Speech Encryption Based On Multi Stage Permutation Using Multiple Chaotic System

[1] **P. Sathiyamurthi,** [2] **T. Sasi Prabha,** [3] **K. R. Vani Sri ,** [4] **V. Vanitha,** [5] **S. Vinitha**

[1,2,3,4,5] Department of Information Technology
Dr. Mahalingam College of Engineering and Technology,
Pollachi, Coimbatore - 642003, India

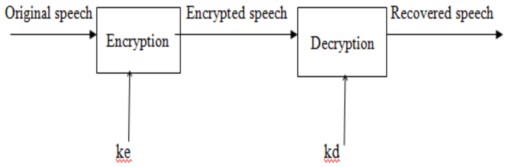
Abstract - In our paper we are using the multiple mapping techniques. Our proposed system provides robustness across open/shared network. The Speech signals are encrypted by means of various effective one dimensional chaotic mapping techniques which provides greater security. Various testing methods are employed to estimate the efficiency of the system. The results from the analysis show that our proposed system of Speech encryption guarantees stronger protection against various security attacks.

***Keywords* - Encryption, Speech Signal, Logistic Map, Chaotic Map.**

1. Introduction

Communication plays a vital role in today's world. Particularly voice based communication has been widely used in many areas, and at the same time security issues has also increased , so it is necessary to take appropriate measures to provide security to these sensitive voice signals from the unauthorized and illegal usage over the networks has been taken into account. To address the need, the chaotic keystreams generator is employed to encrypt the original speech signal. The generator uses the high dimensional chaos like sequences. The experimental analyses like auto-correlation, key space and key-sensitivity analysis shows the effectiveness of the proposed technique for secure voice communication. Other than sender and receiver the third party also have the intention to know the information particularly in the fields such as financial, intelligence, personal and otherdata that are highly confidential. Today, competitors, hackers, or other institutions can divert any call with minimum effort.

Generally, encryption deals with converting data or information from its original form to some other form that hides the information in it. Encryption is a much stronger method of protecting speech communications than any form of unintelligible format to an unauthorised listener. Voice encryptions work by quantizing the conversation at the telephone and applying a cryptographic technique to the resulting bit stream. In order to decrypt the speech, the correct encryption method and key must be used.



Where, ke - Encryption key
kd – Decryption key

Fig. 1: Structure of speech encryption

2. Literature Survey

2.1 Zhaopin Su, Jianguo Jiang, ShiguoLian, Donghui Hu, Changyong Liang, Guofu Zhang, IEEE (2009)

It introduced two selective encryption schemes for G.729 speech. Speech bitstreams are partitioned into two parts based on bit sensitivity, i.e., one is encrypted by a high degree of encryption, and the other is encrypted by a lesser degree.They used cat map and logistic map. The results demonstrate the effectiveness of the selective encryption schemes for power-constrained devices and narrow bandwidth environments.

2.2 EmadMosa, NagyW.Messiha, Osama Zahran, Fathi E. Abd El-Samie, Springer (2011)

Approach is based on permutation of speech segments using chaotic Baker map and substitution using masks in both time and transform domains. Two parameters are extracted from the main key used in the generation of mask. Substitution with Masks is used in this cryptosystem to fill the silent periods within speech conversation and destroy format and pitch information.

Permutation with chaotic Baker map is used in to maximize the benefits of the permutation process in encryption by using large-size blocks to allow more audio segments to be permutated.

2.3 Musheer Ahmad, Bashir Alam and Omar Farooq, Elsevier (2012)

It designed a keystream generator which is employed to work as a symmetric encryption technique to protect voice bitstreams over insecure transmission channel. The generator utilizes the features of high dimensional chaos like Lorenz and Chen systems to generate highly unpredictable and random-like sequences. The encryption keystream is dynamically extracted from the pre-treated chaotic mixed sequences, which are then applied to mask the voice bitstream for integrity protection of voice data.

2.4 Dora M.BallesterosL, JuanM.Moreno A, Science direct (2013)

It proposed a technique which is used in secure mobile telephony and it implements a new scheme of data hiding which takes advantage of the masking property of the Human Auditory System (HAS) to hide a secret (speech) signal into a host (speech) signal. The embedding process is carried out into the wavelet coefficients of the speech signals. The total delay added by the system is low compared to the highest delay allowed for a high quality speech transmission.

3. Proposed System

In our proposed system, the speech signals are sampled, then the random numbers are generated by means of an efficient mapping technique and these numbers are sorted in a logical order. The index values of the sorted random numbers are matched against the index values of original speech signal.

