

# Comparison of Audio Speech Cryptosystem Using 2-D Chaotic Map Algorithms

Mahmoud Farouk<sup>1</sup>, Osama Faragallah<sup>1,2</sup>, Osama Elshakankiry<sup>1,2</sup>, Ahmed Elmalhalawy<sup>1</sup>

<sup>1</sup>Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menofia University, Menouf, Egypt

<sup>2</sup>Department of Information Technology, College of Computers and Information Technology, Taif University, Al-Hawiya, Kingdom of Saudi Arabia

## Email address:

mfs.msc@gmail.com (M. Farouk), o.salah@tu.edu.sa (O. Faragallah), o.bahgat@tu.edu.sa (O. Elshakankiry),  
ahmed.elmalhalawy@el-eng.menofia.edu.eg (A. Elmalhalawy)

## To cite this article:

Mahmoud Farouk, Osama Faragallah, Osama Elshakankiry, Ahmed Elmalhalawy. Comparison of Audio Speech Cryptosystem Using 2-D Chaotic Map Algorithms. *Mathematics and Computer Science*. Vol. 1, No. 4, 2016, pp. 66-81. doi: 10.11648/j.mcs.20160104.11

**Received:** August 30, 2016; **Accepted:** September 8, 2016; **Published:** October 10, 2016

---

**Abstract:** This paper presents a comparison between different audio speech encryption and decryption techniques for audio speech signals based on 2-D chaotic map algorithms with time and transform domains in a search for best of them and study advantages and disadvantages for each of them. Chaotic algorithms will be used because they have advantages of its casual Conduct and sensitivity to values of parameters and primary conditions that enable chaotic algorithms to fulfill the cryptographic systems. We consider doing simulation tests using MATLAB codes for logistic 2D map, Henon map, Standard map and baker map. Real simulation results show that baker map with TD exhibits best quality for both encryption and decryption and has a well balance between its advantages and disadvantages among other algorithms in comparison.

**Keywords:** Audio Speech Encryption, Chaotic Map, Speech Communication, Logistic 2D Map, Henon Map, Standard Map, Chaotic Baker Map

---

## 1. Introduction

Audio Speech communication has an important function in our daily life, we can find its presence in many areas like, politics ,military, e-learning, banking, social networking, phone conversation, chat conversation programs and news broadcasting, with the advancement in technologies like computer networking, multimedia and communication systems. We can find a huge amount of sensitive critical speech information is passing across wire and wireless networks on a daily basis, so there is a dire need to keep these speech information secure before transmission or distribution through any insecure channel. There is a dire need for cryptographic techniques to convert the intelligible form of speech to unintelligible form before transmission into transmission media at transmitter side and decrypt it to an intelligible form at receiver's side.

There are two types of speech encryption: analog and digital [1]. Analog speech encryption techniques have an advantage of fewer requirements for bandwidth. So, it becomes more popular used encryption techniques

nowadays, and depends on a diffusion of speech components in frequency domain [2], time domain [3], both time and frequency domain [4], wavelet transform [5], transform domain [6], blind source separation based method [7], hadamard transform [8], and circulant transformations [9].

Digital speech encryption methods produce digital speech signal, they have an advantage over analog that they provide more security but has a disadvantage that it requires more bandwidth and complex implementation. Examples of digital speech encryption methods are Data Encryption Standard (DES), linear feedback shift register (LFSR), International Data Encryption Algorithm (IDEA), and advanced encryption standard (AES) [10-14].

This paper shows a comparison between different speech encryption and decryption techniques based on chaotic algorithms, in a search for best encryption and decryption algorithm for speech audio Cryptosystems and also explore advantages and disadvantages for each algorithm. The remnant of this paper is orderly arranged as follows. Section 2 gives a general explanation for chaotic system and discuss chaotic algorithms used in simulation test, logistic map, Henon map, Standard map and baker map respectively.

Section 3 discusses an explanation for quality metrics used for speech chaotic algorithms' assessment for both encryption and decryption algorithms. Section 4 presents proposed cryptosystem. Section 5 discusses emulation results. Finally, Section 6 gives concluding remarks.

## 2. Chaotic System

Chaotic system is an encryption system that exhibits a nonlinear deterministic dynamical behavior. It uses maps for rearranging values of items within blocks. The output values of chaotic system are very sensitive in relation with values of input parameters and initial conditions [15].

Chaotic system have two advantages that makes it suitable to satisfy cryptographic properties such as confusion, diffusion and disorder.

1. Its output have an excellent randomness, non-predictability and low correlation.
2. Its random conduct to input parameters and starting points or initial values [16].

In the following sections a brief descriptions for four types of chaotic maps, logistic 2D map, henon map, Standard map and baker map.

### 2.1. Logistic 2-D Map

It is a two-dimensional map (2-D), it has a higher complexity compared to the one-dimensional (1-D) logistic map, and values of  $r$  parameter determine its complexity as a dynamical system. It provides more security and more effectiveness for both confusion and diffusion in stream and block encryptions [17].

Logistic 2D map is expressed as shown in Eq.1.

2D Logistic map:  $x_{i+1} = r(3y_i + 1)x_i(1-x_i)$

$$y_{i+1} = r(3x_{i+1} + 1)y_i(1-y_i) \quad (1)$$

Parameter  $r$  values determine type of dynamicity of chaotic map, if  $r > 1.19$ , system becomes unstable.

$(x_i, y_i)$  represents the point at the  $i$ th iteration,  $(x_{i+1}, y_{i+1})$  represents the point at the  $i+1$ th iteration.

### 2.2. Henon Map

Henon chaotic map discovered in 1978 [18-20] It is two dimensional (2-D), discrete-time nonlinear, exhibits dynamical chaotic attitude, used in cryptography systems, it is defined by:

$$\begin{aligned} X_{n+1} &= 1 + y_n - ax_n^2 \\ Y_{n+1} &= bx_n \end{aligned} \quad (2)$$

The parameters  $a$  and  $b$  have great importance, the system cannot be chaotic unless the value of  $a$  and  $b$  are 1.4 and 0.3 respectively. For other values of  $a$  and  $b$ , the map behaves as chaotic, intermittent, or obtain a periodic orbit.  $x_n$  and  $y_n$  represent initial values work as a symmetric key for chaotic cryptographic system used for both encryption and decryption, both ciphering algorithm and key sensitivity

work together to avoid all kinds of cryptanalysis attacks.

### 2.3. Standard Map

It is also called Chirikov standard map or Chirikov-Taylor map, it is a (2D) chaotic map. It is described by the equation Eq. 3:

$$\begin{aligned} P_{i+1} &= p + k \sin x \\ X_{i+1} &= x + p_{i+1} \end{aligned} \quad (3)$$

Where  $P_{i+1}$  and  $X_{i+1}$  represent variables after one iteration and parameter  $K$  impacts the degree of chaos.

The dynamics can be considered on a cylinder (if taking  $x \bmod 2\pi$ ) or on a torus (if taking both  $x, p \bmod 2\pi$ ), this is because of the periodicity of  $\sin x$  [21].

### 2.4. Baker Map

It is a two dimensional (2D) chaotic map, it uses secret key to rearrange elements in a square matrix in new positions [22]. It retains all best advantages of chaotic system such as non-predictability, good randomness and low correlation [23-25].

Baker map has two kinds, generalized and discretized map. We will focus our research on discretized baker map as it has an advantage that it is an effective method to randomize the elements in a square matrix.

#### 2.4.1. Generalized Baker Map

Generalized chaotic baker map can be represented as the following:

- (a)  $R \times R$  represents a square matrix split into  $k$  vertical rectangles with height  $R$  and with width  $u_i$  while,  $u_1 + u_2 + \dots + u_k = R$ .
- (b) Rectangles must be arranged so that left one at the bottom and the right one at the top.
- (c) Vertical rectangles arranged so that it should be lengthened horizontally.

Figure 1 (a) exhibits an example for generalized chaotic baker map with  $R=3$  and  $k=3$  and with width ( $u$ ) = 1.

#### 2.4.2. Discretized Baker Map

Discretized baker map rearranges an element in a square matrix to another position in the matrix. Suppose discretized Baker map is denoted by  $B(u_1, u_2, \dots, u_k)$ , values of  $k$  integers ( $u_1, u_2, \dots, u_k$ ), is selected so that each integer  $u_i$  divides  $Z$ , and  $Z_i = u_1 + \dots + u_i$ .

