International Journal of Innovative
Computing, Information and Control
Volume **9**, Number **5**, May **2013**

 ISSN 1349-4198
pp. 1865–1879

DIGITAL COMMUNICATION USING A NOVEL COMBINATION OF CHAOTIC SHIFT KEYING AND DUFFING OSCILLATORS

Ashraf A. Zaher

Department of Physics
College of Science
Kuwait University
P. O. Box 5969, Safat 13060, Kuwait
ashraf.zaher@ku.edu.kw

Received February 2012; revised June 2012

Abstract. *In this paper, an improved technique for constructing Chaotic Shift Keying (CSK) for transmitting digital signals is introduced. In contrast to the classical methods where only two chaotic attractors, representing logic 0 and logic 1 are used to build CSK, the proposed system allows the chaotic transmitted signal to alternate among four different chaotic attractors. In addition, the transmitter parameters are used to implement a novel XOR-based encryption function to scramble the secret message. This has the effect of effectively hiding the secret message and providing better security and privacy against intruders' attacks to the public communication channel. The parameters of the transmitter are assumed unknown, and are estimated at the receiver side to accomplish two tasks. The first one is to complete the synchronization process, while the second one is to decrypt the secret message using the duality property of the XOR-based digital function. A Duffing oscillator with smooth cubic nonlinearity is used to build the proposed system, where both synchronization and parameters estimation are carried out using an adaptive Lyapunov-based control approach. Simulation results are provided to illustrate the performance in both time and frequency domains using a single time series. Finally, recommendations for improving the performance are provided via discussing tuning of the control parameters and suggesting different ways to meet hardware constraints when transmitting real-time signals.*

Keywords: Chaos, Secure communication, Synchronization, Duffing oscillator

1. **Introduction.** Recently, and since the pioneer work of chaos synchronization [1], chaos-based secure communication systems have evolved in plenty of forms using different techniques to achieve synchronization between the transmitter and the receiver [2], while identifying the unknown parameters of the transmitter. This is mainly due to two reasons: first, is that chaotic signals, although deterministic, have power spectra that resemble white noise, and consequently can be used to hide secret messages; second, the drive-response synchronization technique has a structure that typically mimics the transmitter-receiver mechanism of communication systems [3]. Classical communication techniques, e.g., amplitude modulation (AM), frequency modulation (FM) and phase modulation (PM), depend on allowing the transmitted signal to directly influence the amplitude, frequency, or phase of a carrier signal that has more power and different dominant frequency. Analogous to that, previous work on chaos-based secure communication systems replaced the carrier with a chaotic signal that is either modulated directly by the transmitted signal, or simply added to it. This was known as chaotic modulation and additive masking respectively. Two more famous techniques, known as chaotic shift keying and chaotic switching, aimed at transmitting digital signals, used different chaotic

trajectories to correspond to the two binary levels of the data. The different chaotic trajectories can be generated from the same system via changing the parameters, or utilizing two completely different chaotic systems. Examples for these different methods can be found in [4-8], while a comparison between them, along with comments regarding the efficient utilization of the public communication channel can be found in [2].

Recently, remarkable works in chaos and its applications in secure communication can be found in the *International Journal of Innovative Computing, Information and Control, and Innovative Computing, Information and Control Express Letters* that are highlighted in the references herein.

Lately, significant research in cryptanalysis was done to break the security and privacy of chaos-based communication systems. This initiated the need for having more robust techniques that use cryptography [9]. Different methods for performing encryption and decryption at the transmitter and the receiver, respectively, were used such that the message is scrambled using a combination of the transmitter states and/or parameters. In addition, this new generation of chaotic cryptosystems used different degrees of complexity via incorporating both time-invariant and time-variant ciphers in both symmetric and asymmetric ways [10].

Chaotic Shift Keying (CSK) is one of the early methods used for transmitting digital signals over public channels [11]. This method received a lot of attention since the successful work in [1,3] to synchronize chaotic systems using drive-response techniques that are quite similar to the transmitter-receiver structure in communication systems. CSK was developed such that 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 of its two binary states [12]. Regarding implementation, either in analog or digital hardware, reconstructing the secret message can be efficiently done using a two-stage process consisting of low-pass filtering followed by thresholding [13]. This method was known to suffer from poor security, especially if the two attractors at the transmitter side are widely separated [14]. However, compared with other generations of chaos-based secure communication systems, it proved 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 [15]. Many techniques for constructing CSK were established, starting from the early work in [4], using both continuous and discrete systems. Differential chaos shift keying (DCSK), chaotic cyclic attractors shift keying (CCASK), binary phase shift keying (BPSK), quadrature phase shift keying (QPSK), and quadrature chaos shift keying (QCSK) are variants of the classical CSK method that are developed with the aim of having better noise rejection and increased data transmission rates [16-24].

Cryptography was used to improve the robustness of chaos-based secure communication systems via introducing complex nonlinear encryption functions and inserting ciphers during the encryption process [9,25-28]. In this paper, a novel combination for cryptography is used, which relies on the well-known XOR digital function, and an adaptive control technique that can synchronize the transmitter and the receiver, while identifying the unknown parameters of the transmitter. It is demonstrated that the proposed technique produces unbiased estimates of the transmitter parameters; hence, the decryption function is assured to faithfully reconstruct the secret message using the dual property of the XOR function. Two parameters of the transmitter are used to construct the encrypted message. Thus, the deficiency of using the trivial XOR-based cryptography is resolved, while maintaining the simplicity of the implementation. Simulation results prove that the proposed system is resilient to cryptanalysis using return map attacks, in addition

to frequency domain filtration techniques. The complete design process is thoroughly explained in Section 4.

Deciding on the structure of the chaotic system is usually the first step in designing a secure communication system. Implementation issues, nature of the signal to be transmitted, noise levels, and hardware constraints are the most important key factors in this step. The Lorenz, Rössler, and Chen systems are examples of autonomous systems that can be used in either chaotic or hyperchaotic ways to implement the suggested technique [29]. However, in this paper, a simple nonautonomous Duffing oscillator is used [30], for which four sets of its parameters are carefully chosen to generate four different chaotic attractors that are used to robustly hide the secret message to be transmitted.

Motivation: Currently reported research in the field of secure communication of digital signals, which relied on chaotic shift keying, made use of only two chaotic attractors for implementation. This made them vulnerable to return map attacks and simple frequency-based filtration techniques. In addition, they mostly relied on autonomous chaotic systems with variable degrees of complexity that, sometimes, employed some form of cryptography to improve the robustness of the system. This had the drawback of complicating the design process as well as resulting in a high-dimensional closed loop system. In this paper, these deficiencies are eliminated via diffusing the secret digital message in four chaotic attractors, while using a novel cryptography approach that relies on an XOR-based function that depends on time-varying parameters with nominal frequencies that overlap with both the nominal frequencies of the chaotic system and the transmitted message. In addition, replacing traditional autonomous chaotic systems with a nonautonomous Duffing oscillator is utilized to simplify the design and improve its real-time characteristics.

