Improving the Security of Chaotic Synchronization With a Δ-Modulated Cryptographic Technique

Xiyin Liang, Jiangfeng Zhang, and Xiaohua Xia, *Senior Member, IEEE*

***Abstract*—A secure chaos-based communication with a Δ-modulated chaotic cryptographic technique is developed in this paper. We prove that a Δ-modulated feedback control of a 1-D discrete-time control system gives rise to a chaotic system. Base on this chaotic system, a modified parameter modulation scheme is proposed to improve security. As illustrated by numerical simulation, the parameter in the sender is protected by a secure cryptosystem against two popular attacks.**

***Index Terms*—Chaos synchronization, chaos cryptography, parameter modulation, Lorenz system, Δ-modulated feedback.**

I. Introduction

THERE is much interest in applying chaotic synchronization to secure communication since the work [17] of Pecora and Carrol was published in 1990. Following this work, various methods for chaos-based communication have been proposed, such as chaotic masking, chaotic modulation and chaotic-shift keying [6], [7], [13]. However, many proposed schemes have a low degree of security [1], [18], [19]. It is possible to extract the encoding messages by a number of ways, even without the knowledge of the system structure. For example, the methods based on power analysis and return map are popular attacks for parameter modulation chaotic communication schemes [1], [18]. They can be used to detect the change of parameter through analyzing the transmitted signal perturbed by parameter variation.

Based on conventional cryptographic techniques, various chaos-based schemes have been developed recently [14], [25]. A common feature of these methods is the utilization of state variables of the chaotic systems as keys in the encryption algorithms. For parameter modulation schemes, more secure methods were proposed in [3] and [15]. In this paper, a modified parameter modulation scheme is proposed to further improve security. The numerical simulation shows that two popular attacks are ineffective to our method and the parameter has a high degree of security. In this modified parameter modulation scheme, a continuous chaotic system with a parameter is used to transmit encoded message. The parameter is generated by some cryptosystem which makes it have a lot of choices corresponding to transmitted bit "0" or "1," and thus be protected against the power analysis and return map attack. As for the construction of the cryptosystem, we use a 1-D discrete-time system controlled by a Δ-modulated feedback, which is quite different from [16] that uses the logistic map. The first reason that we use this Δ-modulated system is the simplicity and speciality of Δ-modulation, which makes it an attractive choice for control practitioners. Yet, there is few attention on the chaotic property of this kind of system. Another reason is that the result can be easily extended to high-dimensional Δ-modulated control systems, which will make the cryptosystem more secure. The complex behavior of this simple control system due to Δ-modulated feedback has been investigated in [10], [21]–[24]. When some parameter $a > 2$ in this particular 1-D discrete system, the system is chaotic ([23], [24]) but not a self-map. Note that the construction of a cryptosystem needs a self-map. In this paper, we prove that when $a \in (\sqrt{2}, 2]$ the system is chaotic and also a self-map.

In the next section, we prove that the 1-D discrete system controlled by a Δ-modulated feedback is chaotic when the parameter $a \in (\sqrt{2}, 2]$. Then two basic requirements for security and the framework of our method are given in Section III. With the help of Lorenz system and a secure cryptosystem based on Δ-modulated feedback control system, our method is also illustrated in detail in Section III. In Section IV, the security of our method is analyzed by numerical simulation. The conclusion is given in Section V.

II. 1-D Discrete System Controlled by Δ-Modulated Feedback

As mentioned in the Introduction, a chaotic discrete self-map is used to construct a secure chaotic cryptosystem. Hence, we introduce the 1-D discrete time chaotic system [23], [24]

$$x^{+}=ax-\Delta\mathrm{sgn}\,(ax), \quad \text{where } \mathrm{sgn(x)} = \begin{cases} 1, & x \geq 0 \\ -1, & x < 0. \end{cases} \tag{1}$$

x^{+} denotes the system state at the next discrete time, a is a real number, and Δ is a positive constant. In [24], the authors proved that (1) is chaotic when $|a| > 2$. In this section we consider $1 < |a| \leq 2$. For simplicity, we only consider $a \in (1, 2]$. We will show that this map is chaotic and maps an interval to itself, when the parameter $a \in (\sqrt{2}, 2]$. Hence, it can be used to implement a similar cryptographic algorithm as proposed in [16]. Based on this algorithm, we illustrate the parameter modulation scheme.

