International Journal of Innovative
Computing, Information and Control
Volume 11, Number 2, April 2015

 ISSN 1349-4198
pp. 569–585

SECURE COMMUNICATION BASED ON CHAOTIC SWITCHING AND RAPID SYNCHRONIZATION USING PARAMETER ADAPTATION

Ashok Kumar Mittal[1,2], Arti Dwivedi[1,2] and Suneet Dwivedi[2]

[1]Physics Department
[2]K Banerjee Centre of Atmospheric and Ocean Studies
University of Allahabad
Allahabad, UP 211002, India
suneetdwivedi@gmail.com

Received April 2013; revised October 2013

Abstract. *A version of the Complete Replacement (CR) coupling scheme is presented in which messages are coded by rapidly switching between several values of a parameter set and are recovered using adaptive synchronization technique in a time much smaller than the attractor time-scale. The advantages of this scheme for communication of digital messages are discussed.*
Keywords: Synchronization, Chaotic systems, Parameter adaptation, Chaos shift keying, Secure communication

1. **Introduction.** Pecora and Carroll [1,2] introduced the idea of synchronizing two chaotic systems. Since then many schemes have been proposed for chaos synchronization such as adaptive sliding mode control [3-5], impulsive synchronization [6,7], finite time stochastic synchronization [8], nonlinear control [9,10], directional synchronization [11,12], adaptive synchronization [13-18]. Several types of communication schemes that use synchronization of chaotic systems have been investigated. Some of the chaos-based communications schemes are additive masking, chaotic parameter modulation and chaotic shift keying. In these schemes there is a chaotic master or drive system, a communication channel and a slave or response system. One or more variables or functions of these variables act as carrier of the information message. This modified signal, which hides the information message, is transmitted via the communication channel to the receiver, driving it to achieve synchronization and recovery of the information signal.

In chaotic signal masking [19-21] the message is simply added to the chaotic signal and transmitted to the receiver. In this method, the message is required to be much weaker than the chaotic carrier. The recovered signal is sensitive to channel noises and parameter mismatches [22].

In chaotic modulation [19,23-25] the information message modifies the transmitter system, usually by modulating one or more parameters. At the receiver's end, by means of synchronization, the receiver can regenerate the corresponding unperturbed chaotic signal and recover the information message by comparing the received perturbed signal with the unperturbed signal.

Chaos Shift Keying (CSK) [26-29] is well suited for communication of digital messages. In early CSK schemes, the sender and the recipient used identical chaotic systems $\dot{u} = f(u, p)$ and $\dot{u}' = f(u', p)$ respectively. Here u and u' denote the set of drive and response variables respectively, and p is the set of parameters (assumed identical for the two systems). In the absence of coupling the two systems evolve independently due to

differences in initial conditions. However, if a signal $s(u)$ from the transmitter system drives the receiver system, it is possible to synchronize the two systems. For example, the systems $\dot{u} = f(u, p)$ and $\dot{u'} = f(u', p) + s(u') - s(u)$ can be made to synchronize in synchronization time, T_s, so that $u' - u$ is negligible for $t > T_s$. The recipient can confirm this synchronization by comparing $s(u)$ and $s(u')$ after time T_s. To communicate a binary message, the parameters of the transmitter system are switched between two values p_0 and p_1. These values represent the symbols '0' and '1' of the binary message. Each value is held constant for the bit duration time, T_d, before switching to a new value depending upon the next symbol of the message. In the receiver system the parameters remain fixed at the value p_0. If $T_d > T_s$, the recipient can decode each bit of the transmitted message by determining whether the two systems synchronized during the corresponding bit duration time T_d. If the systems synchronize, the transmitted bit is '0'; otherwise, it is '1'. For this message communication scheme to work, the recipient must know the structure of the transmitter system described by the function f, the parameters p_0, the signal function s and the bit duration time T_d. This communication scheme will be secure only if an intruder who intercepts the transmitted signal cannot decode the message without knowledge of f, p_0, s and T_d.

Zhou and Lai [30] and Abarbanel et al. [31] showed that an intruder, who knows the structure of the transmitter system, can determine its parameters, severely compromising the security of the communication scheme. Further, even the structure of the transmitter is not needed for an intruder to decode a message, as the message can be decoded by identifying some distinguishing property of the two attractors corresponding to the two parameters p_0 and p_1. However, if the bit duration time is not large enough, during each occurrence of a bit, the transmitted signal will not contain enough information about the attractor for an intruder to discover a one-to-one correspondence between the bit values and the attractors. This suggests that the bit duration time should be made much smaller than the typical oscillation time T_c of the chaotic oscillator in order to frustrate such intruder attacks. However, for synchronization based decoding schemes, the bit duration time must be more than synchronization time because a bit cannot be decoded without synchronization. It follows that the communication system should be so designed that $T_d \cong T_s < T_c$. Table 1 shows the values of T_d, T_s and T_c used in different studies. It is evident from the table that no study has used the design goal inferred above for enhancing security, and indicating the innovative nature of this suggestion.

We achieve the desired rapid synchronization using the technique of adaptive synchronization [40-43]. This technique assumes that the receiver does not know one or more parameters of the driving system. The response system is augmented with equations governing the adaptation of unknown parameters. The synchronization error equations also get augmented to include the synchronization errors in the unknown parameters. If the null vector is a stable equilibrium point of these error equations, all the variables, as well as the parameters, of the drive and response systems synchronize. In this way, the adaptive synchronization technique can be used for determining unknown parameters of a system from knowledge of some of the system variables.

Adaptive synchronization of chaotic systems provides an efficient mechanism for communication of secure messages [32,33,44-46]. A digital message is encoded in the parameters of the drive system. The parameter values of the response system synchronize to the parameter values of the drive and the digital message may be decoded at the receiving end. A distinguishing feature of this approach is that the parameters can be identified by a bona-fide recipient without having to identify the corresponding attractors. This allows parameter identification time, and therefore the bit duration time, to be much smaller than what will be needed by an intruder for attractor identification. However, as

TABLE 1. Synchronization time, switching time, and average time period in different studies

S. No.	Ref. No.	Synchronization time	Switching time	Average time period	Scheme
1	[26]	2	4	0.4 (Chua system)	Chaos-Shift Keying Scheme or chaotic switching
2	[32]	2	4	0.6 (Lorenz system)	Adaptive chaotic parameter modulation
3	[33]	3	5	0.6 (Lorenz system)	Adaptive chaotic parameter modulation
4	[34]	85	100	6 (Rossler System)	Chaotic Adaptive parameter modulation
5	[35]	3	5	0.4 (Chua System)	Chaos-Shift Keying
6	[36]	0.18×10^{-4}	0.5×10^{-3}	0.6×10^{-5} (Lorenz System)	Chaos-Shift Keying
7	[20]	0.4×10^{-1}	0.5×10^{-1}	0.2×10^{-3} (Lorenz System)	Chaotic masking
8	[37]	1.5	2.5	0.8 (Unified chaotic system)	Chaotic parameter modulation
9	[38]	4	5	0.7 (Unified Chaotic system)	Chaos-Shift
10	[39]	Not given	20	2.5 (Chua system)	Hamiltonian approach for synchronization

is evident from Table 1, this possibility has not been exploited. In this paper we exploit this possibility and show how to make the bit duration time smaller than the typical oscillation time thereby enhancing the communication security as explained earlier.

