Secure Communication Based on Hyper-Chaotic Chen System with Time Delay

Hai-Peng Ren, Chao Bai, Zhan-Zhan Huang
Shaanxi Key Laboratory of Complex System Control and Intelligent Information Processing
Xi'an University of Technology, Xi'an, 710048, China
renhaipeng@xaut.edu.cn, moonanimal@sina.com, 182183484@qq.com

Celso Grebogi
Institute for Complex System and Mathematical Biology,
Aberdeen, AB24 3UE, United Kingdom
qreboqi@abdn.ac.uk

Received (to be inserted by publisher)

An experimental secure communication method based on the Chen system with time-delay is being proposed in this paper. The Chen system with time-delay is an infinite-dimensional system having more than one positive Lyapunov exponent. The message to be transmitted is encrypted using an hyper-chaotic signal generated by the Chen system with time-delay and multi-shift cipher function. This encryption makes difficult for an eavesdropper to reconstruct the attractor by using time-delay embedding techniques, return map reconstruction, or spectral analysis, consequently, improving the security. Simulations and experiments on TI TMS320C6713 Digital Signal Processor (DSP) show improved resilience against attack and the feasibility of the proposed scheme.

Keywords: time-delay feedback; active-passive decomposition; hyper-chaos synchronization; n-shift cipher; attacking resilience.

1. Introduction

The idea of using chaos to design secure communication systems and digital ciphers has provoked a great deal of research efforts since the early 1990s [Pecora & Carroll, 1990; Yang, 2004; Ren et al., 2014]. In the fields of secure communication, so far, many ideas and methods have been proposed to tackle the problem of chaotic secure communication, including chaotic masking [Cuomo et al., 2004], chaotic shift keying [Dedieu et al., 1993], chaos modulation [Yang & Chua, 1996], symbolic message bearing method [Hayes, 1993; Ren et al., 2012], and so on [Parlitz et al., 1996; Yang et al., 1997; Minai & Pandian, 1998; Chen et al., 2003; Udaltsov et al., 2003; Bu & Wang, 2004; Hernandez & Serrano, 2005; Ren & Bai, 2015]. Meanwhile, much effort has been devoted to security analysis of the existing chaotic cryptosystems [Wang et al., 2004]; the attacking techniques have also attracted increasing attention [Yang, 1995; Yang et al., 1998a,b; Ren et al., 2008; Kevin, 1994; Perez & Cerdeira, 1995; Kevin & Andrew, 1998; Zhou & Lai, 1999; Ponomarenko & Prokhorov, 2002; Chin et al., 2004; Andrew & Kevin, 2001; Alvarez et al., 2004; Li et al., 2005a]. Chaotic shift keying communication schemes have been reported to be broken by using the short-time zero-crossing rate [Yang, 1995], spectrogram analysis [Yang et al., 1998a], generalized synchronization

2 Ren et al.

[Yang et al., 1998b], and adaptive key identification [Ren et al., 2008]. Some communication schemes using low-dimensional chaotic signals can be unmasked by the dynamical reconstruction of the chaotic system from the time series [Kevin, 1994] or by using a suitable return map [Perez & Cerdeira, 1995]. The results of these efforts have shown that many chaotic communication schemes are not as secure as expected. Some efforts have been devoted to improve the attacking resilience performance, such as hyperchaos communication [Udaltsov et al., 2003; Ren & Bai, 2015], encryption with modulation [Bu & Wang, 2004; Yang et al., 1997], phase synchronization [Chen et al., 2003], and chaotic communication combined with noise [Minai & Pandian, 1998]. However, the outcome of those efforts is limited; the security problems with those new methods were uncovered lately [Kevin & Andrew, 1998; Zhou & Lai, 1999; Ponomarenko & Prokhorov, 2002; Chin et al., 2004; Andrew & Kevin, 2001; Alvarez et al., 2004; Li et al., 2005a].

Just like the relationship between spears and shields, the conflicting efforts both to improve and to crash the security of chaos communication impels the development of chaotic secure communication theory and technology. Both efforts help the development of chaotic communication schemes. As the chaotic communication is reported to be successfully used in commercial fiber optic channel to get higher bit transmission rates [Apostolos & Dimitris, 2005], the chaotic communication research has gained more attention from the practical application viewpoint and the improvement of security using simple system with easy implementation is expected [Ren et al., 2013]. Low dimensional chaotic system has low security, therefore, state-feedback method is often used to introduce a new variable to construct a higher dimensional system, [Li et al., 2005b; Xue et al., 2013; Peng et al., 2014], which makes the system to be more complicated to implement. Hyper-chaos can be generated by time delay [Ren et al., 2006], which is infinite dimensional by definition and it is easy to implement. Chen system with parameters in the chaotic range has a more complicated topology structure and dynamical behavior as compared to the Lorenz system [Ueta et al., 2000]. Chen system with parameters in the non-chaotic range is selected in this work as a paradigm to generate hyper-chaos because it is easy to bring about more complex behaviors with more than one positive Lyapunov exponents [Ren et al., 2006]. In this paper, a chaotic secure communication system is proposed using the hyper-chaotic Chen system and multi-shift cipher scheme to enhance the security. The activepassive decomposition (APD) method [Parlitz et al., 1996] is used to synchronize the Chen system with delay. Two hyper-chaotic signals are used in the proposed scheme. One of the chaotic signals is used to synchronize the chaotic encrypter and the chaotic decrypter. The other is used to encrypt the plain signal in the multi-shift cipher function. Therefore, from this split, several advantages can be obtained. Firstly, a hyper-chaotic signal is used as the transmitted signal, which obstructs the eavesdropper to reconstruct the chaotic attractor using dynamical reconstruction. Secondly, the transmitted signal is not used for masking the message, it is to avoid the return map reconstruction. Thirdly, the multi-shift cipher function is used to encrypt the message transmitted, and to muddle the message with the hyper-chaotic signal. Thus a transmitted signal in the public channel will possess the complicated dependence on the message, on the hyper-chaotic signal and on the multi-shift function. The proposed scheme possesses better attacking resilience performance.

