Hemlata Kohad, Prof. V.R.Ingle,Dr.M.A.Gaikwad / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue4, July-August 2012, pp.1518-1523

Security Level Enhancement In Speech Encryption Using Kasami Sequence

Hemlata Kohad[1] , Prof. V.R.Ingle[2],Dr.M.A.Gaikwad[3]
1(Electronics Engineering, R.C.E.R.T Chandrapur ,India)
2(Electronics Engineering,B.D.C.O.E.,Sevagram,India)
3(Electronics Engineering,B.D.C.O.E.Sevagram,India)

ABSTRACT

Speech scrambling techniques are used to scramble clear speech into unintelligible signal in order to avoid eavesdropping. The residual intelligibility of the speech signal can be reduced by reducing correlation among the speech samples. Security level enhancement in speech encryption system using large set of kasami sequence is described.The speech signal is divided into segments, the polynomial is generated by using chaotic map.Using this polynomial we are generating large set of kasami sequence.Using this sequence as a key the speech signal is encrypted with AES-128 bit algorithm.The evaluation is carried out with respect to noise attack.

Keywords– Chaotic map, Kasami sequence, ,LLR,IS,Cepstrum Distance, SNR

I. INTRODUCTION

While transmitting information through insecure channel their might be unwanted disclosure as well as unauthorized modification of data if that data is not properly secured.Therefore certain mechanism are needed to protect the information when it is transmitted through any insecure channel. One way to provide such protection is to convert the intelligible data into unintelligible form prior to transmission and such a process of conversion with a key is called encryption[15]. At the receiver side the encrypted message is converted back to the original intelligible form by reverse process called decryption.

Public key encryption(asymmetric key) schemes are not suitable for the encryption of large amounts of data and time sensitive application like speech conversation because of relatively slow performance due to its complexity. To provide more security, two levels or even three levels of encryption system can be employed. In this paper ,an efficient high secured encryption system is introduced this system uses chaotic map for the generation of polynomial ,using that polynomial large set kasami sequence is generated ,which is used as key for the encryption .

II. CHAOTIC MAP

Encryption using chaotic map is much better than traditional encryption methods. It makes use of chaotic system properties such as sensitive to initial condition,ergodicity,mixing property,deterministic dynamics and structural complexity can be considered analogous to the confusion ,diffusion with small change in plaintext/secret key

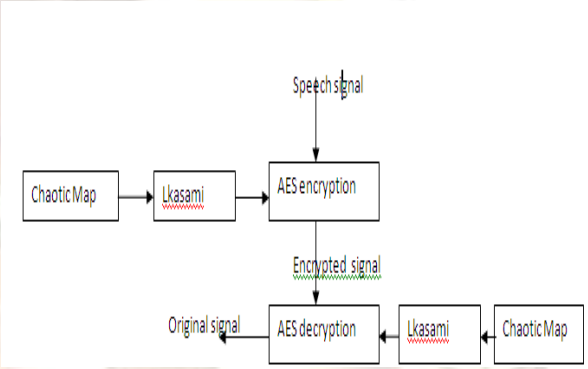

Fig.1 Block diagram of proposed system

With the rapid development of internet , security is becoming an important issue in the storage and communication.In many secure fields such as public safety and military department characters are required to be encrypted. Technologies of cryptography are the core of information security. But most ciphers can be broken with enough computational efforts.So the information security is facing challenge. So in recent years chaotic encryption has become a new research field.

Mathematically chaos refers to a very specific kind of unpredictable deterministic behavior that is very sensitive to its initial conditions. Chaotic systems consequently appear disordered and random. Chaotic system is a kind of complicated non-linear dynamic system.It has perfect security with the following properties good pseudo-random, orbital inscrutability, extreme sensitivity about initial value and the control parameter. Chaos theory is a field of study in mathematics ,physics and philosophy, studying the behavior of dynamical systems that are highly sensitive to initial conditions.This sensitivity is popularly referred to as the butterfly effect.Small differences in initial conditions widely diverging outcomes for chaotic systems rendering long term prediction impossible.This happens even though these systems are deterministic ,meaning that their future behavior is fully determined by their initial

conditions ,with no random elements involved. In other words the deterministic nature of these systems does not make them predictable. This behavior is known as deterministic chaos or simply chaos.The logistic map is a very simple mathematical model of chaotic map . The simple modified mathematical form of the logistic map is given as

Xn+1= λ *xn(1-xn)

Where xn is a state variable which lies in the interval [0,1] and λ is called system parameterwhich can have any value between 1 and 4.