Item at the position  $(r, s)$ , adhere with conditions such that  $0 \leq s \leq z$  and  $Z_i \leq r \leq z_i + u_i$ , Mapped to the new position as the following equation :

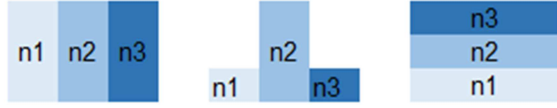
$$B_{(u_1, \dots, u_k)}^{(r, s)} = \left( \frac{Z}{u_i} (r - Z_i) + S \bmod \left( \frac{Z}{u_i} \right), \frac{u_i}{Z} \left( S - S \bmod \left( \frac{Z}{u_i} \right) \right) + Z_i \right) \quad (4)$$

The following conditions are applied to equation.4:

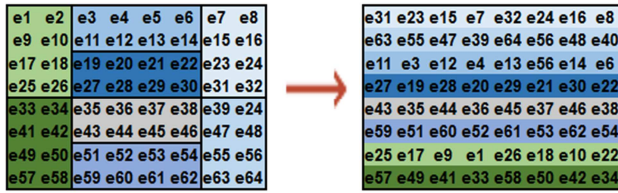
- (a)  $Z$  constitutes a  $Z \times Z$  matrix split into  $k$  vertical rectangles with height  $Z$  and width  $u_i$ .
- (b) For each vertical rectangle, it contains  $u_i$  boxes, and each box contains  $Z$  elements.

- (c) To map each box to a row of elements, a column by column (right box at top and left box at bottom) mapping is achieved.

For more illustration consider an eight  $\times$  eight matrix is shown in Figure 1(b). Suppose secret key being used is (2, 4, 2), hence  $Z=8$ ,  $u_1=2$ ,  $u_2=4$ , and  $u_3=2$ . We will use discretized baker map in permutation phase and to generate the mask.



(a). Generalized Baker Map



(b). Discretized Baker Map – randomization of an 8x8 matrix with a secret key  $u = [2, 4, 2]$

Figure 1. Chaotic Baker Map.

### 3. Quality Metrics for Speech Chaotic Algorithms

Many quality metrics are being used to assess the voice cryptosystem, these metrics can be divided into two main categories. First one is for measuring encryption algorithm and the second one for measuring decryption algorithm. Encryption quality metrics are applied on encrypted signals to assess the immunity of audio cryptosystem against cryptanalysis attacks and evaluate amount of distortion in encrypted speech signal, while decryption quality metrics used to assess the immunity of cryptosystem to noise and distortion due to channel effects, and measure distortion in decrypted signal.

Both Encryption and Decryption quality metrics answer the question, how far is the encrypted or decrypted signal from original signal. It also has a great importance in the design and maintenance of the encryption and decryption algorithm. The purpose of these quality metrics is to:

- Determine the immunity of encryption/decryption algorithm to distortion and cryptanalysis's attacks.
- Indicate amount of distortion introduced by audio cryptosystem.
- Determine the parameter settings.
- Optimize audio cryptosystem

#### 3.1. Encryption Quality Metrics

##### 3.1.1. Histogram

It is an important encryption quality metric. It is a graphical display of tabulated densities of data [26], used to

assess the success of substitution step by indicating that new signal's values are inserted into encrypted signal instead of the original value. The more uniform the histogram the better encryption algorithm.

##### 3.1.2. Correlation Coefficient (CC)

It is an important metric used to evaluate the quality of encryption algorithm of cryptosystem, by comparing similar samples in original audio speech signal and the encrypted speech signal. It is expressed by the following:

$$r_{xy} = \frac{Cv(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (5)$$

$D(x)$  and  $D(y)$  stand for variances of signal  $x$  and  $y$  respectively, and  $c_v(x,y)$  stands for the covariance between original signal  $x$  and the encrypted signal  $y$ .

It can be expressed in numerical formulas as the following [27]:

$$E(x) = \frac{1}{N_x} \sum_{n=1}^{N_x} x(n) \quad (6)$$

$$D(x) = \frac{1}{N_x} \sum_{n=1}^{N_x} (x(n) - E(x))^2 \quad (7)$$

$$c_v(x,y) = \frac{1}{N} \sum_{n=1}^{N_x} (x(n) - E(x))(y(n) - E(y)) \quad (8)$$

$N_x$  stands for the number of speech samples used in the calculations. The encryption quality is good when the value of correlation coefficient becomes low.

##### 3.1.3. Spectral Distortion (SD)

It represents how far is the spectrum of encrypted audio speech signal from that of original signal, It is computed in dB, , it can be described as follows [28,29]:

$$SD = \frac{1}{M} \sum_{m=0}^{M-1} \sum_{n=L_s m}^{L_s m + L_s - 1} |V_s(k) - V_y(k)| \quad (9)$$

where  $V_s(k)$  represents the original audio speech signal in dB for a certain segment, While  $V_y(k)$  represents the processed audio speech signal in dB for the same segment,  $M$  represents the number of segments and  $L_s$  is the segment length. The higher value of SD between original signal and the encrypted signals, the better is the encryption quality.

##### 3.1.4. Processing Time

It represents the time consumed by the encryption or decryption algorithm to finish, lower values of this metric is desirable as it implies a better quality of encryption algorithm as this means shorter time needed to execute the algorithm, we can also consider average time needed time for both encryption and decryption as an average measure.

#### 3.2. Decryption Quality Metrics

There are two approaches that used to evaluate quality of decrypted speech audio signals. These are subjective and objective [30-32], subjective metrics evaluate quality of

decrypted signal by perceptual ratings of a group of listeners. In this research, we will only consider objective quality metrics because it is better than subjective quality metrics for the reasons that it is less expensive, give more consistent results and save time. It is desirable on practical applications as they depend on computational methods and physical parameters.

### 3.2.1. Log Likelihood Ration (LLR)

This metric is an important metric to evaluate the quality of decrypted signal, on which each speech segment can be represented the following [33-34]:

$$s(n) = \sum_{m=1}^{m_p} a_m s(n-m) + G_s u(n) \quad (10)$$

Values of  $m$  for parameter ( $a_m$ ) is ( $m=1, 2, \dots, m_p$ ) represent the coefficients of the all-pole filter,  $u(n)$  is an appropriate excitation source for the filter and  $G_s$  represents the gain of the filter. The audio speech signal is windowed to form frames of 15 to 30 ms length to enable computation of LLR, LLR metric is calculated as in eq. 8 [35]:

$$LLR = \left| \log \left( \frac{\vec{a}_s^T \vec{R}_y \vec{a}_s}{\vec{a}_y^T \vec{R}_y \vec{a}_y} \right) \right| \quad (11)$$

Where  $\vec{a}_s$  represents the LPCs coefficient vector  $[1, a_s(1), a_s(2), \dots, a_s(m_p)]$  for the original clear audio speech signal.

And  $\vec{a}_y$  represents the LPCs coefficient vector  $[1, a_y(1), a_y(2), \dots, a_y(m_p)]$  for the decrypted audio speech signal, and  $\vec{R}_y$  represents the autocorrelation matrix of the decrypted audio speech signal. Quality of decrypted signal becomes better as s value of LLR is low and close to zero.

### 3.2.2. Correlation Coefficient (CC)

The higher the value of correlation coefficient between original and decrypted signal represents the better the quality of decryption algorithm

### 3.2.3. Spectral Distortion (SD)

The lower the value of spectral distortion between original and decrypted signal represents the better the quality of decryption algorithm. We summarize both encryption and decryption quality metrics in Table 1.

Table 1. Summary of Encryption and Decryption Quality Metrics.

Decryption algorithm					Encryption Algorithm			
Log likelihood Ratio (LLR)	Spectral Distortion (SD)	Correlation Coefficient (CC)	Processing time (s)	Histogram	Log likelihood Ratio (LLR)	Spectral Distortion (SD)	Correlation Coefficient (CC)	Processing time (s)
Lowest Value and more near to zero Is the best for more quality of decryption algorithm	Lowest Value Is the best for more quality of decryption algorithm	Highest value is the best for more quality of decryption algorithm	Lowest Value Is the best for more quality of decryption algorithm	The more uniform the histogram the more quality of encryption algorithm	highest value is the best for more quality of encryption algorithm	highest value is the best for more quality of encryption algorithm	Lowest value is the best for more quality of encryption algorithm	Lowest Value Is the best for more quality of encryption algorithm

## 4. Proposed Cryptosystem

As shown in Figure 2, Encryption Phase consists of the following steps:

Step 1: Reformat audio speech signal by doing framing and reshaping into 2-D blocks to a form suitable to be readable by programming language which is MATLAB in our research.

Step 2: Mask generation by using key.

Step 3: Permutation using any of chaotic algorithms in this research (Logistic Map, Henon Map, Standard Map, or Baker Map), in which speech information samples are rearranged and change its position in speech matrix, Substitution, means changing values or amplitudes of speech samples by adding its value to mask's value.

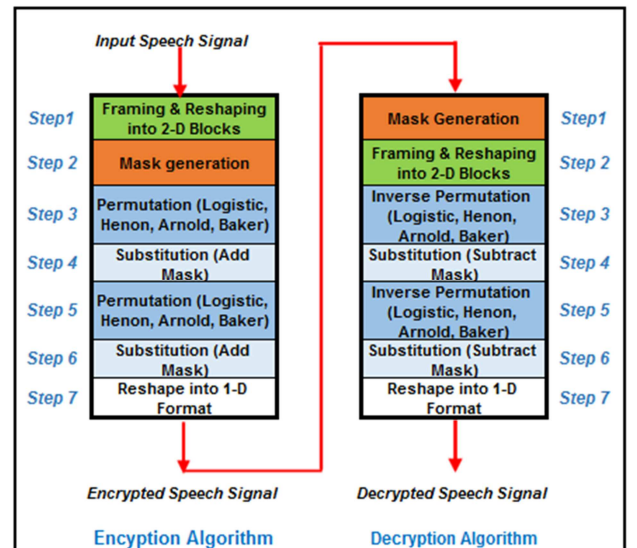


Figure 2. Proposed Cryptosystem.