Performing a state transformation $y = x/\Delta$, then a new map is obtained

$$y^{+} = f(y), \quad \text{where } f(y) = \begin{cases} ay - 1, & y \geq 0 \\ ay + 1, & y < 0. \end{cases} \tag{2}$$

When $a = 2$, this map is equivalent to Baker's map which is chaotic [11]. Hence, in the following we only consider the case $a \in (1, 2)$. When $a \in (1, 2)$, f is surjective on $[-1, 1)$. Before

Manuscript received October 15, 2007. First published June 24, 2008; last published July 16, 2008 (projected). This paper was recommended by Associate Editor J.-P. Barbot.

The authors are with Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Pretoria 0002, South Africa (e-mail: lxiyin@up.ac.za; jfzhang@tuks.co.za; xxia@postino.up.ac.za).

Digital Object Identifier 10.1109/TCSII.2008.921585

stating our main result, the following well-known and frequently used definitions are recalled from [8].

Definition 1: ([8]) Consider a map: $F : I \to I$, where I is an interval, F is *topologically transitive* on I if for any two open sets $U, V \subset I$ there exists an integer $n > 0$ such that $f^n(U) \cap V \neq \emptyset$.

Definition 2: ([8]) Consider a map: $F : I \to I$, where I is an interval, F has *sensitive dependence on initial conditions* if there exists a $\delta > 0$ such that, for any $x \in I$ and any neighborhood N of x, there exist a $y \in N$ and an $n > 0$ such that $|F^n(x) - F^n(y)| > \delta$.

Definition 3: ([8]) Let X be a metric space. A map $F : X \to X$ is said to be *chaotic* on X if :

1) F is transitive;
2) the periodic points of F are dense in X;
3) F has sensitive dependence on initial conditions.

In the above definitions F may not be continuous (cf. [8]). The following lemma can be found in [20] and [12].

Lemma 1: If $a > \sqrt{2}$, then :

1) there is an integer n such that $f^n(J) = [-1, 1)$, where J is a subinterval in $[-1, 1)$;
2) f is topologically transitive;
3) f has sensitive dependence on initial conditions.

In order to prove that the periodic points of f is dense, we define $V_n = \{x \neq 0 | f^n(x) = 0, x \in [-1, 1)\}$ and $\hat{x}_n = \min\{x | x \in V_n \cap [0\ 1)\}$. Obviously, the number of the points in V_n is 2^n at most. From (2), we can obtain that $f^n(-x) = -f^n(x)$ if $f^i(x) \neq 0, i = 1, 2, \ldots, n-1$. In the neighborhood of the discontinuous point 0, we have $\lim_{x \to 0^-} f^n(x) = -f^n(0)$.

Lemma 2: The set $\bigcup_{i=1}^{\infty} V_i$ is dense on $I = [-1, 1)$.

Proof: Owing to $a > 1$, for any open interval U in I which does not include 0, the length of $f^i(U)$ is larger than the length of $f^{i-1}(U)$. Hence, there exists an integer n such that f^n is continuous on U and $0 \in f^n(U)$. Then there is an point $x \in U$ such that $f^n(x) = 0$, and thus $x \in V_n$ and $\bigcup_{i=1}^{\infty} V_i$ is dense on I.

Lemma 3: For any integer N, there exists an integer $m > N$ such that $f^m(0) \in [-1, -1/a]$ or $f^m(0) \in [1/a, 1)$.

Proof: If 0 is a periodic point with period k, then $f^{Nk+1}(0) = -1$.

If 0 is not a periodic point and this lemma does not hold, then there exists an integer N_1 such that $f^n(0) \notin [-1, -1/a] \cup [1/a, 1)$ for all the integer $n \geq N_1$. If $x_0 = f^{N_1}(0) \in (-1/a, 0)$, then $x_1 = f^{N_1+1}(0) \in (0, 1/a)$. Following the same way, we obtain that $x_i = f^{N_1+i}(0) < 0$ when i is even and $x_i = f^{N_1+i}(0) > 0$ when i is odd. After a simple computation, it is obtained that $x_{2i} = [a^{2i}(ax_0 + x_0 + 1) - 1]/(a + 1)$. Because 0 is not a periodic point, $x_0 \neq -1/(a+1)$. Hence, there exists an even integer $2i$ such that $x_{2i} > 0$ or $x_{2i} \leq -1/a$. It contradicts with $x_{2i} \in (-1/a, 0)$. For the other case $x_0 \in [0, 1/a)$, the same conclusion is obtained similarly.

Lemma 4: Assume $a > \sqrt{2}$, for any integer $k > 0$, there exist an integer n and $x_{n+1} \in V_{n+1}$, such that $n > k$, $x_{n+1} < \hat{x}_n < \hat{x}_k$ and $(x_{n+1}, \hat{x}_n) \cap V_i = \emptyset$, $i = 1, 2, \ldots, n+1$.