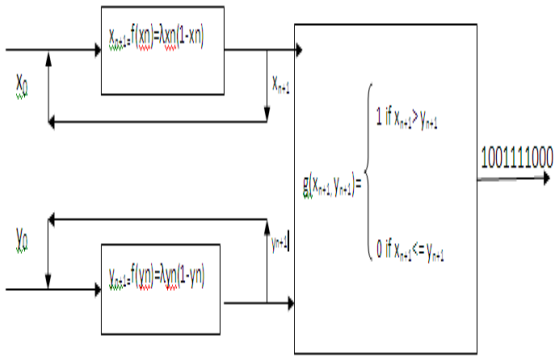

Fig.2 Logistic map

Using two logistic maps we are generating a polynomial i.e. the binary sequence that we are here consider as a coefficients of polynomial. And the output is given to the lkasami sequence generator and the output is given to AES(128 bit) algorithm.

III. PN SEQUENCE

Pseudo random binary sequences (PRBSs), also known as pseudo noise (PN), linear feedback shift register (LFSR) sequences or maximal length binary sequences (m sequences), are widely used in digital communications. In a truly random sequence the bit pattern never repeats[16-19].However, generation of such a sequence is difficult and, more importantly, such a sequence has little use in practical systems. Applications demand that the data appear random to the channel but be predictable to the user. This is where the PRBS becomes useful. A pseudo random binary sequence is a semi-random sequence in the sense that it appears random within the sequence length, fulfilling the needs of randomness, but the entire sequence repeats indefinitely. To a casual observer the sequence appears totally random, however to a user who is aware of the way the sequence is generated all its properties are known. PN sequences have several interesting properties, which are exploited in a variety of applications. Because of their good autocorrelation two similar PN sequences can easily be phase synchronised, even when one of them is corrupted by noise. A PN sequence is an ideal test signal, as it simulates the random Characteristics of a digital signal and can be easily generated. PN sequence are sequences of 1's and 0's .These sequences have random noise properties but these sequences are deterministic , so these sequences are called Pseudo noise sequences. There are different types of PN sequences.

1.m-sequence
2. Gold sequence
3.Kasami sequence

IV. KASAMI SEQUENCE

There are two types of kasami sequence

1. Small set
2. Large set

***1)Small set*:** for the degree n=4 the possible primitive polynomial x^4+x+1, the generated PN sequence will be PN1 = 100010011010111 ,the second sequence generated i.e.PN2 is result after decimation of PN1 by factor q where q is $2^{n/2}+1=5$, PN2=101 101 101 101 101.Kasami sequence generated by PN1+Time shifted version of PN2 mod 2.The number of Kasami sequences generated are $2^{n/2}=4$ [19] small set Kasami Sequence is K={PN1, PN1⊕PN2, PN1⊕T^1PN2,…. PN1⊕$T^{2n/2-2}$PN2},Cross correlation of small set kasami sequence lie in 3 values {-1,-1+$2^{n/2}$,-1-$2^{n/2}$}

2)Large set Kasami sequence :Large set contain all the sequence of small set and gold sequence The correlation function for the sequences takes on the values {-t(n), -s(n),-1,s(n)-2, t(n)-2}

