World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:6, No:11, 2012

Study on the Evaluation of the Chaotic Cipher System Using the Improved Volterra Filters and the RBFN Mapping

Hirotaka Watanabe, Takaaki Kondo, Daiki Yoshida, Ariyoshi Nakayama,
Taichi Sato, Shuhei Kuriyama, and Hiroyuki Kamata

***Abstract*—**In this paper, we propose a chaotic cipher system consisting of Improved Volterra Filters and the mapping that is created from the actual voice by using Radial Basis Function Network. In order to achieve a practical system, 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, in order to withstand the attack from outside, it is necessary that complicate the internal state and improve the sensitivity coefficient. In this paper, we validate the robustness of proposed method from three perspectives of "Chaotic properties", "Randomness", "Coefficient sensitivity".

***Keywords*—**Chaos cipher, 16-bit-length fixed-point arithmetic, Volterra filter, Seacret communications, RBF Network.

I. Introduction

RECENTLY, digital communication network such as the internet has evolved significantly. As a result, the demand for secret communication is increasing. And, the chaotic cipher is a very effective means in the realization of secret communication [1]. The reason for it is based on the characteristics of the chaos: (1) the Sensitive Dependence on Initial Conditions, (2) Orbital Instability, (3) Long-term Unpredictability. By these properties, the correct transfer of information becomes possible only if an initial value and parameters are fully compatible between the sender and receiver.

We have studied and proposed the chaotic cipher using chaotic neuron and linear/nonlinear digital filters [2]. When the modem system using the proposed cipher is realized, the limited bit-length arithmetic with fixed decimal point is used in our study [3] [4] [5]. However, the signal generated by the finite bit length operation will become pseudo-chaos, characteristics of the chaos is lowered. 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.

H. Watanabe is with Graduate School of Science and Technology, Meiji University, 1-1-1 Higashi-mita, Tama-ku, Kawasaki-shi, Kanagawa, 214-8571 Japan (e-mail:ce11101@meiji.ac.jp).

H. Kamata is with School of Science and Technology, Meiji University, 1-1-1 Higashi-mita, Tama-ku, Kawasaki-shi, Kanagawa, 214-8571 Japan (e-mail:kamata@isc.meiji.ac.jp).

T. Kondo and D. Yoshida and A. Nakayama and T. Sato and S. Kuriyama are with Graduate School of Science and Technology, Meiji University, 1-1-1 Higashi-mita, Tama-ku, Kawasaki-shi, Kanagawa, 214-8571 Japan. (e-mail:ce11101@meiji.ac.jp).

In this paper, we examine to incorporate the nonlinear filters called Volterra Filter into the chaotic cipher system. Moreover, by using the Radial Basis Function Network (RBF Network) for pattern classification and function approximation problems, we aim to synthesize fluctuations of vocal cords from real voice and create a robust mapping [6]. Then, the system using these methods is proposed and the robustness is evaluated.

II. Property of the Fixed-Point Arithmetic

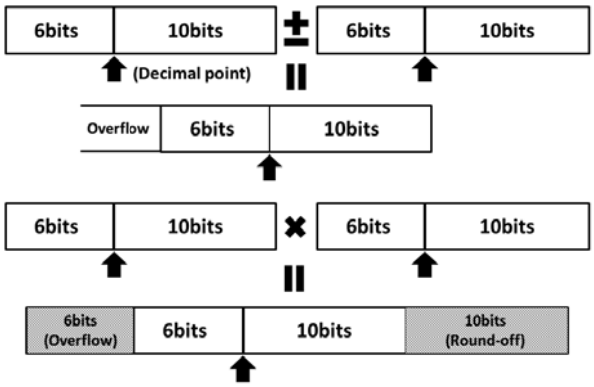

Fig. 1 Flow of the 16 bit-length Fixed-Point Arithmetic

In this study, the chaotic cipher system is assuming the use of 16 bit-length fixed-point arithmetic that used in the Digital Signal Processor. Fig. 1 shows the flow of the 16 bit length fixed-point arithmetic. In the figure, the decimal point is assumed to the tenth bit by the least significant bit. In this research, we call this format"Q_{10} Format".

