# Speech Encryption Technique using S - box based on Multi Chaotic Maps

Sarah Mohammed Abdullah, Iman Qays Abduljaleel

*Department of Computer Science, University of Basrah, Basrah, Iraq*

***Abstract* – This paper proposes the establishment of a secure encryption system for data transmission that includes three stages: first stage is a scrambling stage that is divided into scrambling of different sizes blocks and scrambling bits, the second stage is the use of DNA code to flip the bits and the third stage is the encryption using the Substitution box by 256 keys. The scheme is analysed using a variety of metrics. The findings demonstrate that the proposed system is significantly more reliable and robust against various forms of attacks than several recent related speech signal encryption systems.**

***Keywords* – speech encryption, scrambling, S-box, multi chaotic, DNA.**

## 1. Introduction

The data encryption process is one of the most important requirements of the data transfer process through open and shared networks due to the unauthorized connection that this data may be exposed and different types of attacks. The general target of encryption is to keep data from being taken, lost, annihilated by an aggressor, adjusted, or in any case found by unintended beneficiaries.

Speech signal encryption is one of the most important data encryption processes because of the large number of applications used to transmit speech signal because speech signal is the most common means of communication. Conventional encryption systems such as DES, AES [1], cannot be used for audio data encryption since they take a long time and use significant resources. A major problem for researchers in the area of computer technology is how to implement modern sound encryption systems with top-class security and pace is becoming more popular. Researchers have proposed a large number of ways to encode speech signal such as: [2](Khaleel & Abduljaleel, 2021) propose the process Keys which is produced using quantum map and k-means. There are two forms of scrambling used: the first using the (BiRS algorithm) and the second the K-Means algorithm (block representation scrambling BIRS). While [3](Mohamed, Korany, & El-Khamy, 2021) used four S-Boxes (CFI). The core element of the generation of CFI boxes consists of two elements: an external key and hidden picture. These codes were then encrypted using DNA techniques, where the rules for encoding are variable and governed by hidden keys. These four S-boxes are referred to as DNAFZ S-boxes. In [4] (Sinha, Asha, San, & Sahu, 2018), new approach for transmitting stable data is proposed that includes confusion and diffusion. The proposed algorithm uses the Arnold Cat map to generate the blurred picture. S-box and XOR transformation are employed to provide diffusion and the encryption method requires the use of 128-bit random keys that are replaced with the values in the s-box. The final key is then obtained by moving and mixing in the substituted values. To obtain the final encrypted image, the XORed key is used. There has been an encryption and decryption algorithm written in Lorenz-chaotic registers, which is used in addition to the Lorenz generator and S-box. In [5], (Fadhil, Farhan, & Fadhil, 2021) build an S-Box built on a messy 1D logistic map. The chaotic sequence produced from the 1D logistic map was used to produce hexa code values, which were then used to create the new good S-Box.

DOI: 10.18421/TEM103-54
https://doi.org/10.18421/TEM103-54

**Corresponding author:** Iman Qays Abduljaleel,
*Department of Computer Science,*
*University of Basrah*, Iraq
**Email:** iman.abduljaleel@uobasrah.edu.iq

*Received: 23 April 2021.*
*Revised: 07 August 2021.*
*Accepted: 13 August 2021.*
*Published: 27 August 2021.*

In this paper, an algorithm is proposed for encryption of speech signal using scramble, DNA coding, and substitution boxes in which it is constructed by means of chaotic maps.

## 2. Methodology

This paper utilized a variety of methods and techniques combined to achieve favorable results. Below is an explanation of the basic concepts of these methods and techniques.