The rest of the paper is organized as follows. Section 2 describes the dynamics of the chaotic Duffing oscillator. Building the state observers and the parameters update laws for constructing a drive-response system is illustrated in Section 3. Section 4 proposes a secure communication system to transmit digital signals over public channels using a single time series and an XOR-based cryptosystem. Simulation results are provided for digital signals having different bandwidths, followed by a discussion in Section 5 that highlights the advantages of the proposed system and some recommendations for improving its performance.

2. **The Duffing Oscillator.**

Uncontrolled Duffing oscillators can exhibit different responses, e.g., sustained single period oscillations, multiple-period oscillations, and chaos [31], depending on the structure of the nonlinearity and how the external excitation is included in the dynamics. It may even exhibit bursting oscillations with different waveforms under certain external forcing conditions [32]. The Duffing equation was first introduced by the German engineer Georg Duffing in 1918 and since then, a tremendous amount of work was developed to solve it both analytically and numerically. Since 1970s, it became very popular in chaos-related research to investigate many physical systems in both science and engineering [33]. The Duffing equation has many different forms that represent nonlinear damping [34], along with other forms of strange nonlinearities [35]. The Duffing equation describes forces, acting in a dynamical system, that are governed by the gradient of some potential that can exhibit different forms, e.g. single or double well, with typical applications in physics, electronics, biology, neurology, and many other disciplines. Different synchronization and control methods for the Duffing oscillator, along with both numerical and experimental investigations can be found in [36-41]. In this paper, the model described in [42] is used, for which the dynamics are given by:

$$\ddot{y} + \gamma\dot{y} - y + y^3 = A\cos\omega t \tag{1}$$

where γ and A are two positive constants that represent the damping coefficient and the amplitude of the external forcing function, respectively, while $\omega = 2\pi f$ is the frequency of the external forcing function in rad/s. Equation (1) describes a nonautonomous nonlinear second order system with smooth cubic nonlinearity that can exhibit a variety of different responses ranging from a single steady oscillation, multi-period oscillation, to chaos, depending on the values of both γ and A, for a given value of ω. Using state space analysis, the Duffing system, in Equation (1), can be cast in the form:

$$\left.\begin{array}{l} x_1 = y \\ x_2 = \dot{y} \end{array}\right\} \Rightarrow \begin{array}{l} \dot{x}_1 = \dot{y} = x_2 \\ \dot{x}_2 = \ddot{y} = -\gamma x_2 + x_1 - x_1^3 + A\cos\omega t \end{array} \tag{2}$$

where x_1 and x_2 are the two states of the system. Figures 1 and 2 illustrate the chaotic performance of the system when $\omega = 1$, $\gamma = 0.1$, $A = 10$, and using zero initial conditions for both x_1 and x_2.

For practical implementation of the proposed synchronization scheme, only x_1 is assumed available for both measurement and feedback. This will also ensure better utilization of the public communication channel. Because of the special structure of the Duffing oscillator, illustrated in Equation (2), using a single time series is not a limiting factor in the proposed design, as x_2 can be easily generated from x_1.

3. **Design of the Drive-Response System.** In practice, two identical chaotic systems can never produce the same output due to their sensitivity to initial conditions [43]. Thus,

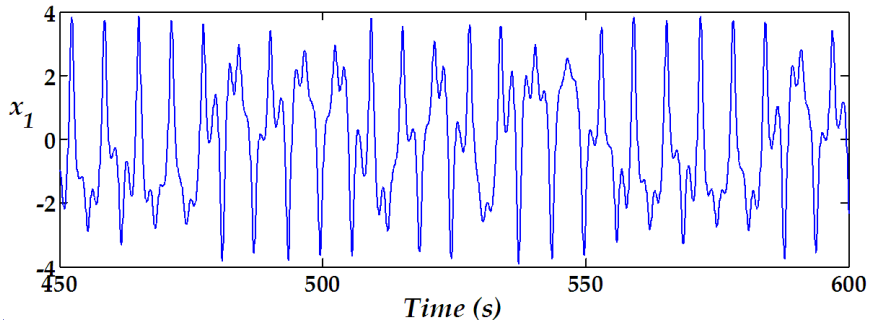


FIGURE 1. Chaotic response of the system for $\omega = 1$, $\gamma = 0.1$ and $A = 10$

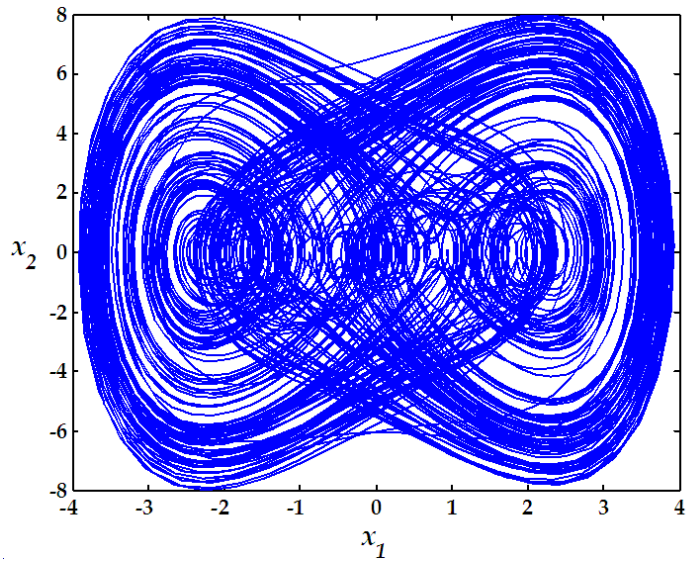


FIGURE 2. The phase plane of the system, illustrating the main chaotic attractor

synchronizing both the transmitter and the receiver should be carried out as a first step when designing chaos-based secure communication systems. When both the transmitter and the receiver have identical structure, a one-way coupling process can be implemented such that the receiver, driven by the transmitter, would follow the transmitter. This drive-response mechanism has a structure that is quite similar to state observers, where the observation errors are forced to zero via forcing the Lyapunov exponents of the receiver to be negative. Depending on the availability of transmitter states, both full and reduced order observation can be utilized.

Identifying unknown/uncertain parameters of the chaotic system is usually achieved via building parameters update laws for which the degree of complexity 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. Different techniques were reported in the literature that rely, some way or another, on the use of local Lyapunov functions to establish the stability and convergence of the parameters identification system [44].