When the Q_{10} Format is used, the overflow may occur during addition and subtraction. Moreover, when multiplication is carried out, because a calculation result is expressed in 32 bit-length data once, both the round-off and the overflow occur by the process that converts the result into 16 bit-length data. By the features on such calculations, the units of the Q_{10} format (Q_{10unit}), minimum value (Q_{10min}), maximum value (Q_{10max}) is as follows.

$$Q_{10unit} = 2^{-10} \cong 0.000977 \quad (1)$$

$$Q_{10\min} = -2^{16-10-1} \cong -32.000000 \quad (2)$$

$$Q_{10\max} = 2^{16-10-1} - Q_{10unit} = 31.999023 \quad (3)$$

In other words, the variables using the Q_{10} format can be operated in this limited range. This feature is effective, so any unstable linear and nonlinear digital filters can be realized with the boundedness by the overflow that occurs during operation. In this study, the feature of the Q_{10} Format has been used for the boundness property that is required for chaos can be realized.

III. Mapping of RBF Network

A. Fluctuation of Vocal Cords

At first glance, Speech waveform of the real voice seems to have a periodic structure. However, the shape of the waveform has been a slight change in every cycle, and that has been changed subtly in width of period accordingly. The difference in width of the period is called "fluctuation of vocal cords".

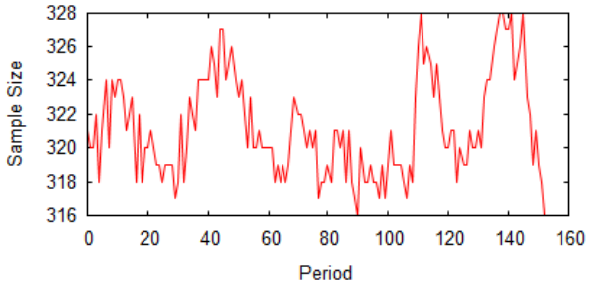

Fig. 2 The Fluctuation of Vocal Cords

B. RBF Network

RBF Network is a kind of deformed three-layer network, and by overlaying the localized basis functions called radial basis function, it has been considered as the way to complement any function as intended.

The formula that represents the structure of RBF Network that obtains one dimensional output $f(x)$ to k dimensional inputs is shown in (4).

$$f(x)=\sum_{i=0}^{M}\omega_i\varphi_i(r) \tag{4}$$

Here, $\varphi_i(r)$ is the basis function, ω_i is the coupling coefficient of it, M is the amount of it. Then, the basis function $\varphi_i(r)$ is using the Gaussian function as follows (5) and Fig. 3.

$$\varphi_i(r)=\exp(-\frac{\|x_k-\mu_i\|}{2\sigma^2}) \tag{5}$$

In addition, we have given 3 dimensional that is number of internal state variables in chaotic cipher to k. Here, x_k is input vector, and σ is variance. μ_i is center vector of the i-th, and it is determined depending on the number of radial basis function. And, the interior of "|| ||" shows the Euclidean norm. The weights ω_i can be obtained by using the least squares method. Result of RBF Network is vary greatly by the value of these center vectors and M.

The structure of the RBF Network is shown in Fig. 4. In this study, we call this mapping "RBFN Mapping".