Lemma 5: The set of periodic points of f is dense in $I = [-1\ 1)$ when $a > \sqrt{2}$.

The proofs of the above two lemmas are given in the Appendix. The idea in the proof for Lemma 4 comes from [5]. By Lemma 1 and 5, we have the following theorem:

Theorem 1: The map defined in (2) is chaotic in $I = [-1, 1)$ when $a \in (\sqrt{2}, 2]$.

III. Chaotic Synchronization Combined With Cryptographic Technique

A. Basic Requirements and the Framework of Our Method

As said in the Section I, security is one of the most important problems in chaotic synchronization. In our opinion, if a chaos-based scheme is secure, it must satisfy the following two basic requirements.

1) The plaintext can not be extracted when the opponent does not know the keys.
2) The keys have a high degree of security.

Obviously, many parameter modulation methods do not satisfy the first requirement. With these methods, the parameter has two states corresponding to "1" and "0." However, the change of the parameters results in the change of the dynamic properties of the chaotic system. Hence, the power analysis or return map attack is easy to distinguish the two states. With reference to the classical cryptography, the system parameters of the chaotic systems can be treated as the secret key. However, as pointed out in [4], many robust and adaptive control methods could be considered for possible attack against secure communication and encryption scheme. That is, the keys have a low degree of security. To solve these problems, we use an encryption function to protect the system parameter.

We consider a continuous chaotic system as

$$\begin{cases} \dot{x} = f(x, p) \\ y = h(x) \end{cases} \tag{3}$$

where $x \in R^n, y \in R^m$ and $p \in R^l$ are the state variable, output, and parameter vector, respectively. The classical parameter modulation method is to change the parameter p with the binary encoded plaintext, namely, p has two states corresponding to "1" or "0" of the plaintext. Our method consists of three steps.

1) Encryption $p = e(P)$, that is, a chaotic encryption function e is applied to encrypt the plaintext P and produce the parameter p;
2) Synchronization: It is not difficult to construct an adaptive observer to estimate the state and parameter at the same time, since many papers concentrate on this topic [2], [26];
3) Decryption $P' = \mathrm{de}(p')$, the inverse of the encryption de is applied to recover the plaintext, once we obtain the estimated parameter value p'.

Without the encryption information, the opponents can not know the plaintext, even they can estimate the parameters. In the following subsections, we illustrate our method by using an cryptographic algorithm introduced in [16].

B. Chaotic Cryptosystem Based on a Δ-Modulated Feedback Control System

A chaotic cryptosystem is proposed by Pareek *et al.* in [16] based on the logistic map, $y = g_\lambda(x) = \lambda x(1 - x)$. It is a symmetric key block cipher which utilizes the essence of chaos, that

is, sensitivity on initial condition as well as on system parameter. It should be noted that the logistic map's chaotic parameter range is $3.57 \leq \lambda \leq 4$.

Now we recall the basic procedure of encryption as well as decryption from [16]. The plaintext and the ciphertext are divided into blocks of 8 bits, since ASCII is an 8-bit code which represents 256 characters

$$P = P_1 P_2 \dots P_n \text{ (plaintext)}$$
$$C = C_1 C_2 \dots C_n \text{ (ciphertext)}$$

where P_i and C_i are single blocks of 8-bits, n is the block length of the plaintext/ciphertext. An external 128-bits secret key $K = K_1 K_2 \dots K_{16}$, is also divided into blocks of 8 bits, where K_i, the session key, is of 8-bits, and the block length is $128/8 = 16$. Let $i = 1$, and do the following steps.