The organization of this paper is given as follows. In Section II, we show the hyper-chaos generated by direct time-delay feedback in the Chen system. In Section III, APD method is used to synchronize two hyper-chaotic Chen systems with time-delay. Then a new method to encode the information with hyper-chaotic signal and n-shift encryption function is presented. Numerical simulations are presented to demonstrate the effectiveness of the proposed scheme. Section IV contains an analysis of attacking resilience of the proposed method. In section V, experiments using digital signal processor (DSP) are conducted to validate the proposed method. Finally, some conclusions are given in Section VI.

2. Hyper-chaos generated by direct time-delay feedback

Hyper-chaotic system is usually defined as a chaotic system with more than one positive Lyapunov exponents, indicating that the chaotic dynamics of the system are expanded in more than one direction [Cafagna & Grassi, 2003]. Hyper-chaos was first reported by Rössler in 1979. Creating a hyper-chaotic attractor, from a non-chaotic or chaotic system with some simple control techniques, is a theoretically very attractive and yet technically quite challenging task [Wang et al., 2000].

Hyper-chaos has been reported to be generated in non-chaotic Chen circuits by using direct time-delay feedback [Ren & Li, 2010]. A typical form of Chen circuits with direct time-delay feedback can be given as follows [Ren et al., 2006]

$$\begin{cases} \dot{x} = a(y-x) \\ \dot{y} = (c-a)x - xz + cy \\ \dot{z} = xy - bz + k(z - z(t-\tau)) \end{cases}$$

$$(1)$$

where a = 35, b = 3, c = 18 are system parameters, k = 2.4 is delay feedback gain and $\tau = 0.5$ is time-delay. The simulation result of this system is shown in Fig. 1.

The dynamics given by Eq. (1) contains time-delay, The dynamics is infinite-dimensional because a continuum of initial conditions over the interval $-\tau < t < 0$ is required to specify the dynamical behavior. By calculating the multiple Lyapunov exponents of the delayed differential equation [Sprott, 2006], we determine that the chaotic system with time-delay has three positive Lyapunov exponents: 0.2219, 0.2216, and 0.0035. Therefore, the chaotic attractor is an infinite-dimensional hyper-chaotic one. It is expected to obtain better performance by using hyper-chaotic Chen system for secure communication.

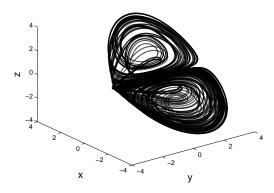


Fig. 1. Chaotic attractor of the hyper-chaotic Chen system with direct time-delay feedback.

Chaotic Communication Scheme Using the Hyper-Chaotic Chen System

3.1. Basic principle of active-passive decomposition synchronization

Consider the following autonomous dynamical system

$$\dot{\mathbf{z}} = \mathbf{F}(\mathbf{z}). \tag{2}$$

It can be rewritten as a non-autonomous system as

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, s),\tag{3}$$

where s is a driving function given by

$$s=h(\mathbf{x}),$$
 (4)

or

$$\dot{s} = h(\mathbf{x}, s). \tag{5}$$

Let

$$\dot{\mathbf{y}} = \mathbf{f}(\mathbf{y}, s) \tag{6}$$

4 Ren et al.

to be a copy of system (3) that is driven by the same signal s. The receiver synchronizes with the transmitter as long as the error system, defined by

$$\mathbf{e} = \mathbf{x} - \mathbf{y}$$

$$\dot{\mathbf{e}} = \mathbf{f}(\mathbf{x}, s) - \mathbf{f}(\mathbf{y}, s) = \mathbf{f}(\mathbf{x}, s) - \mathbf{f}(\mathbf{x} - \mathbf{e}, s),$$
(7)

possesses a stable fixed point at the **e**=0. This can be shown by using stability analysis of the linearized system for small **e** or by using (global) Lyapunov functions. In general, however, the stability has to be checked numerically using the fact that synchronization occurs if all conditional Lyapunov exponents of non-autonomous system (3) are negative. In this case, system (3) is a passive system and the aforementioned decomposition is referred to as active-passive decomposition (APD) of the original dynamical system (2).

