Chaotic Masking of Voice Bitstream Using Mixed Sequences for Authorized Listening

Musheer Ahmad[1], Bashir Alam[1], and Omar Farooq[2]

[1] Department of Computer Engineering, Faculty of Engineering and Technology, Jamia Millia Islamia, New Delhi-110025, India
[2] Department of Electronics Engineering, ZH College of Engineering and Technology, AMU, Aligarh-202002, India

Abstract. The voice-based communication becomes extensively vital in the application areas of military, voice over IP, voice-conferencing, phone banking, news telecasting etc. It greatly demands to preserve sensitive voice signals from the unauthorized listening and illegal usage over shared/open networks. To address the need, we propose a chaos-based symmetric encryption technique to protect voice bitstreams over insecure transmission channel. The technique utilizes the features of high dimensional chaos like Lorenz and Chen systems to generate highly unpredictable and random-like sequences. The encryption keys are dynamically extracted from the pretreated chaotic mixed sequences, which are then used to mask the voice bitstream for integrity protection of voice data. The experimental analyses like auto-correlation, signal distribution, parameter-residual deviation, key space and key-sensitivity demonstrate the effectiveness of the proposed technique for secure voice communication.

Keywords: Voice communication, security, chaotic systems, voice encryption.

1 Introduction

With the advancement of modern wireless telecommunication and multimedia technologies, a huge amount of sensitive voice data travels over the open and shared networks. Voice-based communication becomes prominent in the application areas of military, voice over IP, e-learning, voice-conferencing, phone banking, phone stock market services, news telecasting etc. These applications are critical with respect to integrity protection of voice data and privacy protection of authorized users. The probable security threats in a voice-based communication system as highlighted by voice over IP security alliance [1] are: social threats, interception and modification threats, denial of service threats, service abuse threats, physical access threats and interruption of service threats. Hence, the need of high level security system is pre-requisite of any secure voice communication system to forestall these attacks. The cryptographic techniques are to be developed and deployed which can address and fulfill the increasing security demands of secure voice-based communication. The conventional cryptographic techniques are efficient for the text data. But they computationally fail in providing ample security due to the bulk data capacity and

N. Meghanathan et al. (Eds.): CCSIT 2012, Part II, LNICST 85, pp. 604–611, 2012.

high redundancy of voice data. Therefore, the design of efficient voice security methods demands new challenges which can provide high security to the voice data. To achieve this, a number of voice encryption techniques have been suggested [2-10]. Among them, the chaos-based techniques are considered efficient for dealing with bulky, redundant voice data. They provide fast and highly secure encryption methods. This is because of the reason that the chaotic systems are characterized with high sensitivity to its initial conditions, ergodicity, random behavior, and long periodicity. The cryptographic properties such as diffusion, confusion and disorder can be achieved by applying iteration operations to these systems.

In this paper, a symmetric voice encryption technique is proposed, to meet the demands of high security, privacy and reliability of secure voice communication system. The features of high dimensional chaotic systems are exploited in the design. The sequences generated by chaotic systems are pre-processed, quantized and mixed to produce cryptographically and statistically better encryption keys, which masked the voice bitstream. The results support the effectiveness and suitability of the proposed technique for voice data encryption.

2 Proposed Voice Encryption

The one dimensional chaotic systems have some inherent weaknesses such as: (1) they provide low key space, (2) their iteration operations generate single sequence and (3) they are weak against adaptive parameter synchronous attack [11]. Therefore, the 3D Lorenz and Chen chaotic systems are employed in the design. Each of these systems generates three distinct stochastic chaotic sequences on iteration operations, which makes encryption faster. Moreover, the Lorenz and Chen systems are more complex and generate more unpredictable sequences than 1D systems. The differential equations given below describe the Lorenz and Chen systems.

Lorenz Chaotic System

$$\begin{aligned} \dot{x}_1 &= \sigma(x_2 - x_1) \\ \dot{x}_2 &= r x_1 - x_1 x_3 - x_2 \\ \dot{x}_3 &= x_1 x_2 - \rho x_3 \end{aligned} \tag{1}$$

Chen Chaotic System

$$\begin{aligned} \dot{y}_1 &= a(y_2 - y_1) \\ \dot{y}_2 &= (c-a) y_1 - y_1 y_3 + c y_2 \\ \dot{y}_3 &= y_1 y_2 - b y_3 \end{aligned} \tag{2}$$