Assuming that both γ and A are unknown and that only the time series for x_1 is available for measurement, the following dynamics for the response system can be introduced:

$$\begin{aligned}
\dot{\hat{x}}_1 &= \hat{x}_2 - \mu_1(\hat{x}_1 - x_1) \\
\dot{\hat{x}}_2 &= -\hat{\gamma}\hat{x}_2 + x_1 - x_1^3 + \hat{A}\cos\omega t - \mu_2(\hat{x}_1 - x_1) \\
\dot{\hat{\gamma}} &= f_\gamma(x_1, \hat{x}_1, \hat{x}_2, t) \\
\dot{\hat{A}} &= f_A(x_1, \hat{x}_1, \hat{x}_2, t)
\end{aligned} \tag{3}$$

where μ_1 and μ_2 are the feedback gains of the introduced controllers, and both f_γ and f_A are nonlinear parameter update laws for γ and A respectively. The response system is shown to have a structure that is quite similar to the drive system, given by Equation (2), except for augmenting two control signals, in the state equations of the observed states, as well as having two parameter update laws. The goal is to guarantee that the controllers are noninvasive and that the parameter update laws will provide unbiased estimates for both γ and A. If this goal is achieved, the synchronization process is successful and both the drive system (transmitter) and the response system (receiver) will have identical responses, regardless of the mismatch in the initial conditions of their states and parameters. In addition, in order to have a satisfactory performance, there should be a way to maximize the convergence rate of the parameters update laws and to reduce the time needed to achieve synchronization between the transmitter and the receiver. This should be the role of both μ_1 and μ_2, and any additional control parameters, if needed. To start the design process, the following error functions for both the states and the parameters are introduced:

$$e_1 = \hat{x}_1 - x_1,\ e_2 = \hat{x}_2 - x_2,\ e_\gamma = \hat{\gamma} - \gamma,\ e_A = \hat{A} - A \tag{4}$$

from which Equation (5) can be deduced:

$$\dot{e}_1 = e_2 - u_1,\ \dot{e}_2 = -\hat{\gamma}\hat{x}_2 + \gamma x_2 + e_A\cos\omega t - u_2,\ \dot{e}_\gamma = \dot{\hat{\gamma}},\ \dot{e}_A = \dot{\hat{A}} \tag{5}$$

where $u_1 = \mu_1 e_1$ and $u_2 = \mu_2 e_2$ are assumed to be the controllers. Now, the following simple Lyapunov function is introduced:

$$L = 0.5(k_1 e_1^2 + k_2 e_2^2 + k_\gamma e_\gamma^2 + k_A e_A^2) \tag{6}$$

where k_1, k_2, k_γ, and k_A are positive constants that can be used as *auxiliary* tuning gains for designing both the parameters update laws and the feedback gains of the controller.

Differentiating Equation (6) results in:

$$\begin{aligned}
\dot{L} &= k_1 e_1 \dot{e}_1 + k_2 e_2 \dot{e}_2 + k_\gamma e_\gamma \dot{e}_\gamma + k_A e_A \dot{e}_A \\
&= k_1(e_1 e_2 - \mu_1 e_1^2) + k_2(-\hat{\gamma}\hat{x}_2 e_2 + \gamma x_2 e_2 + e_A e_2 \cos\omega t - \mu_2 e_1 e_2) \\
&\quad + k_\gamma e_\gamma \dot{\hat{\gamma}} + k_A e_A \dot{\hat{A}} \\
&= -\mu_1 k_1 e_1^2 + e_1 e_2(k_1 - \mu_2 k_2) - k_2\left[(\hat{\gamma}\hat{x}_2 e_2 - \gamma \hat{x}_2 e_2) + (\gamma \hat{x}_2 e_2 - \gamma x_2 e_2)\right] \\
&\quad + k_2 e_A e_2 \cos\omega t + k_\gamma e_\gamma \dot{\hat{\gamma}} + k_A e_A \dot{\hat{A}} \\
&= -\mu_1 k_1 e_1^2 + e_1 e_2(k_1 - \mu_2 k_2) - \gamma k_2 e_2^2 - k_2 \hat{x}_2 e_2 e_\gamma + k_2 e_A e_2 \cos\omega t \\
&\quad + k_\gamma e_\gamma \dot{\hat{\gamma}} + k_A e_A \dot{\hat{A}} \\
&= -\left[\mu_1 k_1 e_1^2 - e_1 e_2(k_1 - \mu_2 k_2) + \gamma k_2 e_2^2\right] + e_\gamma(k_\gamma \dot{\hat{\gamma}} - k_2 \hat{x}_2 e_2) \\
&\quad + e_A(k_A \dot{\hat{A}} + k_2 e_2 \cos\omega t)
\end{aligned} \tag{7}$$

which can be simplified via the following choice of the parameters update laws:

$$\begin{aligned}
\dot{\hat{\gamma}} &= f_\gamma(x_1, \hat{x}_1, \hat{x}_2, t) = k_2 \hat{x}_2(\hat{x}_2 - \dot{x}_1)/k_\gamma \\
\dot{\hat{A}} &= f_A(x_1, \hat{x}_1, \hat{x}_2, t) = -k_2(\hat{x}_2 - \dot{x}_1)\cos\omega t/k_A
\end{aligned} \tag{8}$$

where it is seen that k_2 can be absorbed in both k_γ and k_A , which are used as control gains to adjust the speed of convergence of the parameters update laws. Thus, without loss of generality, assuming $k_2 = 1$ can further simplify the design process. Equation (7) now reduces to:

$$\dot{L} = -\left[\mu_1 k_1 e_1^2 - e_1 e_2(k_1 - \mu_2 k_2) + \gamma k_2 e_2^2\right] \tag{9}$$

There exist a wide range of values for the control parameters μ_1 and μ_2 such that Equation (9) can be made negative definite; thus, ensuring asymptotic stability of the receiver dynamics. This adds more versatility to the tuning process that is required during the design of the control part in Equation (3). One possible choice is forcing Equation (9) to represent a perfect square function; thus, solving for μ_1 in terms of μ_2 results in:

$$\mu_1 > \frac{(k_1 - \mu_2 k_2)^2}{4 k_1 k_2 \gamma_{\min}} \Rightarrow \dot{L} \leq -\left(\sqrt{\mu_1 k_1} e_1 \pm \sqrt{\gamma k_2} e_2\right)^2 \tag{10}$$

where $\gamma_{\min}$ is the minimum expected value of γ.

To illustrate the performance of the proposed technique, the following gains were chosen throughout the paper: $k_1 = 12.5$, $k_2 = 1$, $\mu_1 = 5$, $\mu_2 = 10$, $k_\gamma = 10$, and $k_A = 0.25$. These specific values were chosen to satisfy the constraint given in Equation (10), assuming $\gamma_{\min} = 0.05$, and to ensure fast convergence of the parameter update laws without overdriving the control signals. The initial values for x_1, x_2, $\hat{x}_1$, $\hat{x}_2$, $\hat{\gamma}$, and $\hat{A}$ were assumed 0, 0 , 1, 1, 0, and 0 respectively. Figure 3 shows the observation errors for the system states, x_1 and x_2 in (a) and (b) respectively, illustrating identical synchronization between the transmitter and the receiver with a settling time that is almost equivalent to the period of the forcing excitation. The performance of the estimated parameters is shown in Figure 4, illustrating the very important result of having unbiased values. This will prove crucial, when proposing the novel secure communication technique, in Section 4. Despite the coupling between synchronization and parameters estimation, the estimated parameters settled down almost immediately after synchronization is achieved.

