Although the optimal α is the one which minimizes $\xi(\alpha)$, it is not easy in practice to find this value. The reason for this follows from Theorem 5.

Theorem 5: Let $A^T + A = -Q$ with Q positive definite. Then the value of α which minimizes $\xi(\alpha)$ is given by

$$\alpha_{opt} = \frac{\|Ar\|}{\|r\|} \tag{48}$$

where r is the vector obtained by the minimization procedure

$$r = \arg\min_{x\neq 0} \frac{x^T Q x}{\|x\|\|Ax\|}. \tag{49}$$

Proof: The minimization of $\xi(\alpha)$ is equivalent with the minimax problem

$$\min_{\alpha}\max_{x} \frac{\|Ax\|^2 - \alpha x^T Q x + \alpha^2\|x\|^2}{\|Ax\|^2 + \alpha x^T Q x + \alpha^2\|x\|^2} \quad x \in R^n \quad \alpha > 0. \tag{50}$$

This can be reformulated as

$$\min_{\alpha}\max_{x} \left\{ \frac{1}{\alpha}\frac{\|Ax\|^2}{x^T Q x} + \alpha \frac{\|x\|^2}{x^T Q x} \right\}. \tag{51}$$

For any given x, the unique positive value of α which minimizes the expression between the curly brackets of (51) is given by

$$\alpha = \frac{\|Ax\|}{\|x\|}. \tag{52}$$

Since the duality gap [10, p. 23] is therefore zero, we can insert this value for α in (51), and this completes the proof. □

However, the vector r defined by the minimization procedure (49) is not easy to obtain. On the other hand, Theorem 4 guarantees that $\xi(\alpha) < 1$ for $0 < \alpha < \infty$ whenever $A + A^T$ is negative definite, which is always possible by means of a transformation of the state space variables. Hence, any positive value of α results in a stable reduced-order model. In [7] it has been shown that an interval of "good" values for α is given by

$$\frac{2}{\pi}\,\omega_{\max} \leq \alpha \leq \frac{\pi}{2}\,\omega_{\max} \tag{53}$$

where $\omega_{\max}$ is the bandwidth (in rad/s) of the system. Note that the geometric mean of the interval in (51) is $\alpha = \omega_{\max}$, which is therefore a straightforward choice for α.

REFERENCES

[1] B. C. Moore, "Principal component analysis in linear systems: Controllability, observability, and model reduction," *IEEE Trans. Automat. Contr.*, vol. AC-26, pp. 17–31, Feb. 1981.

[2] M. G. Safonov and R. Y. Chiang, "A Schur method for balanced-truncation model reduction," *IEEE Trans. Automat. Contr.*, vol. 34, pp. 729–733, July 1989.

[3] C. De Villemagne and R. E. Skelton, "Model reduction using a projection formulation," *Int. J. Control*, vol. 46, no. 6, pp. 2141–2169, 1987.

[4] W. B. Gragg and A. Lindquist, "On the partial realization problem," *Lin. Alg. Applicat.*, vol. 50, pp. 277–319, 1983.

[5] R. W. Freund, "Reduced-order modeling techniques based on Krylov subspaces and their use in circuit simulation," Bell Laboratories, Murray Hill, NJ, Numerical Analysis Manuscript 98-3-02, Feb. 1998.

[6] D. L. Boley, "Krylov space methods on state-space control models," *Circuits Syst. Signal Processing*, vol. 13, no. 6, pp. 733–758, 1994.

[7] L. Knockaert and D. De Zutter, "Passive reduced order multiport modeling: The Padé–Laguerre, Krylov–Arnoldi-SVD connection," *Int. J. Electron. Commun. (AEÜ)*, vol. 53, no. 5, pp. 254–260, 1999.

[8] L. Knockaert and D. De Zutter, "Laguerre-SVD reduced-order modeling," *IEEE Trans. Microwave Theory Tech.*, vol. 48, pp. 1469–1475, Sept. 2000.

[9] L. Knockaert, "On orthonormal Müntz–Laguerre filters," *IEEE Trans. Signal Processing*, vol. 49, pp. 790–793, Apr. 2001.

[10] D. M. Greig, *Optimization*. London, U.K.: Longman, 1980.

