Voice and Text Encryption using Chaotic Circuits

Baby H. T., Sujatha B.R.

Abstract: An ever-increasing usage of internet from simple data transmission to highly sensitive data storage has given rise to the need to establish techniques for securing such transactions. Cryptography has been widely used in recent decades to provide protection for the Internet data, although mainly used in the diplomatic and military societies. These regularities have made randomness in data processing a key element for security. The generation of random numbers is a subject which continues to interest the researchers since several decades. Chaos theory is one such approach to demonstrate the randomness of the data in Cryptosystems. Chaotic circuits have been used in this paper to produce different multiple keys to be used for both text and voice encryption. The significant difference in the initial constraints of chaotic circuits is seen to produce entirely different keys and cipher text.

Index Terms- Cipher text, Chaos Function, chaotic circuit, Cryptography, Decryption, Encryption, Plain text,

I. INTRODUCTION

Cryptography and steganography are the scientific branch for preserving data secrecy during communication. Present cryptographic systems are based on several number of scientific and mathematical concepts. In a cryptographic system requiring absolute protection, KEY is important for which a Random Number Generator (RNG) is required. Chaos is one of the promising paradigms of hope in cryptography. Chaos based electronic circuits provides an efficient method to generate the KEYS for effective and secure data encryption [1] [2]. The Chaos Circuit is a basic electronic circuit which illustrates chaos and many well-known bifurcation phenomena. In this work an attempt was made to use the concept of ‘Chaos’ to generate KEYS for encrypting voice and text data.

II. CHAOTIC CIRCUITS

The Chaos Circuit is used to develop a laboratory device that can be practically modelled to show chaos by the Lorenz Equations [3-6]. The Chaos (Chua) circuit scheme is shown in figure 1. It has 5 circuit elements- four are linear passive electrical components and an active Chua’s diode. Interconnecting of these passive elements often leads to trivial dynamics, with all elementary voltages and currents tending to be zero. The characteristic of the V-I circuit has a nonlinear negative slope, and is called as an active local resistor [6-10]. Chaos diode is a type of active, nonlinear two-terminal resistor that can be represented by piece-wise linear equations. This experiences chaotic oscillations and is implemented as a nonlinear negative voltage-controlled resistor.

Chaos corresponding diode circuit is shown in figure 2 and a physical circuit for study of the Chaos circuit is shown in figure 3. Chaos circuit can also be modelled as shown in equation (1) by a set of nonlinear differential equations. The resistance graph (Piecewise linear graph) of Chaos diode is represented in figure 4.

\[
\begin{align*}
\dot{x} &= \beta(y-x-g(x)) \\
\dot{y} &= x-y+z \\
\dot{z} &= -\gamma y
\end{align*}
\]

(1)

The three parameters namely \(x\), \(y\), \(z\) represent the capacitor voltages across \(C_1\), \(C_2\) and an inductor current respectively, as symbolized in the schematic shown in figure 3. \(\beta\) and \(\gamma\) values vary based on the circuit components. A piecewise-linear function \(g(x)\) describes the variation in resistance as a function of current across the Chaos Diode:

\[
g(x) = \begin{cases} 
m_0x + (m_n-m_0), & \text{if } x \leq -1 \\
m_1x, & \text{if } -1 < x < 1 \\
m_0x + (m_0-m_n), & \text{if } x \geq 1 
\end{cases}
\]

(2)

Here \(m_0\) and \(m_1\) are the slopes of the middle and two outer segments respectively.

However, these can be represented explicitly as function of component values, voltages and current as indicated in equations (3) and (4):
Voice and Text Encryption using Chaotic Circuits

\[
\begin{align*}
\dot{v}_1 &= \frac{1}{RC_1}(v_2 - v_1) - g(v_1) R \\
\dot{v}_2 &= \frac{1}{RC_2}(v_1 - v_2) + i_i R \\
\dot{i}_i &= \frac{1}{L}(-v_2)
\end{align*}
\]

\[g(v_1) = \begin{cases} 
  m_0 v_1 + (m_0 - m_1) E_1, & \text{if } v_1 \leq -E_1 \\
  m_1 v_1, & \text{if } -E_1 < v_1 < E_1 \\
  m_0 v_1 + (m_1 - m_0) E_1, & \text{if } v_1 \geq E_1
\end{cases}
\]

\[\text{(3)}\]

\[\text{(4)}\]

\[\text{Figure 3: Complete Chaos Circuit}\]

\[\text{Figure 4: Chaos diode resistance graph}\]