Step 4: Apply time domain or transform domain (DCT,DST,DWT), then apply Permutation using same

chaotic algorithm used in step 3, then substitution and finally apply inverse transform domains (IDCT, IDST, IDWT).

Step 5: Apply permutation using same chaotic algorithm used in step 3.

Step 6: Reshape into 1-D format which is the most suitable form to save speech information into a physical file, output file is the encrypted speech file on which we can apply encryption quality metrics.

Decryption Phase consists of the following steps:

Step 1: Mask generation by using key.

Step 2: Framing and reshaping into 2-D blocks, to a form suitable to be read by programming language which is MATLAB in our research.

Step 3: Apply inverse permutation, in which speech information are rearranged and change its location in speech matrix to its original positions.

Step 4: Apply time domain or transform domain (DCT, DST, DWT), then apply substitution (subtract mask), then apply inverse permutation using same chaotic algorithm used in step 3, and finally apply inverse transform domains (IDCT, IDST, IDWT).

Step 5: Apply substitution (subtract mask) then Apply Inverse Permutation.

Step 6: Reshape into 1-D format which is the most suitable form to save speech information into file to save it, output file is the decrypted speech file on which we can apply decryption quality metrics.

#### 4.1. Permutation Step

This step reduces the intelligibility of audio signal as it produces distortion of speech time envelope, as we will apply permutation of audio samples in time domain and transform domains.

#### 4.2. Third Permutation Step

This step is used to complete hiding of audio signal features.

#### 4.3. Substitution Step

It is responsible about changing non-permuted portions of encrypted signal and to change power spectrum of audio signal to overcome cryptanalysis attacks. We accomplish substitution in time domain (TD) [37, 38], DCT domain, DST domain, or DWT domain to determine the best domain for use in speech cryptosystem [39-48].

#### 4.4. Mask

It is generated from the secret key, using key for generating the mask adds an advantage of more secure cryptosystem, and its construction steps are as follows:

- A specific number of ones is inserted to an all-zero block.
- A mask of zero's and ones is constructed by doing permutation on this block with baker map.
- The mask is added to each block of audio signal after reshaping to beat known-plaintext attacks and to hide

silent periods within audio speech signal.

- To make resulting values in the range -1 and 1, a clipping step is applied by subtracting 2 from all values exceeding 1.

Figure 3. shows these steps considering a secret key of {4,2,2,4}, sum of sub-keys equals to 12, which lead to a 12x12 blocks, while number of sub-keys is 4.

0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0.4	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0

(a)

1	1	1	1	1	1	1	1	1	1	1	1
0	0	1	0	0	1	0	0	1	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1
0	0	1	0	0	1	0	0	1	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1
0	0	1	0	0	1	0	0	1	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0

(b)

1	1	1	1	1	1	1	1	1	1	1	1
0	0	1	0	0	1	0	0	1	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1
0	0	1	0	0	1	0	0	1	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1
0	0	1	0	0	1	0	0	1	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0

(c)

-0.5	1	0	-0.5	-0.6	-0.8	-0.8	-0.8	0.7	-0.6	1	1
0.1	0	0	0.5	0.4	-0.8	0.2	0.2	0.7	0	0	1
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
-0.5	1	0	-0.5	-0.6	-0.8	-0.8	-0.8	0.7	1	1	1
0.1	0	0	0.5	0.4	-0.8	0.2	0.2	0.7	0	0	1
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
-0.5	1	0	-0.5	-0.6	-0.8	-0.8	-0.8	0.7	1	1	1
0.1	0	0	0.5	0.4	-0.8	0.2	0.2	0.7	0	0	1
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0

(d)



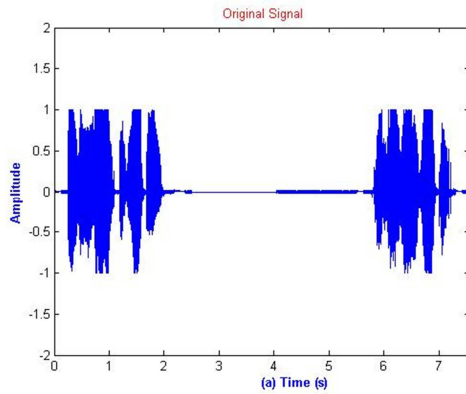
1.1	1	2	1.5	1.4	1.2	1.2	1.2	0.7	1.4	1	1
0.1	0	2	0.5	0.4	1.2	0.2	0.2	0.7	0	0	1
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
1.1	1	2	1.5	1.4	1.2	1.2	1.2	0.7	1	1	1
0.1	0	2	0.5	0.4	1.2	0.2	0.2	0.7	0	0	1
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
1.1	1	2	1.5	1.4	1.2	1.2	1.2	0.7	1	1	1
0.1	0	2	0.5	0.4	1.2	0.2	0.2	0.7	0	0	1
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
1.1	1	2	1.5	1.4	1.2	1.2	1.2	0.7	1	1	1
0.1	0	2	0.5	0.4	1.2	0.2	0.2	0.7	0	0	1
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0
0.1	0	1	0.5	0.4	0.2	0.2	0.2	-0.3	0	0	0

(e)

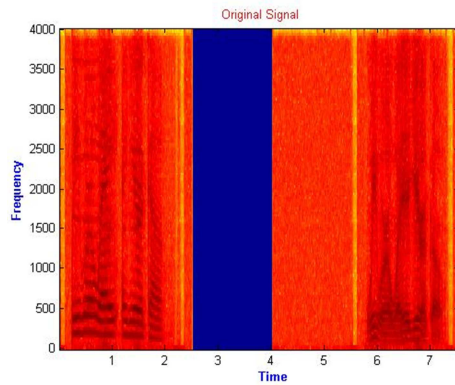
**Figure 3.** (a) original signal, (b) Mask, (c) Permutation of Mask (d) addition of Mask, (e) Final block after clipping.

## 5. Simulation Results

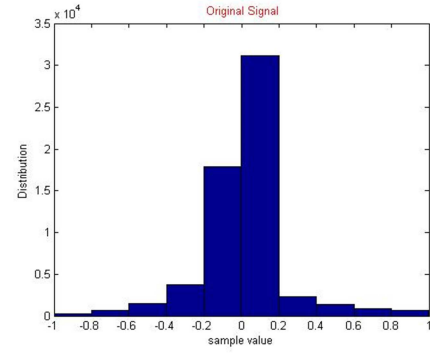
Hardware specification used in this simulation results , represented by a laptop, HP , Pavilion g series , processor intel® Core™ i3 cpu M370 2.40 GhZ, ram 4GB, HDD 500GB, software used for simulation is MATLAB 7.10.1 (R 2010a), Operating system windows 7 ultimate, audio sample used is an artificial speech signal for the sentence "we were away years ago". It consists of first 2.5 seconds for a female saying this sentence, followed by 1.5 seconds of perfect silence period without noise, next 1.5 seconds are for a silence period with room noise, the last 2.5 seconds are for a male saying the same sentence, this signal and its histogram is shown in Figure 4.



(a)



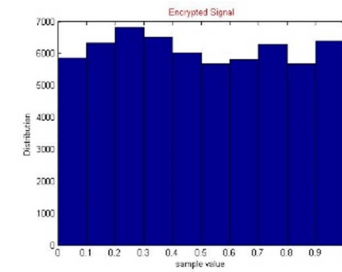
(b)



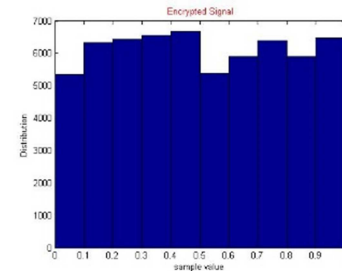
(c)

**Figure 4.** Original speech signal, (b) Spectrogram of Original Signal, (c) Histogram of original Signal.

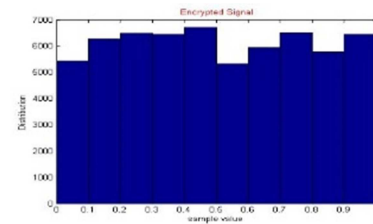
### 5.1. Histogram Analysis



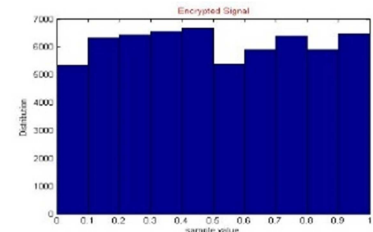
(a)