Figure 5 shows the control signals used to implement the proposed system. Both control signals are noninvasive as the observation error for x_1 decays to zero. The maximum control effort should be taken into consideration when choosing both μ_1 and μ_2 to meet

any real-time constraints when realizing the proposed system in either analog or digital hardware. Introducing any additional nonlinearity caused by saturation of the control signal can drive the system into instability as Equations (8)-(10) will be no longer valid. The Lyapunov function, L, and its derivative, given by Equations (9) and (10) are shown in Figure 6.

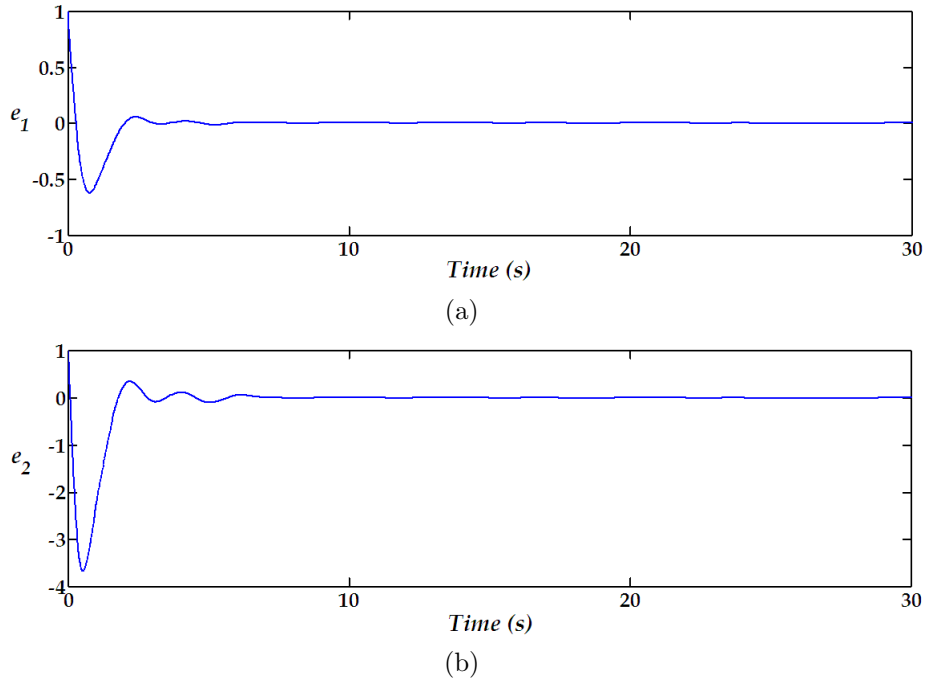


FIGURE 3. The synchronization errors for x_1 and x_2, in (a) in (b) respectively

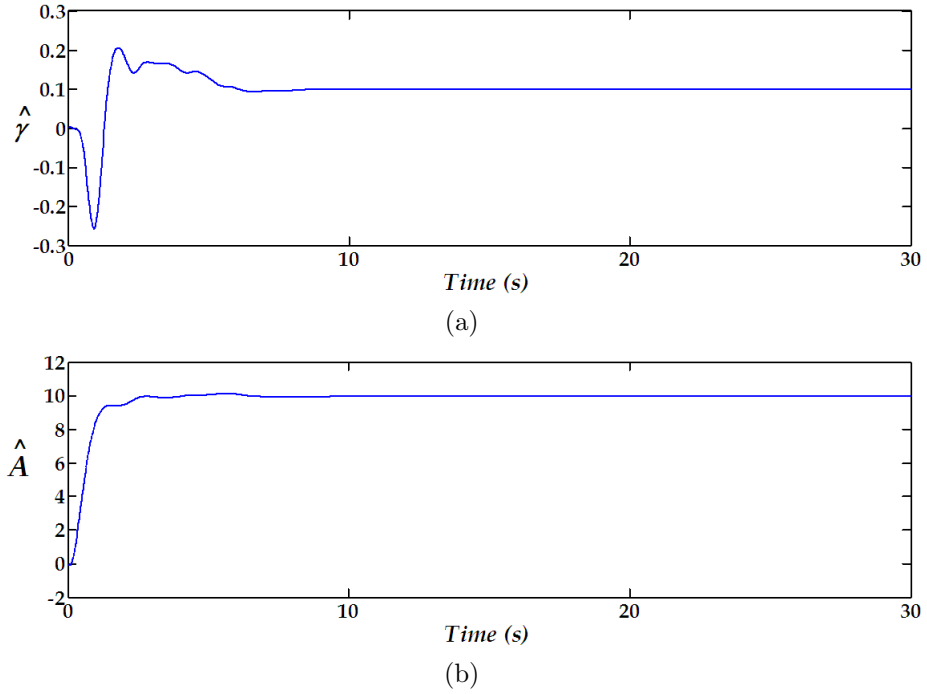


FIGURE 4. Unbiased estimates of the parameters γ and A, in (a) and (b) respectively