Where $t(n)= 1+ 2^{(n+2)/2}$

$s(n)=1/2t(n)+1$

$$KL(u,n,k,m)=\begin{cases} u \\ v \\ u\oplus T^k v \quad k=0,\ldots\ldots,2^n-2 \\ u \oplus T^m w \quad m=0,\ldots\ldots,2^{n/2}-2 \\ v \oplus T^m w \quad m=0,\ldots,2^{n/2}-2 \\ u \oplus T^k v \oplus T^m w \quad k=0,\ldots,2^n-2 \\ \qquad m=0,\ldots,2^{n/2}-2 \end{cases}$$

u= m sequence with period 2^n-1

v= decimation of u by $1+2^{n+2/2}$ with period 2^n-1

W=decimation of u by $1+2^{n/2}$ with period $2^{n/2}-1$

Code set size of KL is $2^{n/2}(2^n+1)$

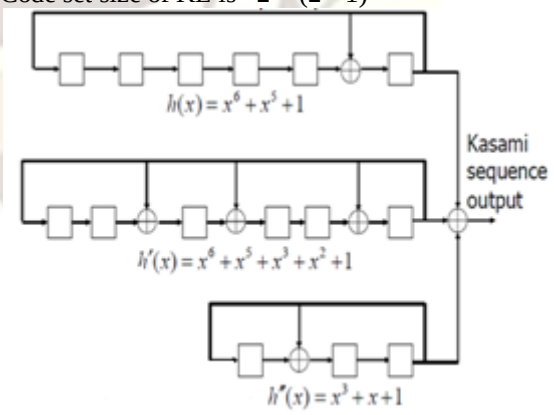

Fig 3. Large set Kasami sequence generator

V. ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard or AES was invented by Joan Daemen and Vincent Rijmen, and accepted by the US federal government in 2001 for top secret approved encryption algorithms. It is also referred to as Rijndael, as it is based off the Rijndael algorithm. Reportedly, this standard has never been cracked. AES has three approved key length: 128 bits, 192 bits, and 256 bits. To try to explain the process in simple terms, an algorithm starts with a random number, in which the key and data encrypted with it are scrambled though four rounds of mathematical processes. The key that is used to encrypt the number must also be used to decrypt it.

VI. ANALYSIS OF SPEECH SIGNAL

Speech quality assessment falls into one of the two categories;subjective and objective quality measures. Subjective quality measures are based on comparision of original and processed speech data by a listener or a panel of listeners.They rank the quality of the speech according to predetermined scale subjectively[22-24].Evaluation results per listener will include some degree of variation in most cases.This variation can be reduced byaveraging the results from multiple listeners.Thus the results from a reasonable number of speakers need to be averaged for controlled amount of variation in the overall measurement result.On the other hand, objective speech quality measures are generally calculated from the original undistorted speech and the distorted speech using some mathematical formula.It does not require human listeners ,and so it is less expensive and less time consuming.There are several methods for analysis of speech.But the following methods are commonly used

A. Short –time Fourier analysis
B. Cepstral analysis
C. Linear Prediction analysis

Linear prediction is a mathematical operation where future values of a discrete –time signal are estimated as a Linear function of previous samples.The most common representation is

$$\hat{x}(n) = \sum_{i=1}^{p} a_i x(n-i)$$

where $\hat{x}(n)$ is the predicted signal value, $x(n-i)$ the previous observed values, and a_i the predictor coefficients. The error generated by this estimate is

$$e(n) = x(n) - \hat{x}(n)$$

where $x(n)$ is the true signal value.

The most common choice in optimization of parameters a_i is the is the root mean square criterion which is also called the autocorrelation criterion. In this method we minimize the expected value of the squared error $E[e^2(n)]$, which yields the equation

$$\sum_{i=1}^{p} a_i R(j-i) = -R(j),$$

for $1 \le j \le p$, where R is the autocerrelation of signal x_n, defined as

$$R(i) = E\{x(n)x(n-i)\},$$

and E is the expected value.

The above equations are called the normal equations orYule-Walker equations. In matrix form the equations can be equivalently written as

$$Ra = -r,$$

where the autocorrelation matrix R is a symmetric, p×p Toeplitz matrix with elements $r_{i,j} = R(i-j)$, $0 \le i,j < p$, the vector r is the autocorrelation vector $r_j = R(j)$, $0 < j \le p$, and the vector a is the parameter vector.

