Sathiyamurthi and Ramakrishnan *EURASIP Journal on Audio, Speech, and Music Processing* (2017) 2017:20
DOI 10.1186/s13636-017-0118-0

EURASIP Journal on Audio, Speech, and Music Processing

RESEARCH Open Access

# Speech encryption using chaotic shift keying for secured speech communication

P. Sathiyamurthi* and S. Ramakrishnan

**Abstract**

This paper throws light on chaotic shift keying-based speech encryption and decryption method. In this method, the input speech signals are sampled and its values are segmented into four levels, namely $L_0$, $L_1$, $L_2$, and $L_3$. Each level of sampled values is permuted using four chaotic generators such as logistic map, tent map, quadratic map, and Bernoulli's map. A chaotic shift keying mechanism assigns logistic map for $L_0$, tent map for $L_1$, quadratic map for $L_2$, and Bernoulli's map for $L_3$ for shuffling the speech samples at every level. Further, the sampled values are permuted using Chen map which uncovers the chaotic behavior. Various testing methods are applied to analyze the efficiency of the system. The results prove that the proposed system is highly secured against the attackers and possesses a powerful diffusion and confusion mechanism for better speech communication in the field of telecommunication.

**Keywords:** Speech processing, Chaos, Mapping, Shift keying, Encryption

## 1 Introduction

Security and privacy are the two major concerns in the ever growing speech communication system. Speech cryptography is a solution used for transmitting spoken information in a masked way by encrypting the data at transmitters' end and decrypting at receivers' end. Cryptography is a method wherein detection of masked messages takes place; even the decoding is hard to come by. The encryption is derived by scrambling the original spectrum, and the reverse process is used for decryption.

In general, there are two types of encryption schemes namely symmetric encryption and asymmetric encryption. Symmetric key otherwise known as secret key or shared key or private key is one of the encryption methods [1] which use one key for encryption as they do for decryption process. Asymmetric cryptography [2, 3] uses different encryption keys for encryption and decryption. In this case, whether it is public or private, an end user on a network has a pair of keys: one for encryption and the other one for decryption. These keys are labeled as public and private keys. Symmetric scheme associates with probability of occurrence of many things for the eavesdropper based on larger numbers of factorization and of mathematical functions. It can be inferred mathematically which is time consuming and lacks clarity.

These two general cryptographic methods are based on algebraic notations and theory of computational complexity. The chaotic methods generally rely on large numbers (chaos) belong to nonlinear dynamics field [4]. Chaotic-based cryptographic functions follow deterministic dynamics, non-guessable behavior with non-linear functions and chaos properties [5–7]. Chaotic-based cryptography combines the traditional cryptographic techniques and the chaotic synchronization to enhance the degree of security [8–14]. In this paper, higher degree of security is achieved by multiple level of permutation process on sampled speech at five levels using five different chaotic maps. Furthermore, the proposed system provides better withstanding capacity against various attacks. The chapterization of the study is furnished below.

Section 2 throws light on five different chaotic mapping techniques. In Section 3, architecture and general principles of proposed speech encryption are discussed in detail. Section 4 introduces the finer aspects of chaotic switching and modulation method. In Section 5, a brief on its security analysis and test results are presented in order to defend the method. Section 6 carries the concluding remarks of the proposed study.

* Correspondence: sathyamurthi.bit@gmail.com
Department of Information Technology, Dr. Mahalingam College of Engineering and Technology, Pollachi 642003, India

## 2 Chaotic generators

### 2.1 Logistic mapping

The logistic map is a one-dimensional mapping, having complex chaotic behavior that can arise from very simple nonlinear dynamical equations [15] (https://en.wikipedia.org/wiki/List_of_chaotic_maps). This kind of map usually takes the form of iterated functions. Mathematically, the logistic map is written as:

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

where $X_n$ is a number between zero and one which represents the ratio of existing population to the maximum possible population and $r$ is the control parameter that controls the behavior of the map.

This nonlinear difference equation is intended to capture two effects:

i. Reproduction where the population will increase at a rate proportional to the current population when the population size is small and
ii. Density dependent mortality where the growth rate will decrease at a rate proportional to the value obtained by taking the theoretical "carrying capacity" of the environment with lesser current population.

The logistic map is a nonlinear transformation when $r = 4$. While varying the parameter $r$, different behaviors are observed. From almost all initial conditions, there is no oscillation of finite period. Minor variation in the initial population yields dramatic change in results over a period of time. The logistic map is used in this proposed work for permutation and substitution of $L_0$ parameters in chaotic switch.

### 2.2 Tent mapping

The tent map with parameter $\mu$ is the real-valued function $f_\mu$ defined by $f_\mu = \mu \min\{X, X - 1\}$. For the values of the parameter $\mu$ within 0 and 2, $f_\mu$ maps the unit interval [0, 1] into itself, thus defining a discrete time dynamical system on it equivalently, a recurrence relation [16] (https://en.wikipedia.org/wiki/List_of_chaotic_maps). In particular, iterating a point $X_0$ in [0, 1] gives rise to a sequence $X_n$:

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

where $\mu$ is a positive real constant. Choosing for instance the parameter $\mu = 2$, the effect of the function $f_\mu$ may be viewed as the result of the operation of folding the unit interval in two, then stretching the resulted interval [0,1/2] to get the interval [0,1]. Iterating the procedure, any point of $X_0$, interval assumes new subsequent positions as specified above, generating a sequence $X_n$ in [0,1]. The $\mu = 2$ case of the tent map is a nonlinear transformation.

Depending on the value of $\mu$, the tent map demonstrates wide range of dynamical behaviors right from predictable to chaotic. If $\mu$ is less than 1, the point $X = 0$ is an attractive fixed point of the system for all initial values of $X$, i.e., the system will converge towards $x = 0$ from any initial value of $X$. If $\mu$ is 1, all values of $X$ less than or equal to 1/2 are fixed points of the system. If $\mu$ is greater than 1, the system has two fixed points, one at 0, and the other at $\mu/(\mu + 1)$. If $\mu$ is between 1 and 2, the interval $[\mu - \mu/2, \mu/2]$ contains both periodic and non-periodic points, although all of the orbits are unstable. The tent map is used in this proposed work for permutation and substitution of $L_1$ parameters in chaotic switch.

