2007 International Symposium on Nonlinear Theory and its Applications
NOLTA'07, Vancouver, Canada, September 16-19, 2007

Chaotic Modulator with Volterra Filter for Cipher

Kazuma Iwata[†], Tsuyoshi Nakamura[†], Toshiyuki Ikeue[†], Hiroyuki Irikura[†] and Hiroyuki Kamata[‡]

[†]Graduate School of Science and Technology, Meiji University
1-1-1 Higashi-mita, Tama-ku, Kawasaki 214-8571, JAPAN
[‡] School of Science and Technology, Meiji University
1-1-1 Higashi-mita, Tama-ku, Kawasaki 214-8571, JAPAN,
Email: kamata@isc.meiji.ac.jp

Abstract– This paper proposes the chaotic modulator with Volterra filter for cipher and secure communications. To achieve the practical chaotic modulator, the system supposes to use the digital communication line, such as the Internet, to maintain the parameter matching between the transmitter and receiver sides. Therefore, the higher coefficient sensitivity is requested when the parameters are mismatched. In particular, the information transmission is done in each packet that the length is 1500[byte] or less; therefore, when the parameter does not adjust, the chaotic system is necessary to shift to other orbits extremely quick.

In this paper, the chaotic cipher with high coefficient sensitivity is proposed and the robustness is evaluated.

1. Introduction

The ciphers and secure communications are typical applications of the chaotic system; various systems with chaos have been proposed[1,2]. The reason why chaos can be used for the cipher is based on the characteristics of chaos. The reasons are (1) the Sensitive Dependence on Initial Conditions, (2) Orbital Instability and (3) Long-term Unpredictability. By these properties, the transfer of correct information becomes possible only when the parameters and the initial values are perfectly corresponding between the transmitter and the receiver.

In addition, these features request the chaotic signal to be transmitted perfectly from transceiver to receiver. Therefore, the use of a digital transmission line or the internal processing of digital computer is practical field of the chaotic system[2].

However, when the chaotic system is realized by computer that carries out the finite bit-length arithmetic, the generated signal becomes pseudo chaos; the properties that chaos originally have are deteriorated. It is impossible to avoid that the generated signal becomes pseudo chaos; therefore, it is necessary to improve sensitive to the parameter mismatch by other approaches.

In particular, the information transmission by Internet is done in each packet that the length is 1500[byte] or less; therefore, the orbit of the chaotic system is needed to shift to the different orbit extremely quick when the parameters are different between the transmitter and receiver.

In this paper, we propose a practical chaotic system for cipher and secure communications. The system is based on the modification of the chaotic neuron type nonlinearity[2]. The chaotic neuron[3] is composed by a nonlinear map and a synchronizing equation on both sides of transmitter and receiver. To improve the parameter sensitivity of the system, two ideas are proposed. One idea is to use a modified Tent map in the nonlinear map[4]. The other idea is to change the synchronizing equation to Volterra filter[5].

In this paper, the proposed chaotic system is explained, and the effectiveness of the system is shown by experimentation.

2. Chaotic Modulator

First, modified chaotic neuron type nonlinearity is proposed as follows:

$$x_1(n) = s(n) - g\left\{x_1(n-1)\right\} + \alpha x_{m+1}(n-1) + \theta_1 \tag{1}$$

$$\begin{aligned} x_2(n) &= \theta_2 + \sum_{i=1}^{m+1} h_i x_i(n-1) \\ &+ \sum_{i=1}^{m+1}\sum_{j=1}^{m+1} h_{ij} x_i(n-1) x_j(n-1) + \cdots + h_{123\cdots m+1} \prod_{i=1}^{m+1} x_i(n-1) \end{aligned} \tag{2}$$

$$x_{2+(i-1)}(n) = x_2(n-i+1) : i = 2, 3, \cdots, m\,. \tag{3}$$

Where, the $s(n)$ shows the information signal that should be encrypted, $x_1(n)$, $x_2(n)$,,, are the internal state variables of the system, and h_i, h_{ij},,, are coefficients that are the private keys of the cipher.

Besides, Eq. (1) shows a nonlinear map based on the chaotic neuron, and Eq. (2) and Eq. (3) show the m-th order Volterra filter. Volterra filter is a nonlinear digital filter that contains the multiplication of internal state variables with coefficients.

In the Eq. (1), $g\{x\}$ is a nonlinear function. We have been examining the chaotic modulator by using the next expression for the function.

$$g_{old}\{x\} = \begin{cases} \kappa x + \sigma & : x \le -\varepsilon \\ \dfrac{\kappa\varepsilon - \sigma}{\varepsilon} x & : -\varepsilon < x < \varepsilon \\ \kappa x - \sigma & : x \ge \varepsilon \end{cases} \tag{4}$$

The reason is that the expression is suitable for use by fixed-point arithmetic. However, the numeric width after mapping is limited according to the coefficient value of κ, σ and ε. In this research, the modified Tent map shown in the next expression is newly used.

