Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Speech Encryption by Fixed Polynomial Multiple Chaotic Maps

Charulata Thapliyal[1], Sanjay Kumar[2]
[1]Uttarakhand Technical University, Sudhowala, Dehradun, Uttarakhand, India
[2]CSE Department, Uttarakhand Technical University, Sudhowala, Dehradun, Uttarakhand, India

Abstract: ***Nowadays transfer of information is essential for online communication in daily life. Information of any type when transferred from one person to another either in physical world or virtual world needs to be secured. For this purpose we use an encryption technique in virtual world before transmission, so that in between the transmission it cannot be in understandable form. Recently encryption in speech has been the top priority in many industries. Although speech encryption is not a new technique it has been performed from 4-5 decades starting from changing its domain like frequency and time. As the number of attacks increases there is a need of new efficient techniques of speech encryption. This work focuses on unpredictable behavior of chaotic map. Since three maps are used in this work one by one that gives a more secure approach. The final encrypted output has more scrambled form so it is hard for an intruder to recover it easily .For a bulk of speech data it is an efficient technique since chaotic map gives better performance for large problem space. The performance result for this algorithm like SNR, pitch and zcr also shows that this is an efficient, reliable and robust technique for secure communication.***

Keyword: Chaotic System, Sierpinski's Triangle, Cubic Map, Polynomial Value Generation, Arnold Cat Map

I. INTRODUCTION

Speech encryption techniques have been used in many industry like phone banking, military, politics and phone stock market industry. With gradual development in modern wireless communication and multimedia technologies speech communication become a important thing for many domains. The speech data can be transfer over open or shared network. So the sensitive data should be protected from a third party intrusion. Speech encryption has become a necessity for confidential speech data. Speech has been encrypted from decades but with increasing communication technologies there is a severe demand for new encryption algorithms. The customary techniques are efficient for text data but for speech data these techniques are not suitable due to large data size and embellishment of data.

Speech encryption can be of two types: two forms digital and analog[1]. In digital encryption such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are more secure but tough in implementation and need large bandwidth for transfer. Therefore, for these limitations analog encryption is preferred [2]. In analog technique scrambling has been used frequency domain scrambling, time domain scrambling and two dimensional scrambling that mingles frequency domain scrambling with time domain scrambling. Other than scrambling there are many techniques in transform domain like fast Fourier `transform, discrete cosine transform and Wavelet transform etc.

Efficient speech encryption method demands new rebellion which can provide high protection of speech data. To attain this goal, new techniques new techniques have been developed. Among them, the chaos –based techniques are regarded as efficient for large size, redundant speech data. These techniques provide rapid and better protected encryption method.

1. Chaotic System

A chaotic system is a nonlinear deterministic dynamical system which exhibits pseudorandom behavior. The output values of chaotic systems vary depending on specific parameters and initial conditions. Different parameter values yield different periods of oscillations at the output of the systems [3]. In mathematics, a function that possesses some kind of chaotic behavior is defined as a chaotic function or map [4].Chaos theory has been evolved since 1970s by number of research domains, such as physics, mathematics, engineering and biology etc[5]. Chaotic systems can produce the pseudo-random sequences with good better randomness therefore these systems are suitable for cryptography. These systems have following features, such as the sensitivity depends on initial conditions and system parameters, pseudorandom property, no periodicity and topological transitivity etc. These properties are useful in diffusion of data.

2. Application of Speech

Protected speech plays an important component for communication. With increment in online communication technologies, we need to secure our speech data. The areas where speech is used discussed as follows:

A. Military: We already know that a military is armor for any country. Any new technology firstly implemented for armed forces. The headquarters are situated at a finite distance there is a need of online communication between authorities , that data should be protected from malicious person since the revelation of the data can harmful to security of a nation.

B. Politics: As a nation representative there is a need to discuss matter of country to another representative. Sometime this talk occurs over a network. This data should be secured, since it is a sensitive matter.