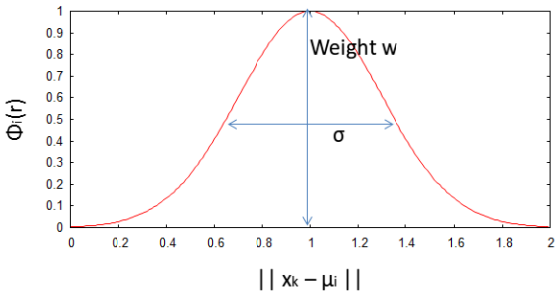

Fig. 3 Gaussian Function of RBF

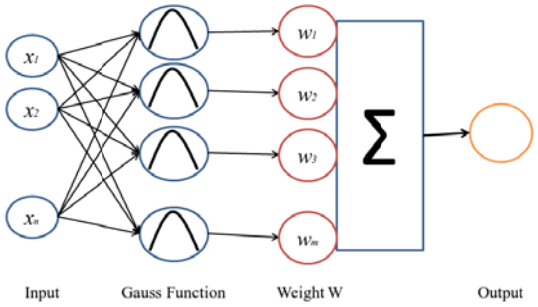

Fig. 4 The Structure of RBF Network

IV. Chaotic Cipher System

Expressions of the conventional method that had been proposed in our study are shown below:

$$x_1(n)=s(n)-G(x_1(n-1))+g_1\cdot x_3(n-1)+\theta_1, \tag{6}$$

$$x_2(n)=\theta_2+\sum_{i=1}^{3}h_i\cdot x_i(n-1)+h_{123}\cdot\prod_{i=1}^{3}x_i(n-1)$$
$$+\sum_{i=1}^{3}\sum_{j=1}^{3}h_{ij}\cdot x_i(n-1)\cdot x_j(n-1), \tag{7}$$

$$x_3(n)=x_2(n-1). \tag{8}$$

The conventional system is constructed by the chaotic neuron type nonlinearity ((6)) and the 2nd order Volterra Filter ((7)).

$$r(n)=x_1(n)+G(x_1(n-1))-g_1\cdot x_3(n-1)-\theta_1, \tag{9}$$

$$x_2(n)=\theta_2+\sum_{i=1}^{3}h_i\cdot x_i(n-1)+h_{123}\cdot\prod_{i=1}^{3}x_i(n-1)$$
$$+\sum_{i=1}^{3}\sum_{j=1}^{3}h_{ij}\cdot x_i(n-1)\cdot x_j(n-1), \tag{10}$$

$$x_3(n)=x_2(n-1). \tag{11}$$

The function $G(x)$ is a discontinuous function: the property of the discontinuous function becomes a parameter key on the cipher. The function $G(x)$ is set to below:

$$G(x)=\begin{cases}\dfrac{(Min-Max)\cdot x+(Max-a_1)\cdot Min}{Min-a_1} & : Min\le x\le a_1\\ \dfrac{(Max-Min)\cdot x+(a_1\cdot Min-a_2\cdot Max)}{a_1-a_2} & : a_1\le x\le a_2\\ \dfrac{(Min-Max)\cdot x+(a_2\cdot Max-a_3\cdot Min)}{a_2-a_3} & : a_2\le x\le a_3\\ \dfrac{(Max-Min)\cdot x+(a_3\cdot Min-Max^2)}{a_3-Max} & : a_3\le x\le Max\end{cases}. \quad (12)$$

If all parameters θ_1, θ_2, g_1, h_i, h_{ij}, h_{123} and the initial value of internal state variables $x_1(0), x_2(0), x_3(0)$ on the transmitter and the receiver sides accord perfectly, the volterra filters of both transmitter and receiver synchronizes, as the results, the information signal $s(n)$ is completely demodulated as $r(n)$. Besides, (6) ~ (12) are originally designed so that it is carried out by the fixed-point arithmetic because the system does not have boundness. Namely, the boundness that is required as a chaotic map is given by the fixed-point arithmetic.

Expressions of the transmitter side in the proposed system that are proposed in this study are shown below:

$$\begin{aligned}&x_1(n)=s(n)+\theta_1\\&+RBFN(x_1(n-1),x_2(n-1),x_3(n-1))\\&+(g_{22}\cdot x_2(n-1)^2+g_{33}\cdot x_3(n-1))\\&+g_{123}\cdot x_1(n-1)\cdot x_2(n-1)\cdot x_3(n-1),\end{aligned} \quad (13)$$

