Journal of Theoretical and Applied Information Technology
31st January 2019. Vol.97. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REVIEW OF DCT AND CHAOTIC MAPS IN SPEECH SCRAMBLING

NIDAA ABDULMOHSIN ABBAS , ZEINA HASSAN RAZAQ
University of Babylon, Faculty of IT, Iraq
University of Babylon, Faculty of IT, Iraq
drnidaa_muhsin@ieee.org, zienah.alhadad@uokufa.edu.iq

ABSTRACT

The communication technology improved recently in many important fields in daily life, this increases the demands for techniques which are more suitable to these situations. Recently the orthogonal transformation represents a good choice for security especially if it combined with a studied way for permutation, this can be provided by chaotic mapping which provides perfect mechanism for permutation. In this paper, we concentrate on the most popular chaotic maps and what are the mappings that used with DCT as an example in our research for orthogonal transformation and finally summarize the performance of this works to give a hint for the researchers to decide the suitable combination for their problems according to their requirement.

Keywords: *Discrete Cosine Transform (DCT), Wavelet Transform(WT), Speech Scrambling, Inverse Discrete Cosine Transform (IDCT), Chaotic Pseudo-Random Number Generators (CPRNGs), Chaotic System (CS)*

1. INTRODUCTION

In the last years, due to the development of the technology of communication and the growing demand of applications of speech, security has become a crucial approach.

The communication of Speech is an important issue in the life, it has compact relation in many fields in our life like education, military, commerce, politics, news telecasting, phone banking, and e-learning. Depending on the improvement of new technologies and telecommunication of multimedia, a very large amount of essential speech information sent in a repetitive routine over networks every day. Important data protected to maintain its security before distribution or transmission. Certain cryptograph techniques are applied to ensure speech security when speech is sending via the unsecured channel, the operation of changing speech from the understandable form to the unintelligible state before carrying (ciphering). Traditionally, two kinds of speech ciphering are there: analog ciphering and digital encryption (scramble).

Digital speech (D.S.) encryption of signal generates encrypted D.S. from selected cryptosystems of digital speech such as DES or AES. While the algorithms of scrambling the speech represented by disarranging of segments of desired speech information either in frequency, time or in time–frequency domain or disarranging of specially calculated coefficients for each block of speech.

Although the Digital encryption algorithms need complex or very hard execution with a required large bandwidth for transmission, Digital encryption has an advantage of analog where it is more secure than analog.

Therefore, when we deal with limited bandwidth channels, the choice of analog scramblers is better. The cryptographic techniques are conventional and suitable in particular for the text information. The increasing need for security for bulk data capacity and redundant data of speech production that it fail computationally.

Therefore, the new needs of security of such bulky, redundant speech data require efficient speech security methods that provide high security for the speech data [1].

Some influential scrambling technique added to the traditional methods in the transform domain in order to improve the security of speech signals and protect the signal from the expected

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

attack types. Most important techniques used in such cases are the permutation methods which are complex in retrieval operation for the unauthorized receiver, and this complexity arises with the increasing of the used permutation. A crucial approach used in permutation methods is chaotic because of its perfect effects in improving the scrambling process.

The essential purpose of this paper is to review the scrambling systems of speech which essentially used the DCT method in speech scrambling with chaotic maps.

2. RELATED WORK

The research that relates to our paper present a survey of using chaotic systems, where some of them focus on using the chaotic system in image and other in audio speech, and some in both. The research that discuss the chaotic system in audio speech as : In [2] Mahmoud F and Osama F. present in their paper a comparison between encryption techniques of audio speech signal, which are different based on 2-D chaotic map algorithms, which are used with time domain and transform domain, they use logistic 2D map, Henon map, Baker map, and Standard map. The research that discusses the chaotic maps in the image as Pooja Kathil, et. al.in [3] analyze the encryption techniques of the digital image by using chaotic maps. And they focus on approaches to cipher the image by using chaotic maps. Because of the defects of image encryption techniques, They use chaotic maps to enhance these techniques. In [4] J. Gayathri and S. Subashini summarize the encryption method used for an image that uses the chaotic system, and then they discuss the efficiency constraint and security. Priya R Sankpal, and P A Vijaya, in [5] focus on their survey on the chaotic methods that used in image encryption, In [6] Ephin M, Judy Ann present a survey of different choose-based encryption techniques used in image encryption. Er. Ankita, and Maneesha in [7] present chaotic maps used in image encryption and decryption, they study different chaotic maps as sine map, Arnold cat map, tent map, and logistic map. Garima T. and Nishchol M. in [8] present the encryption method based on chaotic maps. They analyze the image encryption algorithm and present a comparison between them according to different parameters. Zankhana M and, Hiren V, in [9] present a review on some chaotic techniques used in encrypting the Geological image, they use Chaotic Series and logistic Maps, and they compare the results with AES algorithm. Chetana S. et.al in [10] present Chaotic secret writing scheme for encrypting Image secret writing which is used in medical science, geographical satellite, and military. And the other research that presents the chaotic maps in both audio speech and image as Roman S. et. al. in [11] present the utilization of the discrete dissipative chaotic system and time continuous chaotic system that used as chaotic pseudo-random number generators (CPRNGs). And they simulate, analyze, and compare several chaotic systems. And the book that present the basics of using chaotic in Multimedia security in general where Zhaopin Su et.al.,in [12] present in their book some basic principles that differ between the methods, and discuss them as full encryption, and Partial encryption, according the security, compression ratio test, and time analysis, and they discuss the algorithms based on chaotic stream cipher, and based on chaotic block cipher. And discuss the Chaos-based encryption algorithms for video and audio.