III. METHODOLOGY

A. Key Generation Scheme

1. By using the logistic map equations (5) generate the random keys at both the ends (sender and receiver).

\[
\begin{align*}
\dot{x} &= \frac{1}{c_1} \cdot (G \cdot (y - x) - g) \\
\dot{y} &= \frac{1}{c_2} \cdot (G \cdot (x - y) + x) \\
\dot{z} &= -\frac{1}{c} \cdot y \\
G &= \frac{1}{R}
\end{align*}
\]

\[\text{(5)}\]

where R, L, C and G are the electrical parameters.

2. Randomness of KEYs is increased by taking the 1’s complement of generated values. Also, the KEYs generated are statistically independent of each other.

B. Encryption and Decryption Scheme

(i) For Text data
1. The ASCII value of each character is converted into its equivalent binary form.
2. Simple XOR operation will performed to convert plain text (Binary form) to cipher text using the generated KEYs.

(ii) For Voice signal
Voice Encryption is done by mixing the original signal with the carrier signal generated using parameter values generated by the chaotic circuits (Algorithm depicted in flow chart shown in figure 5). The reverse process of encryption is used to perform the decryption.

IV. SIMULATION RESULTS

Matlab is used for operations involved in generation of KEYs and algorithms of both encryption/decryption methods. The code is checked for various initial chaotic circuit conditions which provides different ciphering data for different chaotic keys. It is also verified considering slight changes in the initial conditions for the same plain text. The tests of the simulation were done for both text data and voice signal.

Case1: For Text data

Table 1 represents the generated random numbers for the different initial conditions at the transmitter side. A single bit change in the initial parameters generates fully different keys and different cipher texts for the same plain text. Figure 6, 7 and 8 shows the plain text and cipher text for the different initial conditions. At the receiver side even a significant change in the initial values generates unreadable plaintext from the received Cipher text, as generated random numbers become fully different compared with the random numbers used in transmitter side. Figure 9 shows the values of the generated N Chaos KEYs from the chaotic circuit.
Figure 10 shows plot of the probability of repetition of the generated N Chaos KEYS from the chaotic circuit. It is obvious from the figure that the likelihood of any KEYS being replicated is very low. For example, out of 256 KEYS generated only 3 KEYS are repeated 2 times with the probability of 0.0135. All other numbers occur with least probability of 0.0067, which indicates that the repetition of the number is very less.

Case 2: For voice data

The voice encryption using CHAOS techniques are done by taking the samples of the original voice message. But the samples are mixture of floating point and negative numbers. These are made positive by adding the required constant. The Positive floating-point numbers are rounded off to nearest value to get the decimal samples. The values generated from the chaotic circuits are used to generate the carrier signal and mixed with original voice signal to obtain the encrypted signal. The resulting values are used as samples of encrypted voice message and create a voice message to communicate. At the receiver end, the samples of the encrypted voice message are divided by the same carrier signal to obtain the original voice signal. The resulting samples are used to recover the original voice signal. Figure 11 shows the signals corresponding to the original voice signal, random numbers generated, encrypted voice and decrypted voice signals. The strong cross correlation existed between the original signal and encrypted signal is shown in figure 12. Figure 13 demonstrates the strong standardized auto correlation occurred between the original and decrypted signals which indicates that decrypted song and original song are same.
In this paper, chaotic circuits are used to generate the highly random KEYS which can be applied to any conventional encryption algorithms to provide security for data. This technique is able to protect the data with a high degree of security due to the randomly generated KEYS which are highly responsive to the initial values. The simulation experiment results showed the good performance of a KEY generation technique based on CHAOS.

REFERENCES

1. Ankur A. Khare, “Secure and Fast Chaos based Encryption System”, LI. Computer Network and Information Security, 2014.
2. Sattar B. Sadkhan, Ali Al-Sherbaz „Rana S. Mohammed, “Chaos based cryptography for voice encryption in wireless communication”, IEEE international conference on Electrical, Communication, Computer, Power, and Control Engineering (ICCECCPCE), Page(s): 191 – 197, 17-18 Dec. 2013.
3. A. A. Elkoony,N. S. Zakaria , M. L. Sobhy,“Communication security using chaotic generator”, 45th Midwest Symposium on Circuits and Systems, MWSCAS, Page(s): 236-238 vol.1, 4-7 Aug. 2002.
4. Jing Liu, Fei Gao, Haisan Ma, “A Speech Chaotic Encryption Algorithm Based on Network”, IEEE international conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008. IHHMS’08, Page(s):283 - 286, 15-17 Aug. 2008.