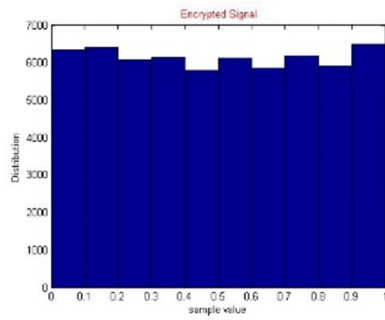
(b)



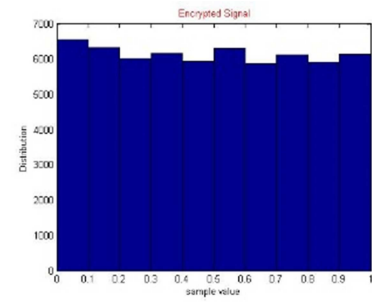
(c)



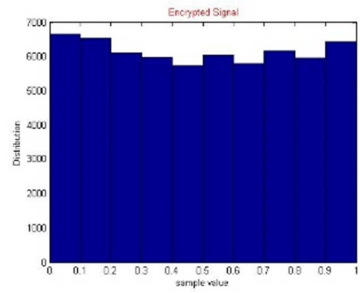
(d)



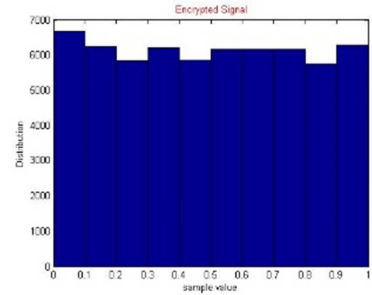
(e)



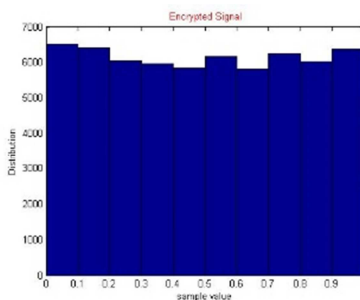
(j)



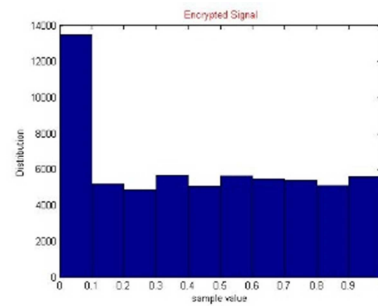
(f)



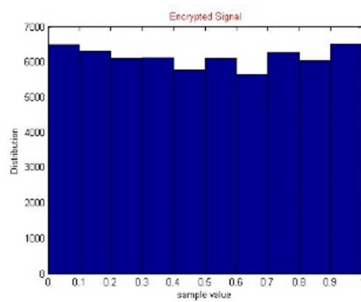
(k)



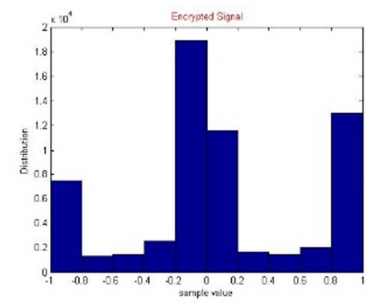
(g)



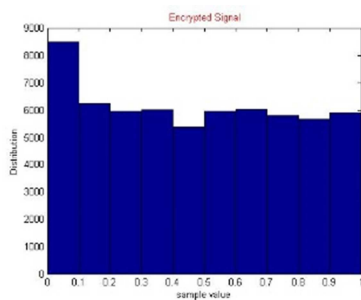
(l)



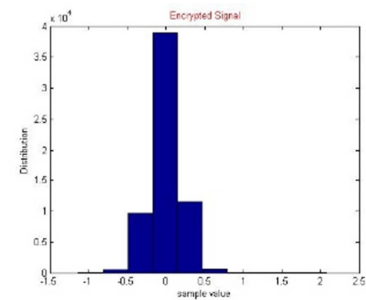
(h)



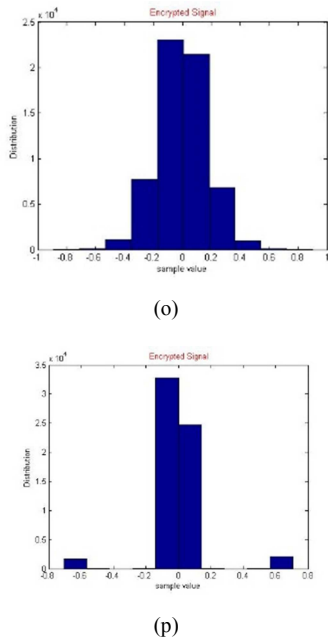
(m)



(i)



(n)



**Figure 5.** Histogram for Encrypted (a) Logistic Map-TD, (b) Logistic Map-DCT, (c) Logistic Map-DST, (d) Logistic Map-DWT, (e) Henon Map-TD, (f) Henon Map-DCT, (g) Henon Map-DST, (h) Henon Map-DWT, (i) Standard Map-TD, (j) Standard Map-DCT, (k) Standard Map-DST, (l) Standard Map-DWT, (m) Baker Map-TD, (n) Baker Map-DCT, (o) Baker Map-DST, (p) Baker Map-DWT

By comparing histogram of original signal shows in Figure 4(c), with that of encrypted logistic map shown in Figure 5(a,p), baker map-DCT shown in Figure 5(n), and baker map-DST shown in Figure 5(o) are showing best uniform histogram compared with other histograms for logistic map, henon map and standard map, while baker map-DCT shown in Figure 5(n) has better uniformity than baker map-DST shown in Figure 5(o) when compared with original signal shown in Figure 4(c), we can conclude that baker map with DCT transform provides best encryption quality based on histogram's quality metric for encryption.

Comparing other quality metrics for both encryption and decryption speech signal, such as correlation coefficient (cc), time taken for encryption and decryption algorithm, spectral distortion and log likelihood can be summarized in the following Table 2. All values are taken from real simulation results, taking into account using same key of length 64 for all chaotic algorithms, the best values are with green background, and the worst values with red background.

**Table 2.** Comparison between four chaotic algorithms for Encryption and Decryption.

Logistic Map	Encryption				Decryption				Average Time (s)
	Time (S)	CC	SD	LLR	Time (S)	CC	SD	LLR	
TD	0.843	-0.0029	15.0721	1.1225	0.816	-0.003	14.9864	1.1342	0.8295
DCT	0.846	0.0057	18.1942	1.1201	0.791	0.0055	14.9025	1.1453	0.8185
DST	0.867	0.0056	18.1525	1.1215	0.813	0.0057	14.9265	1.1633	0.84
DWT	1.201	0.0057	18.1942	1.1201	0.891	0.006	14.906	1.1071	1.046
Henon Map	Encryption				Decryption				Average Time (s)
	Time (S)	CC	SD	LLR	Time (S)	CC	SD	LLR	
TD	1.092	0.00006425	15.1013	1.2021	0.179	-0.0013	15.1229	0.9946	0.6355
DCT	0.917	-0.0068	15.1484	1.0603	0.225	-0.0012	15.1009	1.1396	0.571
DST	0.996	-0.00062593	15.1585	1.108	0.225	0.0012	15.128	1.0419	0.6105
DWT	1.276	-0.0045	15.1032	1.0871	0.272	-0.003	15.0783	1.1138	0.774
Standard Map	Encryption				Decryption				Average Time (s)
	Time (S)	CC	SD	LLR	Time (S)	CC	SD	LLR	
TD	0.823	-0.0113	15.2944	1.1586	0.754	-0.00072818	15.1652	1.173	0.7885
DCT	0.882	-0.0049	15.0921	1.0522	0.82	-0.0031	15.0147	0.9864	0.851
DST	0.865	0.0048	15.1693	1.1225	0.791	-0.0072	14.9675	1.1286	0.828
DWT	1.337	-0.0063	14.7672	1.1335	0.949	-0.0061	15.2912	1.1022	1.143
Baker Map	Encryption				Decryption				Average Time (s)
	Time (S)	CC	SD	LLR	Time (S)	CC	SD	LLR	
TD	0.262	0.0081	22.9029	0.622	0.064	1	0.00073023	4.8659E-08	0.163
DCT	0.307	0.0024	13.9032	0.4008	0.068	0.0014	39.0838	0.488	0.1875
DST	0.243	-0.0016	14.5304	0.4774	0.084	0.9775	1.1796	0.0196	0.1635
DWT	0.482	0.0054	14.5903	0.689	0.132	0.9789	1.1672	0.0104	0.307

## 5.2. Processing time Analysis – Encryption and Decryption

It is apparent from Table 2 that baker map with (DST) has lowest time for its encryption algorithm among other chaotic algorithms, while standard map with DWT has worst value. For decryption, baker with TD has lowest value for its decryption algorithm and standard map with DWT has worst value among other algorithms. Comparing time needed for

encryption and decryption algorithms will be especially beneficial when considering running encryption and decryption algorithm separately on transmitter and receiver's side. By comparing average time for both encryption and decryption algorithm, we can see that baker map with TD shows best value while Standard map with DWT show the worst value.