Our paper reviews the papers that use chaotic maps with Discrete Cosine Transform, which used in encryption and decryption the speech signal.

3. SPEECH SCRAMBLING

Speech scrambling is used in converting the speech information to another unintelligible form.

3.1 Time Domain Scrambler

It is a method in which the order of the time segments rearranged and this scrambling must be agreed between the sender and receiver. This information is named (scrambling code).

3.2 Frequency Domain Scrambler

Scrambling in Frequency domain partition each block of the speech signal to (M) bands of frequency, and then rearranged according to some key, and the inverse of this arrangement applied in the receiver side to obtain the original speech signal block.

3.3Bi-Dimensional (Time-Frequency Scrambler)

Scrambling process in Time-frequency uses merging operation between time domain scrambler with frequency domain scrambler. Firstly, each frame of the selected signal of speech is divided into M homogenous sub bands and split the outputs of the first stage to N segments as the second stage. Then the output segments are permuted and produce a final novel frame of the signal. This scrambling method provides slow intelligibility in the output signal.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.4 Transform-Domain Scramblers (TD)

TD scramblers split the original signal of speech to a number of blocks and a suitable matrix of transformation will be used in multiplying by the selected vector and in order to find the intermediate transformed signal, then these calculated coefficients from the previous transformation are divided into a number of segments in order to rearrange in some certain order. After applying the inverse transformation in receiver side the received signal recover the original one of speech.

4. DISCRETE COSINE TRANSFORM (DCT)

The DCT consist of real part of the discrete Fourier transform (DFT),[23 and 15]and it has good compaction of energy and it provides zero residual intelligibility[17].

The DCT is defined by equation (1):

$$X(k)= \sqrt{2/n}C_k \sum_{n=0}^{N-1} x(n)\, cos(\frac{\pi k(2n+1)}{2N}) \quad (1)$$

$0 \le k \le N-1$

IDCT is defined in equation (2) as:

$$x(n)= \sqrt{2/n} \sum_{n=0}^{N-1} C_k X(n)\, cos(\frac{\pi k(2n+1)}{2N}) \quad (2)$$

$0 \le n \le N-1$

$$\text{Where} C_{m=} \begin{matrix} \frac{1}{\sqrt{2}} & if\ m=0 \\ 1 & otherwise \end{matrix} \quad (3)$$

2D DCT is defined as:

$$F(jk)= a(j)a(k) \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} f(mn) \cos\left(\frac{(2m+1)j\pi}{2N}\right) \cos\left(\frac{(2m+1)k\pi}{2N}\right) \quad (4)$$

The (2D-IDCT) is defined as:

$$F(jk)= \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} a(j)a(k)F(jk)\, cos\left(\frac{(2m+1)j\pi}{2N}\right) \cos\left(\frac{(2m+1)k\pi}{2N}\right) \quad (5)$$

5. CHAOTIC SYSTEM (CS)

A chaotic system can be defined as a system with nonlinear, deterministic and dynamical behavior and provide pseudorandom characteristic. The outputs of these systems vary according to some related parameters and starting conditions. Different values of parameters produce different states of oscillations at the result of chaotic systems.

The main pros of CS are sensitivity to initial conditions, random behavior and the setting of parameters that makes it very important in ciphering to fulfill the properties of cryptographic such as disorder, diffusion, and confusion. A simple variation in starting states or in the setting of parameters may be lead to big differences in the final result after applying few iterations. Thus, this state makes CS very important in generating a pseudorandom number.

Mathematically, a function that introduces chaotic action is clarified as a chaotic map or function [13].The most popular types of chaotic maps:

5.1 Logistic Map:

5.1.1 Logistic1-D Map

The logistic map is a simplest chaotic function that has been raised recently for some applications of cryptography. This function can be explained as:

$$xn+1=r.xn.(1-xn) \quad (6)$$

Where the value of xn is within the period (0, 1),r is a positive number and r <=4.

Value of parameter (r) controls logistic map behavior. When r=3.57 or greater, iterations become completely chaotic and improve the encryption purpose. The maximum value of (r)will be chosen in order to determine a highly chaotic signal.