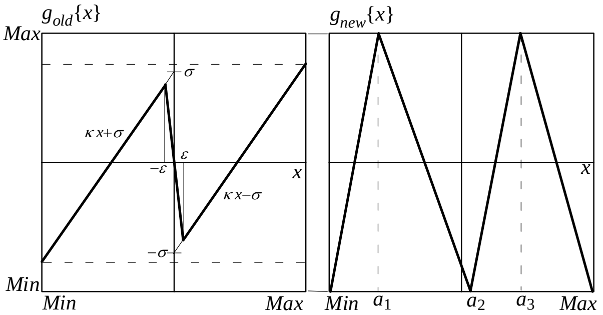


Fig. 1 Nonlinear functions $g_{old}\{x\}$ and $g_{new}\{x\}$.

$$g_{new}\{x\}=\begin{cases}\dfrac{(Min-Max)x+(Max-a_1)M\,\text{in}}{Min-a_1} & : x_{\min}\le x\le a_1\\ \dfrac{(Max-Min)x+(a_1Min-a_2Max)}{a_1-a_2} & : a_1<x\le a_2\\ \dfrac{(Min-Max)x+(a_2Max-a_3Min)}{a_2-a_3} & : a_2<x\le a_3\\ \dfrac{(Max-Min)x+(a_3Min-Max^2)}{a_3-Max} & : a_3<x\le x_{\max}\end{cases} \quad (5)$$

The form of the Eq. (4) and Eq. (5) are shown in Fig. 1. In this study, we have confirmed that the $g_{new}\{x\}$ is also effective in increasing the Lyapunov exponents compared with the $g_{old}\{x\}$.

Besides, the signal that should be transmitted to the receiver is only $x_1(n)$: n=0,1,2,,, in Eq. (1). Therefore, the demodulator of the proposed system is shown as the inverse system of Eq. (1).

$$r(n)=x_1(n)+g\left\{x_1(n-1)\right\}-\alpha x_{m+1}(n-1)-\theta_1, \quad (6)$$

where, $r(n)$ is the recovered signal.

The $x_{m+1}(n\text{-}1)$ in Eq. (6) is generated by the same equations with Eq. (2) and Eq. (3) at the receiver side to keep the synchronization with the transmitter side.

3. Realization by the Fixed-point Arithmetic

In this research, this chaotic modulator is assuming the use of 16 bit fixed-point arithmetic that is carried out in the small CPU with high-performance, such as Digital Signal Processor[1]. In 16-bit fixed-point arithmetic, the addition, subtraction and multiplication can be executed with 32 bit accumulator. However, when the operation results shown by 32 bit-length are substituted for 16 bit-length variables, the overflow is generated. The overflow is effective to realize the boundness of the maps, various expressions can be applied[2].

Here, when the overflow function is shown as $O\{x\}$, Eq. (1) are rewritten as

$$x_1(n)=O\left\{s(n)-g\left\{x_1(n-1)\right\}+\alpha x_{m+1}(n-1)+\theta_1\right\}. \quad (7)$$

Based on the form of Eq. (7),

$$x_i(n)=O\left\{\hat{x}_i(n)\right\}: i=1,2,\cdots,m+1 \quad (8)$$

are assumed. By using this relation, Eq. (7) is rewritten as

$$\hat{x}_i(n)=s(n)-g\left\{O\left\{\hat{x}_1(n-1)\right\}\right\}+\alpha O\left\{\hat{x}_{m+1}(n-1)\right\}+\theta_1. \quad (9)$$

The derivative of the overflow function $O\{x\}$ can be assumed 1; so, even if each Eq. (1) and Eq. (9) is used, both Jacobian of the dynamics are corresponded by using the generated signal with overflow[2]. In this study, the characteristic analysis is carried out based on Eq. (1), Eq. (2) and Eq. (3).

4. Lyapunov Spectrum of the Proposed Modulator

In the m-th order Volterra Filter, many coefficients are included; so the characteristic evaluation of the system is difficult.

