International Journal of Engineering & Technology, 7 (4) (2018) 4550-4557

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 21271
Research paper



A new speech cryptosystem using DNA encoding, genetic and RSA algorithms

Sura F. Yousif *

Department of Chemical Engineering, College of Engineering, Diyala University, Diyala, Iraq
**Corresponding author E-mail: sura.fahmy@yahoo.com*

Abstract

A new system for speech signals encryption and decryption based on the combination of three different encryption techniques which are Deoxyribonucleic Acid (DNA) , Genetic and RSA algorithms is presented in this work. Initially, the one dimensional speech signal is divided to three equal blocks. Secondly, DCT is applied to each block to obtain coefficients of speech samples. Thirdly, each block of speech samples coefficients is encrypted using different encryption method, DNA encoding for the first block whereas Genetic algorithm and RSA algorithm are applied to the second and last blocks respectively. Finally, the three encrypted blocks are combined together to produce ciphered speech signal ready for transmission. The presented speech cryptosystem is implemented and its performance is assessed via different speech encryption and decryption quality criterions and for various speech signals. The results of experiments and comparison prove that the presented algorithm achieves good results for both encryption and decryption and it has the ability to withstand various cryptographic attacks effectively. Further, several kinds of analysis have been performed on the proposed scheme like SNR, PSNR, Correlation Coefficient, NPCR and UACI which are reach to -61.4085 dB, 6.0671 dB, 0.00031683, 99.96 % and 37.2940 % respectively. All these tests reveal that the presented cryptosystem is appropriate to be applied in communication systems for secure real time speech encryption and decryption applications.

Keywords: *Speech Encryption and Decryption; DNA Coding; Genetic Algorithm; RSA Algorithm; Security Analysis.*

1. Introduction

One of the most essential forms in human communications is speech. The speech files can be transmitted and received today over the internet because of the rapid evolution in communications technologies. These files could be accessed during communication for malicious purpose by the unauthorized users. To safeguard the speech signals content while transmission throughout any unsecured channel, cryptographic techniques are introduced. In cryptography, the speech signal is transformed from its understandable form to ambiguous form before transferring via encryption and the inverse process is utilized after reception via decryption [1, 2]. There are two sorts of encryption techniques in general which known as symmetric key encryption and asymmetric key encryption. In symmetric key encryption otherwise called private key or secret key or shared key, one key is utilized for encryption as well as for decryption processes e.g. Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Genetic Algorithm (GA). In asymmetric key encryption otherwise called public key, two distinctive keys are utilized for encryption and decryption processes. The end user on a system in this case regardless whether it is public or private possess a pair of keys: one employed for encryption and the other employed for decryption. These keys are categorized as public key and private key. Asymmetric encryption is ordinary implemented using one-way functions. Mathematically, the computation of these functions is easy in one direction but it is very hard in reverse manner. Today, factoring large prime numbers is a popular one-way function used. Multiplying two prime numbers and obtain the result is very easy but revealing the factors is very hard because there are abundant possibilities. This problem is one of the great difficulties in mathematics e.g. RSA algorithm [1], [3].

DNA encryption is one of the forefront fields in cryptography and this particular field has become the focus by many researchers currently. DNA algorithm is generally represented via the four natural DNA components namely Adenine (A), Guanine (G), Cytosine (C) and Thymine (T). DNA encryption is becoming used in cryptography because of its exclusive features like enormous storage capacity, huge parallelism and ultra-low power consumption. Leonard Adleman, a researcher in Southern California University, was the first who developed DNA computing in 1994. Adleman declared that he had resolved the seven-point Hamiltonian path problem via a small phial of DNA. Advancements have been made to this algorithm since the initial experiments of Adleman because it presents many possibilities [4], [5].

Several approaches have been presented recently by many researchers in order to encrypt and decrypt the speech signals. For instance, Elsayed et.al in 2015 [6], combined optical encryption with chaotic maps for secure digital audio communication. This audio cryptosystem involves two levels of security. Cat map or baker map is used to provide the first level of security while optical encryption based on Double Random Phase Encoding (DRPE) is used to provide the second level of security. Hala and Sundus in 2015 [7], used Hybrid Chaotic System (HCS) and Modified Overlapped Block Shuffling (MOBS) to protect the audio signals during transmission. Permutation is applied to the input audio signal after dividing it to square blocks. Then, shuffling process using Arnold transformation and Henon map is performed to each permutated block. The key matrix which employed for encrypting the shuffled blocks is generated finally by utilizing a hybrid of Arnold Cat map and Henon map. Mahmoud et.al in 2016 [8], applied

Copyright © 2018 Sura F. Yousif. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

secret keys and transform domains in order to perform the permutation and substitution operations on voice samples. Arnold cat map is employed for samples permutation while Henon map is employed for key generation which used in the samples substitution. Sathiyamurthi and Ramakrishnan in 2017 [3], contrived a method for speech signals ciphering relies on chaotic shift keying. The original speech signal is divided to four layers. Each layer is permutated then using four different chaotic maps. The mechanism of chaotic shift keying assigns Logistic map, Tent map, Quadratic map and Bernoulli's map to shuffle the speech samples for the first, second, third and last layers respectively. The final permutation process is performed by utilizing Chen map for further security. Sheela et.al in 2017 [9], connoted a new system that depends on DNA coding, hybrid chaotic shift transform (HCST) and chaotic maps for encrypting the audio signals. Two dimensional modified Henon map is used in this system to implement HCST whereas DNA technology is used to improve the system security. Narendren et.al in 2018 [5], suggested an algorithm that consists of two security layers: RSA and DNA in order to cipher speech signals. DNA technique is used to add more layer of security over RSA. The analysis of security for the introduced algorithm indicates good results.