5.1.2 Logistic 2-D Map

The 2-logistic map has a high complexity compared to 1-D map, and (r) controls its complexity. It gives more effectiveness and security for confusion and diffusion in both block and stream cipher methods.

The logistic 2D map is expressed

$$xi+1 = r(xy+1)xi(1-xi) \quad (7)$$

$$yi+1= r(3xi+1 +1)xi(1-yi) \quad (8)$$

The r determines of dynamicity type of map, and if the value of r greater than (1.19), system becomes unstable.

(xi, yi) are dimensions of point in the (i) th-iteration,(x i+1, y i+1) are dimensions of point in(i+1)th iteration.

5.2 Arnold Cat Map

It is a simple product of some of the principles of chaos. This map is a (2-d) map presented in the equation (9):

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} . \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod\ (N) \quad (9)$$

Where xn ,yn is the position in a square matrix (N×N), n=1,2,3,…, N-1

xn+1,yn+1 are the position mapping of the transformation, a and b are the positive integers arguments. The process of encryption will be done by means of iteration by using Arnold map.

Journal of Theoretical and Applied Information Technology
31st January 2019. Vol.97. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5.3. Henon Map

This map introduced in 1978. It is (2-D), nonlinear and discrete time that provide dynamical chaotic behavior and define by:

$$x_{n+1} = 1 + y_n - ax_n^2 \quad (10)$$

$$Y_{n+1} = bx_n \quad (11)$$

Where a and b the system becomes chaotic if a and b have values 1.4 and 0.3respectively. (xn and yn) is initial values.

5.4 Standard Map

It is also called Chirikov-Taylor and also called Chirikov standard map, it considered a (2-D) map. Which is defined by the equation (12) and (13) as:

$$P_{i+1} = p + k\ sinx \quad (12)$$

$$X_{i+1} = x + p_{i+1} \quad (13)$$

After one iteration, the variables will be (Pi+1 and Xi+1) and K effects the chaos degree.

5.5 Zaslavsky Map

This Map is a nonlinear, dynamical and discrete time system explained in 1978. It produces dynamic and deterministic behavior which represent an essential part of the encryption algorithms. In deterministic chaos, the important features are Pseudo Random Numbers and also the sensitivity to the initial state.

$$y_{n+1} = mod\ (y_n + v(1 + \mu z_n) + \epsilon v \mu z_n \cos(2\pi\ y_n), 1) \quad (14)$$

$$z_{n+1} = e^{-r}(z_n + \cos(2\pi y_n)) \quad (15)$$

Where $\mu = \frac{1-e^{-r}}{r}$

This map provides chaotic behavior when:

r=3.0 $v = \frac{400}{3}$ and $\epsilon = 0.3$

The Zaslavsky map equation(16)is iterated (Ns) times.

$$x_i = mod\ (abs\ (integer\ (z_n * 10^9)), 2) \quad (16)$$

Normalization of the key stream in equation (17):

$$\overline{x} = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (17)$$

The xmin and xmax considered the values of minimum and maximum of the generated keys.

5.6 Baker Map

It represents an example of the (2D) map, it rearranges elements in new places as a square matrix. It has many chaotic system pros like low correlation, good randomness, and non-predictability. There are two kinds of this chaotic map, discretized and generalized.

5.6.1. Generalized Baker Map

The representation of the generalized map is

(1) (N)R*R is square matrix divided to L rectangle arrays that have a width which is ui and height is R where, R = u1+u2+….uk

(2) Rectangle arrays arranged in a special fashion where at the bottom the left one and at the top the right one.

(3) The rectangles which are Vertical arranged horizontally.

Figure (1-a) explain generalized chaotic baker map which has R =3, L =3 and, (u) = 1.

5.6.2. Discretized Baker Map

This map performs rearrangement of each element in the desired square matrix to another calculated position in this matrix. The Discretized Baker map can be explained as B(u1,u2,……,uk), and the values of (k) integers(u1,u2,……,uk), and selected in a way where each integer value (ui) divides (Z) Item at the position (r,s),and Zi = u1 + ……+ui.., such that0 ≤ s ≤ z and the Zi ≤ r ≤ zi +ui, moved to a new position as represented in the equation(18) :

$$B_{(u_i \ldots u_k)(r,s)} = \left[\frac{z}{u_i}(r - N_i) + S\ mod\ \left[\frac{Z}{u_i}\right], \frac{u_i}{Z}\left[S - S\ mod\ \left[\frac{Z}{u_i}\right]\right] + Z_i\right] \quad (18)$$

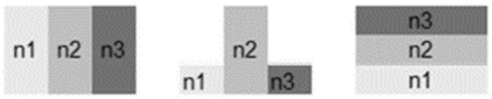
and applying the following conditions:

(1) (Z) matrix constitutes (Z×Z) matrix divided to (k) rectangles which are vertical that has Z and ui as height and width.