Then, the order of Volterra Filter is set to 2nd, and the characteristic evaluation is attempted.

$$x_1(n)=s(n)-g\left\{x_1(n-1)\right\}+\alpha x_3(n-1)+\theta_1 \quad (10)$$

$$\begin{aligned}x_2(n)&=\theta_2+\sum_{i=1}^{3}h_i x_i(n-1)\\ &+\sum_{i=1}^{3}\sum_{j=1}^{3}h_{ij}x_i(n-1)x_j(n-1)+h_{123}\prod_{i=1}^{3}x_i(n-1)\end{aligned} \quad (11)$$

$$x_3(n)=x_2(n-1) \quad (12)$$

The Jacobian of the dynamics becomes as follows.

$$\mathbf{J}(n)=\begin{bmatrix}-\dfrac{\partial}{\partial x_1}g\left\{x_1(n)\right\} & 0 & \alpha\\ J_{10} & J_{11} & J_{12}\\ 0 & 1 & 0\end{bmatrix}$$

$$\begin{aligned}J_{10}&=h_1+2h_{11}x_1(n)+(h_{12}+h_{21})x_2(n)\\ &\quad+(h_{13}+h_{31})x_3(n)+h_{123}x_2(n)x_3(n)\\ J_{11}&=h_2+2h_{22}x_2(n)+(h_{12}+h_{21})x_1(n)\\ &\quad+(h_{23}+h_{32})x_3(n)+h_{123}x_1(n)x_3(n)\\ J_{12}&=h_3+2h_{33}x_3(n)+(h_{13}+h_{31})x_1(n)\\ &\quad+(h_{23}+h_{32})x_2(n)+h_{123}x_1(n)x_2(n)\end{aligned} \quad (13)$$

In the case of the conventional chaotic neuron that used a linear digital filter, the terms J_{10}, J_{11} and J_{12} become constant values according to the coefficients of linear digital filter. If the Lyapunov spectrum is able to be estimated from the generated time series signal $x_1(n)$[6,7], this feature shows that the parameters which become private keys of the chaotic modulator can be presumed.

In the proposed system, each term J_{10}, J_{11} and J_{12} includes many coefficients and the generated signals $x_1(n)$, $x_2(n)$ and $x_3(n)$, respectively. Therefore, the Jacobian has the time variant characteristic, and presuming the private keys by the Lyapunov spectrum analysis based on the time series signal becomes extremely difficult.

Fig. 2(a) shows the maximum Lyapunov exponent of the proposed modulator. In the Fig. 2(c), the maximum Lyapunov exponent of the conventional system that uses linear digital filter is also shown for the comparison.