Chaotic Cryptosystem With High Sensitivity to Parameter Mismatch

K. Li, Y. C. Soh, and Z. G. Li

***Abstract*—In this brief, we present a new sufficient condition for the stabilization and the synchronization of Chua's circuit. The Chua's circuit is used in our chaotic secure cryptosystem and the relaxed stability condition enabled us to obtain a larger bound on the impulsive interval, which leads to a higher efficiency in bandwidth utilization. In the proposed system, we introduce a concept of magnifying glass to enlarge and observe some minor parameter mismatch and hence it increases the sensitivity and the security level of the cryptosystem. We shall use speech transmission as an example to illustrate that the proposed cryptosystem can achieve excellent encryption effect and it is sensitive to the parameter mismatch.**

***Index Terms*—Chaotic cryptosystem, Chua's circuit, impulsive synchronization.**

I. INTRODUCTION

Over the past decade, chaotic dynamics have been successfully exploited in communication applications, and these include chaotic encryption for security, chaotic spreading codes for multiuser access in spread-spectrum systems, and chaotic modulation for the transmission of analog and digital information [1]. The advances in the synchronization of chaotic systems [2]–[4], [9] have created the possibility of communication using chaotic waveforms as carriers, and particularly in application to secure communications. Indeed, a lot of chaotic secure communication systems have been proposed [3]–[10], and the chaotic secure communication systems have moved into the fourth generation [8]. All of the first three generations have adopted the continuous chaotic synchronization scheme. The fourth generation uses impulsive chaotic synchronization [7] to increase the efficiency of bandwidth usage. Various theoretical and experimental results of impulsive chaotic synchronization and applications to chaotic communications systems can be found in [18]–[20]. Although impulsive chaotic synchronization has been widely studied [7], [13], [14], the existing results are still very conservative.

Chaotic cryptography systems [6] are schemes that combine the classical cryptographic techniques and chaotic synchronization to enhance the degree of security. However, the proposed attacks [10]–[12] have shown that most of these methods are still not secure or have a low security. A basic requirement of security is that the intruder must not be able to attack the system by using approximate parameters with a

Manuscript received April 24, 2002; revised November 4, 2002. This paper was recommended by Associate Editor C.-W. Wu.

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

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

Digital Object Identifier 10.1109/TCSI.2003.809808

small decryption error. In the chaotic secure communication systems, chaotic-system parameters play the key role in secure transmission. Thus, to improve the security, we need to increase the sensitivity to system parameters mismatch.

There are two objectives in this brief. One is to derive less conservative impulsive synchronization condition for Chua's circuit, so that a larger bound on the impulsive interval can be obtained and it improves the efficiency of bandwidth utilization. The other is to increase the parameter sensitivity of chaotic self-synchronization systems by the concept of a magnifying glass, so that the security level of the cryptosystem based on chaotic systems can be enhanced. The magnifying glass enlarges and observes minor parameter mismatch and this greatly increases the sensitivity of the cryptosystem. By digitizing the message signals, the system can be used in all types of digital security transmission purposes such as text, image, email transmissions and so on. In this brief, we use audio transmission as an application example.

The organization of this brief is as follows. In Section II, a detailed chaotic cryptosystem is presented. In Section III, a new sufficient condition for the stabilization and the synchronization of Chua's circuit is derived. In particular, a larger impulsive interval is derived. Section IV contains the security analysis of the proposed system. In Section V, an application example of audio transmission system is presented. Finally, some concluding remarks are given in Section VI.

II. New Chaotic Cryptosystem

In this section, a general chaotic cryptosystem that is essentially a stream cipher system is proposed. Chaotic systems are characterized by their sensitivity to initial conditions, random-like behavior, and continuous broadband power spectrum. The central problem in stream cipher cryptography is the difficulty of efficiently generating long running-key sequences from a short and random key [1], [15]. In chaotic cryptosystems, the sequences of binary random variables based on chaotic dynamics are used as the running-key sequences.

The chaotic cryptosystem is mainly composed of two parts: an encrypter and a decrypter. We use Chua's circuits, which have been proven mathematically to be chaotic in the sense of Shil'nikov's theorem, to implement the chaotic system. The details of each part are described as follows.

A. Encrypter

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

$$\begin{cases} \dot{x}_1 = k\alpha(x_2 - x_1 - f(x_1)) \\ \dot{x}_2 = k(x_1 - x_2 + x_3) \\ \dot{x}_3 = k(-\beta x_2 - \gamma x_3) \end{cases} \tag{1}$$

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

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

and where m_0 and m_1 are two negative constants and $m_0 < m_1$. In this Chua's circuit, α, β, γ, m_0 and m_1 are the key parameters and the receiver circuit needs to have these same parameters to ensure synchronization.