### *2.1. Scramble Stage*

Speech scrambling is a technique for transforming speech data to an unintelligible format. [19]

Two methods are used in the scrambling, the first is based on scrambling different sized blocks, and the second by scrambling the bits. Set of Scramble steps are applied as Algorithm1 illustrates:

***Algorithm 1: steps of scramble***

1. Receive speech signal samples from the source.
2. Loop divides the speech signal into blocks of different sizes 256 and 128 samples to length of speech signal.
3. Sorting blocks into matrices according to length to produce two matrices, the first with a length of 256 samples and the other 128 samples.
4. Divide the matrices into two parts, left and right.
5. Rotate the right side so that the row is a column and the column is a row.
6. Apply a chess board to left part.
7. Merging the two matrices into one matrix vertically.
8. Convert the two matrices into a vector and combine them.
9. Convert float to binary.
10. Apply scrambling bits using Fibonacci series by replacing the location of the bits.
11. Convert binary to float.

### *2.2. DNA Encoding*

DNA is an acronym for deoxyribonucleic acid. It is a nucleic acid that contains the genetic material of living organisms. It contains four distinct nucleotide bases: adenine (A), thymine (T), cytosine (C), and guanine (G), where C and G and T and A are complementary pairs. When four bases A, T, C, and G are encoded as 00,11,10,01, we receive 24 distinct encoding schemes. Due to the complementary nature of DNA bases, there are eight distinct categories of coding classes that adhere to the complementary law, as shown in Table 1. Permutations and variations of bases may be used to store and measure data, thus encrypting it [6]. If the second rule in Table 1. is selected, the 8-bit binary "00110110" number can be expressed as "ATCG", if the fourth rule is chosen , then the 8-bit of the binary number "00110110" can be expressed as "CGTA" [7]. In this paper, we use the second rule to encode 8 bits of speech signal as shown in Table 1 , Rule 2= 00-A 01-G 10- C 11-T.

*Table 1. DNA Encoding rules*

| Rule1 | Rule2 | Rule3 | Rule4 | Rule5 | Rule6 | Rule7 | Rule8 |
|---|---|---|---|---|---|---|---|
| **00-A** | **00-A** | **00-C** | **00-C** | **00-G** | **00-G** | **00-T** | **00-T** |
| **01-C** | **01-G** | **01-A** | **01-T** | **01-A** | **01-T** | **01-C** | **01-G** |
| **10-G** | **10-C** | **10-T** | **10-A** | **10-T** | **10-A** | **10-G** | **10-C** |
| **11-T** | **11-T** | **11-G** | **11-G** | **11-C** | **11-C** | **11-A** | **11-A** |

Steps of encryption by DNA are applied as Algorithm 2 illustrates:

***Algorithm 2: DNA Encoding***

1. Convert the vector obtained from the previous step into a binary representation.
2. Using the second base to encode and flip 8 bits
3. Convert the resulting series to decimal representation.

### *2.3. Chaotic Maps*

A chaotic map definition is one that exhibits chaotic behavior. A discrete-time or continuous-time parameter may be used to parameterize maps. More often than not, discrete maps look like function-iterated maps. Dynamical structures are chaotic maps [8], [18].

#### a. Quadratic map

A form of chaotic structure that's commonly used as one that is non-linear is the quadratic map. Following is the equation's description [14]:

$$A(n)= \Upsilon +(1-A(n-1))^2 \qquad (1)$$

Where n is the number of iterations and r is the additive element of chaos, When $\Upsilon \in[0,2]$ , $A \in[0,1]$ in which the chaotic is realized when $\Upsilon \in[1.5,2]$. [8]

#### b. Logistic map

The logistics map is one of the renowned chaotic maps commonly. The logistic map can be forging as:

$$A(n)= ɱ X(n)*(1- A(n)) \qquad (2)$$

Where A(n) and ɱ are the state value and control variables. The logistics map has a chaotic behavior for $3.57\leq ɱ \leq4$ and $0.5< X (0) <1$. And a bifurcation process when the control variables ɱ is in time 4. [9].

#### c. Extended logistic map

The logistic map (2) can be extended in two dimensions using the system of equations (3)[3]:

$$A(n+1)= ɱ1*A(n)*(1-A(n))+\Upsilon1*B(n)^2 \qquad (3)$$

$$B(n+1)=ɱ2*B(n)*(1-B(n))+\Upsilon2*(A(n)^2+A(n)*B(n)) \quad (4)$$

This map presents a chaotic behavior in the state where variables: 2.75<ϻ1<3.4 , 2.7<ϻ2<3.45, 0.15<ϒ1<0.21 and 0.13< ϒ 2<0.15. Where A (0) and B (0) are in the range [0,1].[15].