### 2.3 Quadratic mapping

In simple mathematical formulation, quadratic map exhibits very complicated dynamical properties [16] (https://en.wikipedia.org/wiki/List_of_chaotic_maps) and concerns the asymptotic behavior of iterates, when $n \to +\infty$. Moreover, such features may change in a dramatic way under variation of the parameter $a$. This is related to the fact that for large $n$, being a high degree polynomial, depends in a complicated way on $x$ and $a$. The quadratic mapping can be used as a model for the description of such dynamics with wider scope.

Consider the equation of the quadratic map:

$$x_{n+1} = a - {x_n}^2 \quad for \qquad 0 < a < 2 \tag{3}$$

The areas on the quadratic map splits at certain fixed points. The fixed points are $x_n$. In the proximity around one of our fixed points, if the map is iterated, the solution will likely to vary. Either it will attract the fixed point or repel. In the case of the quadratic map, there exists repulsion and attraction. If there is attraction to the fixed point, the fixed point is stable. If there is repulsion, the fixed point is unstable. In order to get a clear picture of what goes on in the quadratic map, the fixed points ought to be identified and its stability be analyzed. Here, linearization may also be used.

If $x$ is a fixed point, $x = a - x^2$ so, $0 = x^2 + x - a$ and $x = \pm(-1 + (1 + 4a)^{1\backslash 2})/2$. To find the stability and attraction of the fixed point in the neighborhoods around them, let $x_n = x \pm \delta_n$, where $\delta$ is a small distance. Then $x_{n+1}$ becomes $x_{n+1} = a - x_n^2 = a - (x+\delta_n)^2 = a - (x^2 + 2\delta_n x + \delta_n^2) = a - x_2 - 2\delta_n x - \delta_n^2$ because $x_{n+1} = x + \delta_{n+1}$ and $x = a - x^2$, $x + \delta_{n+1} = x - 2\delta_n x - \delta_n^2$. The quadratic map is used in this proposed work for permutation and substitution of $L_2$ parameters in chaotic switch.

### 2.4 Bernoulli's mapping

Bernoulli's map is a one-dimensional map $x_{n+1} = \{2x_n\}$ where the $\{2x_n\}$ designate a fractional part of the number. It is convenient to represent the variable $x$ in a binary notation, and then the digit 0 at the first position after the dot corresponds to residence of the state of the model in the left part of the unit interval, and 1 to reside in the right part. Such a transformation of the binary sequence is called the Bernoulli shift [16] (https://en.wikipedia.org/wiki/List_of_chaotic_maps).

With an initial state defined by a random digital sequence obtained, say, by tossing a coin with a rule of heads or tails: $x_n = 0.0101101....$ It is observed that during course of iterations, this will oscillate towards left or right half of the unit interval exactly to the random sequence defined. Here, it behaves in a chaotic manner. This transformation can also be defined as the iterated function map of the piecewise linear function.

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

In this mapping, a small one-step perturbation of initial condition, the iterations grow twice. The Bernoulli's map is used in this proposed work for permutation and substitution of $L_3$ parameters in chaotic switch.

### 2.5 Chen mapping

Chen map is often represented as Chen map and it is of one-to-one transformation [17] (https://en.wikipedia.org/wiki/List_of_chaotic_maps). It is given by

$$\begin{bmatrix} x^l \\ y^l \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod} N) \quad (5)$$

where $p$ and $q$ are its parameters. It is invertible because the matrix has determinant value of 1, and therefore, its inverse has integer entries with larger numbers.

One of the features is that the signal can be apparently randomized by the transformation but getting back to its original state warrants number of steps. This map is used in this proposed work for permutation and substitution of all the parameters before the chaotic shift keying at encryption side.

## 3 Architecture of proposed cryptosystem

First, the given speech signal is sampled in the range between 0 and 1 and are divided into four levels $L_0 = -1$ to $-0.5$, $L_1 = -0.5$ to 0, $L_2 = 0$ to 0.5, and $L_3 = 0.5$ to 1. Each level of the speech samples is permuted with respect to the corresponding chaotic mapping techniques such as logistic map, tent map, quadratic map, and Bernoulli's map. These chaotic generators are used to generate the same amount of random numbers equal to the speech samples in each segment (Figs. 1, 2, and 3).

The random numbers generated by the chaotic generators are sorted in ascending order, and the corresponding indexes are taken from the sorted list. Based on the indexes of the random numbers, the sampled values of speech signals are permuted. The permuted parameters are substituted with the random numbers generated by corresponding chaotic generator.

The process of selection of chaotic generator for each level of sampled speech is carried out by chaotic switch keying technique. The method of chaotic switching represents the simplest form of modulation with chaotic attractors. The signal $u(t)$ controls the switch which toggles between the chaotic systems and different parameters $L_0$, $L_1$, $L_2$, and $L_3$. The encryption scheme consists of four chaotic subsystems:

i. Subsystem with the parameters $L_0$—active when $-1 \le u(t) < -0.5$
ii. Subsystem with the parameters $L_1$—active when $-0.5 \le u(t) < 0$
iii. Subsystem with the parameters $L_2$—active when $0 \le u(t) < 0.5$, and
iv. Subsystem with the parameters $L_3$—active when $0.5 \le u(t) \le 1$

Transmission of the chaotic attractor $A_0$, generated by the first chaotic circuit based on *logistic mapping* (with the parameters $L_0$), corresponds to the value $-1$ to $-0.5$. Transmission of the attractor $A_1$, generated by the second chaotic circuit based on *tent mapping* (with the parameters $L_1$), corresponds to the value $-1$ to $-0.5$. Transmission of the attractor $A_2$, generated by the third chaotic circuit based on *quadratic mapping* (with the parameters $L_2$), corresponds to the value 0.5 to 0.75. And transmission of the attractor $A_3$, generated by the second chaotic circuit based on Bernoulli's mapping (with the parameters $L_3$), corresponds to the value 0.75 to 1.