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

$$A = \begin{bmatrix} -k\alpha & k\alpha & 0 \\ k & -k & k \\ 0 & -k\beta & -k\gamma \end{bmatrix}. \tag{3}$$

Let ν denote the largest eigenvalue of matrix $(A + A^T)$, i.e., $v = \lambda_{\max}(A + A^T)$.

We further define the following function:

$$\begin{aligned} \chi(\varsigma_1, \varsigma_2) = {} & \max\{\varsigma_1 - 2k\alpha + 2|\alpha m_0|, (1+\alpha)^2/\varsigma_1 \\ & + (\beta - 1)^2/\varsigma_2 - 2k, \varsigma_2 - 2k\gamma\}, \\ & \varsigma_1 > 0; \quad \varsigma_2 > 0. \end{aligned} \tag{4}$$

We are interested in the following set of $(\varsigma_1, \varsigma_2)$

$$\Xi = \{(\varsigma_1, \varsigma_2) | \chi(\varsigma_1, \varsigma_2) < v + 2|\alpha\ m_0|\}. \tag{5}$$

Clearly, if $|\alpha\, m_0| > 0$, then Ξ is a nonempty set.

In our system, the signals are transmitted through a digital channel, therefore the synchronization pulses should be first quantized by a predefined quantizer $Q(\cdot)$, which depends on the amplification factor K used in (6). A fix length of binary bits is used to code each synchronization pulse.

We shall use the state variables of the chaotic circuit to provide the desired key sequence. To further enhance the security of the cryptosystem, we introduce the concept of a magnifying glass, which is composed of an amplifier and an observer.

The amplifier

$$k'(t) = K\left(x_1^2(t) + x_2^2(t) + x_3^2(t)\right)^{1/2}. \tag{6}$$

The observer

$$k(t) = \lfloor k'(t) \rfloor \tag{7}$$

where K is a large number which can be chosen arbitrarily and $\lfloor a \rfloor$ is the integer truncation of a. K is a key design parameter and should be known exactly to the decrypter circuit.

The scrambled signal v_R is given by

$$v_R(t) = E(p(t), k(t)) \tag{8}$$

where $p(t)$ is plaintext, $k(t)$ is key sequences, $E(\cdot,\cdot)$ is an applied stream cipher function and can be chosen according to different system demand.

B. Decrypter

The impulsive differential system in the decrypter is given by

$$\begin{cases} \dot{\tilde{x}}_1 = k\alpha(\tilde{x}_2 - \tilde{x}_1 - f(\tilde{x}_1) \\ \dot{\tilde{x}}_2 = k(\tilde{x}_1 - \tilde{x}_2 + \tilde{x}_3), \qquad t \neq \tau_n, \quad n = 1, 2, \ldots \\ \dot{\tilde{x}}_3 = k(-\beta\tilde{x}_2 - \gamma\tilde{x}_3) \end{cases} \tag{9}$$

and

$$\begin{bmatrix} \tilde{x}_1(\tau_n) \\ \tilde{x}_2(\tau_n) \\ \tilde{x}_3(\tau_n) \end{bmatrix} = \begin{bmatrix} \tilde{x}_1(\tau_n^-) \\ \tilde{x}_2(\tau_n^-) \\ \tilde{x}_3(\tau_n^-) \end{bmatrix} - B \begin{bmatrix} Q(x_1(\tau_n)) - \tilde{x}_1(\tau_n^-) \\ Q(x_2(\tau_n)) - \tilde{x}_2(\tau_n^-) \\ Q(x_3(\tau_n)) - \tilde{x}_3(\tau_n^-) \end{bmatrix}, \quad n = 1, 2, \ldots \tag{10}$$

where B is a 3×3 matrix to be designed to satisfy certain inequality, $Q(\cdot)$ is a predefined quantizer, $\{\tau_n\}(1 \le n < \infty)$ satisfy

$$0 < \tau_1 < \tau_2 < \cdots < \tau_n < \tau_{n+1} < \cdots, \ \tau_n \to \infty \text{ as } n \to \infty$$

with $\tau_n = \sum_{i=1}^{n} T_i$; T_i are impulsive time intervals; τ_n^- are the times immediately prior the times τ_n. The upper bound $\Delta_i (1 \le i < \infty)$ of each impulsive interval T_i in our scheme are defined as follows:

$$\Delta_{2j-1} = \hat{T}_1 \quad \Delta_{2j} = \hat{\xi}_1 \hat{T}_1, \qquad 1 \le j \le \infty. \tag{11}$$

In (11), $\hat{\xi}_1$ is a positive number and is determined by the parameters of Chua's circuit. A typical example is given by $\hat{\xi}_1 = |m_1|$. In our scheme, matrix B and $\hat{T}_1$ are to be designed to ensure the synchronization of the two chaotic systems (1) and (9) in the transmitter and the receiver, respectively. The value of $\hat{T}_1$ is exactly the same as the length of the first packet from the encrypter to the decrypter.