Similarly, the key also undergoes the same process as that of speech signals by using another mapping technique. By doing this we ensure that high level of security is provided.The result of each mapping is given as feedback to next mapping techanique. After this the encrypted signals are decrypted at receiver end by substituting the mapping techniques which are used in the encryption to recover the original speech.

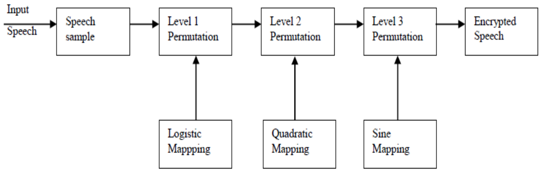


Fig. 2: Block diagram of Encryption

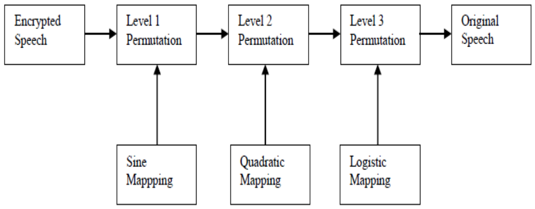


Fig. 3: Block diagram of Decryption

4. Procedure

Step 1 : Read the speech.
Step 2 : Divide the speech into samples.
Step 3 : Generate a random number by using logistic mapping.
Step 4 : Permute the sample using random numbers.
Step 5 : Generate a random number by using Quadratic mapping.
Step 6 : Permute the generated sample with result of logistic mapping.
Step 7 : Generate a random number using Sine mapping.
Step 8 : Generate a key stream by using a feedback mechanism of logistic,
quadratic and sine mapping.
Step 9 : Encrypt by adding the values of speech samples and key
Step 10: Perform decryption to get the original speech.

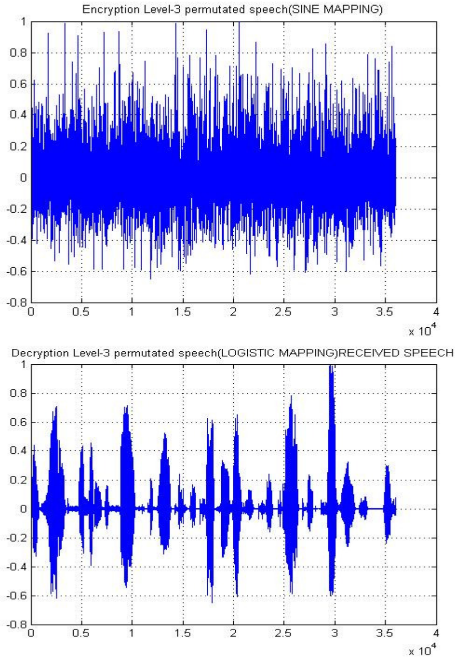


Fig. 4: Procedure

4.1 Logistic Map

The logistic map is a polynomial mapping of degree 2, often referred as an example of how complex, chaotic behaviour can arise from very simple nonlinear dynamical equations. Mathematically, the logistic map is written

$\alpha_{n+1} = r\alpha_n(1-\alpha_n)$

where $\alpha_n$is a number between zero and one that represents the ratio of existing population to the maximum possible population. The values of interest for the parameter *r* are those in the interval (0, 4].

The r=4 case of the logistic map is a nonlinear transformation of both the bitshiftmap and the μ=2 case of the tent map.

4.2 Chaotic Quadratic Map

The mathematics behind the quadratic map reflects that of the system is of the semiconductor lasers. It is a basic example of a chaotic system that can be synchronized through coupling . By definition, a map f is a generated sequence x_n using a recursion $x_{n+1} = f(x_n)$.

$f : R^m \text{->} R^m$

The equation of the quadratic map

$x_{n+1} = a - (x_n)^2$

4.3 Sine Map

The sine map is qualitatively identical to the logistic map, and the superficial similarity has resulted in a much deeper connection. It would be natural to consider splitting the interval at the critical point x = 1/2. The equation of the sine map is,

$x_{n+1} = f_\mu(x_n)$

$f_\mu(x) = \mu\sin(\pi x) x \epsilon\ [0,1],\ \mu > 0$

5. Bifurcation Analysis

Consider an ordinary differential equation (ODE) that depends on one or more parameters α

$$x = f(x,\alpha)$$

where, for simplicity, we assume α to be one parameter only. There is only a quantitatively different behaviour (shifted equilibria, e.g.). This equation is said to be structurally stablein the case there are no qualitative changes occurring. However, the ODE might change qualitatively. At that point, bifurcations will have occurred.

