Secured Speech Communication Based on Chaotic Mapping using Cryptographic Algorithm

S.Gifta Praisy, J.Jeevitha, R.G.Harinee
Liz Alphonsa Chundattu, S.Angeline Rebekah
Electronics and communication department
Karunya Institute of Technology and Sciences
Coimbatore ,Tamilnadu

Abstract-*This paper tosses light on chaotic move keying-based chaotic encryption and decoding technique. In this strategy, the information discourse signals are inspected and its esteems are portioned into four levels, to be specific A_0, A_1, A_2, and A_3. Each level of tested esteems is permuted utilizing four confused generators, for example, logistic map, tent map, quadratic map, and Bernoulli's map. A chaotic move keying component doles out logistic map for A_0, tent map for A_1, quadratic map for A_2, and Bernoulli's map for A_3 for rearranging the chaotic tests at each level. Different testing techniques are connected to break down the proficiency of the framework. The outcomes demonstrate that the proposed framework is exceptionally secured which is masked against the assailants and has an intense dispersion and perplexity system for better chaotic correspondence in the field of media transmission.*

Keywords-*chaotic generators; encryption; decryption; move-keying; masking*

I. INTRODUCTION

Security and protection are the two major worries in the consistently developing chaotic correspondence framework. Chaotic cryptography is an answer utilized for transmitting talked data maskedly by scrambling the information at transmitter's end and decoding at recipient's end. Cryptography is a strategy wherein identification of veiled messages happens; even the interpreting is rare. The encryption is determined by scrambling the first range, and the turn around process is utilized for unscrambling.

When all is said in done, there are two sorts of encryption conspires specifically symmetric encryption and unbalanced encryption. Symmetric key also called mystery key or shared key or private key is one of the encryption strategies which utilize one key for encryption [1] as they improve the situation decoding process. Unbalanced cryptography utilizes distinctive encryption keys for encryption and decryption.

For this situation, regardless of whether it is open or private, an end client on a system has a couple of keys: one for encryption and the other one for decoding. These keys are marked as open and private keys. Symmetric plan partners with likelihood of event of numerous things for the busybody in view of bigger numbers of factorization and of numerical capacities. It can be construed numerically which is tedious and needs clearness.

These two general cryptographic strategies depend on mathematical documentations and hypothesis of computational complexity. The disordered techniques by and large depend on vast numbers (chaos) have a place with nonlinear progression field [2]. Chaotic based cryptographic capacities take after deterministic dynamics, non-guessable conduct with non-straight capacities and chaotic properties[3]. Chaotic based cryptography consolidates the conventional cryptographic procedures and the disordered synchronization to upgrade the level of security[4-9]. In this paper, higher level of security is accomplished by various level of change process on inspected discourse at five levels utilizing five distinctive riotous The chapterization of the investigation is outfitted beneath.

Section 2 tosses light on five distinctive disordered guide ping strategies. In Section 3, engineering and general standards of proposed discourse encryption are talked about in detail. Area 4 presents the better parts of chaotic exchanging and regulation strategy. In Section 5, a brief on its security investigation and test outcomes are presented keeping in mind the end goal to guard the strategy. Area 6 conveys the finishing up comments of the proposed contemplates.

II. CHAOTIC GENERATORS

A. Logistic mapping

The logistic guide is a one-dimensional mapping, having complex disorderly conduct that can emerge from extremely simple nonlinear dynamical conditions . This sort of guide more often than not appears as iterated capacities. Mathematically, the logistic guide is composed as:

$$X_{n+1} = rX_n (1-X_n) \quad (1)$$

where X_n is a number in the vicinity of zero and one which represent the proportion of existing populace to the most extreme conceivable populace and r is the control parameter that controls the conduct of the guide.

This nonlinear distinction condition is planned to top ture two impacts:

i. Reproduction where the populace will increment at a rate relative to the present populace when the populace estimate is little.

ii. Density subordinate mortality where the development rate will diminish at a rate corresponding to the esteem acquired by taking the hypothetical "conveying limit" of nature with lesser current populace.