In the decrypter, the plaintext is recovered via

$$\tilde{k}(t) = \left\lfloor K(\tilde{x}_1^2(t) + \tilde{x}_2^2(t) + \tilde{x}_3^2(t))^{1/2} \right\rfloor \tag{12}$$

$$\tilde{p}(t) = D(v_R(t), \tilde{k}(t)) \tag{13}$$

where $\tilde{p}(t)$ is the recovered encrypted signal, $D(\cdot, \cdot)$ is the corresponding decryption function, and $\tilde{k}(t)$ is recovered in the receiver circuit and should approximate $k(t)$. If the chaotic systems in the decrypter and encrypter are synchronized, the decrypter can find the same $\tilde{k}(t)$, as in the encrypter, $k(t)$.

III. Stabilization and Synchronization of Chua's Circuit

In this section, we shall derive some less conservative conditions for the stabilization and the synchronization of Chua's circuit.

For simplicity, we denote $\varsigma_{10}, \varsigma_{20}$ such that $\chi(\varsigma_{10}, \varsigma_{20}) = \min_{\varsigma_1>0, \varsigma_2>0} \chi(\varsigma_1, \varsigma_2)$, then it can be easily known that

$$\chi(\varsigma_{10}, \varsigma_{20}) < \nu + 2|\alpha m_0|. \tag{14}$$

Introducing the following impulsive control:

$$u(k, X(t)) = BX(t), \qquad t = \tau_n, \qquad n = 1, 2, \ldots \tag{15}$$

We then have the following result.

Theorem 1: The origin of Chua's circuit (1) under impulsive control (15) is asymptotically stable if

$$0 \le \chi(\varsigma_{10}, \varsigma_{20}) \le -2\ln(\xi d_1)/(1 + \hat{\xi}_1)\hat{T}_1 \tag{16}$$

where $\xi > 1$, and d_1 is the largest eigenvalue of $(I + B)^T(I + B)$.

Proof: Choose the Lyapunov function as $V(X) = X^T X$. It follows that $\dot{V}(X) \le \chi(\varsigma_{10}, \varsigma_{20})\|X\|^2$. Similar to the proof of Theorem 2 in [14], the origin of Chua's circuit under impulsive control (15) can be proven to be asymptotically stable. □

Remark 1: Note that the condition for asymptotic stability of Chua's circuit provided in [14] is given by

$$0 \le v + 2|\alpha m_0| \le -2\ln(\xi d_1)/(1 + \hat{\xi}_1)\hat{T}_1.$$

From (16), it is clear that our condition is less conservative. This means that it is easier for the designer to design the impulsive intervals. □

We shall next examine the synchronization of the two Chua's circuits, which are called the driving system and the driven system, respectively in [7] and [14]. In an impulsive synchronization configuration, the driving system is given by (1), whereas the driven system is given by (9).

From (1) and (9), we let $e^T = (e_1, e_2, e_3) = (x_1 - \tilde{x}_1, x_2 - \tilde{x}_2, x_3 - \tilde{x}_3)$ be the synchronization error and $\tilde{X} = (\tilde{x}_1, \tilde{x}_2, \tilde{x}_3)^T$. We then have

$$\begin{cases} \dot{e} = Ae + \Psi(X, \tilde{X}), & t \ne \tau_n, \quad n = 1, 2, \ldots \\ e(\tau_n) = (I + B)e(\tau_n^-) + B(X(\tau_n^-) - Q(X(\tau_n^-)), \\ \qquad n = 1, 2, \ldots \end{cases} \tag{17}$$

where

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

For a constant ξ satisfying $\xi > 1$ and $\xi d_1 < 1$, we define the following time interval bounds:

$$\Delta_1 = -2\ln(\xi d_1)/(1 + \hat{\xi}_1)\chi(\varsigma_{10}, \varsigma_{20})$$
$$\Delta_2 = -2\hat{\xi}_1\ln(\xi d_1)/(1 + \hat{\xi}_1)\chi(\varsigma_{10}, \varsigma_{20}). \tag{18}$$

In view of the fact that we cannot transmit the ciphertext before the two Chua's circuits (1) and (9) are synchronized; it is important to make the synchronization time as short as possible. To achieve this, the impulsive intervals should be as small as possible and for this the constant ξ is chosen to be as large as possible. For example, we choose the impulsive intervals for synchronization as $\Delta_1/4$ and $\Delta_2/4$, respectively.