Relying on the above literature, this work combines three different efficient techniques which are DNA encoding, Genetic algorithm and RSA algorithm for speech signal encryption and decryption in order to achieve higher security level. The current work also utilized DCT to reduce the residual intelligibility of the speech signal at encryption process as well as to enable the reconstruction of speech signal with high quality at decryption process. The encryption and decryption capabilities of speech signal for the proposed speech cryptosystem are assessed for various speech signals and through various kinds of security analysis including statistical and differential analyses which proved the proposed system ability to resist these attacks.

Section 2 introduces theory of the proposed cryptosystem including DNA coding, Genetic algorithm and RSA algorithm. The architecture of speech encryption and decryption for the proposed scheme is discussed in Section 3. Section 4 provides the security analysis and simulation results while the main conclusions are summarized in Section 5.

2. Preliminary theory of the proposed speech cryptosystem

2.1. DNA coding

DNA encryption is a bioscience technology that used to encrypt and compress the messages. It composed of four nucleotides acid bases labeled as Adenine, Thymine, Cytosine and Guanine which can be represented as A, T, C and G respectively. C joins with G and A joins with T where C and G, A and T represent the complementary pairs according to DNA sequence rules. In general, the numbers 0 and 1 are complementary in binary system. Accordingly, 01 and 10, 00 and 11 are also complementary. Hence, if the binary numbers 01, 10, 00 and 11 are coded with the four nucleotides bases, then 24 sorts of encoding combinations can be obtained but there are only 8 encoding schemes out of 24 encoding combinations can be used because they are suitable for the complementarity principle of Watson-Crick. These rules are clarified in Table 1. The simple way to transform any message to DNA sequence is to represent each letter in its binary sequence whose length is 8 and mapped each two bits to DNA four nucleotide bases whose length is 4. The DNA sequence can be inversely decoded to its binary value. For instance, if the number value is 196, then this value is transformed to its binary sequence which is 11000100. This binary sequence can be coded to DNA sequence TACA or TAGA by adopting DNA coding rules 1 or 2 respectively. The erroneous binary sequence 00111011 is obtained if wrong DNA coding rule is utilized to decipher the DNA sequence TACA, which leads to erroneous number value 59. Additionally, several algebraic and biological operations have been introduced by the researchers with the fast evolution in DNA cryptography like exclusive OR (XOR), exclusive NOR (XNOR), addition and subtraction operations. The DNA rules for XOR and XNOR operations are reported in Table 2 [4], [10]. Rule 1 is adopted in this scheme in order to encode and decode the speech signal samples. Furthermore, DNA XNOR operation is utilized in this work for speech samples encryption and decryption because as seen from Table 2, the result of XNOR operation in each row or column is distinctive.

2.2. Genetic algorithm

Based on the studies conducted by John Holland and his colleagues at the Michigan University in 1975, one of the most known evolutional algorithms has become into presence which called Genetic algorithm. Genetic Algorithm or GA is a technology utilized frequently to resolve different optimization problems approximately in computer science. It is a specific category of evolutional algorithms which employed methods inspired by evolutional biology or human evolution operations such as natural selection, inheritance, mutation and crossover (recombination). Three fundamental parameters are involved in Genetic algorithm: selection, crossover and mutation. GA goes throughout this loop subsequently till it reached some stopping criterion. The searching power of Genetic algorithm is come from two reproduction operations which are crossover and mutation.

2.2.1. Selection

Some individuals (or chromosomes) are chosen by using the selection operation from the parent population. In this operation, each chromosome is first evaluated via the fitness function to produce the convenient values which are going then to be normalized.

2.2.2. Crossover

The major technique for initiating new chromosomes is done through crossover operation which plays the mid role in Genetic algorithm. The main scheme for crossover process is executed by alternating a part of genes between two chromosomes to generate new chromosomes. Several various kinds for crossover functions are available but they are depending on what representation is utilized for the chromosomes. Single point, two point and uniform crossover operators are applied for binary string chromosomes.

2.2.3. Mutation

Mutation operation is a small random artifice occurs in the chromosome to obtain new solution that can be used to preserve the variety from one generation of genetic population to the next. This operation is analogous to biological mutation. A standard operation for mutation in binary string including inversion of bits in the chromosome, which means that 1 will mutate to 0 and vice versa [11 - 13].

2.3. RSA algorithm

RSA is an authentication and encryption technique which was designed by three researchers: Ron Rivest, Adi Shamir and Leonard Adleman who first described this algorithm publically in 1977. RSA is one of the famous public key cryptographic systems which frequently used in several cryptographic applications such as encryption of

Table 1: Eight DNA Encoding and Decoding Rules

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 2: DNA rules for XOR and XNOR operations

$\oplus$	A	C	T	G	$\odot$	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

Data blocks, digital signatures, key exchange, banking, e-commerce and e-mail security. The security of RSA is relying upon the difficulty of factoring large integer numbers to their prime integer factors which makes this technique unbreakable to anyone till now. RSA works on the principle of double keys. The public key is utilized for message encryption and it can be visible to anyone whilst the private key is utilized for message decryption and it must be kept confidential. Hence, there is no necessity to send the private key in RSA algorithm over the internet as required in symmetric cryptography. Three stages are involved in RSA operation: key generation, encryption and decryption stages.