### d. Lorenz map

Lorenz maps for a complex three-dimensional and non-repetitive. The Lorenz equations describe [16]:

Aφ(n)= ծ*(Bφ (n-1)-Aφ (n-1)) (5)
Bφ (n)= ϒ *Aφ (n-1)-Bφ (n-1)-Aφ (n-1)*Cφ (n-1) (6)
Cφ (n)=Aφ (n-1)*Bφ (n-1)+b*Cφ (n-1) (7)

The values of ծ, r, b, and their locations in a disorderly environment are dependent on ϒ when ծ is greater than or equal to 10, the map behaves unexpectedly. Aφ, Bφ, and Aφ act as the diffusion keys Strong outcome for a Lorenz chaos map with ծ = 28, ϒ = 8/3, and initial values Aφ = 10, Bφ = 20, and Cφ = 30 [10].

### *2.4. Substitution Box*

The Substitution Box (S-Box) is critical in block ciphers; it creates inconsistency between the initial and encrypted speech signals.[17] As a result, several researchers have attempted to develop a strong S-Box that can be used in the substitution phase and substitutes the standard S-Box to provide a high degree of security [5].

This paper introduces a new approach that causes inconsistency in block ciphers. Due to the great co-dependency of chaos theory and ciphers, we have to use three main replacement chaotic maps in order to construct a new substitution box, this method will provide 256 keys that are used in the encryption. The steps in algorithm 3 steps illustrate the idea of building Substitution Box.

***Algorithm 3: Building Substitution Box***

1. Create an empty matrix
2. Loop the equation (1) of Quadratic Map until get 64 elements
3. Loop the equation (2) and (3) of Extended Logistic Map until get 128 elements in matrix
4. Loop the equation (4),(5), and (6) of Lorenz Map until get 192 elements in matrix
5. Loop the equation of Lorenz Map until get 256 elements in matrix.

In this proposal, the Substitution Box generated as follow: generate the first quarter of the Substitution Box from 1D Quadratic map and generate the second quarter of the Substitution Box from 2D Extended Logistic map, while the last section is built by applying Lorenz map three-dimensional twice, so we get a hybrid Substitution Box of three chaotic maps, Algorithm 4 illustrates the process of using 256 keys to encode a speech signal sample.

***Algorithm 4: Encryption with Substitution Box***

1. Convert the resulting mass from the previous step into binary representation and save it into block.
2. Extract 8 bits from the block.
3. Convert the extracted bits above to decimal representation.
4. Access to the value to be used in the replacement in the S-Box through the value index.
5. Convert to binary representation, extract 8-bit and retrieve at the cut location of the chain.
6. Convert the string to decimal representation for getting an encryption speech.

***Decryption Algorithm of the Speech Signal samples:***

The inverse S-Box will be used during the decryption procedure to retrieve the original data; algorithm 5 illustrates the method of creating the inverse for the current S-Box.[5].

***Algorithm 5: Building Inverse Substitution Box***

1. Input all of the numbers from the S-Box into a loop.
2. The digits' addresses are retrieved and used to reflect the new value to be placed in the inverse S-Box.
3. Repeated until inverse S-Box is filled.

In algorithm 6 are illustrated the steps of Decryption by inverse Substitution Box

***Algorithm6: Decryption by inverse Substitution Box***

1. Convert the encryption speech signal to binary representation.
2. Subtract 8 bits from the binary chain.
3. Converted the subtraction bits above to decimal representation.
4. Access to the index by means of the resulting value of the inverse Substitution Box.
5. Convert the value into binary representation and you will replace it with the cut-out string.
6. Convert string to decimal representation.

In algorithm 7 are illustrated the steps of Decryption DNA Encoding.

***Algorithm 7: Decryption DNA Encoding***

1. Convert the resulting mass from the previous step into binary representation.
2. Use the fourth rule to decrypt.
3. Decimal conversion.

