AN INVERSION APPROACH FOR CHAOS-BASED SECURE DIGITAL COMMUNICATIONS

Yufan Zheng[1], *Guanrong Chen*[2], *Ran Yang*[1]

[1] Department of Electrical and Electronic Engineering
The University of Melbourne, Parkville, VIC. 3010, Australia
email: y.zheng@ee.mu.oz.au
[2] Department of Electronic Engineering
City University of Hong Kong, P. R. China
email: gchen@ee.cityu.edu.h

ABSTRACT

A new approach to real-time digital secure speech communication is proposed based on the inversion theory of nonlinear discrete-time dynamical systems. The proposed approach uses an observable minimal-phase nonlinear discrete-time dynamical system, particularly with chaotic zero-dynamics, as the drive system to generate encrypted message signals for transmission. The receiver is the minimal left-inverse system of the drive system with the capability of synchronization. The receiver decrypts the received signal, recovers the original message in real-time. The effectiveness of the proposed approach and design is demonstrated via several examples for secure speech signals transmission. Performance evaluation of the designed secure communication system is discussed. Both analysis and simulation show that the new scheme is secure, simple, accurate and robust.

1. INTRODUCTION

Since the late 1980s [1, 2] the possibility for self-synchronization of chaotic oscillations has initiated an avalanche of results on possible application of chaos to cryptography [3, 4, 5]. It is now known that due to some intrinsic difficulties of synchronization-based communication schemes, such as channel noise effect, transient information loss, time-delay effect, and the lack of a solid foundation of cryptanalysis, the impact of this approach on the conventional cryptography research has been quite limited. Nevertheless, this approach still has some promising features and potential for further studies, particularly if some new design schemes can be developed to address the aforementioned issues[6, 3].

Regarding nonlinear systems theory, on the other hand, system inversion is one of the fundamental concepts, which has a broad spectrum of applications. Here, roughly speaking, a (left) inverse system problem is as follows: given the output of a (probably unknown) system, determine the input that produces this output through the system, in which the underlying system is in some sense "reversed." Based on this concept, in secure communications an encrypted signal can be considered as the output of a system, generated by an input message signal, and the objective is to recover the message signal from the received (encrypted) signal.

The inverse systems scheme was first proposed in [7, 8] for chaotic communications, where the encoder is a non-autonomous chaotic system. Very recently another approach, which can be classified as inverse system scheme, was proposed by [9]. [9] uses autonomous chaotic system to encrypt the message signal. For [8, 9] the drive system has to satisfy certain special conditions and an observer-based receiver is designed to asymptotically recover the original message. Therefore, only very special invertible input-output system and chaotic model can be used as drive system. Therefore, the method suggested in [8, 9], although elegant ideally, is quite restrictive practically.

In this paper, the newly proposed approach combines some existing theories and methods from chaotic dynamics, minimal inversion of nonlinear dynamical systems, and cryptography into a platform of digital secure communication. The objective is to achieve a practical real-time chaos-based secure communication system design that preserves the merits of both digital encryption and chaotic communication, while bypassing the aforementioned limitations of most existing synchronization-based transmission schemes.

2. MINIMAL-ORDER LEFT-INVERSION OF NONLINEAR SYSTEM

We consider the following discrete-time nonlinear multi-input multi-output system in the state space form:

$$\begin{aligned} x[k+1] &= f(x[k],u[k]) \\ y[k] &= h(x[k],u[k]) \end{aligned} \tag{1}$$

where $x[k] \in \mathbf{R}^n$, $u[k] \in \mathbf{R}^m$, $y[k] \in \mathbf{R}^p$ are the state, input, and output vectors, respectively.

The following dynamical system is a left-inverse system of system (1):

$$\begin{aligned} z[k+1] &= \psi(z[k],y[k],y[k+1],\cdots,y[k+r]) \\ w[k] &= \eta(z[k],y[k],y[k+1],\cdots,y[k+r]) \end{aligned} \tag{2}$$

where $z[k] \in \mathbf{R}^q$ and r is a positive integer, if the output $w[k]$ of system (2) is equal to the input of system (1), provided that $\{y[k],y[k+1],\cdots,y[k+r]\}$ for some $r \geq 0$ and for all $k \geq 0$, are taken as the input vectors of system (2) for some initial state $z[0]$.

The largest observable and uncontrollable subsystem is called as the zero dynamics of an SISO nonlinear system in this paper. A (linear or nonlinear) system is called minimal-phase dynamical system if its zero-dynamics is *Lyapunov* stable.

Compared with linear systems, the zero dynamics of a nonlinear system may have a much more complicated struc-

ture. In fact, the zero dynamics of an observable SISO linear system only consists of *signal* dynamics.

For an observable SISO nonlinear system, however, the zero dynamics could consist of several *independent* dynamics (see Figure 1).

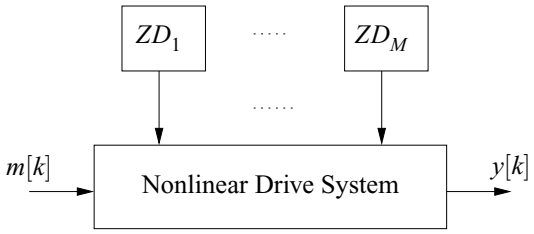

Figure 1: The dynamical structure of a nonlinear system with several zero dynamics.

As we will use the zero dynamics to generate the chaotic encrypted signals, which is bounded, of original information signals for transmission in public communication channels, it is asked that all zero-dynamics are *Lyapunov* stable. I.e. we always adopt the observable, minimal-phase, left-invertible dynamical systems for our purpose.

The following theorem, which is a direct consequence of the results in [10], will be useful in the next section.

Theorem 2.1 *When system (1) is single input system, then it is left-invertible if and only if the relative degree of y is less then n.*

3. DESIGNED SCHEME OF SCRAMBLER/DESCRAMBLER

There are some chaotic communication schemes proposed in order to encrypt message signals: *Chaotic Masking, Chaotic Shift Keying, Chaotic Modulation/Inverse System* [3, 5, 11]. Our approach may belong to the category of *Chaotic Modulation/Inverse System*, but not exactly.

In chaotic masking the chaotic signal $x_c[k]$ is added to the message signal $m[k]$, forming the transmitted signal $y[k]$, as

$$y(k) = x_c(k) + m(k)$$

for $k \geq 0$.

Another type encoder uses the modulation by multiplication. The resultant modulated sequence is, for $k \geq 0$,

$$y[k] = x_c[k] \cdot m[k]$$

When the chaotic signal $x_c[k]$ is not strong enough, our simulations show that the two types of encrypted signals have strong cross-correlation between encrypted signal $y[k]$ and message signal $m[k]$. The waveform of encrypted signal $y[k]$ contains obviously residual information of message signal $m[k]$. Our simulation results also show that the encrypted signal is insensitive to the initial condition of chaotic dynamics for the scheme of modulation by multiplication chaotic signal. On the other hand, if the chaotic signal $x_c[k]$ is too strong, the robustness against transmission disturbance is reduced dramatically.

In this section, to prepare for the chaos-based secure communication system design, we consider

$$x_c[k+1] = \tilde{f}(x_c[k]) \tag{3}$$

which consists of one or several chosen chaotic dynamical systems. The general form of a drive system is constructed as

$$\begin{aligned} x_c[k+1] &= \tilde{f}(x_c[k]) + \tilde{g}(x[k], u[k]) \\ x[k+1] &= \hat{f}(x_c[k], x[k], u[k]) \\ y[k+1] &= h(x_c[k], x[k]) \end{aligned} \tag{4}$$

In the proposed design, the following assumption is made.

Assumption 1 *The drive system* (4) *is always designed to be an observable and left-invertible nonlinear system.*

Firstly, we design several chaotic systems. The following are two models used in our design.

$$x_{c1}[k+1] = -3x_{c1}[k] + 4x_{c1}^3[k] \tag{5}$$

and

$$\begin{aligned} x_{c21}[k+1] &= 1 + 0.3x_{c22}[k] - 1.4x_{c21}^2[k] \\ x_{c22}[k+1] &= x_{c21}[k] \end{aligned} \tag{6}$$

The system (5) is called Cubic Map and the system (6) is a Henon Map.

The chaotic behaviors of systems (5) and (6) appear when initial conditions $x_{c1}[0]$ and $x_{c21}[0], x_{c22}[0]$ belong to some subsets of their state spaces, respectively.

It is well-known that the system dynamics are very sensitive to the initial states. Furthermore, it is worth noting that because of their random property, chaotic signals have impulse-like auto-correlation functions and wide-band power (white-noise-like) spectrum. Also, cross-correlation function of two chaotic signals has a very small value. It is also shown that the two signals generated by two chaotic systems (5) and (6) appear independent stochastic process property. The cross-correlation function of the two signals has very low value, too.

The systems (5) and (6) may be embedded into the drive system in the following way:

$$\begin{aligned} x_{c1}[k+1] &= -3x_{c1}[k] + 4x_{c1}^3[k] \\ x_{c21}[k+1] &= 1 + 0.3x_{c22}[k] - 1.4x_{c21}^2[k] \\ x_{c22}[k+1] &= x_{c21}[k] \\ x[k+1] &= \tfrac{1}{2}(1 - x[k])x_{c1}[k] + \tfrac{1}{2}x_{c21}[k]u[k] \\ y[k] &= x_1[k] \end{aligned} \tag{7}$$

To verify the observability of drive system (7), one calculates the output signal of the drive system (7) under message signal input $u[k]$ using symbolic algorithm.

The encrypted signal by drive system (7) is of very high security. Fig.2 is the time-domain waveform of a speech signal with sampling rate 22050Hz and its spectrum. Fig.3 is the time domain waveform of the scrambled speech signal by the drive system (7) and its spectrum, where initial values $x_{c1}[0] = 0.1, x_{c21}[0] = 0.1, x_{c22}[0] = 0.1$, and $x[0] = 0.205$.

The simulation results clearly show that the encrypted signal $\{y[k]; k \geq 0\}$ generated by the drive system (7) has much better secure performance. By comparing the two spectrum of the encrypted signal and original message over the frequency between 0KHz-2KHz, where the main power of speech spectrum is located, in Fig.4. There is hardly to

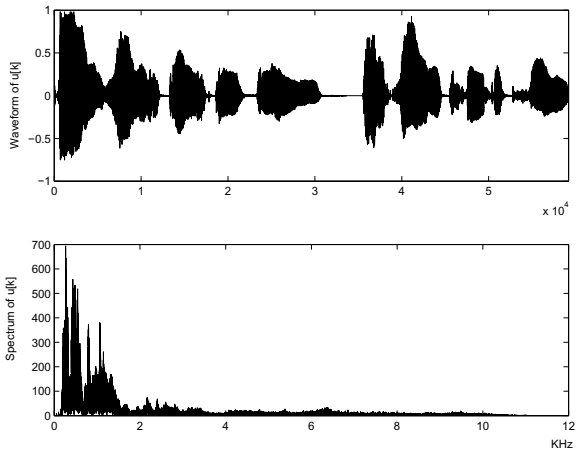

Figure 2: Waveform of original speech signal and its spectra.

find any residual information of original signal in the spectrum of the encrypted signal $\{y[k]; k \geq 0\}$.

It is easy to check that system (7) is left-invertible because $degy = 1$. One can also obtain a minimal left-inverse of system (7) by letting $z_1[k] = x_{c1}[k]$ and $z_{21}[k] = x_{c21}[k]$, $z_{22}[k] = x_{c22}[k]$. As

$$y[0] = x[0],$$
$$y[k+1] = x[k+1] = \tfrac{1}{2}(1-x[k])x_{c1}[k] + \tfrac{1}{2}x_{c21}[k]u[k]$$

one has

$$u[k] = \frac{2y[k+1] - z_1[k](1-y[k])}{z_{21}[k]}$$

Thus, the minimal left-inverse of the drive system (7) is constructed as

$$\begin{array}{rcl} z_1[k+1] & = & -3z_1[k] + 4z_1^3[k] \\ z_{21}[k+1] & = & 1 + 0.3z_{22}[k] + 1.4z_{21}^2[k] \\ z_{22}[k+1] & = & z_{21}[k] \end{array} \tag{8}$$

$$w[k] = \frac{2y[k+1] - z_1[k](1-y[k])}{z_{21}[k]}$$

To get rid of singularity let

$$w[k] = \begin{cases} \frac{2y[k+1] - z_1[k](1-y[k])}{z_{21}[k]}; & if \ z_{21}[k] > 0.1 \\ w[k-1]; & if \ z_{21}[k] \leq 0.1 \end{cases} \tag{9}$$

We can modify the drive model a little bit to avoid such singularity in inverse system. As $z_{21}[k]$ is white-noise like random variable, that $z_{21}[k] \leq 0.1$ is a very rare event. Our simulation shows that the speech message can perfectly restored and (9) is applicable practically. Fig.5 shows some simulation results, where (a) is a piece of the original speech signal; (b) is the encrypted signal, which is the output of the drive system (7); (c) is the encrypted signal (solid line) compared with the original signal (dash line) in a small time scales; (d) shows that the inverse system (8) can recover the original speech signal after decryption.

The drive system consists of two autonomous chaotic dynamics, the encrypted signal is very sensitive to the initial states of the chaotic systems if the initial states belong to some area. Besides, if the initial states are in this area, then the encrypted signal becomes very sensitive to the initial states.

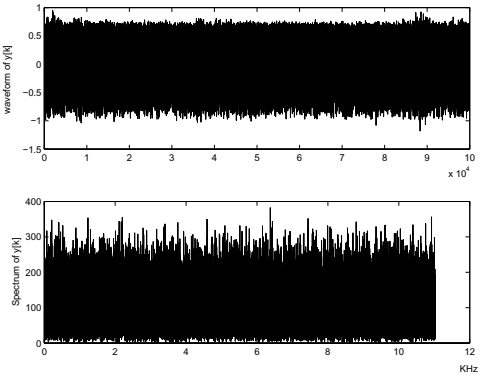

Figure 3: The waveform of the encrypted signal of original message by nonlinear filter (7) and the spectrum of the encrypted signal.

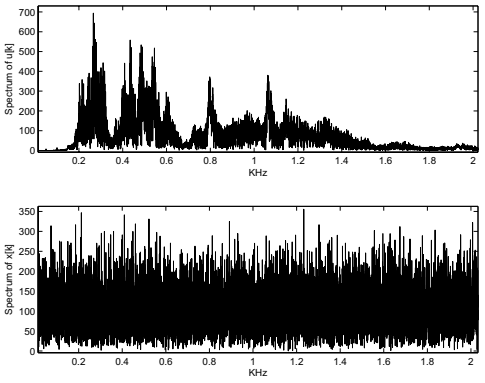

Figure 4: The spectrum of original message and encrypted signal over frequency between 0KHz-2KHz

We can use some values of the initial states of the two chaotic systems as the PIN. The key space, denoted by $\mathscr{K}$, is defined by the total number of the real-valued vectors $\begin{pmatrix} x_{c1}[0] \\ x_{c21}[0] \\ x_{c22}[0] \end{pmatrix} \in \mathscr{K}$, which are sensitive to encrypted signals. In other words, when $\begin{pmatrix} x_{c1}[0] \\ x_{c21}[0] \\ x_{c22}[0] \end{pmatrix} \in \mathscr{K}$, the encrypted signals become very sensitive to the initial states of the two chaotic systems. If the receiver gets a correct key $\begin{pmatrix} z_1[0] \\ z_{21}[0] \\ z_{22}[0] \end{pmatrix}$ such that $z_1[0] = x_{c1}[0]$, $z_2[0] = \begin{pmatrix} z_{21}[0] \\ z_{22}[0] \end{pmatrix} = \begin{pmatrix} x_{c21}[0] \\ x_{c22}[0] \end{pmatrix}$, then the receiver can gets the information message perfectly. When the receiver system use a wrong key, even if it is "very small mistake", then the receiver can not get the message information correctly. For drive system (7), let $x_{c1}[0] = 0.1, x_{c21}[0] = 0.1, x_{c22}[0] = 0.1$, and $x[0] = 0.205$. If $\begin{pmatrix} z_{21}[0] \\ z_{22}[0] \end{pmatrix} = \begin{pmatrix} x_{c21}[0] \\ x_{c22}[0] \end{pmatrix}, z[0] = x[0]$, but $x_{c1}[0] = 0.1 \neq$

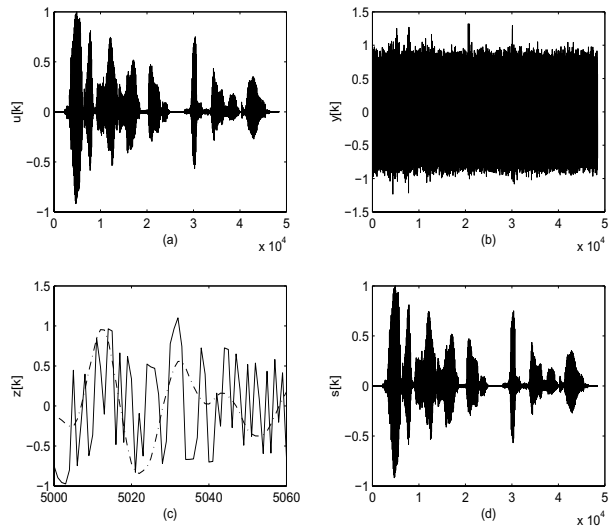

Figure 5: Simulation results of drive and receiver for a piece speech signal

$z_1[0] = 0.1000001$, then it can be seen that the original speech signal cannot be recognized at all.

Our simulations show that the initial state $x_{c1}[0]$ of system (5) is the most sensitive parameter, if $|z_1[0] - x_{c1}[0]| > 10^{-7}$, then the receiver can not get the message information correctly. The initial states $\begin{pmatrix} x_{c21}[0] \\ x_{c22}[0] \end{pmatrix}$ have less sensitive than $x_{c1}[0]$. The $x[0]$ is an insensitive parameter for the drive system (7). Roughly estimate, the key space for the drive system (7) is greater than 10^8 if our calculation is accurate to 7 decimal places.

4. SYNCHRONIZATION

Synchronization is very important to chaos based encryption systems no matter they are analog or digital. There are two groups of identical digital chaos generators, which are located in drive system and receiver separately. The secure communication system works properly if and only if the two groups chaotic signals to start at the same time and from the same initial conditions. The same initial condition is guaranteed if the receiver uses a correct *key*. In our scheme the synchronization can be implemented thanks to the observability of drive system.

As space limitation we will not study synchronization problem intensively in this paper. Some technique problems will be discussed in the following paper.

The proposed technique to synchronize the two chaotic signals was used by [12] called *Impulsive synchronization method*. We assume that the transmitted signal consists of a sequence of frames. Every frame length of N consists of two regions. The first region of the frame is used to check and correct synchronization. The length of the first region is $N_c (\ll N)$, the second region with length N_r is used to transmit the encrypted signal.

In our prototype device we take $N = 128 \times 8 = 1024$ *bits*, where $N_c = 8 \times 8 = 64$ *bits* and $N_r = 964$ *bits*. Each frame carries a piece of 128*ms* speech message. Assume each frame of input signal of drive system is represented by 128 decimal numbers $u[0], u[1], \cdots u[\frac{N_c}{8} - 1], u[\frac{N_c}{8}], \cdots, u[127]$.

As $N_c = 64$ the first region of the k-th frame can represent 8 decimal numbers, which are divided into two group, $u[k], u[k+1], u[k+2], u[k+3]$ and $u[k+4], u[k+5], u[k+6], u[k+7]$. The first 8 decimal numbers, represented by N_c *bits* codes, are secrete to public, but known to receiver. For the k-th frame, one can calculate the value of $y[k+i]$ for $1 \le i \le 8$. On the receiver side one gets data $\hat{y}[k_i]$ for $1 \le k \le 8$ from communication cannel. For the k-th frame we find $\tau \ge 0$ such that the number of i satisfying

$$|\hat{y}[k+i] - y[k+i+\tau]| < \varepsilon, \;\; 0 \le i+\tau \le 8$$

is greater than 4. If $\tau > 0$, then synchronization error takes place. To correct synchronization error let $k+i+\tau := k+i$ the receiver systems is synchronized starting from $k+i+\tau$ in the k-th frame.

REFERENCES

[1] Pecora, L.M. and T.L. Carroll, Synchronizing chaotic systems, *Phys. Review Letters*, Vol.64, No. 8, pp.821-824, 1990.

[2] Carroll, T.L. and L.M. Pecora, Synchronization in chaotic Circuits, *IEEE Trans. Circuts Syst.*, Vol.39, No. 38, pp.453-456, 1991.

[3] Abel, A. and W. Schwarz, Chaos communications - Principles, schemes, and system analysis, *Procedings of the IEEE*, Vol.90, No.5, pp.691-709, May 2002.

[4] Chen, G.(ed) Controlling chaos and bifurcations in Engineering Systems,Boca Raton, FL, USA: CRC Press, 2000.

[5] Lau, F.C.M and C.K. Tse, Chaos-based Digital Communication Systems, Spriner, Berlin, 2003.

[6] Dachselt, F. and W. Schwarz, Chaos and Cryptography, *IEEE Trans. on Circuits and Systems - I: Fundamental Theory and Application*, Vol. 48, No. 12, pp.1498-1509, December, 2001.

[7] Hasler, M., Synchronization principles and applications, in *Circuits and Systems Tutorials*, ed. by C. Toumazou, N. Battersby and S. Porta, IEEE Press, New York, 314-327, 1995.

[8] Feldmann, U., M. Hasler and W. Schwarz, Communication by chaotic signals: the inverse system approach, *Int. J. Circuit Theo and Applications*, Vol.24, pp.551-579, 1996.

[9] Feki, M., B. Robert, G. Gelle, M. Colas, Secure digital communication using discrete-time chaos synchronization, *Chaos Solitons& Fractals*, 18, PP.881-890, 2003.

[10] Zheng, Y.F. and R.J. Evans, Minimal order deiscrete-time nonlinear systems inversion, *Proc. of IFAC-02 World Congress*, Spain, 2002.

[11] Chen, G. and X. Dong, From Chaos to Order: Methodologies, Perspectives and Applications, World Scieitific Pub. Co., Singapore, 1998.

[12] Yang T. and L. O. Chua, Implusive control and synchronization of nonlinear dynamical systems and application to secure communication, *International Journal of Bifurcation and Choas*, Vol. 7, No.3, pp.645-664, 1997.