ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

A Survey on Complex Secret Key Generation Method Based on Manifold Chaotic Mapping Scheme for Speech Encryption

P.Sathiyamurthi[1], Dr.S.Ramakrishnan[2], S.Sharmila[3], B.Sandhiya[4]

Assistant Professor (SS), Dept. of IT., Dr.Mahalingam College of Engineering and Technology, Coimbatore, India[1]

Professor & Head, Dept. of IT., Dr.Mahalingam College of Engineering and Technology, Coimbatore, India[2]

UG Students, Dept of IT., Dr.Mahalingam College of Engineering and Technology, Coimbatore, India [3,4]

ABSTRACT: Our project deals with the speech encryption based on three level of permutation using three different chaotic mapping functions such as Bernoulli's map, Henon map and Arnold Cat map to generate a complex secret key algorithm First, the speech input is sampled with 'N' number of samples. The samples are constructed into (m x n) matrix called original block, where m represents number of rows and n represents number of columns. This original block is randomized by permutation technique in (m-1) levels using PN sequence and one cyclic shifting operation. The PN sequence, generated by three different chaotic mapping functions is sorted and corresponding index is taken for shuffling the values of (m-1) rows. Any one of the row is shifted for three steps in cyclic manner among (m-1) rows. In order to improve the complexity of this algorithm two dimensional chaotic mapping techniques are preferred The proposed system is highly secured with more complex key and minor delay. The decryption process is the reverse operation of the encryption algorithm, carried out without disturbing the intelligibility of the original speech

KEYWORDS: Encryption,Decryption,Chaotic Mapping,permutation,multiple keys

I. INTRODUCTION

The main objective of our project is to provide a highly secured voice message by applying certain mapping techniques to encrypt a speech using Chaotic Mapping. Generally, encryption deals with converting data or information from its original form to another form that hides the information in it. Encryption by chaotic maps is widely used in speech processing due to its random-like behaviour and its sensitivity to initial conditions in addition to high confusion property. In this paper, we try to implement the permutation utilized in chaotic encryption but with cyclic shifts by using secret keys. An efficient low complex speech cryptosystem is introduced. This cryptosystem has the advantage of high degree of security and the smaller implementation time. Speech encryption seek to perform a completely reversible operation on speech by using analog speech-privacy equipments or digital encryption devices to be totally unintelligible to any of these unauthorized listener. Digital encryptions are more secured than the analog encryption but it needs a complex implementation and a large bandwidth for transmission. In the case of limited bandwidth channels, analog scramblers are better to digital scramblers

II. EASE OF USE

A) Advanced Encryption Standard (AES)

The AES was introduced by National Institute of Standards and Technology. It is one of the most secure algorithms used in symmetric key cryptography. It is based on a substitution and permutation algorithm. It has a fixed block size of 128 bits and a key size of 128, 192, 256 bits. The number of rounds of the algorithm is related to the key size. For key sizes of 128, 192, 256 bits, the number of rounds are 10, 12, 14 rounds respectively

Each round has fixed sequence of transformations, except the first and last rounds. These transformations are Sub Bytes, Shift Rows, Mix Columns and Add Round Keys. Although, AES algorithm is a strong and secure algorithm, it is high sensitive to noise due to its high diffusion abilities. The diffusion makes the elements within each block to be

DOI: 10.15680/IJIRCCE.2016. 0402007

dependent on each other. If a single element is more corrupted by noise during the transmission over the channel, will affect the surrounding elements, and the error propagates into next rounds. Decreasing the number of rounds or cancelling the Mix-Column step to reduce the noise effect reduces the security of the algorithm

$$B_{(n_1,\ldots,n_k)}(q,z) = \left(\frac{N}{n_i}(q-N_i) + z \bmod \left(\frac{N}{n_i}\right), \frac{n_i}{N}\left(z - z \bmod \left(\frac{N}{n_i}\right)\right) + N_i\right) \qquad \text{------------ (1)}$$

Where $N_i \le q < N_i + n_i$ and $0 \le z < N$ and $N_1 = 0$.

In steps, the chaotic encryption of $N \times N$ square matrix is performed as follows

(1) The matrix is divided into N rectangles of width n_i and number of elements N
(2) The elements in each rectangle is rearranged in row in the permuted rectangle. Rectangles are taken from left to right in the beginning with upper rectangles and then the lower ones
(3) Inside each rectangle, the scan begins from bottom left corner towards the upper elements
Although the chaotic Baker map solves sensitivity to noise problem of the AES and gives more flexibility in choosing the desired block size, the main drawback of chaotic cryptosystem is the small degree of security

III. PROPOSED CRYPTOSYSTEM

This project deals with a method which encrypts the speech using chaotic maps. Permutation and substitution methods are used. 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. The same process is repeated for another two mapping techniques. The result of each mapping is given as feedback to next mapping technique. By doing this we ensure that high level of security is provided. 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

A) RELATED WORK

A) Encryption and Decryption

In cryptography, Encryption is a process of translating original data into random and meaningless data. Decryption is a process of converting the cipher text into the plaintext. This is usually done with the help of a special knowledge called key. Speech Encryption is a wide area of research. Encryption deals with converting data from its original form into the other form that hides the information. The protection of speech data from the unauthorized access is important. Encryption is employed to increase the speech security