We then have the following result on synchronization time.

Lemma 1: For any $\varepsilon > 0$, we define n_0 as follows:

$$n_0(\varepsilon) = \log_{\xi_1}\|e_0\|/(\varepsilon - (\xi_1\varpi/(\xi_1 - 1))q) \tag{19}$$

where e_0 is the initial error vector, q is the quantization parameter

$$\xi_1 = \xi\exp((3/8)\chi(\varsigma_{10}, \varsigma_{20})(\Delta_1 + \Delta_2)) \tag{20}$$

$$\varpi = (1/2)d_1^{1/2}\|B\|(\exp(\chi(\varsigma_{10}, \varsigma_{20})(\Delta_1 + \Delta_2)/8) + \exp(\chi(\varsigma_{10}, \varsigma_{20})\max\{\Delta_1, \Delta_2\}/8)). \tag{21}$$

If $n \ge n_0(\varepsilon)$, then $\|e(\tau_{2n}, t_0, e_0)\| < \varepsilon$.

Proof: Define a function $V(e)$ for the system (17) as follows:

$$V(e) = \sqrt{e^T e} = \|e\|. \tag{22}$$

It follows that

$$\dot{V}(e) \le (1/2)\chi(\varsigma_{10}, \varsigma_{20})V(e). \tag{23}$$

Similarly from (17), we have

$$V(e(\tau_n)) \le d_1^{1/2}V(e(\tau_n^-)) + (1/2)\|B\|q. \tag{24}$$

We then have

$$V(e(\tau_{2n}, t_0, e_0)) \le V(e_0)/\xi_1^n + (\xi_1\varpi/(\xi_1 - 1))q. \tag{25}$$

Thus, when $n \ge n_0(\varepsilon)$, we have $\|e(\tau_{2n}, t_0, e_0)\| < \varepsilon$. □

After the two Chua's circuits are synchronized, it is desirable to have larger impulsive intervals so that the utilization of channel bandwidth can be significantly improved. To achieve this objective, the constant ξ is chosen to be as small as possible. We also have to maintain the synchronization of Chua's circuit after the impulsive intervals are increased. This is given by the following result.

Theorem 2: For any $\varepsilon > 0$, we denote

$$\tilde{\varepsilon} = \min\{(\varepsilon/(\exp(\chi(\varsigma_{10}, \varsigma_{20})\max\{\Delta_1, \Delta_2\}/2) - \|B\|q/2)d_1^{-1/2}, (\varepsilon - \tilde{\varpi}\ q)\xi\} \tag{26}$$

where

$$\tilde{\varpi} = (1/2)d_1^{1/2}\|B\|(\exp(\chi(\varsigma_{10}, \varsigma_{20})(\Delta_1 + \Delta_2)/2) + \exp(\chi(\varsigma_{10}, \varsigma_{20})\max\{\Delta_1, \Delta_2\}/2)). \tag{27}$$

When $n \ge n_0(\tilde{\varepsilon})$, we have $|\|X\| - \|\tilde{X}\|| < \varepsilon$.

Proof: The proof is similar to that of Lemma 1. □

Based on the above results, our system will work as follows. At the beginning, the constant ξ is chosen as large as possible, the impulsive intervals are chosen as $\Delta_1/4$ and $\Delta_2/4$, respectively. After the two Chua's circuits are synchronized, the constant ξ is then chosen to be as small as possible, and the impulsive intervals are chosen to be closer to Δ_1 and Δ_2, respectively.