The calculated guide is a nonlinear change when r = 4. While changing the parameter r, diverse practices are watched. From every underlying condition, there is no swaying of limited period. Minor variety in the initial populace yields sensational change in comes about over some stretch of time. The strategic guide is utilized as a part of this proposed work for change and substitution of A_0 parameters in chaotic switch. Fig.4 shows the encrypted logistic map.

B. Tent mapping

The tent guide with parameter μ is the genuine esteemed function f_μ characterized by $f_\mu = \mu \min\{X, X - 1\}$. For the estimations of the parameter μ inside 0 and 2, f_μ maps the unit interim [0, 1] into itself, along these lines characterizing a discrete time dynamical framework on it proportionately, a repeat connection [13]. Specifically, emphasizing a point X_0 in [0, 1] offers ascend to a sequence X_n:

$$X_{n+1} = f\mu(X_n) = \begin{cases} \mu X_n & \text{for } X_n<1/2 \\ \mu(1-X_n) & \text{for } 1/2 <X_n \end{cases} \quad (2)$$

where μ is a positive genuine consistent. Deciding for example the parameter μ = 2, the impact of the capacity f_μ might be seen as the aftereffect of the activity of collapsing the unit interim in two, at that point extending the came about interim [0,1/ 2] to get the interim [0,1]. Emphasizing the strategy, any purpose of X_0, interim expect new resulting positions as determined above, producing a grouping X_n in [0,1]. The μ = 2 instance of the tent guide is a nonlinear change.

Contingent upon the estimation of μ, the tent guide exhibits extensive variety of dynamical practices appropriate from unsurprising to disordered. On the off chance that μ is under 1, the point X = 0 is a draw in settled purpose of the framework for every underlying estimation of X, i.e., the framework will unite towards x = 0 from any underlying estimation of X. In the event that μ is 1, all estimations of X not exactly or equivalent to 1/2 are settled purposes of the framework. On the off chance that μ is more noteworthy than 1, the framework has two settled focuses, one at 0, and the other at μ/(μ + 1).. The tent guide is utilized as a part of this proposed work for change and substitution of A_1 parameters in chaotic switch.Fig.5 shows the encrypted tent map.

C. *Quadratic mapping*

In straightforward scientific detailing, quadratic map exhibits extremely convoluted dynamical properties[13] and concerns the asymptotic conduct of repeats, when n → +∞. In addition, such highlights may change in a dramatic path under variety of the parameter a. This is related to the way that for huge n, being a high degree polynomial, depends complicatedly on x and a. The quadratic mapping can be utilized as a model for the depiction of such progression with more extensive degree.

The condition of the quadratic map:

$$x_{n+1} = a-x_n^2 \quad \text{for} \quad 0<a<2 \quad (3)$$

The areas on the quadratic map parts at certain fixed focuses. The fixed focuses are x_n. In the closeness around one of our fixed focuses, if the guide is iterated, the solution will liable to fluctuate. It is possible that it will pull in the fixed point or repulse. On account of the quadratic map, there exists aversion and fascination. In the event that there is appreciation for the fixed point, the fixed point is steady. On the off chance that there is repulsion, the fixed point is unsteady. With a specific end goal to get an unmistakable picture of what goes ahead in the quadratic map, the fixed focuses should be recognized and its dependability be broke down. Here, linearization may likewise be utilized. The quadratic guide is utilized as a part of this proposed work for change and substitution of A_2 parameters in chaotic switch. Fig.6 shows the encrypted quadratic map.

D. Bernoulli's mapping:

Bernoulli's guide is a one-dimensional map $x_{n+1} = \{2x_n\}$ where the $\{2x_n\}$ assign a partial piece of the number. It is advantageous to speak to the variable x in a parallel notation, and after that the digit 0 at the primary position after the speck compares to living arrangement of the condition of the model in the left piece of the unit interim, and 1 to dwell in the correct part. Such a change of the parallel succession is known as the Bernoulli shift[13].

$$f(x) = \begin{cases} 2x & 0\le x<0.5 \\ 2x-1 & 0.5\le x<1 \end{cases} \quad (4)$$

In this mapping, a little one-advance perturbation of initial condition, the cycles develop twice. The Bernoulli's map is utilized as a part of this proposed work for change and substitution of A_3 parameters in chaotic switch.Fig.7 shows the encrypted Bernoulli's map.