1) Define two real number X_s and N_s by
$$X_s = \frac{((K_1)_2 \oplus (K_2)_2 \oplus \cdots \oplus (K_{16})_2)_{10}}{M}$$
$$N_s = (K_1 + K_2 + \cdots + K_{16}) \bmod 256$$
where $M = 256$ (M can be 2^k for any integer $k \geq 8$), K_j and $(K_j)_2$ are the jth session key's ASCII value and binary equivalent of the ASCII value, respectively, $j = 1 \dots 16$. The notation $()_{10}$ is the decimal equivalent of the corresponding binary number, and $\oplus$ is the XOR operation.
2) Choose a K_r randomly from $\{K_1, \dots, K_{16}\}$, and let $X = (X_s + (K_r/M)) \bmod 1$ and $N = N_s + K_r$, where $x \bmod 1 = x - \lfloor x \rfloor$, and $\lfloor x \rfloor$ is the floor (also called truncation) function.
3) Let $\lambda_i = \big((bY_i + c) \bmod m\big)/200 + 3.57$, where $Y_i = (bY_{i-1} + c) \bmod m$, $b = 16, c = 7, m = 81, Y_1 = 0$.
4) Define the encryption/decryption in the following way:
$$C_i = (P_i + \lfloor X_{\text{new}} M \rfloor) \bmod 256 \text{ (encryption)}$$
$$P_i = (C_i + 256 - \lfloor X_{\text{new}} M \rfloor) \bmod 256 \text{ (decryption)} \quad (4)$$
where $X_{\text{new}} = g^N_{\lambda_i}(X)$, and $g^N_{\lambda_i}(X)$ is obtained by iterating the logistic map $g_{\lambda_i}(x) = \lambda_i x(1-x)$ for N times at X.
5) Put the symbols corresponding to the ASCII values of C_i/P_i obtained in steps 4) as the ciphertext/plaintext. If $i = n$, then stop the algorithm, otherwise let $X_s := X_{\text{new}}$, $N_s := C_i$ and $i := i + 1$, and go to step 2).

In order to apply Δ-modulated feedback control system to transmit information by chaotic synchronization, we modify system (2) as

$$x_{j+1} = F_a(x_j) := \begin{cases} \frac{\text{round}(\text{Max}_j)}{M} - 1, & x_j \geq 0 \\ \frac{\text{round}(\text{Max}_j)}{M} + 1, & x_j < 0 \end{cases} \quad (5)$$

round (x) is the roundoff function, and for any integer $k \geq 10$, x_j belongs to the set

$$P = C = \left\{0, \pm\frac{1}{M}, \dots, \pm\frac{M-1}{M}\right\}, \quad \text{where } M = 2^k. \quad (6)$$

Compared with the chaotic range $[3.57, 4]$ of the logistic map, the parameter of system (2) has wider chaotic range, $(\sqrt{2}, 2]$. Hence, to construct the above cryptosystem, we modify step 3) and step 4) and keep the other steps:

3') Let $a_i = \big((bY_i + c) \bmod m\big)/200 + 1.42$, where $Y_i = (bY_{i-1} + c) \bmod m$, $b = 16, c = 7, m = 96$, and $Y_1 = 0$. Obviously, $a_i \in [1.42, 2)$.

4') Let X_{new} be $F^N_{a_i}(X)$, where $F^N_{a_i}(X)$ is obtained by iterating F_{a_i} for N times at the point X. Then define the encryption/decryption in the following way:

$$C_i = (P_i + \lfloor X_{\text{new}} M \rfloor) \bmod 256 \text{ (encryption)}$$
$$P_i = (C_i + 256 - \lfloor X_{\text{new}} M \rfloor) \bmod 256 \text{ (decryption)}. \quad (7)$$

To construct a new cryptosystem based on system (5), we first select a parameter value $M = 2^k$ for some $k \geq 10$, then execute step 1), 2), 3'), 4') and 5) to get a more secure cryptosystem.

C. Detailed Illustration of Our Method

Now we illustrate our method with the help of the celebrated Lorenz system. According to (3), the Lorenz system with output is written as

$$\begin{cases} \dot{x}_1 = -\sigma_1 x_1 + \sigma_2 x_2 \\ \dot{x}_2 = \rho x_1 - x_2 - x_1 x_3 \\ \dot{x}_3 = x_1 x_2 - \beta x_3 \\ y = x_1. \end{cases} \quad (8)$$

It is well known that the system exhibits chaotic behavior with the standard parameters $(\sigma_1, \sigma_2, \rho, \beta) = (10, 10, 28, 8/3)$. For the classical parameter modulation scheme [9], the parameter σ_1 is modulated by binary encoded plaintext, so that it is $\sigma_1 + \delta$ if the plaintext bit is "1" and $\sigma_1 - \delta$ if the plaintext bit is "0," where δ is a constant. Our proposed method consists of three steps.

Step 1 (Encryption): Let $P = P_0 P_1 \dots P_n$ be the plaintext sequence, where P_i is a plaintext block of length 8 bits. Following the procedure introduced in Subsection 3.2, X_{new} is generated is step 4') and C_i is obtained through (7), then we let $\sigma_1 = 10 + C_i/M$. The index r of K_r can be transmitted through the parameter ρ, that is, $\rho = 28 + r/16$.