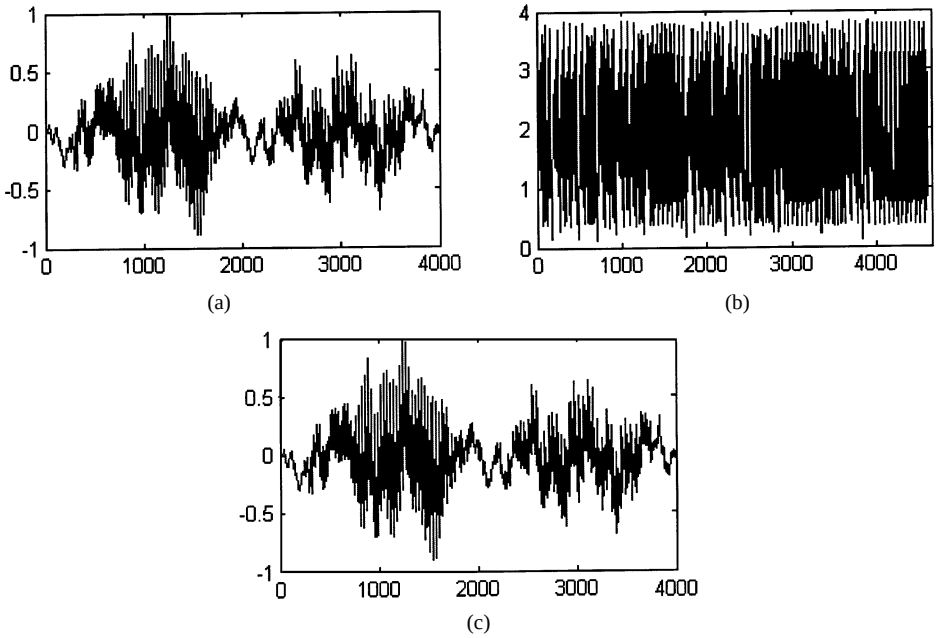

Fig. 1. Simulation results with speech signal. (a) Original speech signal. (b) Transmitted signal. (c) Recovered speech signal.

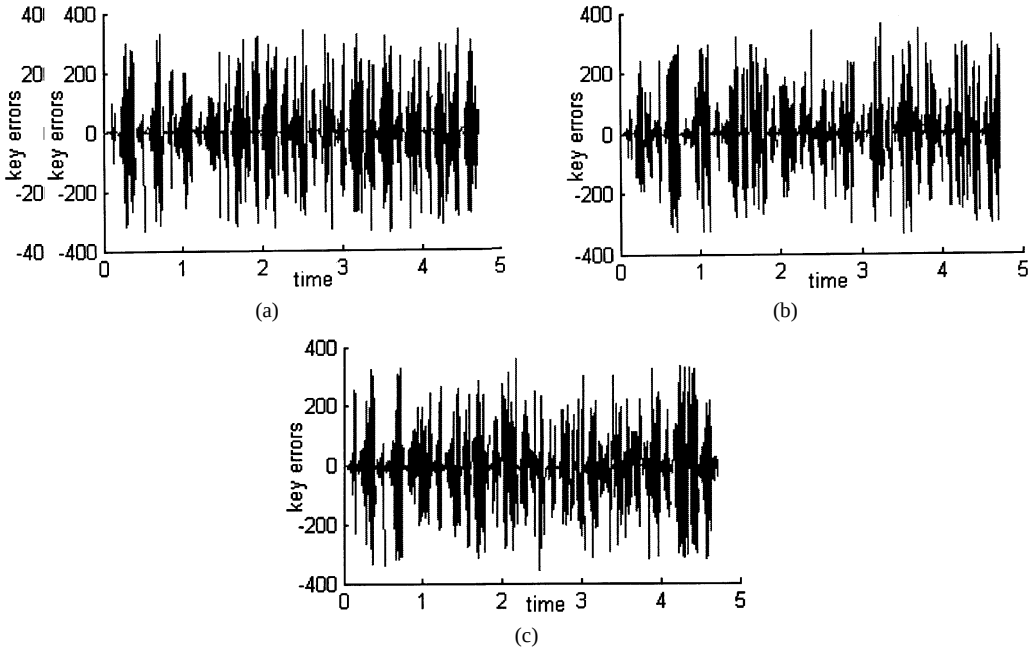

Fig. 2. The error between the key sequences in the encrypter and decrypter when there is 1% parameter mismatch in (a) α; (b) β; and (c) m_0; respectively.

Before we end this section, we shall analyze the effectiveness of our proposed secure chaotic secure communication system. Let the average effectiveness factor of n time frames be given by

$$\mathrm{ATN}\ (\mathrm{i},\ \mathrm{n}) = 1 - \mathrm{nL} \Big/ \sum_{\mathrm{l}=1}^{\mathrm{n}} \mathrm{T_{i+l}} \tag{28}$$

where L is the length of the synchronization impulses.