III. ARCHITECTURE OF PROPOSED CRYPTOSYSTEM:

Initially, the given speech signal is examined in the range between 0 and 1 and are isolated into four levels $A_0 = -1$ to -0.5, $A_1 = -0.5$ to 0, $A_2 = 0$ to 0.5, and $A_3 = 0.5$ to 1. Each level of the speech signal tests is permuted with respect to the comparing chaotic mapping systems, for example, logistic map, tent map, quadratic map, and Bernoulli's map. These chaotic generators are utilized to generate a similar measure of irregular numbers equivalent to the speech tests in each segment.

The irregular numbers created by the chaotic generators are arranged in ascending order.In view of the records of the irregular numbers, the examined estimations of speech signals are permuted. The permuted parameters are substituted with the irregular numbers produced by comparing chaotic generator.

The procedure of determination of chaotic generator for each level of sampled speech is done by confused switch keying method. The strategy for disorderly exchanging speaks to the least difficult type of tweak with chaotic attractors. The signal u(t) controls the switch which flips between the chaotic frameworks and distinctive parameters A_0, A_1, A_2, and A_3. The encryption comprises of four chaotic subsystems:

i. Subsystem with the parameters A_0—dynamic when $-1 \leq u(t) < -0.5$

ii. Subsystem with the parameters A_1—dynamic when $-0.5 \leq u(t) < 0$

iii. Subsystem with the parameters A_2—dynamic when $0 \leq u(t) < 0.5$, and

iv. Subsystem with the parameters A_3—dynamic when $0.5 \leq u(t) \leq 1$

Transmission of the chaotic attractor C_0, created by the primary chaotic circuit in view of calculated mapping (with the parameters A_0), compares to the esteem − 1 to − 0.5. A_1), relates to the esteem − 1 to − 0.5. tent mapping (with the parameters attractor C_2, created by the third chaotic Transmission of the attractor C_1, created by the second chaotic circuit in light of circuit in view of quadratic mapping (with the parameters A_2), relates to the esteem 0.5 to 0.75. What's more, transmission of the attractor C_3, produced by the second chaotic circuit in light of Bernoulli's mapping, compares to the esteem 0.75 to 1.