2.3.1. Key Generation

1) Two prime integer numbers $p\ and\ q$ are randomly selected and the modulus n is computed from their product such that $n = p \times q$.
2) Euler's totient function $\emptyset$ is computed using the following formula: $\emptyset\ (n) = (p-1)(q-1)$.
3) Third integer number e is chosen such that $gcd(e, \emptyset(n)) = 1$ where $1 < e < \emptyset(n)$.
4) d is calculated from the following formula $d = e^{-1} mod\ (\emptyset(n))$.

(e, n) Represents the public encryption key while (d, n) represents the private decryption key. The numbers $d, n, p, q\ and\ \emptyset(n)$ should be kept confidential because they can be utilized for computing d.

2.3.2. Encryption

The message M is encrypted via the public key at the sender to calculate the cipher text C using Equation 1:

$$C = M^e\ mod\ n \qquad (1)$$

2.3.3. Decryption

The cipher text C is decrypted then at the receiver to recover the message M via the private key using Equation 2 [14], [15]:

$$M = C^d\ mod\ n \qquad (2)$$

3. Proposed speech cryptosystem

This work combines various efficient encryption techniques which are DNA, Genetic and RSA algorithms in order to meet the modern cryptography applications requirements with high levels of privacy, authentication and security. The overall structures of the presented speech encryption and decryption scheme are illustrated in Figs. 1 and 2 respectively.

3.1. Speech encryption

The encryption proceedings for the proposed speech cryptosystem are summarized in the following steps:
Step 1: The one dimension input speech signal of size $(M, 1)$ is divided to three equal blocks each of size $(M/3, 1)$.
Step 2: Apply Discrete Cosine Transform (DCT) to each block to obtain the speech samples coefficients blocks (Y_1, Y_2, Y_3).
Step 3: Transform the resulting coefficients from Step 2 for the first block (Y_1) to their equivalent binary matrix B_1 of size $(M/3, 8)$.
Step 4: Perform DNA encoding according to Table 1 in Section 2.1 on the binary matrix B_1 to obtain the encoding matrix B_2 of size $(M/3, 4)$.
Step 5: Generate random numbers via Pseudo Random Number Generator (PRNG), then these numbers are transformed to their equivalent binary matrix A_1 with the same size of B_1 $(M/3, 8)$.
Step 6: Perform DNA encoding according to Table 1 in Section 2.1 on the binary matrix A_1 to obtain the encoding matrix A_2 of size $(M/3, 4)$.
Step 7: Add the two matrices B_2 and A_2 according to XNOR operation rule from Table 2 in Section 2.1 to obtain the new matrix C_1 of size $(M/3, 4)$ using Equation 3:

$$C_1(i,j) = B_2(i,j) \odot A_2(i,j) \qquad (3)$$

Step 8: The matrix C_1 is then decoded according to Table 1 in Section 2.1 to obtain the binary decoded matrix C_2 of size $(M/3, 8)$.
Step 9: Transform the binary matrix C_2 to their equivalent decimal matrix to get the first encrypted speech block C_3 of size $(M/3, 1)$.
Step 10: Divide the resulting coefficients from Step 2 for the second block (Y_2) to equal blocks of size (8×8). Then, these blocks are converted to their equivalent binary matrices $L_1, L_2, \ldots, L_m$, where m is the number of blocks.
Step 11: Apply crossover operation according to Reference 9 by performing circular shift of each byte in the matrices $L_1, L_2, \ldots, L_m$ two bits to the right to obtain the new matrices $L_1', L_2', \ldots, L_m'$. After that, these binary matrices are converted to their equivalent decimal matrices.
Step 12: Add the two matrices $L_1, L_2, \ldots, L_m$ and $L_1', L_2', \ldots, L_m'$ by applying XOR operation between them to get the matrices $D_1, D_2, \ldots, D_m$ according to Equation 4:

$$\begin{aligned} D_1(i,j) &= L_1(i,j) \oplus L_1'(i,j) \\ D_2(i,j) &= L_2(i,j) \oplus L_2'(i,j) \\ D_3(i,j) &= L_3(i,j) \oplus L_3'(i,j) \\ D_m(i,j) &= L_m(i,j) \oplus L_m'(i,j) \end{aligned} \qquad (4)$$

Step 13: Apply mutation operation by transforming the matrices $D_1, D_2, \ldots, D_m$ to their equivalent binary matrices $D_1', D_2', \ldots, D_m'$, then perform NOT operation $(\neg)$ to produce the matrices $E_1, E_2, \ldots, E_m$ according to Equation 5:

$$\begin{aligned} E_1(i,j) &= \neg(D_1'(i,j)) \\ E_2(i,j) &= \neg(D_2'(i,j)) \\ E_3(i,j) &= \neg(D_3'(i,j)) \\ E_m(i,j) &= \neg(D_m'(i,j)) \end{aligned} \qquad (5)$$

Step 14: Convert the matrices $E_1, E_2, \ldots, E_m$ to their equivalent decimal matrices $E_1', E_2', \ldots, E_m'$. Then, these blocks are reconstructed to get the second encrypted speech block F of size $(M/3, 1)$.
Step 15: Perform RSA encryption on the resulting coefficients from Step 2 for the third block (Y_3) according to Equation 1 via the public key (e, n) in Section 2.3.2 to get the third encrypted speech block G of size $(M/3, 1)$ using Equation 6:

$$G(i,j) = (Y_3\ (i,j))^e\ mod\ n \qquad (6)$$

Step 16: Recombine the three encrypted blocks C_3, F and G to get the final encrypted speech signal of size $(M, 1)$.