Then, the effectiveness factor of a scheme can be defined as

$$\mathrm{STE} = \lim_{\mathrm{n}\to\infty} \mathrm{ATE}(0,\ \mathrm{n}). \tag{29}$$

Obviously, the greater the STE, the higher is the effectiveness of the scheme.

For the purpose of comparison, we let STE, $S\hat{T}E$ and $S\tilde{T}E$ denote respectively the effectiveness factors of the schemes in [7], [14] and the present approach. Then the maximum effectiveness of the various schemes is

$$\mathrm{STE}_{\max} = 1 - L(v + 2|\alpha\ m_0|)/|\ln(\xi\ d_1)| \tag{30}$$

$$S\hat{T}E_{\max} = 1 - L(v + 2|\alpha\, m_0|)/|\ln(\xi\ d_1)| \tag{31}$$

$$S\tilde{T}E_{\max} = 1 - L\chi(\varsigma_{10},\ \varsigma_{20})/|\ln(\xi\ d_1)|. \tag{32}$$

Clearly, the effectiveness of the present scheme is improved when compared to the schemes proposed in [7] and [14].

IV. Security Analysis

In the proposed scheme, we have used the magnifying glass to transform the chaotic state variables into key sequences before encrypting

the message signal. Assuming that there is a small mismatch that results in $\Delta x_i(t) = \sigma_i (i = 1, 2, 3)$, then the signal getting through the amplifier has

$$\tilde{k}(t) = \left\lfloor K \left(\sum_{i=1}^{3} (\tilde{x}_i(t) + \sigma_i)^2 \right)^{1/2} \right\rfloor.$$

Since the parameter K is a large number, any mismatch will be enlarged many times. Thus, even a minor mismatch of the parameters will produce a large decryption error, resulting in an incorrect decryption key sequence.

The design of the value of K is related to the asymptotic stable time of the chaotic system and the desired precision of the system. A larger K will produce a more secure system but it requires more synchronization time. Thus, in practice, a tradeoff is required when we choose the value of K.

To recover the plaintext, the two chaotic systems in encrypter and decrypter must be synchronized to get the same key sequences. The intruder who wants to eavesdrop the transmission message must know not only the exact parameters and the structure of the chaotic system but also the synchronization impulses. Since the lengths of impulsive intervals are not constant in our system, it is difficult to perform the inverse prediction and to identify the synchronization impulses and the scrambled signal if the lengths of impulsive intervals are unknown.

V. Secure Speech-Transmission System

In this section, we design a secure speech-transmission system using the proposed chaotic cryptosystem. The speech is compressed by a linear prediction coding (LPC) [16] before being encrypted. The stream cipher encryption function is chosen as

$$E(p(t), k(t)) = k(t) + p(t).$$

The information signal is considered as an additional noise added to the driving signal. It becomes "invisible" within the chaotic signal. Moreover, in order to reduce the transmission burden, we need to decrease the amplitude of the transmitted signal in practice. So, when the scrambled signal v_R is obtained, the actual transmitted signal is that divided by K. Therefore, in the receiver, the received signal needs to be increased K times before decryption.

The parameters chosen for our simulation are as follows. In the two Chua's circuits, the initial conditions are given by $[x_1(0)\, x_2(0)\, x_3(0)] = [-2.12\ -0.05\ 0.8]$ and $[\tilde{x}_1(0)\, \tilde{x}_2(0)\, \tilde{x}_3(0)] = [-0.2\ -0.2\ 0.1]$, respectively. That is, the encrypter and the decrypter are initially not synchronized. Just as in [17], we let $k = 1$, $m_0 = -1.138\,411\,196$, $m_1 = -0.722\,451\,121$, and $\alpha = 9.351\,590\,850$, $\beta = 14.790\,313\,805$, $\gamma = 0.016\,073\,965$. It can be easily computed that $v = 14.4069$, $\varsigma_{10} = 14.25$, $\varsigma_{20} = 16.8705$, $\chi(\varsigma_{10}, \varsigma_{20}) = 16.8385$.

