A New Chaotic Secure Communication System

Zhengguo Li, Kun Li, Changyun Wen, and Yeng Chai Soh

***Abstract*—This paper proposes a digital chaotic secure communication by introducing a concept of magnifying glass, which is used to enlarge and observe minor parameter mismatch so as to increase the sensitivity of the system. The encryption method is based on a one-time pad encryption scheme, where the random key sequence is replaced by a chaotic sequence generated via a Chua's circuit. In our system, we make use of an impulsive control strategy to synchronize two identical chaotic systems embedded in the encrypter and the decrypter, respectively. The lengths of impulsive intervals are piecewise constant and as a result, the security of the system is further improved. Moreover, with the given parameters of the chaotic system and the impulsive control law, an estimate of the synchronization time is derived. The proposed cryptosystem is shown to be very sensitive to parameter mismatch and hence the security of the chaotic secure communication system is greatly enhanced.**

***Index Terms*—Chua's circuit, impulsive control strategy, piecewise-constant impulsive intervals, secure communication system.**

I. Introduction

CHAOTIC circuits and their applications to secure communications have received a great deal of attention since Pecora and Carrol proposed a method to synchronize two identical chaotic systems [1], [22]. The main advantage of a chaotic secure communication system over conventional cryptosystems is that chaotic secure communication systems can often be realized as very simple circuits on a part of a chip [16]. The chaotic secure system can be used in applications that do not require a high level of information security such as remote keyless entry system, video phone, and wireless telephone [16].

Over the past decade, the chaos-based secure communications have updated their fourth generation [2]–[6], [8], [9], [18]. The continuous synchronization is adopted in the first three generations while the impulsive synchronization is used in the fourth generation. Less than 94 Hz of bandwidth is needed to transmit the synchronization signal for a third-order chaotic transmitter in the fourth generation while 30-kHz bandwidth needed for transmitting the synchronization signals in the other three generations [18]. Therefore, the efficiency of the bandwidth usage is improved greatly in the fourth generation. However, the attacks proposed in [10], [11] have shown that most of these methods are not secure or have a low security. It is thus desirable to improve the security of chaotic secure communication.

Paper approved by G.-S. Kuo, the Editor for Communications Architecture of the IEEE Communications Society. Manuscript received April 12, 2000; revised July 19, 2002 and December 23, 2002.

Z. G. Li is with Signal Processing Program; Laboratories for Information Technology, Singapore 119613 (e-mail: EZGLI@lit.org.sg).

K. Li, C. Y. Wen, and Y. C. Soh are with School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 (e-mail: ecywen@ntu.edu.sg; eycsoh@ntu.edu.sg).

Digital Object Identifier 10.1109/TCOMM.2003.815058

The primary aim of this paper is to increase the parameter sensitivity of chaotic synchronization systems so that it enhances the security level of the chaotic secure communication system. Specifically, we propose a digital chaotic secure communication system by introducing a concept of magnifying glass, which is used to enlarge and observe minor parameter mismatch to improve the sensitivity of cryptosystem. The impulsive control strategy proposed in [7], [8] is adopted to synchronize two identical chaotic systems embedded in the encoder and the decoder where the lengths of impulsive intervals are piecewise constant. With these piecewise-constant impulsive intervals, it will be very difficult for an intruder to find the synchronization impulse. The security of chaotic secure communication systems is further improved. To maintain the simplicity of the proposed system, the signal is packetized into packets with fixed size. The packet size is chosen to be the length of the first impulsive interval. The length of other impulsive interval is determined by the length of the first impulsive interval and the parameters of the circuit. Moreover, with the given parameters of chaotic system and the impulsive control law, we are able to give an estimate of the synchronization time required to synchronize the encrypter and decrypter. Since our chaotic secure communication system is based on impulsive synchronization, our system is less sensitive to channel noise than that based on continuous synchronization [18].

The rest of this paper is organized as follows. The digital chaotic secure communication system is proposed in Section II. In Section III, the design of impulsive controller and an estimation of the synchronization time are presented. Then, in Section IV, some experimental results are given to illustrate the effectiveness and efficiency of the proposed scheme. Finally, some concluding remarks are given in Section V.

II. Digital Chaotic Secure Communication Systems

In this section, we shall present a digital chaotic secure communication system that uses a magnifying glass to enlarge the effect of parameter mismatch and an impulsive control strategy [7], [8], [21] for the synchronization of chaotic circuits.

The proposed scheme is essentially a one-time pad [15] with the random signal replaced by a chaotic signal generated from a Chua's circuit. The system block diagram is shown in Fig. 1. The secure system has two major parts: encrypter and decrypter. The input of our system can be of all types of signals, which are first compressed. An interesting example is given in [17].

The encrypter consists of a Chua's circuit and a classical encryption function $e(\cdot)$. The decrypter is composed of an identical Chua's circuit, an impulsive controller and a corresponding decryption function $d(\cdot)$. The function of impulsive controller is to synchronize two Chua's circuits embedded in the encrypter and the decrypter. The key signal $k(t)$ is a combination of all