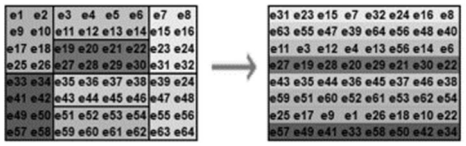
(2) Each vertical rectangle contains ui boxes, where each one has Z elements.

(3) Applying column by column mapping (right box at the top and left one at the bottom).

Consider an (8×8) matrix is explained in Figure (1-b) and use(2, 4, 2) as a secret key, and u1= 2, u2 = 4, and u3 = 2, Z= 8, for applying permutation phase and generating the mask using discretized baker map.



(a) Generalized baker map



ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(b) Discretized Baker Map – randomization of 8 x 8 matrix when the secret key u equal [2, 4, 2]

Figure (1): Baker Map

6. REVIEW OF THE TECHNIQUES USED DCT WITH CHAOTIC MAPS

Some researchers used DCT with suitable simple methods for scrambling, where the author in [21] supposed that the DCT is better performance compared to the other transformations, in the degree of intelligibility in the scrambled speech and the in the quality of the retrieved speech. Dalila S. and, Fatiha M. [22] suggested an encryption speech signals method that is based on selected circular shifting for columns and rows. This encryption system uses three secret keys. The first key generated randomly by using pseudo noise sequence generator, the 2nd and 3rd keys are generated by using the original key then the encryption operation apply (DCT) or the Discrete Sine Transform (DST) to reduce the intelligibility in the encrypted speech. These researchers finally, in future work, suggest replacing the secret keys by chaotic keys in order to increase system strength and security. Cryptosystem that uses the DCT with chaotic as a contribution to the traditional systems for increasing the total security and providing accepted resistance toward the cryptanalyst. The following are the researches according to the ways used for scrambling:

1- DCT & Baker map

Emad M. and Nagy W. et. al. introduced in [14] speech encryption method, by considering the chaotic Baker map in scrambling speech segments and using the masks in the transform domain and the time. They use Discrete Cosine Transform (DCT) or use Discrete Sine Transform (DST) in order to reduce final intelligibility that results after applying scrambling and masking processes in the time domain. They used Baker map for Permutation and maximized the total benefits from scrambling in the encryption method using suitable blocks with selected large-size to perform a permutated operation for more speech segments. The system main features of the system that it has security with high degree, low complexity, and a small delay.

The original speech signal is segmented and rearranged as blocks with fixed size and the secret key control the boxes size as represented in Figure (2). Then perform on elements of the fixed size block firstly the permutation (P), substitution (S), after that the elements permutated and finally rearranged frames with one dimension. The block size can be calculated by summing from secret key sub-keys, which control the substitution and permutation operations.

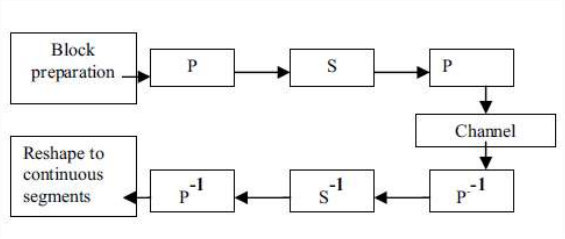


Figure (2): The system block diagram

2- DCT & Henon map, logistic 2D map, Standard map, baker map:

Mahmoud F., Osama F. et. al. [13] explained a useful comparison among different techniques of speech encryption and decryption for speech signals by using algorithms of two dimensions chaotic map in time and\or selected transform domains in order to select the best algorithm among them and discuss advantages and disadvantages of each algorithm. The researchers suggest using DCT, DST, DWT with suitable chaotic maps in order to exploit pros of the casual Conduct and sensitivity to the parameters values and basic conditions which help chaotic algorithms in performing the cryptographic systems. They use Henon, logistic 2D, Standard, baker, and Henon maps. Encryption process consists of the following steps as illustrated in figure (3):

Step 1: Framing and reshaping speech signal into blocks to represent a suitable form that readable by (MATLAB) programming language in this research.

Step 2: using the key in order to generate a suitable mask.

Step 3: using selected chaotic algorithms for Permutation (Henon Map ,Logistic Map, Baker Map, or Standard Map), by sampling and scrambling speech information and swapping their positions in speech matrix, and Substitution (which change values of the selected samples of speech by merging their values with suitable mask's value in accepted way).

Step 4: Applying either time domain or transform domain(DCT, DST, DWT), and then perform scrambling method by using the same chaotic algorithms explained in step 3, after that perform the substitution process and as the final stage in this step perform inversion of the selected transform (IDCT, IDST, IDWT).

Step 5: applying the permutation process by using the accepted chaotic algorithms which are explained in step 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Step 6: Reforming signal to (1-D) format to make it more suitable for saving speech information into a physical file, suitable quality metrics can be applied for the output file.