### 5.3. Correlation Coefficient analysis – Encryption

Lowest value for correlation coefficient means more better for encryption algorithm's quality, as shown from Table 2 that standard map with (TD) exhibits best value, while Henon

DCT comes in second, and logistic map in third, worst value for baker map with TD. It is also shown that baker with DST and DCT have also very good values compared to other algorithms, this is also shown from Figure 7.

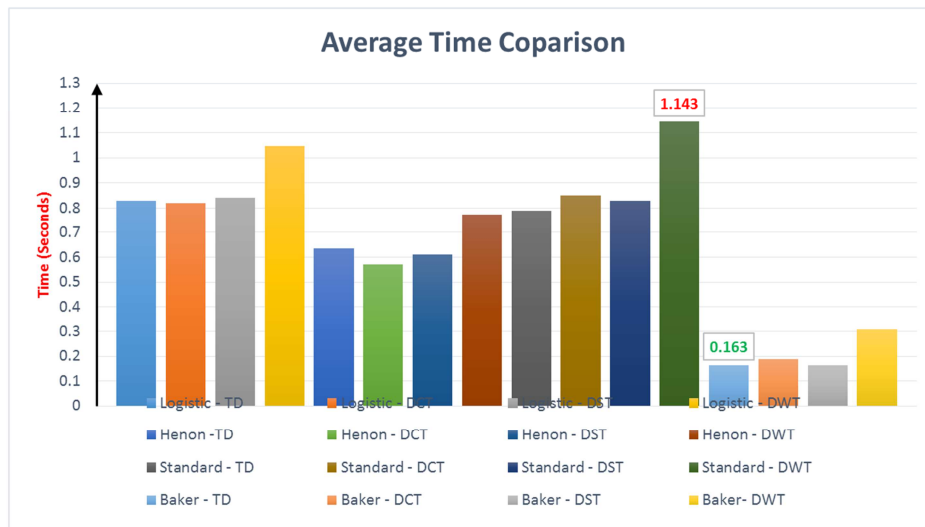


Figure 6. Average Time Comparison.

It is shown from Figure 6 that best average time with baker map – TD with value of 0.163 s, and worst with standard map- DWT with value of 1.143 seconds

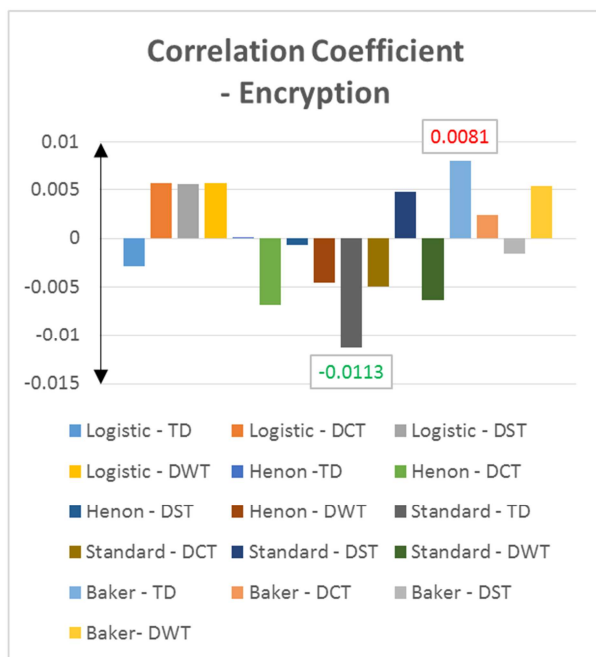
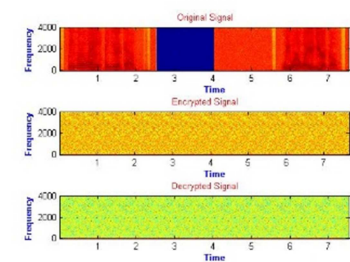


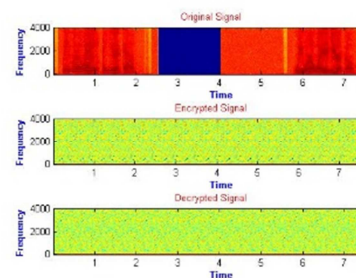
Figure 7. Encryption – Correlation Coefficient Comparison.

### 5.4. Correlation Coefficient Analysis – Decryption

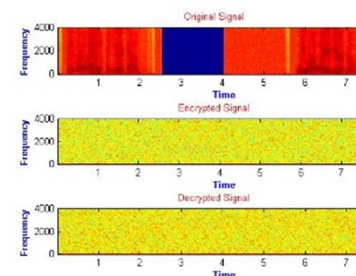
Highest value of correlation coefficient means best quality for decryption algorithm. It is shown from Table 2 that baker map with DWT has the highest value, while standard map with TD has worst value among other algorithms.



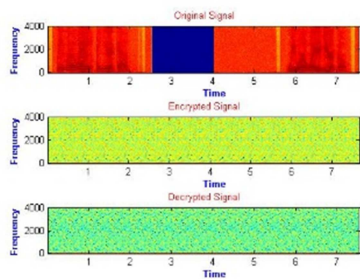
(a)



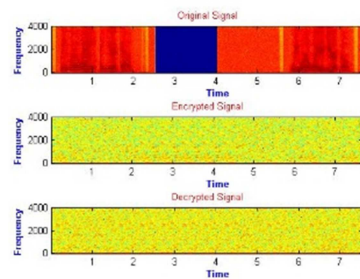
(b)



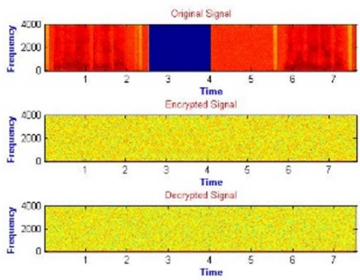
(c)



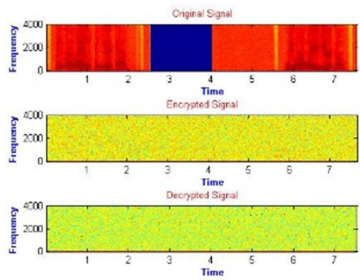
(d)



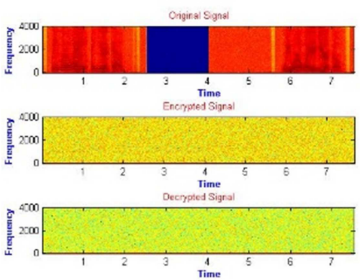
(i)



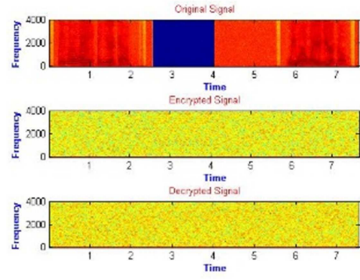
(e)



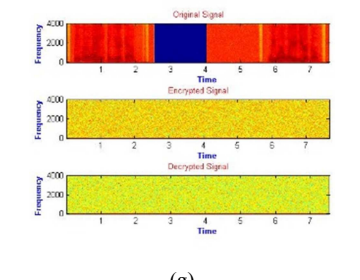
(j)



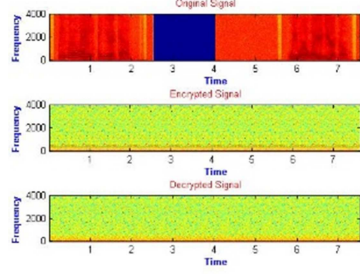
(f)



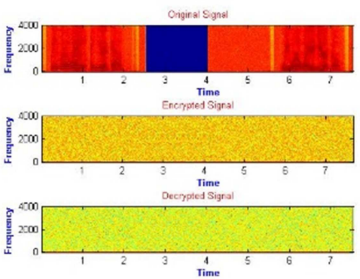
(k)



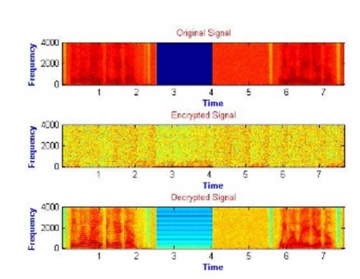
(g)



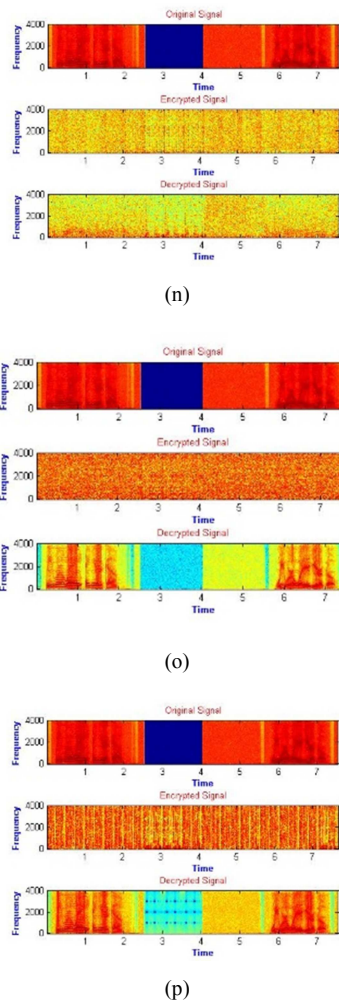
(l)



(h)



(m)



**Figure 8.** Spectrogram for (a) Logistic Map-TD, (b) Logistic Map-DCT, (c) Logistic Map-DST, (d) Logistic Map-DWT, (e) Henon Map-TD, (f) Henon Map-DCT, (g) Henon Map-DST, (h) Henon Map-DWT, (i) Standard Map-TD, (j) Standard Map-DCT, (k) Standard Map-DST, (l) Standard Map-DWT, (m) Baker Map-TD, (n) Baker Map-DCT, (o) Baker Map-DST, (p) Baker Map-DWT.