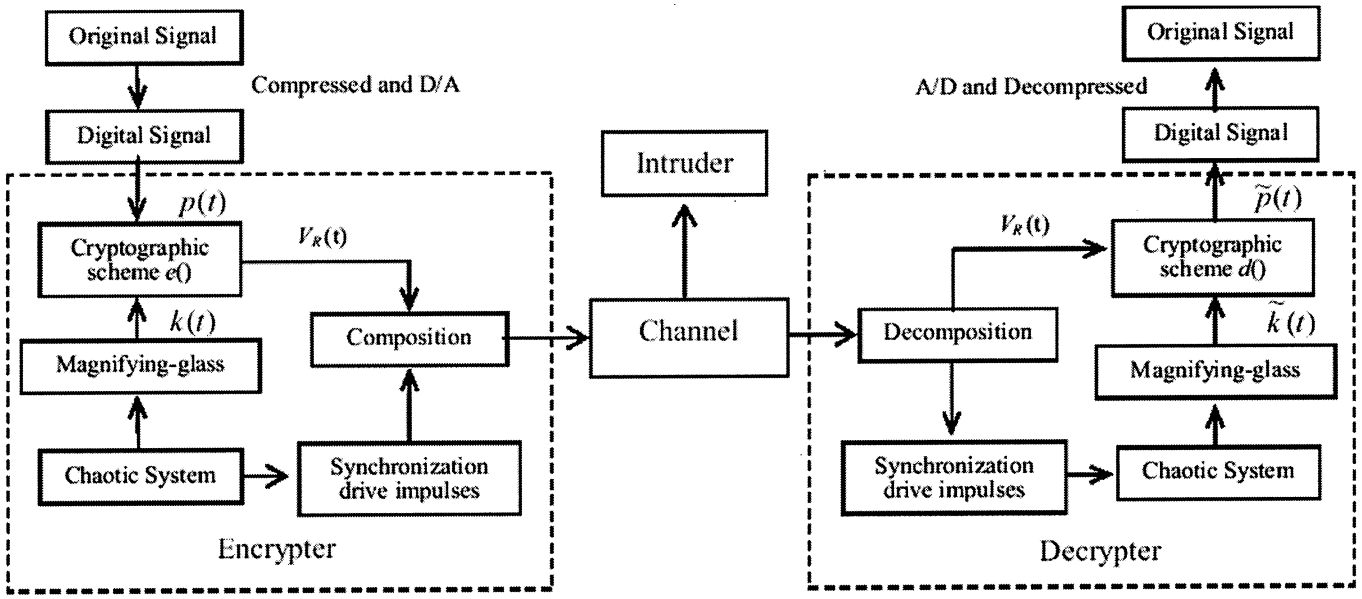


Fig. 1. System block diagram of the chaotic cryptosystem.

three state variables of the Chua's circuit. The ciphertext is obtained from an XOR operation on the plaintext and the key sequence bit by bit. The decryption is the same as the encryption, including the XOR operation of the transmitted scrambled signal with the key signal $k(t)$. When the Chua's circuits in the decrypter and the encrypter are synchronized, the decrypter can find the same key signal sequence $\widetilde{k}(t)$ as in the encrypter $k(t)$.

A. Encrypter

The dimensionless state equations of Chua's circuit are given as

$$\begin{cases} \dfrac{dx_1}{dt} = k\alpha\left(x_2 - x_1 - f(x_1)\right) \\ \dfrac{dx_2}{dt} = k(x_1 - x_2 + x_3) \\ \dfrac{dx_3}{dt} = k(-\beta x_2 - \gamma x_3) \end{cases} \tag{1}$$

where α, β and γ are constants, $k \in [-1, 1]$ and $f(x)$ is the nonlinear characteristic of Chua's diode in Chua's circuit given by

$$f(x) = m_1 x + \frac{1}{2}(m_0 - m_1)\left\{|x+1| - |x-1|\right\} \tag{2}$$

and where m_0 and m_1 are two negative constants. Since the signals are transmitted through a digital channel, the synchronization pulses should be first quantized by a predefined quantizer $Q(\cdot)$, which depends on the amplification factor K used in (3). Since chaos is very sensitivity to initial condition, the quantization error should be less than certain values to ensure that the encrypter and the decrypter can be synchronized [17].

To provide the desired key sequence, we introduce the concept of a magnifying glass, which is composed of an amplifier and an observer. They are given in details as follows.

The amplifier:

$$k'(t) = K\left(x_1^2(t) + x_2^2(t) + x_3^2(t)\right)^{\frac{1}{2}} \tag{3}$$

The observer

$$k(t) = \left(\lfloor k'(t) \rfloor + \lambda\right) \bmod (256) \tag{4}$$

where K is a large number which can be chosen to influence the sensitivity of the system, λ is an arbitrary integer and $\lfloor a \rfloor$ is the integer truncation of a.

The scrambled signal v_R is given by

$$v_R(t) = E\left(p(t)\right) = p(t) \oplus k(t) \tag{5}$$

where $p(t)$ is the plaintext, $k(t)$ is given in (4), $E(p(t))$ is the ciphertext, and $\oplus$ denotes XOR operation.

B. Decrypter

Both Chua's circuit and the impulsive controller in the decrypter are given by

$$\begin{cases} \dfrac{d\widetilde{x}_1}{dt} = k\alpha\left(\widetilde{x}_2 - \widetilde{x}_1 - f(\widetilde{x}_1)\right) \\ \dfrac{d\widetilde{x}_2}{dt} = k(\widetilde{x}_1 - \widetilde{x}_2 + \widetilde{x}_3), \qquad t \neq \tau_n; n = 1, 2, \cdots \\ \dfrac{d\widetilde{x}_3}{dt} = k(-\beta\widetilde{x}_2 - \gamma\widetilde{x}_3) \end{cases} \tag{6}$$