Decryption process represented by the next steps:

Step 1: using the key for generating Mask.

Step 2: reforming and changing (i-D) signal to blocks of 2-D, to make it suitable for reading by MATLAB language in this research.

Step 3: Applying the inverse of the permutation operation, by permuting and changing locations of speech information in a matrix of speech to previous original positions.

Step 4: Applying selected time domain or transform domain (DCT,DST, and DWT), and performing substitution operation (subtract mask), performing selected inverse of permutation by applying the same chaotic algorithms as explained in step 3, then applying inversion of time domain or transform domains (IDCT,IDST, and IDWT).

Step 5: Applying substitution (by subtracting mask), and then performing Inversion of Permutation operation.

Step 6: constructing signal with(1-D) format to make it in suitable form for saving speech information into a final file, finally file can be subjected to decryption quality metrics.

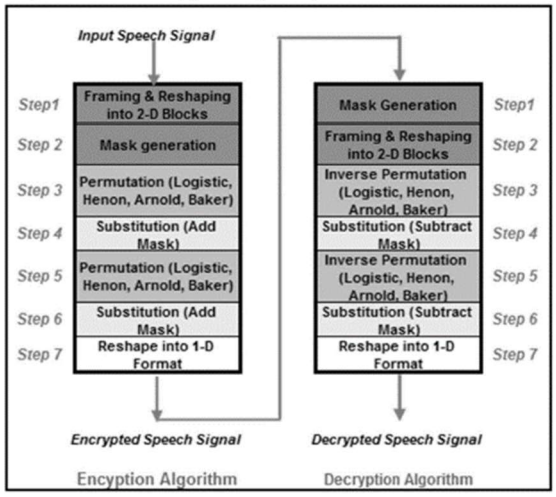


Figure (3)The Cryptosystem.

3- DCT & TD-ERCS chaotic map:

Zeeshan, Jan et.al. [16] Introduced a highly secure speech encryption method depending on efficient of (DCT) scrambling and amplitude scrambling. The permutation process is done by using TD-ERCS chaotic map.

The main importance of that research is designing and constructing a robust and secure speech encryption method. The designed system based on TD-ERCS chaotic maps and DCT. This system implemented and tested by different lengths of samples of speech. The diagram of this system explained in Figure (4). The proposed method is designed for applying the permutation of the speech signal over a band-limited channel, which passes frequencies which have a range (zero to 4 kHz). The speech signal is segmented into frames (consist of 64 samples) with the same length after transforming to the digital domain. Then applying DCT transform on each frame to calculate 64 (AC and DC) coefficients for each frame which is followed by amplitude scrambling of each one.

Sound information passed by applying a low pass filter(LPF) with selected cut-off frequency (3500 Hz)for isolating only the speech Signal of the human voice with suitable frequency range (300-3400) Hz. The information is passed through Analogue to-Digital (AID) converter then sampling process for the data depending on the Nyquist criterion. The information stream is divided into (64-bit) length blocks for the following processing. Each block sample is reversed followed by scaling its DC value down to zero. Then DCT is done on output bits by taking it from the input buffer. The pseudo random noise vector is mixed to the coefficients of the DCT method, obtained in the frequency domain. Here the scrambling in the frequency domain is done using pseudorandom numbers which are generated via TDERCS chaotic map.

Then performing the IDCT on these samples of speech and transforming it again into a time-domain signal.

Journal of Theoretical and Applied Information Technology
31st January 2019. Vol.97. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

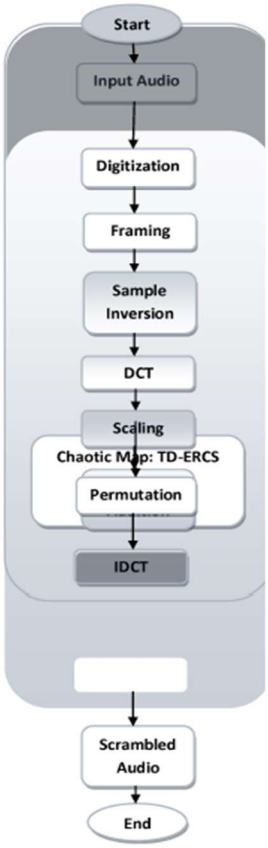


Figure (4): Flowchart of the proposed scheme

4 – DCT & Cat map and Zaslavsky map:

Farsana F J and Gopakumar K proposed a method for scrambling speech signal depend on Cat map and Zaslavsky map transform [17], by applying the following steps

The original signal of speech is first compressed by (DCT) to decrease the intelligibility founded in the signal, the original information is hidden by generating random numbers and Zaslavsky map , the output information is applied using Cat map to perplex the samples of data to make the voice unable to interpreted or intelligible by the authorized person, These two lower dimensional chaotic maps applied together to make the encryption process in higher dimensional space which hence expands the space of key and consequently improve the security against brute force attack, after that the signal of the original speech is converted into cipher text by diffusion process and confusion process of the samples of information with Cat transform and Zaslavsky map. This algorithm is represented in Figure(below). At the other part, the stream of the key is generated using the Zaslavsky method. The Initial conditions and parameters of the system of both maps are the key function which is given as the parameters to the encryption system. The speech signal is transformed to the frequency domain before applying(DCT). Transform domain method like DCT provides residual intelligibility equal to zero.