In algorithm 8 are illustrated the steps of Decryption of Scramble and restore the original speech signal.

***Algorithm 8: Decryption of Scramble***

1. Convert decimal to binary, apply descrambling bits using Fibonacci series by replacing the location of the bits.
2. Divide the resulting vector into two parts. Convert the vector into matrix.
3. Divide the matrix into two matrixes crosswise.
4. Chessboard application to restore the left part.
5. Rotate the right so that the row is column vice versa.
6. Merge the two matrices.
7. Combine blocks of length 128 samples and 256 samples.
8. Restore the original speech signal.

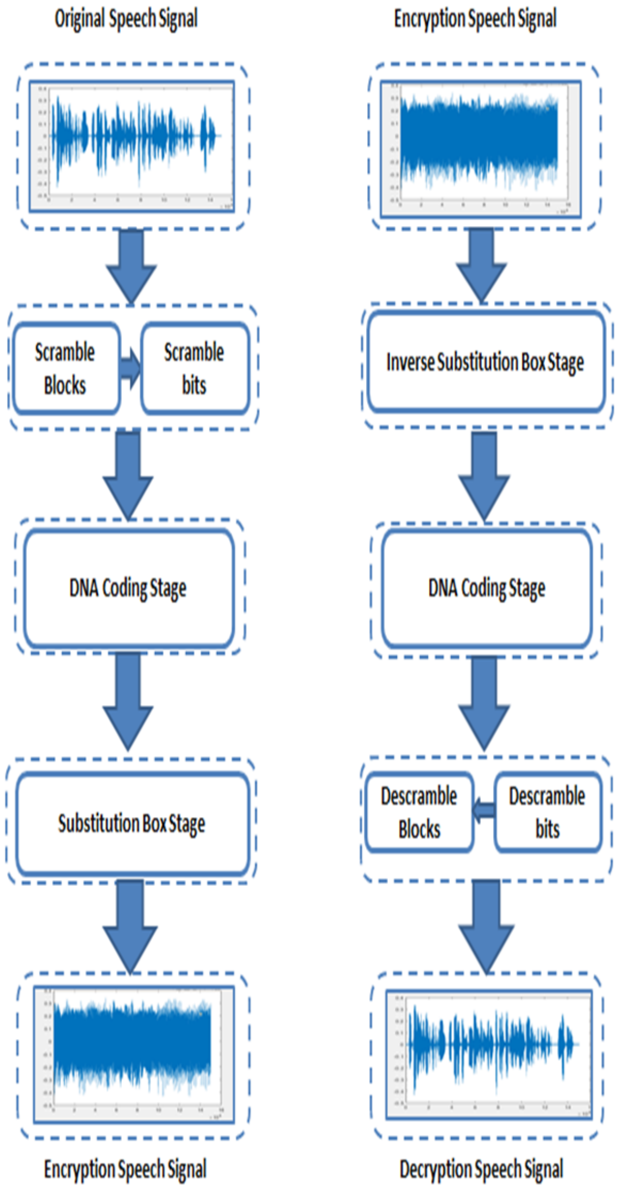

*Figure 1. Illustrates the proposed speech signal encryption scheme's encryption and decryption phases schematically*

## 3. Result and Discussions

The laptop used is Intel(R) Core TM i7-3540M processor running at 3.00 GHz, 4.00 GB of RAM, and 64-bit Windows 10. The proposed scheme is applied to a variety of speech samples of varying sizes, type wav. Kaggle sound library is a corpus of approximately 100 hours read English clean speech, and many tests were conducted to evaluate the proposed algorithm's accuracy used MATLAB R2020a software. The findings are shown in Figure 2.