We illustrate our approach by applying it to a slightly modified technique of synchronization introduced by Pecora et al. [47] called the Complete Replacement technique. Pecora et al. [47] divided an autonomous n-dimensional dynamical system u into two subsystems v and w, of dimensions m and $(n-m)$ respectively. They considered the system $u = \{v, w\}$ as a drive system, with the sub-system v driving a response system $u' = \{v, w'\}$ in which w' is governed by the same equation as w, but with different initial conditions. In the response system u', the v' variables are completely replaced by the v variables of the drive. The two systems u and u' would synchronize only if all the Lyapunov exponents of the w subsystem are negative.

We choose the drive system u in such a way that the variables of the subsystem v can be divided into two subsets, v_1 and v_2, and the w subsystem depends only on the variables of v_1 and w, but not of v_2. Then parameter synchronization and message communication can be made to work without having to transmit the variables in v_2 to the response system $u' = \{v, w'\}$. We illustrate this with the help of a modified Lorenz system as the drive u.

In general, the synchronization errors in the variables and the parameters are governed by equations whose coefficients depend on the variables that move on the attractor. These errors can be shown to vanish asymptotically by constructing a suitable Lyapunov function. The synchronization time scale is determined by the Lyapunov exponents, which depend on the entire attractor over which the variables move. This makes the adaptive parameters fluctuate chaotically on attractor time-scales before synchronization, so that the synchronization time-scale is necessarily more than the attractor time-scale. To overcome this problem we choose the system u, the subsystem w, and the adaptation law for

the unknown parameters in such a way that the evolution of the error system is governed by an appropriate system of linear equations with constant coefficients.

For this it is necessary that the unknown parameters appear as additive constants in the subsystem w. The subsystem w is chosen so that the synchronization errors are governed by linear equations with constant coefficients. The receiver is assumed to have knowledge of the instantaneous values of the needed drive variables, but not the forcing parameters used in the drive system. The response system assumes arbitrary initial values for these parameters and subjects them to adaptation laws such that the rate of change in the parameters depends linearly on the synchronization errors in the variables of the subsystem w. Then synchronization error of the augmented system of the variables and the unknown parameters is governed by the eigenvalues of a constant matrix. The synchronization time scale T_s is independent of the time scale T_c of the chaotic drive system. It can be made much smaller than T_c by appropriate choice of parameters.

This cannot be done when the coefficients of the error equations depend on the variables. In this case the errors decrease if all the Lyapunov exponents are negative. However, the Lyapunov exponents only determine the average rate of error growth; the local error growth can fluctuate chaotically as the coefficients in the error equation traverse different parts of the chaotic attractor. There will be regions where the local Lyapunov exponent is positive. It follows that the synchronization time T_s cannot be much smaller than chaotic oscillation time T_c, independent of initial conditions. Therefore, T_d has to be larger than T_c. This makes available a large part of an attractor during each bit duration time allowing an intruder to use return map and attractor reconstruction techniques to decode the message. Moreover, because of the chaotic fluctuations in the values of the response parameter, the separation between the values of the parameters that can be used for coding has to be relatively large. As a consequence, fewer parameter values can be used for coding which means lower information transfer rates. Moreover, fewer parameter values, and greater separation between them, make it easier for an intruder to decode the message using a return map technique or some other technique to separate the attractors for different values of the parameter.

The approach presented in this paper overcomes these shortcomings as is illustrated with the example of a modified forced Lorenz system. Lower synchronization time allows faster transmission rate. More number of parameter values that can be used for coding allow increased information transfer rate. More parameter values, less separation between them and availability of only small portions of an attractor for each parameter value, make it very difficult for an intruder to separate the attractors corresponding to the different values of the parameter.

The scheme presented is analytically very simple. It is quite flexible and can easily incorporate additional features of security. The coding scheme and the switching time, instead of being fixed, can depend on a shared secret key. The output of the drive system itself can be subjected to a transformation based on a shared secret key before transmission. The secret keys can be shared either by private meeting or through public key encryption.

In Section 2, we describe in detail a modified version of the CR synchronization scheme. The transmitting system, the receiving system and the parameter adaptation laws are so chosen that the augmented error matrix is a suitable constant. In Section 3, we show how this scheme can be used for secure communication of digital messages by modulation of a forcing parameter. Section 4 discusses in detail the security aspects of the scheme. Conclusions are given in Section 5.

2. **Synchronization with Parameter Adaptation.** Pecora and Carroll [1,2] introduced the idea of synchronizing two chaotic systems. They divided an autonomous n-dimensional dynamical system

$$\dot{u} = f(u) \tag{1}$$

into two subsystems v and w, of dimensions m and $(n-m)$ respectively, governed by equations of the form

$$\dot{v} = g(v, w), \quad \dot{w} = h(v, w) \tag{2}$$

They created a new subsystem w' identical to the subsystem w, substituted the variables v for the corresponding variables v' in the function h above and augmented Equation (2) with this new subsystem to obtain

$$\dot{v} = g(v, w), \quad \dot{w} = h(v, w), \quad \dot{w}' = h(v, w') \tag{3}$$

In effect they considered a drive system $u = \{v, w\}$ and a response system $u' = \{v', w'\}$ in which the v' variables are completely replaced by the v variables of the drive. This technique of synchronization has been called the Complete Replacement (CR) technique [47]. The two systems u and u' would synchronize only if all the Lyapunov exponents of the w subsystem are negative.

In general the equation governing $e_w = w' - w$ satisfies

$$\dot{e}_w = M e_w \tag{4}$$

In all the well-known examples of the CR method the matrix M depends on the chaotic variables v, w and w' and therefore varies with time. Synchronization takes place only if the null solution is a globally stable solution of Equation (4).

Adaptive synchronization techniques [41-44] assume that the receiver does not know one or more parameters of the driving system. The response system is augmented with equations governing the adaptation of unknown parameters. The synchronization error equations also get augmented to include the synchronization errors in the unknown parameters. The augmented error equations can be expressed as

$$\begin{aligned} \dot{e}_w &= M e_w + N e_p \\ \dot{e}_p &= Q e_w \end{aligned}$$

These equations can be expressed as

$$\dot{e}_a = L_a e_a \tag{5}$$

where $e_a = \begin{bmatrix} e_w \\ e_p \end{bmatrix}$ and $L_a = \begin{bmatrix} M & N \\ Q & 0 \end{bmatrix}$.

In general the coefficients of the augmented error matrix depend on the variables and parameters of the drive and the response systems. However, the parameter adaptation laws cannot depend on the parameter values, as these values are not available to the receiver. It is for this reason that the parameter error evolution equation does not depend on the parameter errors and only depends on the synchronization error of the variables. If the null vector is a stable equilibrium point of (5), the drive and response systems synchronize. In this way, the adaptive synchronization technique can be used for determining unknown parameters of a system from knowledge of some of the system variables.

The main design goal of this paper is to achieve rapid synchronization in a time much smaller than the chaotic oscillation time scale. A simple approach, towards realizing this goal using parameter adaptation, is to choose the transmitter system and the parameter adaptive receiver system in such a way that the resulting augmented error matrix L_a in Equation (5) is a constant matrix.