$$\begin{aligned}&x_2(n)=\theta_2+(h_1x_1(n-1)+h_3x_3(n-1))\\&+(h_{12}\cdot x_1(n-1)\cdot x_2(n-1)\\&+h_{13}\cdot x_1(n-1)\cdot x_3(n-1)\\&+h_{23}\cdot x_2(n-1)\cdot x_3(n-1)\\&+h_{31}\cdot x_3(n-1)\cdot x_1(n-1)\\&+h_{32}\cdot x_3(n-1)\cdot x_2(n-1))\\&+h_{123}\cdot x_1(n-1)\cdot x_2(n-1)\cdot x_3(n-1),\end{aligned} \quad (14)$$

$$\begin{aligned}&x_3(n)=x_2(n-1)+(g_1x_1(n-1)+g_3x_3(n-1))\\&+(g_{12}\cdot x_1(n-1)\cdot x_2(n-1)\\&+g_{21}\cdot x_2(n-1)\cdot x_1(n-1)\\&+g_{31}\cdot x_3(n-1)\cdot x_1(n-1)\\&+g_{32}\cdot x_3(n-1)\cdot x_2(n-1).\end{aligned} \quad (15)$$

Expressions of the receiver side in the proposed system that are proposed in this study are shown below:

$$\begin{aligned}&x_1(n)=s(n)-\theta_1\\&-RBFN(x_1(n-1),x_2(n-1),x_3(n-1))\\&-(g_{22}\cdot x_2(n-1)^2+g_{33}\cdot x_3(n-1))\\&-g_{123}\cdot x_1(n-1)\cdot x_2(n-1)\cdot x_3(n-1),\end{aligned} \quad (16)$$

$$\begin{aligned}&x_2(n)=\theta_2+(h_1x_1(n-1)+h_3x_3(n-1))\\&+(h_{12}\cdot x_1(n-1)\cdot x_2(n-1)\\&+h_{13}\cdot x_1(n-1)\cdot x_3(n-1)\\&+h_{23}\cdot x_2(n-1)\cdot x_3(n-1)\\&+h_{31}\cdot x_3(n-1)\cdot x_1(n-1)\\&+h_{32}\cdot x_3(n-1)\cdot x_2(n-1))\\&+h_{123}\cdot x_1(n-1)\cdot x_2(n-1)\cdot x_3(n-1),\end{aligned} \quad (17)$$

$$\begin{aligned}&x_3(n)=x_2(n-1)+(g_1x_1(n-1)+g_3x_3(n-1))\\&+(g_{12}\cdot x_1(n-1)\cdot x_2(n-1)\\&+g_{21}\cdot x_2(n-1)\cdot x_1(n-1)\\&+g_{31}\cdot x_3(n-1)\cdot x_1(n-1)\\&+g_{32}\cdot x_3(n-1)\cdot x_2(n-1)).\end{aligned} \quad (18)$$

The proposed system is constructed by the RBFN Mapping ((13)) and the two Volterra Filters ((14), (15)). But, the two Volterra Filters are has been modified as follows: some parameters ($\theta_1, h_{11}, h_{22}, h_{33}, h_{123}$) in the third formula have been transposed to the first formula, some parameter that don't have a significant impact at the sophisticate of encryption have been erased. The reason for this modification is as follows: Improvement of properties that are sensitive to parameter mismatch, the optimization of encryption processing. In this study, we call this filter"Improved Volterra Filters".

In addition, as with the conventional method, if all parameters θ_1, θ_2, g_i, g_{ij}, g_{123}, h_i, h_{ij}, h_{123} and the initial value of internal state variables $x_1(0)$, $x_2(0)$, $x_3(0)$ on the transmitter and the receiver sides accord perfectly, as the results, the information signal $s(n)$ is completely demodulated as $r(n)$.

V. Evaluation of the Each Systems

In this chapter, we evaluate property of the conventional and proposed systems. The each system is evaluated by three types items: in the chaotic property, randomness, the sensitivity coefficient. In each evaluation, the initial value of internal state variables are 0.0, and the value of the unchanging parameters is as follows:

$$g_i=g_{ij}=g_{123}=h_i=h_{ij}=h_{123}=1.0,$$
$$\alpha=1.0,\theta_1=\theta_2=0.1,$$
$$Min=0X0000,Max=0XFFFF,$$
$$a_1=-16.0,a_2=0.0,a_3=16.0.$$

The parameters of RBF Network are as follows:

$$\sigma=48.0,M=10.$$

A. Chaotic Property

In this subsection, we try to evaluate the chaotic property of the proposed cipher based on the Lyapunov exponents [7]. The Lyapnov exponent is one of the quantitative indexes of chaos.