Step 2 (Synchronization): Construct an adaptive observer as introduced in [2] to estimate the state and parameters simultaneously. When the synchronization is achieved, we have $|\sigma_1 - \sigma_1'| < \epsilon$ and $|\rho - \rho'| < \epsilon$, where σ', ρ' are the estimated parameters and ϵ is a small enough positive constant.

Step 3 (Decryption): At the receiver end, the same X_{new} can be generated by the discrete chaotic system in the step 4') of Subsection 3.2, once r is estimated. Then P_i is obtained through (7).

Remark: In the classical parameter modulation method, the parameter p has two states corresponding to "1" or "0" of the plaintext. This method only transmits one bit when the synchronization is achieved. Compared with classical parameter modulation scheme, σ_1 has more choices in our method. The plaintext P_i is a block of 8-bits, thus our method also can transmit more information.

IV. Security Analysis With Simulation Results

Now we use system (8) to transfer the plaintext "Chaotic cryptosystem" with the secret key "wh91-qa9g-k*xd/.." and the estimated value of the ciphertext C_i which is obtained by the adaptive observer introduced in [2]. The initial conditions of state variables and estimated state variables $\hat{x}$ are [0.1 0.2 0.3] and [0.4 0.5 0.6], respectively. The initial conditions of estimated parameters $\hat{p}$ and $\hat{r}$ both are 1. As for he other variables in the observer, $S_x(0) = I$, $S_\theta(0) = I$ and $\Lambda(0) =$

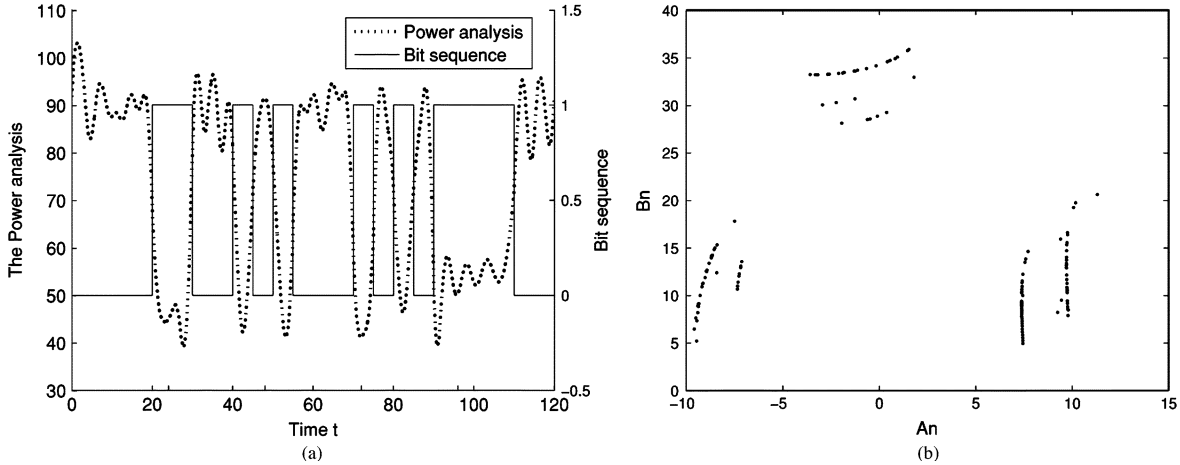

Fig. 1. For the transmitted signal generated by the classical parameter modulation: (a) bit sequence and the result of power analysis and (b) return map.