Speech information is confused by XOR-ing with the key stream of Zaslavsky map. The scrambles of Speech are confused through Cat transform. After the process confusion and diffusion, transformed encrypted signal of speech is converted back to the time domain by applying inverse DCT(IDCT). After modulation, the encrypted speech is sent through the channel. Recovering of the signal of original speech is performed at the receiver side. The encrypted speech is converted to transform domain by DCT prior to the diffusion process. Apply IDCT to recover the signal of the original speech. Decryption process structure similar to the encryption process structure. The same key should be generated by the receiver for retrieving the original signal. Therefore the transmitter and receiver should have the same keys(control parameters and initial values). The encryption and decryption processes are represented in figure (5):

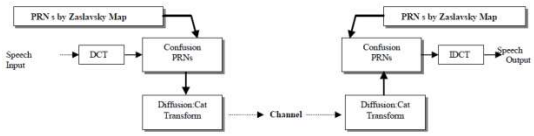


Figure (5): the encryption and decryption process

5- DCT & Tinkerbell map:

Farsana F J, AnuAssis, et .al. proposed encryption method based on Tinkerbell map asPseudo Random Number Generator (PRNG). Tinkerbell map used to produce Random Numbers to hide the original data to omit true sense of the original speech signal. Input speech signal initially compressed by applying (DCT) algorithm to decrease the final intelligibility. The encryption process and decryption process follows the process with a single level in lower dimensional space that will cause the computational simplicity of the algorithm.

The encryption of speech technique introduced depend on Tinkerbell map as pseudo-random bits generator which is a two dimensional chaotic map which shows discrete-time nonlinear dynamic behavior. This map presents deterministic random behavior.

Sensitivity to initial parameters and noise (Pseudo Random Numbers) are the important two key features of deterministic chaos. Pseudorandom bit generation methods are a crucial component in confusing the data samples to make information unintelligible to eavesdropping.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Various analyses show that this method is suitable for applications of cryptographic. The mathematical equations of Tinkerbell map is explained by:

$$x_{n+1} = x_n^2 - y_n^2 + ax_n + by_n \quad (19)$$

$$y_{n+1} = 2x_n y_n + cx_n + dy_n \quad (20)$$

Where x (0), and y (0) represent the initial condition, and the variables a, b, c, and d representthe control parameters. The system considered chaotic inthe nextstate:

x(0)=0.14562230 ,y(0)= -0.7427997,a=0.9,b=-0.6, c=2.0, d=0.5,

Keystream (PRNs) is generated through iterating theTinkerbell map for Ns (bit stream limit) times as follows:

$$z_i = mod\ (\ abs\ (\ integer\ (x_n * 10^9)), 2) \quad (21)$$

Normalization of the pseudo random numbers can be represented as follows:

$$\overline{z} = \frac{z - z_{min}}{z_{max} - z_{min}} \quad (22)$$

where zminis the min value of the constructed key zmaxis the max value of the constructed stream of the key.

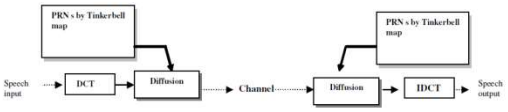


Figure (6) the encryption and decryption process

In the encryption process at the sender part, a key stream generated using two dimensional Tinkerbell map. The speech signal is converted to frequency domain by applying (DCT) before performing the encryption process, speech scrambles are diffused by XOR-ing each key stream with the speech scrambles as follows:

$$e_i = \overline{z} \oplus m_i \quad (23)$$

mi and ei are the samples of original speech and samples of encryption speech respectively. After the diffusion process transform domain, the encrypted speech signal is converted to the time domain by (IDCT). After modulation, the encrypted voice is transmitted through the channel.

In the Decryption process, the Retrieval of the plan speech signal is performed in the receiver side. The encrypted speech is converted to transform domain by applying DCT prior to the diffusion process. Apply IDCT to recover the original signal of speech. Decryption process has a structure similar to it in the encryption process. The Receiver side, the same stream of the key must be generated to recover the planned signal.