and

$$\begin{bmatrix} \widetilde{x}_1(\tau_n) \\ \widetilde{x}_2(\tau_n) \\ \widetilde{x}_3(\tau_n) \end{bmatrix} = \begin{bmatrix} \widetilde{x}_1(\tau_n^-) \\ \widetilde{x}_2(\tau_n^-) \\ \widetilde{x}_3(\tau_n^-) \end{bmatrix} - B \begin{bmatrix} Q\left(x_1(\tau_n)\right) - \widetilde{x}_1(\tau_n^-) \\ Q\left(x_2(\tau_n)\right) - \widetilde{x}_2(\tau_n^-) \\ Q\left(x_3(\tau_n)\right) - \widetilde{x}_3(\tau_n^-) \end{bmatrix}, \quad n = 1, 2, \cdots \tag{7}$$

where B is a 3×3 matrix to be designed to satisfy certain inequality, $Q(\cdot)$ is a predefined quantizer, and τ_n^- are the times immediately prior the times τ_n; $\{\tau_n\}, 1 \leq n < \infty$, satisfy

$$\begin{aligned} &0 < \tau_1 < \tau_2 < \cdots < \tau_n < \tau_{n+1} < \cdots, \quad \tau_n \to \infty \; as \; n \to \infty \\ &\tau_1 - \tau_0 = \tau_3 - \tau_2 = \cdots = \tau_{2i+1} - \tau_{2i} = \cdots \\ &\tau_2 - \tau_1 = \tau_4 - \tau_3 = \cdots = \tau_{2i} - \tau_{2i-1} = \cdots \end{aligned} \tag{8}$$

Let $\Delta_1 = (\tau_{2i} - \tau_{2i-1})$ and $\Delta_2 = (\tau_{2i+1} - \tau_{2i})$. Δ_1 and Δ_2 satisfy that

$$\Delta_2 = \hat{\xi}_1 \Delta_1 \tag{9}$$

In (9), $\hat{\xi}_1$ is an arbitrary number. The parameter $\hat{\xi}_1$ is usually determined by the parameters of Chua's circuit. An example is given by $\hat{\xi}_1 = (|\alpha/\beta|)$. Matrix B and Δ_1 are chosen to synchronize the two chaotic systems (1) and (6) in the transmitter and the receiver, respectively.

We let A denote the linear system matrix of (1) and (6), i.e.

$$A = \begin{bmatrix} -k\alpha & k\alpha & 0 \\ k & -k & k \\ 0 & -k\beta & -k\lambda \end{bmatrix} \tag{10}$$

Then B and Δ_1 are chosen according to the requirement of impulsive control strategy to satisfy [8]

$$0 \le v + 2|\alpha m_0| \le -\frac{2}{(1+\hat{\xi}_1)\Delta_1} \ln(\xi d_1) \tag{11}$$

where $\xi > 1$, v is the largest eigenvalue of $(A + A^T)$ and d_1 is the largest eigenvalue of $(I + B)^T(I + B)$. It has been shown from Theorem 3 in [8] that the chaotic systems proposed in the encrypter and the decrypter are globally synchronized.

In the decrypter, the plaintext is recovered via

$$\widetilde{k}(t) = \left(\left\lfloor K \left(\widetilde{x}_1^2(t) + \widetilde{x}_2^2(t) + \widetilde{x}_3^2(t) \right)^{\frac{1}{2}} \right\rfloor + \lambda \right) \bmod(256) \tag{12}$$

$$\widetilde{p}(t) = \widetilde{E}\left(p(t)\right) = v_R(t) \oplus \widetilde{k}(t) \tag{13}$$

where $\widetilde{E}(p(t))$ is the recovered encrypted signal. $\widetilde{k}(t)$ is recovered in the receiver circuit and should approximate $k(t)$.

It can be known from (12) and (13) that the original signal can be recovered only when two identical chaotic circuits in both the encrypter and the decrypter are synchronized. Similarly, an intruder can know the original message only when he knows the parameters and the structure of the circuits and the synchronization impulses.

Remark 1: Here, we have used the magnifying-glass to transform the chaotic state variables which act as key sequence before XOR with the plaintext. Assuming that there is a small mismatch that results in perturbations $\Delta x_i(t) = \sigma_i (i = 1, 2, 3)$, then the signal getting through the amplifier has $k(t) = (\lfloor K(\sum_{i=1}^{3}(x_i(t) + \sigma_i)^2)^{1/2} \rfloor + \lambda) \bmod(256)$. Since the parameter K is a large number, we can see that the signal is enlarged many times, which implied that the parameters mismatch can be enlarged. Thus even a minor mismatch in the parameters will produce a large decryption error, resulting in a decryption key sequence that is not the same as the encryption key signal. So, one cannot recover the plaintext signal. The security of the chaotic communication system is thus improved. □

Before transmitting the ciphertext through a digital channel, it is necessary to packetize the ciphertext. To simplify the operation, we use a packetization algorithm in which the packet length is fixed. The length of the packets is the same as the length of the first impulsive interval. Since the lengths of the impulsive intervals are piecewise constant, it is difficult to find the synchronization impulse. The security of the system can then be improved.

III. Synchronization Time Estimation

In this section, we shall show that the time-varying impulsive intervals do not effect the synchronization of two identical chaotic circuits embedded in the encrypter and the decrypter, and we are able to estimate the time required for synchronization.