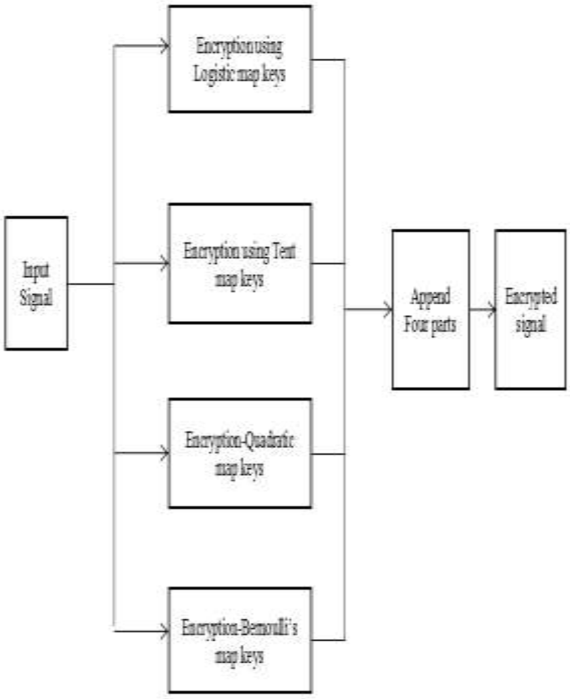

Fig 1.Block diagram of Encryption process

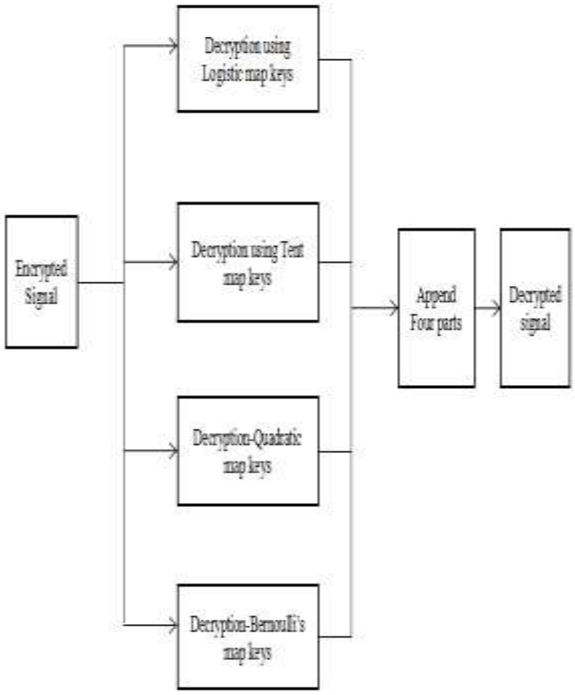

Fig 2.Block diagram of Decryption process

The whole framework goes about as a control which switches between the attractors C_0, C_1, C_2, and C_3. The recipient likewise comprises of four chaotic subsystems which must be indistinguishable and synchronized with the transmitter side. The first is intended for demodulating the qualities between − 1 and − 0.5, the second one for the qualities between − 0.5 and 0, the third one for values in the vicinity of 0 and 0.5, and the fourth one for the qualities in the vicinity of 0.5 and 1. The demodulation is completed based on choices inside a customary time interim. A powerful demodulation of a specific esteem is conceivable just when the confused frameworks on the transmitter and the collector sides are precisely synchronized. After arrangement of permutation process, the whole discourse tests are added.

IV. CHAOTIC SWITCHING AND MODULATION

The technique for chaotic switching speaks to the least complex type of adjustment with chaotic attractors [11]. It is reasonable for translating advanced signs. The substance of the chaotic balance alludes to balance of the information signal y(t) by a chaotic signal u(t) produced by the disordered flag generator. The signal y(t) is balanced by the signal u(t) in the chaotic modulator where augmentation happens. The modulated signal s(t) is transmitted over the communication channel to the recipient where in the chaotic demodulator, the demodulation or division of the modulated signal s(t) with the chaotic signal u(t) is done. The fairness of the beneficiary's and the transmitter's parameters and their synchronization is a condition for effective demodulation.