In this paper, we choose the system u so that it can be decomposed into the sub-systems v and w as in (3) but with the additional requirement that the function h in Equation

(3) depends only on a proper sub-set v_1 of the variables in sub-system v so that (3) is replaced by

$$\dot{v} = g(v, w), \quad \dot{w} = h(v, w), \quad \dot{w}' = \tilde{h}(v_1, w') \tag{6}$$

where $h(v_1, w)$ and $\tilde{h}(v_1, w)$ are given by

$$\begin{aligned} h(v_1, w) &= H(v_1) + Lw + IF \\ \tilde{h}(v_1, w) &= H(v_1) + Lw' + IF' + \tilde{L}(w' - w) \end{aligned} \tag{7}$$

Here H is an arbitrary function, L and $\tilde{L}$ are constant matrices, F and F' are constant column vectors and I is the identity matrix of appropriate dimensions.

The vector F is not known to the recipient. In the receiving system the vector F' is given an arbitrary initial value and it evolves according to the parameter adaptation rule

$$\dot{F}' = Q(w' - w)$$

where Q is a constant matrix. Then the augmented error equations will be governed by Equation (5) with

$$L_a = \begin{bmatrix} L + \tilde{L} & I \\ Q & 0 \end{bmatrix} \tag{8}$$

If all the eigenvalues of L_a have negative real part, the drive and response systems synchronize. The matrix L_a may be so chosen that the synchronization time is less than the chaotic oscillation time of the drive variables.

In [1,2] the Lorenz system with parameters $\sigma = 10$, $b = 8/3$, $r = 60$ was taken as the u system. It was found that all the conditional Lyapunov exponents were negative for two choices of the w system: (i) $w = \{y, z\}$ and (ii) $w = \{x, z\}$.

We illustrate our approach by considering the u system as a modified forced Lorenz system governed by

$$\begin{aligned} \dot{x} &= \sigma(y - x) \\ \dot{y} &= rx - zx - y \\ \dot{z} &= x^2 - bz + F \end{aligned} \tag{9}$$

where F is a constant. The response system is governed by

$$\dot{z}' = x^2 - bz' + F' + (b - p)(z' - z) \tag{10}$$

where p is a constant whose value is to be chosen. This system satisfies the requirements (6), (7) and (8) with $v = \{x, y\}$, $v_1 = \{x\}$, $v_2 = \{y\}$, $w = \{z\}$, $g = \begin{bmatrix} \sigma(y - x) \\ rx - zx - y \end{bmatrix}$, $H = x^2$, $L = -b$ and $\tilde{L} = b - p$.

The value of parameter F is not known to the response system. The parameter F' of the response system is assigned an arbitrary initial value and is subjected to a parameter adaptation law

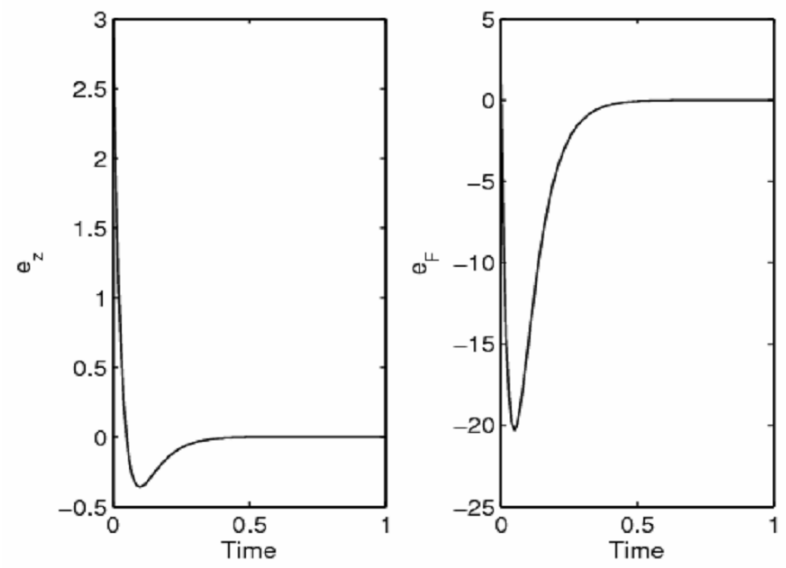
$$\dot{F}' = -s(z' - z) \tag{11}$$

where s is a constant whose value is to be chosen. Thus the synchronization error, $e_z = z' - z$ is governed by the equations

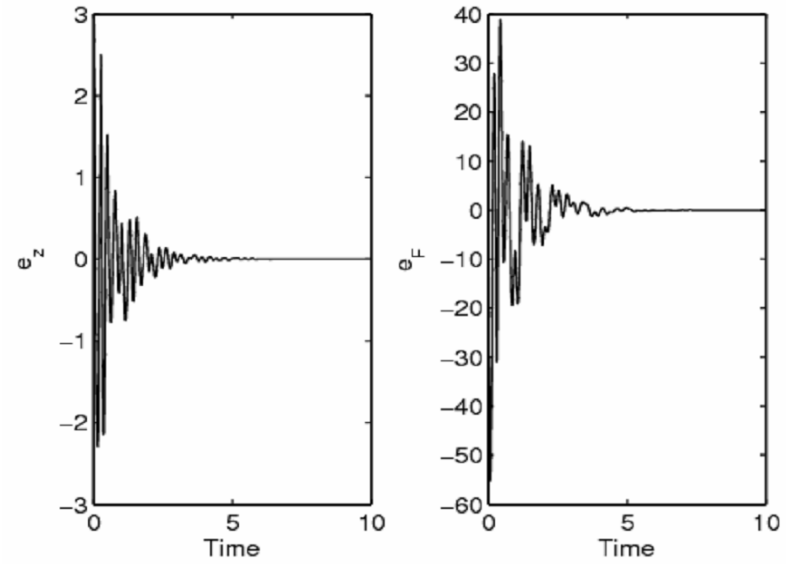
$$\begin{aligned} \dot{e}_z &= -pe_z + e_F \\ \dot{e}_F &= -se_z \end{aligned} \tag{12}$$

where $e_F = F' - F$. The synchronization time scale T_s, which is governed by the eigenvalues of (12), is independent of the oscillation time scale T_c of the chaotic drive system, so it can be made smaller than T_c by appropriate choice of parameters.

Figure 1(a) shows that the response system synchronizes with the drive system and the parameter F' converges rapidly to F. This figure was obtained for the parameter of the drive system $F = 1$. The initial values of the variables (x, y, z) were taken to be



(a)



(b)

FIGURE 1. Synchronization errors as a function of time for the augmented error system governed by: (a) Equation (12) having constant coefficients and (b) Equation (13) having chaotic variables as coefficients

$(1, -1, 0.01)$. For the response system, the initial values of the parameters (z', F') were taken to be $(3, 2)$, whereas $p = 40$ and $s = 400$ were chosen.

The advantages of our approach can be seen by comparing it with a similar scheme, but for which all the coefficients of the error equations are not constant. For this purpose, we consider the x-coupling synchronization scheme of Pecora and Carroll [1,2], augmented with a parameter adaptation law identical to that in Equation (12) so that the drive system is governed by

$$\begin{aligned} \dot{x} &= \sigma(y - x) \\ \dot{y} &= -xz + rx - y \\ \dot{z} &= xy - bz + F \end{aligned} \tag{13}$$

and the corresponding response system with parameter adaptation law is governed as

$$\begin{aligned} \dot{y} &= -xz' + rx - y' \\ \dot{z} &= xy' - bz' + F' \\ \dot{F}' &= -s(z' - z) \end{aligned} \tag{14}$$

In this case, the synchronization error equations would be given by

$$\begin{aligned} \dot{e}_y &= -e_y - xe_z \\ \dot{e}_z &= xe_y - be_z + e_F \\ \dot{e}_F &= -400e_z \end{aligned} \tag{15}$$

Figure 1(b) shows that the synchronization errors eventually vanish because the Lyapunov exponents are negative. However, the synchronization time is much larger than Figure 1(a). Also the synchronization errors fluctuate chaotically before convergence. The basic reason for this is that the error Equation (15) explicitly depends on the chaotic x variable whereas the error Equation (12) has constant coefficients.