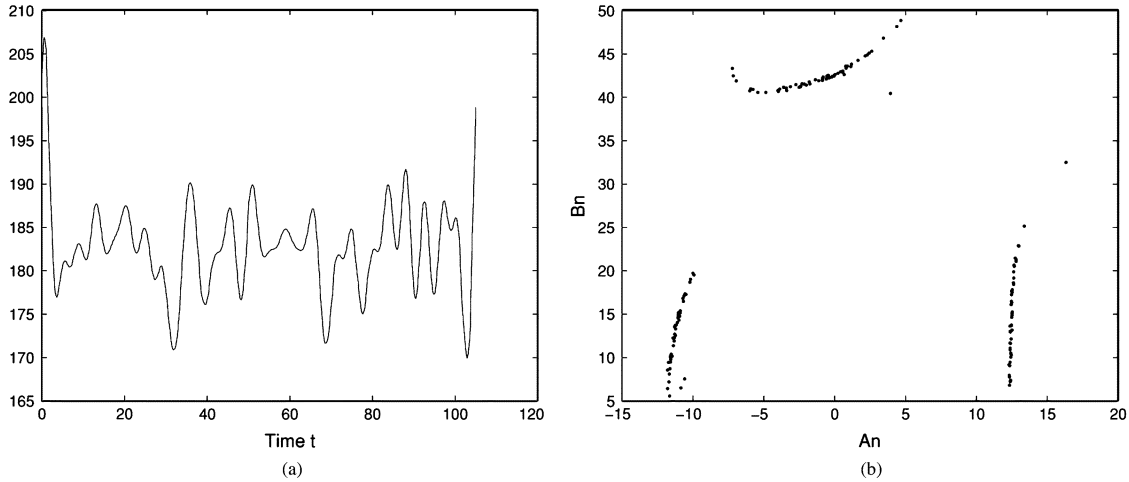

Fig. 2. For the transmitted signal generated by our method: (a) the result of power analysis and (b) return map.

$[10\ 10\ \ldots\ 10]$. As a comparison, we also use classical parameter modulation scheme to transfer a bit sequence [9], which is plotted in Fig. 1(a). In order to investigate the security of our proposed method, we consider two popular attacks developed in [1] and [18], that is, power analysis attack and return map attack. For the transmitted signal generated by classical parameter modulation scheme, the results of two attacks are plotted in Fig. 1. When the transmitted signal is generated by our method, the corresponding result is plotted in Fig. 2. The power analysis attack first filters the transmitted signal by a low-pass filter, and then recovers the plaintext utilizing a binary quantizer. Fig. 1(a) plots the bit sequence and the result of power analysis for the classical parameter modulation scheme. Fig. 2(a) is the result of power analysis under our method. Compared with Fig. 1(a), it is obviously that the attacker can not recovery the binary sequence "1" or "0" from Fig. 2(a). As described by Perez and Cerdeira [18], a small change in the parameters of the sender affects the attractor of chaotic system. Hence, a modified return map (A_n, B_n) is defined by $A_n = (X_n + Y_n/2)$, and $B_n = X_n - Y_n$, where X_n and Y_n are the nth local maximum and minimum of the transmitted signal, respectively. In Fig. 1(b), the plot of return map shows that all the segments are divided into two parts. Fig. 2(b) shows that all the segments merge together for different parameter. Then the attacker can not distinguish the parameter variations. Hence, the above two attack methods are ineffective to our scheme.

V. Conclusion

In this paper, a modified parameter modulation scheme, combined with cryptographic technique, is proposed to improve security. As a theoretical basis of the proposed communication scheme, we prove some 1-D discrete system controlled by a Δ-modulated feedback is chaotic when the parameter a is in $(\sqrt{2}, 2]$. This chaotic map is used to construct a secure cryptosystem which generates the parameter in the communication scheme. The complex parameter generating process improves much the security of the communication scheme, and numerical simulation shows that the two popular attacks, power analysis attack and return map attack, are ineffective to our communication scheme. The result will be extended to high dimensional discrete systems to further improve security.

Appendix

Proof of Lemma 4: For any integer $k > 0$, it follows from Lemma 1 that there exists N_k such that $f^{N_k}([0, \hat{x}_k]) = [-1, 1)$. Hence, $[0, \hat{x}_k] \cap V_i \neq \emptyset$ for all $i \geq N_k$. Therefore, for any integer k, there exists an integer $N > \max\{k, N_k\}$ such that $\hat{x}_m < \hat{x}_k$

for all $m > N$. Apply Lemma 3 for this integer N, then there exists an integer $n > N$ such that $f^n(0) \in [-1, -1/a]$ or $f^n(0) \in [1/a, 1)$. Now we consider the first case of $f^n(0) \in [1/a, 1)$. This case includes the following two subcases: $(0, \hat{x}_n) \cap V_i = \emptyset$ for all $i < n$ and $(0, \hat{x}_n) \cap V_i \neq \emptyset$ for some $i < n$.

i) If $(0, \hat{x}_n) \cap V_i = \emptyset$ for all $i < n$, then $f^n([0, \hat{x}_n]) = [f^n(0), 0] \supset [-1/a, 0]$ and f^n is continuous on $[0, \hat{x}_n]$. Hence, there exists a point $x' \in [0, \hat{x}_n]$ such that $f^n(x') = -1/a$. Then $x' \in V_{n+1}$ and $(x', \hat{x}_n) \cap V_i = \emptyset$ for all $i \leq n+1$.

