Hide Medical Images in a Speech Signal using DNA Coding and Fuzzy C-Means

1st Iman Qays Abduljaleel
dept. Computer Science
College of Computer Science and Information Technology,
University of Basrah
Basrah, Iraq
iman.abduljaleel@uobasrah.edu.iq

2nd Amal Hameed Khaleel
dept. Computer Science
College of Computer Science and Information Technology,
University of Basrah
Basrah, Iraq
amal.khaleel@uobasrah.edu.iq

***Abstract*—Medical images possess great privacy, as the patient's information must be completely confidential if it is transferred from one hospital to another via a hospital intranet or the internet to take medical consultations by specialized doctors. This paper presents a safe new method to transfer medical images by hiding them within a speech signal file, and this is done at three levels: First, a scrambling algorithm proposal to ensure a change in the original medical image based on the binary representation of the image values and using the Zaslavsky map, the second level is encryption the scrambled image relying on DNA coding and a series of keys generated by a proposed hybrid algorithm based on (Tinkerbelle map and 3D Hénon) that provided us with good image distortion and provided difficulty in retrieving it by any intruder. The last level is to hide the contents of encrypted medical images in a speech signal depending on (integer wavelet transform and LSB algorithm), then using the proposed algorithm based on (fuzzy c-means clustering algorithm and short-time energy) to determine the locations of speech to hide in it. The results of this paper showed that using statistical measures of hiding and encryption were good in maintaining the confidentiality of medical image information compared to previous researches. Consequently, the use of encryption and hiding techniques together has provided double protection against the problems of malicious manipulation and privacy leakage on the internet as well as lack the hospital's intranet to security tools.**

Keywords—speech signal, medical image, Chaotic map, DNA coding, fuzzy c-means clustering

I. INTRODUCTION

Applications for telemedicine are particularly vulnerable to attacks of cybersecurity that have significant effects on credibility and authentication. Telemedicine, however, can be useful to humans in areas that are isolated and remote, where it is not possible for doctors to offer immediate treatment [1].

Audio steganography is a method where secret knowledge is hidden in an innocent audio cover. The most difficult method is encoding hidden messages in audio since the human auditory system (HAS) has such a wide range that it can listen. The HAS is experiencing an unusual phenomenon known as the masking effect which states that another type of sound affects the hearing threshold of one type of sound. Because of this property, some data within an audio file be concealed without being found [2] [3].

Medical images form essential components of medical diagnostic techniques, as they provide non-invasive methods to analyze anatomical cross-sections of internal organs. Medical images data are considered one of the most important and sensitive data in the area of information security. Medical image encryption plays an important role in solving the confidentiality problems around telemedicine applications. Sending medical images data over the network needs a robust encryption algorithm to be resistant to cryptographic attacks. When the medical image pixels are scrambled and encrypted using different methods, it is prevents interference and the unauthorized use of medical data [4].

Encrypting medical images is important to keep data confidential, but hiding increases the level of security and protection. We used the speech signal to hide in our research. Since it contains many frequencies that fall in close range and any change in them leads to distortion. Where the special characteristics of the sound itself, namely short-time energy, were relying on and adopted in a particular method to create a secret key that could not be repeated or revealed even if the same speech clip was recorded due to the changing characteristics of the sound.

The remainder of the paper is organized as follows: presents in section II related work. The proposed work is outlined in section III. Section IV explains the experimental results & discussion. The paper concludes with Section V.

II. RELATED WORK

Medical data hiding is one of the most sensitive and attracts tremendous attention from the academic community across the globe. There are different methods used in the hiding and encryption of data in an audio file.

In encryption methods, Weijia et al. [5], presented an algorithm for medical image data encryption using edge maps or fuzzy edge maps derived from a source image (i.e. source is any image). The method consists of three parts: decomposition of the bit-planes, random sequence generators, and permutation. The proposed algorithm possesses a significantly broad key space and high key sensitivity to secure different types of medical images and facilitate safety efficiency with a machine-friendly binary system. Parthasarathi and Shreekala [6], Introduced an algorithm that is a simple enhancement of steganographic algorithms using specific methods to achieve minimum predictive error distortion and data size overhead. This method is based on the related prediction error and the difficulty in managing the phase of nonlinear quantization. Hanisha et al. [7], offered an audio steganography technique and encrypting it with a unique key consisting of a 10-digit number within the speech

978-1-7281-9169-0/20/$31.00 ©2020 IEEE
DOI 10.1109/AiCIS51645.2020.00029

signal. The data embedded in the frame samples of the LSB and the unique key added to the stenographic signal for better safe transmission, thereby reducing the impact on the retrieved signal quality.

In steganography methods, Dhandapani and Buvaneswari [8], proposed three steganography techniques which embed a bit stream of the message and effectively extract the hidden secret message without using the original cover video in the coefficients of the IWT, DWT and using the LBP technique to form stego-video file. They have applied suggested algorithms to grayscale and color images. Dalia et al. [9], presented a symmetric cryptosystem that relies on two distinctive non-consecutive chaotic diffusion phases and one DNA scrambling phase between the image being transmitted, and the key is used to increase the difficulty of the connection. These phases allow more robustness of the proposed image encryption scheme against cipher image attacks. Firas et al. [10], proposed a data hiding method using an integer lifting wavelet transformation based on DNA coding using the key extracted from the cover image to ensure total data reversibility. The generated DNA sequence is used to create the key to encrypt the hidden data and to choose the pixels in HL, LH, HH sub-bands to hide in them. Roayat et al. [11], suggested the two-phase steganography and cryptography scheme. In the first phase, hiding the patient's medical image data used the LSB technique. In the second phase, the medical image was encrypted using DNA encoding and a new HST map incorporating Hénon and ten maps to generate high random chaotic series.