Comparison of Figures 1(a) and 1(b) clearly shows that our approach leads to rapid and smooth synchronization. This property can be exploited for faster and more secure communication as discussed below.

3. **Secure Communication of Digital Messages.** Several studies [44,45] have shown how the adaptive synchronization of chaotic systems can be used for communication of secure messages. One or more parameters of the transmitter are modulated by the digital message to be communicated. The parameter values of the receiver synchronize to the parameter values of the transmitter and the digital message may be recovered.

We assume that a digital message is composed from a set of 10 symbols denoted by $\{0, 1, \ldots, 9\}$. Corresponding to the digit k, the value of F is taken to be $F_k = 0.1(k + 1)$. The system (9) remains chaotic for this range of F. In order to communicate the digital symbol k, F is held at a constant value F_k for a time T_d. If the switching time T_d is greater than the synchronization time T_s, the value of F' will converge sufficiently close to F_k so that the digital symbol of the message can be deciphered. After the switching time interval T_d, the value of F is changed to a value corresponding to the next digital symbol in the message. In this way the receiver can decipher the digital message communicated using $k_n = 10\tilde{F}'_n - 1$, where $\tilde{F}'_n$ is the value of F' at time nT_d rounded to the nearest integer.

Large initial error in the z variable causes a large and rapid overshoot in F'. To overcome this problem, the operation of the adaptation law is suspended for time T_d before transmission of the message. During this period the value of F is kept constant at pre-decided value known to the receiver. For this duration, the parameter F' of the response system is also kept constant. This leads to a reduction in the synchronization error of the z variable at time $t = 0$, when the transmission of the message is started. Figure 2 shows the value of F as a function of time modulated by the digital message {9 4 5 0 3 9 3 3 9 0}.

In Figure 3 we show how the receiver can recover the message by observing F' at integral multiples of switching time T_d. Figure 3(a) corresponds to the choice $w = \{z\}$ using our approach whereas Figure 3(b) corresponds to the choice $w = \{y, z\}$ of [1,2] with identical parameter adaptation law. The horizontal line before time $t = 0$ corresponds to the pre-agreed value $F = F' = 0.1$ to prevent overshooting as explained earlier.

Figure 3(a) shows that the receiver parameter converges rapidly and smoothly to a value very close to the transmitter value. The bit duration time is chosen sufficiently large so that the bit value can be identified unambiguously in this time. There is no need for separate confirmation of synchronization, and it is built into the choice of bit

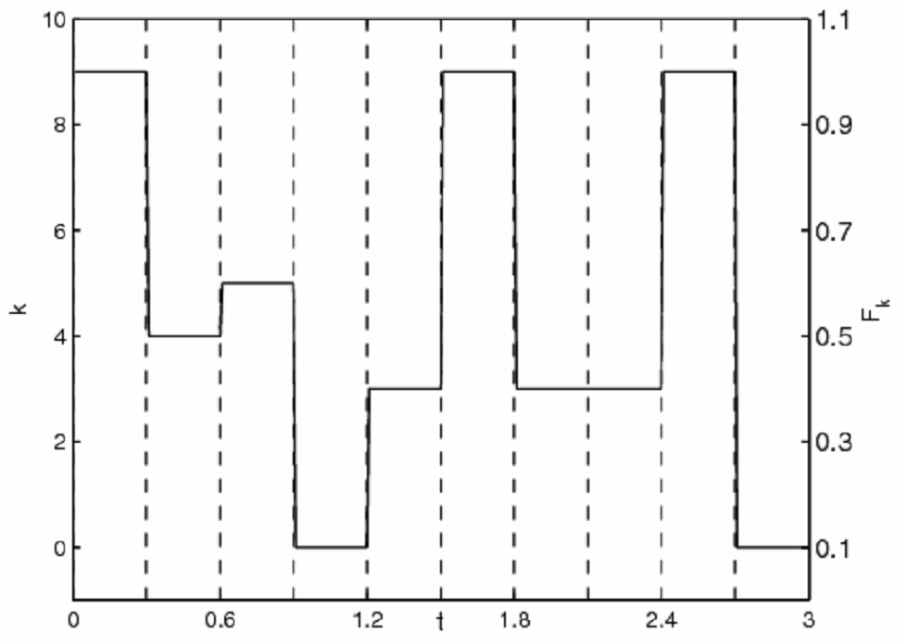
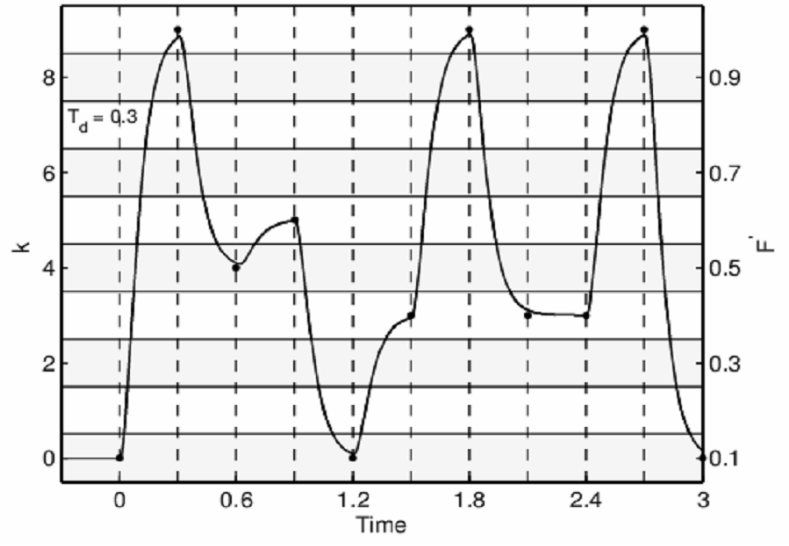


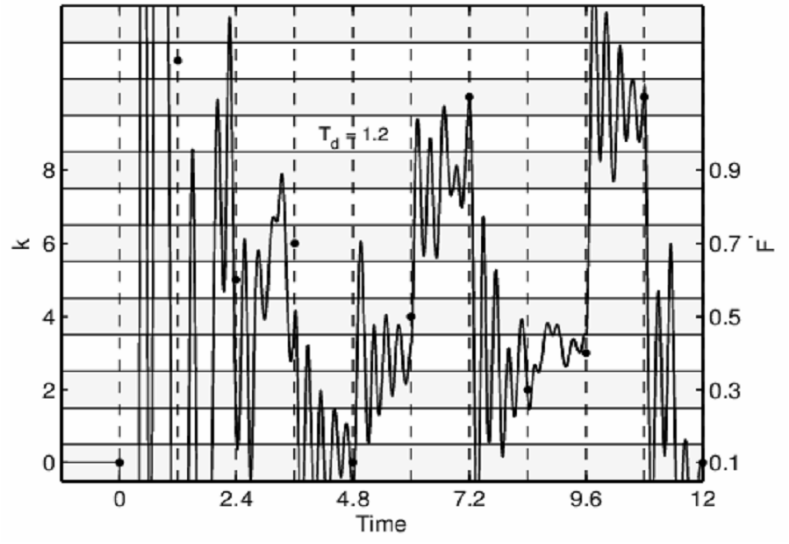
FIGURE 2. The forcing parameter F modulated by the digital message {9 4 5 0 3 9 3 3 9 0}

duration time. The receiver will give an acceptable output (all parameter values close to the agreed parameter values at the agreed time intervals) only to those input signals which emerge from a transmitting system with the correct w-subsystem, the correct choice of switching parameter values and the correct switching time intervals. This rapid and smooth convergence will not, in general, be possible for nonlinear parameter modulation as that would make the coefficients of the augmented error equations depend on the chaotic variables. This in turn would make the synchronization time more than the chaotic oscillation time, limit the speed and reduce the security.