If the maximum Lyapnov exponent is a positive number, the system can be categorized into chaotic.

When the Lyapunov exponent is calculated, the Jacobian of the chaotic dynamics is required. The Jacobian of conventional system in this study is shown below:

$$\overrightarrow{J(n)} = \begin{bmatrix} -\frac{\partial}{\partial x_1} G(x_1(n)) & 0 & g_1 \\ J_1 & J_2 & J_3 \\ 0 & 1 & 0 \end{bmatrix}. \quad (19)$$

$$J_1 = h_1 + 2 \cdot h_{11} \cdot x_1(n) + (h_{12} + h_{21}) \cdot x_2(n) + (h_{13} + h_{31}) \cdot x_3(n) + h_{123} \cdot x_2(n) \cdot x_3(n)$$

$$J_2 = h_2 + 2 \cdot h_{22} \cdot x_2(n) + (h_{12} + h_{21}) \cdot x_1(n) + (h_{23} + h_{32}) \cdot x_3(n) + h_{123} \cdot x_1(n) \cdot x_3(n)$$

$$J_3 = h_3 + 2 \cdot h_{33} \cdot x_3(n) + (h_{13} + h_{31}) \cdot x_1(n) + (h_{23} + h_{32}) \cdot x_2(n) + h_{123} \cdot x_1(n) \cdot x_2(n)$$

The Jacobian of proposed system in this study are shown below:

$$\overrightarrow{J(n)} = \begin{bmatrix} J_{11} & J_{12} & J_{13} \\ J_{21} & J_{22} & J_{23} \\ J_{31} & J_{32} & J_{33} \end{bmatrix}. \quad (20)$$

$$J_{11} = \frac{\partial}{\partial x_1} RBFN(x_1(n), x_2(n), x_3(n)) + g_{123} \cdot x_2(n) \cdot x_3(n)$$

$$J_{12} = \frac{\partial}{\partial x_2} RBFN(x_1(n), x_2(n), x_3(n)) + g_{123} \cdot x_1(n) \cdot x_3(n)$$

$$J_{13} = \frac{\partial}{\partial x_3} RBFN(x_1(n), x_2(n), x_3(n)) + g_{123} \cdot x_1(n) \cdot x_2(n)$$

$$J_{21} = h_1 + h_{123} \cdot x_2(n) \cdot x_3(n) + (h_{12} \cdot x_2(n) + (h_{13} + h_{31}) \cdot x_3(n))$$

$$J_{22} = (h_{12} \cdot x_1(n) + (h_{23} + h_{32}) \cdot x_3(n)) + h_{123} \cdot x_1(n) \cdot x_3(n)$$

$$J_{23} = h_3 + h_{123} \cdot x_1(n) \cdot x_2(n) + ((h_{13} + h_{31}) \cdot x_1(n) + (h_{23} + h_{32}) \cdot x_2(n))$$

$$J_{31} = g_1 + ((g_{12} + g_{21}) \cdot x_2(n) + g_{31} \cdot x_3(n))$$

$$J_{32} = 1 + ((g_{12} + g_{21}) \cdot x_1(n) + g_{32} \cdot x_3(n))$$

$$J_{33} = g_3 + (g_{31} \cdot x_1(n) + g_{32} \cdot x_2(n))$$

In the proposed system, each term J_{ij} includes many coefficients and the generated internal state variables $x_1(n)$, $x_2(n)$ and $x_3(n)$, respectively, compared to the conventional method. Therefore, the Jacobian has the time variant more advanced characteristic, and estimate the private keys by the Lyapunov spectrum analysis based on the time series signal becomes extremely difficult.