ii) If $(0, \hat{x}_n) \cap V_i \neq \emptyset$ for some $i < n$, then there exists a maximal positive integer k_1, such that $0 < n - k_1 < n$ and the point $\hat{x}_{n-k_1} \in [0, \hat{x}_n]$. Thus, $f^{n-k_1}([0, \hat{x}_n]) = [f^{n-k_1}(0), f^{n-k_1}(\hat{x}_n)]$ and $f^{n-k_1}(0) < 0 < f^{n-k_1}(\hat{x}_n)$. Now we prove that there exists a point $x_1 \in (\hat{x}_{n-k_1}, \hat{x}_n)$ such that $f^{n-k_1}(x_1) = -f^{n-k_1}(0) < f^{n-k_1}(\hat{x}_n)$. If it does not hold, then there is a point $x_2 \in (0, \hat{x}_n)$ such that $f^{n-k_1}(x_2) = -f^{n-k_1}(\hat{x}_n)$. Hence, $f^{k_1}(f^{n-k_1}(x_2)) = 0$ and $x_2 \in V_n$. It contradicts with the definition of $\hat{x}_n$, hence $-f^{n-k_1}(0) < f^{n-k_1}(\hat{x}_n)$. Because f^{n-k_1} is continuous and monotonic on $(\hat{x}_{n-k_1}, \hat{x}_n)$, there is a point $x_1 \in (\hat{x}_{n-k_1}, \hat{x}_n)$ such that $f^{n-k_1}(x_1) = -f^{n-k_1}(0)$. To find a point $x' \in V_{n+1}$ in $(x_1, \hat{x}_n)$ such that this lemma holds, it is also considered in two situations. Firstly, if $(x_1, \hat{x}_n) \cap V_i = \emptyset$ for all $i < n$, that is, $(-f^{n-k_1}(0), f^{n-k_1}(\hat{x}_n)) \cap V_i = \emptyset$ for all $i < k_1$, then $f^{k_1}(-f^{n-k_1}(0)) = -f^n(0) < f^{k_1}(f^{n-k_1}(\hat{x}_n)) = 0$. Since f^{k_1} is continuous on $(x_1, \hat{x}_n)$, there exists a point x' such that $f^{n+1}(x') = f(f^n(x')) = f(-1/a) = 0$. Hence, $x' \in V_{n+1}$ and $(x', \hat{x}_n) \cap V_i = \emptyset$ for $i \leq n+1$. Secondly, if $(x_1, \hat{x}_n) \cap V_i \neq \emptyset$ for some $i < n$, then there exists a maximal positive integer $k_2 < k_1$ such that the point $x_{n-k_2} \in (x_1, \hat{x}_n)$, where $x_{n-k_2} \in V_{n-k_2}$. Because the number of points in V_i is finite for all $i \leq n$, we can repeat the above procedure until we find a point x' such that this lemma holds.

As for the second case of $f^n(0) \in [-1, -1/a]$, by the fact that $\lim_{x \to 0-} f^n(x) = -f^n(0)$, the same conclusion is obtained.

Proof of Lemma 5: For any interval $[\alpha, \beta] \subset [0, \delta]$ where $0 < \delta < 1/2$, it follows from Lemma 2 that there is an $x_n \in V_n$ in (α, β). Since the number of the points in V_i is finite for all $i \leq n$, there exists also an $x_{n+k} \in V_{n+k}$ in (x_n, β) such that $(x_n, x_{n+k}) \cap V_i = \emptyset$ for all $i \leq n+k$. Hence, $f^n([x_n, x_{n+k}]) = [0, \hat{x}_k]$ and continuous on $[x_n, x_{n+k}]$. By Lemma 4, there are two points $x_{m+1} < \hat{x}_m$ in $(0, \hat{x}_k)$ such that $(x_{m+1}, \hat{x}_m) \cap V_i = \emptyset$ for all $i \leq m+1$, where x_{m+1} is some point in V_{m+1}. Because f^n is continuous and monotonic on $[x_n, x_{n+k}]$, there are two points $x_2 < x_1$ in (x_n, x_{n+k}) such that $f^n(x_2, x_1) = (x_{m+1}, \hat{x}_m)$ and $(x_2, x_1) \cap V_i = \emptyset$ for all $i \leq m+n+1$. Therefore, $f^{m+n}([x_2, x_1]) = [-1/a, 0]$ and f^{m+n} is continuous on $[x_2, x_1]$. Hence, there exists a small enough positive ε such that $[x_2, x_1 - \varepsilon] \subset f^{m+n+1}([x_2, x_1 - \varepsilon])$ and f^{m+n+1} is continuous on $[x_2, x_1 - \varepsilon]$. Therefore, there is a periodic point in $[\alpha, \beta]$.