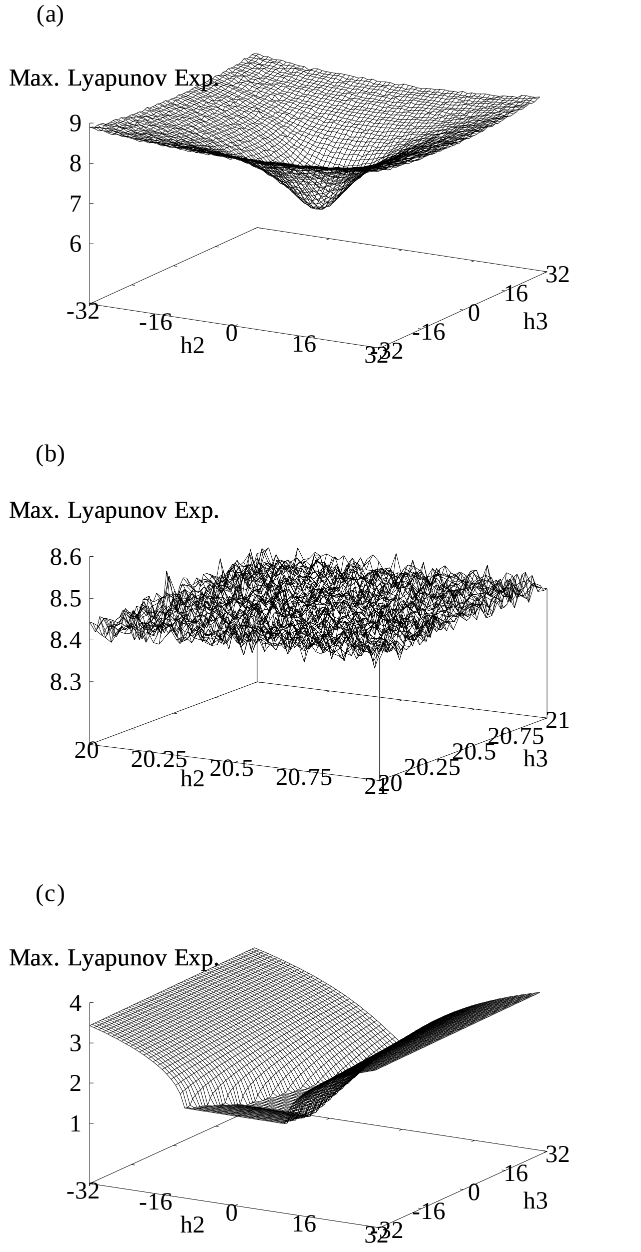


Fig. 2 Maximum Lyapunov exponent of the chaotic modulator with 2nd order Volterra filter.
Q10 format of fixed-point arithmetic is used.
Parameters: a_1= -16, a_2= 0, a_3= 16. θ= 0.138672. α =1.
(a), (b) :h_1=h_{11}=h_{12}= $\cdots$ =h_{123}=1.
(c) : h_1=1, h_{11}=h_{12}= $\cdots$ =h_{123}=0.(Linear filter is simulated)

As the Fig. 2(a) shows, the value of the Lyapunov exponent is larger than the result shown in Fig. 2(c). Furthermore, in the Fig. 2(b) that a part of Fig. 2(a) is expanded, the surface of the Lyapunov exponent becomes bumpy; therefore, the presumption of the parameters based on the calculation result of Lyapunov spectrum becomes more difficult.

5. Proposal of the Experimental Structures

The number of coefficients included in Eq. (11) becomes 14. When 16 bit fixed-point arithmetic is employed for the system realization, the number of combination by coefficients becomes $65,536^{14}$ $= 2.69\times10^{67}$. The hugeness of the number of combination is effective for the chaotic modulator and demodulator, and the robustness of the chaotic cipher and the secure communications can be obtained.

However, it is still difficult to evaluate the system for all of the combination. Then, the next two structures are attempted in this research.

5.1. Chaotic Modulator with Logistic Map

Chaotic modulator that includes Logistic map is expressed by Eq. (1) and the next Eq. (14).

$$x_2(n) = x_1(n-1) + ax_2(n-1)\left(1 - x_2(n-1)\right) \qquad (14)$$

The Jacobian of the dynamics becomes

$$\mathbf{J}(n) = \begin{bmatrix} -\dfrac{\partial}{\partial x_1} g\left\{x_1(n)\right\} & \alpha \\ 1 & a - 2ax_2(n) \end{bmatrix}. \qquad (15)$$

5.2. Chaotic Modulator with Henon Map

Chaotic modulator that includes Henon map is expressed by Eq. (1) and Eq. (16).

$$\begin{aligned} x_2(n) &= x_1(n-1) + 1 - ax_2^2(n-1) + bx_3(n-1) \\ x_3(n) &= x_2(n-1) \end{aligned} \qquad (16)$$

The Jacobian of the dynamics becomes

$$\mathbf{J}(n) = \begin{bmatrix} -\dfrac{\partial}{\partial x_1} g\left\{x_1(n)\right\} & 0 & \alpha \\ 1 & -2ax_2(n) & b \\ 0 & 1 & 0 \end{bmatrix}. \qquad (17)$$

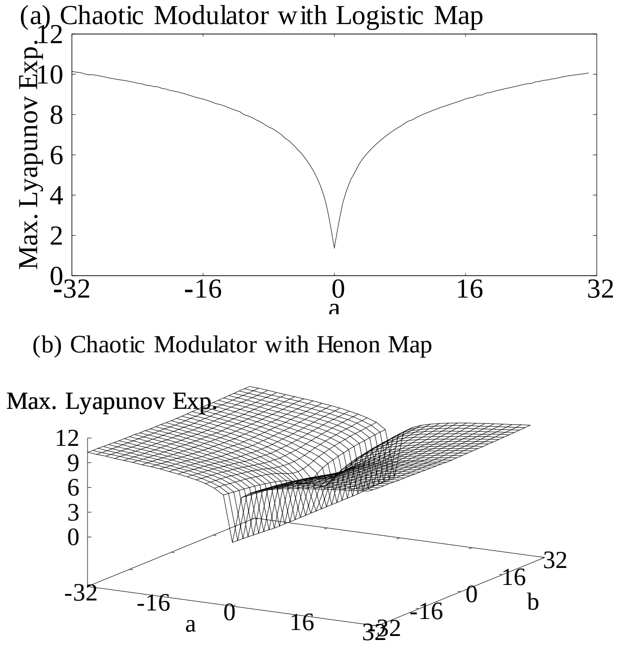
5.3. Properties of These Two Structures

The equation of each Logistic map and Henon map can be expressed as a kind of Volterra filter; however, the number of parameters is reduced, respectively.

Fig. 3 shows the Maximum Lyapunov exponent of these modulators. As the figure shows, the Lyapunov exponents indicate high values though the structure is simple. However, the bumpily characteristic as shown in Fig. 2(b) is lost.