Another, more general, approach is to minimize the sum of squares of the errors defined in the form

$$e(n) = x(n) - \hat{x}(n) = x(n) - \sum_{i=1}^{p} a_i x(n-i) = -\sum_{i=0}^{p} a_i x(n-i)$$

where the optimisation problem searching over all $a_i$must now be constrained with $a_0 = -1$. This constraint yields the same predictor as above but the normal equations are then

$$Ra = [1, 0, ..., 0]^{\mathrm{T}}$$

where the index i ranges from 0 to p, and R is a $(p + 1) \times (p + 1)$ matrix.

The speech production process can be modeled efficiently with the linear production (LP) model.There are a number of objective measures that use the distance between two sets of linear prediction coefficients(LPC) calculated on the original and the distorted speech.

$$d_{LLR}(\mathbf{a}_d, \mathbf{a}_c) = \log\left(\frac{\mathbf{a}_d \mathbf{R}_c \mathbf{a}_d^T}{\mathbf{a}_c \mathbf{R}_c \mathbf{a}_c^T}\right)$$

where **a***c* is the LPC vector for the clean speech, **a***d* is the LPC vector for the distorted speech, **a***T* is the transpose of **a**, and **R***c* is the auto-correlation matrix for the clean speech.

The Itakura-Saito (IS) distortion measure is also a distance measure calculated from the LPC vector. This measure, *dIS* is given by

$$d_{IS}(\mathbf{a}_d, \mathbf{a}_c) = \left[\frac{\sigma_c^2}{\sigma_d^2}\right]\left[\frac{\mathbf{a}_d \mathbf{R}_c \mathbf{a}_d^T}{\mathbf{a}_c \mathbf{R}_c \mathbf{a}_c^T}\right] + \log\left(\frac{\sigma_c^2}{\sigma_d^2}\right) - 1$$

where $\sigma_c 2$ and $\sigma_d 2$

are the all-pole gains for the clean and degraded speech.The Cepstrum Distance (CD) is an estimate of the log-spectrum distance between clean and istorted speech. Cepstrum is calculated by taking the logarithm of the spectrum and converting back to the time-domain. By going through this process, we can separate the speech excitation signal (pulse train

signals from the glottis) from the convolved vocal tract characteristics. Cepstrum can also be calculated from LPC parameters with a recursion formula.
CD can be calculated as follows:

$$d_{CEP}(c_d, c_c) = \frac{10}{\log 10}\sqrt{2\sum_{k=1}^{P}\{c_c(k) - c_d(k)\}^2}$$

where c_c and c_d are Cepstrum vectors for clean and distorted speech, and P is the order. Cepstrum distance is also a very efficient computationmethod of log-spectrum distance. It is more often used in speech recognition to match the input speech frame
to the acoustic models .
Spectral Distance

$$SD = \sqrt{\sum_{k=1}^{16}(x_k^c - \hat{x}_k^c)^2}$$

where x_k^c and $\hat{x}_k^c$ be the cepstral coefficients of the clean signal and the estimated signal

VII. SECURITY ANALYSIS AND RESULTS

A good encryption scheme should resist all kinds of known attacks .The security of the proposed speech cryptosystem is investigated under the noise attack.For evaluation purpose ,we used LLR ,SD,IS,CD . Typical results are presented in fig.9 to fig 12 shows distance measures from a comparision of the original speech segment with the resulting scrambled speech . It is seen that the proposed system produces scrambled speech resulting in the largest distance for LLR and lower spectral distance indicating that it has the lowest residual intelligibility.

VIII. CONCLUSION

The performance of LPC technique, which is equivalent to auto regressive (AR) modeling of the speech signal, however degrades significantly in the presence of noise.As the signal to noise ratio increases LLR,SD,CD decreases.In the evaluation of speech encrypted signal high value of these parameters represents low residual intelligibility and it gives more security. The results of computer simulation illustrate the proposed system has a high level of security and excellent audio quality. The encryption algorithm is very sensitive to the secret key with good diffusion and confusion properties. Experimental results show that the proposed cryptosystem randomize the signal and change the characteristics of it looks like random noisy signal.