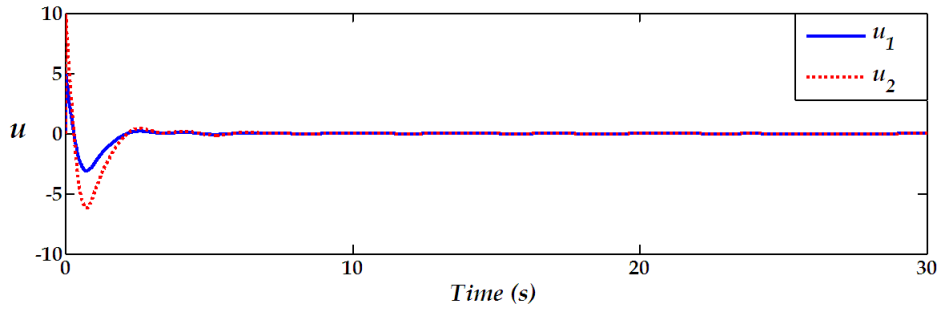


FIGURE 5. The noninvasive control signal

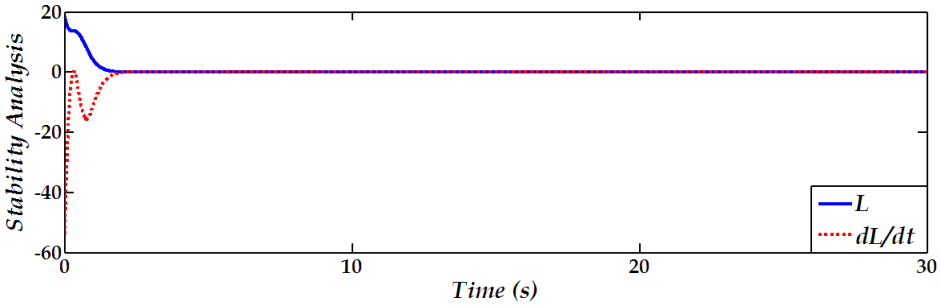


FIGURE 6. Stability analysis of the proposed system

The control signals, used in Equation (3), require access to $\hat{x}_1$ in order to construct e_1. Thus, it was required to use a full state observer to build the response system. Examining Equation (9) shows that setting k_1, μ_1, and μ_2 to zero, regardless of the value of k_2, can greatly simplify the design process as there are fewer gains to tune. This simplicity resulting from using a reduced-order state observer will be on the expense of having less control on the convergence rate of the synchronization errors and increasing the coupling effects in Equation (3).

4. **The Proposed Secure Communication System.** The nominal frequency of the chaotic Duffing oscillator is governed by its external excitation. The simulation results of the drive-response system, designed in the previous section, show that synchronization, as well as parameters estimation, are achieved within a time frame that is proportional to the nominal frequency of the original Duffing oscillator. To accommodate the transmission of signals with different nominal frequencies and bandwidths, the following modified version of the original chaotic Duffing oscillator is used:

$$\begin{aligned}
&\frac{1}{T}\dot{x}_1 = x_2 \\
&\frac{1}{T}\dot{x}_2 = -\gamma x_2 + x_1 - x_1^3 + A\cos\omega\frac{t}{T} \\
&\frac{1}{T}\dot{\hat{x}}_1 = \hat{x}_2 - \mu_1(\hat{x}_1 - x_1) \\
&\frac{1}{T}\dot{\hat{x}}_2 = -\hat{\gamma}\hat{x}_2 + x_1 - x_1^3 + \hat{A}\cos\omega\frac{t}{T} - \mu_2(\hat{x}_1 - x_1) \\
&\frac{1}{T}\dot{\hat{\gamma}} = k_2\hat{x}_2\left(\hat{x}_2 - \frac{1}{T}\dot{x}_1\right)/k_\gamma \\
&\frac{1}{T}\dot{\hat{A}} = -k_2\left(\hat{x}_2 - \frac{1}{T}\dot{x}_1\right)\cos\omega t/k_A
\end{aligned} \tag{11}$$

where T is a time scaling factor that is used to adjust the fundamental period of the chaotic attractor of the original Duffing oscillator. Assuming the existence of different sets of values, for the Duffing oscillator parameters, that can generate chaos, as illustrated by the dotted region in Figure 7, four different points can be chosen such that chaotic performance is maintained for a given range of the system parameters. The two different sets for both γ and A corresponding to $\{0.1, 10\}$ and $\{0.05, 5\}$ satisfy such requirement. This was verified via inspecting the phase plane of each sub-system, in addition to calculating its corresponding Lyapunov exponents.

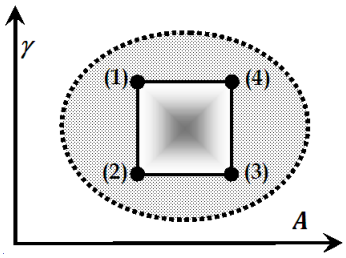


FIGURE 7. Regions of the chosen chaotic attractors

The dual property of the XOR function made it a typical candidate for performing simple cryptography for digital communication. A secret message can be XORed with a cipher at the transmitter (TX) to produce an encrypted signal. At the receiver side (RX), decryption can be easily performed via XORing the received signal with the same cipher. However, breaking the security of such systems, even for long ciphers, is a very simple process using current technology. In this section, a novel cryptography-based secure communication system is proposed such that two ciphers are used in the encryption process. The following functions are introduced at TX:

$$\begin{aligned} \gamma &= 0.05[1 + P(t)] \\ Q(t) &= P(t) \oplus m(t) \\ A &= 5.0[1 + Q(t)] \end{aligned} \tag{12}$$

where $m(t)$ is the secret message, $P(t)$ is the first cipher that is only known to the sender, and $Q(t)$ is generated via XORing both $P(t)$ and $m(t)$. Both $P(t)$ and $Q(t)$ are used to alternate the values of both γ and A between the two chosen sets that correspond to *four* different chaotic attractors. Assuming that only x_1 is available for transmission in the public channel, and using the procedure outlined in Section 3, the recipient can synchronize RX with TX and estimate both the values of $P(t)$ and $Q(t)$ to reconstruct the original message, using Equation (13):

$$\begin{aligned} \hat{P}(t) &= 20\hat{\gamma}_{ss} - 1 \\ \hat{Q}(t) &= 0.2\hat{A}_{ss} - 1 \\ \hat{m}(t) &= \hat{P}(t) \oplus \hat{Q}(t) \end{aligned} \tag{13}$$

where the subscript "*ss*" stands for steady state. Thus, allowing for a short delay such that the parameters update laws settle down to their final values, after achieving synchronization, is required in order not to introduce wrong patterns for the reconstructed bits (binary values). Consequently, the pulse width for each bit should be much more than the settling time of the parameter update laws. Efficient utilization of the public communication channel is assured because the transmitted signal, x_1, is the only required signal to establish both synchronization and encryption. Traditional CSK algorithms alternate

between only two chaotic attractors, which make them vulnerable to return-map attacks [11]. The proposed technique does not suffer from this deficiency as illustrated in Figure 8 as the attacker cannot find two distinct trajectories for the two binary states of the signal; instead, a diffused pattern is obtained.

To exemplify the proposed technique, the transmission of $m =$ 'Z', corresponding to an ASCII code of 90, using $P = 200$ and consequently $Q = 146$, is illustrated. Based on Equation (11), the time scaling factor, T, is set to 1000, and the pulse width for each transmitted bit is set to 40 ms, which is about four times the settling time of both the synchronization and parameter identification processes, shown in Figures 3 and 4. This allows enough time for the transient response to die out; hence, ensuring a satisfactory performance.