From (1) and (6), we let $e^T = (e_x, e_y, e_z) = (x_1 - \widetilde{x}_1, x_2 - \widetilde{x}_2, x_3 - \widetilde{x}_3)$ be the synchronization error and $\widetilde{X} = (\widetilde{x}_1, \widetilde{x}_2, \widetilde{x}_3)^T$. We then have

$$\begin{cases} \dot{e} = Ae + \Psi(X, \widetilde{X}); \quad t \neq \tau_n, \quad n = 1, 2, \cdots \\ e\left(\tau_n^+\right) = (I + B)e(\tau_n) + B\left(X(\tau_n) - Q\left(X(\tau_n)\right)\right), \quad n = 1, 2, \cdots \end{cases} \tag{14}$$

where $\Psi(X, \widetilde{X}) = [-\alpha f(x_1) + \alpha f(\widetilde{x}_1), 0, 0]^T$.

Define the Lyapunov function $V(\mathrm{e})$ as $V(e) = e^T e = \|e\|^2$. We then have

$$\begin{aligned} \dot{V}(e) &\le (v + 2|\alpha m_0|) V(e) \\ V\left(e\left(\tau_n^+\right)\right) &\le d_1 V\left(e(\tau_n)\right) + \|B\|^2 \frac{q^2}{4} + q\|B\| d_1^{\frac{1}{2}} \|e(\tau_n)\| \\ &\le d_1 V\left(e(\tau_n)\right) + c_1 q \end{aligned}$$

where q is the quantization parameter and $c_1 = \|B\|^2 q/4 + \|B\| d_1^{1/2} \sup(\|e(\tau_n)\|)$.

Since $\|e(\tau_n)\|$ is always bounded [9], c_1 is a finite number. For simplicity, we denote

$$\begin{aligned} \lambda(\tau) &= (v + 2|\alpha m_0|)\tau \\ \overline{\omega} &= d_1 c_1 \left(\exp\left((v + 2|\alpha m_0|)(\Delta_1 + \Delta_2) \right) \right. \\ &\qquad \left. + \exp\left((v + 2|\alpha m_0|) \max\{\Delta_1, \Delta_2\} \right) \right) \end{aligned}$$

First of all, we have

$$\begin{aligned} & V\left(e(\tau_{2n}, t_0, e_0)\right) \\ &\le V\left(e\left(\tau_{2n-1}^+, t_0, e_0\right)\right) \exp\left(\lambda(\tau_{2n}) - \lambda(\tau_{2n-1})\right) \\ &\le \left(d_1 V\left(e(\tau_{2n-1}, t_0, e_0)\right) + c_1 q\right) \exp\left(\lambda(\tau_{2n}) - \lambda(\tau_{2n-1})\right) \\ &\le \left(d_1 \left(d_1 V\left(e(\tau_{2n-2}, t_0, e_0)\right) + c_1 q\right)\right. \\ &\quad \times \exp\left(\lambda(\tau_{2n-1}) - \lambda(\tau_{2n-2})\right) + c_1 q) \\ &\quad \left. \times \exp\left(\lambda(\tau_{2n}) - \lambda(\tau_{2n-1})\right)\right) \\ &= d_1^2 \exp\left(\lambda(\tau_{2n}) - \lambda(\tau_{2n-2})\right) V\left(e(\tau_{2n-2}, t_0, e_0)\right) \\ &\quad + d_1 c_1 \exp\left(\lambda(\tau_{2n}) - \lambda(\tau_{2n-1})\right) q \\ &\quad + d_1 c_1 \exp\left(\lambda(\tau_{2n}) - \lambda(\tau_{2n-2})\right) q \end{aligned}$$

It can be known from (8) and (11) that $d_1^2 \exp(\lambda(\tau_{2n}) - \lambda(\tau_{2n-2})) \le (1/\xi^2)$. Thus

$$\begin{aligned} V\left(e(\tau_{2n}, t_0, e_0)\right) &\le \frac{1}{\xi^2} V\left(e(\tau_{2n-2}, t_0, e_0)\right) + \overline{\omega} q \\ &\le \frac{V(\mathrm{e}_0)}{\xi^{2n}} + \frac{\xi^2 \overline{\omega}}{\xi^2 - 1} q. \end{aligned}$$

So, for any $\tau_{2n} < t < \tau_{2n+1}$, and for all $n \geq 1$, we have

$$\begin{aligned} V(e(t,t_0,e_0)) &\leq V\left(e\left(\tau_{2n}^{+},t_0,e_0\right)\right)\exp\left(\lambda(t)-\lambda(\tau_{2n})\right) \\ &\leq \left(d_1 V\left(e(\tau_{2n},t_0,e_0)\right)+c_1 q\right) \\ &\quad \times \exp\left(\lambda(t)-\lambda(\tau_{2n})\right) \\ &\leq \left(\frac{d_1 V(e_0)}{\xi^{2n}}+\frac{d_1\xi^2\overline{\omega}}{\xi^2-1}q+c_1 q\right) \\ &\quad \cdot \exp\left((v+2|\alpha m_0|)\max\{\Delta_1,\Delta_2\}\right)) \end{aligned}$$

It can be known from (4) that the error cannot be observed if $|K\|X\| - K\|\widetilde{X}\|| < 1$. Note that $|\|X\| - \|\widetilde{X}\||^2 \leq V(e(t,t_0,e_0))$. Therefore the error cannot be observed if

$$\begin{aligned} n \geq \log_{\xi^2}\Big(d_1 V(e_0)\cdot\Big(\big(K^2\exp\left((v+2|\alpha m_0|\right) \\ \times\max\{\Delta_1,\Delta_2\}\big)^{-1}-c_1 q-\frac{d_1\xi^2\overline{\omega}}{\xi^2-1}q\Big)^{-1} \end{aligned} \tag{15}$$

The estimate of synchronization time needed is then given by

$$t_{syn} = n\cdot(T_{2i-1}+T_{2i}) \tag{16}$$

where $T_{2\mathrm{i}-1}$ and $T_{2\mathrm{i}}$ are pre-defined. The chaotic system in the receiver will be synchronized with that in the transmitter after t_{syn}.