3.2. Speech decryption

The encryption procedures are similar to the decryption procedures but the steps are applied by the recipient on the encrypted

speech signal in inverse order to acquire the decrypted speech signal which is analogous to the original one.

4. Simulation results and security analysis

Several quality metrics are used in this section in order to verify the quality of the encrypted and decrypted speech signals as well as to determine the cryptosystem immunity

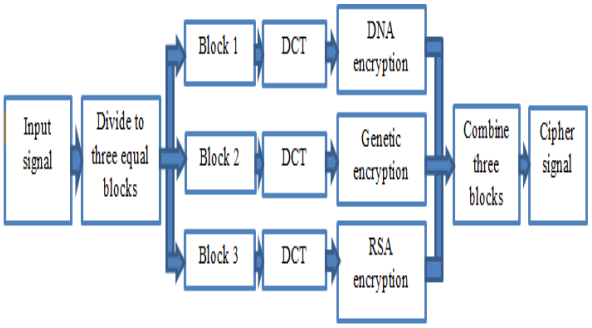


Fig. 1: Structure of the Presented Speech Encryption Scheme.

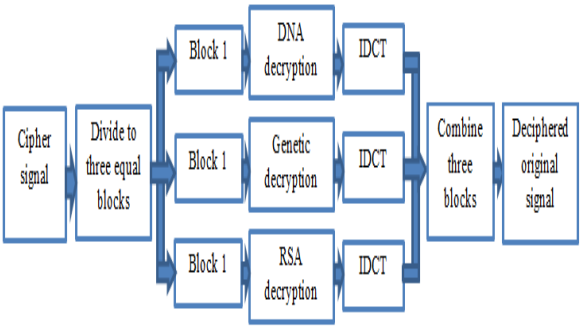


Fig. 2: Structure of the Presented Speech Decryption Scheme.

Against various cryptanalysis attacks [9]. The simulation results are implemented via Matlab (R2013a), on personal laptop of type HP (Intel CORE i3) with Windows 7. Five speech signals are selected randomly from TIMIT database, as test materials with length of 1.4150, 2.8550, 3.3150, 4.7350, 5.3950 seconds respectively and 16 KHz as sampling frequency. The waveforms of the original, ciphered and deciphered speech signals for the last test speech signal are shown in Fig. 3. By comparing Figs. 3a and 3b, it can be noticed that the ciphered speech signal produced by the presented scheme is totally different from the input speech signal. It is unintelligible, analogous to white noise and extremely uniform which means that there is no residual intelligibility in the ciphered speech signal. On the other hand, by comparing Figs. 3a and 3c, it can be noticed that the deciphered speech signal obtained from the decryption process and the original signal are identical. This indicates that the retrieved signal is of good quality and high precision.

4.1. Statistical analysis

Generally, for any cryptosystem, passing the statistical analysis is of decisive significance on cipher speech signal. In fact, a good cipher should resist any kind of statistical attack. In order to manifest the security of the presented speech cryptosystem, the following statistical are executed.

4.1.1. Histogram analysis

A histogram is a schematic representation of the tabulated intensity of data. Histogram test is applied to the proposed scheme to assess its immunity against statistical attacks [6]. The histogram of input and ciphered speech signals achieved by the presented system for the last test speech signal are shown in Fig. 4. It is obvious from Fig. 4b that the histogram of the ciphered speech signal is completely different from that of the input signal and it is reasonably uniform which implies good encryption result. Thus, the proposed scheme does not supply any original data and can withstand the statistical analysis.

4.1.2. Correlation coefficient analysis

One of the most common statistical measurements which utilized to determine the quality of encryption in speech cryptosystem is Correlation Coefficient or CC. If the value of CC is close to zero, this implies that the relationship between the original and the ciphered speech signals is very weak. Otherwise, if the value of CC is close to one, this means that the relationship between the original and the decrypted or recovered speech signals is very strong. This measure can be calculated as shown in Equations 7 and 8 [3], [10]:

$$CC = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{\sum_{i=1}^{L}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{L}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{L}(y_i - E(y))^2}} \quad (7)$$

Where

$$E(x) = \frac{1}{L}\sum_{i=1}^{L} x_i \quad (8)$$

Where $cov(x, y)$ represents the covariance between the original and ciphered speech signals x *and* y respectively, $E(x)$ represents the mean and L represents the number of speech samples utilized in calculations. The values of

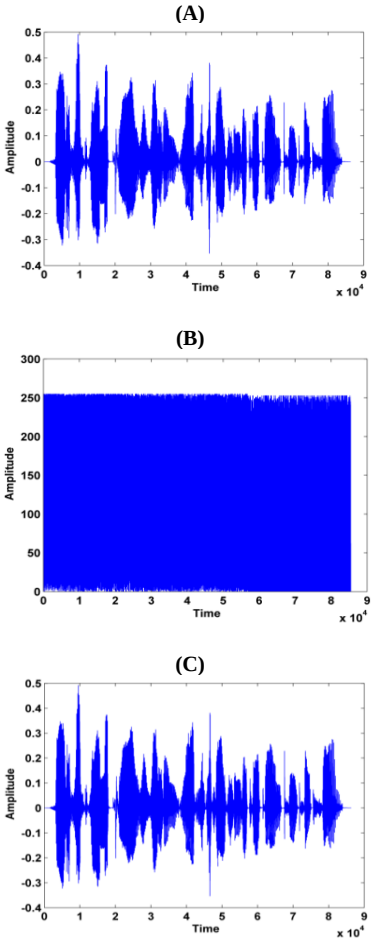


Fig. 3: (A) Original Speech Signal, (B) Ciphered Speech Signal, (C) Deciphered Speech Signal.