III. PROPOSED METHOD

In the proposed method, we introduce three levels: Firstly, a scrambling algorithm using the Zaslavsky map. Secondly, encryption relying on DNA coding, Tinkerbelle map, and 3D Hénon. The last level is to hide a medical image encrypted in a speech signal depending on the integer wavelet transform, LSB algorithm, fuzzy c-means clustering, and short-time energy. The details of these algorithms used in the proposed method are mentioned in section (A) and the algorithms of the three levels of the proposed method are explained in section (B) as follows:

A. Basic algorithms

1) Zaslavsky map

The Zaslavsky map is a generator of the pseudorandom bit. This Map is a nonlinear, discrete-time system that produces dynamic behavior. It constitutes a significant part of the encryption algorithms. Zaslavsky's map is used to mask the sample of the data in order to create diffusion. The Zaslavsky map is defined as [12] [13] [14]:

$$\begin{cases} x_{n+1} = mod\,(\,x_n + v(1+\mu\,y_n\,) + \varepsilon\,v\,\mu\,cos\,(2\,\pi x_n), 1) \\ y_{n+1} = e^{-c}\,(y_n + \,cos(2\pi x_n)) \end{cases} \quad (1)$$

Where, v, c, ε are control parameters and e is exponentiation, and $\mu = \frac{1-e^{-c}}{c}$.

The key set for the Zaslavsky map is $\{x_0, y_0, v, c, \varepsilon\}$.
In our paper, we used: x_0=0.12, y_0=0.13, v=0.2, c=5, ε= 9.

2) DNA coding

DNA coding is the method of encrypting data based on molecular DNA. Because DNA has a massive capacity for information, it can be used to store a large amount of information. DNA computing is a modern type of molecular biology-based computation and simulation of the biomolecular structure of DNA. DNA refers to a nucleic acid that carries living organisms' genetic data. A sequence of DNA consists of four separate basic nucleotides, called Adenine, Cytosine, Thymine, and Guanine (i.e., A, C, T, and G), but the pairing is allowed just between A and T and C and G only. The four components A, C, T, G are encoded to 00, 10, 11, and 01. We can get 24 forms of encoding methods, but in the software the pairing rules have to be followed, which A bases have to be paired with T and C have to be paired with G, because only eight types (R.1,…,R.8) of encoding are efficient.

The rules (R) for DNA coding are summarized in Table 1 [15] [16] [17].

Table 2 shows the complement results of basic nucleotides whereas Table 3 shows the subtraction results of DNA where if (A=01) subtracts of (A=01), the result is (C=00), etc. [15] [16].

TABLE 1. DNA CODING RULES

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

TABLE 2. DNA COMPLEMENTARY

Basic Nucleotides	**Binary Value**
A	01
C	00
T	10
G	11

TABLE 3. DNA SUBTRACTION

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

3) Tinkerbelle map

Tinkerbell map used to generate Random numbers to hide the original data in order to omit the true meaning of the original speech signal. Tinkerbell map is a chaotic two-dimensional map displaying nonlinear dynamic behavior in a discrete-time. This map introduces deterministic chaos to initial parameters and noise (Pseudo-Random Numbers).

The mathematical equations for the Tinkerbell map are mentioned by [12] [14].

$$\text{Tinkerbell map} = \begin{cases} x_{n+1} = x_n^2 - y_n^2 + ax_n + by_n \\ y_{n+1} = 2x_n y_n + cx_n + dy_n \end{cases} \quad (2)$$

Where x_n, y_n are current chaotic values; x_{n+1}, y_{n+1} are next chaotic values; a, b, c, and d control parameters.
In our paper, we used: x_0=-0.1, y_0= 0.3, a= 0.9, b=-0.6013, c=2.0, d=0.5

4) Hénon map

The Hénon map is a nonlinear and discrete-time system that was introduced by Michel Hénon to provide dynamical chaotic behavior. The Hénon map is periodic and non-convergent, therefore it contains excellent pseudo randomness and unpredictability [18] [19] [20].

$$\text{Hénon map}(3D) = \begin{cases} x_{n+1} = a - x_n^2 - bz_n \\ y_{n+1} = x_n \\ z_{n+1} = y_n \end{cases} \quad (3)$$

Where, a, b are state variables (two bifurcation parameters (a > 0 & b > 0, x_n^2 is seed map.
In our paper, we used: a=1.6, b=0.5, x_0=0, z_0=0

5) Integer wavelet transform

Integer wavelet transform (IWT) is a type of wavelet transform which maps integer data set with another integer data set and mainly used for signaling techniques. IWT has the important property that its coefficients have the same dynamical range as the original signal. The IWT domain has an advantage over other frequency domain steganography techniques, thus providing good perceived quality and robustness [21] [22].