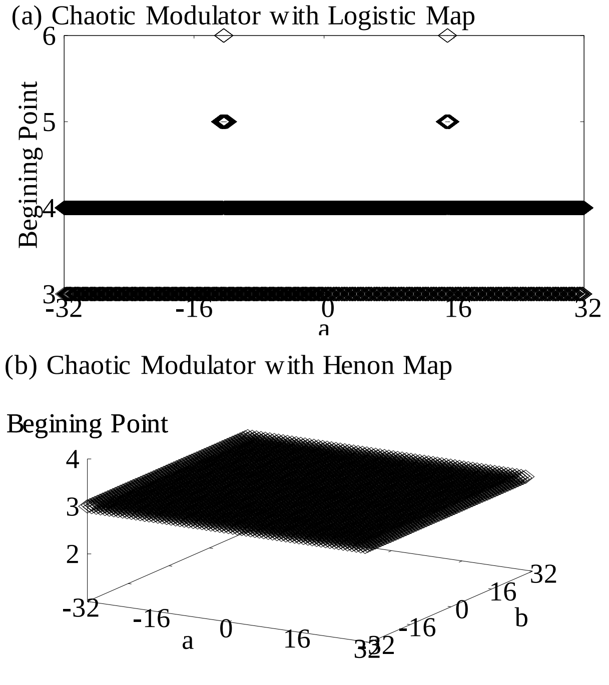
5.4. Robustness to the Parameter Mismatch

Because the system which generates the chaotic cipher can take a variegated structure, so it is first necessary to specify the structure for the decipherment. In this research, assuming that the structure of the chaotic modulator was clarified, the robustness of the system to parameter mismatch is verified. Namely, this verification is assumed the Brute Force Attack that tries to set the total combination of parameters.


(a) Chaotic Modulator with Logistic Map

(b) Chaotic Modulator with Henon Map

Fig. 3 Maximum Lyapunov Exponents.


(a) Chaotic Modulator with Logistic Map

(b) Chaotic Modulator with Henon Map

Fig. 4 Beginning point where shifts to the different orbit when a parameter of receiver side has minimum error. Q10 format is used.
(a), (b): a(Receiver)=a(Transmitter)+0.000977.
Other parameters are corresponding on both the transmitter and receiver sides.

By the Sensitive Dependence on Initial Conditions of chaotic map, if the parameters are different, the orbit of the chaotic system can be expected to shift quickly to another different orbit. In this section, the beginning point that shifts to a different orbit is measured when one of the parameters is different. The difference of the parameter on both sides of the transmitter and receiver is assumed to be a minimum difference that can be shown by the format of the fixed-point arithmetic.

Fig. 4 shows the experimental results of this verification. As the figure shows, the orbits are shifted to the different orbit in few samples when a parameter is different. This excellent characteristic is not obtained in the conventional method that used a linear filter. Particularly, when the chaotic modulator with Henon map is used, the orbit has changed by 3 samples in all thought parameters.

6. Conclusions

The novel chaotic modulator for chaotic cipher and secure communications has been proposed in this study. The proposed system includes the Volterra filter and the modified Tent map. By these attempts, extremely high sensitivity to the parameter mismatch can be obtained. However, the chaotic modulator with Volterra filter can realize various structures, an overall evaluation is insufficient. We will report on this research continuously in the future.

References

[1] H. Kamata, T. Endo and Y. Ishida, “Secure communication using chaos via DSP implementation” IEEE, Proc. ISCAS'96, Vol.3, pp.112-115, 1996.

[2] H. Kamata, Y. Umezawa, M. Dobashi, T. Endo and Y. Ishida, “Private communications with chaos based on the fixed-point computation” Trans. IEICE, Vol. E83-A, No. 6, 2000.

[3] K. Aihara, “Chaotic neural Netowork” Bifurcation Phenomena in Nonlinear Systems and Theory of Dynamical System, pp. 143-161, 1990.

[4] N. Masuda and K. Aihara, “Chaotic Cipher by Finite-State Baker’s Map” Trans. IEICE Vol. J82-A, No. 7, 1999(Japanese).

[5] M. Schetzen, “The Volterra and Wiener Theories of Nonlinear System” Wiley, 1980.

[6] M. Sano and Y. Sawada, “Measurement of the Lyapunov spectrum from a chaotic time series” Physical Review Letters, Vol.55, No.10 pp.1082-1085, 1985.

[7] J. P. Eckmann, S. O. Kamphorst, D. Ruelle and S. Ciliberto, “Lyapunov exponents from time series” Physical Review A, Vol. 34, No. 6, 1986.