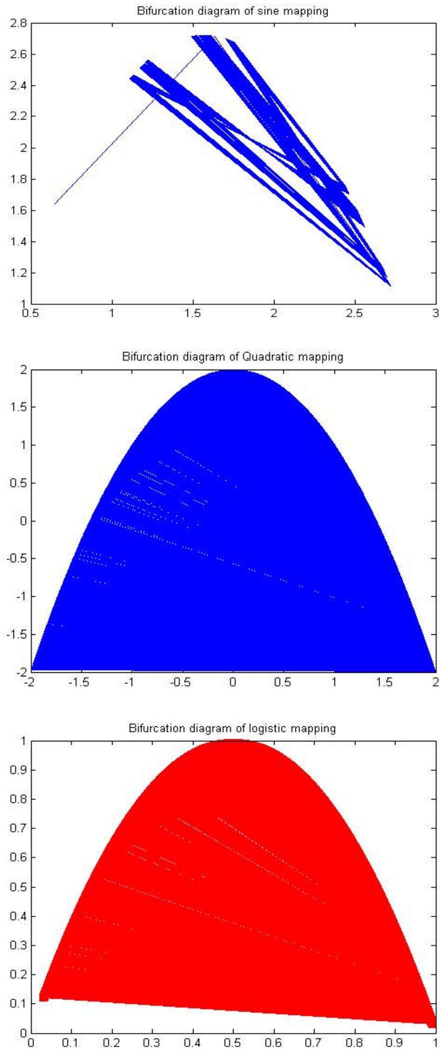


Fig. 5: Bifurcation Analysis

6. Experimental Results

In order to evaluate and quantify the properties of the proposed system we make some of the testing process.

6.1 NPCR Testing

NPCR(Number of Pixels Change Rate) is a common quantity used to evaluate the strength of the encryption with respect to differential attacks. Conventionally, a high NPCR score is usually intrepreted as a high resistance to differentian attacks. For a plain image P1 and its encryption C1,NPCR is defined by the following formula

NPCR=

For M and N represent respectively the number of rows and columns of both P1 and C1.The minimum obtained value of NPCR is 99.09%.This value indicates the efficiency of the proposed encryption technique using chaotic maps.

Table 1:Teting Analysis

Test terms	**Proposed System**	**Required values**	**Para meters**

Runs Test(χ_1)	3.5876
	5.4818
	6.4361
	6.8299
		<9.4880
		<12.592
		<15.507
		<18.307
			k=3
			k=4
			k=5
			k=6

Serial Test (χ_2)	0.512	<5.9915	
Frequency Test(χ_3)	0.89	<3.8415	
Autocorrelation(χ_4)	0.121	No Test	$-1.96 < \chi_4 < 1.96$

6.2 Encryption Results

To evaluate the encryption performance of the proposed system, itis employed toencrypt the speech signal. An original speech signal is taken having samples.

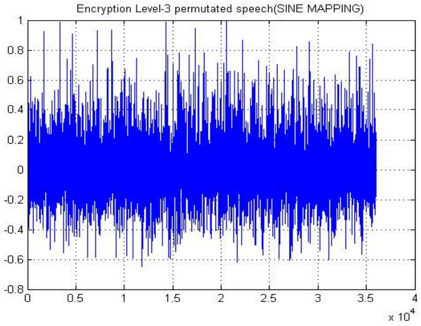


Fig. 6: Encryption Results

6.3 Auto-correlation

The auto-correlation function shows the random distribution of a signal. A high random 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 . It is evident from the plot 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 a random signal like characteristics.