Figure 3(a) shows that a switching time as small as 0.3 can be used for communicating a message composed from ten distinct symbols. The switching time is less than the average chaotic oscillation time, which is about 0.5. The switching time can be made as small as desired, by suitably choosing p and s; it is limited only by hardware considerations. Therefore, each symbol in the message will be represented by a small fragment of the attractor corresponding to the symbol; different occurrences of the same symbol will be represented by different portions of the attractor. Moreover, a large number of closely spaced parameters can represent several symbols. All these features make it very difficult for an intruder to identify the different attractors. All cryptanalysis techniques against CSK type schemes assume that the message is coded as a binary, the bit duration time is sufficiently long and the parameter values represent the two bits sufficiently separated that a recipient can distinguish between the two attractors. These techniques find some property that can help distinguish the two attractors without knowledge of the corresponding parameters [48-50]. As the switching time decreases, it becomes more difficult for an intruder to decode the message using the return map technique [48]. Yang et al. [50] have also made the observation that if the switching frequency between two parameter sets is too high and comparable to the frequency of the attractor, then it is difficult to recover the message signal, but the performance of chaos shift keying may degrade dramatically if the switching frequency is too high. We have shown in this paper that parameter adaptation can make it possible to decrease the switching time even below the



(a)



(b)

FIGURE 3. Recovery of the digital message {9 4 5 0 3 9 3 3 9 0} at the receiving end from the values of the response parameter F' observed at integral multiples of the switching time for the choice (a) $w = \{z\}$ of this paper (b) $w = \{y, z\}$ of references [1,2]

attractor oscillation time, without degrading the performance of the CSK scheme. It is also not necessary to communicate all the variables of the drive system, so full information about the drive system is not available to an intruder even for a short time.

On the other hand, in the case of Figure 3(b) even for a relatively large switching time of 1.2, the message cannot be decoded correctly. Moreover, the parameter F' oscillates chaotically, undergoing large variations in small time intervals around the time values at which it is measured. Thus it is necessary to make measurements of F' at very precise moments. Extremely small errors in the measurement moment would lead to decoding errors. Also in any physical implementation, large rapid fluctuations of parameters are undesirable.

For simplicity of presentation, we have illustrated our approach using a simple example in which only one message is transmitted. This scheme can be used to transmit several messages in parallel by increasing the dimensionality of the w-subspace in Equation (2).

4. **Security Analysis.** Apart from increasing the communication speed, our approach leads to enhanced security because a very small part of the attractor is available to an intruder before the transmitter system shifts to another chaotic system. In this section we analyze in detail, the security features of our scheme.

Several studies have demonstrated the vulnerability of published secure communication schemes to intruder attacks. Alvarez and Li [51] have listed several suggestions that designers of chaotic communication schemes must keep in mind to ensure security of communication in conformity with the principles of modern cryptology.

In cryptology the message to be communicated is called plaintext. The encrypted message is called the ciphertext. A pair of algorithms that encrypt and decrypt the message is called the cipher. The detailed operation of the cipher is controlled by these algorithms, which depend on a secret key that is known only to the sender and the intended recipient. For digital communication via computers the key is typically a binary sequence of length N. An intruder needs to scan 2^N different keys in order to identify the secret key by a brute force technique. Clearly, a key must be at least so long that it makes brute force cracking approach unpractical. However, the larger the key lengths is, the slower are the encryption and decryption speeds. Thus security should be sought only to the extent needed. A communication scheme can be useful even if it is not perfectly secure against all possible attacks. Security is adequate if the cost of cracking the system is greater than the possible gain to an intruder.

Study of the methods by which an intruder can decrypt an intercepted message without having knowledge of the secret key is called cryptanalysis. An intruder may have access only to the ciphertext. The attacks on security, that such an intruder may make, are called ciphertext-only attacks. An intruder may also have access to some samples of plaintext along with the corresponding ciphertext. This can make the task of the intruder much easier. A possible attack with such additional information is called known-plaintext attack.

We make a security analysis of our communication scheme from the cryptology perspective presented above. In our scheme, the plaintext is first converted into a sequence of digits chosen from a set of p values. Each digit is represented by a distinct parameter value. This brings one layer of encryption and can be made as strong as desired. The ciphertext is the string of chaotic variables which is transmitted, with the parameter values of the chaotic transmitter system switched in correspondence with the digital plaintext.

In cryptology it is assumed that, for a fixed key, the ciphertext is a single-valued function of the plaintext. This is clear from the block diagram [51] in Figure 4. Figure 5 shows the manner in which our proposed scheme differs from the cryptologic scheme of Figure 4. In this case the ciphertext depends not only on the message x and the secret key k, but also on an additional handle l chosen from a set L, where l includes the function g and the initial values. Information about l is not transmitted to the recipient as it is not needed for decryption. The ability to alter the ciphertext for the same plaintext and the same key can help make an intruder's task more difficult without adding to the key transfer problem.

One of the desirable properties required of a cryptosystem is that of diffusion – small changes in either the plaintext or the key should lead to a big change in the ciphertext. For the scheme of this paper, ciphertext can change drastically even without any change in either the plaintext or the key. Thus our scheme satisfies the property of diffusion, *par*

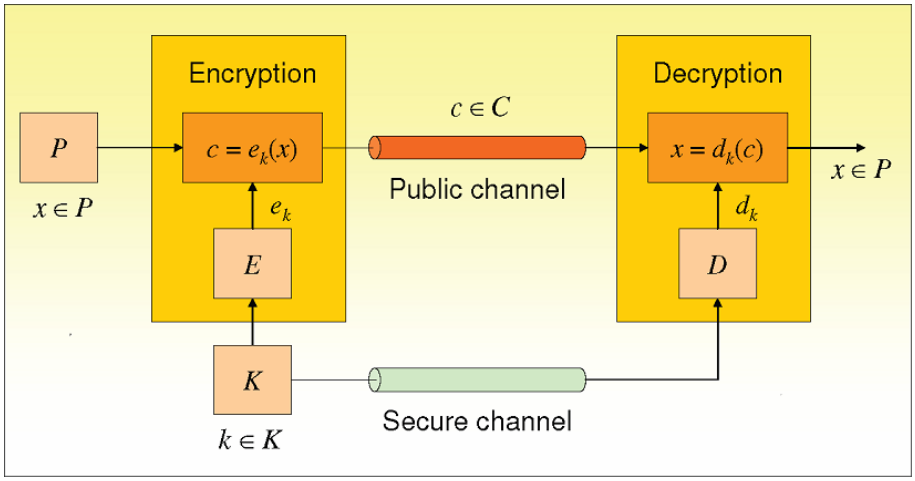


FIGURE 4. Block diagram of a standard cryptosystem [51]