3.2. Synchronization of the hyper-chaotic Chen system using APD

The active-passive decomposition of the hyper-chaotic Chen system can be given as

$$\begin{cases} \dot{x}_1 = s - (a-1)x_1 \\ \dot{x}_2 = (c-a+1)x_1 - x_1x_3 + (c-a)x_2 + s \\ \dot{x}_3 = x_1x_2 - bx_3 + k(x_3 - x_3(t-\tau)) \end{cases}$$
(8)

with $s = ax_2 - x_1$, and the corresponding receiver is

$$\begin{cases} \dot{y}_1 = s - (a-1)y_1 \\ \dot{y}_2 = (c-a+1)y_1 - y_1y_3 + (c-a)y_2 + s \\ \dot{y}_3 = y_1y_2 - by_3 + k(y_3 - y_3(t-\tau)) \end{cases}$$
 (9)

The dynamics of the difference of the states $\mathbf{e} = \mathbf{x} - \mathbf{y}$ can be obtained by the difference of (8) and (9). By using the methods proposed in Sun [2004], we can obtain that synchronization can be achieved as shown in Fig. 2(a). The square root error of the system, defined as $e_s = \sqrt{(e_1^2 + e_2^2 + e_3^2)}$, is shown in Fig. 2(b). The range of coupling strength k and the time-delay τ to guarantee the chaotic dynamical behavior of the system and the synchronization between the transmitter and the receiver is shown in Fig. 2(c). The other parameters are the same as that for Eq. (1). We have that the two systems are in synchronization with each other after a short transient state.

3.3. Encoding information with an hyper-chaotic signal and n-shift encryption function

A secure chaotic communication scheme is shown in Fig. 3. At the transmitter end, one state variable of the hyper-chaotic Chen system, referred to as k(t), is used as key to encrypt the plain text p(t) using the n-shift encryption function $e(\bullet)$. The output of the encryption function is y(t). The transmitted signal s(t) is a type of combination of the state variables that is determined by the APD.

At the receiver end, a copy of the hyper-chaotic Chen system driven by the transmitted signal is used to decrypt the plain text. According to the APD method, if the transmitted signal is selected properly, the transmitter hyper-chaotic system and the receiver hyper-chaotic system will synchronize after a transient state from any initial conditions. The corresponding states of both the transmitter and the receiver can be treated as the same. Therefore, the transmitted plain text can be recovered by using an inverse process of encryption.

An analytical description of the secure communication scheme is given as follows: The transmitter can be given as

$$\begin{cases}
\dot{x}_1(t) = s(t) - (a-1)x_1(t) \\
\dot{x}_2(t) = (c-a+1)x_1(t) - x_1(t)x_3(t) + (c-a)x_2(t) + s(t) , \\
\dot{x}_3(t) = x_1(t)x_2(t) - bx_3(t) + k(x_3(t) - x_3(t-\tau))
\end{cases}$$
(10)

where

$$s(t) = ax_2(t) - x_1(t) + y(t). (11)$$

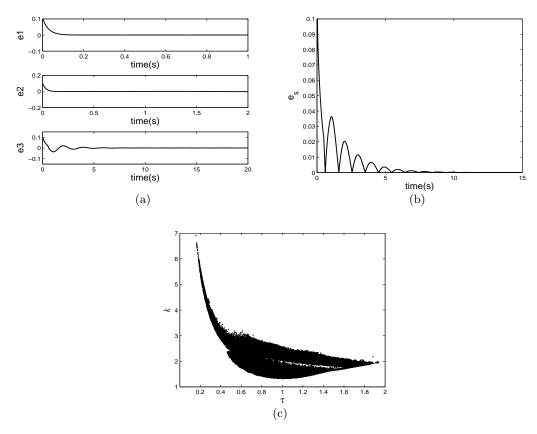


Fig. 2. Active-passive synchronization of the hyper-chaotic Chen system. (a) The error component of the different state between the transmitter and the receiver; (b) the square root error, e_s , of the state of the systems. (c) The parameter range of k and τ to guarantee the chaotic dynamics and the synchronization.

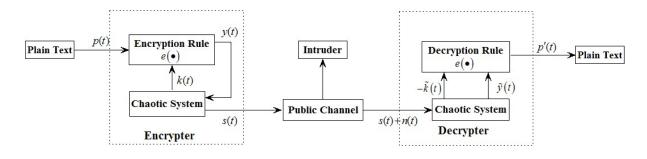


Fig. 3. Block diagram of the chaotic cryptosystem.

Here

$$y(t) = e(p(t), k(t))$$

 $k(t) = x_1(t)/10$ (12)

is the transmitted signal.

$$e(p(t), k(t)) = \underbrace{f_1(...f_1(f_1(p(t), x_1(t)), x_1(t)), ..., x_1(t))}_{n}$$
(13)

6 Ren et al.

is the output of n-shift cipher function. The n-shift function is given as

$$f_1(u,v) = \begin{cases} (u+v) + 2h, -2h \le (u+v) \le -h \\ (u+v), -h < (u+v) < h \\ (u+v) - 2h, h \le (u+v) \le 2h \end{cases}$$
 (14)

At the receiver end, the copy of the transmitter can be given as

$$\begin{cases}
\dot{y}_1(t) = s(t) - (a-1)y_1(t) \\
\dot{y}_2(t) = (c-a+1)y_1(t) - y_1(t)y_3(t) + (c-a)y_2(t) + s(t) \\
\dot{y}_3(t) = y_1(t)y_2(t) - by_3(t) + k(y_3(t) - y_3(t-\tau))
\end{cases}$$
(15)

The receiver is driven by the transmitted signal s(t) (combined with noise n(t)). If the APD synchronization occurs, by defining

$$\tilde{y}(t) = s(t) - ay_2(t) + y_1(t),$$
(16)

we have

$$\tilde{y}(t) = y(t). \tag{17}$$

By an inverse procedure of the n-shift function, the plain text can be recovered by

$$p'(t) = \underbrace{f_1(...f_1(f_1)(\tilde{y}(t), -\tilde{k}(t)), -\tilde{k}(t)), ..., -\tilde{k}(t))}_{n}, \tag{18}$$

where

$$\tilde{k}(t) = y_1(t)/10.$$
 (19)

The features of this new method lie in the following: Firstly, neither the key signal k(t) nor the encrypted signal y(t) is directly transmitted in a public channel, since the encrypted signal y(t) has been sent to the chaotic attractor. It is different from the traditional discrete cryptosystem, where both the key and the encrypted signal must be transmitted to the decrypter. Secondly, a hyper-chaotic signal is used as the transmitted signal, which obstructs the eavesdropper to reconstruct the chaotic attractor using dynamical reconstruction [Kevin, 1994]. Thirdly, in the n-shift cipher, the key signal $x_1(t)$ is used n times to encrypt the plain signal. Since the encrypted signal is a function of $x_1(t)$ and p(t), and the output of the n shift function is also used to drive the hyper-chaotic Chen system, it hides the dynamical and statistical characteristics of both signals $x_1(t)$ and p(t).

3.4. Numerical simulation

Numerical simulations have been performed to show the results of the proposed secure communication method. The n-shift cipher function parameters are n=5 and h=0.4. The initial conditions of the transmitter and the receiver hyper-chaotic system are given as $(x_1(0), x_2(0), x_3(0)) = (0.1, 0.6, 0.1)$ and $(y_1(0), y_2(0), y_3(0)) = (-0.1, -0.4, -0.1)$, respectively. The initial conditions $x_3(t), y_3(t), -\tau < t < 0$, are set to zero and other parameters are the same as in Eq. (1). The results are given in Fig. 4. The plain text $p(t) = 0.4 \sin(\pi t)$ is given in Fig. 4 (a); the output of n-shift cipher function y(t) is given in Fig. 4(b); the transmitted signal s(t) in the public channel is given in Fig. 4(c); the power spectrum of transmitted signal is given in Fig. 4(d); the recovered signal is given in Fig. 4(e); the error between the plaintext and the recovered signal is given in Fig. 4(f). From Fig. 4, we have that the plain text is recovered after a transient state of synchronization. From the transmitted signal, one cannot obtain any time domain or frequency domain information about the plain texts and the key signal, and the spectrum of the transmitted signal is fully embedded into the chaotic signal spectrum.

The transmitted signal in the public channel is, of course, susceptible to noise. When the transmitted signal is polluted by the noise from the public channel, it happens one of the main concerns in real applications. A noise with variance of 0.1 percent of the amplitude of the transmitted signal is incorporated into the transmitted signal; the transmitted signal with noise is then used to drive the receiver hyper-chaotic

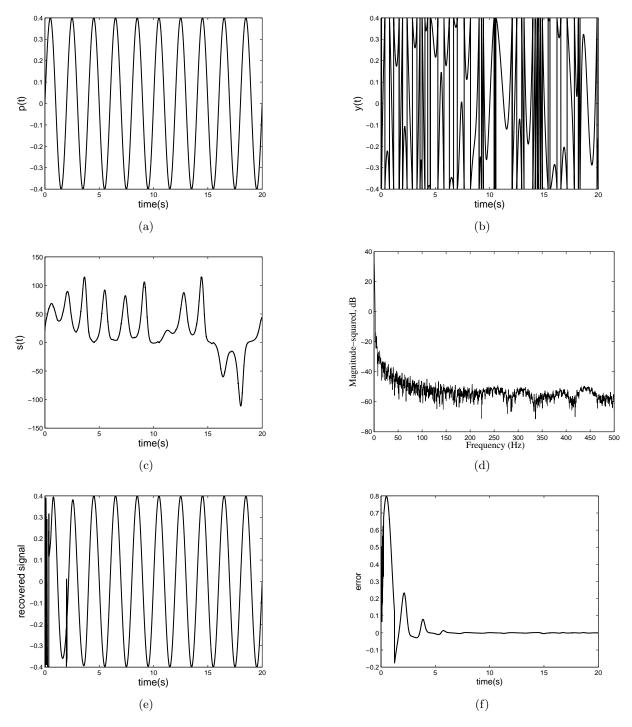
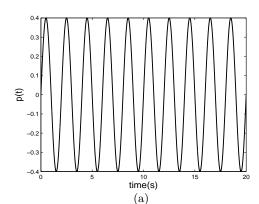


Fig. 4. Simulation results of the proposed secure hyper-chaotic communication scheme. (a) The plain text to be transmitted; (b) the output of n-shift cipher function; (c) the transmitted signal in the public channel; (d) the power spectrum of the transmitted signal; (e) the recovered signal; (f) the error between the plain text signal and the recovered signal.

system to synchronize with the transmitter. The results are given in Fig. 5, in which the plain text and the recovered signal are given in subplot (a) and (b), respectively. The plain text can be recovered even though the transmitted signal is polluted by the noise. The recovered plain text is also affected by the noise, but it is still eligible.

The proposed scheme is also used as secure voice communication. The results are given in Fig. 6. Here, the voice testing, 1-2-3, testing, 1-2-3 is used as transmitted signal, there exists transmitting noise



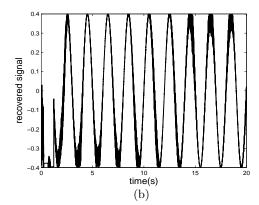
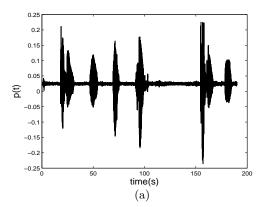


Fig. 5. Results of the proposed secure hyper-chaotic communication method with the transmitting noise. (a) The plain text to be transmitted; (b) the recovered signal when the transmitted signal is polluted by noise.



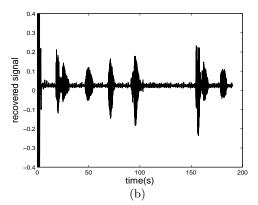


Fig. 6. Results of the secure voice communication using the proposed scheme. (a) The voice signal to be transmitted; (b) the recovered voice signal.

as the case in Fig. 5. The transmitted voice signal and the recovered signal are given in Fig. 6(a) and 6(b), respectively. Although there are significant differences in the wave form of the recovered signal and transmitted signal, the recovered voice is still intelligible even by the naked ears.

So far we have shown the effectiveness of the proposed secure communication method. The attacking resilience property is another concern of the real application. In the following, we will show this property of the proposed scheme.

4. Attacking Resilience Analysis

Researches have shown that it is possible to use nonlinear dynamic (NLD) forecasting [Andrew & Kevin, 2001], which are based on the reconstruction of the dynamics of the transmitter from the transmitted signal to break communication schemes. There also existed other breaking methods such as return map reconstruction [Yang et al., 1998c]. Dynamic behavior of the system is mapped to a nearly one-dimensional attractor. Different return maps of a chaotic transmitted signal can reveal the amplitude and frequency information of a message signal.

4.1. The features of the proposed method

By analyzing the attacking resilience of the method proposed in this paper, we see that the synchronization and encoding schemes given in this paper are more complicated but they are resilient. Firstly, our method is different from [Hernandez & Serrano, 2005] and [Andrew & Kevin, 2001], since our proposed secure com-

munication system is based on an hyper-chaotic system. The hyper-chaotic Chen system has, by definition, more than one positive Lyapunov exponent and has rich dynamic characteristics [Ren & Li, 2010; Xu, 2013. The infinite dimensional hyper-chaotic behavior of the system (with three positive Lyapunov exponents) make the phase space of the signal be extremely complicated and difficult to devise it by time-delay embedded method [Ponomarenko & Prokhorov, 2002], return map [Perez & Cerdeira, 1995], and nonlinear dynamical forecasting [Andrew & Kevin, 2001]. Secondly, unlike using XOR operation in [Wang et al., 2011] and [Wang & Wang, 2014] to encrypt the plain text, a more complicated n-shift cipher function is used in our method, where the key signal is used n times to encrypt the plain signal. Since the encrypted signal is a nonlinear function of the plain text and key signal, it is very difficult to predict the plain text from the output of the n-shift function. Thirdly, the key signal is transmitted in the public channel in [Wang & Wang, 2014], however, in our proposed method, neither the key signal nor the encrypted signal is directly transmitted in the public channel. The output of the encrypted signal is sent to the chaotic attractor, which hides both the dynamical and the statistical characteristics of both the key signal and the plain text. The chaos synchronization between the transmitter and the receiver is implemented by using the transmitted signal to decode the information. The intruder cannot use the intercepted signal alone to reconstruct the key stream with enough accuracy to partially decrypt the plain text signal. Finally, when we use the hyper-chaotic Chen system to encrypt the plain signal, since the shape of the return maps being strips, the change of the return maps are more irregular and the intruder cannot access any effective information by the change of the return maps [Yang, 2004]. From the above analysis we see that this secure communication scheme has a higher degree of security. Simulations of the sinusoidal waveform and voice signals show the validity of the assertion on the proposed scheme.

4.2. Key space Analysis

In general, the security of a system depends on the security of the system parameters of both transmitter and receiver. System parameters are equivalent to the keys of traditional cryptography [Wang et al., 2011]. Herewith we analyze the numerical parameters. In the proposed method, there are seven parameters (a,b,c,k,n,h) and an assumption that the double-precision (2^{-32}) is used. Therefore, the system parameter space size is $2^{32\times7} = 2^{224}$, which means that the key space is big enough to stand up to an exhaustive attack [Wang et al., 2011; Wang & Wang, 2014].

The sensitivity of parameters 4.3.

From the simulation results of perturbation in the parameter a (or c) and the initial value, we obtain the system sensitivity to parameters, as shown in Fig. 7. The plain text is given in Fig. 7(a), whose parameters are same as Eq. (1) (a = 35, b = 3, c = 18); the recovered signal with same parameters is given in Fig. 7(b), the recovered signal with a = 35.1 and c = 17.95 are given in Fig. 7(c) and Fig. 7(d), respectively. From Fig. 7, we find that the proposed method is sensitive to the parameters. The transmitted signal cannot be resolved with the parameters of the system being real numbers; the useful information can only with the true parameters.

4.4. Statistical analysis

It is known that the statistical property of a cipher is an important point to evaluate the performance of the system, therefore, a good method should be robust against any statistical analysis [Wang & Wang, 2014. A histogram is plotted according to the value of the voice testing, 1-2-3, testing, 1-2-3 with step 0.0001, as shown in Fig. 8. The statistical distribution of the voice signal can be seen from Fig. 8(a). But this distribution has disappeared after encryption, as shown in Fig. 8(b).

4.5. Computation Cost

We also carried out computation cost comparisons with [Ren & Bai, 2015; Yang, 1995] and [He, 2013]. In the experiment, the voice Hello with 1.5 seconds time duration are encoded in the same configuration. The

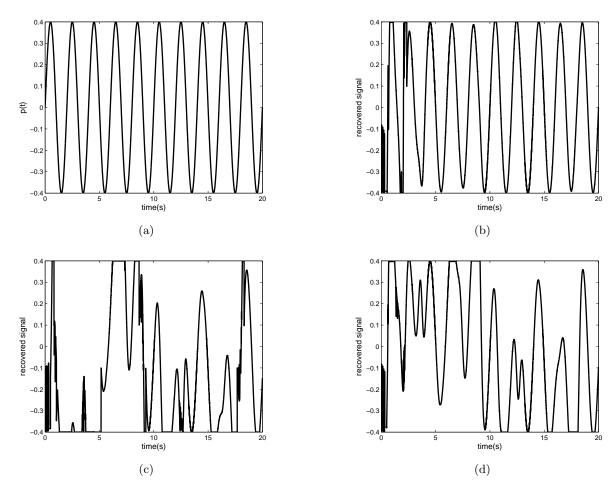


Fig. 7. The parameter sensitivity analysis of the proposed method. (a) The plain text to be transmitted, whose parameters are same as in Eq. (1); (b) the recovered signal with the same parameter as the transmitter; (c) the recovered signal with a=35.1; (d) the recovered signal with c=17.95.

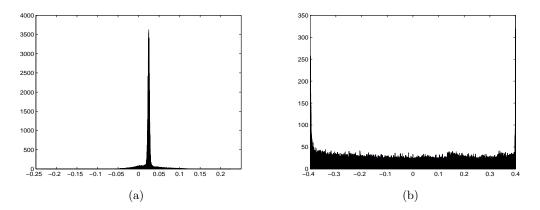
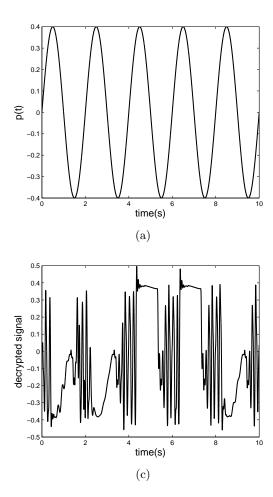


Fig. 8. The distribution of the voice value. (a) The distribution of the plain text; (b) the distribution of the cipher text.

experiment environment is MATLAB 2010a with the same computer. The computation costs of the three methods are shown in Table 1. From Table 1 we surmise that the proposed method is efficient in the sense of using less time to encode the same information.

Comparisons of the proposed method with other methods regarding computation speed (unit: second).

	The Proposed method	[Ren & Bai, 2015]	[Yang, 1995]	[He, 2013]
The voice of "Hello" with 1.5s	3.5	3.8	4.0	6.6



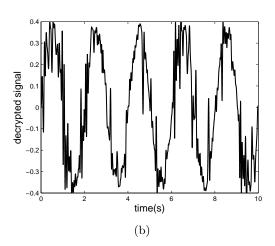


Fig. 9. The attacking results using method in [Yang et al., 1997]. (a) The transmitted plain text; (b) the decrypted signal for the method [Yang et al., 1997] by the intruder; (c) the decrypted signal for the proposed method by the intruder.

4.6. The ability to resist attack

Some more complicated attacking methods are proposed in [Andrew & Kevin, 2001], in which the dynamical reconstruction, low pass filter, shifting analysis are used to break the chaotic communication scheme. We use the method from [Andrew & Kevin, 2001] to attack the secure communication scheme proposed in this paper and the secure scheme in [Yang et al., 1997]. The plain text $p(t) = 0.4\sin(\pi t)$ is given in Fig. 9(a). The results by attacking method [Yang et al., 1997] and the proposed method are given in Fig. 9(b) and 9(c), respectively. For the method [Yang et al., 1997], we see that the intruder can obtain the information transmitted in the public channel from the decrypting signal shown in Fig. 9(b). Although the decrypting signal is not smooth, one can reduce its influence through a low-pass filter. For the proposed method, the intruder cannot get any useful information from Fig. 9(c).

5. DSP Experiment

The experimental validation of the proposed communication scheme is implemented by using two floating-point DSPs, i.e., TMS320C6713 developed starter kit (DSK) board and the block diagram of the experiment are given in Fig. 10. The voice signal is sampled by the analog-to-digital (A/D) converter TLC320AIC23,

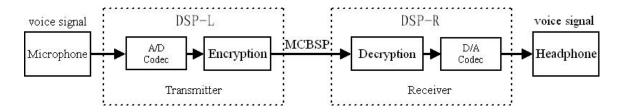


Fig. 10. Block diagram of the experimental setup for the proposed secure communication scheme.

which is embedded on the DSK board. The sampled signal is encrypted by the proposed algorithm and then transmitted through multichannel buffered serial port (MCBSP), a kind of series communication channel in the DSP chip, to the receiver end. At the receiver end, the transmitted plain text is recovered by using a reverse process of encryption in DSP and replayed through the digital-to-analog (D/A) converter to the headphone. The experiment results are given in Fig. 11. The plain text signal is given in Fig. 11(a); the recovered signal is given in Fig. 11(b); the cryptograph signal is given in Fig. 11(c); the error between the plain text signal and the received signal is shown in Fig. 11(d). Although there are some errors between the transmitted signal and the received signal, the voice can be identified by the naked ear. From Fig. 11, we find that the plain text is recovered after a short transient state of synchronization, and the experimental results show the feasibility of the proposed method.

6. Conclusions

In this paper, a hyper-chaos generated by direct time-delay feedback and the APD synchronization method are used in a secure chaotic communication scheme. In order to improve the security of message transmission, a hyper-chaotic communication method based on multi-shift ciphering is presented. The proposed secure hyper-chaotic communication scheme is different from the traditional ones due to employing hyper-chaotic dynamics and two different chaotic states for the synchronization and the encryption. To inspect the performance of the proposed scheme, the sinusoidal waveform and voice signals are used as the plain texts. The results show that the proposed scheme is effective even though there is noise in the public channel. The security analysis has shown that the proposed method is immune against the conventional nonlinear dynamics (NLD) forecasting techniques and return map reconstruction. It is also difficult for the special designed complex decryption method in [Andrew & Kevin, 2001] to predict the transmitted signal. Finally, the DSP experiment shows the feasibility and the validity of the proposed communication scheme.

Acknowledgments

This research is partially supported by National Natural Science Foundation of China (61172070, 60804040), Fok Ying Tong Education Foundation Young Teacher Foundation(111065), Innovative Research Team of Shaanxi Province(2013KCT-04), The Key Basic Research Fund of Shaanxi Province (2016ZDJC-01), Chao Bai was supported by Excellent Ph.D. research fund (310-252071603) at XAUT.

References

Andrew, T. P. & Kevin, M. S. [2001] "Reconstructing the key stream from a chaotic encryption scheme," *IEEE Transactions on Circuits Systems-I*, **48**, 624–630.

Alvarez, G., Montoya, F., Pastor, G. & Romera, M. [2004] "Breaking a secure communication scheme based on the phase synchronization of chaotic system," *Chaos*, **14**, 274–278.

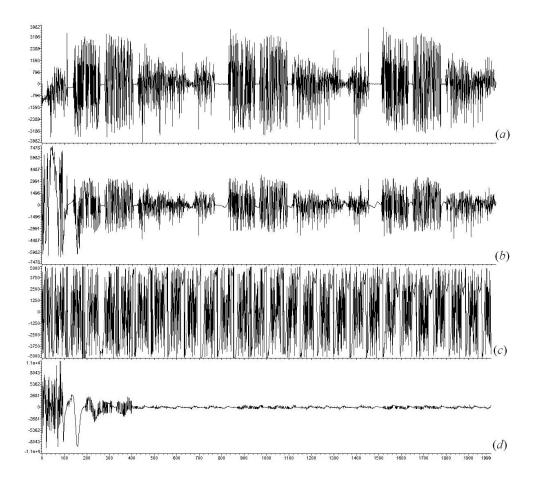


Fig. 11. Experimental results of secure voice communication by using DSPs.

- Apostolos, A. & Dimitris, S. [2005] "Chaos-based communications at high bit rates using commercial fiber-optic links," *Nature*, **438**, 343–346.
- Bu, S. & Wang, B. H. [2004] "Improving the security of chaotic encryption by using simple modulating method,", Chaos, Solution and Fractal, 19, 919–924.
- Cafagna, D. & Grassi, G. [2003] "New 3D scroll attractors in hyper-chaotic Chuas circuits forming a ring," International Journal of Bifurcation and Chaos, 13, 2889–2903.
- Chen, J. Y., Wang, K. W., Cheng, L. M. & Shuai, J. W. [2003] "A secure communication scheme based on the phase synchronization of chaotic systems," Chaos, 13, 508–514.
- Chin, Y. C., Xu, D. L. & Steven, R. B. [2004] "A Zero-crossing approach to uncover the mask by chaotic encryption with periodic modulation," Chaos, Solution and Fractals, 21, 1129–1134.
- Cuomo, K. M., Oppenheim, A. V. & Strogatz, S. H. [2004] "Synchronization of Lorenz-based chaotic circuits with application to communication," IEEE Transactions on Circuits Systems-II, 40, 626–658.
- Dedieu, H., Kennedy, M. & Hasler, M. [1993] "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chuas circuits," IEEE Transaction on Circuits Systems-II, **40**, 634–675.
- Hayes, S. T., Grebogi, C. & Ott, E. [1993] "Communication with chaos," Physical Review Letter, 70, 3031-3034.
- Hernandez, C. C. & Serrano, G. H. [2005] "Cryptosystems based on synchronized Chuas circuits," Proceedings of the 16th IFAC world congress, 21, 143–192.
- He, J. B. [2013] "Parameter modulation for secure communication via the synchronization of hyper-chaotic Chen systems," Systems Science and Control Engineering, 2, 718–726.
- Kevin, M. S. [1994] "Steps towards unmasking secure communications," International Journal of Bifurca-