Haar wavelet transform can be calculated as follows [23]:

$$s_{1,n} = \frac{(s_{0,2n} + s_{0,2})}{2} \quad (4)$$

$$d_{1,n} = s_{0,2n} - s_{0,2n} \quad (5)$$

Where $S_{i,1}$ is the n^{th} low frequency; $d_{i,1}$ is the high frequency at the i^{th} level.
The result of the Haar wavelet transform in (4) and (5) is not an integer, therefore it recalculates using these steps as follows:

$$d_{1,n} = s_{0,2n+1} - s_{0,2n} \quad (6)$$

$$s_{1,n} = s_{0,2n} + d_{1,\frac{n}{2}} \quad (7)$$

The inverse transform can be calculated as follows:

$$s_{0,2n} = s_{1,n} - d_{1,\frac{n}{2}} \quad (8)$$

$$s_{0,2n+1} = d_{1,n} + s_{0,2n} \quad (9)$$

6) *The least significant bit*

The least significant bit (LSB) method is a widely used spatial domain method and is often used for audio steganography. LSB is used to cause more distortion in the cover file embedding [3] [8].

7) Fuzzy C-means

Clustering algorithms are considered to be a good technique for dealing with the similarity and uncertainty of the image, which groups pixels into different clusters based on particular criteria. Fuzzy C-means (FCM) is an algorithm based on the fuzzy theory that allows the element to belong to multiple classes with varying memberships.
The modified FCM algorithm is a non-membership function to generate an intuitional fuzzy set and a mechanism of determining initial clustering centers based on grayscale characteristics. Details of fuzzy C means algorithm can be found in [24].

B. Algorithms of the proposed method

Suggested algorithm to hide encrypted medical images in speech signal file
It consists of three levels as follows:

1) Scrambling algorithm

Input: gray medical image
Output: scrambled medical image
The working mechanism as follows (it shows in Fig. 1):

- Open the gray medical image
- Convert the gray image matrix to a one-dimensional vector
- Convert the vector values of the gray image to values in binary representation, as each symbol expresses it in 8 bits, and save the values in a new vector (contents are either 0 or 1).
- Divide the binary symbols into two equal halves, then work on the following
  a) Read two symbols from the end of the second half, then work to rotate the symbols and save them in the new file
  b) Reading two symbols from the beginning of the first half and saving them directly in the new file
  c) Completion of these steps (a, b) until the file is completely finished
- Generate a key string using the Zaslavsky map with a length equal to the number of symbols in the binary vector.
- Arrange the keys in ascending order, keeping the original location of each key before arranging
- Rearrange the bits of the image file, depending on the order of the keys
- Convert the binary vector to decimal value, and then convert the decimal vector to a two-dimensional matrix that its dimensional is equal to the dimensions of the original image
- Save the resulting image after the scrambling to using for the next stage (image encrypting).

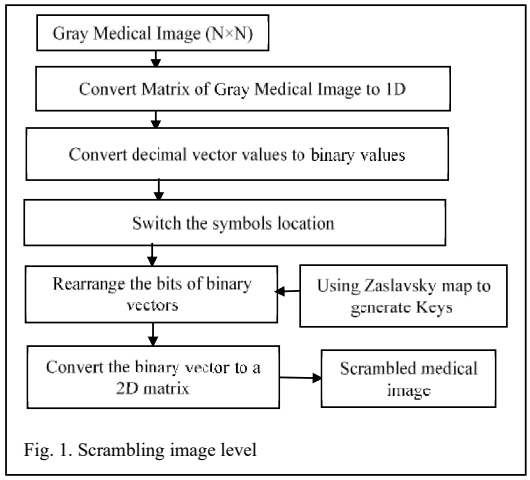


Fig. 1. Scrambling image level

2) Encrypting Image algorithm

Input: scrambled medical image
Output: encrypted medical image
The working mechanism as follows (it shows in Fig. 2):

- Read the gray image array and convert the array to a one-dimensional vector, then convert each value in it from decimal to binary representation
- Use DNA coding to convert the bits of the binary file into a DNA representation
- Generate a key chain using (Tinkerbell map and 3D Hénon map) to create a hybrid key chain with a length equal to the number of symbols in the binary representation of the vector of image (i.e, the generated keys are in binary representation (0 or 1)).
- Use DNA coding to convert the bits of the keys file into a DNA representation
- According to the complementing Table 2, make a comparison between the values of the medical image vector and the values of the keys file after converting them to DNA format in order to encrypt the medical image.
- Convert the resulting file after using the DNA format to binary representation, to restore the symbolic values in their binary encoded form
- Convert values from DNA format to values (zero and one) using the DNA subtraction Table 3.
- Convert symbols from their binary representation to decimal, then convert the resulting vector to a two-dimensional array with a size equal to the size of the original image matrix.
- Save the resulting 2D array as an encrypted image.

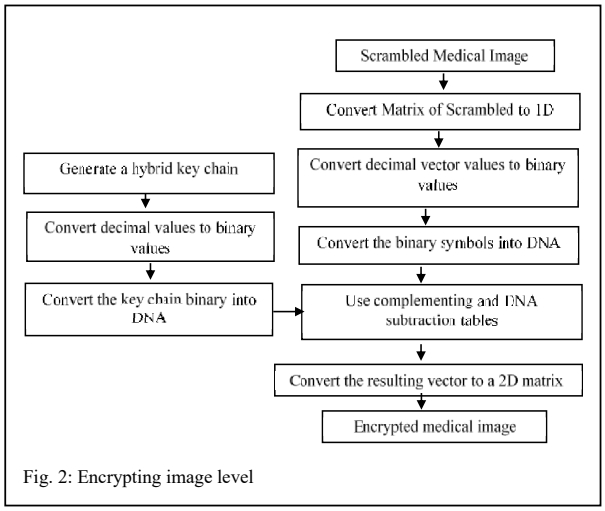


Fig. 2: Encrypting image level

3) Hiding algorithm

It is used to hide an encrypted medical image in a speech signal file
Input: encrypted medical image, speech signal file
Output: speech signal file hiding an encrypted image
The working mechanism as follows (it shows in Fig. 3):

