Fuzzy Model-Based Discrete-Time Chiang Type Chaotic Cryptosystem*

Tung-Sheng Chiang† and Peter Liu
Department of Electrical Engineering
Ching-Yun Institute of Technology
Chung-Li, Taiwan 320, R.O.C.
Tel: +886-3-4581196 ext. 304
Email: tschiang@cyit.edu.tw
Keywords — T-S fuzzy, chaotic system, cryptology

Abstract

In this paper we proposed a class of new chaotic system as so-called Chiang type chaotic system. First the chaotic system is represented into T-S fuzzy models. Then based on this type of chaotic system, a new cryptosystem is developed. The advantage of this cryptosystem is a significant increase in the plaintext to chaotic signal ratio which is beneficial in coping with channel noise. In addition, this cryptosystem is allows increase of the power of plaintext and maintain high security.

I. Introduction

Recently, synchronization of chaotic systems and its application to chaos-based communication have received considerable attention [1, 2]. Different methods have been developed in order to hide the contents of a message using chaotic signals. However, the attacks propose in [3] have shown that most of these methods are not secure or have a low security.

The authors [5] and [6] have proposed cryptography based on chaotic systems. When consider the large channel noise, the synchronization based chaotic communication may not be used, since the property of synchronization does not exist or induce large error. One possible way to solved is increase the magnitude of transmitting binary message and avoid destroying chaotic signal characteristics, then recover the binary signal at the receiver end with low bit error ratio. But in signal masking applications, the message can not be too large as to destroy the original chaotic signal. Since the noise in the coupling channel is not under our control, we must therefore hope to find a chaotic signal that allows larger amplitudes of message and meanwhile not destroy the chaotic characteristics. The Chiang type chaotic system fits such requirements. In addition, to further ensure security, cryptology is applied.

II. Discrete-Time Chaos-based Cryptosystem

A block diagram illustrating the cryptosystem is given in Fig.1 which consists of three parts.

Part 1: The discrete-time modulated chaotic system is described by a T-S fuzzy model [7] in output injection form, the drive fuzzy model is composed of the following rules:

$$\begin{aligned} \textit{Rule } i: \quad & \text{IF } z_1(k) \text{ is } F_{1i} \text{ and } \cdots \text{ and } z_g(k) \text{ is } F_{gi} \text{ THEN} \\ & x(k+1) = G_i x(k) + \eta + Ly(k) \\ & y(k) = C_i x(k) + e_n(k),\ i = 1, 2, ..., r, \end{aligned}$$

where $x \in R^n$, $y(k) \in R$ are the state vector, output, respectively; $z_1(t) \sim z_g(t)$ are the premise variables which would consist of the state of the system; F_{ji} $(j = 1, 2, \cdots, g)$ are the fuzzy sets; $G_i = A_i - LC_i$ with A_i, C_i and L as system matrices and gain with appropriate dimensions, respectively; $\eta \in R^n$ denotes the bias term; $e_n(k)$ is ciphertext; and r is the number of fuzzy rules which is generated by the exact fuzzy modeling procedure.

The fuzzy inferred output of the transmitter can be expressed in the form:

$$x(k+1) = \sum_{i=1}^{r} \mu_i(z) \{G_i x(k) + \eta + Ly(k)\} \qquad (1)$$

$$y(k) = \sum_{i=1}^{r} \mu_i(z) \{C_i x(k) + e_n(k)\}, \qquad (2)$$

where $z = [z_1(k)\ z_2(k)\ \cdots\ z_g(k)]^{\mathrm{T}}$, and $\mu_i(z) = \omega_i(z)/(\sum_{i=1}^{r} \omega_i(z))$ with $\omega_i(z) = \prod_{j=1}^{g} F_{ji}(z_j(k))$, for $i = 1, 2, ..., r$.

The discrete-time chaotic system which are applicable are the so-called Lure type systems. Some well-known examples that fall into this category [7]: 1) logistic, parabolic map for one-dimension; 2) Henon, cubic for two-dimensions; 3) the three-dimensions discrete-time chaotic system in [7]; and 4) the higher order generalized Henon map. It note that if $e_n(k) = 0$ equation (1) and (2) can be expressed Lure type chaotic system.

Part 2: In order to encrypt the plaintext $m(k)$, a *p-shift* cipher is chosen [4]:

$$e_n(k) = \underbrace{f(\cdots(f}_{p}(\, m(k), \underbrace{K(k)), \cdots), K(k))}_{p}$$

where the encryption function

$$f(a,b) = \begin{cases} a+b+2h & -2h \,\square\, a+b \,\square\, -h \\ a+b & , -h \,\square\, a+b \,\square\, h \\ a+b-2h & , h \,\square\, a+b \,\square\, 2h \end{cases}$$

*This work was supported by the National Science Council, R.O.C. under Grant NSC-90-2213-E-231-005.
†Corresponding addressee

; p and h is a positive scalar parameter in function $f(\cdot)$. Therefore the decrypter is

$$\hat{m}(k) = \underbrace{f(\cdots(f(}_{p}\ \hat{e}_n(k), \underbrace{-\hat{K}(k)),\cdots),-\hat{K}(k))}_{p}$$

where $\hat{e}_n(k), \hat{K}(k)$ are the reconstructed signals.