C. Phone Banking: As evolution of banking industry there is a savior need to introduced technology to banking. As a result phone banking came in existence, in which phone communication is main component. Since the system directly deals with money so communication obviously need to be protected.

*D. Phone Stock Market Industry***:** Phone stock market industry also works on speech communication. The investment of money has been done through speech so it should be confidential for both parties.

E. Telephony: Although telephony is not a new concept for us. It had developed decades ago. It also purely based on speech data. Since a connection allotted to a subscriber so the data of that user ought to be secured.

In this work three chaotic map are used i.e. triangle map , Arnold Cat Map and Cubic map since triangle map is a less used chaotic map so it provide a better security from attackers due to less exploration.

II. LITERATURE REVIEW

We already know that speech encryption algorithm is not a new technique for hiding the sensitive data. But evaluation in new technologies and advancement in hacking brings the new tools and techniques. Here present a overview in speech encryption:

As early days of speech encryption, S.Sridharan[6] et al presented a idea to apply Fast Fourier Transform Techniques . An alternative technique of speech scrambling which had received considerable attention makes use of the Fast Fourier Transform(FFT) Technique and performed scrambling in the frequency domain .In this method the DFT coefficients of frames of speech were permuted. At that time this is a very innovative technique for speech security. Zhaopin Su [7]et al present a new selective speech encryption technique using chaotic map for a standard coding algorithm G.729.In this scheme, sensitive parts are separated. Highly sensitive parts encrypted by high level ciphers and less sensitive parts are encrypted through low level ciphers. It focuses on productive approach for communication. There work encrypted the sensitive 24 bits using high level ciphers and remaining 56 bits using less power cipher using cat map and logistic map for encryption techniques. The main concern is that sometimes knowledge of less sensitive speech can help to predict the sensitive part of speech. E. Mosa [8] et al proposed a work based on permutation of speech segments using chaotic Baker map and substitution using masks in both time and transform domains. Either the Discrete Cosine Transform (DCT) or the Discrete Sine Transform (DST) can be used to remove the residual intelligibility. Masking used for hiding the silent part of speech, while the chaotic baker map gives privilege to encrypt large size audio samples. M. Ahmad, Alam and Farooq[9] presented a mixed key stream generation using high dimensional Lorenz and Chen chaotic map. Chaotic maps generate a complex and random sequence that further mixed and quantized .Hence produced a good key stream for voice encryption. Miss. Divya Sharma [10] proposed a cryptography technique for audio to increases the security of audio data meant to be transferred on an insecure medium. The audio was recorded in real time using microphone which is applied with five level of encryption which created a cipher signal which was routed through an insecure line for the recipient who on receiving that signal decrypts the cipher signal in order to retrieve the signal back. Althogh security of this technique is good but the time to encrypt in five levels is also large. M. A. Ulkarrem[11] et al gave a technique that used chaotic map and Blowfish algorithm. This work first transforms time domain to frequency domain using wavelet transformation then encrypted using logistic map and blowfish algorithm. The Blowfish Encryption algorithm uses a variable length key from 32 bits to 448 bits. S.N.A. Shaad and E. Hato[12] discussed a new technique of encryption based on Arnold cat and logistic map.This scheme uses two permutation key1 and key2, key2 then transform using either DWT or the DCT. In next level mask keys XORed with speech signal. Last level process involves 2D conversion then apply Arnold cat map and again convertinto 1D format. This is the entire encryption methodology. Masking and a large key space provide a better security to this system. Key sensitivity is better for this system. The number of steps for this work makes it a bit complicated for encryption.

III. PROPOSED TECHNIQUE

The original speech signal consists of two channels. It has frequency of 16000 HZ and 10 sec duration. After wavread it, the signal stored in matrix form. Figure 1 shows original wave form. This technique uses following functions.