Figure 9 shows the identification of both γ and A, in (a) and (b) respectively, governed by Equations (11)-(13). The response of the parameter update law for γ is shown to exhibit large overshoot due to using $k_\gamma = 10$. Decreasing the value of k_γ was found to increase the settling time for $\hat{\gamma}$, while having minor effect of the overshoot. This

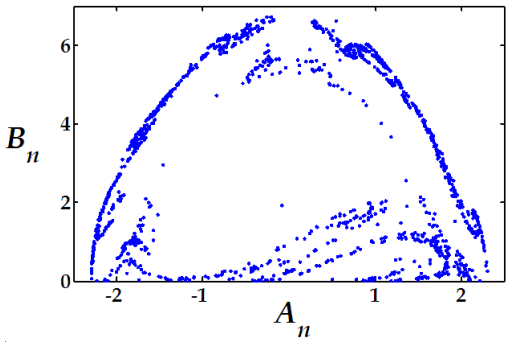
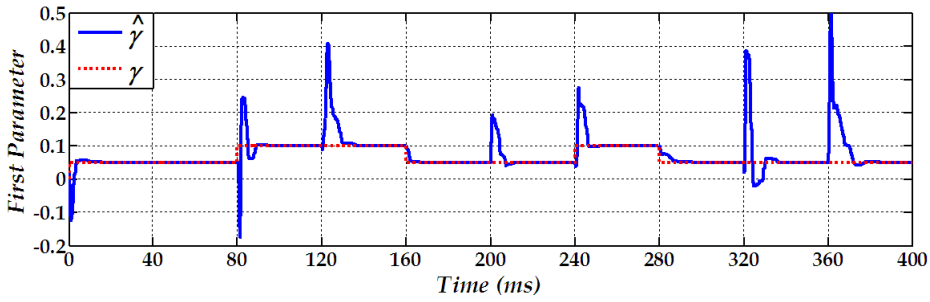
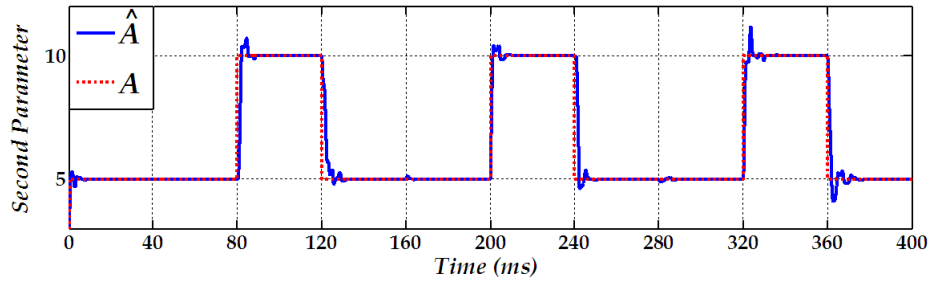


FIGURE 8. The return map of the proposed system



(a)



(b)

FIGURE 9. Performance of the parameters update laws

behaviour is due to the nonlinear structure of the Duffing oscillator and the three-way coupling between the synchronization mechanism, the parameter identification, and the control signals u_1 and u_2.

Figure 10 shows the reconstruction of P, Q, and m in (a), (b), and (c) respectively, using the same control parameters and initial conditions in Section 3. A delay time of 20 ms was used for each bit.

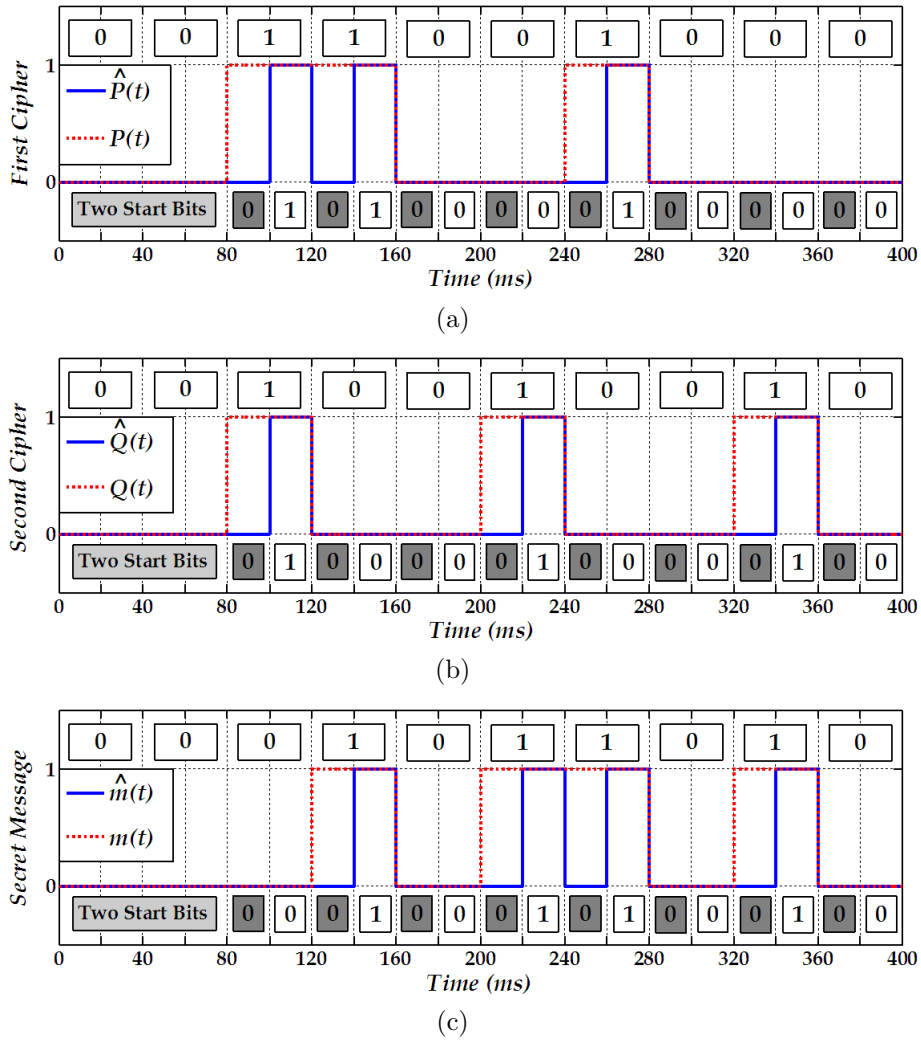


FIGURE 10. Reconstructing the original secret message

Examining Figure 10 shows that each original bit occupies 40 ms. The reconstructed signals are obtained via masking each bit of the response of Figure 9 after rescaling it using Equation (13) with 2 bits, each having 20 ms pulse width. The most significant bit of the 2-bit mask is 0, while the least significant bit is equal to the steady state value of the cipher to be identified. Digitally ORing the two bits of the mask will result in the correct bit pattern for the reconstructed ciphers, and consequently the reconstructed secret message. This simple process is easy to implement and avoids introducing any additional delays caused by utilizing low pass filters and any glitches caused by the improper use of thresholders. The proposed technique allows inserting any number of start and/or stop bits. Two start bits and zero stop bits were used in running the simulation in Figure 10.