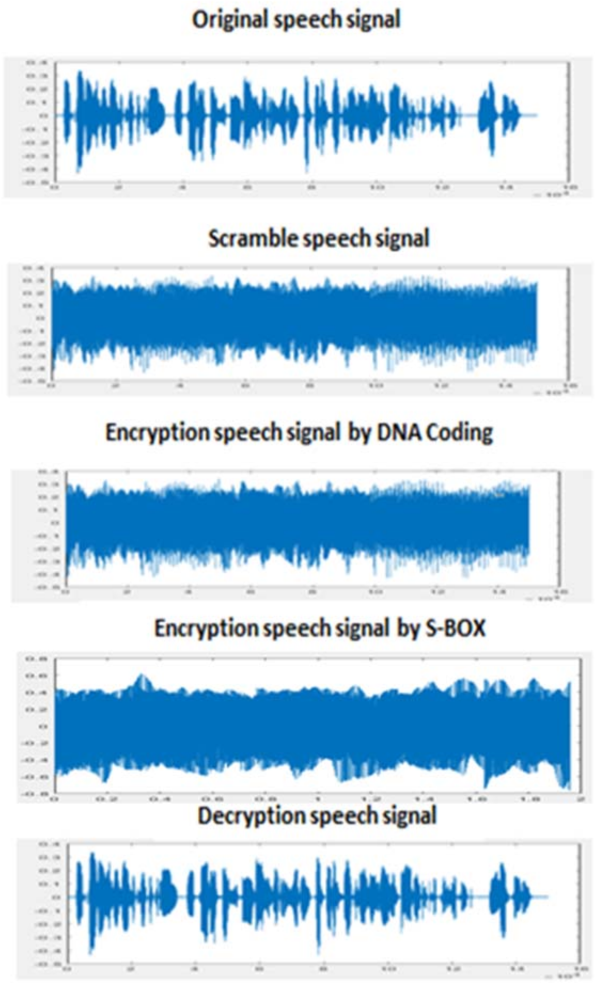

*Figure 2. Simulation results*

The scheme transforms the initial speech signal into an encrypted speech signal that resembles noise. The process of scrambling was on multiple levels, and this confused a kind of difficulty in retrieving data. Our simple opinion is that the scrambling was the first line of defense against any attacks and it was very difficult to penetrate because it gradient from the highest level to the bit level.

## 4. Security Analysis

A secure speech encryption scheme must be resistant to all known types of attacks. The proposed scheme's defense can be evaluated using a variety of metrics, including the Correlation Coefficient Analysis, the Signal to Noise Ratio, the Log-Likelihood Ratio, and the Segmental Signal to Noise Ratio. Table 2. shows the security analysis of the proposed algorithm using the measures.

*Table 2. Speech signal samples*

| Speech signal | length | SNR | segSNR | correlation | LLR |
|---|---|---|---|---|---|
| Speech1 | 2 | -22.8483 | -24.6104 | -0.0037 | 3.3931 |
| Speech2 | 3 | -20.8834 | -23.5071 | -0.0028 | 3.1841 |
| Speech3 | 4 | -23.0296 | -26.4107 | -0.0029 | 2.8841 |
| Speech4 | 7 | -20.6945 | -24.5492 | -7.7788 | 4.5179 |
| Speech5 | 10 | -21.6945 | -26.5339 | -9.5342 | 4.5510 |

### 4.1. *Correlation Coefficient Analysis (CC)*

It can be used to test the power of encryption against different kinds of statistical attacks On the whole, it verifies the relationship between the initial samples of speech signal segments and the encrypted samples of speech signal. A strong encryption algorithm would convert the speech file to an unpredictable signal with a low correlation factor. It can be measured as [20]:

$$\mathrm{r}_{xy} = \frac{cov(x,y)}{\sigma^x\sigma^y} = \frac{\frac{1}{n}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\frac{1}{N_s}\sum_{i=1}^{N_s}(x_i - E(x))^2}\sqrt{\frac{1}{n}\sum_{i=1}^{N}(y_i - E(y))^2}}$$

and $\sigma_{x1,}\sigma_y=0$ (8)