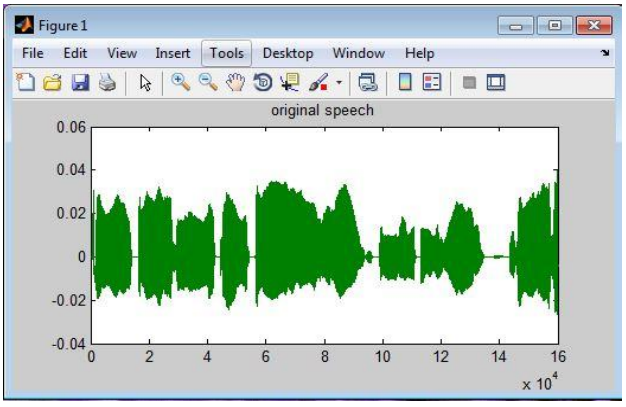

Figure 1

1. Sierpinski's Triangle

It is a unique example of a fractal, and one of the simplest ones. It is recursively defined and thus has infinite detail. It starts as a triangle and every new iteration of it creates a triangle with the midpoints of the other triangles of it. Sierpinski's Triangle has an infinite number of triangles in it. At higher level of iteration triangle become so close.

The formula is as follows:

X=[0,0]; Y=[4,0]; f=[2.0000,3.4641]; F=[N,2];

Random value r , where 0<r<1.

There are three different cases depending on r.

For i=1 to N and j=1 to 2 (1)

If r<1/3 (2)

$F_{n+1,j}=1/2((F_{n,j}+(X-F_{n,j}))$; (3)

Else If r<2/3 (4)

$F_{n+1,j}=1/2((F_{n,j}+(Y-F_{n,j}))$; (5)

Else

$F_{n+1,j}=1/2((F_{n,j}+(f-F_{n,j}))$; (6)

Where F matrix gives the values those adds to speech matrix and produced a noise like structure. Following Figure 2 shows wave after applying Sierpinski's triangle.

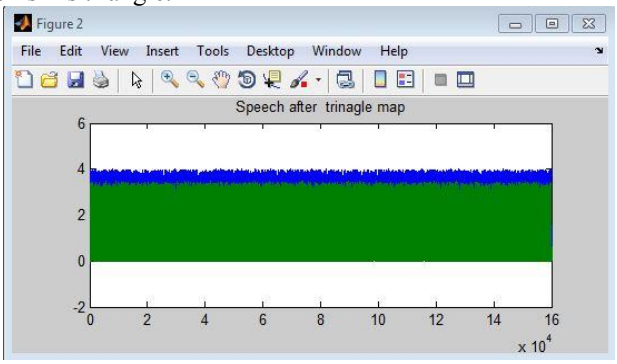

Figure 2

2. Polynomial Value Generation

In this step generate values with a fix polynomial of degree 3 that is X^3-3X^2-2X+1.And generate values of length of speech matrix using Matlab function polyval. This function generate values in m*1 matrix form. So we transpose the generated matrix and divide each value since values are very large. To produce less amplitude values this division operation plays a very important role.

$p = X^3-2X^2-3+1$; (7)

Generate values from 1 to maxSize of speech matrix. Where maxSize is Length of original Speech. Values store in a matrix .S is transpose of this and divide each values with a higher constant for avoiding higher values of amplitude . Figure 3 shows speech signal after polynomial values.