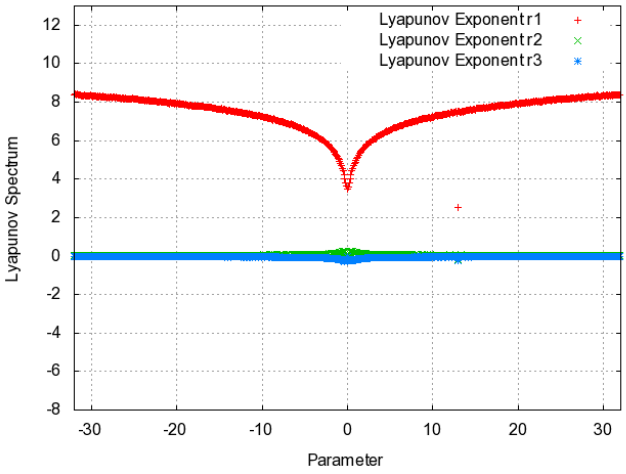

Fig. 5 Estimation of the Lyapunov Spectrum (The Conventional System) based on the Time Series Signal. Horizontal Axis Shows the Parameter $h1/1024$(Q_{10}Format) of the Cipher

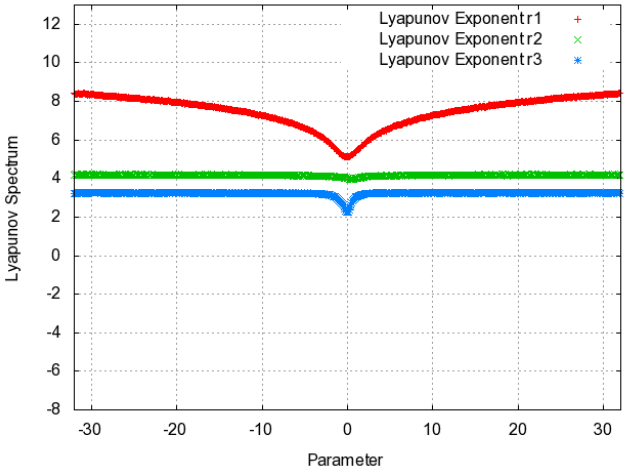

Fig. 6 Estimation of the Lyapunov Spectrum (The Proposed System) based on the Time Series Signal. Horizontal Axis Shows the Parameter $h1/1024$(Q_{10}Format) of the Cipher

The number of sample that is used to estimate the Lyapunov exponent is 10,000. When parameter h_{123} is varied in each method, the results from the evaluation of the Lyapunov exponent shown in Fig. 5, 6. In this evaluation, the parameter is changed in increments of 0. 1 in the range from Q_{10min} to Q_{10max}. As the Fig. 6 shows, the value of the second and third Lyapunov exponent is larger than the result shown in Fig. 5. Furthermore, the decrease of the value has been reduced in the vicinity of the zero point in the first Lyapunov exponent, compared to the conventional method.

B. Randomness

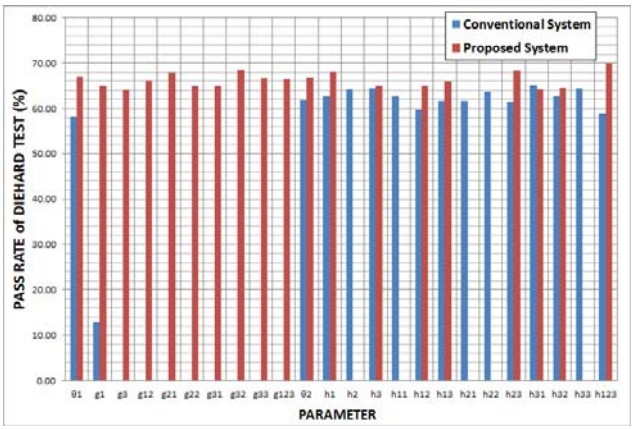

Fig. 7 The result of *Diehard Test* in each method

In this subsection, we evaluate the randomness of the cryptographic system using random test called "*Diehard Test*". *Diehard Test* is randomness test developed by Dr. George Marsaglia. *Diehard Test* consists of 18 different statistical tests, and certifies that signal that has a high likelihood of randomness when it passes all the tests. We compare the randomness of the proposed method with the conventional method by *Diehard Test* and check the validity of the proposed method.