### 5.5. Spectral Distortion Analysis – Encryption

The highest value for spectral distortion means that best quality for encryption algorithms. It is apparent from Table 2 that baker map with TD has the best value providing best quality for encryption. The worst value for baker with DCT, is apparent from spectrograms shown in Figure 8(m,n). While values for SD for other algorithms (standard map, henon map, and logistic map) show a reasonable value for a good quality of encryption algorithms, in which standard map with TD comes in second arrangement after baker map with TD.

### 5.6. Spectral Distortion Analysis – Decryption

The lowest value for spectral distortion, provides best quality for encryption algorithm. Baker map with TD shows

the best decryption quality for audio speech signal, as it has the lowest value among others. Standard map with DWT comes second, and baker map with DCT has the worst value. This is apparent from spectrograms shown in Figure 8 (m,l,n) respectively. As shown from Figure 8(m), decryption spectrogram for baker map TD is the best similar to spectrogram of original speech signal than other spectrograms for decryption for other algorithms.

### 5.7. Log Likelihood Ratio Analysis – Encryption

The higher the value of log likelihood for encryption algorithms the better quality for encryption algorithm. It is shown from Table 2 that henon map with TD has the best value among others, standard map with TD comes next, and the worst value for baker map with DCT.

### 5.8. Log Likelihood Ratio Analysis – Decryption

The lowest value while nearest for zero is the value that means that decryption algorithm provide best decryption algorithm. From Table 2, we can find that the lowest value near to zero value is for baker map with TD, baker map with DWT comes next, while Logistic-2D map with DST has the worst value.

### 5.9. Key Sensitivity Test Analysis – Decryption

To consider decryption algorithm as a good decryption algorithm, it is expected to be sensitive enough to any small change in key used for decryption. We generate another two keys by changing small value of different sub-keys in the original key to form another two different decryption keys and achieve tests again using these two new keys (key2, key3) and compare results with results generated by original key (key 1) in Table 2 to conclude which algorithms exhibit a strong decryption algorithm.

Results collected for correlation coefficient (CC), spectral distortion (SD) and log likelihood ratio (LLR) for decryption algorithms for four chaotic algorithms are shown in Table 3:

Logistic-2D map exhibits a reasonable overall absolute percent change for both two keys. For key 2, which makes it a good enough decryption algorithm. It has maximum change percent with DWT of a average overall change of 32.11% change and lowest with TD of value 4.24%. For key 3, it has maximum change percent with DCT of a average overall change of 6.68% change and minimum with DST of value 3.42%.

Henon map also presents an overall acceptable absolute change for both two keys, but less sensitive than logistic 2D map. For key 2, it has maximum change percent with TD of a average overall change of 5.66% change and lowest with DCT of value 1.53%. For key 3, it has maximum change percent with DST of a average overall change of 5.77% change and minimum change value with DCT of value 2.02%.

**Table 3.** key sensitivity test, (a) Logistic Map, (b) Henon Map, (c) Standard Map, (d) Baker Map.

(a)

Key2	Time (S)	Absolute Change% from Key1	CC	Absolute Change% from Key1	SD	Absolute Change% from Key1	LLR	Absolute Change% from Key1	Average Time (s)	Absolute Change% from Key1	Overall Average Change %
TD	0.725	72.50%	-0.0011	0.11%	1.50E+01	1500.23%	1.16E+00	115.74%	0.7495	74.95%	352.71%
DCT	0.702	70.20%	-0.0025	0.25%	16.2378	1623.78%	1.1169	111.69%	0.746	74.60%	376.10%
DST	0.748	74.80%	-0.0026	0.26%	16.22	1622.00%	1.0839	108.39%	0.7585	75.85%	376.26%
DWT	0.744	74.40%	-0.0015	0.15%	16.1817	1618.17%	1.119	111.90%	0.8825	88.25%	378.57%
Key3	Time (S)	Absolute Change% from Key1	CC	Absolute Change% from Key1	SD	Absolute Change% from Key1	LLR	Absolute Change% from Key1	Average Time (s)	Absolute Change% from Key1	Overall Average Change %
TD	0.829	82.90%	0.0069	0.69%	1.50E+01	1496.27%	1.02E+00	102.12%	0.873	87.30%	353.86%
DCT	0.826	82.60%	0.0013	0.13%	15.0735	1507.35%	1.2208	122.08%	0.867	86.70%	359.77%
DST	0.815	81.50%	7.63E-04	0.08%	15.0641	1506.41%	1.1528	115.28%	0.856	85.60%	357.77%
DWT	0.946	94.60%	9.48E-04	0.09%	15.0799	1507.99%	1.1683	116.83%	1.0695	106.95%	365.29%

(b)

Key2	Time (S)	Absolute Change% from Key1	CC	Absolute Change% from Key1	SD	Absolute Change% from Key1	LLR	Absolute Change% from Key1	Average Time (s)	Absolute Change% from Key1	Overall Average Change %
TD	0.164	16.40%	-0.0029	0.29%	1.51E+01	1510.68%	1.10E+00	110.05%	0.491	49.10%	337.30%
DCT	0.208	20.80%	0.0042	0.42%	15.0783	1507.83%	1.1334	113.34%	0.5965	59.65%	340.41%
DST	0.223	22.30%	0.0055	0.55%	15.1633	1516.33%	1.0066	100.66%	0.5305	53.05%	338.58%
DWT	0.216	21.60%	-0.009	0.90%	15.0891	1508.91%	1.0502	105.02%	0.6425	64.25%	340.14%
Key3	Time (S)	Absolute Change% from Key1	CC	Absolute Change% from Key1	SD	Absolute Change% from Key1	LLR	Absolute Change% from Key1	Average Time (s)	Absolute Change% from Key1	Overall Average Change %
TD	0.16	16.00%	0.0002	0.02%	1.51E+01	1510.28%	1.06E+00	105.78%	0.6115	61.15%	338.65%
DCT	0.203	20.30%	-0.0049	0.49%	15.1053	1510.53%	1.155	115.50%	0.6265	62.65%	341.89%
DST	0.179	17.90%	0.0052	0.52%	15.1597	1515.97%	1.1986	119.86%	0.5605	56.05%	342.06%
DWT	0.233	23.30%	9.74E-04	0.10%	15.0982	1509.82%	1.0846	108.46%	0.7325	73.25%	342.99%

(c)

Key2	Time (S)	Absolute Change% from Key1	CC	Absolute Change% from Key1	SD	Absolute Change% from Key1	LLR	Absolute Change% from Key1	Average Time (s)	Absolute Change% from Key1	Overall Average Change %
TD	0.758	75.80%	0.0036	0.36%	1.53E+01	1534.64%	1.13E+00	113.04%	0.7725	77.25%	360.22%
DCT	0.843	84.30%	-0.0022	0.22%	15.0242	1502.42%	1.2308	123.08%	0.865	86.50%	359.30%
DST	0.768	76.80%	-0.0053	0.53%	15.1858	1518.58%	1.0892	108.92%	0.7915	79.15%	356.80%
DWT	0.818	81.80%	0.004	0.40%	15.3044	1530.44%	1.0374	103.74%	0.954	95.40%	362.36%
Key3	Time (S)	Absolute Change% from Key1	CC	Absolute Change% from Key1	SD	Absolute Change% from Key1	LLR	Absolute Change% from Key1	Average Time (s)	Absolute Change% from Key1	Overall Average Change %
TD	0.827	82.70%	-0.003	0.30%	1.50E+01	1499.03%	1.16E+00	115.67%	0.8635	86.35%	356.81%
DCT	0.9	90.00%	0.0034	0.34%	15.0832	1508.32%	1.1975	119.75%	0.939	93.90%	362.46%
DST	0.849	84.90%	-0.0041	0.41%	15.0613	1506.13%	1.0579	105.79%	0.892	89.20%	357.29%
DWT	0.913	91.30%	2.30E-03	0.23%	15.43	1543.00%	1.0603	106.03%	1.057	105.70%	369.25%

(d)