Where $x_1(0)$, $x_2(0)$, $x_3(0)$ are initial conditions, while σ, r, ρ are positive constants of Lorenz system. Let σ=10 and ρ=8/3, the research shows that the Lorenz system exhibits chaotic behaviour when $r > 24.74$. Where as, $y_1(0)$, $y_2(0)$, $y_3(0)$ are initial conditions and a, b, c are parameters of Chen system. The Chen system is chaotic for a=35, b=3, $20 \leq c \leq 28.4$. The equations of Lorenz and Chen systems are quite similar, but topologically they are very different due to parameters r of Lorenz and c of Chen system. These 3D differential equations are solved using RungeKutta-4 method with step size of 0.001. The ideal cryptographic sequence should have good statistical properties. The pre-processing done in Eq. 3 and 4 enhances the statistical properties of the chaotic sequences generated by the Lorenz and Chen systems [11,12].

$$\hat{x}_k(i) = x_k(i) \times 10^5 - floor(x_k(i) \times 10^5) \tag{3}$$

$$\hat{y}_k(i) = y_k(i) \times 10^6 - floor(y_k(i) \times 10^6) \tag{4}$$

Where k=1, 2, 3 and $i > 0$ is iteration count. Now, the pre-processed chaotic sequences $0 < x_k(i), y_k(i) < 1$ are quantized and converted into binary bitstreams $\omega_k(i)$ and $\varphi_k(i)$. The quantization is governed by the following transformation:

$$\omega_k(i) = \begin{cases} 0 & if \quad \hat{x}_k(i) < 0.5 \\ 1 & if \quad \hat{x}_k(i) \geq 0.5 \end{cases} \tag{5}$$

$$\varphi_k(i) = \begin{cases} 0 & if \quad \hat{y}_k(i) > 0.5 \\ 1 & if \quad \hat{y}_k(i) \leq 0.5 \end{cases} \tag{6}$$

The six bitstreams $\omega_k(i)$ and $\varphi_k(i)$ are combined and mixed using XOR operations according to the rules described in Eq. 7 to generate cryptographically better chaotic mixed bitstreams Φ_1, Φ_2, Φ_3 and Φ_4. On mixing, the bitstreams become highly random and uncorrelated. After mixing operation, the mixed bitstreams are fed to a 4×1 multiplexer which dynamically selects one of randomly generated bits $\Phi_1(i)$, $\Phi_2(i)$, $\Phi_3(i)$, $\Phi_4(i)$ to produce the next member of output keystream. The multiplexer require two select lines S_1S_0, the select lines should not be static for dynamic operation of MUX. The select lines are made dependent to the random bits $\omega_k(i)$ and $\varphi_k(i)$ for its dynamic operation. The select lines for iteration i are evaluated as $S_0=\omega_1(i)\oplus\omega_2(i)\oplus\omega_3(i)$ and $S_1=\varphi_1(i)\oplus\varphi_2(i)\oplus\varphi_3(i)$. The diagram of proposed voice encryption system is shown in Fig. 1.

$$\left.\begin{aligned}
\phi_1(i) &= \omega_1(i) \oplus \varphi_2(i) \oplus \omega_3(i) \\
\phi_2(i) &= \varphi_3(i) \oplus \omega_1(i) \oplus \varphi_1(i) \\
\phi_3(i) &= \omega_2(i) \oplus \varphi_1(i) \oplus \varphi_2(i) \\
\phi_4(i) &= \omega_3(i) \oplus \omega_2(i) \oplus \varphi_3(i)
\end{aligned}\right\} \tag{7}$$