- Read the encrypted medical image and convert it from a two-dimensional array to a one-dimensional vector
- Convert all vector values from decimal to binary representation and save each binary code (0 or 1) in a separate location within the value vector of the encrypted image file
- Read the speech signal file and divide a value into blocks in each block with 256 values
- For each block, extract the short time energy parameter in it and store these values in a vector
- Choose the highest 16 short time energy values and save the original locations of these blocks
- For each of the 16 blocks, convert the 256 block values to a 16×16 binary array
- Divide the resulting matrix using fuzzy c-means clustering algorithm where we get a vector with a length of 16 values that contains the values (1 and 2). To obtain a vector with a length of 256 values that represents a private key (PK) that is exchanged between the sender and the recipient, we repeat this process over the rest of the 16 blocks.
- Use integer wavelet transforms for each block that is not among the 16 blocks to get the ca and cd coefficients. The length of each of (ca, cd) is 128, since we use these 128 locations to hide the image
- Convert the ca values from the fraction to the binary representation with length equal to 64 bits.
- Cut 8 bits from the locations 25-32 for each binary representation of ca (B= b_1 b_2 b_3 b_4 b_5 b_6 b_7 b_8), and use the LSB algorithm to replace the last bit with the encoded image (M) to be hidden using these steps, depending on PK:

- If PK = 1, do XOR (b_5, b_6) = W_1 as the first stage. Next do XOR (W_1, M) = W_2 as the second stage. Then use LSB algorithm to replace bit 8 of the vector (B) with W_2 value (i.e. the new values of the vector (B) is b_1 b_2 b_3 b_4 b_5 b_6 b_7 W_2)
- If PK = 2, do XOR (b_7, b_8) = W_1 as the first stage. Next do XOR (W_1, M) = W_2 as the second stage. Then use LSB algorithm to replace bit 8 of the vector (B) with W_2 (i.e. the new values of the vector (B) is b_1 b_2 b_3 b_4 b_5 b_6 b_7 W_2)

- Combine the new values of vector (B) in locations (25-32) of the ca value then convert the value of new ca from binary to decimal representation.
- Perform an inverse IWT transform to construct the original speech signal based on the same cd value and the new ca value.
- Reconstruct the speech signal by merging the blocks after performing the hiding process to get a speech signal file included on the encrypted image inside it.

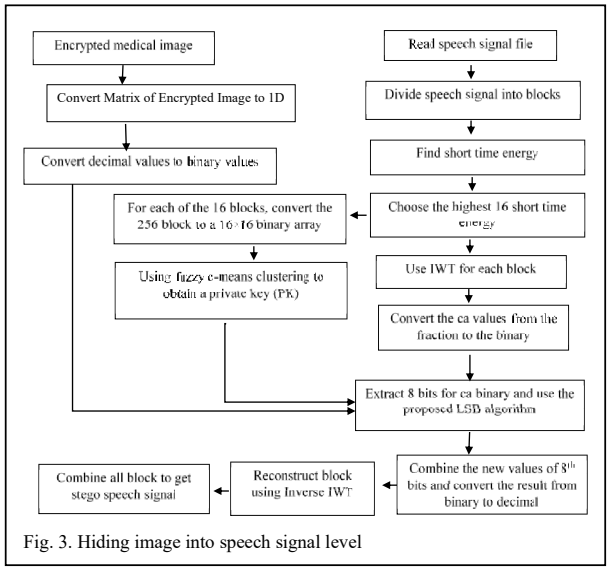


Fig. 3. Hiding image into speech signal level

IV. RESULTS

To evaluate our method, we conducted several experiments using many databases. First, for speech, we used the speech sample database from an LJ speech library test [25]. The library consists of short clips of 13100 sound clips from 1 to 10 seconds. Secondly, for medical images, we used two databases, Database1: ChestX-ray8 database which is 112,120 X-ray images with disease labels from 30,805 unique patients [26]. Database2: The brain CT database consists of head CT (Computed Tomography) images in jpg format. It contains 2500 brain window images and 2500 bone window images, for 82 patients [27].

We performed our tests on a PC with Pentium Corei7, CPU @2.60 GHz, 6.00 GB RAM, 64 bit Windows 10 OS to evaluate the implementation results. We used MATLAB R2018a tools for all the simulations.