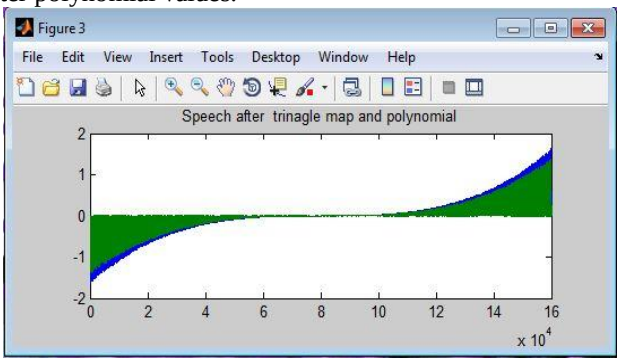

Figure 3

3. Arnold Cat Map

is used for shuffling the positioning of amplitudes. The main work of this map is to create diffusion, where as all other maps are used for confusion. Arnold cat map originally invented from an image of a cat by its founder. It changes position slightly. But after a fixed number of iteration the original position reappear. So for effective shuffling number of iteration should be chosen wisely.

The cat map applied from 1 to maxSize .

Spi = (mod(((i-1) + (j-1)),maxSize) + 1); (8)

Spj = (mod(((i-1) + 2*(j-1)),2) + 1); (9)

Spi and Spj are new position of amplitudes. It is important to note that a single iteration of Arnold cat map shuffle slightly in the position. In the Figure 4 wave form after applying Cat map is shown.

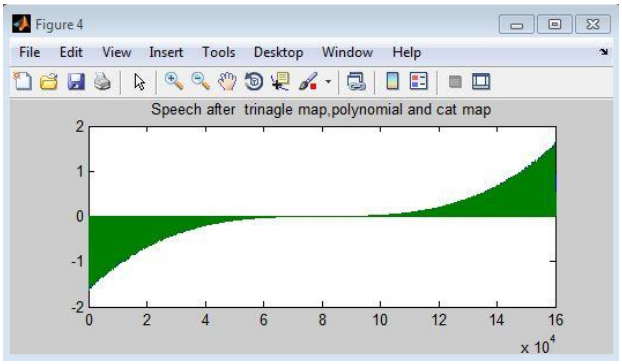

Figure 4

4. Cubic map

Cubic map is similar to logistic chaotic map but it is less implement in encryption algorithm. Where Rc is a control parameter should exist between 0 and 3.These maps possess chaotic behavior in the range of 2.59 to 3.
It produced discrete random values. It is a 1D map that generates real discrete numbers.

$$X_{n+1}=Rc.X_n- X_n^3 \quad (10)$$

After generating the values from cubic map we apply singular value decomposition .The svd command computes the matrix singular value decomposition.

s = svd(X) (11) returns a value of singular vector.

Below in following Figure 5 shows the final encrypted waveform.

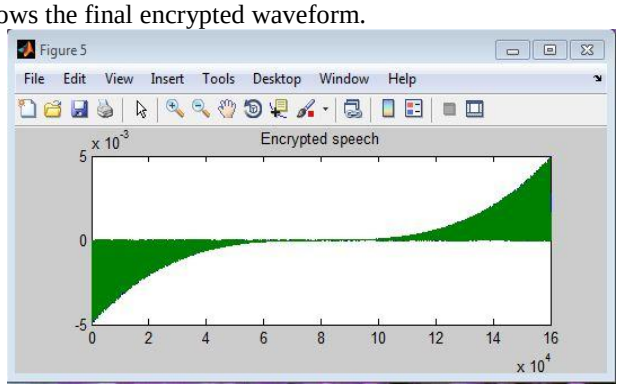

Figure 5

5. Algorithm

Step 1: Load an audio of .wav format.
Step 2: wavread it into a matrix w .
Step 3: 3.1 Generate points using Sierpinski Triangle map. With initial values X=[0,0]; Y=[4,0]; f=[2.0000,3.4641]; scale=1/2;

```
 for n=1:maxSize
  rvalue=rand(1);
if rvalue<1/3;
F(n+1,:)=F(n,:)+(X-F(n,:)).*scale;
elseif rvalue<2/3;
 F(n+1,:)=F(n,:)+(Y-F(n,:)).*scale;
 else
F(n+1,:)=F(n,:)+(f-F(n,:)).*scale;
```