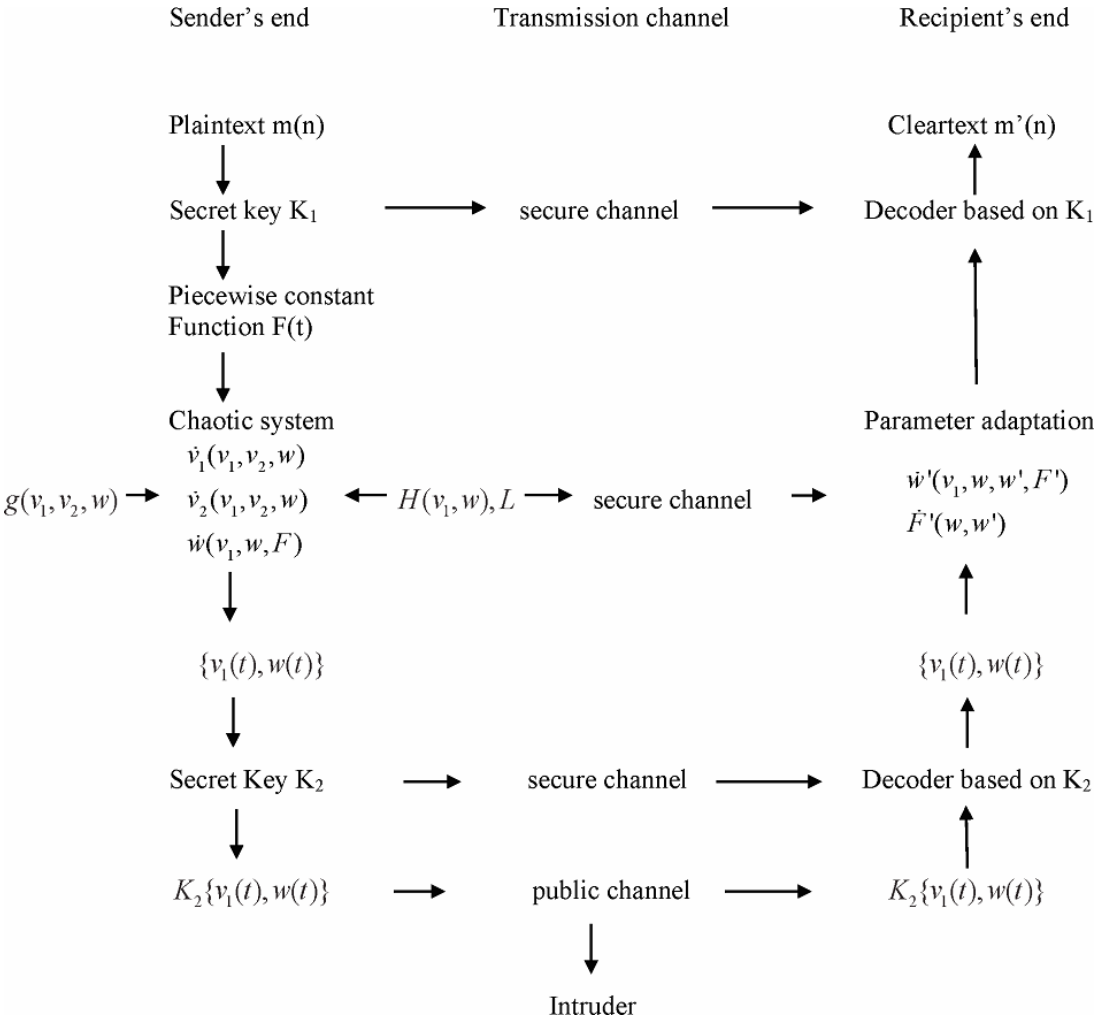


FIGURE 5. Block diagram of the scheme proposed in this paper

excellence. Available cryptanalytic techniques assume that a parameter is held constant long enough for an intruder to identify the attractor corresponding to that parameter. An intruder, who can do this, can replace the ciphertext by a sequence of attractor names.

Then the one-to-one correspondence between plaintext and ciphertext (for a fixed key) is restored and the security of the cryptosystem gets reduced to that of this correspondence.

Many studies that demonstrate the vulnerability of specific chaos-based coding-decoding schemes explicitly assume that the entire encrypting process is known to an intruder except the parameter values of the master chaotic system, thereby making these parameter values the secret key. This is called the Kerckhoffs' principle [52] or the Shannon maxim. However, any chaotic cryptosystem based on master-slave synchronization is quite weak if the secret key consists only of the parameter values of the drive system. Such a system is vulnerable to attack because of parameter adaptive techniques and the requirement of robustness with respect to small parameter mismatches. Security is greatly enhanced if the structure of the master chaotic system is made a part of the secret key – information available only to the sender and bona-fide recipient. We wish to argue that the Kerckhoffs' principle is not relevant for all applications; there is no application independent principle that can decide what should be regarded as a key and what should be regarded as public, what can be treated as secure and what cannot. Thus there is no compelling reason to regard the structure of the transmitting chaotic system and the details of the encoding process as public.

The secret key for the cryptosystem we propose consists of the following:

i. The function H and the matrix L in Equation (7).
ii. The set of parameter values used for chaotic switching in the transmitter system.
iii. Switching time.
iv. The algorithm K_1 used for converting a plaintext into a piecewise continuous function that describes the dependence of the switching parameters on time.
v. The algorithm K_2 used for scrambling the variables before transmitting them via an insecure channel.
vi. Parameter values of the header signals.

If required, each of the above can be made to fit a classical cryptology framework by suitably defining a key space from which these will be chosen. The net effect is that the key space is greatly enhanced and the difficulty of the intruder is greatly amplified.

A question can arise that if these secret keys can be communicated through secure channels, why cannot the messages also be sent through the same secure channels. Here we need to understand the nature of secret channels. One way of securing a secret channel is to meet privately and agree upon the secret keys. For many applications this may be quite feasible and practical. However, for applications in multiple-user open environment, the problem of secure key management becomes acute. In recent times, a way was found to make secure communication without the need for shared secure keys [53]. This mode of encryption is called public key encryption. In this mode the recipient creates a pair of keys, which are long strings of binary digits. It is easy to create such pairs, but given one member of a pair, it is computationally impossible with present technology to obtain the other member. It is also impossible to decipher any message without using both the keys. The recipient retains one of the keys as a secret key and transmits the other key, called a public key, to the transmitter over a public (insecure) channel. The transmitter can encrypt a message using this key and send it to the recipient. An intruder, who can obtain the encrypting key, cannot decipher the message without the secret key. Public key encryption obviously has its advantages. However, it is slow compared to encryption based on shared secret keys. For this reason, it is advantageous to have hybrid encryption systems, which combine the advantages of public key encryption and encryption based on shared secret keys. In such systems the secret keys are communicated through public key encryption, whereas the bulk communication relies on secret keys so communicated.

In CSK techniques which use synchronization without parameter adaptation, the switching time necessarily has to be long enough that the recipient can identify the shift in the attractor. The main point of our paper is that with parameter adaptation, this is no longer necessary. It is possible to design a receiver system based on parameter adaptation so that the recipient, who knows the structure of the encrypting scheme, can identify the parameters in a time much smaller than that is needed for identifying a shift in the chaotic attractor. As a consequence, the parameters of the transmitting system can be changed so rapidly that an intruder cannot identify switches in parameter values from the cipher-text.