### 4.2. *Signal to Noise Ratio (SNR)*

A metric is used to determine the signal's efficiency. As bigger t values exceed 0 dB, the signal exceeds the noise. Given a speech signal that is both encrypted and unencrypted, it can be measured as [7]:

$$SNR = 10 * log_{10}\frac{\sum_{i=1}^{N_s} x_i^2}{\sum_{i=1}^{N_s}(x_i - y_i)^2} \quad (9)$$

### 4.3. *Log-Likelihood Ratio (LLR):*

A distance calculation that can be determined directly from the original LPC vector for encrypted and unencrypted, it can be measured as [10]:

$$d_{LLR(a_d,a_c)} = log\left|\frac{a_c, R_d\, a_c^T}{a_d, R_d\, a_d^T}\right| \quad (10)$$

### 4.4. *Segmental Signal-to-Noise-Ratio (segSNR)*

The lower the segSNR amount, the more noise there is in the encrypted signal, rendering it more strength to attack.

Where S is the number of samples in a block and Nblocks is the number of blocks in a speech signal with a length of (L=SNblocks) [12].

$$segSNR. = \frac{10}{N_{\text{blocks}}}\sum_{i=1}^{N_{\text{blocks}}} log10\, \frac{\sum_{i=SN_{\text{blocks}}}^{SN_{\text{blocks}}+S-1} x^2(i)}{\sum_{i=SN_{\text{blocks}}}^{SN_{\text{blocks}}+S-1}[x(i)-y(i)]^2}$$

(11)

## 5. Comparative Study

This portion would assess the suggested scheme's strengths in comparison to other schemes. The most often used protection metrics, such as Signal to Noise Ratio (SNR), Segmental Signal-to-Noise-Ratio (segSNR), Log-Likelihood Ratio (LLR), and Correlation Coefficient (CC). As a consequence, the correlation coefficient between the original speech signal and its encrypted equivalent is found to be the lowest in the proposed scheme, indicating the least resemblance and since the suggested scheme has the lowest SNR and segSNR values, as a result, it is the most resistant to differential threats. Table 3. illustrates comparison to other schemes.

*Table 3. Comparison*

| | Length | SNR | segSNR | Correlation | LLR |
|---|---|---|---|---|---|
| Ref.[1] | 4 | - | -17.7001 | -0.011300 | 2.9136 |
| Ref[11] | 4 | -12.1727 | | 0.03709 | 3.9031 |
| Ref[13] | 4 | 244.7936 | 135.2033 | 0.9981 | - |
| Proposed scheme | 4 | -23.0296 | -26.4107 | -0.0029 | 2.8841 |

## 6. Conclusion

The suggested scheme is a reliable method of transmitting speech. The scheme include three stages. The first stage is to scramble the speech signal by dividing the speech signal into blocks of different sizes 256 samples and 128 samples and sorting blocks into matrices according to the length to produce two matrices, after that divide each matrix according to its size into two parts, left and right and rotate only the right side so that the row is a column The column is a row while on the other side a chessboard is applied. That effectively eliminates the high similarity between adjacent speech signal samples. The second stage is DNA encoding of the scrambled speech signal by using a second rule to get an encryption speech signal. The third stage consists of an encryption with a Substitution Box that consists of multi chaotic maps. The scheme is analyzed using a variety of metrics, including the Signal to Noise Ratio (SNR), Segmental Signal-to-Noise-Ratio (segSNR), Log-Likelihood Ratio (LLR), and Correlation Coefficient (CC). The findings demonstrate that the proposed system is significantly more reliable and robust against various forms of attacks than several recent related speech signal encryption systems.

## References

[1]. Al Saad, S. N., & Hato, E. (2014). A speech encryption based on chaotic maps. *International Journal of Computer Applications*, *93*(4), 19-28.

[2]. Khaleel, A. H., & Abduljaleel, I. Q. (2021). A novel technique for speech encryption based on k-means clustering and quantum chaotic map. *Bulletin of Electrical Engineering and Informatics*, *10*(1), 160-170.

[3]. Mohamed, A. G., Korany, N. O., & El-Khamy, S. E. (2021). New DNA coded fuzzy based (DNAFZ) S-boxes: Application to robust image encryption using hyper chaotic maps. *IEEE Access*, *9*, 14284-14305.