3.2 Add these generated point to w and put into spch

Step 4: 4.1 Take a polynomial i.e. $X^{3-}3X^2-2X+1$
4.2 Evaluate values of length of speech matrix.
4.3 Transpose the matrix then divide each value with higher constant to avoid a large values.
4.4 Multiply this matrix with spch and put into spch0
Step 5: Apply Arnold Cat map into spch0 and put into spX

```
Spi = (mod(((i-1) + (j-1)),maxSize) + 1);
Spj = (mod(((i-1) + 2*(j-1)),2) + 1);
spX(Spi,Spj) = spch0(i,j);
```

In last statement the original i and j rearrange as Spi and Spj.
Step 6: 6.1 Generate values from Cubic map with equation

```
xlogcub(k,1)=3*xlogcub(k-1,1)*(1-(xlogcub(k-1,1))^2);
```


Where initial xlogcub=.1; and Acub=3;
6.2 Apply svd (single value decomposition) to these points
6.3Divide spX point with svd and put value into spch2
6.4 Wavwrite spch2 .

Decryption is a reverse process of this. It means we first divide svd from spch2. Then further steps executed as the reverse order. This process does not need any extra computation because only operations will reverse means if add two operand in encryption then subtract in decryption process.

IV. EXPERIMENTAL ANALYSIS RESULT

The following figure 6 shows the decrypted signal which is same as original and different from encrypted one.

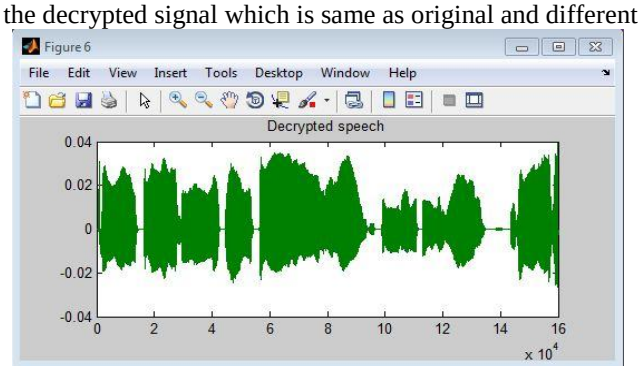

Figure 6

1. Signal to Noise Ratio

As signal is transmitted through a channel, undesired signal in the form of noise gets mixed up with the signal, along with the distortion introduced by the transmission media. Signal-to-noise ratio (SNR) is a measurement of noise in a signal. It is common measurement for residual intelligibility of the scrambled speech and the quality of the recovered speech.

Table 1 Signal to noise Ratio of encrypted Samples

Sample File	SNR
sa.wav	48.579
pi.wav	76.737
a.wav	78.529788
samp3.wav	19.938

The encrypted speech signals have high SNR values which mean that the residual intelligibility is high, and the encrypted signals of good quality. The above table shows that the encrypted sample have high SNR value thus high residual intelligibility.

2. Pitch Detection

Sounds may be generally characterized by pitch, loudness, and quality. The perceived pitch of a sound is just the ear's response to frequency, i.e., for most practical purposes the pitch is just the frequency. The below table shows that samples have a good pitch variation for encrypted and decrypted form.

Table 2 Pitches of original, encrypted and decrypted Samples

Sample File	Pitch Original	Pitch ENC	Pitch Dec
sa.wav	0.0166	4.9401e-06	0.0166
pi.wav	1.5037	6.3885e-07	1.5037
a.wav	11.5054	7.2133e-07	11.5054
samp3.wav	0.0853	0.0853	0.0853

3. ZCR

A zero-crossing is a point where the sign of a mathematical function changes (e.g. from positive to negative), represented by a crossing of the axis (zero value) in the graph of the function. At audio frequencies, such as in modern consumer

electronics like digital audio players, these effects are clearly audible, resulting in a 'zipping' sound when rapidly ramping the gain, or a soft 'click' when a single gain change is made. In the speech encryption algorithm zcr calculated to find out how many times a signal crossed the zero voltage. If encrypted and decrypted sample matched the zcr values it means algorithm's security level is low.