5. **Discussion.** The dynamics of the Duffing oscillator provide a rich environment for employing chaos in constructing secure communication systems. It is a typical example of nonautonomous systems that need to be excited by an external signal to produce chaos, in contrast to autonomous chaotic systems such as the Lorenz system. Its simple second order structure makes it easier to perform synchronization and parameters estimation, compared with autonomous systems that are at least third order, or fourth order, in the hyperchaotic case. It was demonstrated that using Lyapunov-based control methods, the system states and parameters could be identified using a single time series that corresponds to x_1. In this paper, the full-order state observer was used. However, the reduced version of the state observer could have been used as well, for which there is no guarantee that e_1, will decay to zero, and consequently no control signals can be used. This should not be considered as a deficiency as it is only required to force e_2 to zero to observe x_2, since observing x_1 is not required.

To ensure causality of the proposed design, meeting hardware constraints and maintaining real-time compatibility, certain rules should apply when tuning the control parameters of the proposed system. Proper values for the control gains should be chosen to ensure that the parameters update laws will settle down within, at most, 50% of the time period of the digital pulse that represents the binary sequence of $m(t)$. The value of the time scaling factor, T, should be chosen to ensure that the chaotic system is faster than $m(t)$, i.e., the fundamental period of the chaotic attractor is much smaller than that of the transmitted message. Only time scaling was done in this paper; however, magnitude scaling to meet the maximum control effort, could have been done as well. The existence of the external excitation forcing function caused the system to be persistently excited. This condition allowed the response system to arrive at the correct, unbiased, values of the unknown system parameters, while achieving synchronization. Although it was required to find the optimum values for six control gains, the tuning effort was found to be moderate. Only linear feedback control was used in the design to simplify the analysis, although it was possible to add other forms of *useful* nonlinearities to improve the transient performance.

The proposed CSK method is considered novel as the system states were allowed to alternate among four chaotic attractors, and not between just two. This means that the proposed design is immune to return map attacks. The simple cryptography, based on the digital XOR function, was extended to include the two parameters of the transmitter. This proved to be robust, yet simple to implement. Other, more complicated, digital functions could have been used to perform the encryption, at the expense of increasing the decryption effort, e.g., $P(t)$, instead of being constant, can be made a function of other ciphers that are only known to both the sender and the recipient. The rate at which the two parameters of the system are allowed to change is comparable to that of the bit rate of the secret message to be transmitted; thus, their power spectra are overlapping in the frequency domain and there is no way to only extract the secret message from the encrypted time series, x_1, using filtration technique. This is an added advantage to the proposed design.

The decay rate of the error signals for both synchronization and parameters estimation is demonstrated to be very fast and is considered superior, when compared with the work done in [1-3,6-8,25-27]. This was achieved via simple tuning of the introduced control parameters. In addition, the simple, but robust, XOR-based cryptography method is another advantage of the proposed system when compared with other cryptography-based techniques that were reported in [5,10]. Moreover, the proposed system relies on using identical synchronization, which makes the decryption function a simple dual for the encryption function; thus, simplifying the design while ensuring robustness. This is an

added advantage when compared with other methods that rely on using multiple chaotic systems, e.g., a Logistics Map, a 2-D Baker Map, and a 4-D hyperchaotic Map. The design effort, in this paper, in terms of mathematical computations and order of the augmented system is minimum and can be easily implemented in both analog and digital hardware. Compared with other nonlinear techniques, the proposed system is superior in terms of accuracy, speed of convergence, and the number of parameters to be tuned. The effect of noise is shown to be minimum due to the masking process, illustrated in Figure 10. Compared with the work done in [45], the effectiveness of the proposed system in handling digital signals is obvious, as simple signal preprocessing step that includes low-pass filtering and thresholding can cause any transients or unwanted artifacts in Figure 9 to be eliminated.

Although only digital signals were considered to exemplify the proposed secure communication system, other varieties could have been used to transmit analog signals. This can be achieved via changing the scheme used for both the encryption and decryption functions. Moreover, the proposed technique is not restricted to only ASCII-based text, and can be applied to securely transmit audio signals, images and video streams, with minimum impact on the design effort, via performing a preprocessing step to convert the multi-dimensional spatiotemporal information into a one-dimension vector, and reversing this step during the decryption process at the receiver side.

Acknowledgment. This work was supported by Kuwait University, Research Grant No. [SP04/09].

REFERENCES

[1] L. Pecora and T. Carroll, Synchronization in chaotic systems, *Physical Review Letters*, vol.64, no.8, pp.821-825, 1990.

[2] T. Yang, A survey of chaotic secure communication systems, *Computational Cognition*, vol.2, no.2, pp.81-130, 2004.

[3] L. Pecora and T. Carroll, Driving systems with chaotic signals, *Physical Review A*, vol.44, no.4, pp.2374-2383, 1991.

[4] H. Dedieu, M. Kennedy and M. Hasler, Chaos shift keying – Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits, *IEEE Transactions on Circuits and Systems II*, vol.40, no.10, pp.634-642, 1993.

[5] Y. Shimizu, M. Miyazaki, F. Qian and H. Lee, A method of the secrecy communication using fuzzy and chaos, *International Journal of Innovative Computing, Information and Control*, vol.5, no.1, pp.97-108, 2009.

[6] X. Liu, W. Xiang and Y. Huangfu, An adaptive H-infinity synchronization scheme for secure communication, *ICIC Express Letters*, vol.5, no.12, pp.4541-4546, 2011.

[7] A. Skander, M. Nadjim and B. Malek, Synchronization chaotic communications with closed cryptographic systems, *ICIC Express Letters*, vol.2, no.3, pp.269-274, 2008.

[8] H. Chen, Q. Ding, L. Ding and X. Dong, Experimental study on secure communication of different scroll chaotic systems with identical structure, *ICIC Express Letters*, vol.2, no.2, pp.201-206, 2008.

[9] T. Yang, C. Wu and L. Chua, Cryptography based on chaotic systems, *IEEE Transactions on Circuits and Systems I*, vol.44, no.5, pp.469-472, 1997.

[10] E. Dong, Z. Chen, Z. Chen, H. Li and C. Xia, A novel image encryption algorithm based on double hyper-chaotic systems, *ICIC Express Letters*, vol.4, no.5(A), pp.1439-1444, 2010.

[11] A. Zaher and A. Abu-Rezq, On the designs of chaos-based secure communication systems, *Communications in Nonlinear Science and Numerical Simulations*, vol.16, no.9, pp.3721-3737, 2011.

[12] U. Parlitz, L. Chua, L. Kocarev, K. Halle and A. Shang. Transmission of digital signals by chaotic synchronization, *Bifurcation and Chaos*, vol.2, no.4, pp.973-977, 1992.

[13] A. Zaher, An improved chaos-based secure communication technique using a novel encryption function with an embedded cipher key, *Chaos, Solitons, and Fractals*, vol.42, no.5, pp.2804-2814, 2009.

[14] T. Yang, Recovery of digital signals from chaotic switching, *Circuit Theory and Applications*, vol.23, no.6, pp.611-615, 1995.