The results of *Diehard Test* in each method are shown in Fig. 7. In this evaluation, the parameter is changed in increments of 0. 1 in the range from Q_{10min} to Q_{10max}.

The results show that the proposed method is better than the conventional method in the randomness.

C. Sensitivity Coefficient

Because the chaotic cipher system can take a variegated structure, it is first necessary to specify the structure for the demodulation. In this subsection, assuming that the structure of the chaotic modulator was clarified, the robustness of the system to mismatch of the parameters is validated. Namely, this evaluation is assumed the Brute Force Attack that tries to set the all combination of parameters.

By the Sensitive Dependence on Initial Conditions of chaos, if the parameters are different, the orbit of the chaotic cipher system can be expected to shift quickly to another different orbit. Therefore, when the values of all other parameters are correct, we examine the value that is demodulated by changing the value of a parameter. If the input signal is demodulated only at the parameter set the correct value, that parameter can be used as an encryption key.

Table I shows the bit length that can be used as an encryption key in the each method. In this evaluation, the parameter is changed in increments of Q_{10unit} in the range from Q_{10min} to Q_{10max}.

TABLE I
THE BIT LENGTH THAT CAN BE USED AS AN ENCRYPTION KEY

	Conventional	Proposed
The length of the encryption key (bits)	224	288

One of the encryption key is 16bits.

VI. CONCLUSION

In this study, we aim to achieve chaos cryptography and secure communication, and tried to propose the robust system than ever before. Therefore, for protecting information signals from attacks of third parties, we have incorporated the improved Volterra Filters into the proposed system and complicated the change of the internal state. In addition, we focused on the chaotic property in fluctuation of the vocal cords. Then, we have created the mapping that is difficult to predict changes in value by the RBF Network from real voice data, and incorporated into the system. And, we have evaluated by comparing with conventional chaos cipher system about robustness of the proposed system.

As a result, it has verified that the proposed method is superior to the conventional method in each of evaluation of three types: "chaotic property", "randomness", "sensitivity coefficient". However, the Improved Volterra Filters and the RBFN Mapping in the proposed system change dramatically the structure by giving the parameters. Therefore, it is necessary that we repeated verification and continue to seek a more effective combination of parameters.

REFERENCES

[1] K.Iwata, T.Nakamura, and H.Kamata, "Chaotic modulator with volterra filter for cipher," *IEICE, Proceeding of NOLTA*, pp. 216–219, Sep 2007.

[2] H.Watanabe, D.Yoshida, A.Nakayama, T.Sato, Y.Kawanishi, and H. Kamata, "Parameter setting for chaotic cipher using simultaneous volterra filters," *on the 24th workshop on circuits and systems in Awaji*, pp. 22–a1–2–2, Aug 2011.

[3] Y. Hideaki, K. Hiroyuki, E. Tetsuro, and I. Yoshihisa, "Chaos signal generation system using both linear and nonlinear digital filters with overflow via fixed-point computation and its application." *IEIC Technical Report*, vol. 99, no. 365, pp. 53–60, Oct 1999.

[4] 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, pp. 1238–1246, Jun 2000.

[5] H. Watanabe, T. Sato, A. Nakayama, D. Yoshida, Y. Kawanishi, and H. Kamata, "Study on the characteristic analysis and evaluation of digital chaotic system operated by the fixed point arithmetic," *Proceedings of 2012 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing*, vol. 5PM1-1/ 2, pp. 377–380, 2012.

[6] Y. Naniwa, T. Kondo, K. Kamiyama, and H. Kamata, "Study on the artificial synthesis of human voice using radial basis function networks," *JSST2011, Proc. of International Conference on Modeling and Simulation Technology.*, vol. 0077, pp. 228–235, Oct 2011.

[7] 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.