The entire system acts as a control which switches between the attractors $A_0$, $A_1$, $A_2$, and $A_3$. The receiver also consists of four chaotic subsystems which have to be identical and synchronized with the transmitter side. The first one is designed for demodulating the values between $-1$ and $-0.5$, the second one for the values between $-0.5$ and 0, the third one for values between 0 and 0.5, and the fourth one for the values between 0.5 and 1. The demodulation is carried out on the basis of decisions within a regular time interval. An effective demodulation of a particular value is possible only when the chaotic systems on the transmitter and the receiver sides are exactly synchronized. After sequence of permutation process, the entire speech samples are appended.

## 4 Chaotic switching and modulation

The method of chaotic switching represents the simplest form of modulation with chaotic attractors

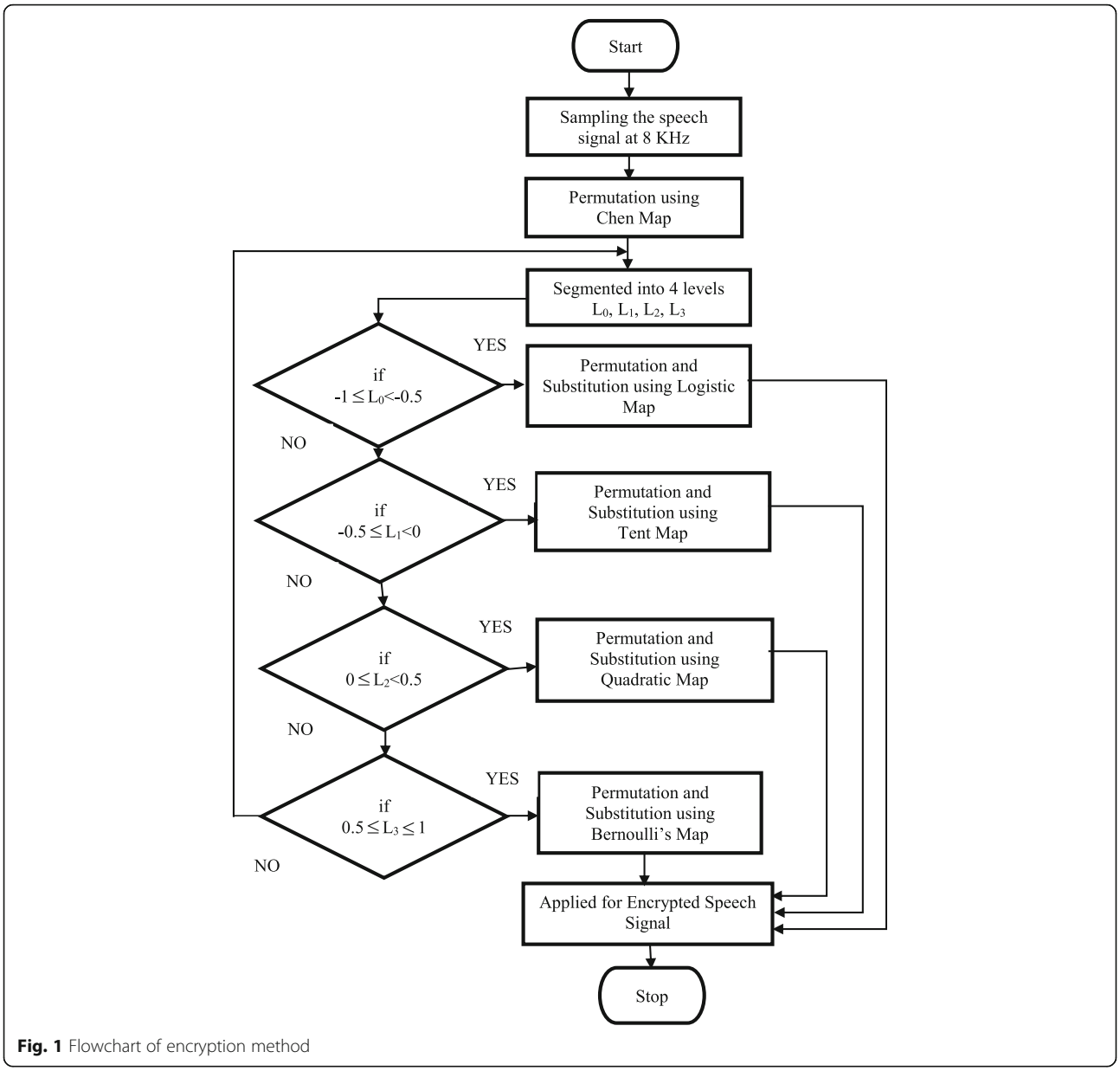


**Fig. 1** Flowchart of encryption method

[18–20]. It is suitable for deciphering digital signals. The essence of the chaotic modulation refers to modulation of the input signal $y(t)$ by a chaotic signal $u(t)$ generated by the chaotic signal generator. The signal $y(t)$ is modulated by the signal $u(t)$ in the chaotic modulator where multiplication occurs. The modulated signal $s(t)$ is transmitted over the communication channel to the receiver where in the chaotic demodulator, the demodulation or division of the modulated signal $s(t)$ with the chaotic signal $u(t)$ is carried out. The equality of the receiver's and the transmitter's parameters and their synchronization is a condition for successful demodulation

## 5 Results and discussion

The proposed system was tested in Matlab. This system was subjected to correlation test, SNR test, PSNR test, security analysis, randomness test, sensitivity test, histogram analysis, and robustness test which are carried out to prove the performance metrics [21]. Four sample speech signals are taken randomly from TIMIT database and are sampled at 8 kHz with length of 3 Sec to 8 Sec and 8000 samples per frame. The higher the chaos to signal ratio, the more secure the system is considered [22] so that five chaotic generators are used in this proposed system in which one is the primary and remaining four are secondary.