Remark 2: From (16), we can see that the value of K will influence the synchronization stable time of two identical chaotic systems and the desired precision of the system. A larger K will require longer synchronization time. On the other hand, the security of the system is higher with a larger K. A tradeoff should be obtained in practice. □

IV. Experimental Results

In this section, we provide some experimental results to illustrate the performance of the proposed chaotic secure communication system. Since the audio has been widely studied by many researchers [2]–[4], [16], [17], we shall study text transmission. To further improve the sensitivity of our system, arithmetic coding is adopted to reduce the redundancy of the messages [13], [14], [26], [27].

The most significant portion of an arithmetic-coded message belongs to the first symbols. During the rest of the encoding process, each new symbol will further restrict the possible range of the output number. While encoding, there are high and low variables, which are both maintained by the decoder with a code variable. During arithmetic decoding, the high and low variables should track exactly the same values as those during the encoding process, and the code variable should reflect the bit stream as it is read in from the input file. Once one symbol is determined, the symbol is outputted and the current high and low values are stored and will be used in the next step of the decoding process. The arithmetic-encoded output bits are interrelated. The code value of current symbol affects the correctness of next decoded symbol. If the front symbol cannot be determined correctly, the subsequent symbols cannot be decoded, so the beginning part of input is the most sensitive part in arithmetic decoding. We shall fully adopt this property to design our system. Since the propagation of the error needs a period of time, the state of synchronization will remain for a period of time, after which the errors become larger and they become divergence. To improve the security, the encrypted plaintext is the reverse of the arithmetic-coded message, the less sensitive part of the plaintext is encrypted in the beginning of each impulsive interval while the more sensitive part of the plaintext is encrypted in the end of each interval. It is therefore difficult to recover the original message from this decrypted result by arithmetic decoding, even though there is still synchronization at the beginning.

In order to make our encryption system can be widely used in the computer, we use 256 characters ASCII code, which includes 128 standard ASCII codes and other 128 that are known as extended ASCII. Thus, the ciphertext in the simulation has not only the standard characters, but also some local symbols and marks. When the ciphertext can be decrypted by correct key, the message is exactly recovered as shown in Table I. Otherwise, the recovered message are spread in the extend ASCII code.

In our study, we choose the parameters of Chua's circuit as $k = 1$, $\alpha = 9.351\ 590\ 85$, $\beta = 14.790\ 313\ 805$, $\gamma = 0.016\ 072\ 965$, $m_0 = -1.138\ 411\ 196$ and $m_1 = -0.722\ 451\ 121$. Note that $v = 14.407\ 0$. We choose the impulsive controller as $\hat{\xi}_1 = 0.5$, and matrix B as

$$B = \begin{bmatrix} -1.05 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

and $d_1 = 0.002\,5$. For any ξ satisfying $\xi > 1$ and $0 < |\xi d_1| \leq 1$, we choose $\xi = 300$. To synchronize the two chaotic systems (1) and (6) in the transmitter and the receiver, Δ_1 has to satisfy (11), i.e.

$$\Delta_1 \leq -\frac{2\left(\ln(\xi)+2\ln|\theta+1|\right)}{1.5\left(v+2|a\alpha|\right)} = 1.07\times 10^{-2}\ s$$

In our experiments, we choose the frame length as $T_{2i-1} = 5\times 10^{-3}s$ and $T_{2i} = 2\times 10^{-3}s$.

The initial condition is given by $[x_1(0), x_2(0), x_3(0)] = [-2.12;\ -0.05;\ 0.8]$ and $[\widetilde{x}_1(0), \widetilde{x}_2(0), \widetilde{x}_3(0)] = [-0.2;\ -0.02;\ 0.1]$, respectively. So the encrypter and decrypter are initially not synchronized, and the initial error is $e(0) = [-1.92;\ -0.03;\ 0.7]$. We choose the magnifying glass as $K = 1\times 10^3$ and $\lambda = 12$. The quantization step is $q = 5\times 10^{-8}$.

Numerical calculated the required synchronization time, we have $n > 5$, and hence $t_{syn} = n\cdot(T_{2i-1}+T_{2i}) = 0.035\ s$. Therefore, the cryptosystem will be synchronized in a 0.035-s process by impulsive control. After the encrypter and decrypter are synchronized, they will generate the same key sequences. It is shown in Fig. 2 that the synchronization error approaches zero very quickly, and it is less than what was estimated. This is because the estimation of the synchronization time is a conservative estimation.

The ciphertext that is transmitted through the public channel is shown in Fig. 3. In Table I, we show one example frame of the original message; the corresponding arithmetic-coded message, which is the plaintext in encryption; the transmitted ciphertext; the decrypted text; and the decompressed message, respectively. We can see that the ciphertext is completely different from the

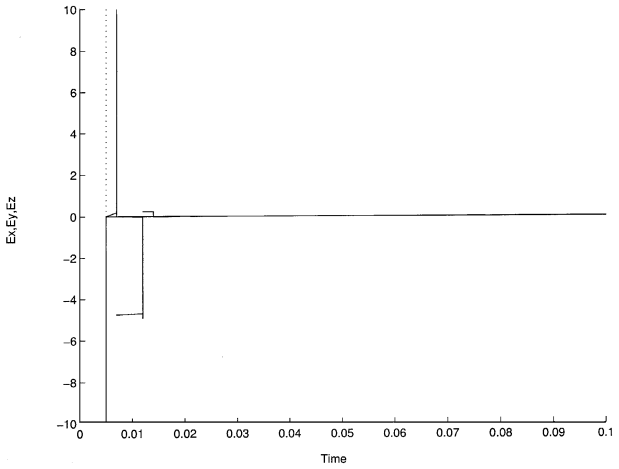


Fig. 2. The time responses of $e^T = (e_x, e_y, e_z)$.