Moreover, without parameter adaptation, the parameter values chosen for chaos shift keying cannot be very close, because the decryption has to be based on identification of attractor switching. With parameter adaptation, closer parameter values can be chosen for chaos shift keying because parameter identification in this case does not rely on identification of attractor switches.

Our scheme offers greatly enhanced security because: (i) the switching time (not publically announced), is much smaller than the chaotic oscillation time of the oscillator so that very few consecutive maxima or minima will correspond to the same attractor and (ii) a large number (unknown to an intruder) of closely spaced parameter values are used for encryption. In the absence of knowledge about the structure of the transmitting system including the number of equations governing the transmitting chaotic system, the switching time, the number of distinct symbols, the parameter values used for representing these symbols and the encrypting algorithm, there is no evident method by which an intruder can make a successful ciphertext attack or known-plaintext attack against the proposed scheme.

The problem for the intruder can be further magnified by increasing the dimensionality of the w-subspace so that several parameters can be made to change simultaneously. Under these circumstances, it is not easy to see how any cryptanalytic technique can reliably identify so many distinct patterns from return maps, when consecutive maxima and minima do not belong to the same parameter set.

Most chaotic communication systems rely on sending one signal to minimize the amount of information available to an eavesdropper. One might think that because the method proposed in this paper uses more than one signal, therefore, it makes far more information available to an eavesdropper making it much less secure. However, because the parameter sets are switched rapidly in the proposed method, the availability of more than one signal cannot help an intruder decode the message. On the other hand, when a parameter set is held constant for a long time, as is the case with most chaotic communication systems that transmit one signal, the time series of a single variable is sufficient for an intruder to identify distinct attractors or use attractor reconstruction for cryptanalysis.

In most chaotic communication systems, the modulation of a linear parameter, as is done in our approach, is avoided because of the possibility that if the additive parameter is periodically switched, it will cause a large peak at the switching frequency in the power spectrum of the transmitted signal. From this, an intruder can infer the switching rate of the information signal making the detection of the message much easier. This problem of large peak at switching frequency in the power spectrum can be overcome in several ways. (i) The switching time can be so chosen that the frequency peak lies within the broadband spectra of the chaotic system. Our approach allows the use of close values of parameters to represent different bits, so the amplitude of the peak can be made small enough that it does not stand out in the power spectra. (ii) The bit duration time need not be constant and may be varied according to some secret key shared with the *bona-fide* recipient. (iii) The synchronization rate is independent of the function g in Equation (6). The sender

can vary this function without interfering with parameter adaptation. In particular the value of σ in our illustration can be made time dependent. This will have the effect of creating peaks in the power spectra of the transmitted variables. In this way an intruder can be duped by a spurious message, whereas a *bona-fide* recipient can extract the correct message.

It is not our claim that the scheme is impervious to all possible attacks; only that it amplifies the task of an intruder by a significant factor. It would require a major cryptanalytic effort that may not be worth the effort in many applications.

5. **Conclusions.** In this paper we have presented an approach that uses a version of the complete replacement technique of synchronization along with parameter adaptation such that the synchronization error is governed by a system of linear equations with constant coefficients. We compared the synchronization achieved using our approach, in which the error equations have constant coefficients, with that achieved for a very similar system, but for which the error equations explicitly depend upon the chaotic variables. We have shown that our approach leads to faster and smoother synchronization.

This synchronization is used for communication of digital messages using parameter switching. We have illustrated how this approach allows smoother synchronization in a time smaller than the chaotic oscillation time scale. As a result, an intruder cannot identify the different values of the coding parameters using a return map technique or any other technique based on attractor identification. Moreover, our approach allows larger number of values of coding parameters with smaller separation between them, thus enabling even faster and more secure communication.

We have indicated how this approach can be used to create a strong cryptosystem. Full implementation details cannot be given because practical implementation requires consideration of several factors beyond the scope of this paper.

Most communication schemes make two tacit assumptions. The bit duration time has to be larger than the chaotic oscillation time and only one channel is to be used for transmission of signals. Such schemes suffer from limitation of communication speed and from possibility of cryptanalytic attack using return map like techniques. In this paper we have demonstrated a way around these problems by suggesting an approach based on shortening the synchronization time using parameter adaptation. This shortening comes at the cost of requiring more than one communication channels. However, because of rapid parameter switching, increase in communication channels does not lead to reduced security.

Acknowledgment. AD thanks DST and CSIR for providing fellowship. AKM and SD thank ISRO/NCAOR/DST for providing financial assistance in the form of research projects. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] L. M. Pecora and T. L. Carroll, Synchronization in chaotic systems, *Phys. Rev. Lett.*, vol.64, pp.821-825, 1990.

[2] L. M. Pecora and T. L. Carroll, Driving systems with chaotic signals, *Phys. Rev. A.,* vol.44, pp.2374-2384, 1991.

[3] H.-T. Yau, Y.-C. Pu and S. C. Li, Application of chaotic synchronization system to secure communication, *Information Technology and Control*, vol.41, pp.274-282, 2012.

[4] Z. Rabiei, G. B. Bidari and N. Pariz, Synchronization between two different chaotic systems using adaptive sliding mode control, *International Journal of Information and Electronics Engineering*, vol.3, pp.83-86, 2013.