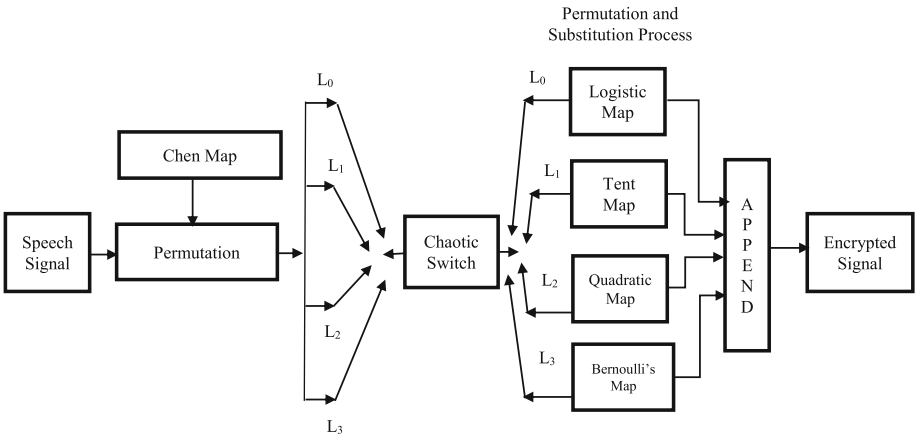


**Fig. 2** Block diagram of encryption method

Four samples are taken into account for SNR test and PSNR tests to measure the intelligibility of the speech and encrypted signal. The measuring tests are given below:

### 5.1 Correlation test

The auto-correlation function identifies the chaotic system that produces a strong encryption [23]. A useful measure to assess the encryption quality of any cryptosystem is correlation coefficient between similar segments in the clear signal and the cipher signal. It is calculated as:

$$r_{xk} = \frac{C(x,k)}{\sqrt{V(x)}\sqrt{V(k)}} \tag{6}$$

where $C(x, k)$ is the covariance between the original signal $x$ and the encrypted signal $k$. $V(x)$ and $V(k)$ are the variances of the signals $x$ and $k$. The variance $V(x)$ is computed as:

$$V(x) = \frac{1}{N_s}\sum_{i=1}^{N_s}(x(i)-E(x))^2 \tag{7}$$

$$E(x) = \frac{1}{N_s}\sum_{i=1}^{N_s}(x(i) \tag{8}$$

$$C(x,k) = \frac{1}{N_s}\sum_{i=1}^{N_s}(x(i)-E(x))(k(i)-E(k)) \tag{9}$$

where $N_s$ is the number of speech samples. The low value of the correlation coefficient $r_{xk}$ shows an encryption with good quality. The correlation coefficients for the three different encrypted speech samples with the chaotic maps are illustrated in Fig. 10, and the encrypted

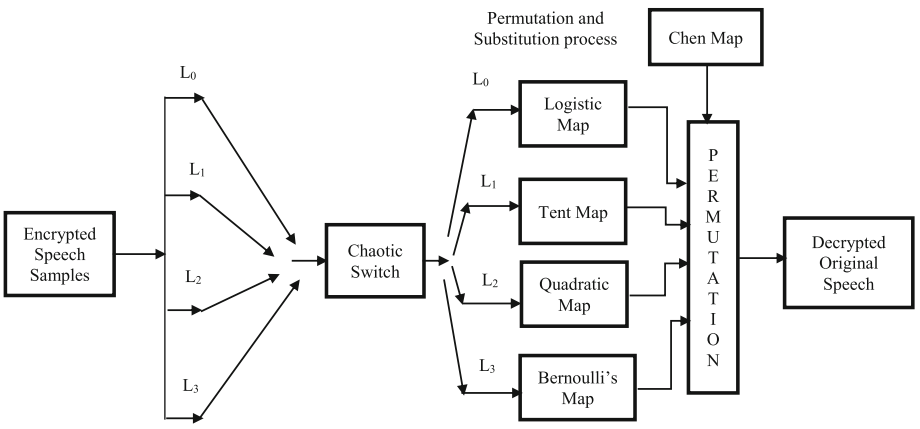


**Fig. 3** Block diagram of decryption method

speech signals with proposed method using five different chaotic random number generator are tabulated in Table 1. From these results, we infer that the proposed algorithm produces encrypted speech with low correlation between similar segments in the original speech and the encrypted speech.

In other words, the encryption method offers good encryption results. In this proposed method, we have obtained correlation coefficient as 0.998; it shows that the original speech signal has been permuted to the extent of almost 100% in decryption process so it is tough to the eavesdroppers to hack the speech signal in channel during transmission.

### 5.2 SNR test

Signal-to-noise ratio (SNR) test is an ideal estimator for measuring the speech signal intelligibility [23]. The popular time domain metric is the SNR, which is defined as the average of the SNR values of short segments of the output signal and is calculated as:

$$\mathrm{SNR} = 10\log_{10}\frac{\sum_{i=1}^{N_s} x^2(i)}{\sum_{i=1}^{N_s}\left(x(i)-y(i)\right)^2} \tag{10}$$

where $y(i)$ is decrypted speech signal. If the SNR is closer to zero, the higher is the quality of the decrypted signal. In this proposed method, we have obtained SNR value as $0.23 \times 10^{-14}$; it shows the original speech signal has been almost recovered in decryption process. A quality measure of the proposal algorithm for four speech signals is represented in Table 2.