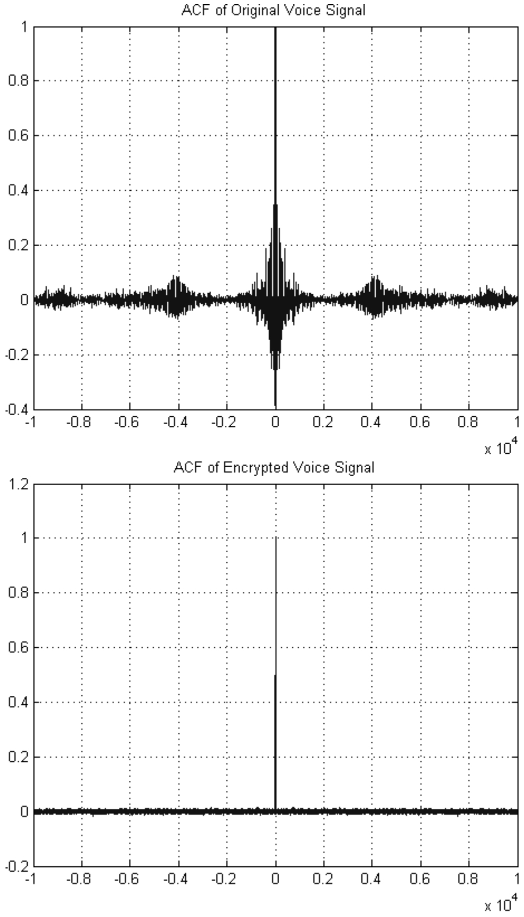


Fig.7: Auto-correlation

6.4 Key Sensitivity Analysis

The original speech signal is encrypted using secret key taken from the output generated from the 1st level mapping(logistic) which is then give to the level-by-level mapping(quadratic & sine).

Table 2:Key Sensitivity Analysis

Chaotic system	**Subkey value**	**Subkey value (one bit change)**	**% of difference**

Logistic	r=0.346
	b=3.9
		r=0.34601
		b=3.90001
			99.62

Quadratic	q=1.467
	a=2
		q=1.46701
		a=2.00001
			98.76

Sine	u=3
	y=0.758
		u=3.00001
		y=0.75801
			99.43

7. Conclusion

Today speech encryption is most important one to secure the speech from various attacks. Since our system is implemented with different chaotic maps like Logistic, Quadratic and Sine mapping technique, it is more robust and efficient than other existing systems.

References

[1] Y. Niu, X. Wang, "An anonymous key agreement protocol based on chaotic maps", Elsevier Journal on Communication in Nonlinear Science and Numerical Simulator 16 (2011) pp.13-15

[2] EmadMosa, Nagy W.Messiha, Osama Zahran, Fathi E. Abd El-Samie, "Chaotic encryption of speech signals", International Journal of Speech Technology (2011) pp.285-296

[3] Musheer Ahmad, Bashir Alam and Omar Farooq ," Chaos Based Mixed Keystream Generation for Voice Data Encryption", International Journal on Cryptography and Information Security (2012) Vol. 2, No. 1, pp.36-45

[4] Dora M.BallesterosL, JuanM.Moreno A, "Real-time, speech-in-speech hiding scheme based on least significant bit substitution and adaptive key", Elsevier International Journal (2013)

[5] SK Hafizul Islam, "Design and analysis of a three party password based authenticated key exchange protocol using extended chaotic maps", Elsevier International Journal on Information Sciences (2015) pp. 104-130

[6] Iasonas Kokkinos, Petros Maragos, "Nonlinear Speech Analysis Using Models for Chaotic Systems", IEEE Transactions on Speech and Audio Processing (2005)

[7] Howard M. Heys and Stafford E. Tavares, "Avalanche Characteristics of Substitution-Permutation Encryption Networks", IEEE transactions on computers (2005) vol.44, pp. 9

[8] Barboza R, "Dynamics of a hyper chaotic Lorenz system", Springer International Journal on Bifurcation Chaos (2007) pp.4285–4294

[9] Azzaz MS, Tanougast C, Sadoudi S, Dandache A, Monteiro F, "Real-time image encryption based chaotic synchronized embedded cryptosystems", 8th IEEE international NEWCAS conference (2010) pp. 61–64

[10] Kumar KJJ, Salivahanan S, Reddy KCK, "Implementation of low power scalable encryption algorithm", International Journal on Computer Applications (2010) pp.14–18

[11] K. W. Tang, and W. K. S. Tang, "A Chaos-based Secure Voice Communication System",International Conference on Industrial Technology (2005) pp. 571–576

[12] K. P. Man, K. W. Wong and K. F. Man, "Security Enhancement on VoIP using Chaotic Cryptography", International Conference on Industrial Electronics (2006) pp. 3703–3708

[13] Mosa E, Messiha NW, Zahran O, "Chaotic encryption of speech signals in transform domains", International conference on computer engineering & systems (2009) pp.300–305

[14] H. Tseng, R. Jan, W. Yang, "A chaotic maps-based key agreement protocol that preserves user anonymity", IEEE International Conference in Communications (ICC09) (2009) pp. 1–6

[15] Zhaopin Su, Jianguo Jiang, ShiguoLian, Donghui Hu, Changyong Liang, Guofu Zhang, "Selective Encryption for G.729 Speech Using Chaotic Maps", International Conference on Multimedia Information Networking and Security, (2009) pp. 488- 492