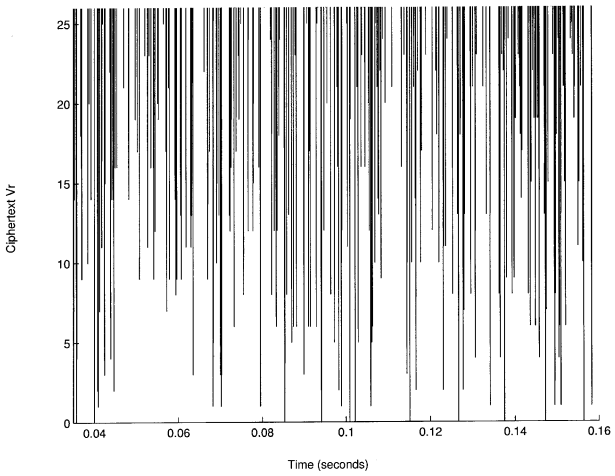


Fig. 3. The transmitted ciphertext v_R.

TABLE I
SAMPLE OF SIMULATION RESULT

Message	*Chaotic Secure Communication System*
Plaintext (Compressed)	*=›kž□~{ XR□ m"³Ð\E§-Í□u¢`„fÌEm¡o□*
Ciphertext	*□¥U£2CG26ci#3W©‰éé|Ÿ•õ1B•V²Pù pX•[0*
Recovered	*=›kž□~{ XR□ m"³Ð\E§-Í□u¢`„fÌEm¡o□*
De-compressed	*Chaotic Secure Communication System*

plaintext in transmission while the decrypted text is the exact version of the plaintext, so we are able to recover the original message by arithmetic decoding.

Clearly, in our system, if the numbers, K and λ have small mismatches, it will be impossible to recover the plaintext. These are key design parameters in our scheme and are therefore assumed to be known exactly. So, we do not consider the effect of error in these two parameters in this paper.

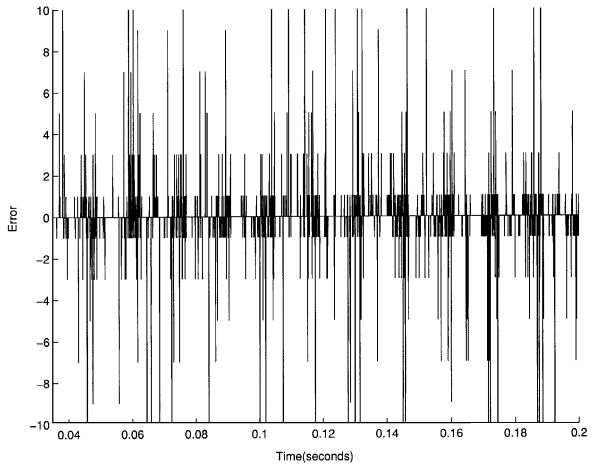


Fig. 4. The error between plaintext and decrypted text with 1% mismatch in α.

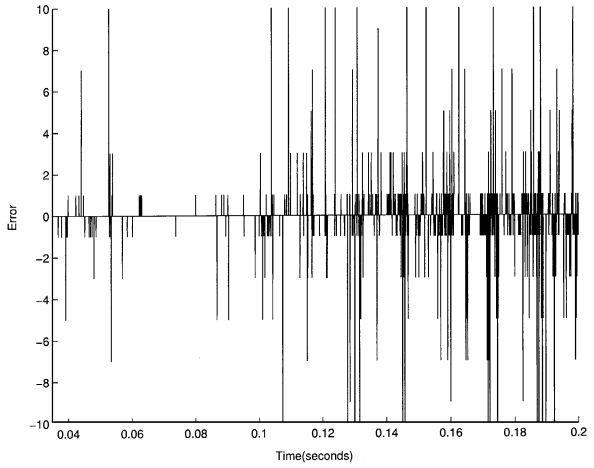


Fig. 5. The error between plaintext and decrypter text with 1% mismatch in β.

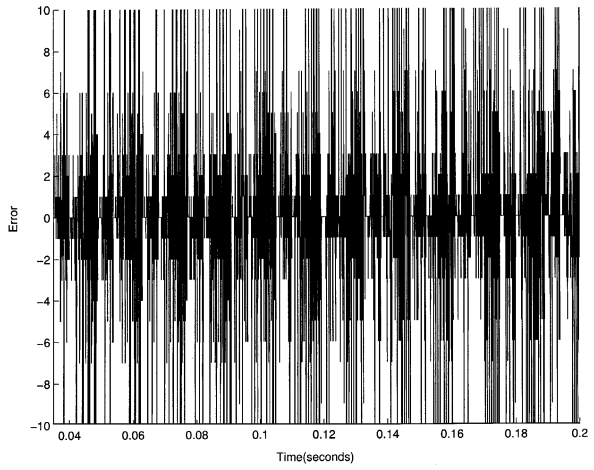


Fig. 6. The error between plaintext and decrypted text with 1% mismatch in m_0.