Now we consider any interval $K \subset I$. By Lemma 1, this K is contained in $f^i([0, \delta])$ for some i. Since the set of periodic points of f is dense in $[0, \delta]$, we can find a periodic point p in $[0, \delta]$ and $f^i(p)$ in K.

REFERENCES

[1] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Breaking parameter modulated chaotic secure communication system," *Chaos, Solitons Fractals*, vol. 21, no. 4, pp. 783–787, 2004.

[2] G. Besançon, J. De. León-Morales, and O. Huerta-Guevara, "On adaptive observers for state affine systems," *Int. J. Contr.*, vol. 79, no. 6, pp. 581–591, 2006.

[3] S. Bu and B.-H. Wang, "Improving the security of chaotic encryption by using a simple modulating method," *Chaos, Solitons Fractals*, vol. 19, no. 4, pp. 919–924, 2004.

[4] S. Celikovsky and G. Chen, "Secure synchronization of a class of chaotic systems from a nonlinear observer approach," *IEEE Trans. Autom. Contr.*, vol. 50, no. 1, pp. 76–82, Jan. 2005.

[5] Y. Choi, "Attractors from one dimensional Lorenz-like maps," *Discrete Continuous Dyn. Syst.*, vol. 11, no. 2/3, pp. 715–730, 2004.

[6] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 40, no. 10, pp. 626–633, Oct. 1993.

[7] K. Cuomo and A. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, no. 1, pp. 65–68, 1993.

[8] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems*. Reading, MA: Addison-Wesley, 1989.

[9] M. Feki, "An adaptive chaos synchronization scheme applied to secure communication," *Chaos, Solitons Fractals*, vol. 18, no. 1, pp. 141–148, 2003.

[10] R. Gai, X. Xia, and G. Chen, "Complex dynamics of systems under Delta-modulated feedback," *IEEE Trans. Autom. Contr.*, vol. 51, no. 12, pp. 1888–1902, Dec. 2006.

[11] P. Glendinning, "Stability, instability and chaos," in *Cambridge Texts in Applied Mathematics*. Cambridge, U.K.: Cambridge Univ. Press, 1994.

[12] J. Guckenheimer and P. Holmes, *Nonlinear Oscillations, Dynamical Systems, and Bifurcations of Vector Fields*. New York: Springer, 1983.

[13] D. Herve, K. M. Peter, and H. Martin, "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process.*, vol. 40, no. 10, pp. 634–642, Oct. 1993.

[14] Z.-P. Jiang, "A note on chaotic secure communication systems," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 49, no. 1, pp. 92–96, Jan. 2002.

[15] P. Palaniyandi and M. Lakshmanan, "Secure digital signal transmission by multistep parameter modulation and alternative driving of transmitter variables," *Int. J. Bifurc. Chaos*, vol. 11, no. 7, pp. 2031–2036, 2001.

[16] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using external key," *Phys. Lett. A*, vol. 309, no. 1/2, pp. 75–82, 2003.

[17] L. Pecora and T. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–825, 1990.

[18] G. Pérez and H. Cerdeira, "Extracting messages masked by chaos," *Phys. Rev. Lett.*, vol. 74, no. 11, pp. 1970–1973, 1995.

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

[20] R. F. Williams, "The structure of Lorenz attractors," *Publ. Math. IHES*, vol. 50, pp. 73–99, 1979.

[21] X. Xia and A. S. I. Zinober, "Delta-modulated feedback in discretization of sliding mode control," *Automatica*, vol. 42, pp. 771–776, 2006.

[22] X. Xia and A. S. I. Zinober, "Periodic orbits from Delta-modulation of stable linear systems," *IEEE Trans. Autom. Contr.*, vol. 49, no. 8, pp. 1376–1380, Aug. 2004.

[23] X. Xia, R. Gai, and G. Chen, "Periodic orbits arising from Delta-modulated feedback control," *Chaos, Solitons, Fractals*, vol. 19, pp. 581–595, 2004.

[24] X. Xia and G. Chen, "On delta-modulated control: A simple system with complex dynamics," *Chaos, Solitons, Fractals*, vol. 33, pp. 1314–1328, 2007.

[25] T. Yang, C. Wu, and L. Chua, "Cryptography based on chaotic systems," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 44, no. 5, pp. 469–472, May 1997.

[26] Q. Zhang, "Adaptive observer for multiple-input-multiple-output (MIMO) linear time-varying systems," *IEEE Trans. Autom. Contr.*, vol. 47, no. 3, pp. 525–529, Mar. 2002.