Table 3 zcr values of encrypted and decrypted Samples

Sample File	ZCR ENC	ZCR DEC
sa.wav	0.0356	0.0724
pi.wav	0.0437	0.0570
a.wav	0.0445	0.0462
samp3.wav	0.0138	0.1131

V. CONCLUSION AND FUTURE SCOPE

Speech is an audible form of human thought. Since scheme presented an encryption technique using multiple chaotic maps and a fixed polynomial. So these function introduced a considerable amount of noise in encrypted form which has completely different properties as compared to original signal. This is verified by plotting these signals calculating SNR ,Pitch and Zcr values. Thus the experimental results and numerical analysis demonstrates the security, effectiveness, reliable and robustness of the proposed cryptosystem. This scheme can be implemented in future using other chaotic maps as well such as one of 3D chaotic maps.

REFERENCES

[1] Sadhakan Satta B. and Abbas Nidaa A., "Performance Evaluation of Speech Scrambling Methods Based on Statistical Approach"ATTI DELLA "Fonazione Giogio Ronchi" Anno Lxvi,Np. 5 PP . 605-6014 (2011)

[2] Mosa E.; Messiha N. W.; Zahran O. and Abd El-Samie F.E "Encryption of Speech Signal with Multiple Secret Keys in Time Trasform Domains" Int J Speech Technol., Vol 13 PP . 231-242 (2010)

[3] Prabu A.V.; Srinivasarao S.;Tholada Apparao, Jaganmohan Rao M. and Babu Rao K., "Audio Encryption in Handsets" International Journal of Computer Applications (0975 - 8887), Vol. 40 No. 6 PP. 40-45 (2012).

[4] Swati Rastogi and Sanjeev Thakur," Security Analysis of Multimedia Data Encryption Technique Using Piecewise Linear Chaotic Maps", International Journal on Recent and Innovation Trends in Computing and Communication Vol. 1 Issue 5 PP. 458 – 461 (2013).

[5] Shubo Liu , Jing Sun , Zhengquan Xu "An Improved Image Encryption Algorithm based on Chaotic System", Journal of Computers ,Vol 4 ,N0 11 , pp 1091,(2009)

[6] S. Sridharan , E. Dawson and B. Goldburg, " Fast fourier transform based speech encryption system ," Proceedings of the Int. Conf. on Communications, Speech and Vision, IEEE Press, Anchorage, AK, pp. 215-223, 1991

[7] Zhaopin Su,Jianguo Jiang, Shiguo Lian,Donghui Hu, Changyong Liang, Guofu Zhang "Hierarchical selective encryption for G.729 speech based on bit sensitivity," Journal of Internet Technology vol. 11, no. 5, pp. 599-608(2010).

[8] Emad Mosa, Nagy W. Messiha, Osama Zahran,Fathi E. Abd El-Samie , "Chaotic Encryption Of Speech signals" Springer Science+Business Media LLC (2011)

[9] M. Ahmad, B. Alam and O. Farooq, "Chaos based mixed key stream generation for voice data encryption," International Journal on Cryptography and Information Security, vol. 2, no. 1, pp. 39-48, (Mar. 2012)

[10] Miss. Divya Sharma "Five Level Cryptography in Speech Processing Using Multi – Hash and Repositioning of Speech Elements" International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 5, May 2012)

[11] Maysaa abd ulkareem and Iman Qays Abduljaleel "Speech Encryption Using ChaoticMap and Blowfish Algorithms" Journal of Basrah Researchers (Sciences) Vol. (39). No (2).A (2013)

[12] Saad Najim Al Saad, Eman Hato , " A Speech Encryption on Chaotic Maps" International Journal of Computer Application (0975-8887) volume 93-No 4, (May 2014)