### 5.3 PSNR test

Peak signal-to-noise ratio (PSNR) is the ratio between the maximum possible power of original speech signal and the power of encrypted signal [23]. PSNR is a calculation of encryption quality of the original signal. A higher PSNR indicates that the encryption or reconstruction is of higher quality. The PSNR is obtained from:

$$\mathrm{PSNR} = 10\log\frac{nx^2}{\|x-k\|^2} \tag{11}$$

**Table 1** Correlation test

| S.No | Speech sample | Encrypted speech | Decrypted speech |
|---|---|---|---|
| 1. | Audio1.wav | 0.0233 | 0.999 |
| 2. | Audio2.wav | 0.0384 | 0.999 |
| 3. | Audio3.wav | 0.0157 | 1 |
| 4. | Audio4.wav | 0.0119 | 1 |

**Table 2** SNR and PSNR tests

| S.No | Speech sample | Duration in seconds | SNR in dB | PSNR in dB |
|---|---|---|---|---|
| 1. | Audio1.wav | 7 | 33.7464 | 59.7989 |
| 2. | Audio2.wav | 8 | 32.5781 | 59.2281 |
| 3. | Audio3.wav | 5 | 33.0569 | 59.6304 |
| 4. | Audio4.wav | 3 | 34.7112 | 62. 3189 |

where $x$ is the maximum absolute square value of the original speech signal, $n$ is the length of encrypted signal, and $x - k$ is the energy of the difference between original and encrypted signals.

### 5.4 Security analysis

The sensitivity test is performed in view of security analysis to evaluate the protection of the proposed cryptosystem against various attacks [24]. To ensure the sensitivity of encrypted speech, the input speech signal is permuted for multiple levels using multiple chaotic maps to change the position of sampled values as the chaotic generators generate a voluminous random numbers. For testing the sensitivity of the proposed cryptosystem, the encrypted signal is decrypted with the reverse process of encryption method using the corresponding chaotic maps at the same four levels and resulting good quality speech recovered.

### 5.5 Histogram analysis

This test is applied to evaluate the immunity of the algorithm against differential attacks, and few speech samples are chosen randomly from TIMIT dataset. The histogram analysis has been taken account to prove the strength of our algorithm, and the results are shown in Figs. 4, 5, 6, 7, 8, 9, and 10. Histogram of input speech sample shown in Fig. 4 is very closer to the histogram of decrypted signal shown in Fig. 9. The encrypted speech signal shown in Fig. 8 is very strong and fully masked. Figure 5 shows the histogram of splitted speech signal into $L_0$, $L_1$, $L_2$, and $L_3$, and Fig. 6 shows the histogram of permutation and substitution of parameters $L_0$, $L_1$, $L_2$, and $L_3$ using four different chaotic generators. Figure 7 shows the histogram of reconstructed parameters $L_0$, $L_1$, $L_2$, and $L_3$. The result shown in Fig. 7 shows that the splitted signals $L_0$, $L_1$, $L_2$, and $L_3$ have been reconstructed perfectly.

### 5.6 Robustness test

The LSB of each speech sample is inverted and obtained a modified speech signal. Actual and modified speech signals are encrypted using the same key, and two ciphered speech signals are generated. These ciphered speech signals are then compared by the number of sample change rate (NSCR) and the unified average changing intensity (UACI) [25]. The NSCR is given by