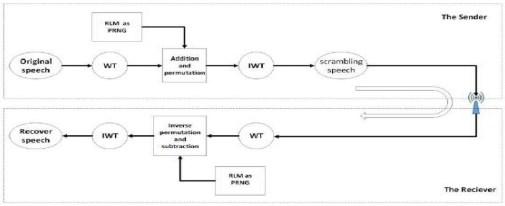
Therefore the same key and parameters should be provided to the sender and receiver:

$$m_i = \overline{z} \oplus e_i \quad (24)$$

6- DCT & Lorenz, Chen map:

Rana S. and Sattar B. proposed in [18] applied modification in two chaos maps (Lorenz, Chen) and used modified maps for the purpose of pseudorandom number generator (PRNG). By testing the noisy chaotic dynamics, the results explained that the modified maps have the best randomness compared with original maps. One method is using proposed random Lorenz map (RLM) as PRNG to permute the values of Wavelet coefficients in the speech signal. And the other select the modification of random Chen map (RCM) and using it as PRNG to permute the values of (DCT)for the speech signal.

The authors in this search use the two modified chaos maps and each one of them used for the purpose of pseudorandom number generation (PRNG). The following two figures explained the block diagram of the system of speech scrambling/descrambling using (RLM) as(PRNG) with using wavelet transform and using (RCM) as (PRNG) with using discrete cosine transform.



Figure(7): A block diagram of the proposed system of speech scrambling using (RLM)with(WT)

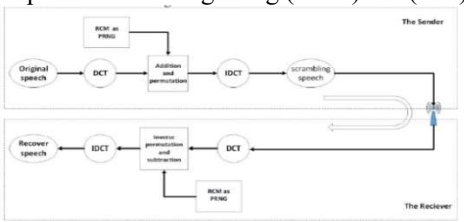


Figure (8): the block diagram of the speech scrambling system by using (RCM)with(DCT).

In the figure (7), which represent the sender side uses (RLM) as (PRNG) to get real random valuesRel_{RLM} .The proposed encryption process can be clarified as follows

1- Applying(WT)on the input signal of speech.
2- Applying Addition and scrambling processes between real values(coefficient) of WT of the planned signal withRel_{RLM},
3- Finally applying IWT on the scrambled values to get on the encrypted speech.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

At the receiver side, the same series of operations of RLM must be applied in order to perform the process of descrambling correctly and successfully. The descrambling process applying (WT) on the scrambled signal of speech. To retrieve the original speech signal, the operation of inverse permutation and subtraction must be done between WT coefficient that results from the scrambled signal andRel_{RLM}, and finally applying IWT on the values produced from the performing inverse permutation process.

In the second figure, both the sender side and receiver side apply(RCM) as (PRNG)for obtaining random and real values Rel_{RLM} to permute (DCT/ IDCT) signal for speech.

7- DCT & Lorenz map:

Sattar B. and Rana in [19] suggest and proposed the using of random Lorenz map (RLM) for the purpose of generating(PRN) and (PRB) and performing it in speech encryption of both women and men. The results become more chaotic compared with Lorenz map. Authors suggested a novel method for encryption speech by generating(PRN)for the purpose of permuting the values of speech signal after applying (DCT) encryption method.

Figure(9)explained a suggested block diagram of the encryption/decryption speech signal by using the desired map for generating(PRN)and using the DCT method.

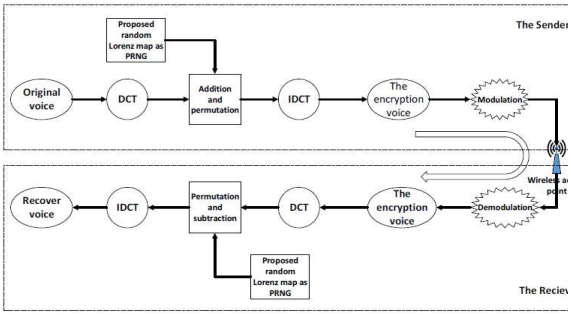


Figure (9): suggested block diagram of the proposed system of encryption/decryption of voice signal.

The pure input speech firstly is recording with decided(sampling frequency 8 KHz) and store it as.WAV file and treating the speech signal in the format of integer (16 bits) to avoid losing process of speech information when translating it to binary format and then recovering it to plan information.

The sender side perform random map of Lorenz for generating(PRN) to calculate random real values (Rel_{RLM}) or (Rel_{RLMi}). Then The encryption process can be done by applying DCT method on the plain voice signal, process such a as Addition and permutation between real DCT values of input voice signal with (Rel_{RLM}) or (Rel_{RLMi}), and finallyapplying IDCT on the output informationto calculate the encrypted final speech.

At the other side, the receiver must generate the same series of random Lorenz map by performing the decryption process successfully.

The decryption operation can be performed by applying DCT method in order to cipher speech signal, operations such as re-permutation and subtraction among real values of (DCT)for the signal of cipher speech and (Rel_{RLM}) or (Rel_{RLMi}), and finally the (IDCT) w,ill be applied on the re-permuted values to retrieve the originalspeech.