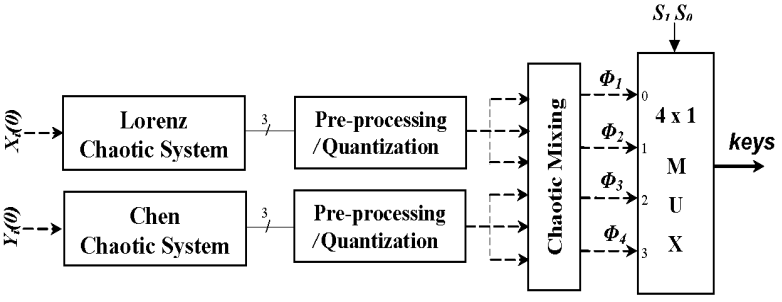

Fig. 1. Block diagram of proposed chaos-based voice encryption system

3 Results and Discussions

In this section, the experimental analyses are presented to demonstrate the effectiveness of the proposed system. The initial values taken for experimentation are as follows: $X(0)=(x_1(0)=13.3604,\ x_2(0)=7.2052,\ x_3(0)=21.5026,\ \sigma=10,\ \rho=8/3,\ r=28)$, $Y(0)=(y_1(0)=-10.058,\ y_2(0)=0.368,\ y_3(0)=37.368,\ a=35\ b=3,\ c=28)$ and $t=4000$. The two chaotic systems are first iterated t times and these $6\times t$ values are discarded to remove the transient effect. The auto-correlation function of the output keytream is shown in Fig. 2. It is clear from the figure that keystream has good delta-function form thereby meeting the requirement of cryptographic random sequence. The function has a maximum value of 0.0056984 for non-zero shift.

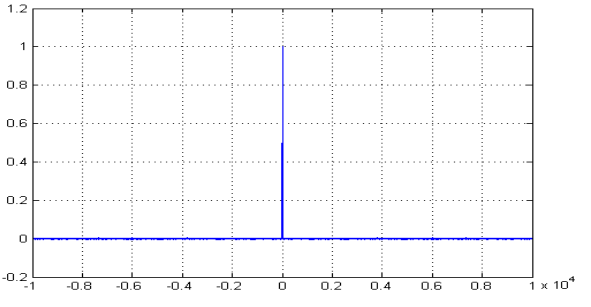

Fig. 2. Auto-correlation function of output keystream

A voice signal having 59114 samples, sampled at rate of 16 KHz is encrypted using the proposed system. The original voice signal is pre-processed and quantized to get the corresponding voice bitstream. The voice bitstream is then XORed with the keystream. The simulation of voice encryption is shown in Fig. 3. As it can be seen that the encrypted voice signal shown in Fig. 3(b) is totally distinct from the original voice signal shown in Fig. 3(a) and it is randomly distributed like a noise signal. The signal distribution in Fig. 3(b) is completely flat/uniform at two extreme ends. This shows the effectiveness and suitability of the proposed scheme for voice encryption.

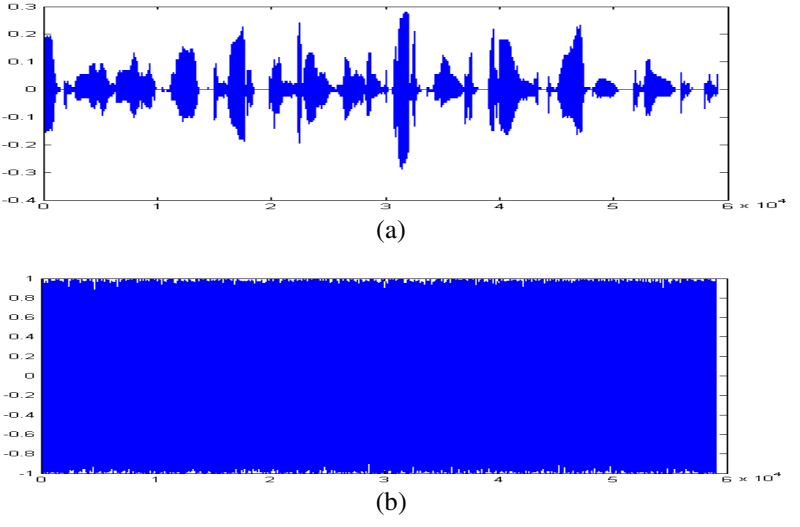

Fig. 3. Voice encryption: (a) Original voice signal (b) Encrypted voice signal

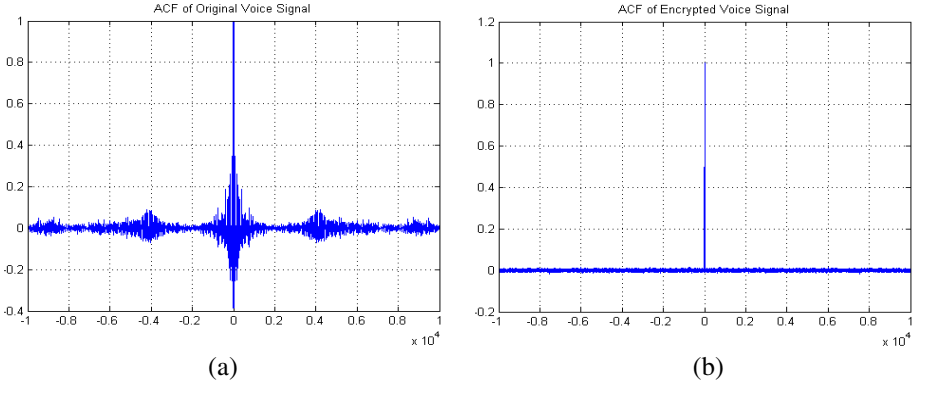

Fig. 4. Auto-correlation function of (a) Original and (b) Encrypted Voice Signals