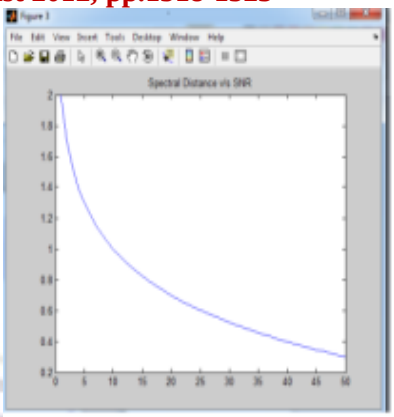

Fig 9.Spectral Distance Vs SNR

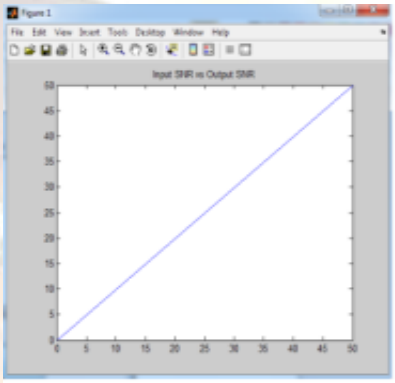

Fig 10.Input SNR Vs Output SNR

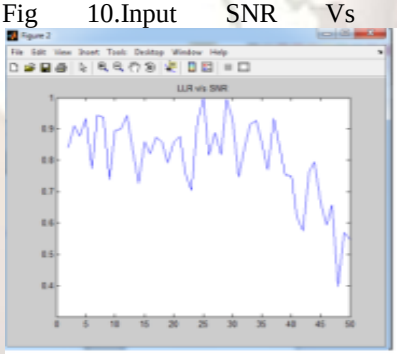

Fig.11.LLR Vs SNR

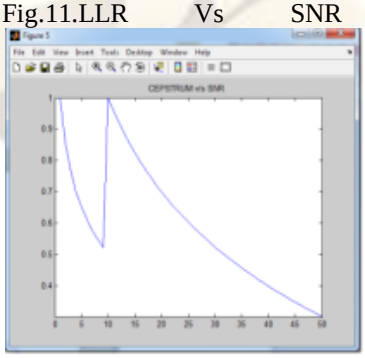

Fig12.Cepstrum Distance Vs SNR

REFERENCES

Journal Papers:

1) Lin Shan Lee Ger-Chih Chou "A New Time Domain Speech Scrambling System Which Does Not Require Frame Synchronization" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. SAC-2, NO, 3, MAY 1984 443
2) Jameel Ahmed Dr. Nassar Ikram "Frequency-Domain Speech ScramblingDescrambling Techniques Implementation and Evaluation on DSP "Proceedings IEEE INMlC 2003
3) Mohammad Saeed Ehsani, Shahram Etemadi Borujeni "Fast Fourier Transform Speech Scrambler " 2002 FIRST INTERNATIONAL IEEE SYMPOSIUM "INTELLIGENT SYSTEMS", SEPTEMBER 2002
4) E. Mosa, Nagy.W. Messiha, and O.Zahran "Chaotic Encryption of Speech Signals in Transform Domains ""978-1-4244-5844-8/09/$26.00 ©2009 IEEE
5) R. H. Laskar, F. A. Talukdar, B. Bora, K. S. P. Fernando, J. Anthony and L. Doley 9 "Complexity Reduced Multi-tier Perceptual Based Partial Encryption for Secure Speech Communication" 78–1–4244–4547–9/09/$26.00 c 2009 IEEE 1 TENCON EEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, VOL. 55, NO. 4, MAY 2008
6) Shujun Li, Chengqing Li, Kwok-Tung Lo, Member, IEEE, and Guanrong Chen, Fellow, IEEE "Cryptanalyzing an Encryption SchemeBased on Blind Source Separation" IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, VOL. 55, NO. 4, MAY 2008
7) Qiu-Hua Lin, Fu-Liang Yin, Tie-Min Mei, and Hualou Liang, Senior Member, IEEEIEEE "A Blind Source Separation Based Method for Speech Encryption" TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, VOL. 53, NO. 6, JUNE 2006
8) Qiu-Hua Lin, Fu-Liang Yin, Tie-Min Mei , Hua-Lou Liang0 "A Speech Encryption Algorithm Based on Blind Source Senaration" -7S03-8647-7/04/S20.000 2004 IEEE.
9) Ate! Mermoul and Adel Belouchra "A SUBSPACE-BA ED METHOD FOR SPEECH ENCRYPTION" 10th International Conference on Information Science, Signal Processing and their Applications (ISSPA 2010)
10) V. Anil Kumar, Abhijit Mitra and S.R. Mahadeva Prasanna "On the Effectivity of Different Pseudo – Noise and Orthogonal sequences for Speech Encryption from Correlation Properties" International journal of information technology 2007
11) Da-Peng Guo, Qiu-Hua Lin "Fast Decryption utilizing correlation calculation for BSS based speech encryption system "2010 Sixth International Conference on Natural Computation (ICNC 2010)
12) Esmael H. Dinan &Bijan Jabbari, George Mason university "Spreading codes for direct sequence CDMA & wideband CDMA cellular networks"IEEE communication magazine 1998
13) S.Chattopadhyay[(1)],S.K.Sanyal[(2)],R.Nandi" DEVELOPMENT OF ALGORITHM FOR THE GENERATION AND CORRELATION STUDY OF MAXIMAL LENGTH SEQUENCES FOR APPLICABILITIES IN CDMA MOBILE COMMUNICATION SYSTEMS "
14) Abhijit Mitra "On the Construction of m-Sequences via Primitive Polynomials with a Fast Identification Method "World Academy of Science, Engineering and Technology 45 2008
15) V. Anil Kumar, Abhijit Mitra and S. R. Mahadeva Prasanna "On the Effectivity of Different Pseudo-Noise and Orthogonal Sequences for Speech Encryption fromCorrelation Properties" International Journal of Information and Communication Engineering 4:6 2008
16) Mark Goresky, *Associate Member, IEEE, and Andrew Klapper, Senior Member, IEEE* "Pseudonoise Sequences Based on Algebraic Feedback Shift Registers
17) Abhijit Mitra "On the Properties of Pseudo Noise Sequences with a Simple Proposal of Randomness Test "International Journal of Electrical and Computer Engineering 3:3 2008
18) Abhijit Mitra " On Pseudo-Random and Orthogonal Binary Spreading Sequences "World Academy of Science, Engineering and Technology 48 2008
19) Yuh-Ren Tsai* and Xiu-Sheng Li "Kasami Code-Shift-Keying Modulation for Ultra Wideband communication Systems"
20) John Mokhoul linear Prediction: A Tutorial Review PROCEEDINGS OF THE IEEE, VOL. 63, NO. 4, APRIL 1975
21) Lawrence R. Rabiner1 and Ronald W. Schafer Introduction to Digital Speech Processing Foundations and TrendsR_ in

Signal Processing Vol. 1, Nos. 1–2 (2007) 1–194 2007

22) K. Kondo, *Subjective Quality Measurement of Speech*, 7 Signals and Communication Technology, DOI: 10.1007/978-3-642-27506-7_2, © Springer-Verlag Berlin Heidelberg 2012" Speech Quality"

23) *Shuzhen Wu and Louis C. W. Pols* a distance measure for objective quality evaluation of speech communication channels using also dynamic spectral features

24) Yi Hu and Philipos C. Loizou, *Senior Member, IEEE* Evaluation of Objective Quality Measures for Speech Enhancement IEEE TRANSACTIONS ON AUDIO, SPEECH, AND LANGUAGE PROCESSING, VOL. 16, NO. 1, JANUARY 2008