In order to retrieve the plaintext, it is necessary to generate the key at the receiver. This objective is achieved by designing the decrypter as a nonlinear observer for the state of the encrypter. This leads to the third part of the designed work.

Part 3: Given the encrypter (1) and (2), the decrypter is the dynamic system

$$\begin{aligned} \textit{Rule } i: \quad & \text{IF } \hat{z}(k) \text{ is } F_i \text{ THEN} \\ & \hat{x}(k+1) = G_i\hat{x}(k) + \eta(k) + Ly(k) \\ & \hat{y}(k) = C_i\hat{x}(k),\ i = 1,2,...,r, \end{aligned} \tag{3}$$

The fuzzy inferred output of the receiver can be expressed in the form:

$$\hat{x}(k+1) = \sum_{i=1}^{r} \mu_i(\hat{z})\{G_i\hat{x}(k) + \eta + Ly(k)\} \tag{4}$$

$$\hat{y}(k) = \sum_{i=1}^{r} \mu_i(\hat{z}))C_i\hat{x}(k),\ i = 1,2,...,r. \tag{5}$$

Therefore, (4) and (5) have to be designed such that $\hat{x}$ converges to state x. In other words, find C_i such that synchronization error $\tilde{x} = x - \hat{x}$ approaches zero asymptotically. If $\tilde{x} \to 0$ as $k \to \infty$ for any initial conditions, system (1) and (2) are said to be a global asymptotic observer of (4) and (5).

The Equations (1) and (2) can be regarded as an extension of modulated chaotic communications [7]. To recover the message, the fuzzy receiver is designed as (3), which yields the error dynamics:

$$\tilde{x}(k+1) = \sum_{i=1}^{r} \mu_i(z)G_ix(k) - \sum_{i=1}^{r} \mu_i(\hat{z})G_i\hat{x}(k) \tag{6}$$

$$\tilde{y}(k) = \sum_{i=1}^{r} \mu_i(z)C_ix(k) - \sum_{i=1}^{r} \mu_i(\hat{z})C_i\hat{x}(k) + e_n(k) \tag{7}$$

where $\tilde{x}(k) \equiv x(k) - \hat{x}(k)$, and $\tilde{y}(k) \equiv \tilde{y}(k) - \hat{y}(k)$.

Theorem 1: *The error system described by (6) for DFS is asymptotically stable if there exist a common positive definite matrix $P = P^T$ and gains C_i, for $i = 1,2,...,r$, which can be determined by solving the following eigenvalue problem:*

$$\underset{M_i,\ X}{minimize}\ \varepsilon$$

subject to $X > 0,\ \varepsilon > 0$

$$\begin{bmatrix} X & (A_iX - LM_i)^{\mathrm{T}} \\ A_iX - LM_i & X \end{bmatrix} > 0 \text{ for all } i \tag{8}$$

$$\begin{bmatrix} \varepsilon I & * \\ A_1X - LM_1 - (A_iX - LM_i) & I \end{bmatrix} > 0,\ 2 \le i \le r, \tag{9}$$

where $M_i = C_iP^{-1}$, for $i = 1,2,...,r$, and $X = P^{-1}$. Then the overall error dynamics become $\dot{\tilde{x}}(k+1) = G\tilde{x}(k)$, where $G = G_1 = G_i$, for $i = 1,2,...,r$. The error system described by the above equation for DFS is stabilized if the corresponding Lemma 1 and Thm. 1 are satisfied. Therefore $\tilde{y}(k) \to e_n(k)$ as $k \to \infty$. 2

It has long been known that the message-to-channel noise ratio for the signal masking chaotic communications is almost 10 dB [1]. Therefore, this may cause problems such as unrecoverable messages due to large noise or the message amplitude is too large such that the chaotic characteristics are destroyed. This is the reason to introduce Chiang type chaotic system in the next section.

III. Chiang type Cryptosystem

Chiang type chaotic systems are a modified example of original Lure type discrete-time chaotic systems. First, we show that Chiang type chaotic system, modified Henon map as an example

$$\begin{aligned} x_1(k+1) &= -x_1^2(k) + \beta x_2(k) + 1.4 \quad rem\ 1.73 \\ x_2(k+1) &= x_1(k) \qquad\qquad\qquad\quad rem\ 1.73 \end{aligned} \tag{10}$$

indeed has chaotic characteristics, where $rem(\cdot)$ denotes $rem(a,b) \equiv a - b \cdot \lceil a/b \rfloor$; $\lceil \cdot \rfloor$ is a fix operation, i.e. $\lceil c \rfloor$ is rounds of elements of c to the nearest integers towards zero. We illustrate the bifurcation diagram by setting the parameter of β varying from 0.2 to 0.4 and is shown in Fig. 2. The phase portrait of the modified Henon map $x_1(k) - x_2(k)$ is shown in Fig. 3. The phase portrait is different from the original Henon map, due to the fix operation.