We choose the impulsive controller as $\hat{\xi}_1 = 0.5$, $B = [-1.05\ 0\ 0;\ 0\ -1\ 0;\ 0\ 0\ -1]\theta = -1.05$. Then, $d_1 = 0.0025$. For any ξ satisfying $\xi > 1$ and $0 < |\xi d_1| \leq 1$, we choose $\xi = 300$ at the beginning. After the two Chua's circuits are synchronized, choose $\xi = 1.1$. We have $\Delta_1(300) = 2.275 \times 10^{-2}$, $\Delta_2(300) = 1.137 \times 10^{-2}$ and $\Delta_1(1.1) = 12.76 \times 10^{-2}$, $\Delta_2(1.1) = 6.38 \times 10^{-2}$. As a comparison, their values in [14] can be computed as $\Delta_1(300) = 1.07 \times 10^{-2}$; $\Delta_2(300) = 5.4 \times 10^{-3}$, and in [7], $\Delta_{\max}(300) = 8.03 \times 10^{-3}$. Therefore, in our scheme, the upper bounds of impulsive interval are greatly improved.

In our experiments, we choose the impulsive intervals as $T_{2i-1} = 5 \times 10^{-3}$ s and $T_{2i} = 2 \times 10^{-3}$ s at the beginning and choose them as $T_{2i-1} = 1.2 \times 10^{-1}$ s and $T_{2i} = 6 \times 10^{-2}$ s after the two Chua's circuits are synchronized. We use $K = 100$. The quantizer step is $q = 5 \times 10^{-8}$.

In the transmitter LPC analysis, the original speech signal is divided into frames of size 20 ms (160 samples), with an overlap of 10 ms (80 samples). Fig. 1 shows the simulation results of the speech signal. Fig. 1(a) is the original speech signal, the word "matlab." Fig. 1(b) is the transmitted signals and Fig. 1(c) is the recovered signal.

To illustrate the effectiveness of the proposed system, we study its sensitivity when there is parameter mismatch in Chua's circuit. We investigate the cases when α, β, and m_0 have 1% mismatch in the receiver, respectively. Fig. 2 shows the key sequences errors between the encrypter and the decrypter. We can see that the error signals are not stable, that is, the key sequences in the encrypter and the decrypter are completely different. The original speech signal cannot be recovered from the incorrect reflection coefficients and the residual signal in the receiver.

VI. Conclusion

We have proposed minor parameter mismatch and using an impulsive control synchronization strategy, the proposed system is shown to be sensitive to parameter mismatch and it improves the security of the chaotic secure communication system.

References

[1] M. P. Kennedy, R. Rovatti, and G. Setti, *Chaotic Electronics in Telecommunication*. Boca Raton, FL: CRC Press, 2000.

[2] L. K. Pecora and J. L. Carroll, "Synchronization in chaotic systems," *Phy. Rev. Lett.*, vol. 64, no. 2, pp. 821–824, 1990.

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

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

[5] U. Feldmann, M. Hasler, and W. Schwarz, "Communication by chaotic signal: The inverse system approach," in *Proc. IEEE ISCAS'95*, 1995, pp. 680–683.

[6] 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.

[7] T. Yang and L. O. Chua, "Impulsive stabilization for control and synchronization of chaotic systems: Theory and application to secure communication," *IEEE Trans. Circuit Syst. I*, vol. 44, pp. 976–988, Oct. 1997.

[8] T. Yang, "Chaotic secure communication systems: History and new results," *Telecomm. Rev.*, vol. 9, no. 4, pp. 597–631, 1999.

[9] 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. 391–403, Mar. 2000.

[10] 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.

[11] K. M. Short, "Steps toward unmasking secure communication," *Int. J. Bifurcation Chaos*, vol. 4, no. 4, pp. 959–977, 1994.

[12] ——, "Unmasking a modulated chaotic communications scheme," *Int. J. Bifurcation Chaos*, vol. 6, no. 2, pp. 611–615, 1996.

[13] Z. G. Li, C. Y. Wen, and Y. C. Soh, "Analysis and design of impulsive control system," *IEEE Trans. Automatic Control*, vol. 46, pp. 894–897, June 2001.

[14] 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.

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

[16] A. Nejat Ince, *Digital Speech Processing: Speech Coding, Synthesis, and Recognition*. Norwell, MA: Kluwer Academic, 1992.

[17] R. N. Madan, *Chua's Circuit: A Paradigm for Chaos*. Singapore: World Scientific, 1993.

[18] M. Itoh, T. Yang, and L. O. Chua, "Conditions for impulsive synchronization of chaotic and hyperchaotic systems," *Int. J. Bifurcation Chaos*, vol. 11, no. 2, pp. 551–560, 2001.

[19] T. Yang, *Impulsive Control Theory*. Berlin, Germany: Springer-Verlag, Aug. 2001, vol. 272.

[20] ——, *Impulsive Systems and Control: Theory and Applications*. Huntington, NY: Nova Science, Sept. 2001.