Key2	Time (S)	Absolute Change% from Key1	CC	Absolute Change% from Key1	SD	Absolute Change% from Key1	LLR	Absolute Change% from Key1	Average Time (s)	Absolute Change% from Key1	Overall Average Change %
TD	0.052	5.20%	1	100.00%	6.28E-04	0.06%	6.90E-08	0.00%	0.095	9.50%	22.95%
DCT	0.077	7.70%	0.0064	0.64%	39.78	3978.00%	0.3901	39.01%	0.125	12.50%	807.57%
DST	0.145	14.50%	0.9812	98.12%	1.7093	170.93%	0.009	0.90%	0.264	26.40%	62.17%
DWT	0.128	12.80%	0.9817	98.17%	1.0991	109.91%	0.0096	0.96%	0.3255	32.55%	50.88%
Key3	Time (S)	Absolute Change% from Key1	CC	Absolute Change% from Key1	SD	Absolute Change% from Key1	LLR	Absolute Change% from Key1	Average Time (s)	Absolute Change% from Key1	Overall Average Change %
TD	0.054	5.40%	1	100.00%	7.49E-04	0.07%	7.89E-08	0.00%	0.1	10.00%	23.09%
DCT	0.071	7.10%	0.0081	0.81%	39.0418	3904.18%	0.5807	58.07%	0.162	16.20%	797.27%
DST	0.131	13.10%	0.9433	94.33%	5.6352	563.52%	0.0264	2.64%	0.195	19.50%	138.62%
DWT	0.125	12.50%	0.9866	98.66%	0.822	82.20%	0.0142	1.42%	0.379	37.90%	46.54%



Standard map, shows an adequate overall acceptable absolute change for both keys. It is better sensitive than henonm, but less than logistic 2D map. For key 2, it has maximum change percent with DWT of a average overall change of 8.16% change and lowest value with TD of value 4.96%. For key 3, it has maximum change percent with DCT of a average overall change of 9.08% change and minimum change value with DST of value 5.79%.

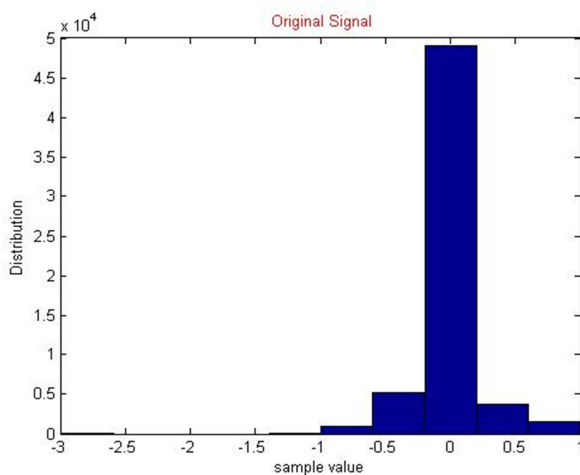


Figure 9. Original Modified Signal.

Baker map shows best sensitivity values among other algorithms. For key 2, it has maximum change percent with DCT of a average overall change of 17.41% change and the lowest with TD of value 1.6%. For key 3, it has maximum change percent with DST of a average overall change of 91.50% change and minimum change value with TD of value 1.46%.

It is concluded that baker map shows overallly the best sensitive behaviour among other algorithms for both keys.

This means that baker map has the best value as a decryption algorithm. It is the first one ,standard map comes after it, logistic map comes in third and finally henon map.

#### 5.10. Sensitivity for Plain Audio Test- Encryption

Another method to test the validity and strength of encryption algorithm is to change values of a byte of information for source audio file as shown in Figure 9, and then run tests again and check for possible changes in output values for encryption metric. A more overall change percentage means more strong and secure encryption algorithm and a less overall change percentage means less strong and less secure encryption algorithm. We run these tests on same audio speech file after modulation in values of one byte of its information and using same original key (key1). Results collected for four algorithms for encryption algorithms are listed in Table 4.

Logistic 2D map shows acceptable values of overll change percent to be strong enough as an encryption algorithm for speech voice. It has the best value with DWT of value 2.26% and the worst value with DST with value of 0.98%.

Henon map exhibits show very good values for overall change percent to be strong encryption algorithm for speech voice. It has the best value with DWT of value 8.85% and the worst value with DCT with value of 3.32%.

Standard map shows enough acceptable values to be a strong encryption algorithm for audio speech voice. It has the best value with TD of value 6.69% and the worst value with DST with value of 1.35%.

Finally, baker map exhibits very good values that makes, it a strong encryption algorithms for audio speech signals. It has the best value with DCT of value 6.01% and the worst value with DWT with value of 3.33%.

Table 4. Sensitivity for plain audio test, (a) Logistic Map, (b) Henon Map, (c) Standard Map, (d) Baker Map.

(a)

	Time (S)	Absolute Change% from Key1	CC	Absolute Change% from Key1	SD	Absolute Change% from Key1	LLR	Absolute Change% from Key1	Average Time (s)	Absolute Change% from Key1	Overall Average Change %
TD	0.856	85.60%	-0.0032	0.32%	1.50E+01	1502.29%	1.13E+00	112.61%	0.8345	83.45%	356.85%
DCT	0.885	88.50%	5.70E-03	0.57%	18.2242	1822.42%	1.1235	112.35%	0.8315	83.15%	421.40%
DST	0.873	87.30%	0.0055	0.55%	18.1824	1818.24%	1.1236	112.36%	0.829	82.90%	420.27%
DWT	1.147	114.70%	0.0057	0.57%	1.82E+01	1822.42%	1.1235	112.35%	1.0205	102.05%	430.42%

(b)

	Time (S)	Absolute Change% from Key1	CC	Absolute Change% from Key1	SD	Absolute Change% from Key1	LLR	Absolute Change% from Key1	Average Time (s)	Absolute Change% from Key1	Overall Average Change %
TD	0.903	90.30%	0.0019	0.19%	1.51E+01	1507.26%	1.12E+00	112.01%	0.532	53.20%	352.59%
DCT	0.917	91.70%	-3.60E-03	0.36%	15.0391	1503.91%	1.1009	110.09%	0.558	55.80%	352.37%
DST	0.939	93.90%	0.0017	0.17%	15.0172	1501.72%	1.1776	117.76%	0.5615	56.15%	353.94%
DWT	1.068	106.80%	-0.0011	0.11%	1.49E+01	1493.25%	1.1108	111.08%	0.7375	73.75%	357.00%



(c)

	Time (S)	Absolute Change% from Key1	CC	Absolute Change% from Key1	SD	Absolute Change% from Key1	LLR	Absolute Change% from Key1	Average Time (s)	Absolute Change% from Key1	Overall Average Change %
TD	0.875	87.50%	-0.001	0.10%	1.52E+01	1515.36%	1.25E+00	125.06%	0.828	82.80%	362.16%
DCT	0.926	92.60%	-1.40E-03	0.14%	14.9709	1497.09%	1.0932	109.32%	0.8875	88.75%	357.58%
DST	0.86	86.00%	0.0049	0.49%	15.1447	1514.47%	1.1571	115.71%	0.831	83.10%	359.95%
DWT	1.199	119.90%	-0.0038	0.38%	1.47E+01	1473.28%	1.1493	114.93%	1.095	109.50%	363.60%

(d)

	Time (S)	Absolute Change% from Key1	CC	Absolute Change% from Key1	SD	Absolute Change% from Key1	LLR	Absolute Change% from Key1	Average Time (s)	Absolute Change% from Key1	Overall Average Change %
TD	0.148	14.80%	0.0085	0.85%	2.28E+01	2276.10%	6.17E-01	61.67%	0.124	12.40%	473.16%
DCT	0.174	17.40%	0.0021	0.21%	13.9433	1394.33%	0.4101	41.01%	0.121	12.10%	293.01%
DST	0.178	17.80%	-0.001	0.10%	14.6082	1460.82%	0.4884	48.84%	0.124	12.40%	307.99%
DWT	0.546	54.60%	0.0052	0.52%	14.6453	1464.53%	0.6829	68.29%	0.348	34.80%	324.55%

It is concluded that henon map exhibits the best value as it g encryption algorithm among other algorithms, then standard map comes finally comes logistic 2D map.

## 6. Conclusion

It is concluded that all of four chaotic map algorithms are quite enough for using them in an audio cryptosystem in both time and transform domains. Standard map shows the best value as a strong encryption algorithm and a very good decryption algorithm, but requires more time than others for encryption and decryption time. While logistic map shows a considerable results that make it a very good decryption algorithm with very good short times required for both encryption and decryption. But, it comes in fourth arrangement as an encryption algorithm compared with other algorithms. Henon exhibits very good values as a strong encryption algorithm, but it is the last considerable decryption algorithm among others. Finally, baker map can be regarded as a well balanced in its merits and demerits. It exhibits the best value for encryption and decryption chaotic algorithm for audio signal in transform domains and time domain, while it is regarded as third choice as a decryption algorithm. Exclusively baker map with (TD) exhibits the best value for encryption and decryption and has the fast execution time as well. It is recommended to use baker map with (TD) in cryptosystem to provide the best enhancement for speech security and the less timing requirements as well.