Based on the fuzzy driving concept, a new scheme of modulated chaotic communications is proposed here. Now, the fuzzy chaotic transmitter is given as compact form

$$\begin{aligned} \textit{Rule } i: \quad & \text{IF } x_1(k) \text{ is } F_i \text{ THEN} \\ & \underline{x}(k+1) = G_ix(k) + \eta + Ly(k) \\ & y(k) = C_ix(k) + e_n(k),\ i = 1,2,...,r, \end{aligned}$$

where $\underline{x}$is inferred output state; the state $x(k)$ is obtained from $x(k) = rem(\underline{x}, d)$. The fuzzy inferred output of the transmitter is expressed in the form:

$$\underline{x}(k+1) = \sum_{i=1}^{r} \mu_i(x_1)\{G_ix(k) + \eta + Ly(k)\} \tag{11}$$

$$x(k) = rem(\underline{x}(k), d)$$

$$y(k) = \sum_{i=1}^{r} \mu_i(x_1)\{C_ix(k) + e_n(k)\}, \tag{12}$$

The receiver is design as

$$\begin{aligned} \textit{Rule } i: \quad & \text{IF } \hat{x}_1(k) \text{ is } F_i \text{ THEN} \\ & \underline{\hat{x}}(k+1) = G_i\hat{x}(k) + \eta + Ly(k) \\ & \hat{y}(k) = C_i\hat{x}(k),\ i = 1,2,...,r, \end{aligned}$$

with overall inferred output as

$$\underline{\hat{x}}(k+1) = \sum_{i=1}^{r} \mu_i(\hat{x}_1)\{G_i\hat{x}(k) + \eta + Ly(k)\} \tag{13}$$

$$\hat{x}(k) = rem(\underline{\hat{x}}(k), d)$$

$$\hat{y}(k) = \sum_{i=1}^{r} \mu_i(\hat{x}_1)\{C_i\hat{x}(k)\}. \tag{14}$$

The error dynamics between the transmitter and receiver:

$$\begin{aligned}\tilde{x}(k+1) &= \sum_{i=1}^{r}\mu_i(x_1)G_i x(t) - \sum_{i=1}^{r}\mu_i(\hat{x}_1)G_i\hat{x}(k) \\ &\quad - \sum_{i=1}^{r}\mu_i(x_1)d\cdot\left\lfloor\frac{G_i x(k)+\eta+Ly(k)}{d}\right\rfloor \\ &\quad + \sum_{i=1}^{r}\mu_i(\hat{x}_1)d\cdot\left\lfloor\frac{G_i x(k)+\eta+Ly(k)}{d}\right\rfloor\end{aligned}$$

where $\tilde{x}(t) \equiv x(t) - \hat{x}(t)$, and $\tilde{y}(t) = \sum_{i=1}^{r}\mu_i(x_1)C_i x(k) - \sum_{i=1}^{r}\mu_i(\hat{x}_1)C_i\hat{x}(t) + e_n(t)$.

Even if the EL condition is satisfied, i.e, $\beta\|X\| \simeq 0$ such that $G = G_i$ for $i = 1, 2$, G is not always stable. Therefore the condition (8) is also needed guarantee to stabilize the system matrix. Since the fix calculation is a nonlinear operator, it is difficult to obtain an analytical solution. Therefore we will rely on numerical *Monte-Carlo runs* to verify the projected results. From Fig. 4 show that if G is nilpotent the state error achieves dead-beat synchronization (note that the coupling signal is activated at $k \geq 10$).

Example: For the sake of simplicity, the original Henon map and modified Henon map (10) are used as example. The ciphertext $e_n(k)$ has been chosen to encode the plaintext $m(k)$ and set parameter $p = 5$, $h = 1.73$, $K(x(k)) = x_1(k)$ and $K(\hat{x}(k)) = \hat{x}_1(k)$. The fuzzy model are set as

$$A_1 = \begin{bmatrix} -d & 0.3 \\ 1 & 0 \end{bmatrix}, A_2 = \begin{bmatrix} d & 0.3 \\ 1 & 0 \end{bmatrix}, \eta = \begin{bmatrix} 1.4 \\ 0 \end{bmatrix},$$

with fuzzy sets

$$F_1 = \frac{1}{2}(1 - \frac{x_1(k)}{d}),\ F_2 = 1 - F_1 \text{ and } d = 1.73. \qquad (15)$$

Then $C_1^T = \begin{bmatrix} -1.73 & 0.3 \end{bmatrix}$,$C_2^T = \begin{bmatrix} 1.73 & 0.3 \end{bmatrix}$, $L = \begin{bmatrix} 1 & 0 \end{bmatrix}^T$ obtain from Thm1.