5. Kwan-Pok Man, Kwok-Wo Wong, Kim-Fung Man, “Security Enhancement on VoIP using Chaotic Cryptography”, IEEE 32nd Annual Conference on IEEE Industrial Electronics .IECON 2006, Page(s):3703 - 3708, 6-10 Nov. 2006.
6. Alzahraa Mostafa, Naglaa. F. Soliman, “Mohanoud Abdallah, Fathi E. Abd El-samie, “Speech encryption using two dimensional chaotic maps”, IEEE 11th International Computer Engineering Conference (ICENCO), Page(s):235 – 240, 29-30 Dec. 2015.
7. S. E. Hamamci, “A new chaotic system with chaos entanglement”, IEEE conference on Signal Processing and Communications Applications (SIU), Page(s):2597 – 2600, 2015.
8. Sattar B. Sadkhan, Rana Saad Mohammed., “Proposed random unified chaotic map as PRBG for voice encryption in wireless communication”, International Conference on Communication, Management and Information Technology (ICCMIT) 2015, Page(s):314 – 323, 2015.
9. Mina Mishra, Vijay H. Mankar, “Chaotic Encryption Scheme Using 1-D Chaotic Map”, Int. J. Communications, Network and System Sciences, volume 4, Page(s):452-455, 2011.
10. Hongmei Wang, Limin Qu, “A Scheme of Triangular-hiding Based on Two-dimensional Chaotic Maps”, IEEE Fourth International Conference on Intelligent Control and Information Processing (ICICIP) June 9 – 11, 2013, Beijing, China.
11. Muhammad Rezal, “Chaos Based Cryptography: An Alternative to Algebraic Cryptography”, Research Bulletin of Institute for Mathematical Research.
12. Chen Dongrung, Zhu Zhihong, Yang Guangming, “An improved Image Encryption Algorithm Based on Chaos”, The 9th International Conference for Young Computer Scientists, IEEE, 2008.
13. Cristian-Iulian and Alexandru S „Chaos-based cryptography. A possible solution for information security”, Bulletin of the Transilvania University of Brașov • Vol 2(51) Series III. Mathematics, Informatics, Physics, pp: 113-126, 2009.
14. Nur Azman Abu and Shahrin Sahib, “Random Ambience Key Generation Live on Demand”, 2nd International Conference on Signal Processing Systems (ICSPS), IEEE, 2010.
15. Zhaoqin Su. Jiang,Shuqun Lian, “Selective Encryption for G.729 Speech using Chaotic Maps”,International conference on Multimedia Information Networking and Security,Volume 1, pp:488-492,Nov. 2009

AUTHORS PROFILE

Baby H.T. graduated in Electronics and Communication Engineering from the University of Mysore in the year 2001. She obtained her Master’s degree in Digital Communication and Networking in the year 2005 from Visvesvaraya technological University, Belgaum. She is pursuing Ph.D. degree in Visvesvaraya technological University. Presently she is working as Associate Professor in the Department of E&CE, Government Engineering College, Hassan. She has 15 years of teaching experience. She has presented two papers in National and International conferences and published one paper in international journal. Her areas of interest include Network security, Information Theory and Coding. She is a life member of ISTE.

Dr. B.R. Sujatha obtained her degrees in Electronics and Communication Engineering-BE (Univ.of Mysore,1983), ME(IISC,1990). PhD (VTU,2013). She has 35 years of teaching experience at various levels. Presently she is working as Professor and HOD in the Department of E&CE, Malnad College of Engineering, Hassan. She has published 44 papers in National and International conferences and journals. She has conducted and organized various short term courses, conferences and symposium including International Conference on ‘Intelligent and Autonomous Systems’ ICIAS 2015.She has been awarded the ‘Outstanding project award’ at 36th series KSCST sponsored project exhibition at Belgaum for the project ‘Antenna design for Spectroscopy applications’. She is presently guiding seven PhD scholars. Her areas of interest include Wireless networks, Information Theory and Coding and Network Security. She is a Life Member of ISTE, Fellow member of IETE and Senior member of IEEE.