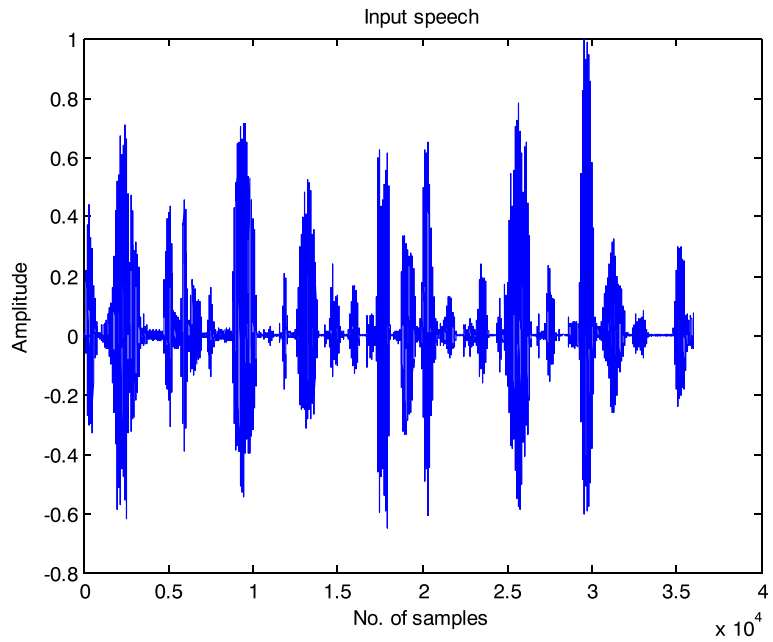


**Fig. 4** Histogram of input speech signal

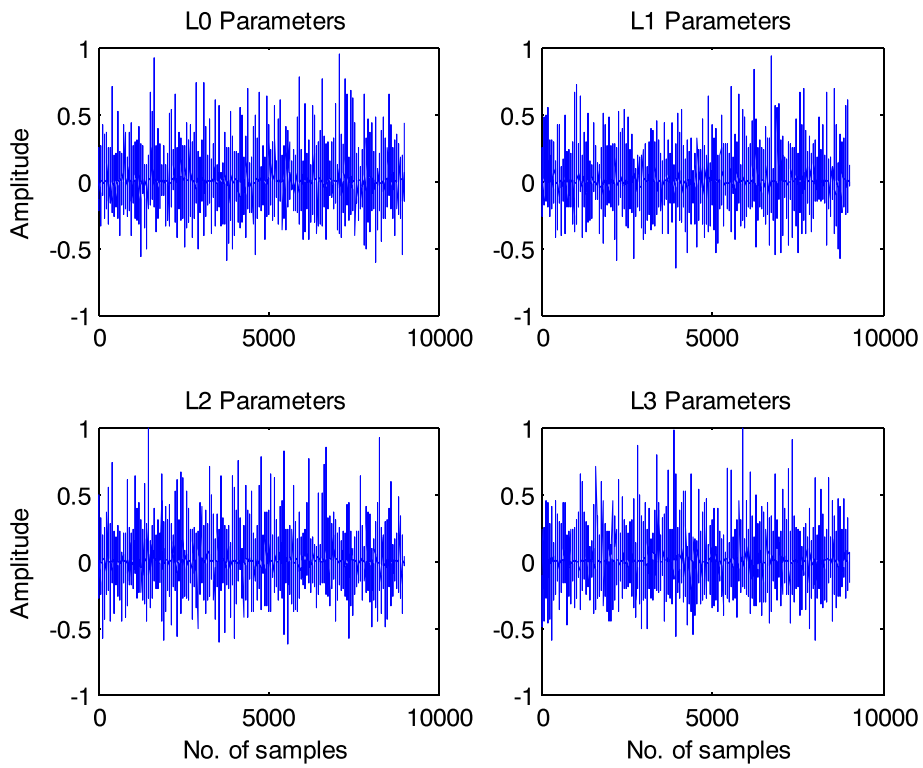


**Fig. 5** Histogram of splitted signals $L_0$, $L_1$, $L_2$, and $L_3$

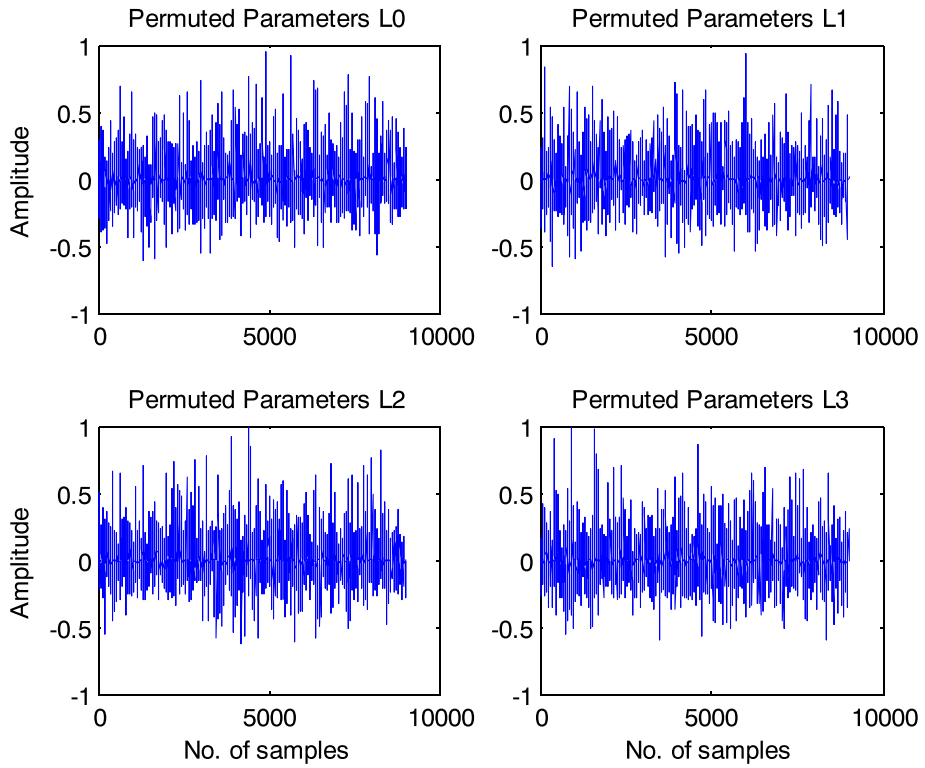


**Fig. 6** Histogram of permuted and substituted parameters $L_0$, $L_1$, $L_2$, and $L_3$

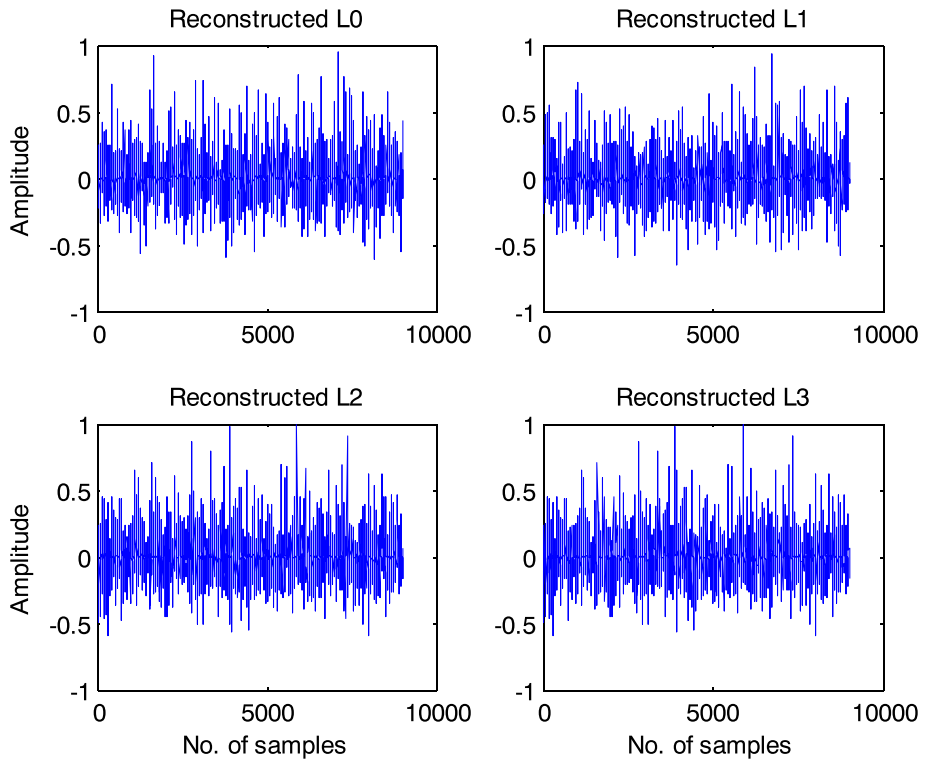


**Fig. 7** Histogram of reconstructed parameters $L_0$, $L_1$, $L_2$, and $L_3$

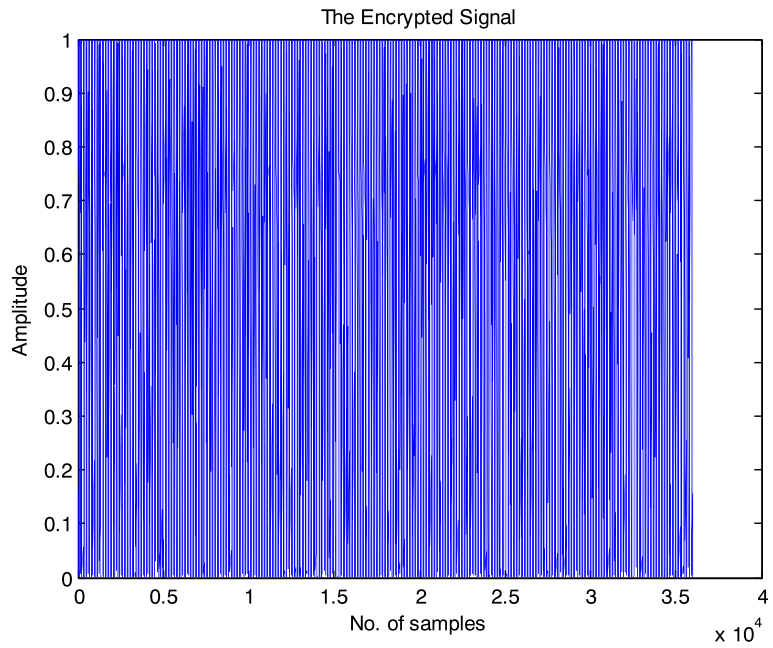


**Fig. 8** Histogram of encrypted speech signal

$$\mathrm{NSCR} = \sum_i \frac{d_i}{l} \times 100\% \tag{12}$$

and

$$\mathrm{UACI} = \frac{1}{l}\left[\frac{\sum_i x_i - x_i'}{65535}\right] \tag{13}$$

where

$$d_i = \begin{cases} 1, & x_i \neq x_i' \\ 0, & \text{Otherwise} \end{cases} \tag{14}$$