The transmitted binary $m(k) \in \{ -0.6,\ 0.6 \}$ is uniformly distribution random. The channel noise $n(k) = \{ -0.02,\ 0.02 \}$ is uniformly distribution random. Figure 5 shows the (a) coupling signal with channel noise;(b) message $m(k)$; and (c) error of message $m(k) - \hat{m}(k)$.

We can make a conclusion that indeed this type cryptosystem is allowed significant increase the magnitude of transmitted signal and maintain high security.

Conclusion

In this paper has proposed a class of new cryptosystem so-called Chiang type cryptosystem. Based on Chiang type chaotic system, a Chiang type cryptosystem is developed. The advantage of this cryptosystem is significant increase the plaintext to chaotic signal ratio against the channel noise. The Chiang type cryptosystem is allowed increase the power of plaintext and hold high security. The numerical simulations illustrate the Chiang type cryptosystem with low bit-error-rate while channel noise is considered. Actual work of discussing channel noise effect on the encrypter and decrypter function is further work

REFERENCES

[1] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst. II,* vol. 40, Oct., pp. 626-633, 1993.

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

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

[4] Yang, C. W. Wu and L.O. Chua, " Cryptography based on chaotic systems," *IEEE Trans. Circuits Syst. I,* vol. 44, no. 5, pp. 469-472, 1997.

[5] G. Grassi and S. Mascolo, "A system theory approach for designing cryptosystems based on hyperchaos," *IEEE Trans. Circuits Syst. I,* vol. 44, no. 9, pp. 1135-1138, 1999.

[6] H. Nijmeijer and I. M. Mareels, "Nonlinear observer design to synchronization," *IEEE Trans. Circuits Syst. I,* vol. 44, pp. 882-890, 1997.

[7] K. Y. Lian, T. S. Chiang, and P. Liu, and C. S. Chiu, "Synthesis of fuzzy model-based designed to synchronization and secure communication for chaotic systems," *IEEE Trans. syst., man, and Cyber.: Part B,* vol. 31, no. 1, pp. 66-83, 2001.

[8] T.-L. Liao and N.-S. Huang, "An observer-based approach for chaotic synchronization with applications to secure communications," *IEEE Trans. Circuits Syst. I,* vol. 46, no. 9, pp. 1144-1150, 1999.

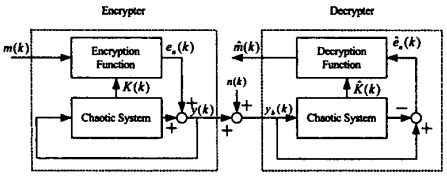

Fig. 1 Structure of cryptosystem.

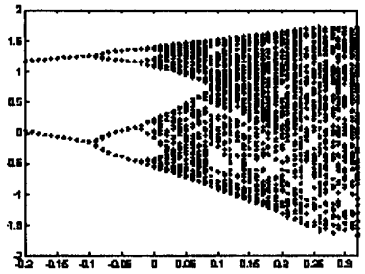

Fig. 2 Bifurcation of Chiang map (modified Henon map) dependent on β parameter.

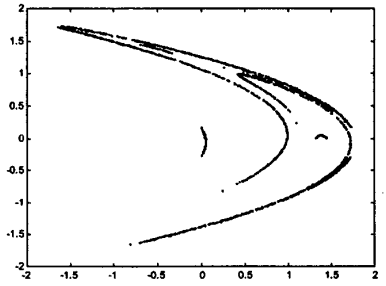

Fig.3 Phase portrait of Chiang map (modified Henon map).

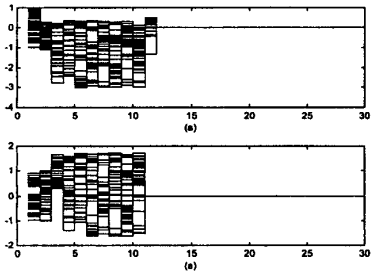

Fig.4 This illustrates the synchronization error when G is nilpotent (a) x_1; (b) x_2

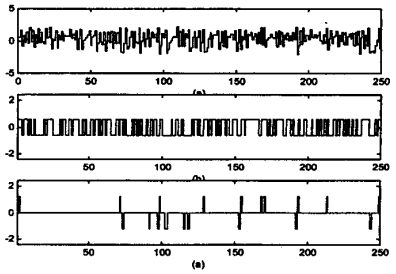

Fig.5 This illustrates (a) driving signal; (b) message; (c) error of message.