The auto-correlation function depicts the random distribution of signal. According to the Golomb's randomness postulate, the sequence should have equality/uniformity in signal distribution and auto-correlation is delta-function. The auto-correlation of

the original and encrypted signals are sketched and shown in Fig. 4. It is evident from the plot shown in Fig. 4(b) that the encrypted voice signal has delta-function form. The auto-correlation functions of original and encrypted voice signals have a maximum value of 0.8707092 and 0.0152536 for non-zero shift, respectively. Hence, the encrypted signal is exhibiting random signal like behaviour. In order to determine the extent to which the encrypted signal is deviated from the original signal, Sufi *et al.* [13] uses percent residual deviation (PRD) parameter described in Eq. 8. The parameter provides the measure of dissimilarity between original and encrypted signals. The percent residual deviation (ψ) for original *O(i)* and encrypted *E(i)* voice signals comes out as 1695.196, where as it is found to be 0.0 for original and decrypted signals. This shows that the encrypted signal is deviated up to a large extent from its original signal.

$$\psi = 100 \times \sqrt{\frac{\sum_{i=1}^{n} [O(i) - E(i)]^2}{\sum_{i=1}^{n} O^2(i)}} \tag{8}$$

To demonstrate the key sensitivity, only one parameter of key is changed at a time by a tiny amount of $\Delta = 10^{-10}$, keeping all other parameters of key unchanged and the scheme is applied to recover the voice signal. The results of demonstration are shown in Fig. 5. To quantify the sensitivity, the percentage difference between original and recovered voice signals is calculated and listed in the Table 1. It is clear from the Fig. 5 and Table 1 that voice recovered with tiny changed key has random behaviour and is totally different from the original voice.

Table 1. Percentage difference between original voice and voice recovered with incorrect key

#	Test	% difference	#	Test	% difference
1	$x_1(0) + \Delta$	99.664	8	$y_1(0) + \Delta$	99.657
2	$x_2(0) + \Delta$	99.617	9	$y_2(0) + \Delta$	99.648
3	$x_3(0) + \Delta$	99.629	10	$y_3(0) + \Delta$	99.639
4	$\sigma + \Delta$	99.599	11	$a + \Delta$	99.582
5	$\rho + \Delta$	99.583	12	$b + \Delta$	99.641
6	$r + \Delta$	99.630	13	$c + \Delta$	99.576
7	$t + 1$	99.572	14	$\Delta = 0$	0.0

The key space of the encryption system should be large enough to resist the brute-force attack. In the proposed scheme, all initial conditions and parameters constitute the secret key of encryption system. For a 10^{-10} floating point precision, all key parameters can take 10^{10} possible values. Therefore, the key space comes out as $t \times (10^{10})^{12} \approx 2^{408}$, which is large enough to resist the exhaustive attack. The proposed voice encryption system is highly sensitive to a tiny change in secret keys.