$x$ and $x'$ are the two ciphered speech signals whose corresponding original signals have only one-sample difference; the values of the samples at position $i$ of $x$ and $x'$ are respectively denoted by $x_i$ and $x_i'$; $l$ corresponds to the length of the speech vector. The ideal values for

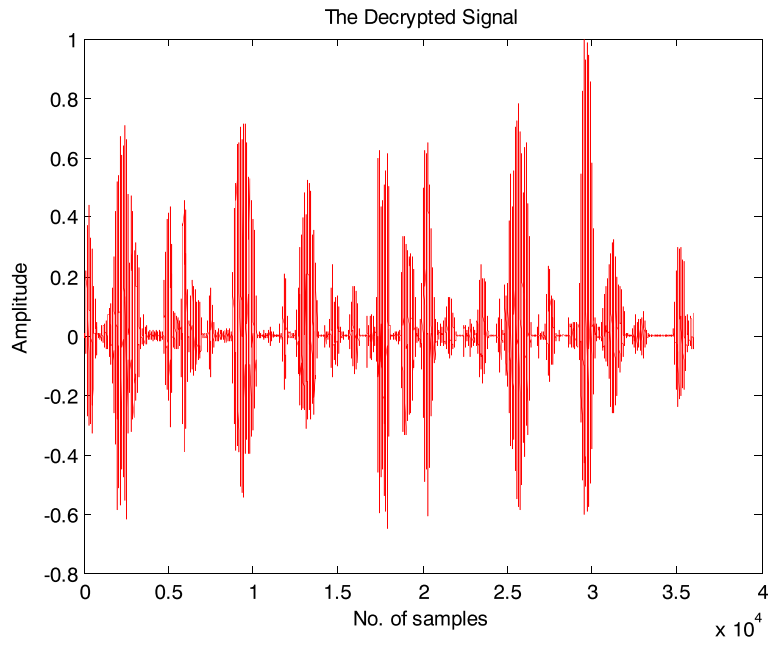


**Fig. 9** Histogram of decrypted speech signal

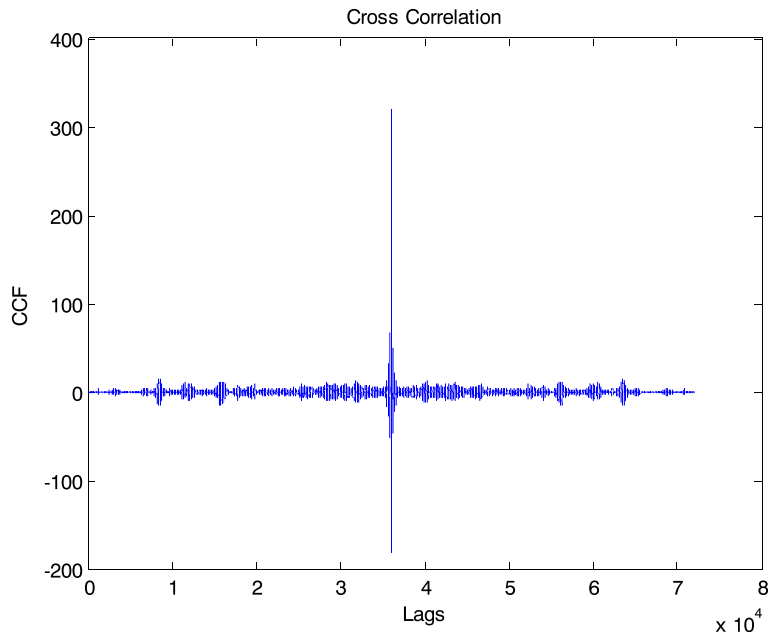


**Fig. 10** Correlation test

NSCR and UACI are 100% and 33.3%. In Table 3, the minimum, maximum, and average values of NSCR and UACI, computed from the encryption of four different modified versions of each speech signal are given. The results are considerably close to the ideal values and independent on the position of the modified sample as compared with [25].