We next study the effects of parameter mismatch in the decrypter Chua's circuit. Fig. 4 shows the error between the plaintext signal and the received text signal when α in the decrypter has a 1% mismatch compared with that in the encrypter. Fig. 5 shows a frame of the error when β has a 1% mismatch. Fig. 6

shows a frame of the error when m_0 as a 1% mismatch. We can see that the state of synchronization will remain for a period of time, after which the errors become larger and they become divergence. In view of the implementation of the system, where the encrypted plaintext is the reverse of the arithmetic-coded message, the sensitive part of the plaintext is encrypted in the end of each impulsive interval. It is, therefore, difficult to recover the original message from this decrypted result by arithmetic decoding. Furthermore, one cannot recover the original message by guessing one part of it. The differences in the received plaintexts in the above three cases are illustrated below.

Original message is given as follows:

Increased security measures are attracting more American doctors to the Internet. The physicians are using the network in a number of ways, including communicating with colleagues and keeping up with current medical research.. . .

1) When there is no mismatch, the recovered message is given as follows:

Increased security measures are attracting more American doctors to the Internet. The physicians are using the network in a number of ways, including communicating with colleagues and keeping up with current medical research.. . .

2) When α has 1% mismatch, the recovered message is given as follows:

J&ŽCÝ□ 8W˜□ôš/‹‹□□ªŒ
ä¬f0-©^Z|cxàz*
)□ÖñCÑÙ“ÄZ9m{ ôúŽÃþÜX–÷=ÙuÏJ×Ý=¥
lO-

3) When β has 1% mismatch, the recovered message is given as follows:

J&ŽCÝ□ 8W˜□ôš/‹‹□□ªŒ
ä¬fDC¸¿□
¸tÝ'□´8“
□¿|\□
$C´á%îCèVCtg□×Œ¸¸ˆ^□y-sc`ß`…#&J
wU□MÚ□¦áÍàsTÛW Cu{Ó
…

4) When m_0 has 1% mismatch, the recovered message is given as follows:

òWáa^i²'„□gi¦Ñ†7Œ%KIµÜ·D<ò□G ª¦ˆ×A«¢ôýªÝ#±Ñif¬ii-ÂÑÂ“/*
□ ›¿~ ?4òig…Ô´Â4□Z—□òx□äxhA›^>3v ˆ
„~ìi¬Ô¢>□u®—
□2)GWÜ®®ïŽ¥GIû úÊ±¤ù¥§¶¥@,Öp±yä/xê›c®ã;l¶Žt²ø□~-
atc§)K6ûæ
*□u§>¸Œ□]§~uöà²¶u¼¥Ø□Ptææ_ú~ìiÜ□i«²ö»/fòGÂc□ÏŽ'ÔzÂ¥c^^*
Ü õ
gæ-8¡„~ì4-
*'X□¾~x¦ä_ÖïúÖ}2ÔÃ'¢Û{Óû'□¼□úG®¿ø„□uÇ□ÊÕ¢Ña@Ñ-æ^*
—õ
…

When K is chosen to be a larger value, the system is more sensitive to the parameter mismatch, thus ensuring a more secure communication. However, a longer synchronization time will be required. Thus, in practice, a tradeoff is required when we choose the value of K.

V. Conclusion

We have presented a novel digital chaotic secure communication system by introducing a concept magnifying glass to enlarge observed errors due to parameter mismatch and an impulsive control strategy with piecewise-constant intervals to synchronize chaotic circuits. The proposed system is a combination of a conventional cryptographic scheme and a chaotic secure communication scheme. Our secure communication system is shown to be very sensitive to parameter mismatch.

References

[1] L. K. Pecora and J. L. Carroll, “Synchronization in chaotic systems,” *Phy. Rev. Lett.*, vol. 64, pp. 821–824, 1990.

[2] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, “Synchronization of Lorenz-based chaotic circuits with application to communication,” *IEEE Trans. Circuits Syst. I*, vol. 40, pp. 626–633, Oct. 1993.

[3] C. W. Wu and L. O. Chua, “A simple way to synchronize chaotic system with application to secure communication system,” *Int. J. Bifurc. Chaos*, vol. 3, no. 6, pp. 1619–1627, 1993.

[4] U. Feldmann, M. Hasler, and W. Schwarz, “Communication by chaotic signal: the inverse system approach,” in *Proc. IEEE Int. Symp. Circuits and Systems, ISCAS’95*, 1995, pp. 680–683.

[5] T. Yang, C. W. Wu, and L. O. Chua, “Cryptography based on chaotic systems,” *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 469–472, May 1997.

[6] H. Zhou and Y. T. Ling, “Problems with the chaotic inverse system encryption approach,” *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 268–271, Mar. 1997.

[7] Z. G. Li, C. Y. Wen, and Y. C. Soh, “Analysis and design of impulsive control systems,” *IEEE Trans. Automat. Contr.*, vol. 46, pp. 894–897, June 2001.

[8] Z. G. Li, C. Y. Wen, Y. C. Soh, and W. X. Xie, “The stabilization and synchronization of Chua’s oscillators via impulsive control,” *IEEE Trans. Circuits Syst. I*, vol. 48, pp. 1351–1355, Nov. 2001.

[9] T. Yang and L. O. Chua, “Impulsive stabilization for control and synchronization of chaotic systems: theory and application to secure communication,” *IEEE Trans. Circuits Syst. I*, vol. 44, pp. 976–988, May 1997.