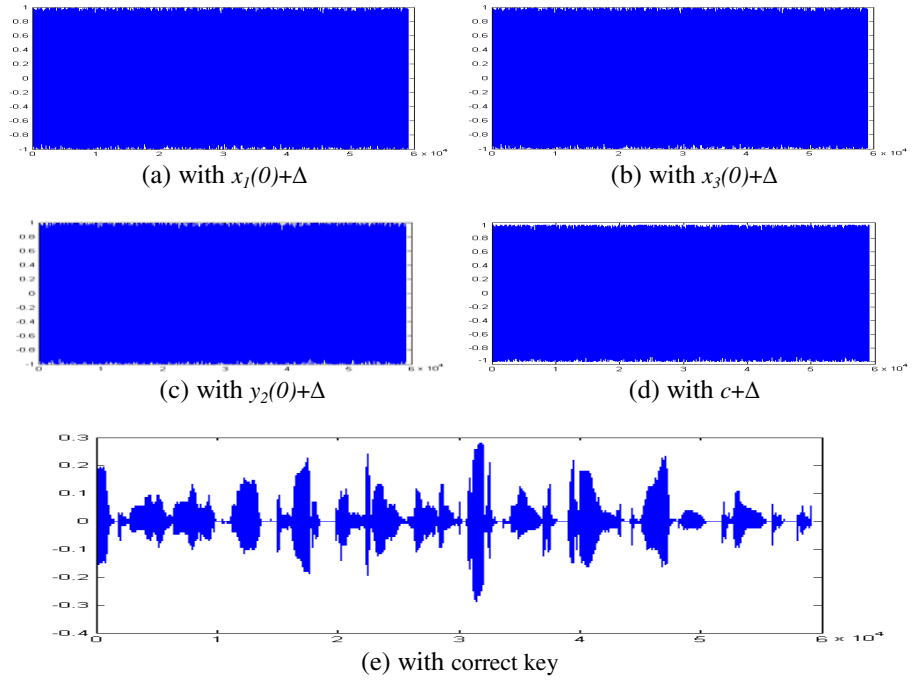

Fig. 5. Recovered voice signals with (a) $x_1(0)+\Delta$, (b) $x_3(0)+\Delta$, (c) $y_2(0)+\Delta$, (d) $c+\Delta$ and (b) $\Delta=0$ i.e. correct key

4 Conclusion

In this paper, a chaos based voice encryption scheme is proposed. The voice bitstream is masked using randomly generated chaotic mixed binary sequences. High dimensional chaotic systems like Lorenz and Chen are employed to generate more complex and unpredictable six chaotic sequences. After quantization and mixing operations, the method generates statistically and cryptographically better encryption keys. Experimental analysis demonstrates the effectiveness of the scheme for voice encryption. The results of statistical analyses like auto-correlation function, signals distribution, percent-residual deviation, key space and key sensitivity indicate high security and suitability of the proposed scheme for practical voice encryption.

References

1. VoIP Security Alliance. VoIP Security and Privacy Threat Taxonomy, version 1.0, `http://www.voipsa.org/Activities/taxonomy.php` (last accessed in July 2011)
2. Orceyre, M.J., Heller, R.M.: An Approach to Secure Voice Communication Based on the Data Encryption Standard. IEEE Communications Society Magazine, 41–50 (1978)

3. Lin, Q.H., Yin, F.L., Mei, T.M., Liang, H.: A Blind Source Separation Based Method for Speech Encryption. IEEE Transaction on Circuits and Systems-I 53(6), 1320–1328 (2006)
4. Su, Z., Jiang, J., Lian, S., Hu, D., Liang, C., Zhang, G.: Selective Encryption for G.729 Speech using Chaotic Maps. In: Multimedia Information Networking and Security, pp. 488–492 (2009)
5. Guo, J.I., Yen, J.C., Pai, H.F.: New Voice over Internet Protocol technique with Hierarchical Data Security Protection. IEE Proceedings Vision, Image & Signal Processing 149(4), 237–243 (2002)
6. Wong, K.W., Man, K.P., Li, S., Liao, X.: A more Secure Chaotic Cryptographic scheme based on Dynamic Look-up table. Circuits, Systems and Signal Processing 24(5), 571–584 (2005)
7. Tang, K.W., Tang, W.K.S.: A Chaos-based Secure Voice Communication System. Industrial Technology, 571–576 (2005)
8. Man, K.P., Wong, K.W., Man, K.F.: Security Enhancement on VoIP using Chaotic Cryptography. Industrial Electronics, 3703–3708 (2006)
9. Qi, H.F., Yang, X.H., Jiang, R., Liang, B., Zhou, S.J.: Novel End-to-End Voice Encryption Method in GSM System. Networking, Sensing and Control, 217–220 (2008)
10. Palmieri, F., Fiore, U.: Providing true end-to-end security in converged voice over IP infrastructures. Computers & Security 28(6), 433–449 (2009)
11. Fu, C., Zhang, Z., Cao, Y.: An Improved Image Encryption Algorithm Based on Chaotic Maps. Natural Computation, 189–193 (2007)
12. Ahmad, M., Farooq, O.: A Multi-level Blocks Scrambling based Chaotic Image Cipher. In: Ranka, S., Banerjee, A., Biswas, K.K., Dua, S., Mishra, P., Moona, R., Poon, S.-H., Wang, C.-L. (eds.) IC3 2010. CCIS, vol. 94, pp. 171–182. Springer, Heidelberg (2010)
13. Sufi, F., Han, F., Khalil, I., Hu, J.: A Chaos-based Encryption Technique to Protect ECG Packets for Time Critical Telecardiology Applications. Security and Communication Networks 4(5), 515–524 (2011)