[15] M. Hasler and T. Schimming, Chaos communication over a noisy channel, *Bifurcation and Chaos*, vol.10, no.4, pp.719-735, 2000.
[16] T. Wren and T. Yang, Orthogonal chaotic vector shift keying in digital communications, *IET Communications*, vol.4, no.6, pp.739-753, 2010.
[17] Y. Xia, C. Tse and F. Lau, Performance of differential chaos-shift-keying digital communication systems over a multipath fading channel with delay spread, *IEEE Transactions on Circuits and Systems II*, vol.51, no.12, pp.680-684, 2004.
[18] H. Chen, J. Feng and C. Tse, A general noncoherent chaos-shift-keying communication system and its performance analysis, *Proc. of IEEE ISCAS, New Orleans, USA*, pp.2466-2469, 2007.
[19] T. Schimming and M. Hasler, Comparison of different chaos shift keying methods, *Proc. of ECCTD, Espoo, Finland*, pp.185-188, 2001.
[20] T. Heil, J. Mulet, I. Fischer, C. Mirasso, M. Peil, P. Colet and W. Elsäβer, On/Off phase shift keying for chaos-encrypted communication using external-cavity semiconductor lasers, *IEEE J. of Quantum Electronics*, vol.38, no.9, pp.1162-1170, 2002.
[21] Y. Xu, P. Charge and D. Prunaret, Chaotic cyclic attractors shift keying, *Proc. of IEEE ICNNSP*, Zhenjiang, China, pp.62-66, 2008.
[22] Z. Galias and G. Maggio, Quadrature chaos-shift keying: Theory and performance analysis, *IEEE Transactions on Circuits and Systems I*, vol.48, no.12, pp.1510-1519, 2001.
[23] J. Cuenot, L. Larger, J. Goedgebuer and W. Rhodes, Chaos shift keying with an optoelectronic encryption system using chaos in wavelength, *IEEE J. of Quantum Electronics*, vol.37, no.7, pp.849-855, 2001.
[24] R. Kharel, K. Busawon and Z. Ghassemlooy, Modified chaotic shift keying using indirect coupled chaotic synchronization for secure digital communication, *Proc. of the 3rd Chaotic Modeling and Simulation Int. Conference*, Chania, Crete, Greece, pp.207-214, 2010.
[25] J. Liu, J. Lu, Y. Shi, X. Li and Q. Tang, Different type of synchronization phenomena in unidirectional coupled unified chaotic systems, *International Journal of Innovative Computing, Information and Control*, vol.3, no.3, pp.697-708, 2007.
[26] J. Chu, Adaptive logic-based switched observer for chaotic synchronization, *ICIC Express Letters*, vol.5, no.12, pp.4351-4357, 2011.
[27] C. Chen and C. Jiang, Synchronization of spatiotemporal chaos via sliding mode control, *ICIC Express Letters*, vol.5, no.4(A), pp.1077-1082, 2011.
[28] A. Orue, G. Alvarez, G. Pastor, M. Romera, F. Montoya and S. Li, A new parameter determination method for some double-scroll chaotic systems and its applications to chaotic cryptanalysis, *Communications in Nonlinear Science and Numerical Simulations*, vol.15, no.11, pp.3471-3483, 2010.
[29] A. Zaher, Parameter identification technique for uncertain chaotic systems using state feedback and steady-state analysis, *Physical Review E*, vol.88, no.3, pp.036212:1-12, 2008.
[30] A. Zaher, Secure communications using duffing oscillators, *Proc. of IEEE ICSIPA, Kuala Lumpur, Malaysia*, pp.557-562, 2011.
[31] X. Wu, J. Cai and M. Wang, Global chaos synchronization of the parametrically excited duffing oscillators by linear state error feedback control, *Chaos, Solitons, and Fractals*, vol.36, no.1, pp.121-128, 2008.
[32] P. Han and C. Hou, Chaos control in periodically forced complex duffing system, *ICIC Express Letters*, vol.6, no.1, pp.255-260, 2012.
[33] I. Kovacic and M. Brennan, *The Duffing Equation: Nonlinear Oscillators and Their Behavior*, John Wiley and Sons, Ltd., 2011.
[34] A. Sharma, V. Patidar, G. Purohit and K. Sud, Effects on the bifurcation and chaos in forced Duffing oscillator due to nonlinear damping, *Communications in Nonlinear Science and Numerical Simulations*, vol.17, no.6, pp.2254-2269, 2012.
[35] Y. Ueda, Random phenomena resulting from nonlinearity in the system described by Duffing's equation, *Non-Linear Mechanics*, vol.20, no.5-6, pp.481-491, 1985.
[36] A. Luo and F. Min, The chaotic synchronization of a controlled pendulum with a periodically forced, damped Duffing oscillator, *Communications in Nonlinear Science and Numerical Simulations*, vol.16, no.12, pp.4704-4717, 2011.
[37] C. Feng, Y. Wu and W. Zhu, Response of duffing system with delayed feedback control under combined harmonic and real noise excitations, *Communications in Nonlinear Science and Numerical Simulations*, vol.14, no.6, pp.2542-2550, 2009.
[38] A. Harb, A. Zaher, A. Al-Qaisia and M. Zohdy, Recursive backstepping control of chaotic Duffing oscillators, *Chaos, Solitons and Fractals*, vol.34, no.2, pp.639-645, 2007.

[39] A. Al-Qaisia, A. Harb, A. Zaher and M. Zohdy, Robust estimation-based control of chaotic behavior in an oscillator with inertial and elastic symmetric nonlinearities, *Vibration and Control*, vol.9, no.6, pp.665-684, 2003.

[40] M. Akhmet and M. Fen, Chaotic period-doubling and OGY control for the forced duffing equation, *Communications in Nonlinear Science and Numerical Simulations*, vol.17, no.4, pp.1929-1946, 2012.

[41] E. Wembe and R. Yamapi, Chaos synchronization of resistively coupled Duffing systems: Numerical and experimental investigations, *Communications in Nonlinear Science and Numerical Simulations*, vol.14, no.4, pp.1439-1453, 2009.

[42] S. Kim, Bifurcation structure of the double-well Duffing oscillator, *Modern Physics*, vol.14, no.17, pp.1801-1813, 2000.

[43] S. Boccaletti, J. Kurths, G. Osipov, D. Valladares and C. Zhou, The synchronization of chaotic systems, *Physics Reports*, vol.366, no.1-2, pp.1-101, 2002.

[44] U. Parlitz, Estimating model parameters from time series by autosynchronization, *Physical Review Letters*, vol.76, no.8, pp.1232-1235, 1996.

[45] L. Xing, J. Liu, G. Shang and P. Dong, Noise-induced and noise-enhanced synchronization of Chen's chaotic systems, *ICIC Express Letters*, vol.4, no.2, pp.577-582, 2010.