losing continuity.



**InTech Europe**
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

**InTech China**
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen