INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2025, VOL. 71, NO. 1, PP. 69-78
Manuscript received March 05, 2024; revised March 2025. doi: 10.24425/ijet.2025.153546

Speech signal security scheme based on multiple chaotic maps with deoxyribonucleic acid coding algorithm

Sura F. Yousif, and Hussein A. Abdulkadhim

Abstract—**This article presents a novel speech cryptosystem by using chaotic maps and Deoxyribonucleic Acid coding. Initially, the speech signal is divided into four equal blocks. Then the speech samples in each block are submitted to confusion/diffusion via four different chaotic maps. The gained ciphered speech samples and the obtained chaotic sequence from Sine map are encoded via DNA rules. The consequent coded sequences from the previous step are merged via DNA/XNOR to get the coded DNA signal. Ultimately, the resulted signal is decoded to acquire the definitive ciphered signal. The experiments prove the efficiency and robustness of the suggested method.**

Keywords—**communication; speech security; chaotic maps; DNA coding; security analysis**

I. Introduction

VOICE communication considers an important part in various applications such as teleconferencing, e-banking, e-learning, military sectors, corporate etc. The main concern in these applications is to provide data integrity, confidentiality, authentication and right delivery of the transferred speech signals to the concerned party [1]. Cryptography represents the key to protect the speech signal content during the transmission from destruction or unauthorized access. The speech data is converted from its intelligible form to ambiguous one through encryption at the sender's end and the inverse process is used to retrieve the original data through decryption at the recipient's end [1]. Generally, cryptography techniques can be classified broadly into two types: symmetric and asymmetric. In the symmetric cryptography, one key is utilized in the encryption as well as for the decryption, while in the asymmetric cryptography; two different keys (public & private) are employed for the encrypting and decrypting operations. These two popular cryptographic techniques are relying on computational complexity theory and algebraic notations. Application of the symmetric techniques such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) for speech encryption can achieve a high security level, but due to their small key space, they are vulnerable to the attacks [1], [2]. Also, because of the bandwidth expansibility of the ciphered speech signal, degradation in the performance of signal to noise ratio and high redundancy level between speech samples, these algorithms are rarely utilized in the speech encryption systems [3]. Furthermore, these schemes demand a long computation time and high calculation power due to the complicated shuffling process for a small part of data. Additionally, the asymmetric methods are not appropriate for the speech encryption because of their complexity and low rapidity [2]-[4]. Thus, it is requisite to seek about simple and fast speech ciphering schemes that can provide high security level whilst keeping recovered speech signal with perfect audio quality.

In the other side, many researchers in this regard have noticed the possibility of implementing the disordered behaviour of chaos theory in cryptography. Chaotic techniques are generally relying on chaos or large numbers derived from dynamic nonlinear field. Chaotic systems have prominent properties such as mixing, non-periodicity, pseudo-randomness, topological transitivity and high sensitiveness to the control parameters/initial conditions. Moreover, these systems provide the prerequisite speed, security and complexity. All these features meet the cryptography requirements such as avalanche, balance, and confusion/diffusion properties. Therefore, chaos encryption algorithms have become the focus of attention in many fields due to their enormous benefits [5]-[8]. However, applying the chaotic systems only for speech ciphering approaches is not securing enough; which necessitates the use of new technology in order to improve the speech security. DNA technology is one of the approaches that introduced so as to increase the chaos speech security. This algorithm can be applied in cryptography field for carrying and storing data as well as for computation. The DNA is implemented in the speech coding for adding more security and rapidity to other encryption methods because of its exclusive features like massive data storage, ultra-low power consuming and enormous parallelism [5]-[9].

Several methods have been introduced recently for the speech signals security. For instance, the authors in [10] applied 2D Baker map for permutation/substitution of the speech samples in time and transform domains, while in [11], Circle and Logistic maps are exploited to achieve the confusion/diffusion structure to encrypt the speech signal segments. Authors in [12] encipher the speech signals by adopting Logistic and Arnold cat maps to perform the permutation/substitution principle. An encryption technique is suggested in [13] based on the combination of optical encryption and chaotic maps for ciphering the audio files. In

Sura F. Yousif and Hussein A. Abdulkadhim are with University of Diyala, College of Engineering (e-mail: sura.fahmy@yahoo.com, hussein73@mail.ru).

[14], a voice ciphering scheme is described that relies upon Arnold and Henon maps to execute the samples permutation/ substitution. A combined method is presented in [5] to encrypt/decrypt the audio information via hybrid chaotic shift transform (HCST), chaotic maps and DNA coding technique. The original signal is divided into four layers in [6]. Then, Logistic, Tent, Quadratic and Bernoulli's maps are utilized so as to realize the permutation stage on these layers. Multiple ciphering method is designed in [15] by joining the Fast Fourier Transform, Logistic and Sine maps to encrypt the audio signal. In [16], a developed cryptosystem is proposed for ciphering the speech file that depends on DNA code and various chaotic systems namely Quadratic, Logistic, Extended Logistic and Lorenz maps. Cubic model is applied in [17] to rearrange the plain speech file. Then, Gingerbread and Henon chaotic maps are employed to improve the robustness of the encryption process. One dimensional Logistic and Cubic maps are merged to build a new chaotic system in [18]. Next, the combined system is implemented for the speech encryption/decryption by carrying out the concept of confusion/diffusion. In [19], the speech segments are shuffled and defused by utilizing Jacobian Elliptic chaotic map to improve the drawbacks of the presented speech ciphering mechanism during communication. Three levels of encryption are considered in [20] namely: fusion, replacement and permutation in order to increase the level of security. 3D Arnold map and Tent chaotic maps are integrated in [21] for speech ciphering by changing the positions/values of samples in the input signal. Eventually, the audio file is compressed in [22] to remove the residual intelligibility between samples. Next, the compressed file is enciphered via modified Henon/Lorenz chaotic systems.

To reduce the shortcoming in the classical encryption techniques and enhance the security, a novel and efficient speech security system that merges between chaotic systems and DNA coding method is proposed in this paper. Firstly, the input speech signal is partitioned to four equal blocks. Secondly, the speech samples in the blocks are enciphered by adopting the confusion/diffusion principle via four various chaotic maps namely Quadratic map, Ikeda map, Tinkerbell map and Chebyshev map, respectively. The sub-signals obtained from the blocks are integrated to yield the main ciphered signal. Thirdly, the consequent signal from the second stage and the produced random sequence from Sine chaotic map are encoded by performing the DNA coding rules to produce the encoded DNA sequences. Fourthly, the generated two coded sequences from the prior phase are added together by exploiting the DNA coding operations to obtain the encoded DNA signal. Finally, the DNA decoding rules are applied on the encoded signal resulted from the fourth step to acquire the ultimate encrypted speech signal. Generally, the main contributions of this scheme are summarized as follows: (1) Merging two different powerful mechanisms including the chaos theory and DNA encoding rules/operations to ameliorate the robustness of the presented approach to famous cryptographic attacks. (2) Applying the confusion/diffusion architecture to further increase the cryptosystem security. (3) Expanding the size of key space to attain better security level against exhaustive attack by adopting five different chaotic maps. (4) Giving an extensive study to investigate and assess the encryption/decryption capabilities of the suggested algorithm using various speech quality measures and for different speech signal files.

The rest of this paper is arranged as follows: the basic theory of the presented scheme including the used chaotic generators and DNA coding method is introduced in Section 2. Section 3 discusses in details the architecture of the presented speech cryptosystem including encryption/decryption algorithms, while the test results of security analysis are given in Section 4. Comparison with the existing schemes is presented in Section 5, and finally, the main conclusions and suggestions for future work are provided in Section 6.