## References

- [1] Li, T. and Jiang, J. Digital signal processing: fundamentals and applications. Academic Press, 2013.
- [2] Azriel, R. and Kak, A. Digital picture processing. Vol. 1. Elsevier, 2014.
- [3] Badih, G., et al. "Sample-optimal average-case sparse fourier transform in two dimensions." arXiv preprint arXiv: 1303.1209 (2013).
- [4] Ehsan, V., Wong, V. and Blake, I. "An Overview of Cryptography: A Guide to Modern Cryptography, Concepts, Methodologies, Tools, and Applications (2013): 102.
- [5] Zhongyun, H., et al. "2D Sine Logistic modulation map for image encryption." Information Sciences 297 (2015): 80-94
- [6] Kunal Kumar, k., et al. "Comparative study of image encryption using 2D chaotic map." Information Systems and Computer Networks (ISCON), 2014 International Conference on. IEEE, 2014.
- [7] Lin, Q., et al. "A blind source separation based method for speech encryption", IEEE Trans. On Circuits and Systems-I, vol. 53, no. 6, pp. 1320-1328, 2006.
- [8] Wu, Y. and Ng, B.P. "Speech scrambling with Hadamard transform in frequency domain", Proc. 6th Int. Conf. on Signal Processing, vol. 2, pp. 1560-1563, 2002.
- [9] Manjunath, G. and Anand, G. V. "Speech encryption using circulate transformations", Proc. IEEE, Int. Conf. Multimedia and Exp, vol. 1, pp. 553-556, 2002.
- [10] "Advanced Encryption System", Federal Information Processing Standards Publication, 197, 2001
- [11] Ghada, Z., et al. "Efficient and secure chaotic S-Box for wireless sensor network." Security and Communication Networks 7.2 (2014): 279-292.
- [12] Ahmed, A., et al. "Defense against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard." (2014): 1-1.
- [13] Prempratap, S. Gosawi, G. and Dubey, S. "Genetic Algorithms: A Technique For Cryptography Real Time Data Transmission." Binary Journal of Data Mining & Networking 4.2 (2014): 37-40.
- [14] Mosa E., et al "Encryption of Speech Signal with Multiple Secret Keys in Time Transform Domains " Int. J Speech Technol., Vol. 13 PP. 231-242 (2010).
- [15] Yicong, Z., Bao, L. and Philip Chen, CL. "A new 1D chaotic system for image encryption." Signal processing 97 (2014): 172-182.
- [16] Xiong, W. and Chen, G. "Constructing a chaotic system with any number of equilibria." Nonlinear Dynamics 71.3 (2013): 429-436.

- [17] Chittaranjan, P., et al. "Robust Watermarking Technique using 2D Logistic Map and Elliptic Curve Cryptosystem in Wavelets." *International Journal on Recent Trends in Engineering and Technology* 10.2 (2014): 70-77.
- [18] Rajinder, K. and Singh, Er. "Comparative Analysis and Implementation of Image Encryption Algorithms." *International Journal of Computer Science and Mobile Computing (IJCSMC)* 2.4 (2013): 170-176.
- [19] Samuel, S. and Takahasi, H. "Equilibrium measures for the Hénon map at the first bifurcation." *Nonlinearity* 26.6 (2013): 1719.
- [20] Narcís, M., Simó, C. and Viero, A. "From the Hénon conservative map to the Chirikov standard map for large parameter values." *Regular and Chaotic Dynamics* 18.5 (2013): 469-489.
- [21] Yushu, Z. and Xiao, Di. "Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform." *Optics and Lasers in Engineering* 51.4 (2013): 472-480.
- [22] Wei, Z., et al. "An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion." *Communications in Nonlinear Science and Numerical Simulation* 18.8 (2013): 2066-2080.
- [23] Iqtadar, H., et al. "Efficient method for designing chaotic S-boxes based on generalized Baker's map and TDERC chaotic sequence." *Nonlinear Dynamics* 74.1-2 (2013): 271-275.
- [24] Xiao-Jun, T. "Design of an image encryption scheme based on a multiple chaotic map." *Communications in Nonlinear Science and Numerical Simulation* 18.7 (2013): 1725-1733.
- [25] Wang, X. and Lin-Tao, L. "Cryptanalysis and improvement of a digital image encryption method with chaotic map lattices." *Chinese Physics B* 22.5 (2013): 050503.
- [26] Reza, D. and Gottemukkula, V. "Quality metrics for biometric authentication." U.S. Patent No. 8,724,857. 13 May 2014.
- [27] Sang Yeob, O. and Chung, K. "Target speech feature extraction using non-parametric correlation coefficient." *Cluster Computing* 17.3 (2014): 893-899.
- [28] El-Samie, F., et al. *Image Encryption: A Communication Perspective*. CRC Press, 2013.
- [29] Abdul Hamid, R., et al. "Encryption Quality Evaluation of Robust Chaotic Block Cipher for Digital Imaging." *International Journal of Recent Technology and Engineering (IJRTE)* ISSN: 2277-3878.
- [30] Mona, M., et al. "A New Image Encryption Scheme Based on Multiple Chaotic Systems in Different Modes of Operation."
- [31] Ahmed, E., et al. "Optical image encryption based on chaotic baker map and double random phase encoding." *Journal of Lightwave Technology* 31.15 (2013): 2533-2539.
- [32] ON, EFFICIENT VISUAL QUALITY INDEX BASED. "An Effective and Efficient Visual Quality Index based on Local Edge Gradients." *Visual Evaluation, Scaling and Transport of Secure Videos* (2013): 53.
- [33] Gilbert, M. and Peng, D. *Introduction*. Springer International Publishing, 2014.
- [34] Leeuwen, V., David A., and Brümmer, N. "The distribution of calibrated likelihood-ratios in speaker recognition." *arXiv preprint arXiv:1304.1199* (2013).
- [35] Navjot, K. and Kaur, U. "Audio Watermarking using Arnold transformation with DWT-DCT." *Issues* 1.1: 286-294.
- [36] Cheng, L. "On computing the two-dimensional (2-D) type IV discrete cosine transform (2-D DCT-IV)", *IEEE Signal Processing Letters*, vol. 8, Issue. 8, pp. 239 – 241, August 2001.
- [37] Jyoti, R. and Ahmad, T. "Performance Optimized DCT Domain Watermarking Technique with JPEG." *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, ISSN: 2278-3075.
- [38] Kekre, H. B., et al. "Comparative Performance of Image Scrambling in Transform Domain using Sinusoidal Transforms." *International Journal of Image Processing (IJIP)* 8.2 (2014): 49.
- [39] Ehab H., et al. "Robust and secure fractional wavelet image watermarking." *Signal, Image and Video Processing* (2014): 1-10.
- [40] Kekre, H. B., Sarode, T. and Natu, S. "Robust Watermarking Technique using Hybrid Wavelet Transform Generated from Kekre Transform and Discrete Cosine Transform." *International Journal of Scientific and Research Publications*: 152.
- [41] Xueyao, L. Hua, X. and Bailing, C. "Noisy Speech Enhancement Based on Discrete Sine Transform", *First International Multi-Symposiums on Computer and Computational Sciences, IMSCCS 2006*, vol. 1, pp. 199 – 202, 2006.
- [42] Bernadin, S. L. and Foo, S. Y. "Wavelet Processing for Pitch Period Estimation", *Proceedings of the 38th Southeastern Symposium on System Theory Tennessee Technological University Cookeville, TN, USA, 5-7 March, 2006*.
- [43] Krishnan, V. and Jayakumar, A. "Speech Recognition of Isolated Malayalam Words Using Wavelet Features and Artificial Neural Network", *4th IEEE International Symposium on Electronic Design, Test & Applications, DELTA2008*, PP. 240- 243, 23-25 January, 2008.
- [44] Tufekci Z. and Gowdy J. N, "Feature Extraction Using Discrete Wavelet Transform for Speech Recognition", *Southeastcon 2000. Proceedings of the IEEE*, pp. 116 – 123, 7-9 April 2000.
- [45] Malik, S. and Afsar, F. A. "Wavelet Transform Based Automatic Speaker Recognition", *IEEE 13th International Multitopic Conference (INMIC2009)*, PP. 1-4, 14-15 December, 2009.

## Biography



**Mahmoud Farouk** is a M.Sc. student, he has more than 20 years of extensive managerial and technical professional experience leading head key international projects worldwide, his experience is covering domains like, ITIL, PMP, Networking (CCIE Voice, R&S), network security, data centre, cloud computing, he is interested in research in fields like voice security, mobile networking, cloud computing, and wireless network security.



**Osama A. Elshakankiry** received B.Sc. and M.Sc in Computer Science & Engineering from Faculty of Electronic Engineering, Menoufia University, Egypt in 1998 and 2003 respectively, and a Ph.D. in Computer Science from School of Computer Science, Faculty of Engineering and Physical Sciences, University of Manchester, UK in 2010. His research interests cover Network Security, Internet Security, Multimedia Security, Cryptography, and Steganography.



**Dr. Eng. Ahmed M. Elmahalawy** had earned his PhD from Czech technical university in 2009. He works as a lecturer in Computer Engineering and science Department, Faculty of Electronic Engineering, Minufiya University. His interest is in artificial Intelligence mainly Agent technology and multi Agent System and machine learning. He had many publications in these fields.