[10] K. M. Short, “Steps toward unmasking secure communication,” *Int. J. Bifurc. Chaos*, vol. 4, no. 4, pp. 959–977, 1994.

[11] ——, “Unmasking a modulated chaotic communications scheme,” *Int. J. Bifurc. Chaos*, vol. 6, no. 2, pp. 611–615, 1996.

[12] R. N. Madan, *Chua’s Circuit: A Paradigm For Chaos*, Singapore: World Scientifc, 1993.

[13] I. H. Written, R. M. Neal, and J. G. Cleary, “Arithmetic coding for data compression,” *Commun. ACM*, vol. 30, no. 6, pp. 520–540, 1987.

[14] P. G. Howard and J. S. Vitter, “Arithmetic coding for data compression,” *Proc. IEEE*, vol. 82, pp. 857–865, June 1994.

[15] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. New York: Wiley, 1996.

[16] O. Gonzales, G. Han, J. Gyvez, and E. Sanchez-Sinencio, “Lorenz-based chaotic cryptosystem: a monolithic implementation,” *IEEE Trans Circuits Syst. I*, vol. 47, pp. 1243–1247, Aug. 2000.

[17] Z. He, K. Li, L. Yang, and Y. Shi, “A robust digital secure communication scheme based on sporadic coupling chaos synchronization,” *IEEE Trans Circuits Syst. I*, vol. 47, pp. 397–403, Mar. 2000.

[18] Y. Tao, “Chaotic secure communication systems: history and new results,” *Telecommun. Rev.*, vol. 9, no. 4, pp. 597–634, 1999.

[19] J. Cruz and L. O. Chua, “An IC chip of Chua’s circuit,” *IEEE Trans. Circuits Syst. I*, vol. 40, pp. 614–625, Oct. 1993.

[20] A. I. Panas, T. Yang, and L. O. Chua, “Experimental results of impulsive synchronization between two Chua’s circuits,” *Int. J. Bifurc. Chaos*, vol. 8, no. 8, pp. 639–644, 1998.

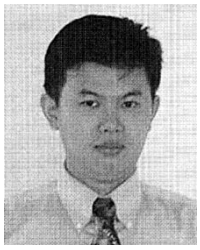
[21] Z. G. Li, C. B. Soh, and X. H. Xu, “Stability of impulsive differential systems,” *J. Math.Anal. Applicat.*, vol. 216, no. 6, pp. 644–653, 1997.

[22] G. Heidari-Bsteni and C. MCGillem, “A chaotic direct-sequence spread-spectrum communication system,” *IEEE Trans. Commun.*, vol. 42, pp. 1524–1527, Feb./Mar./Apr. 1994.

[23] G. Elmasry, “Joint lossless-source and channel coding using automatic repeat request,” *IEEE Trans. Commun.*, vol. 47, pp. 953–955, July 1999.

[24] C. Boyd, J. Cleary, S. Irvine, I. Rinsma-Melchert, and I. Witten, “Integrating error detection into arithmetic coding,” *IEEE Trans. Commun.*, vol. 45, pp. 1–3, Jan. 1997.

[25] R. Anand, K. Ramchandran, and I. Kozintsev, "Continuous error detection (CED) for reliable communication," *IEEE Trans. Commun.*, vol. 49, pp. 1540–1549, Sept. 2001.
[26] J. Jou and P. Chen, "A fast and efficient lossless data-compression method," *IEEE Trans. Commun.*, vol. 47, pp. 1278–1283, Sept. 1999.
[27] Y. Kim and J. Modestino, "Adaptive entropy-coded subband coding of image sequences," *IEEE Trans. Commun.*, vol. 41, pp. 975–987, June 1993.



Zhengguo Li received the B. S. degree and the M. Eng. Degree from Northeastern University, China, in 1992 and 1995, respectively, and the Ph.D. degree from Nanyang Technological University, Singapore, in 2001.

Currently, he is with the Agency for Science, Technology and Research. His research interests include hybrid systems, video processing and chaotic secure communication.

Kun Li received the B.Eng. and M. Eng. degrees in electrical engineering from the Harbin Institute of Technology, Harbin, China, in 1996 and 1998, respectively, and she is currently working toward the Ph.D. degree at the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore.

Her main research interests are chaos control and synchronization, and secure communications.

Changyun Wen was born in Chongqing, China. He received the B.Eng from Xian Jiaotong University, China, in 1983, and Ph.D. degree from the University of Newcastle, Newcastle, Australia.

From August 1989 to August 1991, he was a Postdoctoral Fellow at the University of Adelaide, Australia. Since August 1991, he has been with the School of Electrical and Electronic Engineering at Nanyang Technological University, Singapore, where he is currently an Associate Professor. His major research interests are in the areas of control and signal processing as well as their applications.

Dr. Wen has served on the IEEE TRANSACTION ON AUTOMATIC CONTROL as an Associate Editor from 2000 to 2002.

Yeng Chai Soh received the B.Eng. (Hons. I) degree in electrical and electronic engineering from the University of Canterbury, Christchurch, New Zealand, in 1983, and the Ph.D. degree in electrical engineering from the University of Newcastle, Newcastle, Australia, in 1987.

From 1986 to 1987, he was a research assistant in the Department of Electrical and Computer Engineering, University of Newcastle. He joined the Nanyang Technological University, Singapore, in 1987 where he is currently a professor in the School of Electrical and Electronic Engineering. Since 1995, he has been the Head of the Control and Instrumentation Division. His current research interests are in the areas of robust system theory and applications, signal processing, estimation and filtering, model reduction, and hybrid systems.