II. Preliminaries

A. Chaotic Generators Used

1) Quadratic Map

One dimensional Quadratic map can be written as:

$$x_{n+1} = r - x_n^2 \qquad 0 < r < 2 \tag{1}$$

where x_n symbolizes the initial value, n symbolizes the iterations number, and r symbolizes the system parameter which controls the map behavior [6], [23].

2) Ikeda Map

The mathematical equations for two-dimensional Ikeda map can be described as:

$$\begin{gathered} x_{n+1} = 1 + u(x_n \, cos\, t_n - y_n \, sin\, t_n) \\ y_{n+1} = u(x_n \, sin\, t_n + y_n \, cos\, t_n) \\ t_n = 0.4 - \frac{6}{(1 + x_n^2 + y_n^2)} \qquad u > 0.6 \end{gathered} \tag{2}$$

where (x_n, y_n) represent the system's initial values which lies between (0, 1), whilst u represents the control parameter of the map [24].

3) Tinkerbell map

Tinkerbell map is a two-dimensional dynamical system which can be given as:

$$\begin{gathered} x_{n+1} = x_n^2 - y_n^2 + a x_n + b y_n \\ y_{n+1} = 2x_n \, y_n + c x_n + d y_n \end{gathered} \tag{3}$$

where x_n and y_n point to the system's initial conditions, whereas a, b, c and d point to the equation parameters. The common values used for these parameters are: $a = 0.9, b = -0.6$, $c = 2$ and $d = 0.5$ [25].

4) Chebyshev Map

One dimensional Chebyshev map is defined mathematically as:

$$y_{n+1} = \cos\,(k cos^{-1}(y_n)) \tag{4}$$

where the symbols y_n and k indicate to the initial condition and system parameter, respectively. In order to be in chaotic state, the values of y_n and k should be: $y_n \in [-1, 1]$ and $k \geq 2$ [23].

5) Sine Map

This one-dimensional chaotic map has one control parameter μ and one initial condition x_n. Sine map can be depicted using the iterated equation:

$$x_{n+1} = \mu \sin\,(\pi\, x_n) \tag{5}$$

where $\mu \in (0, 1]$ and $x_n \in (0, 1)$. Sine map is in chaotic case if $\mu = 1$, which implies that the generated sequence is non-convergent, aperiodic and extremely sensitive to the initial condition x_n [26].

B. DNA Coding and Decoding

Deoxyribonucleic Acid (DNA) is made up four nucleic acid bases which combine to compose chains. These nucleic bases contain two pyrimidines: Thymine (T) and Cytosine (C), and two purines: Guanine (G) and Adenine (A). The bases of DNA pair with each other, G links with C, and T links with A to brew units known as base pairs. Hence, (G, C) and (T, A) represent the complementary pairs. This complementary base resembles binary order, in which 0 and 1 are complementary as well as 01 and 10, 00 and 11 are likewise complementary. 24 sorts of coding combinations can be found, but only 8 of them can attain the Watson-Crick complementary rule. The 8 coding rules of DNA sequence are clarified in Table I. Simply, to convert any message to the DNA sequence, each character in the message is expressed as its corresponding binary form whose length is 8. Then, each two bits are mapped to one of four DNA nucleic bases whose length is 4. Contrariwise, the DNA sequence can be decoded to its original character value. For example, if the character value is 200, this value is converted to its corresponding binary string as 11001000. This binary string can be encoded into DNA sequence TAGA or TACA by utilizing Rule 1 or Rule 2, respectively. The wrong binary string 01100010 is gained which lead to wrong character value 98 if the wrong DNA rule (for example Rule 6) is utilized to decode the DNA sequence TAGA. Furthermore, the researchers have presented some algebraic and biology processes including addition, subtraction, exclusive OR (XOR) and exclusive NOR (XNOR). Details of DNA XOR and XNOR operations rules are reported in Table II [5], [8], [9]. In the present work, Rule 1 is adopted for speech samples encoding and decoding, whilst XNOR process of the DNA technology is employed because, as seen from Table II, the outcome of this operation in each column/row is distinctive and unique.

TABLE I
RULES OF DNA CODING AND DECODING

DNA bases	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7	Rule 8
A	00	00	01	01	10	10	11	11
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01
T	11	11	10	10	01	01	00	00

TABLE II
XOR AND XNOR PROCESSES OF DNA

⊕	A	C	T	G	⊙	A	C	T	G
A	A	C	T	G	A	C	A	G	T
T	T	G	A	C	T	T	G	C	A
C	C	A	G	T	C	A	C	T	G
G	G	T	C	A	G	T	G	A	C

III. THE PROPOSED SYSTEM SCHEME

Overall architectures of the presented speech encryption /decryption schemes are depicted in Figs. 1 and 2, respectively. The presented speech cryptosystem involves five major stages to meet the security demands. In the first stage, the plain signal is divided equally into four blocks. In the second stage, the speech samples in the four blocks are confused and diffused by the chaotic sequences. The sequences are generated via Quadratic map for the first block, Ikeda map for the second block, Tinkerbell map for the third block, and eventually Chebyshev map for the last block. Confusion operation is utilized to randomly shuffle the positions of speech samples. Diffusion operation is employed to change the speech samples values sequentially. Confusion and diffusion phases are often integrated so as to satisfy a satisfactory performance. Next, the obtained blocks are joined to get the cipher signal. In the third stage, the chaotic sequence generated from Sine map and the resulted enciphered signal from the second phase are encoded via the DNA coding rules to get the coded DNA streams. In order to ameliorate the security and further encrypt the cipher signal, the output coded sequences from the previous phase are added in the fourth stage by implementing the DNA XNOR operation to obtain the encrypted DNA signal. In the final stage, the DNA decoding rules are utilized on the consequent signal from the prior step to produce the ultimate encrypted speech signal. The resulting technique assures high security against different sorts of statistical, exhaustive and differential analyses. The details of the encryption/decryption procedures are illustrated in the following subsections.

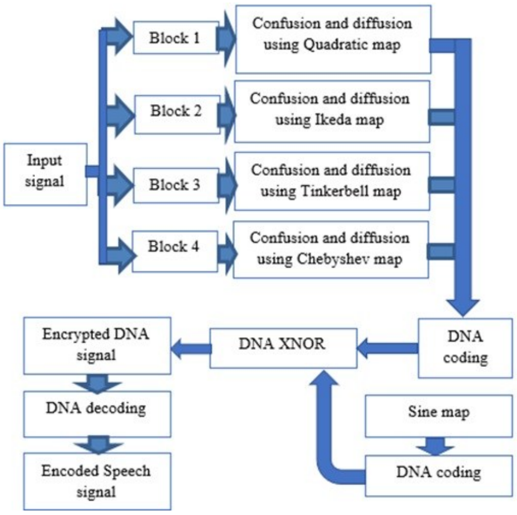

Input signal
Block 1
Block 2
Block 3
Block 4
Confusion and diffusion using Quadratic map
Confusion and diffusion using Ikeda map
Confusion and diffusion using Tinkerbell map
Confusion and diffusion using Chebyshev map
DNA coding
DNA XNOR
Encrypted DNA signal
DNA decoding
Encoded Speech signal
Sine map
DNA coding

Fig. 1. Architecture of the presented speech encryption scheme

A. Speech Encryption Algorithm

The encryption operation of the presented speech cryptosystem is outlined in the steps below:

Step 1: Divide the original one-dimension speech signal $y\ (M,1)$ into four equal blocks y_1, y_2, y_3 and y_4, each of size $(M/4,1)$.

Step 2: Convert y_1, y_2, y_3, y_4 from one-dimension into two-dimension signal to obtain the matrices P_1, P_2, P_3 and P_4, each of size (M_1, N_1).

Step 3: Generate the first chaotic sequence x_1 based on the (x_n, r) using (1) for Quadratic map and reshape it with the same size of P_1.

Step 4: Generate the second chaotic sequence x_2 based on the $(x_n\ , y_n, u)$ using (2) for Ikeda map and reshape it with the same size of P_2.

Step 5: Produce the third chaotic sequence x_3 based on the (x_n,y_n a, b, c, d) using (3) for Tinkerbell map and reshape it with the same size of P_3.

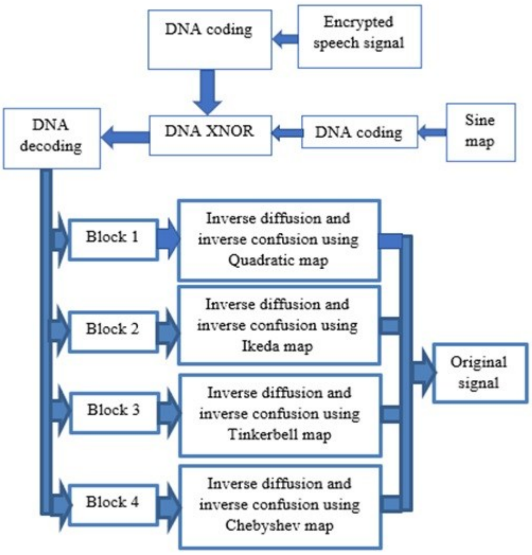

DNA coding
Encrypted speech signal
DNA decoding
DNA XNOR
DNA coding
Sine map
Block 1
Inverse diffusion and inverse confusion using Quadratic map
Block 2
Inverse diffusion and inverse confusion using Ikeda map
Block 3
Inverse diffusion and inverse confusion using Tinkerbell map
Block 4
Inverse diffusion and inverse confusion using Chebyshev map
Original signal

Fig. 2. Architecture of the presented speech decryption scheme

Step 6: Produce the fourth chaotic sequence x_4 based on the (y_n,k) using (4) for Chebyshev map and reshape it with the same size of P_4.

Step 7: Sort the chaotic sequences x_1, x_2, x_3 and x_4 that generated from the Steps 3, 4, 5, and 6, respectively in ascending order to get the new sequences X_1, X_2, X_3 and X_4 according to the formula:

$$[X_1, L_1] = sort\ (x_1)\ , [X_2, L_2] = sort\ (x_2) \quad (6)$$
$$[X_3, L_3] = sort\ (x_3), [X_4, L_4] = sort\ (x_4)$$

where L_1, L_2, L_3 and L_4 represent the index value of X_1, X_2, X_3 and X_4, respectively.

Step 8: Perform the confusion process by shuffling the speech samples in P_1, P_2, P_3 and P_4 via the indexes of the chaotic sequences produced in Step 7 to gain the permuted speech samples matrices P_1', P_2', P_3' and P_4' according to:

$$P_1'(i,j) = P_1\big(L_1(i,j)\big)\ , P_2'(i,j) = P_2\big(L_2(i,j)\big) \quad (7)$$
$$P_3'(i,j) = P_3\big(L_3(i,j)\big)\ , P_4'(i,j) =$$
$$P_4\big(L_4(i,j)\big)$$

Step 9: Execute the diffusion process by substitute the permuted speech samples matrices P_1', P_2', P_3' and P_4' with the chaotic sequences matrices X_1, X_2, X_3 and X_4 to acquire the diffused speech samples B_1, B_2, B_3 and B_4 as shown:

$$B_1(i,j) = B_1(i,j-1) \oplus P_1'(i,j) \oplus X_1(i,j)$$
$$B_2(i,j) = B_2(i,j-1) \oplus P_2'(i,j) \oplus X_2(i,j) \quad (8)$$
$$B_3(i,j) = B_3(i,j-1) \oplus P_3'(i,j) \oplus X_3(i,j)$$
$$B_4(i,j) = B_4(i,j-1) \oplus P_4'(i,j) \oplus X_4(i,j)$$

Step 10: Merge the four diffused speech matrices B_1, B_2, B_3 and B_4 to gain the ciphered matrix Y (W_1, W_2) as follows:

$$Y = Recombine\ (B_1, B_2, B_3, B_4) \quad (9)$$

Then, Y is transformed to its equivalent binary matrix $Y'(W_1 \times W_2, 8)$.

Step 11: Employ Rule 1 on the $Y'$to gain the encoded matrix $C_1(W_1 \times W_2, 4)$.

$$\mathrm{C_1 = Encode(Y')} \quad (10)$$

Step 12: Generate the fifth chaotic sequence x_5 based on the (x_n, μ) using (5) for Sine map and reshape it with the same size of Y. Then, the chaotic sequence x_5 is transformed to its equivalent binary matrix $x_5'(W_1 \times W_2, 8)$.

Step 13: Carry out Rule 1 on the x_5' to acquire the coded matrix $C_2(W_1 \times W_2, 4)$.

$$C_2 = Encode(x_5') \quad (11)$$

Step 14: Add the two encoded matrices C_1 and C_2 by utilizing the DNA XNOR according to Table II to get the encrypted matrix $C_3(W_1 \times W_2, 4)$ using the equation:

$$C_3(i,j) = C_1(i,j) \odot C_2(i,j) \quad (12)$$

Step 15: Carry out Rule 1 on the C_3 to earn the binary decoded matrix $C_3'(W_1 \times W_2, 8)$.

$$C_3' = Decode(C_3) \quad (13)$$

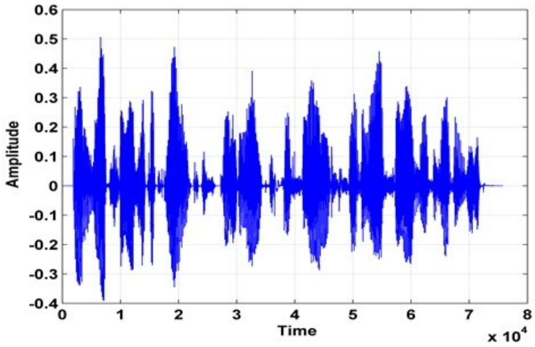
Step 16: Transform C_3' to its equivalent decimal matrix $C_4(W_1, W_2)$. The final step is converting C_4 from two dimensions to one dimension in order to obtain the definitive encrypted speech signal D $(M, 1)$.

B. *Speech Decryption Algorithm*

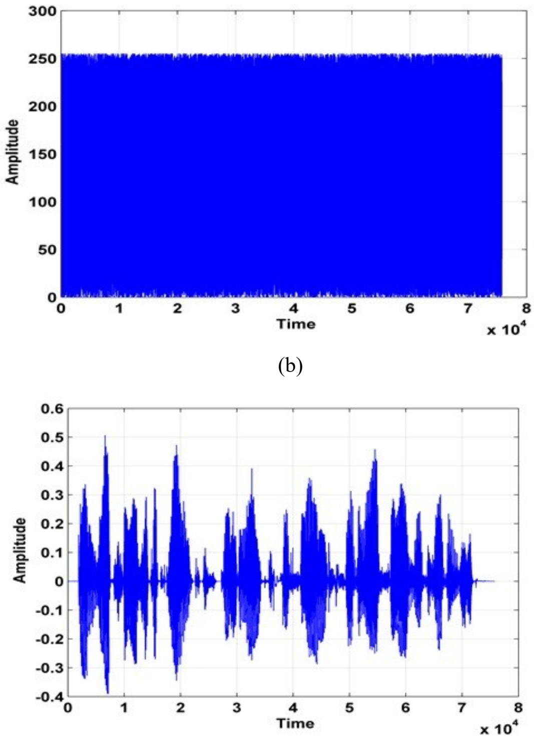
The decryption mechanism utilizes the same operations mentioned above, but in inverse manner. This means that the decryption procedure starts with the encrypted signal D and ends with the original signal y. The receiver should have the same secret keys employed by the sender for encryption so as to retrieve the original signal at decryption.

IV. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

Many speech quality measures are utilized in this section so as to evaluate the presented encryption mechanism immunity against cryptanalysis attacks. Also, these measures are used to validate the quality and residual intelligibility of the ciphered/deciphered speech signals [13]. The proposed encryption and decryption methods have been modeled via a personal HP laptop of Core i3 Processor, RAM of 3.90 GB, CPU of 2.40 GHz for Windows 7 and MATLAB R2013a as a programming language. For cryptosystem experimentations, four speech signal samples have been selected randomly from TIMIT library as test materials with sampling rate of 16 KHz and duration of 1.4150, 2.8550, 3.3150 and 4.7350 seconds, respectively. The original, ciphered and deciphered speech signals generated by the proposed technique for the last test speech file are presented in Fig. 3. The ciphered speech signal is totally different from the original signal and it is analogous to white noise, unintelligible and extremely uniform, which demonstrates the removal of the residual intelligibility in the ciphered signal. This implies that the introduced speech encryption scheme is of high quality. On the other hand, the deciphered speech signal is very identical to the original signal. This implies that the introduced speech decryption scheme is of high quality.



(a)



(b)

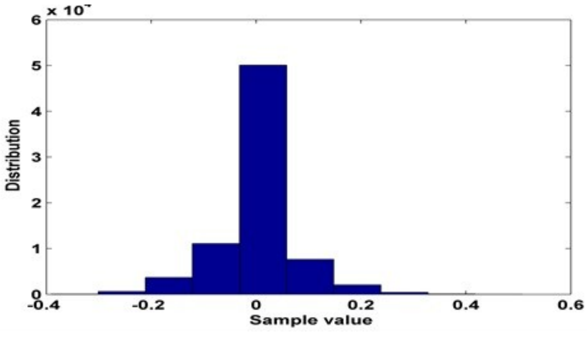
(c)

Fig. 3. (a) Original signal, (b) Ciphered signal, (c) Deciphered signal

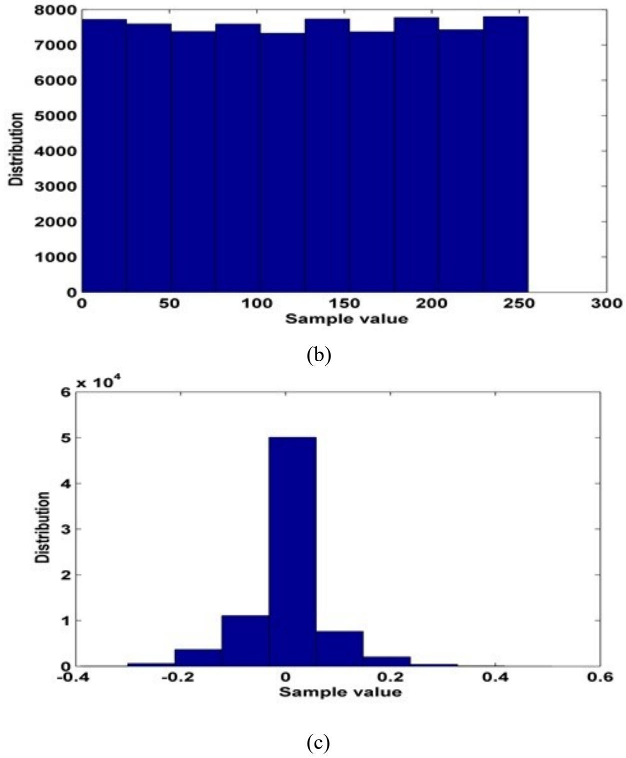
A. Statistical Analysis

1) Histogram Analysis

A histogram represents an important characteristic in data analysis and can be defined as a schematic representation of the tabulated information. In general, a good speech encryption algorithm should have a reasonably uniform distribution of its samples [12], [27]-[29]. This analysis is performed in the proposed research so as to assess its immunity and confirm its strength against the statistical attack. The histogram results of the ciphered and deciphered speech signals for the last test speech sample are shown in Fig. 4. The ciphered signal histogram is clearly different from the input signal histogram, random-like and fairly uniform. This manifests that the suggested method does not supply any helpful statistic data in the encrypted speech signal and it can effectively tolerate the statistical analysis attack. Also, the deciphered signal histogram is identical to that of the original signal histogram. This indicates that the introduced approach possesses excellent reconstruction effect.



(a)



(b)

(c)

Fig. 4. Histograms of (a) Input signal, (b) Ciphered signal, (c) Deciphered signal

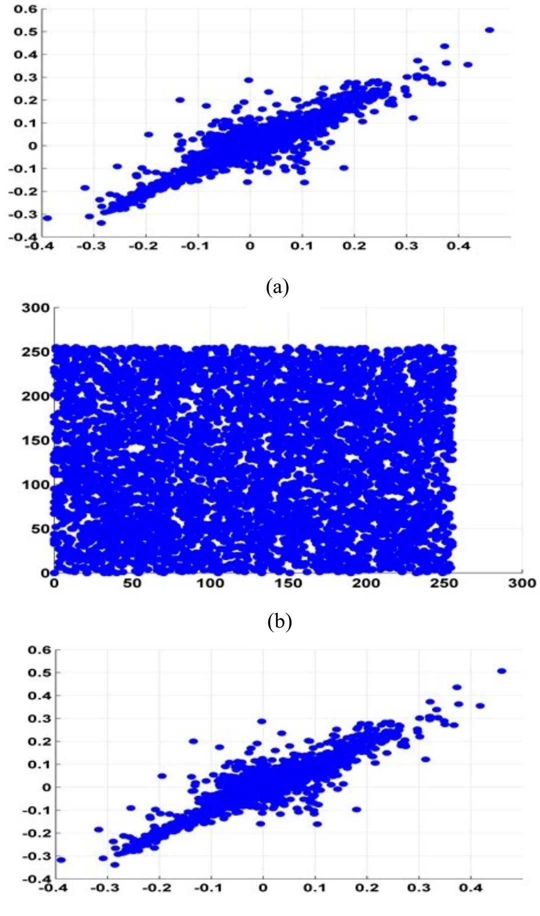
2) Correlation Coefficient Analysis

Analysis of the correlation coefficient represents a statistical mechanism that used to confirm the cryptosystem quality. Correlation Coefficient (CC) clarifies the correlation among neighbouring samples in the original and ciphered speech samples. Generally, the original speech signal is characterized by strong correlation, while ciphered signal in a good cipher should characterized by weak correlation among the neighbouring samples. If the value of CC is close or equal to one, then the original and the decrypted or reconstructed speech signals are extremely similar to each other or identical, whereas if the value of CC is close or equal to zero, then the original and the encrypted speech signals are entirely different. Thus, lower correlation coefficient values validate the success of the cryptographic operation. The CC is computed as:

$$CC = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{\sum_{i=1}^{L}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{L}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{L}(y_i - E(y))^2}} \qquad (14)$$

$$E(x) = \frac{1}{L}\sum_{i=1}^{L} x_i \quad , \quad E(y) = \frac{1}{L}\sum_{i=1}^{L} y_i$$

where x and y denote to the original and encrypted or decrypted speech signals, respectively. L denotes to the samples number, $E(x)$ denotes to the value of the mean, whilst cov denotes to the covariance [2], [5], [11], [30]-[32]. The correlation coefficients values of neighboring samples in the original, ciphered speech signals, and between the original speech and its corresponding ciphered speech for the four test signals produced by the suggested method are presented in Table III. The distribution of correlation coefficients among neighboring samples for the last test signal in the original, ciphered and deciphered signals are illustrated in Fig. 5. Also, the values of correlation coefficients between the original speech and its corresponding deciphered speech signals are given in Table IV. The results of CC in Table III point out that the CC values among neighboring speech samples in the original signal are relatively high. Moreover, these values in the ciphered speech signal, and between the original and its corresponding ciphered speech signals are very low (negative values and almost zero). Fig. 5a exhibits linear distribution for CC among neighboring samples in the original signal, while Fig. 5b exhibits random distribution for CC among neighboring samples in the ciphered signal. Furthermore, the results of CC in Table IV and Fig. 5c suggest that the CC values between the original and deciphered speech signals are very high (one). The results in Tables III and IV, and Fig. 5 show that the suggested cryptosystem offers extremely good results in terms of encryption and decryption processes and can counter the statistical analysis efficiently.



(a)

(b)

(c)

Fig. 5. Correlation coefficients distribution among neighboring samples in the: (a) Original speech signal, (b) Ciphered speech signal, (c) Deciphered speech signal

B. Signal to Noise Ratio Analysis

Signal to Noise Ratio or SNR is utilized to measure the level of distortion in the speech signal. It is a good estimator to quantify the quality of deciphered speech signal as well as the residual intelligibility of the ciphered signal. The ciphered signal is generally characterized by low value of SNR which points out to a higher level of distortion, whilst high value of SNR denotes to a high precision and good quality of the deciphered speech signal [6], [10], [11]. This measurement is given as:

$$SNR = 10 \times log_{10} \frac{\sum_{i=1}^{L} x_i^2}{\sum_{i=1}^{L}[x_i - y_i]^2} \qquad (15)$$

The SNR measures for different tested speech signals introduced by the proposal method in the case of encryption and decryption are represented in Tables III and IV, respectively. In general, all the ciphered speech files in Table III are characterized by having low values of SNR which demonstrates a low residual intelligibility and high encryption quality. Contrary, the deciphered speech files in Table IV are characterized by having high values of SNR which implies a high residual intelligibility and high decryption quality.

C. Key Analysis

1) Key Space Analysis

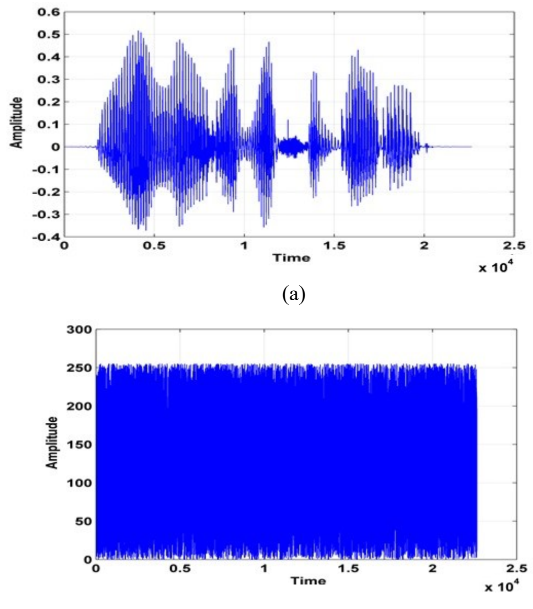
The key space size in any cryptographic method represents the overall number of various keys which can be utilized to accomplish the encryption/decryption procedures. It should be sufficient large in order to resist all types of attacks. The key space should be greater than 2^{100} for ideal cryptosystem. The key space size is determined by the initial conditions/control system parameters of the chaotic maps used [11], [14]. The set of keys utilized in the presented work are: for Quadratic map: $(x_n,\ r)$, for Ikeda map: $(x_n, y_n,\ u)$, for Tinkerbell map: $(\ x_n, y_n,\ a, b, c,\ d)$, for Chebyshev map: $(y_n,\ k)$, and finally for Sine map: $(x_n,\ \mu)$. Thus, the key space composed of fifteen real values. If 10^{-14} is used as precision for each secret key, then the total key space size will be $(10^{14})^{15} = 10^{210} \approx 2^{698}$. Hence, the proposed speech approach has sufficient key space to tolerate any type of brute force attack.

2) Key Sensitivity Analysis

Key sensitivity is the most significant characteristic of chaotic maps. Secure encryption scheme should be quite sensitive to a slight alteration in its secret keys so as to withstand the exhaustive attack. The effect of this analysis can be observed on the proposed technique by using two different methods. The first method is concerned with encryption process. This means that if two different keys with slight change between them are utilized to cipher the same signal, then totally two different encrypted signals should be obtained [7], [9], [14]. For Quadratic map, the secret keys are: $x_n = 0.01, r = 1.9$. For Ikeda map, the secret keys are: $x_n = 0.08, y_n = 0.08, u = 0.9$. For Tinkerbell map, the secret keys are: $x_n = -0.72, y_n = -0.64, a = 0.9, b = -0.6013, c = 2,$ $d = 0.5$. For Chebyshev map, the secret keys are: $y_n = 0.03, k = 2$. Finally, for Sine map, the secret keys are: $x_n = 0.5, \mu = 0.9425$. To assess the key sensitivity analysis of the first method, the first test speech sample is ciphered by utilizing the above parameters as presented in Fig. 6 b. Fig. 6 c shows the ciphered speech signal obtained by utilizing a small alteration on x_n of Quadratic map by adding $\Delta = 10^{-14}$, whereas other parameters are kept the same. The results in Figs. 6 b and 6 c demonstrate that a slight variation in one of the secret keys yields an entirely different ciphered signal. Further, the presented approach is evaluated by measuring SNR and the correlation coefficients between the two ciphered speech signals. The simulation results of CC and SNR are tabulated in Table V. Form the results in this table; it is clear that the two ciphered signals produced by the suggested cryptosystem have very small values of correlation and SNR. The second method is concerned with decryption process. To evaluate the key sensitivity analysis of the second method, the last test ciphered speech signal is deciphered using slightly altered secret keys. The deciphered signals with these wrong keys are displayed in Fig. 7. A minor manipulation in one of the secret keys can results a totally different reconstructed speech signal. Hence, the correct deciphering cannot be accomplished thereby maintaining the security over any noisy communication channel. Moreover, the suggested cryptosystem is validated by calculating SNR, and the correlation coefficients between the original and decrypted speech signals gained from a small variation on the secret keys and the results are illustrated in Table VI. The results of SNR and correlation coefficients in this table indicate that their values are extremely small. It can be concluded that the encryption/decryption processes achieved by the introduced algorithm are highly sensitive to the secret keys. This reveals that the proposed mechanism is capable of enduring exhaustive attack successfully.

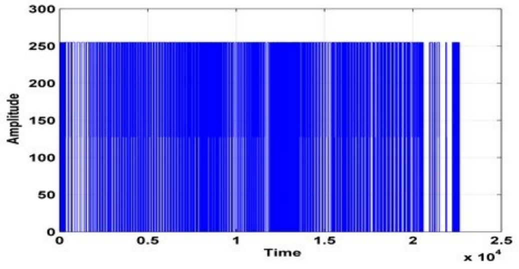
D. *Differential Analysis*

Cryptanalysis usually tries to make a slight alteration in the input signal and utilizes the proposed technique to cipher the input signal before and after alteration. Then, these two ciphered signals are compared so as to extract the relation between the original and the ciphered signals, thus obtaining the secret key. This analysis in cryptography is known as differential analysis. In order to avert this attack, a tiny modification in the plain signal should cause a considerable variation in the ciphered signal. Then, the differential attack becomes useless and inefficient. Two common criteria namely Number of Samples Change Rate (NSCR) and Unified Average Changing Intensity (UACI) are used in order to measure the impact of changing one sample in the original signal on the corresponding ciphered signal by the suggested algorithm. These two measures are calculated as:



(a)

(b)

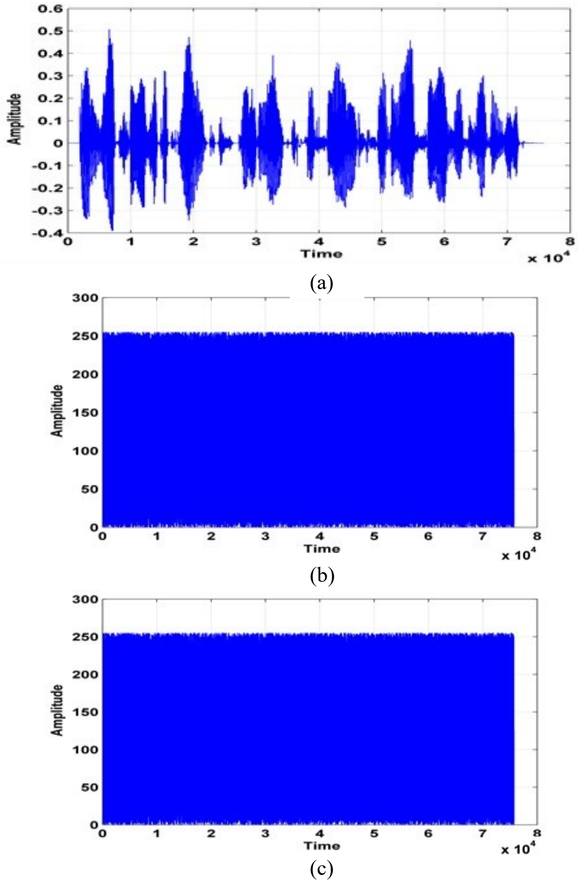


(c)

Fig. 6. Key sensitivity analysis at the encryption process: (a) Original speech signal, (b) Ciphered speech signal using the original secret key, (c) Ciphered speech signal using Key 1

$$NPCR = \frac{\sum_i D(i)}{l} \times 100\%$$
$$UACI = \frac{1}{l}\left[\sum_i \frac{|x_1(i)-x_2(i)|}{255}\right] \times 100\% \qquad (16)$$
$$D(i) = \begin{cases} 0 & if\ x_1(i) = x_2(i) \\ 1 & if\ x_1(i) \neq x_2(i) \end{cases}$$

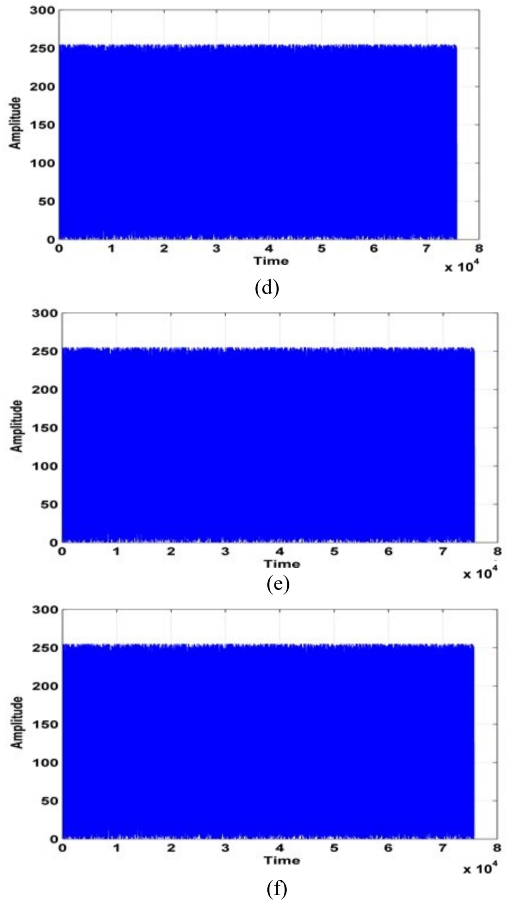
where x_1 and x_2 are the two encrypted speech signals that corresponding to the actual speech signals with one sample change only, l is the speech vector length. The optimum NSCR and UACI values are 100% and 33.3%, respectively [4], [6], [32]. Table III clarifies the values of NSCR and UACI calculated by applying the presented encryption scheme on the four different versions of speech signals. The experimental results obtained in Table III manifest that NSCR and UACI values are extremely close to the optimum values, which proves the introduced cryptosystem sensitivity to the input signal and thus it can endure differential analysis effectively.



(a)

(b)

(c)



(d)

(e)

(f)

Fig. 7 Key sensitivity analysis at the decryption process: (a) Original speech signal, (b) Deciphered speech signal using Key 1, (c) Deciphered speech signal using Key 2, (d) Deciphered speech signal using Key 3, (e) Deciphered speech signal using Key 4, (f) Deciphered speech signal using Key 5

TABLE III
RESULTS OF ENCRYPTION QUALITY MEASURES FOR THE TEST SPEECH SIGNALS

Speech sample	Signal 1. wav	Signal 2. wav	Signal 3. wav	Signal 4. wav
CC among neighboring samples in the original speech signal	0.9812	0.8991	0.9307	0.9252
CC among neighboring samples in the ciphered speech signal	0.0053	0.0091	-0.0096	0.0060
CC between original and ciphered speech signals × 10^{-4}	-8.4313	-8.2362	-1.6632	-2.5525
SNR (dB)	-62.7023	-64.0226	-63.7279	-66.0396
UACI (%)	33.1124	33.8550	33.2981	33.1289
NSCR (%)	99.99	100	99.99	100

TABLE IV
RESULTS OF DECRYPTION QUALITY MEASURES FOR THE TEST SPEECH SIGNALS

Speech sample	CC between original and deciphered speech signals	SNR (dB)
Signal 1. wav	1	217.1832
Signal 2. wav	1	215.8365
Signal 3. wav	1	216.1914
Signal 4. wav	1	213.8042

TABLE V
RESULTS OF KEY SENSITIVITY ANALYSIS AT ENCRYPTION FOR THE FIRST TEST SPEECH SIGNAL

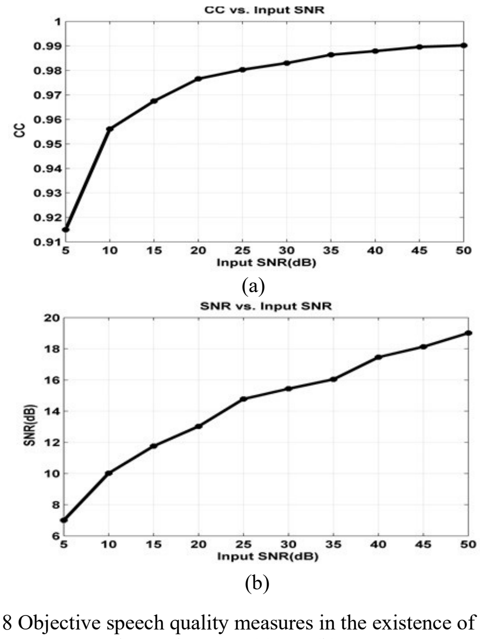
Chaotic map	Parameter + Δ	Gained key	CC between two ciphered speech signals	SNR (dB)
Quadratic map	$x_n + \Delta$	Key 1	0.0093	-62.6954
Ikeda map	$u + \Delta$	Key 2	0.0089	-62.6786
Tinkerbell map	$c + \Delta$	Key 3	0.0044	-62.7253
Chebyshev map	$y_n + \Delta$	Key 4	-0.0060	-62.7424
Sine map	$\mu + \Delta$	Key 5	-0.0039	-62.9033

TABLE VI
RESULTS OF KEY SENSITIVITY ANALYSIS AT DECRYPTION FOR THE LAST TEST SPEECH SIGNAL

Gained key	CC between original and deciphered speech signals	SNR (dB)
Key 1	-0.0131	-66.0426
Key 2	-0.0211	-66.0405
Key 3	-0.0259	-66.0363
Key 4	-0.0174	-66.0386
Key 5	-0.0103	-66.3989

E. Noise Effect on the Decryption Process

Noise effect on the introduced method efficiency is a significant matter must be considered [5], [10], [12]. The speech cryptosystem performance is assessed in the existence of noise for the second test speech file at various levels of SNR. The added noise is White Gaussian Noise (WGN) varying from 5 to 50 dB. The noise effect on the objective speech quality measures including correlation coefficient and Signal to Noise Ratio are computed in the case of decryption. The CC and SNR variations with respect to WGN of different levels for the suggested cryptosystem are explained in Fig. 8. The values of speech quality measures in the decryption are improved at high values of SNR, which point out that the introduced approach can endure noise efficiently with low power.



(a)

(b)

Fig. 8 Objective speech quality measures in the existence of WGN for decryption case (a) CC (b) SNR

TABLE VII
COMPARISON OF PERFORMANCE MEASURES WITH EXISTING SCHEMES

Correlation Coefficient Comparison

Scheme	Ref. 2	Ref. 6	Ref. 11	Ref. 12	Ref. 13	Ref. 14	Ref. 17	Ref. 18	Ref. 19	**Proposed**
CC Encryption	0.000569	0.0233	-0.0014	-0.009221	0.0051	-0.00118	0.4703	0.0032	0.000889	**-0.00025525**
CC Decryption	-	0.999	-	0.992882	-	1	-	1	-	**1**

SNR Comparison

Scheme	Ref. 2	Ref. 5	Ref. 11	Ref. 14	Ref. 17	Ref. 18	**Proposed**
SNR (dB) Encryption	-22.45	-	-13.3015	-41.05	7.020	-10.4925	**-66.0396**
SNR (dB) Decryption	-	193.6586	30.2338	240.16	-	39.2841	**213.8042**

Key Space Comparison

Scheme	Ref. 2	Ref. 11	Ref. 12	Ref. 14	Ref. 17	Ref. 18	**Proposed**
Key space	2^{477}	10^{84}	2^{348}	10^{128}	2^{512}	2^{180}	**2^{698}**

NSCR and UACI Comparison

Scheme	Ref. 6	Ref. 29	**Proposed**
NSCR (%)	99.9996	99.6320	**100**
UACI (%)	33.3066	33.6823	**33.1289**

V. COMPARISON WITH EXISTING SCHEMES

To prove the supremacy of the presented cryptosystem, it is compared to some other existing speech encryption approaches in terms of several performance indicators as shown in Table VII. For correlation coefficient comparison, the correlation coefficient value obtained in this scheme is closer to zero in the case of encryption and one in the case of decryption as compared with the existing approaches. For SNR comparison, the high negative SNR value in the encryption case gained by the current method indicates the high quality of ciphered signal, whereas the high positive SNR value in the decryption case demonstrates the good quality of deciphered signal. For key space comparison, the key space is larger in comparison to other references, which makes the suggested technique more resistible to exhaustive attack. And lastly for NSCR, UACI comparison, the values of NSCR and UACI in Table VII are higher, which manifests that the speech cryptosystem has a strong capability of resisting the differential attack analysis. The comparison results revel that, in the most of performance criteria, the introduced work outperforms the existing encryption mechanisms and yields good quality encrypted/decrypted speech signal.

VI. CONCLUSIONS

This paper introduces a new mechanism for speech signal encryption/decryption based on chaotic systems and DNA coding algorithm. The suggested method composes of two stages of security. The first security stage is accomplished by utilizing multiple chaotic maps in order to perform confusion/diffusion operations of speech samples, whilst the second security stage is accomplished by utilizing the DNA coding technique. The usage of DNA coding rules/XNOR process enhances the ciphering randomness as well as improves the speech samples diffusion impact of the current scheme. The speech cryptosystem performance is assessed through various evaluation criteria. The security analysis and inclusive simulation outcomes point out that the proposed system defeats several kinds of known cryptographic analyses such as histogram analysis, correlation analysis, SNR analysis, key analysis and differential analysis. In addition, the presented cryptosystem can encrypt/decrypt various sorts of speech signals with high degree of security. The introduced work presents better efficiency in comparison to existing similar schemes. Besides, the suggested cryptosystem is robust to noise distortion with high signal to noise ratio. All these characteristics revel that the given method is appropriate to be implemented in ciphering applications of real time speech signals. For future work, the suggested scheme can be applied upon other multimedia data like text message, digital image or video information. Additionally, this mechanism can be also executed on FPGA environment.

REFERENCES

[1] S. F. Yousif, "Encryption and Decryption of Audio Signal Based on RSA Algorithm", International Journal of Engineering Technologies and Management Research, vol.5, no.7, pp. 57-64, 2018. https://doi.org/10.29121/ijetmr.v5.i7.2018.259

[2] Farsana F J and Gopakumar K, "A Novel Approach for Speech Encryption: Zaslavsky Map as Pseudo Random Number Generator", Procedia Computer Science, 6th International Conference on Advances In Computing & Communications, ICACC, vol. 93, pp. 816 – 823, 2016. https://doi.org/10.1016/j.procs.2016.07.302

[3] O. A. Imran, S. F. Yousif, I. S. Hameed, W. N. Al-Din Abed, and A. T. Hammid, "Implementation of El-Gamal algorithm for speech signals encryption and decryption" Procedia Computer Science, International Conference on Computational Intelligence and Data Science (ICCIDS), vol. 167, pp. 1028–1037, 2020.
https://doi.org/10.1016/j.procs.2020.03.402

[4] S. F. Yousif, "Secure voice cryptography based on Diffie-Hellman algorithm", 2nd International Scientific Conference of Engineering Sciences (ISCES), IOP Conf. Series: Materials Science and Engineering, vol. 1076, pp. 012057, 2021. https://doi.org/10.1088/1757-899x/1076/1/012057

[5] S. J. Sheela, K. V. Suresh, and D. Tandur, "A Novel Audio Cryptosystem Using Chaotic Maps and DNA Encoding", Journal of Computer Networks and Communications, vol. 2017, pp. 1-12, 2017. https://doi.org/10.1155/2017/2721910

[6] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption using chaotic shift keying for secured speech communication", EURASIP Journal on Audio, Speech, and Music Processing, vol. 2017, No. 1, pp. 1-11, 2017. http://dx.doi.org/10.1186/s13636-017-0118-0

[7] S. F. Yousif, "Speech Encryption Based on Zaslavsky Map", Journal of Engineering and Applied Sciences, vol. 14, no. 17, pp. 6392-6399, 2019. http://dx.doi.org/10.36478/jeasci.2019.6392.6399

[8] S. F. Yousif, "A new speech cryptosystem using DNA encoding, genetic and RSA algorithms", International Journal of Engineering & Technology, vol. 7, no. 4, pp. 4550-4557, 2018.
https://doi.org/10.14419/ijet.v7i4.21271

[9] S. F. Yousif, A. J. Abboud, and R. S. Alhumaima, “A new image encryption based on bit replacing, chaos and DNA coding techniques”, Multimedia Tools and Applications, vol. 81, pp. 27453–27493, 2022. https://doi.org/10.1007/s11042-022-12762-x

[10] E. Mosa, N. W. Messiha, O. Zahran, and F. E. Abd El-Samie, “Chaotic encryption of speech signals”, International Journal of Speech Technology, vol. 14, no. 4, pp. 285-296, 2011. https://doi.org/10.1007/s10772-011-9103-7

[11] S. M. H. Alwahbani and E. B. M. Bashier, “Speech Scrambling Based on Chaotic Maps and One Time Pad”, INTERNATIONAL CONFERENCE ON COMPUTING, ELECTRICAL AND ELECTRONIC ENGINEERING (ICCEEE), pp. 128-133, 2013. https://doi.org/10.1109/ICCEEE.2013.6633919

[12] S. N. Al Saad and E. Hato, “A Speech Encryption based on Chaotic Maps”, International Journal of Computer Applications, vol. 93, no. 4, pp. 19-28, 2014. https://doi.org/10.5120/16203-5488

[13] E. M. Elshamy, E. M. El-Rabaie, O. S. Faragallah, O. A. Elshakankiry, F. E. Abd El-Samie, H. S. El-sayed, and S. F. El-Zoghdy, “Efficient audio cryptosystem based on chaotic maps and double random phase encoding”, International Journal of Speech Technology, vol. 18, no. 4, pp. 619-631, 2015. https://doi.org/10.1007/s10772-015-9279-3

[14] M. F. A. Elzaher, M. Shalaby, and S. H. El Ramly, “Securing Modern Voice Communication Systems using Multilevel Chaotic Approach”, International Journal of Computer Applications, vol. 135, no.9, pp. 17-21, 2016. https://doi.org/10.5120/ijca2016908497

[15] Y. Alemami, M. A. Mohamed, S. Atiewi, and M. Mamat, “Speech encryption by multiple chaotic maps with fast fourier transform”, International Journal of Electrical and Computer Engineering (IJECE), vol. 10, no. 6, pp. 5658-5664, 2020. https://doi.org/10.11591/ijece.v10i6.pp5658-5664

[16] S. M. Abdullah and I. Q. Abduljaleel, “Speech Encryption Technique using S - box based on Multi Chaotic Maps”, TEM Journal, vol. 10, no. 3, pp. 1429-1434, 2021. https://doi.org/10.18421/TEM103-54

[17] N. F. Hassan, A. Al-Adhami, and M. S. Mahdi, “Digital Speech Files Encryption based on Hénon and Gingerbread Chaotic Maps”, Iraqi Journal of Science, vol. 63, no. 2, pp. 830-842, 2022. https://doi.org/10.24996/ijs.2022.63.2.36

[18] S. Mokhnache and M. E. Daachi, T. Bekkouche, and N. Diffellah “A Combined Chaotic System for Speech Encryption”, Engineering, Technology & Applied Science Research, vol. 12, no. 3, pp. 8578-8583, 2022. https://doi.org/10.48084/etasr.4912

[19] O. M. Al-Hazaimeh, A. A. Abu-Ein, K. M. Nahar, and I. S. Al-Qasrawi, “Chaotic elliptic map for speech encryption”, Indonesian Journal of Electrical Engineering and Computer Science, vol. 25, no. 2, pp. 1103-1114, 2022. https://doi.org/10.11591/ijeecs.v25.i2.pp1103-1114

[20] H. A. Abdallah and S. Meshoul, “A Multilayered Audio Signal Encryption Approach for Secure Voice Communication”, Electronics, vol. 12, no. pp. 2, 2023. https://doi.org/10.3390/electronics12010002

[21] C. M. Nițu, M. Răducanu, and D.-G. Cheroiu, “Fast speech encryption algorithm based on Arnold 3D chaotic system”, Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies XI, vol. 12493, pp. 592-599, 2023. https://doi.org/10.1117/12.2643008

[22] F.J. Farsana, V.R. Dev, and K. Gopakumar, “An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams”, Applied Computing and Informatics, vol. 19, no. 3/4, 2023, https://doi.org/10.1016/j.aci.2019.10.001

[23] S. F. Yousif, “Grayscale Image Confusion and Diffusion Based on Multiple Chaotic Maps”, 1st International Scientific Conference of Engineering Sciences - 3rd Scientific Conference of Engineering Science (ISCES), pp. 114-119, 2018.

https://doi.org/10.1109/NCCCS.2012.6412989

[24] M.Y. M. Parvees and J. A. Samath, “A Colour Byte Scrambling Technique for Efficient Image Encryption Based on Combined Chaotic Map”, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 1067-1072, 2016. https://doi.org/10.1109/ICEEOT.2016.7754851

[25] S. Yuan, T. Jiang, and Z. Jing, “Bifurcation and chaos in the Tinkerbell map”, International Journal of Bifurcation and Chaos, vol. 21, no. 11, , pp. 3137–3156, 2011. https://doi.org/10.1142/S0218127411030581

[26] T. Gopalakrishnan and S. Ramakrishnan, “Chaotic Image Encryption with Hash Keying as Key Generator”, IETE Journal of Research, vol. 63, no. 2, pp. 172–187, 2017.

http://dx.doi.org/10.1080/03772063.2016.1251855

[27] H. N. Abdullah, S. F. Yousif, and A. A. Valenzuela, “Wavelet Based Image Steganographic System Using Chaotic Signals”, 6th International Conference on Information Communication and Management, pp. 130-135, 2016. http://dx.doi.org/10.1109/INFOCOMAN.2016.7784229

[28] H. N. Abdullah, S. F. Yousif, and A. A. Valenzuela, “Efficient Steganography Scheme for Color Images based on Wavelets and Chaotic Maps”, Iraqi Journal of Information and Communications Technology(IJICT), vol. 2, no. 4, pp. 1-10, 2019. https://doi.org/10.31987/ijict.2.4.86

[29] H. N. Abdullah, S. F. Yousif, and A. A. Valenzuela, “Spatial and Transform Domain based Steganography Using Chaotic Maps for Color Images”, Journal of Fundamental and Applied Sciences, vol. 10, no. 4S, 2018, pp. 551-556, 2018. http://dx.doi.org/10.4314/jfas.v10i4s.212

[30] SURA F. YOUSIF, ALI J. ABBOUD, and HUSSEIN Y. RADHI, “Robust Image Encryption With Scanning Technology, the El-Gamal Algorithm and Chaos Theory”, IEEE Access, vol. 8, pp. 155184-155209, 2020. http://dx.doi.org/10.1109/ACCESS.2020.3019216

[31] S. A. Gebereselassie and B. K. Roy, “A new Secure Speech Communication Scheme Based on Hyperchaotic Masking and Modulation”, IFAC-PapersOnLine, vol. 55, no. 1, pp. 914-919, 2022, https://doi.org/10.1016/j.ifacol.2022.04.150

[32] F. J. Farsana and K. Gopakumar, “Speech Encryption Algorithm Based on Nonorthogonal Quantum State with Hyperchaotic Keystreams”, Advances in Mathematical Physics, vol. 2020, pp. 1-12, 2020. https://doi.org/10.1155/2020/8050934