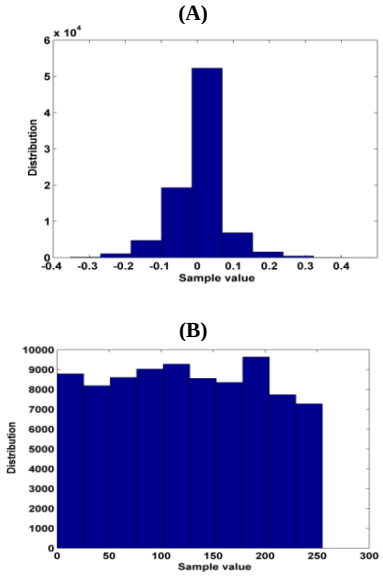


Fig. 4: (A) Histogram of Original Speech Signal, (B) Histogram of Ciphered Speech Signal.

Correlation coefficients between the original and ciphered speech signals for the five test speech samples are tabulated in Table 1 whereas the distribution of correlation coefficients between the samples in original and ciphered speech signals is plotted in Fig. 5. It can be observed from the results in this table, that the values of correlation between similar samples in the input and ciphered speech signals achieved by the presented cryptosystem are very low (close to zero). Moreover, the distribution between samples of the ciphered signal in Fig. 5 is fairly uniform which indicates the good quality of encryption process. On the other hand, the values of correlation coefficients between the original and recovered speech signals are illustrated in Table 2. From this table, it can be noticed that the values of correlation between the original and recovered speech signals are very high (one) which indicates the good quality of decryption process. Thus, the proposed cryptosystem is capable of tolerating the statistical analysis. The correlation coefficient comparison of the proposed scheme with other related schemes for the last test speech file in both encryption and decryption cases is provided in Table 3. This table points out that the correlation coefficient generated by the presented cryptosystem is closer to zero than other encryption schemes which reveals that it can resist the statistical analysis better. Additionally, the correlation coefficient results in decryption is better when compared with existing schemes in almost all cases which implies that the presented method can recover the original speech signal without any loss of information.

4.1.3. Signal to noise ratio (SNR)

SNR can be defined as the rate of SNR values for short frames in the output speech signal. It is an ideal estimator to measure the quality of the reconstructed speech signal as well as the residual intelligibility of the ciphered speech signal. This measure is computed as shown in Equation 9:

$$SNR = 10 * log10 \frac{\sum_{i=1}^{L} x_i^2}{\sum_{i=1}^{L} [x_i - y_i]^2} \quad (9)$$

Where x represents the input speech signal while y represents the encrypted or decrypted speech signal. If the value of SNR is low, then the noise level in the ciphered speech signal is high while if the value of SNR is high, then the quality of the decrypted or retrieved speech signal is high [7, 16]. The values of SNR obtained by the proposed method for the test speech signals in the case of encryption and decryption are represented in Tables 1 and 2 respectively. It is clear from Table 1 that all the ciphered speech files are characterized by low value of SNR which indicates low residual intelligibility while the retrieved speech signals in Table 2 are characterized by high value of SNR which manifests high residual intelligibility. In addition, the retrieved speech signals are of good quality and high precision. The SNR comparison of the proposed algorithm with other related approaches for the last test speech signal in both encryption and decryption cases

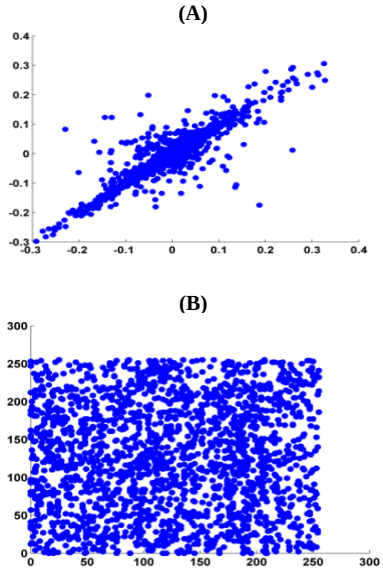


Fig. 5: Distribution of Correlation Coefficient in the (A) Original Speech Signal, (B) Ciphered Speech Signal.

is shown in Table 3. This table clarifies that SNR values produced by the proposed algorithm are much lower in encryption process and much higher in decryption process than the existing approaches which reveals that the presented algorithm quality of encryption and decryption is better.

4.1.4. Peak signal to noise ratio (PSNR)

PSNR represents the proportion between the maximum power in the original speech signal and the power in the encrypted or decrypted speech signal. PSNR is utilized to assess the quality of encryption and decryption processes for the speech cryptosystem. This measure can be obtained as shown in Equation 10:

$$\mathrm{PSNR} = 10 \times \log_{10} \frac{\mathrm{nX}^2}{\|\mathrm{x}-\mathrm{k}\|^2} \quad (10)$$

Where n represents the length of the encrypted or decrypted speech signals, X represents the value of maximum absolute square of the input signal x while $(x - k)$ represents the difference energy between the original and encrypted or decrypted speech signals [17]. Lower values of PSNR demonstrate the higher quality of encryption whereas the higher values of PSNR imply the higher quality of decryption. The PSNR values for the test speech files obtained via the presented technique in the case of encryption and decryption are reported in Tables 1 and 2 respectively. The results in Table 1 point out that PSNR values for encrypted speech signals are very low which means good encryption quality whereas the results in Table 2 indicate that PSNR values for decrypted speech signals are very high which manifests good reconstruction quality.

4.2. Differential analysis

The least significant bit in each sample is reversed and an altered speech signal is obtained. Two encrypted speech signals are produced by ciphering the input and altered speech signals via the same key. Then, these two encrypted speech signals are compared by utilizing two common criterions: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). These two criterions are given in Equations 11, 12 and 13:

$$\mathrm{NPCR} = \frac{\sum_i D(i)}{l} \times 100\% \quad (11)$$

$$\mathrm{UACI} = \frac{1}{l}\left[\sum_i \frac{|x_1(i) - x_2(i)|}{255}\right] \times 100\% \quad (12)$$

$$D(i) = \begin{cases} 0 & \text{if } x_1(i) = x_2(i) \\ 1 & \text{if } x_1(i) \neq x_2(i) \end{cases} \quad (13)$$

Where x_1 and x_2 represent the two encrypted speech signals which corresponding to two original speech signals with changing one sample only and l represents the speech vector length. The optimum values are 100% and 33.3% for NPCR and UACI respectively [3], [18]. The NPCR and UACI values obtained via the proposed work for different speech files are listed in Table 1. It can be seen from this table that all values of NPCR and UACI are extremely near to the optimum values. Hence, the proposed speech cryptosystem can withstand the differential analysis.

4.3. Spectrogram analysis

A spectrogram is a visional representation of the frequencies spectrum as they alter with time in the speech signal [6, 8]. The spectrograms of the original, ciphered and deciphered speech signals produced by the presented cryptosystem are presented in Fig. 6. It is easy to notice by comparing Figs. 6a and 6b that the ciphered signal spectrogram is totally different from the original signal spectrogram which denotes that the encryption process is of high quality. Furthermore, it is obvious by comparing Figs. 6a and 6c that the spectrograms of the deciphered and original signals are identical which demonstrates that the decryption process is of high quality.

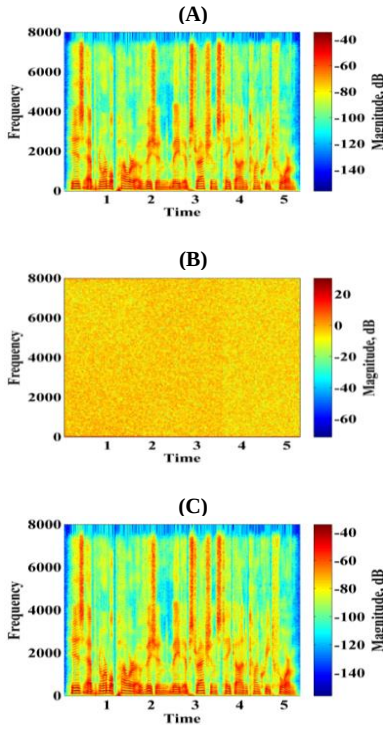


Fig. 6: Spectrograms of (A) Original Speech Signal, (B) Ciphered Speech Signal, (C) Deciphered Speech Signal.

4.4. Elapsed time analysis

The elapsed time is the time required for encrypting and decrypting the speech signal. This time relies on several factors which are used in algorithm implementation such as the programming language, operating system used and its configuration. It is also relies on the size of the speech file. The speed of encryption process is high when the elapsed time is low [2], [6], [9], [16]. For experiential findings, the environment utilized is Matlab (R2013a) on 2.40 GHz for CPU, Intel (R) Core (TM) i3 and 3.90 GB for RAM with Windows 7 as operating system. The elapsed time for encryption and decryption processes recorded by the presented speech cryptosystem and for the test speech signal files of sampling frequency 16 KHz are explained in Fig. 7. From the results in this figure, it is evident that when the size of speech signal increased, the time of encryption and decryption is also increased. . For the last speech signal of length 5.3950 seconds, the proposed scheme requires only 18.877647 seconds and 17.123279 seconds for both encryption and decryption processes respectively. This revealed that the suggested technique can be utilized efficiently in real time speech cryptosystems.

Table 1: Quality Metrics Values for Encrypted Signal

Signal name	SNR (dB)	PSNR (dB)	NPCR	UACI	CC
Signal 1	-61.4085	6.0671	99.96	37.2940	3.1683×10^{-4}
Signal 2	-62.7880	6.0823	99.96	37.2066	-1.6828×10^{-4}
Signal 3	-62.5135	6.1119	99.96	37.0317	4.8035×10^{-4}
Signal 4	-64.8471	6.0914	99.98	37.1593	-7.2535×10^{-4}
Signal 5	-65.4124	6.1153	99.97	36.9895	-6.2950×10^{-4}

Table 2: Quality Metrics Values for Decrypted Signal

Signal name	SNR (dB)	PSNR (dB)	CC
Signal 1	217.0701	284.5457	1
Signal 2	215.6531	284.5233	1
Signal 3	215.9138	284.5391	1
Signal 4	213.5800	284.5185	1
Signal 5	212.9712	284.4989	1

4.5. Noise effect on the decrypted speech signal

The noise effect is an important issue that needs to be considered in order to assess the speech cryptosystem efficiency. Therefore, the speech cryptosystem performance is assessed by adding white Gaussian noise

Table 3: Comparison of Correlation Coefficient and SNR Values with Other Schemes

Correlation Coefficient comparison							
Scheme	Ref. 3	Ref. 6	Ref. 7	Ref. 8	Ref. 16	Ref. 19	Proposed scheme
CC Encryption	0.0233	0.0051	-0.0023	-0.00118	-0.0014	-0.009221	-0.0006295
CC Decryption	0.999	-	1	1	-	0.992882	1
SNR comparison							
Scheme	Ref. 1	Ref. 7	Ref. 8	Ref. 9	Ref. 16	Proposed scheme	
SNR (dB) Encryption	-3.0013	-11.7794	-41.05	-	-13.3015	-65.4124	
SNR (dB) Decryption	-	63.069	-	193.6586	30.2338	212.9712	

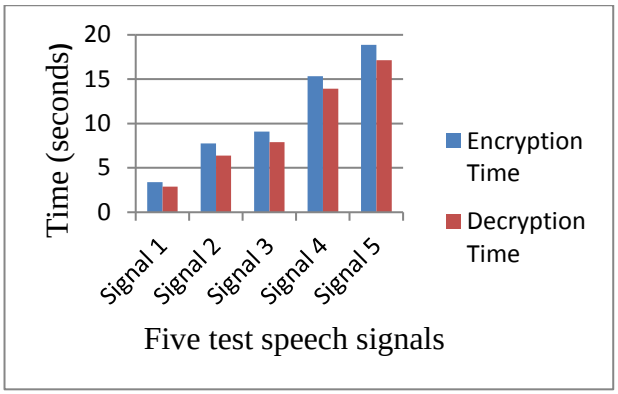


Fig. 7: Elapsed Time of Encryption and Decryption for the Test Speech Signals.

of various power levels to the last test speech signal in the decryption case [9], [19]. The noise effects on the SNR, PSNR and CC measures are carried out in the noise presence at different SNR values that vary from 0 dB to 50 dB. The relations between SNR, PSNR and CC, and SNR for the proposed scheme are illustrated in Fig. 8. From the results in this figure, it is obvious that the values of objective quality measurements at high values of SNR are better. So, the presented cryptosystem has the ability to withstand the noise effect with low power.

5. Conclusions

Assuring the accessibility, reliability, confidentially and

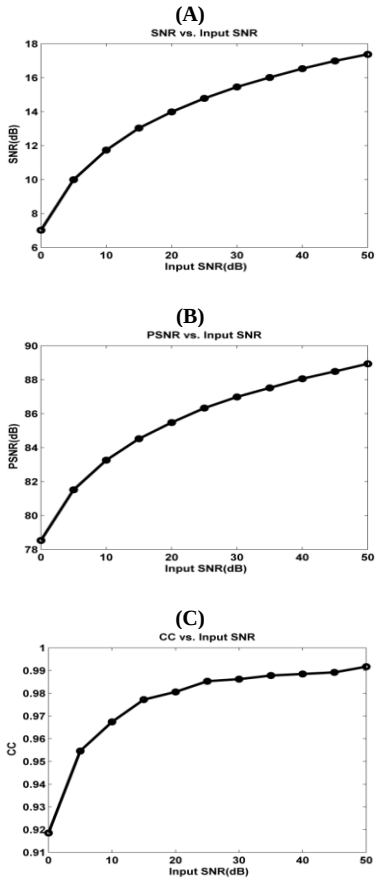


Fig. 8: Speech Quality Measures in the White Gaussian Noise Presence for Decrypted Signal (A) SNR, (B) PSNR, (C) CC.

secrecy of information is the main concerning of speech security. Speech security aims to safeguard speech cryptosystems from modification, extermination, disruption, unauthorized access and illegal usage over the network. Thus, a new cryptosystem for speech signals encryption and decryption that depends on three different techniques is presented in this work. The original speech signal is divided into three equal blocks. Then, DNA coding technology along with Genetic algorithm and RSA algorithm are utilized to encrypt the coefficients of speech samples of the first, second and third blocks respectively after applying DCT into each block. The security of speech signal is improved by combining these efficient technologies which makes the cryptanalysis of the proposed scheme is a hard task for the attacker. The presented speech cryptosystem is implemented and its performance is assessed through the security analysis. Through comprehensive simulation results for various test speech signals, it can be verified that the proposed scheme can encrypt the speech signal at high degree of security so that the encrypted signal is very noisy and unintelligible. Otherwise, the decrypted speech signal is very analogous to the original one which indicates the high quality of the reconstruction process and further it has the ability to withstand various cryptographic analyses such as statistical and differential analyses. Results demonstrates that the new approach is robust, resilient and convincing enough as compared to other existing approaches. Moreover, the suggested method can endure Gaussian noise with high levels of SNR while preserving good quality of decrypted speech signal. All these properties including fast speed of encryption and decryption endorse that the proposed system can be employed in applications such as secured telephone communication, narrowband radio systems, real time speech encryption and decryption systems as well as secure transferring of confidential data throughout the Internet.

References

[1] A. Mostafa, N. F. Soliman, M. Abdalluh, and F. E. Abd EI-samieD, Speech Encryption Using Two Dimensional Chaotic Maps, IEEE, (2015), 235-240, available on line: https://ieeexplore.ieee.org/document/7416354.

[2] D. Slimania and F. Merazka, Encryption of Speech Signal with Multiple Secret Keys, International Conference on Natural Language and Speech Processing, Procedia Computer Science 128, (2018), 79–88, available on line: https://www.sciencedirect.com/science/article/pii/S1877050918302242. https://doi.org/10.1016/j.procs.2018.03.011.

[3] P. Sathiyamurthi and S. Ramakrishnan, Speech Encryption Using Chaotic Shift Keying for Secured Speech Communication, EURASIP Journal on Audio, Speech, and Music Processing, Springer, (2017), 1-11, available on line: https://asmp-eurasipjournals.springeropen.com/articles/10.1186/s13636-017-0118-0.

[4] A. Agrawal, A. Bhopale, J. Sharma, M. S. Ali, and D. Gautam, Implementation of DNA Algorithm for Secure Voice Communication, International Journal of Scientific & Engineering Research, Vol. 3, Issue 6, (2012), 1-5, available on line: https://www.ijser.org/researchpaper/Implementation-of-DNA-algorithm-for-secure-voice-communication.pdf.

[5] Narendren S, Y. B. Yathish, and C. Mohan B, A Cryptosystem using Two Layers of Security - DNA and RSA Cryptography, International Journal of Pure and Applied Mathematics, Vol. 119, No. 7, (2018), 217-224, available on line: https://acadpubl.eu/jsi/2018-119-7/articles/7a/23.pdf.

[6] E. M. Elshamy, E. 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, Springer, 2015, available on line: https://link.springer.com/article/10.1007/s10772-015-9279-3.

[7] H. B. Abdul Wahab and S. I. Mahdi, Modify Speech Cryptosystem Based on Shuffling Overlapping Blocks Technique, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. 4, Issue 2, (2015), 70-75, available on line: http://www.ijettcs.org/Volume4Issue2/IJETTCS-2015-03-20-41.pdf.

[8] M. F. Abd Elzaher, M. Shalaby, and S. H. El Ramly, Securing Modern Voice Communication Systems using Multilevel Chaotic Approach, International Journal of Computer Applications (0975 – 8887), Vol. 135, No.9, (2016), 17-21, available on line: http://adsabs.harvard.edu/abs/2016IJCA..135i..17M.

[9] 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, (2017), 1-12, available

on line: http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwj6wcrF9prfAhWysqQKHSDNDXIQFjABegQIC-BAC&url=http%3A%2F%2Fdownloads.hindawi.com%2Fjournals%2Fjcnc%2F2017%2F2721910.pdf&usg=AOvVaw0jIfU77c-BacUFy9yhXyz-.

[10] X. Li, C. Zhou, and N. Xu, A Secure and Efficient Image Encryption Algorithm Based on DNA Coding and Spatiotemporal Chaos, International Journal of Network Security, Vol. 20, No.1, (2018), 110-120, available on line: http://ijns.femto.com.tw/contents/ijns-v20-n1/ijns-2018-v20-n1-p110-120.pdf.

[11] S. Arunpandian, and K. Mahesh, Image Enciphering Using Genetic Algorithm, International Journal of Engineering and Technology (IJET), Vol. 9, No. 5, (2017), 3570-3574, available on line: http://www.enggjournals.com/ijet/docs/IJET17-09-05-311.pdf. https://doi.org/10.21817/ijet/2017/v9i5/170905311.

[12] R. Choudhary and P. Abrol, Genetic Algorithm Based Image Cryptography to Enhance Security, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 6, Issue 6, (2017), 873-878, available on line: http://ijarcet.org/wp-content/uploads/IJARCET-VOL-6-ISSUE-6-873-878.pdf.

[13] R. Jhingran, V. Thada, and S. Dhaka, A Study on Cryptography using Genetic Algorithm, International Journal of Computer Applications (0975 – 8887), Vol. 118, No. 20, (2015), 10-14, available on line: https://pdfs.semanticscholar.org/2ea1/89f876f6167ceca1e064404bcf6d67f51a3e.pdf.

[14] R. B. Vyavahare, A. J. Bajaj, H. P. Fuse, and P. K. Patil, Study of Secure Data Transmission Using Audio File, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 2, (2015), 146-149, available on line: https://ijarcce.com/wp-content/uploads/2015/03/IJARCCE3B.pdf. https://doi.org/10.17148/IJARCCE.2015.4232.

[15] A. E. T. El_Deen, E.A. El-Badawy, and S. N. Gobran, Digital Image Encryption Based on RSA Algorithm, IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), Vol. 9, Issue 1, (2014), 69-73, available on line: https://pdfs.semanticscholar.org/e0ee/c327cec4aac470a562c2d35dbf1bdc88e93c.pdf.

[16] 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), IEEE, (2013), 128-133, available on line: https://ieeexplore.ieee.org/document/7759928.

[17] S. M. Hameed, H. A. Sa'adoon, and M. Al-Ani, Image Encryption Using DNA Encoding and RC4 Algorithm, Iraqi Journal of Science, Vol. 59, No.1B, (2018), 434-446, available on line: http://oaji.net/articles/2017/6146-1524128349.pdf.

[18] S. Chakraborty, A. S., M. Roy, and K. Mali, A Novel Lossless Image Encryption Method using DNA Substitution and Chaotic Logistic Map, International Journal of Security and Its Applications, Vol. 10, No. 2, (2016), 205-216, available on line: https://www.earticle.net/Article/A269974. https://doi.org/10.14257/ijsia.2016.10.2.19.

[19] S. N. Al Saad and E. Hato, A Speech Encryption based on Chaotic Maps, International Journal of Computer Applications (0975 – 8887), Vol. 93, No. 4, (2014), 19-28, available on line: https://pdfs.semanticscholar.org/9bec/6c202e227ae9245fcd21c321ecbb9020d4b4.pdf.