We used the measures SNR "Signal to Noise Ratio", PSNR "Peak Signal to Noise Ratio", MSE "Mean Square Error", Structural Similarity Index Metric (SSIM), and Correlation to measure the work efficiency in the hide algorithm, and in measuring the efficiency of the encryption algorithm, we used the measures PSNR, MSE, NPCR "Number of Pixels Change Rate", and UACI "Unified Average Changing Intensity".
The following equations are computed in [11] [17] [24] as follows:

$$SNR = 10\ log_{10}\left(\frac{\sum_{i=1}^{n} o(i)^2}{\sum_{i=1}^{n}(o(i)-s(i))^2}\right) \quad (10)$$

$$PSNR = 10log_{10}\left[\frac{\max(o(i),s(i))^2}{abs(o(i)-s(i))^2}\right] \quad (11)$$

$$MSE = 10log_{10}\sum_{i=1}^{m}\sum_{i=1}^{n}\frac{(o(i)-s(i))^2}{M*N} \quad (12)$$

$$SSIM(O,S) = \frac{(2\mu_o\mu_s+co_1)(2\sigma_{os}+co_2)}{(\mu_0^2+\mu_s^2+co_1)(\sigma_0^2+\sigma_s^2+co_2)} \times 100 \quad (13)$$

$$C_{os} = \frac{\sum_{i=1}^{n}(o_i-\mu_o).(s_i-\mu_s)}{[\sum_{i=1}^{n}(o_i-\mu_o)^2]^{1/2}[\sum_{i=1}^{n}(s_i-\mu_s)^2]^{1/2}} \quad (14)$$

$$NPCR = \frac{1}{N\times M}\left(\sum_{i,j} D(i,j)\right) \times 100\% \quad (15)$$

$$UACI = \frac{1}{N\times M}\left(\sum_{i,j}\left|\frac{d_1(i,j)-d_2(i,j)}{255}\right|\right) \times 100\% \quad (16)$$

$$D(i,j) = \begin{cases} 0 & d_1(i,j) = d_2(i,j) \\ 1 & d_1(i,j) \neq d_2(i,j) \end{cases} \quad (17)$$

Where:

n is the numbers of rows and m are the columns in cover speech signals file input
o is the sample with index number in the original speech signals file
s is the sample with index number in the stego - speech signals file
μ_o and μ_s are the mean values of o and s respectively
σ_o and σ_s are the standard deviation values of o and s respectively
$Co_1 = (k_1L)^2$, and $Co_2 = (k_2L)^2$ are two constants used for null denominator avoidance
L is the dynamic range of the signal values (typically this is 2# bits per signal -1).
d_1 = an encrypted image without any modification of the original image
d_2= an encrypted image after a one-pixel change in the original image.

We used two databases for medical images with different grey color degrees (the first database: chest rays images that color gamut tends to whiteness and the second database for brain rays, the color gamut tends to blackness).

The results we obtained through several experiments using these databases showed that the hiding rate is pretty good.

Where in Table 4 and Table 5, we used gray images (1, 2, and 3) with a size (128 x 128 pixels) from Database 1 with several speech signals of different sizes, while in Table 6 and Table 7 we used gray images (4, 5, 6, 7, 8 and 9) with a size (64 x 64 pixels) from Database 2 With several speech signals in different sizes as well.

Tables 4 and 6 show high values for the two statistical measures (SNR, PSNR). As for the (MSE) measure, the error rate was very low, which indicates the clarity of the speech signal after it was hidden, as well as the hiding rate, is very good.

Likewise, the results of the two measures (correlation, SSIM) in Tables 5 and 7 show that similarity and correlation are strong between the original speech signal and the speech signal after hiding, as their values approach one.

Through the results in Table 8, we used three different gradation styles of medical images to determine whether or not the white and black ratio affects our method used. We found that the values of the results in the images (Medical Img4, Medical Img5, and Medical Img6) different. Where (UACI) and (PSNR) values are higher and smaller than the rest of the images of the database respectively, and thus we conclude that the gradations of gray color in medical images affect the accuracy of the results and reduce the quality and make a big difference between the original and encrypted images.

TABLE 4. SNR, PSNR, AND MSE RESULTS OF HIDING DIFFERENT GRAY IMAGE SIZE (128×128 PIXELS) IN DIFFERENT SPEECH SIGNAL LENGTH

Cover speech	Length	Medical Image	SNR	PSNR	MSE
Signal1	20ms	Medical Img1	111.162	129.509	3.609E-14
Signal2	30ms		110.772	129.119	3.949E-14
Signal3	40ms		116.041	134.388	1.173E-14
Signal4	50ms		135.443	153.790	1.347E-16
Signal1	20ms	Medical Img4	111.162	129.509	3.610E-14
Signal2	30ms		110.772	129.119	3.949E-14
Signal3	40ms		116.042	134.389	1.173E-14
Signal4	50ms		135.518	153.865	1.323E-16
Signal1	20ms	Medical Img7	111.161	129.508	3.610E-14
Signal2	30ms		110.772	129.119	3.949E-14
Signal3	40ms		116.042	134.388	1.173E-14
Signal4	50ms		135.507	153.854	1.327E-16

TABLE 5. CORRELATION AND SSIM RESULTS OF HIDING DIFFERENT GRAY IMAGE SIZE (128×128 PIXELS) IN DIFFERENT SPEECH SIGNAL

Cover speech	Length	Medical Image	Correlation	SSIM
Signal1	20ms	Medical Img1	0.999	0.999
Signal2	30ms		0.999	0.999
Signal3	40ms		0.999	0.999
Signal4	50ms		0.999	1
Signal1	20ms	Medical Img4	0.999	0.999
Signal2	30ms		0.999	0.999
Signal3	40ms		0.999	0.999
Signal4	50ms		0.999	1
Signal1	20ms	Medical Img7	0.999	0.999
Signal2	30ms		0.999	0.999
Signal3	40ms		0.9999	0.999
Signal4	50ms		0.9999	1

TABLE 6. SNR, PSNR, AND MSE RESULTS OF HIDING DIFFERENT GRAY IMAGE SIZE (64×64 PIXELS) IN DIFFERENT SPEECH SIGNAL LENGTH

Cover speech	Length	Medical Image	SNR	PSNR	MSE
Signal1	4ms	Medical Img1	129.633	147.361	5.701E-16
Signal2	7ms		131.969	149.812	2.208E-16
Signal3	10ms		112.022	130.369	2.961E-14
Signal4	20ms		111.192	129.539	3.584E-14
Signal1	4ms	Medical Img4	129.576	147.304	5.777E-16
Signal2	7ms		132.035	149.878	2.175E-16
Signal3	10ms		112.021	130.368	2.961E-14
Signal4	20ms		111.192	129.540	3.584E-14
Signal1	4ms	Medical Img7	129.526	147.254	5.844E-16
Signal2	7ms		131.922	149.765	2.232E-16
Signal3	10ms		112.021	130.368	2.962E-14
Signal4	20ms		111.192	129.539	3.584E-14

TABLE 7. CORRELATION AND SSIM RESULTS OF HIDING DIFFERENT GRAY IMAGE SIZE (64×64 PIXELS) IN DIFFERENT SPEECH SIGNAL

Cover speech	Length	Medical Image	Correlation	SSIM
Signal1	4ms	Medical Img1	0.999	1
Signal2	7ms		0.999	1
Signal3	10ms		0.999	0.999
Signal4	20ms		0.999	0.999
Signal1	4ms	Medical Img4	0.999	1
Signal2	7ms		0.999	1
Signal3	10ms		0.999	0.999
Signal4	20ms		0.999	0.999
Signal1	4ms	Medical Img7	0.999	1
Signal2	7ms		0.999	1
Signal3	10ms		0.999	0.999
Signal4	20ms		0.999	0.999

TABLE 8. RESULTS OF EXPERIMENT BETWEEN INPUT MEDICAL IMAGE AND ENCRYPTED MEDICAL IMAGE

Image	Dimension	PSNR	MSE	NPCR	UACI
MedicalImg1	128×128	8.1482	9960.10	99.58	32.02
MedicalImg2		8.2536	97211.52	99.61	31.65
MedicalImg3		7.6389	11199.01	99.56	33.66
MedicalImg4		6.7256	13820.38	99.79	39.10
MedicalImg5		6.6659	14011.37	99.75	39.72
MedicalImg6		6.7117	13864.51	99.71	39.12
MedicalImg7		8.1947	9853.84	99.69	31.12
MedicalImg8		8.3397	9530.24	99.68	30.56
MedicalImg9		8.1852	9875.48	99.71	31.17
MedicalImg1	64×64	8.0344	10224.38	99.56	32.45
MedicalImg2		8.1358	9988.38	99.60	32.20
MedicalImg3		7.6448	11839.78	99.63	33.53
MedicalImg4		6.8401	13460.67	99.82	38.16
MedicalImg5		6.7036	13890.39	99.75	38.69
MedicalImg6		6.7626	13703.01	99.58	38.73
MedicalImg7		8.0431	10203.84	99.70	31.59
MedicalImg8		8.0981	10075.56	99.70	31.35
MedicalImg9		8.1202	10024.29	99.73	31.63

Fig. 4 and Fig. 5 are shown the scrambling and encryption process of the medical images (Img1, Img4, and Img7) with size (128×128 pixels and 64×64 pixels). While Fig. 6 and Fig. 7 are shown hide image (64×64 pixels) in speech signal length 20ms and 4ms respectively.

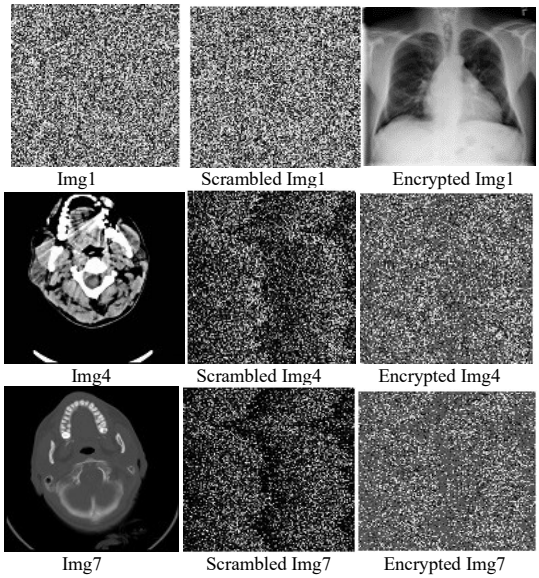


Fig. 4. The scrambling and encryption process of the medical images (Img 128×128 pixels)

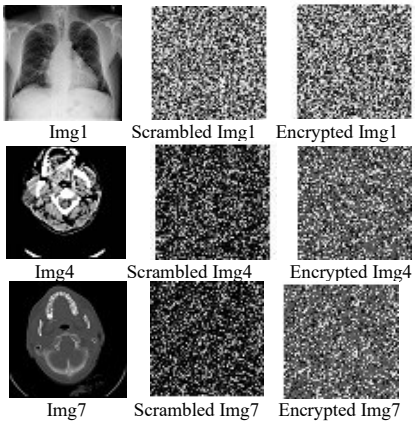
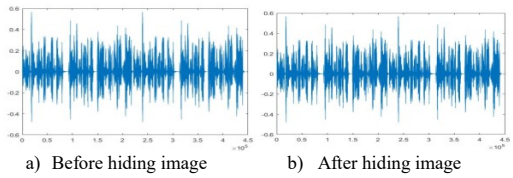
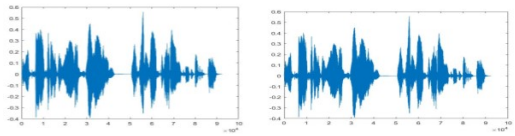


Fig. 5: the scrambling and encryption process of the medical images (Img 64×64 pixels)



a) Before hiding image b) After hiding image

Fig. 6. Hide image 64×64 pixels in speech signal length 20ms



a) Before hiding image b) After hiding image

Fig. 7. Hide image 64×64 pixels in speech signal length 4ms

To evaluate the proposed hiding and encryption algorithms using quality measurements a comparison is made with other techniques. The comparison is presented in Table 9, and Table 10, sequentially.

TABLE 9. COMPARISON PROPOSED METHOD WITH EXISTING SCHEMES OF HIDING IMAGE IN SIGNAL

Paper	Correlation	SSIM	SNR	PSNR	MSE
Abduljaleel [23]	-	-	-	87.6718	0.0001
Hameed [28]	-	-	81.60	-	-
Our paper	0.999	1	135.507	153.854	1.327E-16

TABLE 10. COMPARISON PROPOSED METHOD WITH EXISTING SCHEMES OF ENCRYPTION IMAGE

Paper	PSNR	MSE	NPCR	UACI
Joshua et al. [4]	-	-	99.64	33.43
Cao et al. [5]	-	-	99.66	33.50
ElKamchouchi et al. [9]	-	-	99.6150	33.4205
Abdelfattah et al. [11]	6.36	15144.68	99.613	33.571
Q. Liu and L. Liu [15]			99.61	32.20
Al-Mashhadi and Abduljaleel [16]	-	-	99.63	28.90`
Ali and R. Ali [29]	-	-	99.60	33.43
Our paper	8.1852	9875.48	99.71	31.17

V. CONCLUSION

In the healthcare industry, Medical images are carefully transmitted from source to destination and this transmission of this information requires more security through the internet, where the problems of malicious manipulation and hackers, as well as privacy leakage, are present.

In this paper, the hiding and encryption techniques have been used for hiding images in the speech signals. Firstly, the medical image of the patient is encrypted using the suggest encryption method that contains DNA coding and a series of keys generated by (Tinkerbell map and 3D Hénon map) to achieve the confusion and diffusion. Also for scrambling the medical image, we used the Zaslavsky map. Secondly, the encrypted medical image is hidden in speech signal using (integer wavelet transform and LSB algorithm), then using (fuzzy c-means clustering algorithm and short-time energy) to determine locations of the speech signal to hide in it.

Finally, we used measures (MSE, PSNR, NPCR, and UACI) to measure the effectiveness of the encryption algorithm, and measures (SNR, PSNR, MSE, Correlation, and SSIM) to measure the effectiveness of the hiding algorithm. We obtained good results compared to similar researches. The security analysis reveals that our method has a high degree of protection and is capable of withstanding all forms of attacks in comparison with other methods as explained in the section on results.

We used square medical images (i.e. the length and width are equal). In the future, we could apply our algorithms to images of different lengths and widths.

REFERENCES

[1] V. Pavithra and C. Jeyamala, "A Survey on the Techniques of Medical Image Encryption," *2018 IEEE Int. Conf. Comput. Intell. Comput. Res. ICCIC 2018*, pp. 1–8, 2018, doi: 10.1109/ICCIC.2018.8782432.

[2] P. G. R. babu Vaishali Sarangpure, Prof. Roshani Talmale, "Implementation on Hiding Data and Image in Audio- Video Using Anti Forensics Technique," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 3(9), no. 2320–9801, pp. 8159–8164, 2015.

[3] R. Tanwar, K. Singh, M. Zamani, A. Verma, and P. Kumar, "An Optimized Approach for Secure Data Transmission Using Spread Spectrum Audio Steganography, Chaos Theory, and Social Impact Theory Optimizer," *J. Comput. Networks Commun.*, vol. 2019, 2019, doi: 10.1155/2019/5124364.

[4] E. O. A. Joshua C. Dagadu, Jian-Ping Li, "Medical Image Encryption Based on Hybrid Chaotic DNA Diffusion," Springer Sci. Media, LLC, part Springer Nat., https://doi.org/10.1007/s11277-019-06420-z, 2019.

[5] W. Cao, Y. Zhou, C. L. P. Chen, and L. Xia, "Medical image encryption using edge maps," *Signal Processing*, vol. 132, pp. 96–109, 2017, doi: 10.1016/j.sigpro.2016.10.003.

[6] M. Parthasarathi, T. Shreekala, T. Nadu, and T. Nadu, "Secured Data Hiding in Audio Files Using Audio Steganography Algorithm," *Int. J. Pure Appl. Math.*, vol. 114, no. 7, pp. 743–753, 2017.

[7] H. N. Chowdary, K. Karan, K. P. Bharath, and R. M. Kumar, "Data hiding in speech signal using steganography and encryption," *2018 3rd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. RTEICT 2018 - Proc.*, pp. 1219–1223, 2018, doi: 10.1109/RTEICT42901.2018.9012508.

[8] D. Samiappan and P. R. Buvaneswari, "Video steganography using IWT, DWT, LBP methods and its research," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 6 Special Issue 3, pp. 2022–2026, 2019, doi: 10.35940/ijeat.F1287.0986S319.

[9] K. H. M. Dalia H. ElKamchouchi, Heba G. Mohamed, "A Bijective Image Encryption System Based on Hybrid Chaotic Map Di usion and DNA Confusion," *entropy*, vol. 22, 180, no. doi:10.3390 , pp. 1–18.

[10] N. A. T. Firas A. Abdullatif, Alaa A. Abdullatif, "Data hiding using integer lifting wavelet transform and DNA computing," *Period. Eng. Nat. Sci.*, vol. 1, no. ISSN 2303-4521, pp. 58–66, 2020.

[11] R. Ismail Abdelfattah, H. Mohamed, and M. E. Nasr, "Secure Image Encryption Scheme Based on DNA and New Multi Chaotic Map," *J. Phys. Conf. Ser.*, vol. 1447, no. 1, 2020, doi: 10.1088/1742-6596/1447/1/012053.

[12] D. Riadh and R. Shaker, "Implementation of Gray Image Encryption using Multi-Level of Permutation and Substitution," *Int. J. Appl. Inf. Syst.*, vol. 10, no. 1, pp. 25–30, 2015, doi: 10.5120/ijais2015451458.

[13] F. J. Farsana and K. Gopakumar, "A Novel Approach for Speech Encryption: Zaslavsky Map as Pseudo Random Number Generator," *Procedia Comput. Sci.*, vol. 93, no. September, pp. 816–823, 2016, doi: 10.1016/j.procs.2016.07.302.

[14] Z. H. R. Nidaa Abdulmohsin Abbas, "Review Of Dct And Chaotic Maps In Speech Scrambling," *J. Theor. Appl. Inf. Technol.*, vol. 97, no. 1992–8645, pp. 569–582.

[15] Q. Liu and L. Liu, "Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System," *IEEE Access*, vol. 8, pp. 83596–83610, 2020, doi: 10.1109/ACCESS.2020.2991420.

[16] H. M. Al-Mashhadi and I. Q. Abduljaleel, "Color image encryption using chaotic maps, triangular scrambling, with DNA sequences," *Int. Conf. Curr. Res. Comput. Sci. Inf. Technol. ICCIT 2017*, pp. 93–98, 2017, doi: 10.1109/CRCSIT.2017.7965540.

[17] F. J. Farsana and K. Gopakumar, "Speech Encryption Algorithm Based on Nonorthogonal Quantum State with Hyperchaotic Keystreams," *Adv. Math. Phys.*, vol. 2020, 2020, doi: 10.1155/2020/8050934.

[18] A. Prof., "Proposed Hyperchaotic System for Image Encryption," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 1, pp. 37–40, 2016, doi: 10.14569/ijacsa.2016.070105.

[19] S. Zhou, F. Xu, P. Ping, Z. Xie, and X. Lyu, "Non-square colour image scrambling based on two-dimensional sine-logistic and hénon map," *KSII Trans. Internet Inf. Syst.*, vol. 11, no. 12, pp. 5963–5980, 2017, doi: 10.3837/tiis.2017.12.015.

[20] F. J. Farsana, V. R. Devi, and K. Gopakumar, "An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams," *Appl. Comput. Informatics*, no. xxxx, pp. 1–11, 2019, doi: 10.1016/j.aci.2019.10.001.

[21] C. Yang and K. Lin, "Hiding Data in Electrocardiogram Based on IWT Domain via Simple Coefficient Adjustment," vol. 04, no. 03, pp. 69–76, 2016.

[22] 2M.Sivaram R.Punidha, "Integer Wavelet Transform Based Approach For High Robustness Of Audio Signal Transmission," *Int. J. Pure Appl. Math.*, vol. 116 (23), no. 1314–3395, pp. 295–304, 2017.

[23] I. Q. Abduljaleel, "Hiding medical image in an audio signal Using (Curvelet / IWT) transforms And modified LBS method," vol. 34, no. 1, pp. 11–23, 2016.

[24] J. Kong, J. Hou, M. Jiang, and J. Sun, "A novel image segmentation method based on improved intuitionistic fuzzy C-Means clustering algorithm," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 6, pp. 3121–3143, 2019, doi: 10.3837/tiis.2019.06.020.

[25] Z. Lin, Y. Huang, and J. Wang, "RNN-SM: Fast Steganalysis of VoIP Streams Using Recurrent Neural Network," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 7, pp. 1854–1868, 2018, doi: 10.1109/TIFS.2018.2806741.

[26] Wang X, Peng Y, Lu L, Lu Z, Bagheri M, "Summers RM. ChestX-ray8: Hospital-scale Chest X-ray Database and Benchmarks on Weakly-Supervised Classification and Localization of Common Thorax Diseases". *IEEE CVPR 2017*, ChestX-ray8Hospital-ScaleChestCVPR, 2017.

[27] Hssayeni, M, "Computed Tomography Images for Intracranial Hemorrhage Detection and Segmentation." *PhysioNet*., DOI: 10.13026/w8q8-ky94, 2019.

[28] A. S. Hameed, "High Capacity Audio Steganography Based on Contourlet Transform," Tikrit J. Eng. Sci., vol. 25, no. 1, pp. 1–7, 2018, doi: 10.25130/tjes.25.1.01.

[29] T. S. Ali and R. Ali, "A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map," IEEE Access, vol.8, pp. 71974–71992, 2020, doi: 10.1109/ACCESS.2020.2987615.