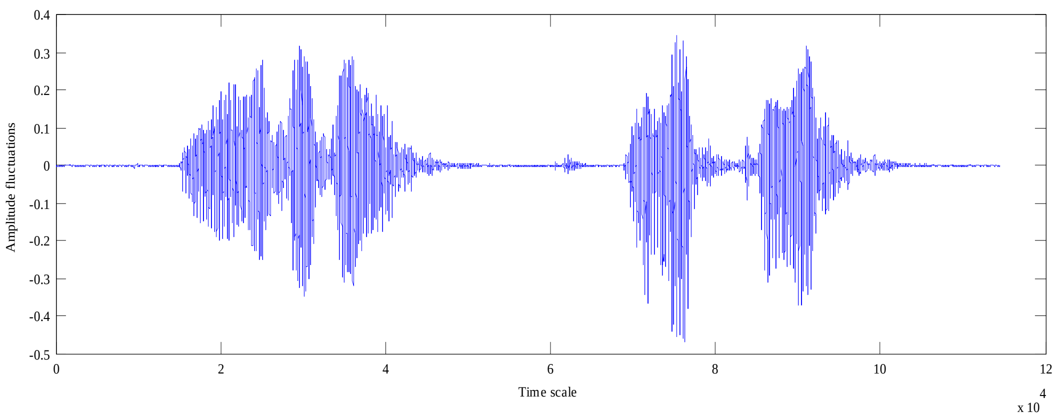

Figure3. Input speech signal

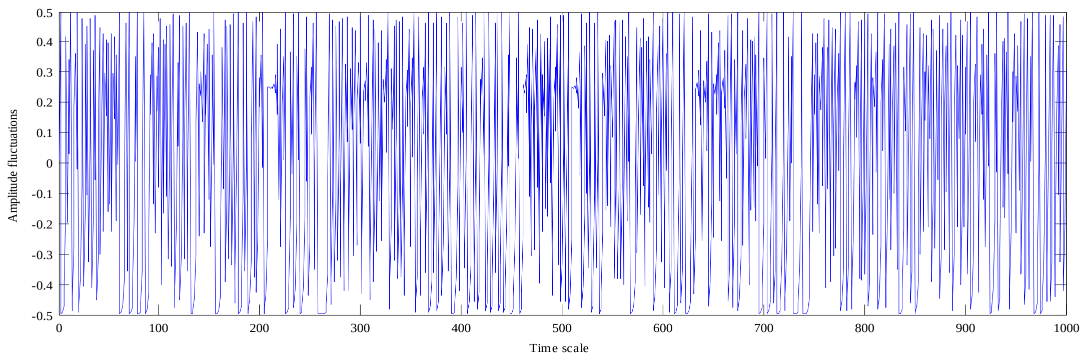

Figure4. Encrypted logistic map

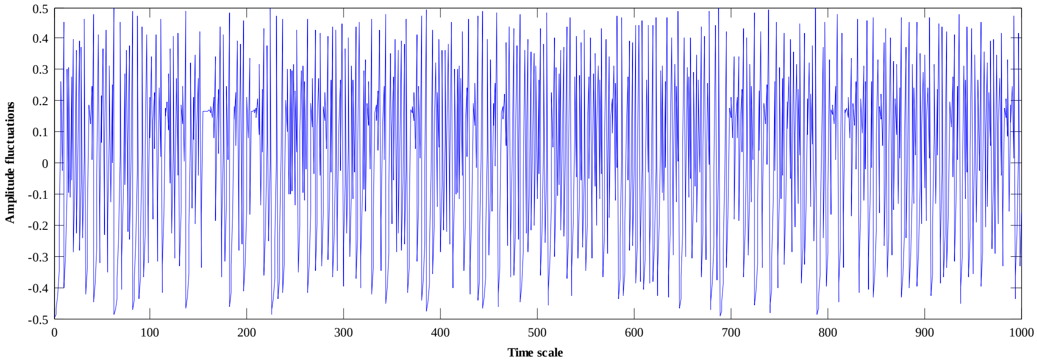

Figure5. Encrypted tent map

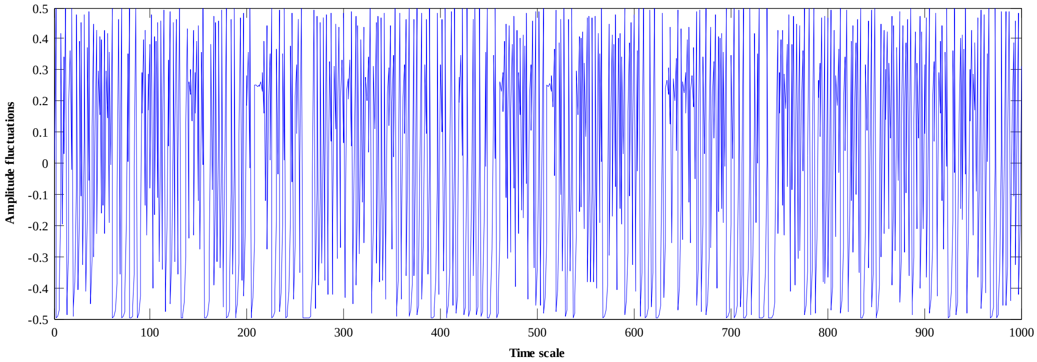

Figure6. Encrypted quadratic map

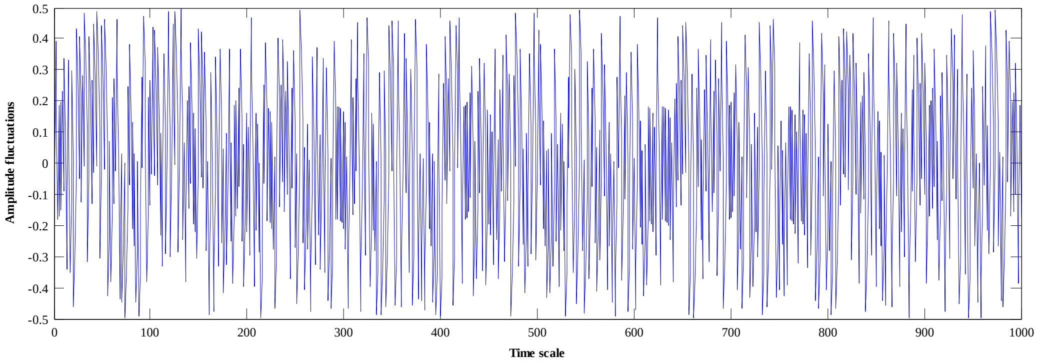

Figure7. Encrypted Bernoulli's map

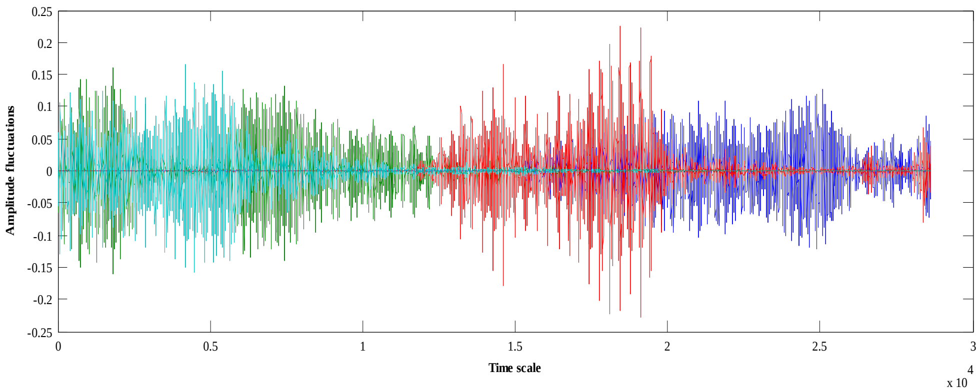

Figure8. Encrypted signal

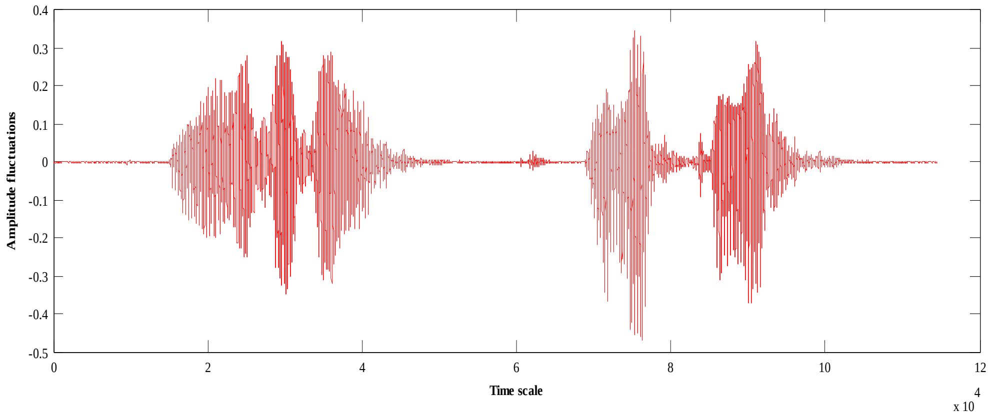

Figure 9. Decrypted signal

V. RESULTS AND DISCUSSION

The proposed framework was tried in Matlab. This system was subjected to correlation test and histogram analysis which are auto tried out to demonstrate the execution measurements .The higher the chaos to signal proportion, the more secure the framework is considered with the goal that the five chaotic generators are utilized as a part of this proposed framework in which one is the primary and remaining four are secondary.

A. Correlation test

The auto relationship work distinguishes the disorderly system that delivers a solid encryption. A helpful measure to survey the encryption nature of any cryptosystem is connection coefficient between comparative sections free flag and figure signal. It is computed

$$r_{xk} = \frac{c(x,k)}{\sqrt{v(x)}\sqrt{v(k)}} \quad (5)$$

where C(x, k) is the covariance between the first flag x and the scrambled flag k. V(x) and V(k) are the differences of the signs x and k.Fig.10 shows the output of correlation test

B. Histogram analysis

This test is connected to assess the resistance of the algorithm against differential assaults.The histogram investigation has been considered to demonstrate the quality of our calculation. Histogram of input speech sample test appeared in Fig. 11 is nearer to the histogram of decoded signal appeared in Fig. 12.

