Hindawi
Journal of Computer Networks and Communications
Volume 2017, Article ID 2721910, 12 pages
https://doi.org/10.1155/2017/2721910

Research Article

A Novel Audio Cryptosystem Using Chaotic Maps and DNA Encoding

S. J. Sheela,[1] K. V. Suresh,[1] and Deepaknath Tandur[2]

[1]*Department of E and C, Siddaganga Institute of Technology, Visvesvaraya Technological University, Tumakuru, India*
[2]*Corporate Research India, ABB, Bengaluru, India*

Correspondence should be addressed to S. J. Sheela; sheeladinu@sit.ac.in

Received 27 April 2017; Accepted 2 July 2017; Published 6 August 2017

Academic Editor: Nasrollah Pakniat

Chaotic maps have good potential in security applications due to their inherent characteristics relevant to cryptography. This paper introduces a new audio cryptosystem based on chaotic maps, hybrid chaotic shift transform (HCST), and deoxyribonucleic acid (DNA) encoding rules. The scheme uses chaotic maps such as two-dimensional modified Henon map (2D-MHM) and standard map. The 2D-MHM which has sophisticated chaotic behavior for an extensive range of control parameters is used to perform HCST. DNA encoding technology is used as an auxiliary tool which enhances the security of the cryptosystem. The performance of the algorithm is evaluated for various speech signals using different encryption/decryption quality metrics. The simulation and comparison results show that the algorithm can achieve good encryption results and is able to resist several cryptographic attacks. The various types of analysis revealed that the algorithm is suitable for narrow band radio communication and real-time speech encryption applications.

1. Introduction

Secured speech communication plays a significant role in military, voice over Internet protocols, confidential voice conferences, and corporate sectors. This necessitates the development of a reliable, fast, and robust security system to provide data confidentiality, integrity, and authentication. In this regard, researchers have developed many cryptographic algorithms to suite the evolvement in wireless communication technologies. The traditional symmetric cryptographic schemes such as advanced encryption standard (AES) and data encryption standard (DES) can attain high level of security. But they have small key space which in turn suffers from brute force attack. These cryptographic algorithms cannot be utilized in real-time speech encryption due to high degree of redundancy among the samples, bandwidth expansion of the encrypted signal, and reduction of signal to noise ratio performance. Because of complex permutation process, these algorithms require more computational time and high computing power. Further, asymmetric encryption algorithms are not suitable for encryption owing to slow speed and complexity [1–3]. Hence, it is necessary to explore the simple speech encryption techniques that can provide high level of security and high speed while attaining excellent audio quality of the decrypted speech signal.

In this contest, many researchers have identified the possibility of applying dynamic and disordered behavior of chaotic system in cryptography. These chaotic systems have outstanding features such as high sensitivity to initial conditions/system parameters, erratic behavior, high security, and simplicity. These subtle nonlinear properties make them a novel and efficient way of providing secured speech communication with low complexity. However, there are some challenges that need to be faced when using chaos theory in the field of cryptography [4]. There exists a data redundancy and all the chaotic maps are not random. Some of them utilize various one-dimensional (1D) chaotic maps in the development of speech security systems [5]. 1D chaotic maps result in single simple predictable chaotic orbits. As a result, the attacker can obtain the initial states and/or system parameters of the chaotic map easily. Further, one-dimensional chaotic map suffers from small key space and weak security.

On the other hand, security can be enhanced by increasing the dimension which in turn increases the nonlinearity. The higher dimensional (HD) chaotic maps are widely used in multimedia encryption owing to tough prediction of a time series and more numbers of positive Lyapunov exponents [6]. Hence, in this paper, two-dimensional modified Henon map is introduced. The 2D-MHM is obtained by using Henon map (HM) as seed map. The dynamic analysis in [7] has shown that the map has broad chaotic regime over an extensive range of system parameters, maximum Lyapunov exponent, and better chaotic performance when compared to seed map. Hence, the speech encryption algorithm using MHM is proposed in [8]. Further, it has been proved that the encryption schemes using only chaos are less secure which necessitates the introduction of new mechanism to enhance the security of the cryptosystem [9–11].

In order to make chaos based cryptosystem more secure, DNA technology has been infiltrated due to its exclusive characteristics such as huge parallelism, enormous information storage, and ultralow power consumption [12, 13]. DNA cryptography uses biomolecular concepts which give hope in the design of unbreakable algorithms. Hence, a new speech encryption scheme based on chaotic maps and DNA encoding is proposed in this paper. The position of speech samples is shuffled by using the sequences generated from 2D-MHM thereby achieving the confusion. Further, DNA encoding and the sequences generated from standard map change the value of the speech samples. The scheme uses dynamic DNA encoding instead of fixed coding which in turn increases the security [14]. The encryption capability of the speech encryption algorithm is assessed through security analysis for various speech signals.

The organization of the paper is as follows. Section 2 introduces the chaotic maps along with their dynamical behavior. The design of speech encryption scheme based on HCST and DNA encoding is discussed in Section 3. The results of security analysis are provided in Section 4. The final section concludes the paper.

2. Preliminary Theory of the Algorithm

This section reviews the chaotic maps used for speech encryption such as MHM and standard map (SM) along with their dynamical behavior. The comparison of dynamical behaviors of MHM and HM through bifurcation diagram is also considered. Further, the basics of DNA encoding along with algebraic operations is presented.

2.1. Modified Henon Map. The modified Henon map [7] is given by

$$H(x_k, y_k) = \begin{pmatrix} x_{k+1} \\ y_{k+1} \end{pmatrix} = \begin{pmatrix} 1 - b_1 \cos(x_k) - b_2 y_k \\ -x_k \end{pmatrix}, \quad (1)$$

where b_1 and b_2 are control parameters and (x_k, y_k) represents the two-dimensional state of the system. In the seed map [15], x_k^2 term is replaced by the nonlinear term $\cos(x_k)$ and $b_2 \neq 0$ thereby increasing the chaotic region. For modified Henon map, the bounded solutions will be obtained for all values of b_1 and $|b_2| < 1$. A wide chaotic range can be obtained by selecting one of the system parameters $b_2 = 0.3$. The chaotic range of MHM is compared with seed map which is evidenced through bifurcation diagram. Bifurcation diagram plots output sequences of a chaotic map along with the change of its system parameter(s). Figure 1 shows the comparison of Henon map and MHM with respect to bifurcation diagram. From the bifurcation diagram, it is clear that Henon map is chaotic for the range of $b_1 \in [1.06, 1.22] \cup [1.27, 1.29] \cup [1.31, 1.4]$ whereas modified Henon map is chaotic for the range of $b_1 \in [2.19, 2.5] \cup [>2.54]$ in the interval $0 \leq b_1 \leq 5$. Thus, the simulation results show an improvement in the chaotic range ratio of 7% to 56% in this interval [7]. The MHM has at least three advantages when compared to seed map which are as follows: (1) The map has broad array chaotic regime over an extensive range of system parameters. (2) MHM is more dynamic as the Lyapunov exponents are greater than those of Henon map. (3) The map is highly sensitive to their initial conditions and system parameters as the correlation between the chaotic sequences is less. Hence, MHM is more suitable to provide secured communication.

2.2. Standard Map. The 2D standard map is the simplest conservative system which originates from the field of particle physics [16, 17]. It is defined by

$$\begin{pmatrix} Z_{n+1} \\ W_{n+1} \end{pmatrix} = \begin{pmatrix} (Z_n + W_n) \bmod 2\pi \\ Z_n + r \sin(Z_n + W_n) \bmod 2\pi \end{pmatrix}, \quad (2)$$

where Z_n, $W_n \in [0, 2\pi)$. The nonlinearity of the map is directly proportional to the system parameter. The SM can be discretized from $[0, 2\pi) \times [0, 2\pi)$ to $S \times S$ by substituting $z = ZS/2\pi$, $w = WS/2\pi$, and $R = rS/2\pi$ in (2). The resulting discretized map is given by

$$\begin{pmatrix} z_{n+1} \\ w_{n+1} \end{pmatrix} = \begin{pmatrix} (z_n + w_n) \bmod S \\ z_n + R \sin\left(\frac{z_{n+1} S}{2\pi}\right) \bmod S \end{pmatrix}, \quad (3)$$

where R can take any real value and S is any integer value. The discretized standard map properties may not be as good as the original one, but integer domain implementation is possible which in turn reduces the computational efforts [18]. Further, SM is commonly used in the design of block symmetric cipher because its structure resembles Fiestel network [19]. Hence, SM is more appropriate for real-time information security.

2.3. DNA Encoding. A single DNA sequence is composed of four nucleic bases, namely, adenine (A), cytosine (C), guanine (G), and thymine (T). According to DNA rules, A pairs with T and C pairs with G, where A and T are complementary and C and G are complementary [20]. This complementary rule resembles the binary system. Because 0 and 1 are complementary in binary system, 00 and 11 are complementary and 01 and 10 are also complementary. Thus, there are 24 types of coding combinations. According to Watson-Crick complement rule, only 8 code combinations

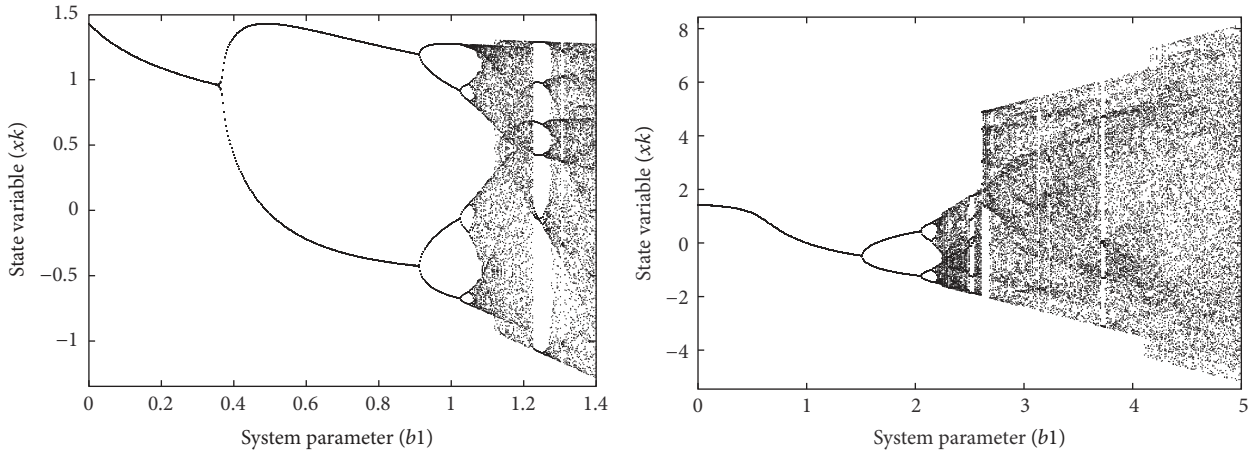


Figure 1: (a) Bifurcation diagram of Henon map for the system parameter ($b_2 = 0.3$). (b) Bifurcation diagram of MHM for the system parameter ($b_2 = 0.3$).

Table 1: DNA encoding and decoding rules.

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

Table 2: DNA XOR operation.

	A	T	C	G
A	A	T	C	G
T	T	A	G	C
C	C	G	A	T
G	G	C	T	A

can be used out of 24 coding combinations [21] which are listed in Table 1. With the rapid development in DNA cryptography, researchers have introduced several biological and algebraic operations such as exclusive OR (XOR), addition, and subtraction [22, 23]. In this paper, DNA XOR operation is used to encrypt and decrypt the speech samples. Table 2 shows the DNA XOR operation which is reflexive.

3. HCST and DNA Based Speech Cryptosystem

In this section, the detailed architecture HCST and DNA encoding mechanism adopted for speech encryption is presented. The algorithm uses chaotic maps and DNA encoding to perform primitive operations of cryptography such as confusion and diffusion. These two chaotic maps generate the secret key for the proposed algorithm. The secret key contains the information of initial conditions and control parameters of these maps. Hence, the key set used for encryption/decryption is (x_0, y_0, b_1, b_2, z_0, w_0, R, S). Two chaotic maps are used to increase the key space and security performance of the algorithm. Confusion and diffusion are applied to shuffle speech sample positions randomly and to change the value of the speech samples, respectively. The complete architecture of the encryption scheme is shown in Figure 2.

3.1. Hybrid Chaotic Shift Transform. In this section, hybrid chaotic shift transform [24] is proposed to shuffle the positions of the speech samples thereby reducing the correlation between the samples. The inherent features of the chaotic map such as random nature and sensitivity to initial conditions/system parameters make them a good candidate to perform confusion operation.

3.1.1. Definition of HCST. Firstly, generate $2N$ chaotic values $(x_1, x_2, \ldots, x_N)$, $(y_1, y_2, \ldots, y_N)$ from the MHM using (1). Sort the chaotic sequence x_k in descending order and get the column shift matrix from the positions of the sorted sequence which is given by $B = [b_1, b_2, \ldots, b_N]$. Similarly, get the row shift matrix by sorting the chaotic sequence y_k in ascending order which is given by $C = [c_1, c_2, \ldots, c_N]$, where b_i and c_i represent the step size cyclic up/down shift in column i and cyclic right/left shift in row i, respectively.

Let I be an original speech signal which is processed frame by frame with the frame size and frame shift of M with the frame length of 15–30 ms and T be the corresponding shuffled speech signal. Then hybrid chaotic shift transform is defined as

$$T_1 = F(I, B)$$
$$T = F(T_1, C), \tag{4}$$

where T represents the row shifted speech block. The hybrid CST function F is described in Algorithm 1. Therefore,

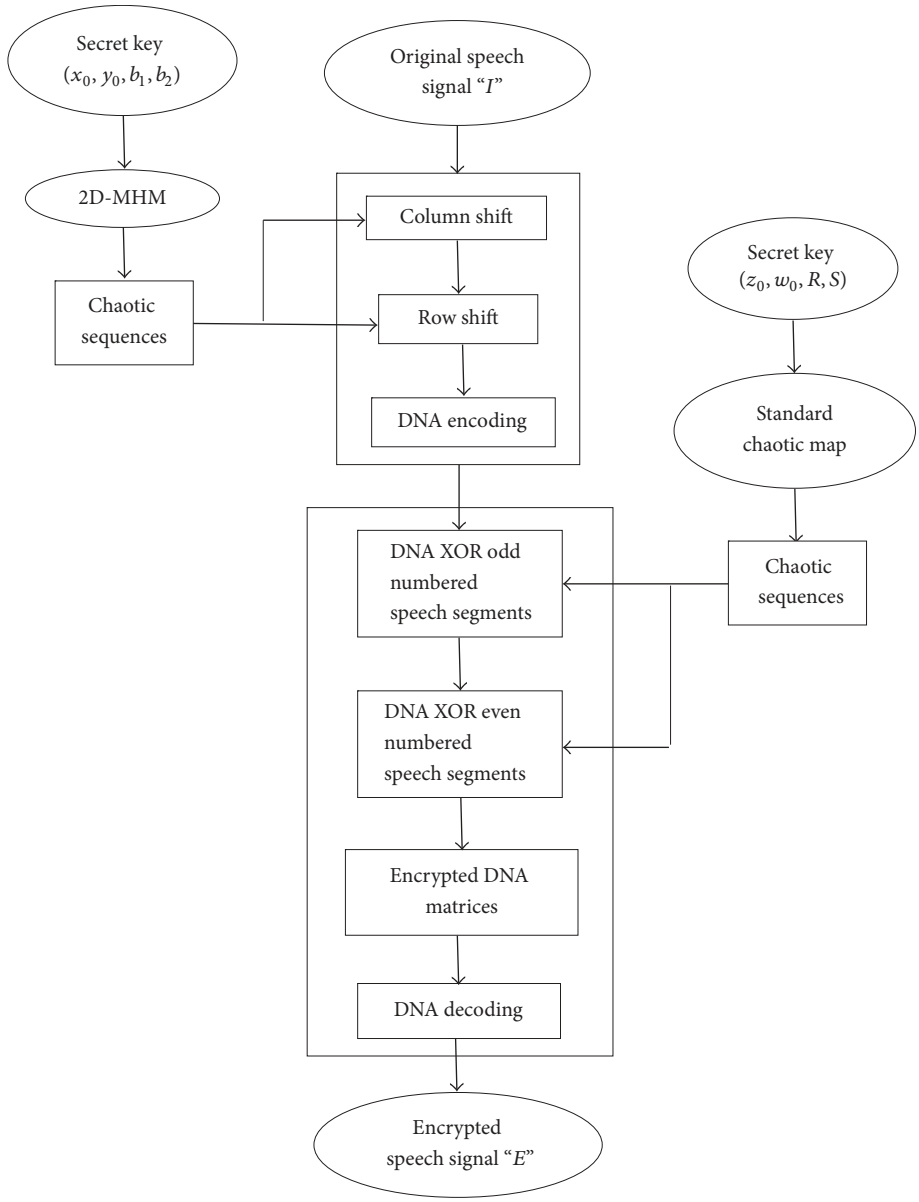


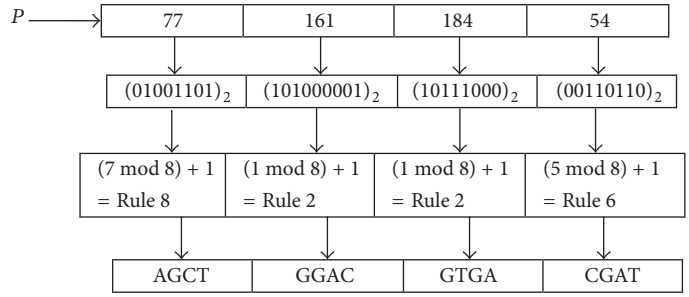
Figure 2: Proposed encryption scheme flow diagram.

HCST shuffles the positions of the speech samples efficiently thereby reducing the correlation among samples. Further, without the knowledge of initial conditions and system parameters of MHM it is not possible to predict the results of HCST.

3.2. Dynamic DNA Encoding. In this section, the dynamic DNA encoding mechanism is presented to change the value of the speech samples thereby spreading the effect of plaintext across the ciphertext. In order to enhance the security, the dynamic DNA coding is used instead of fixed coding. The values in the confused speech block are converted to their equivalent decimal values by using 16-bit quantization. The detailed operation of DNA encoding scheme is described and shown in Algorithm 2 and Figure 3.

4. Security Analysis

An efficient encryption algorithm should satisfy mainly two objectives: (1) The algorithm should offer resistance against all kinds of known attacks. (2) It should possess both confusion and diffusion property [25]. The confusion property corresponding to a tiny change in the key should produce entirely different ciphertext, whereas diffusion property refers to spreading the effect of slight change in the plaintext over the corresponding ciphertext. Further, a good cipher should be robust under noisy environment. Hence, the security of the proposed algorithm is evaluated and compared with other existing schemes in this section [5, 8]. Many metrics have been used in the literature to verify the quality of the decrypted signal and residual intelligibility of the encrypted



Similarly, encode the matrix "Q" by using the same procedure.

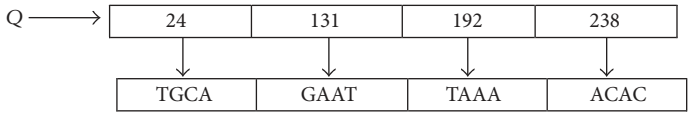


Figure 3: An example of DNA encoding process.

Input: The original speech signal I and chaotic series matrices B and C
Output: The column and row shuffled speech block T
(1) Generate the column and row shift matrices by sorting x_k and y_k chaotic sequence
(2) **for** $i = 1$ to N **do**
(3) **if** mod(b_i, 2) = 0 **then**
Cyclic shift the speech segment in column i of I to down with the step size of b_i;
(4) **else**
Cyclic shift the speech segment in column i of I to up with the step size of b_i;
(5) **end if**
(6) **end for**
(7) Denote the column shifted speech block as T_1.
(8) **for** $i = 1$ to N **do**
(9) **if** mod(c_i, 2) = 0 **then**
Cyclic shift the speech segment in row i of T_1 to right with the step size of c_i;
(10) **else**
Cyclic shift the speech segment in row i of T_1 to left with the step size of c_i;
(11) **end if**
(12) **end for**
(13) Denote the row shifted speech block as T.

Algorithm 1: The hybrid chaotic shift transform algorithm.

signal. The metrics also determine the immunity of the encryption scheme to cryptanalysis attacks.

4.1. Residual Intelligibility of Encrypted Signal. In order to evaluate the encryption capability of the proposed algorithm, different American English speech signals with sampling rate of 8 KHz and 16 KHz are encrypted. The original, encrypted, and decrypted speech signal are shown in Figure 4. From the figure, it is clear that the encrypted signal is similar to white noise without any original intonations. This indicates the absence of residual intelligibility in the encrypted signal.

4.2. Statistical Analysis. It has been revealed in the literature that statistical analysis effectively evaluates the cryptosystem [17, 25]. Statistical analysis has been performed to demonstrate the confusion and diffusion property of the cryptosystem which in turn offers resistance against statistical attacks. This has been illustrated by using histogram analysis, correlation analysis, and percent residual deviation (PRD).

4.2.1. Histogram Analysis. Histogram analysis evaluates the cryptosystem to determine its ability to resist against statistical attacks. Figure 5 shows the histogram of clean and

Input: Confused speech block T and encoding matrices P and Q
Output: Encrypted speech signal E
(1) Generate the encoding matrices from the chaotic sequence generated from SM.
(2) Encode P and Q using different DNA rules as depicted in Figure 3.
(3) Encode the confused speech block T using DNA rule 1.
(4) **for** $i = 1$ to M **do**
(5) **if** $\mathrm{mod}(T(:, i), 2) = 0$ **then**
$E(:, i) = P(:, i)$ XOR $T(:, i)$
Rotate P right by one byte
(6) **else**
$E(:, i) = Q(:, i)$ XOR $T(:, i)$
Rotate Q right by one byte
(7) **end if**
(8) **end for**
(9) Decode the encrypted DNA matrix using DNA rule 3.

Algorithm 2: Dynamic DNA encoding.

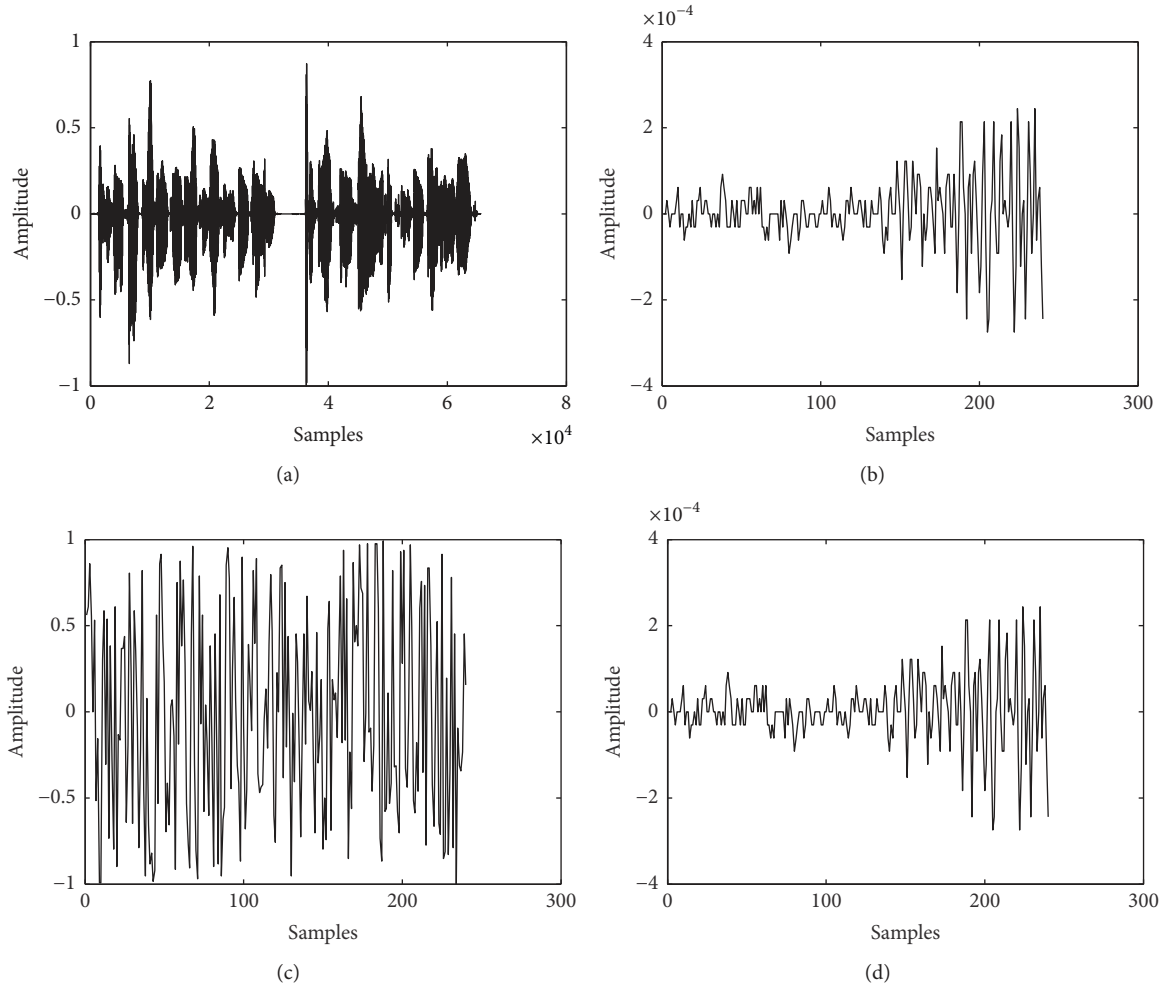


Figure 4: (a) Original speech signal (Julia 8). (b) Original signal for first frame. (c) Corresponding Encrypted speech signal. (d) Decrypted speech signal.

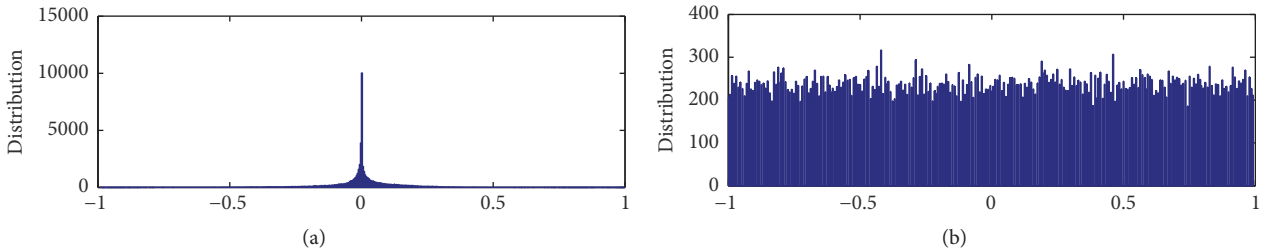


Figure 5: Histogram of (a) clean speech signal (Mel 8) and (b) encrypted speech signal.

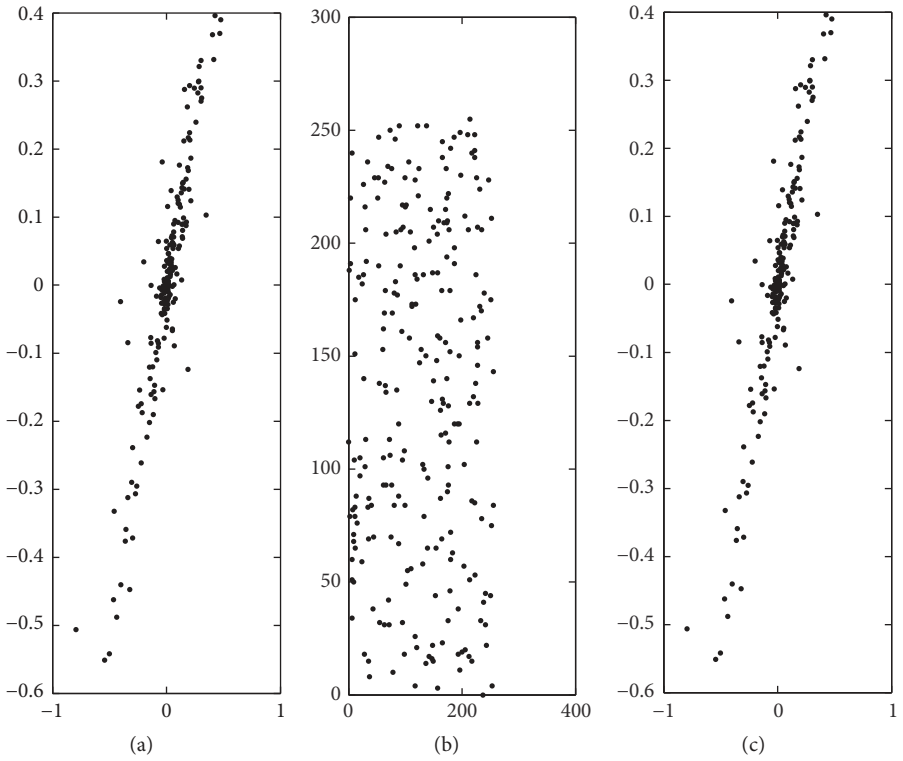


Figure 6: Correlation between the samples in (a) original speech signal (Rich 8), (b) encrypted speech signal, and (c) decrypted speech signal.

encrypted speech signals. It is clear that the histogram of the ciphered signal is fairly uniform indicating the best encryption results. Hence, the algorithm does not provide any original information and possesses good confusion property.

4.2.2. Correlation Coefficient Analysis. Correlation coefficient (CC) is one of the statistical measures which determine the encryption quality of the cryptosystem. This analysis measures the correlation between the two speech samples whose value lies between −1 and +1. The correlation coefficient being near zero indicates the weakest relationship between the two samples and it is not possible to predict the secret key by the attackers [1]. The correlation coefficient values between original and encrypted speech signals and their comparison with other algorithms are tabulated in Table 3. Figure 6 shows the correlation coefficient distribution of original and encrypted speech signal. It has been observed that the correlation values are closer to zero which indicates the good encryption quality. The correlation coefficient of this method is less when compared with the existing methods [5, 8] in almost all the trails, shown in Figure 7. The correlation coefficient r_{xy} is calculated [1] using

$$
\begin{aligned}
E(x) &= \frac{1}{T_s}\sum_{i=1}^{i=T_s} x_i \\
D(x) &= \frac{1}{T_s}\sum_{i=1}^{i=T_s} \left(x_i - E(x_i)\right)^2 \\
\operatorname{cov}(x,y) &= \frac{1}{T}\sum_{i=1}^{i=T_s} \left(x_i - E(x_i)\right)\left(y_i - E(y_i)\right) \\
r_{xy} &= \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)\,D(y)}},
\end{aligned}
\tag{5}
$$

where x and y are the audio values of the two adjacent audio levels in the speech signal, $E(x)$ is the mean value, $D(x)$ is

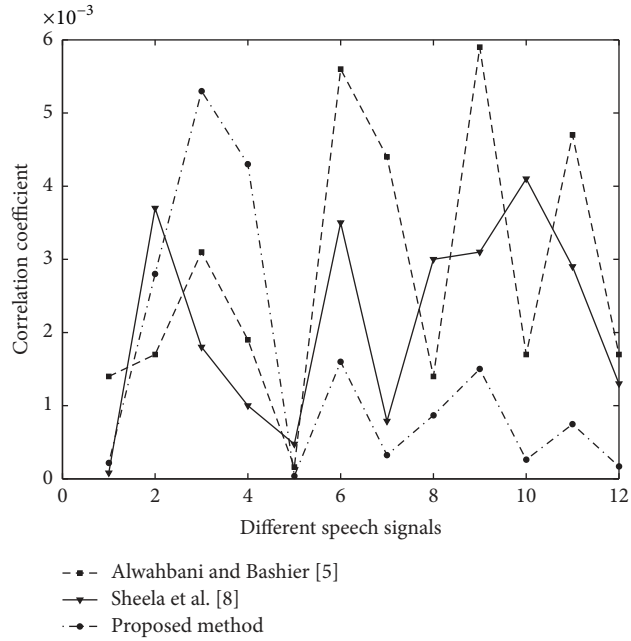


Figure 7: Comparison of proposed method with existing method with respect to correlation coefficient between samples of original speech signal and encrypted speech signal.

the variance, and cov(x, y) is the covariance between x and y. The number of samples used in calculations is denoted by T_s.

4.3. Percent Residual Deviation. This parameter measures the deviation of the encrypted speech signal from original signal [26]. The calculated values of the percent residual deviation for original and encrypted speech signal for different speech signals are given in Table 3. It has been observed that the encrypted signal is highly deviated from its original signal. For the given original signal $I(i)$ and obtained encrypted speech signal $E(i)$, the PRD is defined as

$$\varphi = 100 \times \sqrt{\frac{\sum_{i=1}^{n} \left[I(i) - E(i)^2\right]}{\sum_{i=1}^{n} I^2(i)}}. \quad (6)$$

4.4. Quality of the Decrypted Signal. It is necessary to measure and compare the quality of the decrypted signal with that of the original signal in order to prove the efficiency of the cryptosystem. The two approaches, namely, objective and subjective metrics, have been adopted in the literature to verify the quality of the decrypted signal. In objective metrics, the quality is measured using physical parameters and computational models. The subjective speech quality metrics require a panel of trained listeners which itself is a very tedious process. In real-time applications, the objective metrics are desirable because they give more consistent results in a shorter period [27]. Signal to noise ratio (SNR), Perceptual Evaluation of Speech Quality (PESQ), and so on are some of the speech quality metrics used to validate the algorithm.

4.4.1. Signal to Noise Ratio (SNR). SNR is used to measure residual intelligibility of the encrypted signal and quality of the decrypted signal. Generally, the encrypted signal is characterized by low SNR value indicating the higher noise level than the original speech signal whereas the good quality decrypted signal is characterized by high SNR value. The SNR [1, 2] is calculated using

$$\text{SNR} = 10 \log_{10} \frac{\sum_{i=1}^{T_s} I^2(i)}{\sum_{i=1}^{T_s} (I(i) - D(i))^2}, \quad (7)$$

where $D(i)$ is the decrypted speech signal. The SNR values for different speech signals are tabulated in Table 4. Further, the results are compared with existing algorithms [5, 8] which is shown in Figure 8. The comparison results show that the proposed algorithm yields good quality decrypted signal.

4.4.2. Perceptual Evaluation of Speech Quality. PESQ is one of the widely used and reliable methods used to measure the quality of the decrypted signal. Higher value of the PESQ indicates the better quality of the recovered speech signal. The PESQ score ranges from 1.0 to 4.5 [28, 29]. The PESQ scores for different speech signals are tabulated in Table 4 resulting with average score of 3.7738. Further, the effect of slightly altered key on PESQ is illustrated in Table 6. From the table, it is clear that PESQ value is sensitive to key.

4.5. Key Space. The key space of the encryption algorithm should be larger than 2^{100} to make the brute force attack infeasible [4, 30]. System parameters and initial conditions of the chaotic map determine the key space. The key set used

Table 3: Encrypted signal quality metrics.

Name	Correlation between original and encrypted signal	Alwahbani and Bashier [5]	Sheela et al. [8]	PRD
Claire 8	−0.00021724	−0.0014	0.00001855	2.4379×10^7
Julia 8	−0.0028	0.0017	−0.0037	2.6233×10^7
Lauren 8	0.0053	−0.0031	−0.0018	2.2872×10^7
Mel 8	0.0043	0.0019	−0.0010	2.2492×10^7
Ray 8	0.000038157	−0.00016	0.0001474	2.2362×10^7
Rich 8	−0.0016	−0.0056	−0.0035	2.0496×10^7
Claire 16	−0.00032371	−0.0044	0.0007885	1.3880×10^8
Julia 16	−0.00086778	0.0014	−0.0030	1.5012×10^8
Lauren 16	−0.0015	0.0059	0.0031	1.2983×10^8
Mel 16	−0.000266126	0.0017	−0.0041	1.2752×10^8
Ray 16	0.00074651	−0.0047	−0.0029	1.2721×10^8
Rich 16	−0.00016772	−0.0017	−0.0013	1.1656×10^8

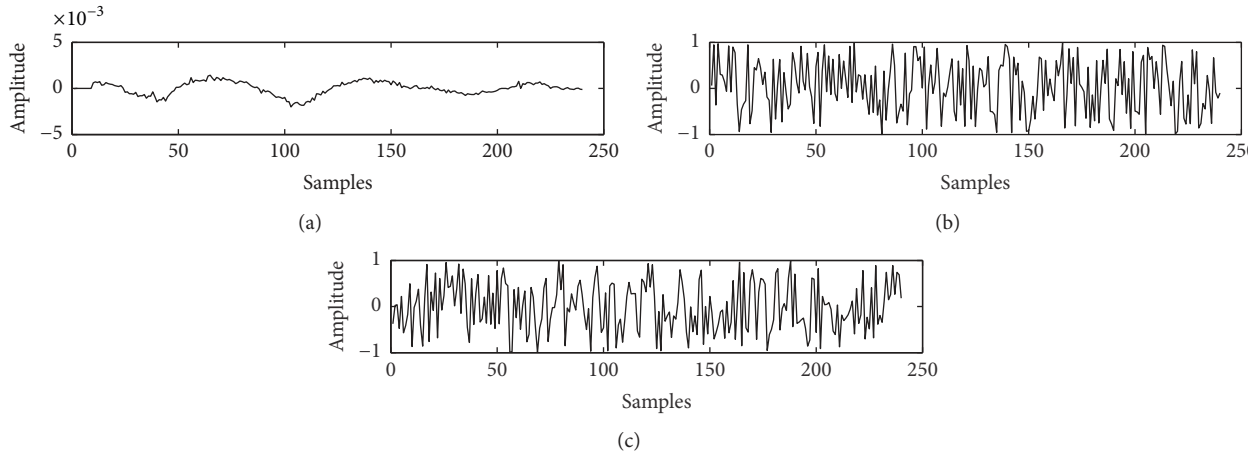


Figure 8: Key sensitivity test on encryption process: (a) original speech signal for first frame (Lauren 8); (b) encrypted speech signal for original key; (c) encrypted signal for Key A.

by cryptosystem contains eight parameters: seven floating point numbers and one integer, where z_0, $w_0 \in (0, 2\pi)$. R can take any real value which is greater than 18.0 and S takes any integer value greater than 100. The total number of possible values which can be used as a part of the key space from the MHM is 10^{56}, for the precision of 10^{-14}. Similarly, the total number of possible values which can be used as a part of the key space for z_0 and w_0 is $(6.28)^2 \times 10^{28}$. In the proposed cryptosystem, R has infinite number of possible values which can take part of the key space. But in a particular interval of 2π, R can take 6.28×10^{14} different possible values. Actually, the possible values that the parameter S can take are infinite. The total number of possible values that can be used as a part of the key space is 10^3, if S is ranging from 100 to 1100. So, the complete key space of the proposed algorithm is $(6.28)^3 \times 10^{101}$ which is large enough to resist brute force attack. Further, the key space is very large when compared to existing chaos based and traditional algorithms [5, 19].

4.6. Secret Key Sensitivity Analysis. A secure cryptosystem should be extremely sensitive to its secret key in order to resist exhaustive attack. The effect of key sensitivity on encryption process is verified by using slightly different keys to encrypt the same plaintext. A test speech signal "Lauren 8" is encrypted using the secret key ($x_0 = 0.1, y_0 = 0.6675, b_1 = 5.85, b_2 = 0.3, z_0 = 3.98, w_0 = 0.35, R = 26.4, S = 110$) which is shown in Figure 8(b). The encrypted signal which is obtained by applying a tiny change on x_0 with the variation of 10^{-10} is shown in Figure 8(c). The simulation results show that a tiny change in the key will result in completely different encrypted signal. The difference between two encrypted signals is about 94.4938%. Further, the algorithm is quantified by measuring the correlation between two encrypted signals which are tabulated in Table 5. It has been observed that the two encrypted signals have the least correlation.

The decryption process is analyzed through key sensitivity test by decrypting the encrypted signal with slightly modified key. Figure 9 shows the decryption of the test signal "Claire 8" for the slightly modified key (Key B). From the figure, it is clear that the correct decryption is not at all possible even for the slight change in secret key thereby providing secure communication over noisy wireless channel.

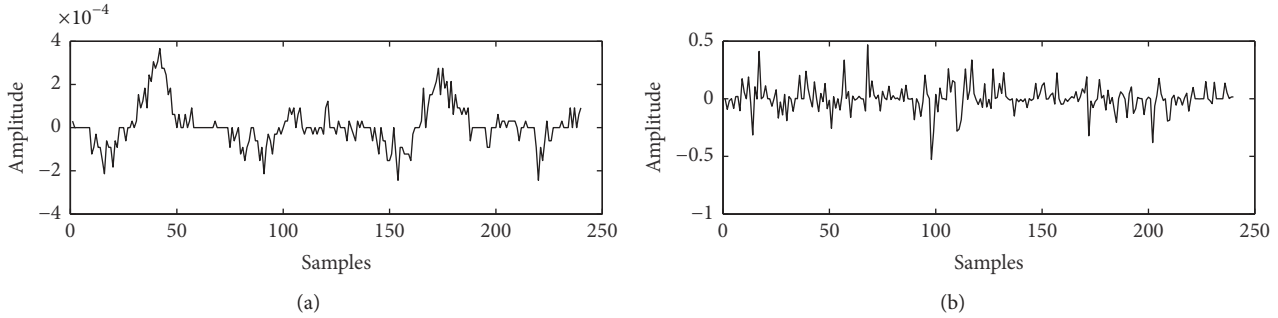


Figure 9: Key sensitivity test on decryption process: (a) original speech signal for the first frame (Claire 8); (b) decrypted speech signal for Key B.

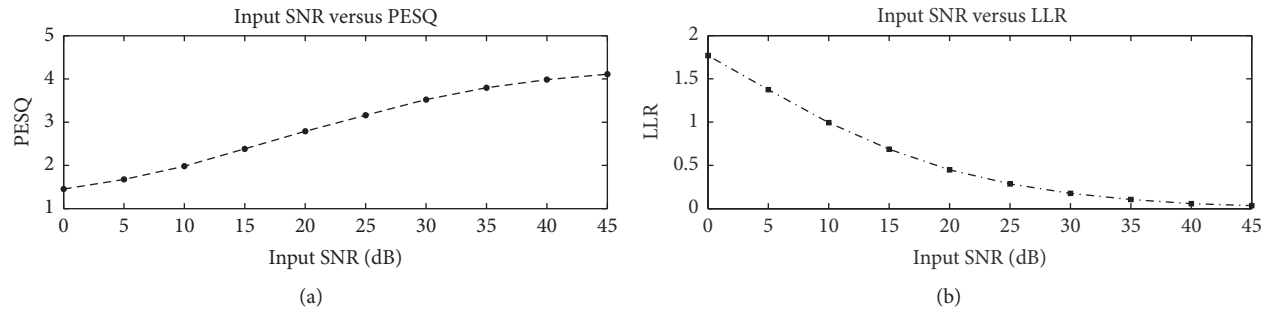


Figure 10: Speech quality metrics for the decrypted signal in the presence of AWGN noise: (a) PESQ; (b) LLR.

Table 4: Decrypted signal quality metrics.

Name	SNR in dB	Alwahbani and Bashier [5]	Sheela et al. [8]	PESQ
Claire 8	193.6586	30.2338	31.7008	3.34962
Julia 8	192.7466	29.5594	24.9047	3.28308
Lauren 8	194.1332	30.6980	19.1031	3.43439
Mel 8	193.9288	30.9975	22.4523	4.50000
Ray 8	194.6899	30.8710	25.2435	4.50000
Rich 8	194.9421	31.6812	21.7338	3.67965
Claire 16	190.6556	32.2487	25.0827	3.29362
Julia 16	189.6684	32.5668	17.3681	3.23237
Lauren 16	191.1387	33.7090	28.6808	3.37061
Mel 16	190.9293	33.8067	10.7542	4.50000
Ray 16	191.6308	32.8276	31.3426	4.50000
Rich 16	191.8984	34.6931	19.6978	3.64210

Table 5: Key sensitivity results for encryption process test signal as "Lauren 8."

Parameter changed with variation of 10^{-10}	Key obtained	CC between two encrypted signals
x_0	Key A	0.0025
y_0	Key B	0.0050
b_1	Key C	−0.0056
b_2	Key D	−0.0035

Table 6: Key sensitivity results for decryption process test signal as "Claire 8."

Key used	CC between original and decrypted signal	PESQ
Key A	−0.0099	1.3352
Key B	−0.0030	0.6341
Key C	0.0021	1.0854
Key D	0.0075	1.7541

The decrypted signal for slightly modified key is noise-like encrypted signal. In order to validate the algorithm, the correlation between original and decrypted signals obtained from slightly modified keys compared to the encrypted keys is calculated. The correlation and PESQ values are tabulated in Table 6. PESQ of about 2.5 is required for good speech quality [28]. From the results, it is clear that the correlation and PESQ are very small. Hence, the algorithm gratifies the sensitivity property of the cryptosystem.

4.7. Effect of Noise. The effect of noise needs to be considered in order to evaluate the efficiency of the cryptosystem. Hence, the performance of the cryptosystem is evaluated in the presence of noise for the test speech signal "Ray 8." In order to evaluate the performance of the cryptosystem, the white Gaussian noise varying from 0 to 45 dB is added to the original signal. The effects of noise on objective metrics such as PESQ and log likelihood ratio (LLR) [26–28] are calculated for decrypted signal. The variation of PESQ and LLR with respect to different noise levels is shown in Figure 10. From

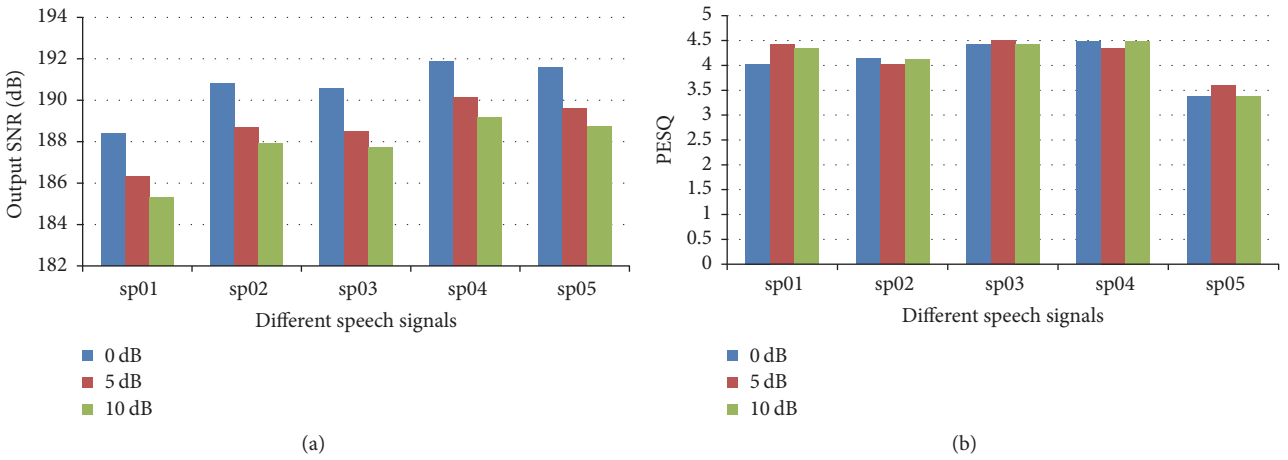


Figure 11: Speech quality metrics for the decrypted signal in the presence of babble noise: (a) SNR; (b) PESQ.

the speech quality and noise perception point of view, PESQ score above 2.5 and LLR close to zero are desirable [28, 29]. It has been observed that the decryption quality metrics are better at high SNR values which can withstand noise with low power.

Further, in order to evaluate the algorithm the clean speech sentences which are corrupted by babble noise varying from 0 to 10 dB are considered. These signals are taken from NOIZEUS database for experimentation [31]. The objective metrics such as SNR and PESQ are calculated which is shown in Figure 11. From the results it is clear that the proposed algorithm works satisfactorily. Hence, the algorithm can be used for real-time speech encryption applications.

4.8. Timing Analysis. The time required to encrypt/decrypt the plaintext depends on various factors such as configuration of the system, programming language, and operating system. The environment used for experimental findings is MATLAB 2009 on 1.88 GHz Intel CPU with 2.99 GB RAM in Windows XP Professional operating system. The average encryption and decryption time taken by the cryptosystem for a speech signal with sampling rate of 8 KHz are 59.65358 s and 27.19384 s, respectively. The cryptosystem uses dynamic DNA coding mechanism in order to increase the security which in turn impacts the speed to some extent. The existing algorithm in [5] is faster when compared to the proposed cryptosystem. However, the run time operation can be further improved with hardware as well as software optimization in order to meet the practical requirements. A suitable trade-off between the speed and the required security needs to be considered.

5. Conclusion

In this paper, a new speech encryption scheme based on chaotic maps and DNA encoding is proposed. The algorithm uses chaotic maps such as 2D-MHM and SM along with HCST. The modified Henon map has broad chaotic range over an extensive range of system parameters when compared to seed map. Further, in order to increase the security of the cryptosystem DNA encoding technology is integrated. The performance of the cryptosystem is evaluated and compared with existing algorithms. Extensive simulation results show that the proposed algorithm can encrypt different types of speech signals with a high security level and resist several attacks. The algorithm offers more security when compared with the existing algorithm. Further, the algorithm can tolerate different types of noise with high SNR. Therefore, the proposed algorithm can be used in real-time speech encryption applications, secured telephone, and narrow band radio communication.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] 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.

[2] F. J. Farsana and K. Gopakumar, "A novel approach for speech encryption: Zaslavsky map as pseudo random number generator," in *Proceedings of the 6th International Conference On Advances In Computing and Communications, ICACC 2016*, pp. 816–823, September 2016.

[3] S. B. Sadkhan and R. S. Mohammed, "Proposed random unified chaotic map as PRBG for voice encryption in wireless communication," in *Proceedings of the International Conference on Communications, Management, and Information Technology, ICCMIT 2015*, pp. 314–323, April 2015.

[4] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 16, no. 8, pp. 2129–2151, 2006.

[5] S. M. H. Alwahbani and E. B. M. Bashier, "Speech scrambling based on chaotic maps and one time pad," in *Proceedings of the 2013 1st IEEE International Conference on Computing, Electrical and Electronics Engineering, ICCEEE 2013*, pp. 128–133, August 2013.

[6] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Optics and Lasers in Engineering*, vol. 78, pp. 17–25, 2016.

[7] S. J. Sheela, K. V. Suresh, and D. Tandur, "Performance evaluation of modified henon map in image encryption," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10063, pp. 225–240, 2016.

[8] S. J. Sheela, K. V. Suresh, and D. Tandur, "Chaos based speech encryption using modified Henon map," in *Proceedings of the IEEE International Conference on Electrical, Computer and Communication Technologies*, pp. 522–529, 2017.

[9] C. Cokal and E. Solak, "Cryptanalysis of a chaos-based image encryption algorithm," *Physics Letters A*, vol. 373, no. 15, pp. 1357–1360, 2009.

[10] R. Bechikh, H. Hermassi, A. A. Abd El-Latif, R. Rhouma, and S. Belghith, "Breaking an image encryption scheme based on a spatiotemporal chaotic system," *Signal Processing: Image Communication*, vol. 39, pp. 151–158, 2015.

[11] E. Y. Xie, C. Li, S. Yu, and J. Lu, "On the cryptanalysis of Fridrichs chaotic image encryption scheme," *Signal Processing*, vol. 132, pp. 150–154, 2016.

[12] T. Head, G. Rozenberg, R. S. Bladergroen, C. K. D. Breek, P. H. M. Lommerse, and H. P. Spaink, "Computing with DNA by operating on plasmids," *BioSystems*, vol. 57, no. 2, pp. 87–93, 2000.

[13] X. Zheng, J. Xu, and W. Li, "Parallel DNA arithmetic operation based on n-moduli set," *Applied Mathematics and Computation*, vol. 212, no. 1, pp. 177–184, 2009.

[14] J. Zhang, D. Hou, and H. Ren, "Image encryption algorithm based on dynamic DNA coding and Chen's hyperchaotic system," *Mathematical Problems in Engineering*, vol. 2016, Article ID 6408741, 11 pages, 2016.

[15] M. Henon, "A two-dimensional mapping with a strange attractor," *Communications in Mathematical Physics*, vol. 50, no. 1, pp. 69–77, 1976.

[16] K.-W. Wong, "Image encryption using chaotic maps," in *Intelligent Computing Based on Chaos*, vol. 184 of *Stud. Comput. Intell.*, pp. 333–354, Springer, Berlin, 2009.

[17] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 8, no. 6, pp. 1259–1284, 1998.

[18] F. Rannou, "Numerical study of discrete plane area-preserving mapping," *Astronomy and Astrophysics*, vol. 31, pp. 289–301, 1974.

[19] B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C*, John Wiley & Sons, New York, NY, USA, 1996.

[20] X. Wang and C. Liu, "A novel and effective image encryption algorithm based on chaos and DNA encoding," *Multimedia Tools and Applications*, pp. 1–17, 2016.

[21] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Journal of Systems and Software*, vol. 85, no. 2, pp. 290–299, 2012.

[22] Q. Zhang, L. Guo, and X. Wei, "Image encryption using DNA addition combining with chaotic maps," *Mathematical and Computer Modelling*, vol. 52, no. 11-12, pp. 2028–2035, 2010.

[23] O. D. King and P. Gaborit, "Binary templates for comma-free DNA codes," *Discrete Applied Mathematics*, vol. 155, no. 6-7, pp. 831–839, 2007.

[24] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Optics and Lasers in Engineering*, vol. 84, pp. 26–36, 2016.

[25] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[26] F. Sufi, F. Han, I. Khalil, and J. Hu, "A chaos-based encryption technique to protect ECG packets for time critical telecardiology applications," *Security and Communication Networks*, vol. 4, no. 5, pp. 515–524, 2011.

[27] E. M. Elshamy, E.-S. M. El-Rabaie, O. S. Faragallah et al., "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.

[28] J. Ma, Y. Hu, and P. C. Loizou, "Objective measures for predicting speech intelligibility in noisy conditions based on new band-importance functions," *Journal of the Acoustical Society of America*, vol. 125, no. 5, pp. 3387–3405, 2009.

[29] J. F. De Andrade Jr., M. L. R. De Campos, and J. A. Apolinário Jr., "Speech privacy for modern mobile communication systems," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP*, pp. 1777–1780, April 2008.

[30] V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitution-diffusion based image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 7, pp. 3056–3075, 2009.

[31] Y. Hu and P. C. Loizou, "Subjective comparison and evaluation of speech enhancement algorithms," *Speech Communication*, vol. 49, no. 7-8, pp. 588–601, 2007.