## 6 Discussion and conclusions

Speech encryption using multiple chaotic generators and dynamic chaotic shift keying is a proven model. In this method, the four different speech signals with different time duration are sampled and its values are permuted using logistic map and further the permuted values are segmented into four levels. Each level is permuted using four different chaotic generators. Chaotic shift keying mechanism is dynamically assigning different chaotic maps to different levels of sampled values for shuffling the speech samples at every level. The histogram of the encrypted signal shows that more sensitivity entails more security. The decrypted signal is very similar to the original speech as it shows the stability of reconstruction of original signal. Correlation test, SNR test, and PSNR testing methods are applied to estimate the performance of the system. The result obtained by the proposed system is highly screened from attackers and has a powerful diffusion and confusion mechanism and better for real-time speech communication. It is verified that the proposed method has high level of security and can recover the original signals quickly with good audio quality. Robustness test has also been carried out by using NSCR and UACI to assess the withstanding capacity of the algorithm against various attacks. The results endorse that the speech signal is highly masked from eavesdroppers.

**Table 3** Robustness test analysis

| S.No | Speech file | Metric | Proposed system in % | | | Lima and Neto system [25] in % | | |
|---|---|---|---|---|---|---|---|---|
| | | | Max | Min | Avg. | Max | Min | Avg. |
| 1. | Audio1.wav | NSCR | 100 | 99.9982 | 99.9996 | 100 | 99.9967 | 99.9992 |
| | | UACI | 33.4161 | 33.1197 | 33.3066 | 33.4091 | 33.1850 | 33.2924 |
| 2. | Audio2.wav | NSCR | 100 | 99.9999 | 99.9999 | 100 | 99.9973 | 99.9992 |
| | | UACI | 33.3893 | 33.1520 | 33.2714 | 33.4743 | 33.1931 | 33.3012 |
| 3. | Audio3.wav | NSCR | 100 | 99.9998 | 99.9999 | 100 | 99.9961 | 99.9992 |
| | | UACI | 33.3990 | 33.1681 | 33.2683 | 33.4770 | 33.1858 | 33.3570 |
| 4. | Audio4.wav | NSCR | 100 | 99.9997 | 99.9998 | 100 | 99.9967 | 99.9993 |
| | | UACI | 33.4371 | 33.2192 | 33.3218 | 33.4367 | 33.2030 | 33.3196 |

**Authors' contributions**
PS and SR have equally contributed in proposing the ideas, discussing the results, and writing and proofreading the manuscript. The authors have implemented the algorithms and carried out the experiments. Both authors read and approved the final manuscript.

**Competing interests**
The authors declare that they have no competing interests.

## Publisher's Note



Received: 4 May 2017 Accepted: 30 August 2017
Published online: 07 September 2017

**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. Anoop(2007), Public key cryptography—applications algorithm and mathematical explanations.
3. Thongpon, T., & Sinchai, K. (2009). Accelerating asymmetric-key cryptography using parallel-key cryptographic algorithm. *6th International Conference on Computer and Information Technology, 2*, 812–815.
4. Ljupco Kocarev(2002), Chaos-based cryptography: a brief overview, IEEE Circuits and Systems Magazine, pp 7-21.
5. Azzaz, M. S., Tanougast, C., Sadoudi, S., & Bouridane, A. (2013). Synchronized hybrid chaotic generators: application to real-time wireless speech encryption. *Elsevier: Communications in Nonlinear Science Numerical Simulation, Volume, 18*, 2035–2047.
6. Yang, T., Wu, T. W., & Chua, L. O. (1997). Cryptography based on chaotic systems. *IEEE Transactions on Circuits and Systems I, 44*, 469–472.
7. Yang, T., & Chua, L. O. (1997). Impulsive stabilization for control and synchronization of chaotic systems: theory and application to secure communication. *IEEE Transactions on Circuits and Systems I, 44*, 976–988.
8. Osman Hilmi Koçal, Emrah Yürüklü, and ˙Ismail Avcıbas (2008), Chaotic-type features for speech steganalysis, IEEE Transactions on Information Forensics and Security, Volume 3, No. 4, pp 651-661.
9. Yang, T. (1999). Chaotic secure communication systems: history and new results. *Telecomm. Rev., 9*(4), 597–631.
10. 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.
11. Sheu, L. J. (2011). A speech encryption using fractional chaotic systems. *Nonlinear dynamics, 65*(1–2), 103–108.
12. Baker, H. J., & Piper, F. C. (1985). *Secure Speech Communications,* Academic Press Publisher.
13. Bianco M E, Reed D A (1991) Encryption system based on chaos theory, US Patent No. 5048086, USA, 1-12 http://www.google.co.in/patents/US5048086
14. 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.
15. Alzharaa Mostafa, Naglaa F Soliman, Mohamoud Abdalluh, Fathi E Abd El-samie (2016), Speech encryption using two dimensional chaotic maps, IEEE Xplore, 11th International Conference on Computer Engineering (ICENCO), Feb 2016.
16. 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.
17. 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.
18. 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.
19. 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.
20. Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and Chaos, 8*(6), 1259–1284.
21. Kocarev, L., & Lian, S. (2011). *Chaos-Based Cryptography Theory, Algorithms and Applications,* Springer-Verlag Publisher
22. Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal on Bifurcation Chaos, A, 44*, 2129–2151.
23. Matej Salamon (2012), Chaotic Electronic Circuits in Cryptography, From the book Applied Cryptography and Network Security, InTech.
24. Li, K., Soh, Y. C., & Li, Z. G. (2013). Chaotic cryptosystem with high sensitivity to parameter mismatch. *IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications, 50*(4), 579–583Publisher 13, pp 295-317.
25. Lima, J. B., & da Silva Neto, E. F. (2016). Audio encryption based on the cosine number transform. *Springer Multimedia Tool Applications, 75*, 8403–8848.