.

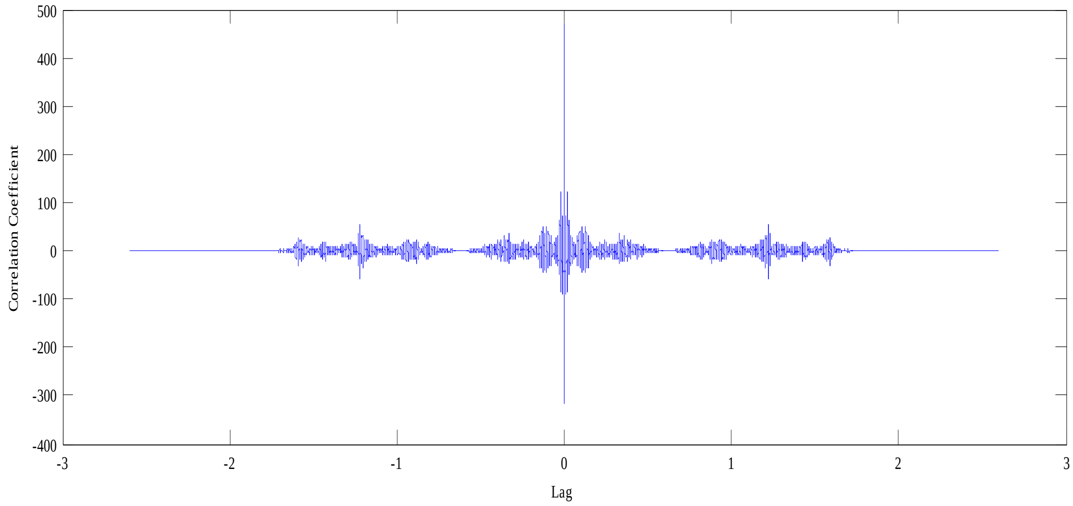

Figure10. Correlation test

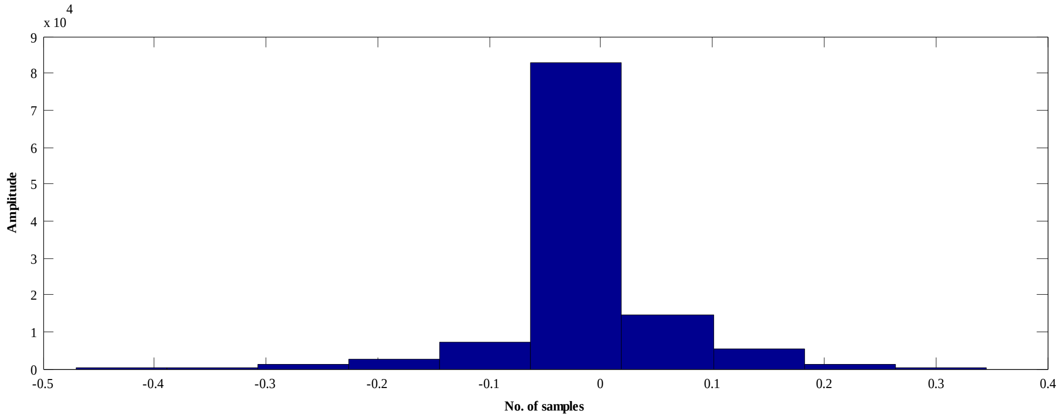

Figure11. Histogram of input signal

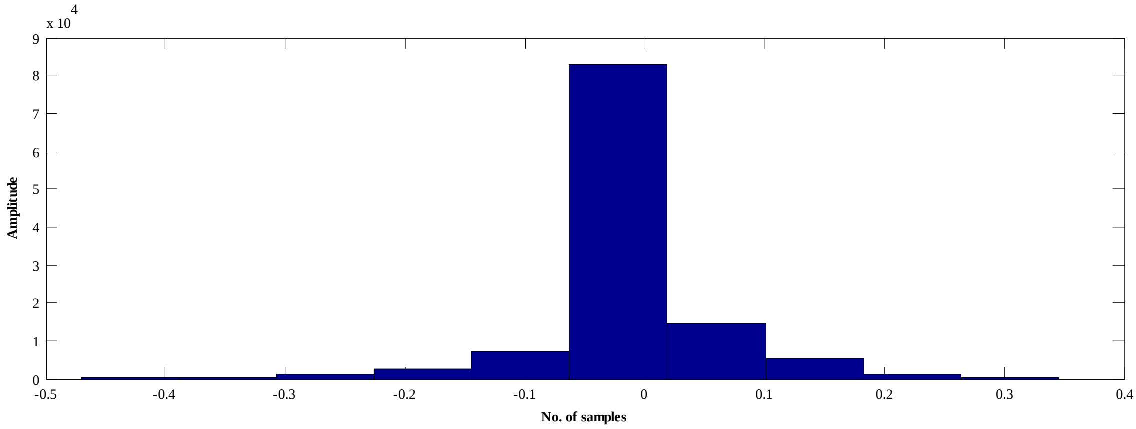

Figure12. Histogram of output signal

VI. DISCUSSION AND CONCLUSIONS

Speech encryption utilizing various chaotic generators and chaotic disordered move keying is a demonstrated model. In this strategy, the four diverse speech signals with various time length are inspected and its esteems are permuted utilizing logistic guide and further the permuted esteems are divided into four levels. Each level is permuted utilizing four distinctive disordered generators. chaotic move keying instrument is powerfully doling out various disordered maps to various levels of examined esteems for rearranging the speech tests at each level. The histogram of the encrypted signal demonstrates that greater affectability involves greater security. The decoded signal is fundamentally the same as the first speech as it demonstrates the dependability of remaking of unique signal. The outcome acquired by the proposed framework is exceedingly screened from aggressors and has an intense dispersion and perplexity instrument and better for constant discourse correspondence. The outcomes underwrite that the speech signal is exceedingly veiled from eavesdroppers

.

References

1. Fridrich J. (1998), Symmetric ciphers based on two-dimensional chaotic maps, International Journal of Bifurcation and Chaos, Volume 8(6), 1259–1284.
2. Ljupco Kocarev(2002), Chaos-based cryptography: a brief overview, IEEE Circuits and Systems Magazine, pp 7-21.
3. Yang, T., Wu, T. W., & Chua, L. O. (1997). Cryptography based on chaotic systems. IEEE Transactions on Circuits and Systems I, 44, 469–472.