[4]. Sinha, R. K., Asha, B., San, N., & Sahu, S. S. (2018, July). Chaotic Image Encryption Scheme Based on S-Box Substitution. In *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 664-669). IEEE.

[5]. Fadhil, M. S., Farhan, A. K., & Fadhil, M. N. (2021, February). Designing Substitution Box Based on the 1D Logistic Map Chaotic System. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1076, No. 1, p. 012041). IOP Publishing.

[6]. Sheela, S. J., Suresh, K. V., & Tandur, D. (2017). A novel audio cryptosystem using chaotic maps and DNA encoding. *Journal of Computer Networks and Communications*, *2017*.

[7]. Abdelfatah, R. I. (2020). Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic DNA computations. *IEEE Access*, *8*, 69894-69907.

[8]. Mokhtar, M. A., Sadek, N. M., & Mohamed, A. G. (2017, March). Design of image encryption algorithm based on different chaotic mapping. In *2017 34th National Radio Science Conference (NRSC)* (pp. 197-204). IEEE.

[9]. Essaid, M., Akharraz, I., Saaidi, A., & Mouhib, A. (2019, April). A novel image encryption scheme based on permutation/diffusion process using an improved 2D chaotic system. In *2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)* (pp. 1-6). IEEE.

[10]. Zaid, O. M. A. ( 2020 ). Voice Scrambling Algorithm based on 3D Chaotic Map System (VSA3DCS) to Encrypt Audio Files (IJACSA). *International Journal of Advanced Computer Science and Applications, 11*(5).

[11]. Hato, E., & Shihab, D. (2015). Lorenz and rossler chaotic system for speech signal encryption. *International Journal of Computer Applications*, *128*(11), 25-33.

[12]. Wahab, H. B. A., & Mahdi, S. I. (2015). Modify speech cryptosystem based on shuffling overlapping blocks technique. *International Journal of Emerging Trends & Technology in Computer Science*, *4*(2), 70-75.

[13]. Abduljaleel, I. Q., & Khaleel, A. H. (2020). Hiding text in speech signal using K-means, LSB techniques and chaotic maps. *International Journal of Electrical & Computer Engineering (2088-8708)*, *10*(6).

[14]. Ramadan, N., Ahmed, H. E. H., Elkhamy, S. E., & El-Samie, F. E. A. (2016). Chaos-based image encryption using an improved quadratic chaotic map. *American Journal of Signal Processing*, *6*(1), 1-13. doi:DOI: 10.5923/j.ajsp.20160601.01

[15]. Albhrany, E. A., Jalil, L. F., & Saleh, H. H. (2016). New Text Encryption Algorithm Based on Block Cipher and Chaotic Maps. *Int. J. Sci. Res. Sci. Eng. Technol.(IJSRSET)*, *2*, 67-73.

[16]. Sathiyamurthi, P., & Ramakrishnan, S. (2020). Speech encryption algorithm using FFT and 3D-Lorenz–logistic chaotic map. Multimedia Tools & Applications, 79.

[17]. Yassin, H. M., Mohamed, A. T., Abdel-Gawad, A. H., Tolba, M. F., Saleh, H. I., Madian, A. H., & Radwan, A. G. (2019, July). Speech encryption on FPGA using a chaotic generator and S-Box table. In *2019 Fourth International Conference on Advances in Computational Tools for Engineering Applications (ACTEA)* (pp. 1-4). IEEE.

[18]. Hameed, Y., & Ali, N. (2018). An efficient audio encryption based on chaotic logistic map with 3D matrix. *Journal of Theoretical and Applied Information Technology*, *96*(16), pp5142-5152.

[19]. Abbas, N. A., & Razaq, Z. H. (2019). Review of dct and chaotic maps in speech scrambling. *Journal of Theoretical and Applied Information Technology*, *97*(2), 569-582.

[20]. Wang, X., & Su, Y. (2019). An audio encryption algorithm based on DNA coding and chaotic system. *IEEE Access*, *8*, 9260-9270.