[5] H.-C. Chen, B. Y. Liau and Y. Y. Hou, Hardware implementation of lorenz circuit systems for secure chaotic communication applications, *Sensors*, vol.13, pp.2494-2505, 2013.
[6] G. Feng and J. Cao, Master-slave synchronization of chaotic systems with a modified impulsive controller, *Advances in Difference Equations*, vol.24, pp.1-12, 2013.
[7] H. Zhang, X. Liu, X. Shen and J. Liu, Intermittent impulsive synchronization of hyperchaos with application to secure communication, *Asian Journal of Control*, vol.15, pp.1-14, 2013.
[8] R. Luo and Y. Wang, Finite time stochastic combination synchronization of three different chaotic systems and its application to secure communication, *Chaos*, vol.22, no.2, p.023109, 2012.
[9] A. A. M. Farghaly, Chaos synchronization of complex Rossler system, *Appl. Math. Inf. Sci.*, vol.7, pp.1415-1420, 2013.
[10] L. Liu, H. Song, J. Zhao and G. Wang, Fast synchronization of continuous chaotic system, *Journal of Information & Computational Science*, vol.10, pp.3087-3092, 2013.
[11] A. Sambas, M. Sanjaya and W. S. Halimatussadiyah, Unidirectional chaotic synchronization of Rossler circuit and its application to secure communication, *WSEAS Transactions on Systems*, vol.11, pp.506-515, 2012.
[12] A. Sambas, M. Sanjaya, M. Mamat and W. S. Halimatussadiyah, Design and analysis bidirectional chaotic synchronization of Rossler circuit and its application for secure communication, *Applied Mathematical Sciences*, vol.7, pp.11-21, 2013.
[13] T.-L. Liao and S. H. Tsai, Adaptive synchronization of chaotic systems and its applications to secure communication, *Chaos Solitons and Fractals*, vol.11, pp.1387-1396, 2012.
[14] M. Srivastava, S. K. Agrawal and V. Mishra, Adaptive synchronization between different chaotic systems with unknown parameters, *International Conference & Workshop on Advanced Computing*, 2013.
[15] C.-H. Yang, Symplectic synchronization of Lorenz-Stenflow system with uncertain chaotic parameters via adaptive control, *Hindawi Publishing Corporation Abstract and Applied Analysis*, vol.2013, pp.1-14, 2013.
[16] L. Ning, The adaptive output synchronization of different-order chaotic system, *Journal of Theoretical and Applied Information Technology*, vol.51, pp.442-446, 2013.
[17] B. Andrievsky, Information transmission based on adaptive synchronization of chaotic lorenz systems over digital communication channel, *Cybernetics and Physics*, vol.2, pp.10-14, 2013.
[18] N. Smaoui, A. Karouma and M. Zribi, Adaptive synchronization of hyperchaotic Chen systems with application to secure communication, *International Journal of Innovative Computing Information and Control*, vol.9, no.3, pp.1127-1144, 2013.
[19] K. M. Cuomo and A. V. Oppenheim, Circuit implementation of synchronized chaos with applications to communications, *Phys. Rev. Lett.*, vol.71, pp.65-68, 1993.
[20] K. M. Cuomo, A. V. Oppenheim and S. H. Strogatz, Synchronization of Lorenz based chaotic circuits with applications to communications, *IEEE T. Circuits Syst. – II*, vol.40, pp.626-633, 1993.
[21] T.-L. Liao and N.-S. Huang, An observer based approach for chaotic synchronization with application to secure communications, *IEEE T. Circuits Syst. – I*, vol.46, pp.1144-1150, 1999.
[22] T. Yang, A survey of chaotic secure communication systems, *Int. J. Comput. Cognition*, vol.2, pp.81-130, 2004.
[23] S. Bowong, F. M. M. Kakmeni and M. S. Siewev, Secure communication via parameter modulation in a class of chaotic systems, *Commun. Nonlinear Sci. Numer. Simulat.*, vol.12, no.3, pp.397-410, 2007.
[24] T. Yang, Secure communication via chaotic parameter modulation, *IEEE T. Circuits Syst. – I: Fundamental Theory and Applications*, vol.43, pp.817-819, 1996.
[25] C. W. Wu and L. O. Chua, A simple way to synchronize chaotic systems with applications to secure communication systems, *Int. J. Bifurcat. Chaos*, vol.3, pp.1619-1627, 1993.
[26] U. Parlitz, Transmission of digital signals by chaotic synchronization, *Int. J. Bifurcation and Chaos*, vol.2, pp.973-977, 1992.
[27] H. Dedieu, M. P. Kennedy and M. Hasler, Chaos shift keying, modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuit's, *IEEE Transactions on Circuits and Systems – II: Analog and Digital Signal Processing*, vol.40, pp.634-642, 1993.
[28] G. Kolumban, M. P. Kennedy and L. O. Chua, The role of synchronization in digital communications using chaos part II: Chaotic modulation and chaotic synchronization, *IEEE Transactions on Circuits and Sys. – I: Fundamental Theory and Applications*, vol.45, pp.1129-1140, 1998.
[29] M. P. Kennedy and G. Kolumban, Digital communications using chaos, *Signal Processing*, vol.80, pp.1307-1320, 2000.

[30] C. Zhou and C.-H. Lai, Decoding information by following parameter modulation with parameter adaptive control, *Phys. Rev. E.*, vol.59, pp.6629-6636, 1999.
[31] H. D. I. Abarbanel, D. R. Creveling and J. M. Jeanne, Estimation of parameters in nonlinear systems using balanced synchronization, *Phys. Rev. E.*, vol.77, pp.016208-1-14, 2008.
[32] C.-S. Zhou and T.-L. Chen, Transmitting multiple information signals by a single chaotic carrier, *Chin. Phys. Lett.*, vol.14, pp.161-164, 1997.
[33] M. Feki, An adaptive chaos synchronization scheme applied to secure communication, *Chaos, Solitons and Fractals,* vol.18, pp.141-148, 2003.
[34] G. J. Xing and D. B. Huang, Encoding-decoding message for secure communication based on adaptive chaos synchronization, *J. Shanghai Univ.*, vol.12, pp.400-404, 2008.
[35] W. Yua, J. Cao, J.-W. Wong and J. Lu, New communication schemes based on adaptive synchronization, *Chaos*, vol.17, pp.03311-4-13, 2007.
[36] I. A. Kamil and O. A. Fakolujo, Lorenz-based chaotic secure communication, *Ubiquitous Computing and Communication Journal*, vol.7, pp.1248-1254, 2012.
[37] C. Hua, B. Yang, G. Ouyang and X. Guan, A new chaotic secure communication scheme, *Phys. Lett. A.*, vol.342, pp.305-308, 2005.
[38] W. Xia and J. Cao, Adaptive synchronization of a switching system and its applications to secure communications, *Chaos*, vol.18, pp.023128-1-15, 2008.
[39] R. M. López-Gutiérrez, E. Rodríguez-Orozco, C. Cruz-Hernández, E. Inzunza-González, C. Posadas-Castillo, E. E. García-Guerrero and L. Cardoza-Avendaño, Secret communications using synchronized sixth-order Chua's Circuit, *World Academy of Science, Engineering and Technology*, vol.54, pp.608-613, 2009.
[40] U. Parlitz, Estimating model parameters from time series by autosynchronization, *Phys. Rev. Lett.*, vol.76, pp.1232-1235, 1996.
[41] T.-L. Liao, Adaptive synchronization of two Lorenz systems, *Chaos, Solitons & Fractals*, vol.9, pp.1555-1561, 1998.
[42] S. Chen and J. Lu, Parameter identification and synchronization of chaotic systems based upon adaptive control, *Phys. Lett. A.,* vol.299, pp.353-358, 2002.
[43] S. Chen, J. Hu, C. Wang and J. Lu, Adaptive synchronization of uncertain Rossler hyperchaotic system based on parameter identification, *Phys. Lett. A.*, vol.321, pp.50-55, 2004.
[44] B. Andrievsky, Adaptive synchronization methods for signal transmission on chaotic carrier, *Mathematics and Computers in Simulation*, vol.58, pp.285-293, 2002.
[45] I. Pehlivan and Y. Uyaroglu, Simplified chaotic diffusionless Lorenz attractor and its application to secure communication systems, *IET Commun.*, vol.1, pp.1015-1022, 2007.
[46] J. Xing and D. Huang, Encoding-decoding message for secure communication based on adaptive chaos synchronization, *J. Shanghai Univ.*, vol.12, pp.400-404, 2008.
[47] L. M. Pecora, T. L. Carroll, G. A. Johnson, D. J. Mar and J. F. Heagy, Fundamentals of synchronization in chaotic systems, concepts and applications, *Chaos*, vol.7, no.4, pp.520-543, 1997.
[48] G. Perez and H. A. Cerdeira, Extracting messages masked by chaos, *Phys. Rev. Lett.*, vol.74, pp.1970-1973, 1995.
[49] T. Yang, L. B. Yang and C. M. Yang, Breaking chaotic secure communication using a spectogram, *Phys. Lett. A*, vol.247, pp.105-111, 1998.
[50] T. Yang, L. B. Yang and C. M. Yang, Cryptanalysing chaotic secure communications using return maps, *Phys. Lett. A*, vol.245, pp.495-510, 1998.
[51] G. Alvarez and S. Li, Some basic cryptographic requirements for chaos based cryptosystem, *International Journal of Bifurcation and Chaos*, vol.16, no.8, pp.2129-2151, 2006.
[52] A. Kerckhoffs, La cryptographie militaire, *Journal Des Sciences Militaries* $1X$, vol.5, pp.161-191, 1883.
[53] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, vol.22, pp.644-654, 1976.