- tion and Chaos, 4, 959–977.
- Kevin, M. S. & Andrew, T. P. [1998] "Unmasking a hyper-chaotic communication scheme," *Physics Review* E, **58**, 1159–1162.
- Li, S. J., Alvarez, G., Chen, G. R. & Mou, X. Q. [2005] "Breaking a chaos-noise based secure communication scheme," *Chaos*, **15**, 137–148.
- Li, Y. X., Tang, Wallace K. S. & Chen, G. R. [2005] "Generating hyperchaos via state feedback control," International Journal of Bifurcation and Chaos, 15, 3367–3375.
- Minai, A. A. & Pandian, T. D. [1998] "Communication with noise: How chaos and noise combine to generate secure encryption," *Chaos*, **8**, 621–628.
- Pecora, L. M. & Carroll, T. L. [1990] "Synchronization in chaotic systems," *Physics Review Letter*, **64**, 821–824.
- Perez, G. & Cerdeira, H. A. [1995] "Extracting messages masked by chaos," *Physics Review Letter*, **74**, 1970–1972.
- Parlitz, U., Kocarev, L., Stojanovski, T., & Preckel, H. [1996] "Encoding messages using chaotic synchronization," *Physics Review E*, **53**, 4351–4361.
- Ponomarenko, V. I. & Prokhorov, M. D. [2002] "Extracting information masked by the chaotic signal of a time-delay system," *Physics Review E*, **66**, 026215.
- Peng, Z. P., Wang, C. H., Lin, Y. & Luo, X. W [2014] "A novel four-dimensional multi-wing hyper-chaotic attractor and its application in image encryption," *Acta Physica Sinica*, **63**, 240506.
- Ren, H. P., Liu, D. & Han, C. Z. [2006] "Anti-control of chaos via direct time delay feedback control," *Acta Physica Sinica*, **55**, 2694–3701.
- Ren, H. P., Han, C. Z. & Liu, D. [2008] "Breaking Chaotic Shift Key Communication via Adaptive Key Identification," *Chinese Physics B*, **17**, 1202–1208.
- Ren, H. P. & Li, W. C. [2010] "Heteroclinic Orbits in Chen Circuit with Time Delay," Communications in Nonlinear Sciences and Numerical Simulation, 15, 3058–3066.
- Ren, H. P., Baptist, M. S. & Grebogi, C. [2012] "Uncovering missing symbols in communication with filtered chaotic signals," *International Journal of Bifurcation and Chaos*, **22**, 1250199.
- Ren, H. P., Baptist, M. S. & Grebogi, C. [2013] "Wireless communication with chaos," *Physics Review Letter*, **110**, 184101.
- Ren, H. P., Baptist, M. S. & Grebogi, C. [2014] "Robustness of chaos to media with multipath propagation," *Boca Raton: CRC press*, 423–437.
- Ren, H. P. & Bai, C. [2015] "Secure communication based on spatiotemporal chaos," *Chinese Physics B*, **24**, 080503.
- Sun, J. [2004] "Delay-dependent stability criteria for time delay chaotic systems via time-delay feedback control," Chaos, Solution and Fractals, 21, 143–150.
- Sprott, J. C. [2006] "Lyapunov Exponents for Delay Differential Equations," http://sprott.physics.wisc.edu/chaos/ddele.htm.
- Ueta, T. & Chen, G. [2000] "Bifurcation analysis of Chen's equation," *International Journal of Bifurcation and Chaos*, **10**, 1917–1931.
- Udaltsov, V. S., Goedgebuer, J. P., Larger, L., et al. [2003] "communicating with hyper-chaos: the dynamics of a DNLF emitter and recovery of transmitted information," *Optics Spectroscopic*, **95**, 114–121.
- Wang, X. F. Chen, G. R. & Yu, X. [2000] "Anticontrol of chaos in continuous-time systems via time-delay feedback," Chaos: An Interdisciplinary Journal of Nonlinear Science, 10, 771–779.
- Wang, X. G., Zhan, M., Lai, C. H. & Gang, H. [2004] "Error function attack of chaos synchronization based encryption schemes," *Chaos*, 14, 128–137.
- Wang, X. Y., Zhang, N., Ren, X. L. & Zhang, Y. L. [2011] "Synchronization of spatiotemporal chaotic systems and application to secure communication of digital image," *Chinese physics B*, **20**, 020507.
- Wang, X. Y., Wang, Q. [2014] "A fast image encryption algorithm based on only blocks in cipher text," Chinese physics B, 23, 030503.
- Xu, J. [2013] "Hyper-chaotic attractor generated by time-delay and its circuits," Master thesis of Xi'an University of Technology.
- Xue, W., Qi, G. Y., Mu, J. J., Jia, H. Y. & Guo, Y. L [2013] "Hopf bifurcation analysis and circuit

- implementation for a novel four-wing hyper-chaotic sytem," Chinese Physics B, 22, 080504.
- Yang, T. [1995] "Recovery of digital signal from chaotic switching," International Journal of Circuits Theory and Application, 23, 611–615.
- Yang, T. & Chua, L. O. [1996] "Secure communication via chaotic parameter modulation," IEEE Transactions on Circuits Systems-I, 43, 817-825.
- Yang, T., Chai, W. W., & Leon, O. C. [1997] "Cryptography Based on Chaotic Systems," IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, 44, 469–472.
- Yang, T., Yang, L. B. & Yang, C. M. [1998a] "Breaking chaotic secure communications using a spectrogram," Physics Letter A, 247, 105–111.
- Yang, T., Yang, L. B. & Yang, C. M. [1998b] "Breaking chaotic switching using generalized synchronization: examples," IEEE Transactions on Circuits and Systems-I, 45, 1062–1067.
- Yang, T., Yang, L. B. & Yang, C. M. [1998c] "Crypt analyzing chaotic secure communications using return maps," Physics Letter A, **245**, 495–510.
- Yang, T. [2004] "A survey of chaotic secure communication systems," International Journal Computational Cognition, 2, 81–130.
- Zhou, C. & Lai, C. H. [1999] "Extracting messages masked by chaotic signals of time-delay systems," Physics Review E, **60**, 320–332.