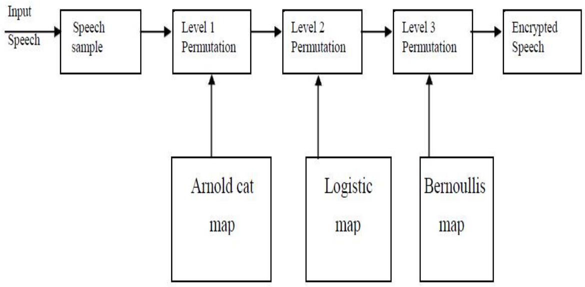

Fig 1: Block Diagram of Proposed System-Encryption

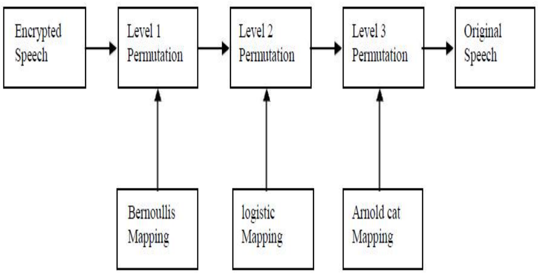

Fig 2: Block Diagram of Proposed System-Decryption

B) Chaotic Maps

The one dimensional dynamical system can be defined by the difference equation similar to where the variable k represents time. A dynamical system consists of set of possible states, together with a rule which determines the present state in terms of past states. A chaotic orbit that continues to experience the unstable behavior of an orbit exhibits near the source but that is not itself fixed or periodic

1) Bernoulli Map

The Bernoulli number is defined as Bernoulli(n) = Bernoulli(n,0).An error occurs if n is a numerical value not representing any nonnegative integer. If n is an integer larger than that of value returned by Pref::auto Expansion Limit(), then the call Bernoulli(n) is returned. Use expand(Bernoulli(n)) to get the explicit numerical result for large integers n.

```
p(ni) = (Bb*p(ni-1)) - Aa;
else
p(ni) = (Bb*p(ni-1)) + Aa;
```

------------ (2)

If n contains the non numerical symbolic identifiers, then the call Bernoulli(n) is returned. In most cases, the same holds true for calls Bernoulli(n,x)

2) Arnold Cat Map

In mathematics, Arnold cat map is a chaotic map from the torus into itself, which is named after the Vladimir Arnold, who demonstrated its effects in the 1960's using an image of a cat, hence the name

$$\Gamma\,:\,(x,y)\to(2x-y,x+y)\bmod 1.$$

In matrix notation

$$\Gamma\left(\begin{bmatrix}x\\y\end{bmatrix}\right)=\begin{bmatrix}2&1\\1&1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}\bmod 1=\begin{bmatrix}1&1\\0&1\end{bmatrix}\begin{bmatrix}1&0\\1&1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}\bmod 1.$$

------------ (3)

3) Henon Map

The Hénon map is discrete-time dynamical system. It is one among the most studied examples of dynamical systems that exhibit chaotic behavior. Hénon map takes a point (x_n, y_n) in the plane and maps it to the new point

$$\begin{cases}x_{n+1}=1-ax_n^2+y_n\\ y_{n+1}=bx_n.\end{cases}$$

------------ (4)

The map depends on two parameters, they are *a* and *b*, for the classical Hénon map have values of *a* = 1.4 and *b* = 0.

IV. ALGORITHM

1. Read the speech
2. Divide the speech into samples to get the original block
3. Generate a random number by using Arnold cat mapping
4. The random number generated is then sorted
5. The index of the original random number is found
6. Then Arnold cat map is applied to the first row
7. Generate a random number by using logistic mapping
8. The index of the original random number is found
9. Then logistic map is applied to the first row
10. Generate a random number by using logistic mapping
11. The third row is shifted by using cyclic shifts.
12. The same process is carried out by applying Bernoulli's mapping to the fourth row
13. Encrypted speech is sent to the receiver

14. Decryption is done by substituting the mapping in reverse order to get the original speech

V.CONCLUSION

An efficient speech cryptosystem has been proposed using several tests. Security analysis and the experimental results show that this cryptosystem can be used in practical applications. The encryption in this cryptosystem is performed along with permutation and masking process using multiple keys in several rounds to increase the confusion and the diffusion of data. A small change in secret key length or value gives a great change in encryption mechanism and encrypted signal. This system has large key sensitivity because, if a small change in the secret key causes large change in the encrypted signal. The proposed cryptosystem can be used for the noisy environment

REFERENCES

1. Abd El Samie, F. E. An efficient singular value decomposition algorithm for a digital audio watermarking. The International Journal of Speech Technology, 12(1), 27–45 (2009)
2. Hassan, E. S., Zhu, X., El-Khamy, S. E., Dessouky, M. I., El-Dolil, S. A., and Abd El-Samie, F. E. A chaotic interleaving scheme for the continuous phase modulation based on the single carrier frequency domain equalization. Wireless Personal Communications. doi:10.1007/s11277-010-0047-z (2010)
3. Advanced Encryption System and Federal Information Processing Standard Publications (2001)
4. Andrade, J. F., Campos, M. L., &Apolinario, J. A. Speech privacy for modern mobile communication system. In IEEE international conference on acoustics, speech and signal processing(2008)
5. Anoop, Public key cryptography application, algorithm and mathematical explanations (2007)
6. Daemen, J., &Rijndael, V. R. The advanced encryption standard. Dr. Dobb's (2001)
7. Fridrich, J., Symmetric cipher based on two dimensional chaotic maps. The International Journal of Bifurcation and Chaos(1998)
8. Goldburg, B., Sridharan, S., and Dawson, E. Design and cryptanalysis of transformation based on the analog speech scramblers. IEEE Journal of Selected Areas on Communication, 11, 735743(1993)
9. Kuo, C. J. Novel image encryption technique and application in the progressive transmission. Journal of Electronic Imaging, 2(4),345–351(1993)
10. Koduru, S. C., and Chandrasekaran, V. Integrated confusion and diffusion mechanisms for chaos based on image encryption. In IEEE 8th international conference on computer and information technology (2008)