4. Yang, T. (1999). Chaotic secure communication systems: history and new results. Telecomm. Rev., 9(4), 597–631.
5. Mosa, E., Messiha, N. W., Zahran, O., & Abd El-Samie, F. E. (2011). Chaotic encryption of speech signals. International Journal of Speech Technology, 14, 285–296.
6. Sheu, L. J. (2011). A speech encryption using fractional chaotic systems. Nonlinear dynamics, 65(1–2), 103–108.
7. Baker, H. J., & Piper, F. C. (1985). Secure Speech Communications, Academic Press Publisher.
8. Bianco M E, Reed D A (1991) Encryption system based on chaos theory, US Patent No.5048086, USA, 1-12
9. Yau, H. T., Pu, Y. C., & Li, S. C. (2012). Application of chaotic synchronization systems to secure communication. International Journal of Information Technology and Control, Volume, 41, 274–282.
10. Addabbo, T., Alioto, M., Bernardi, S., Fort, A., Rocchiand, S., & Vignoli, V. (2004). The digital tent map: performance analysis and optimized design as a source of pseudorandom bits. IEEE Transaction on Instruments and Measurements, Volume, 2, 1301–1304.
11. Yang, T., & Chua, L. O. (1997). Secure communication via chaotic parameter modulation. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 43(9), 817–819.
12. Mittal, A. K., Dwivedi, A., & Dwivedi, S. (2015). Secure communication based on chaotic switching and rapid synchronization using parameter adaptation. International Journal of Innovative Computing Information and Control, 11(2), 569–585.
13. Mohammed, R. S., & Sadkhan, S. B. (2016). Speech scrambler based on proposed random chaotic maps. IEEE International Conference on Multidisciplinary in IT and Communication Science and Applications, Baghdad, 2016, 1–6.