8- DCT & Arnold cat map:

Saad N. and Eman H. in [20] introduced speech encryption system based on permutation and substitution samples of speech by using special secret keys in time and transform domains. The system is a multilevel system to increase the security of the total system and to provide a final output signal with low residual intelligibility. The system used a chaotic logistic map for generating the keys and then applying the permutation process and mask keys to be done in the permutation and substitution processes. Arnold cat map is performed for maximizing the benefits of the permutation process in the final results. Arnold cat map performed in the final level of the proposed system to permute the speech samples. Expected results explain that the proposed encryption system provides an output speech signal with final low residual intelligibility, high quality of the recovered speech signal and the sensitivity of the key. The space of the keys in the encryption system can be determined as (2^348), which is very large enough for protecting the encryption signal against attacks like brute force.

The operations for describing the encrypted proposed cryptosystem for the speech signal can be illustrated in Figure (10). It consists of two essential stages: encryption and decryption for speech signals.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

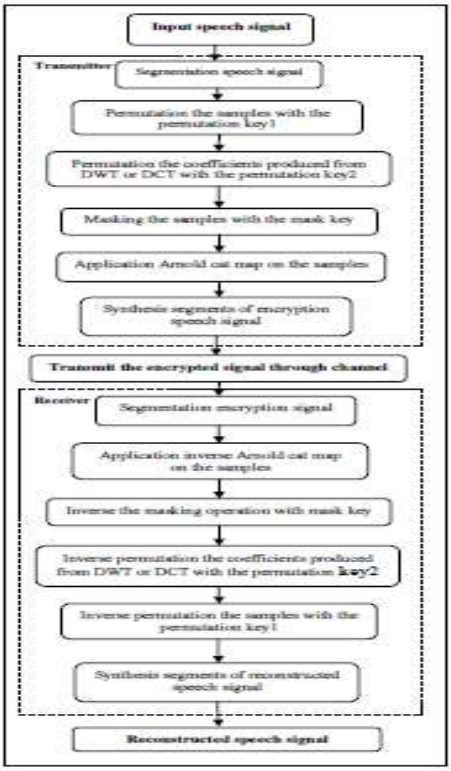


Figure (10): encryption and decryption for speech signals.

The first key used in the system is constructed by selecting two logistic maps and cross-coupled. The generated signal that output from the first map is entered as the input in the second map (initial condition) and vice versa.

The second key generated from the first one by applying permutation operation for the first key values. Initially, The first key used for permuting the samples of the voice signal in time domain whereas the other one used for permuting the (DWT or DCT) coefficients in the frequency domain and then Generation of Mask Key, Substitution process is performed for changing the samples amplitudes in each block because the permutation operation only changes positions, not values. Value of any sample replaced by applying(XOR) operation with a mask of the key values. The desired mask is constructed from six logistic maps:

$$x_{n+1} = r_n . x_n . (1 - x_n) \quad for \ 1 \leq n \leq 6 \quad (25)$$

The final output of these maps is real numbers in the interval (0, 1). And these real values converted into bits (0 or 1)according to the following equations:

$$A_i = \begin{cases} 0 & if \ x_i < 0.5 \\ 1 & if \ x_i \geq 0.5 \end{cases} \quad (26)$$

for $1 \leq i \leq 3$

$$A_i = \begin{cases} 0 & if \ x_i > 0.5 \\ 1 & if \ x_i \leq 0.5 \end{cases} \quad (27)$$

for $4 \leq i \leq 6$

The six values of A (i) are combined by using (XOR) operation to produce eight bits as in the following equations:

Bit1=A1 ⊕ A5 ⊕ A3
Bit2=A2 ⊕ A4 ⊕ A5
Bit3=A3 ⊕ A2 ⊕ A6
Bit4=A4 ⊕ A2 ⊕ A6
Bit5=A5 ⊕ A1 ⊕ A3
Bit6=A6 ⊕ A5 ⊕ A3
Bit7=A1 ⊕ A2 ⊕ A3
Bit8=A4 ⊕ A5 ⊕ A6

The (8) Bits represent the final output from one iteration for six maps. Each (8) Bits merged with the followed(8) Bits which are generated from the next iteration. The (16) Bits are changed to an integer number and then applying(XOR) operation with one sample in the block.

Another step of permutation is done on the samples of the speech in the time domain to increase the security level and prevent any cryptanalyst from expecting the original speech. Finally, each block is scrambled by applying Arnold map.

7. COMPARISON BETWEEN THE RESEARCHERS

In Table1 and Table2 we summarize the description of the previous ways we explain in the last subsection to highlight the performance of the techniques used, where we focus in Table1 and Table2 on the papers discussed above and a comparison between them, where the better performance in research [14] according to the Quality Assurance, Accuracy and security which give better outcomes.

Whereas in [13] the authors used a comparison between more than two methods of combination, where they use DCT with Henon, DCT with standard map, and DCT with Baker map. From this, we found that among these combinations the best is the DCT with the Logistic map.

8. CONCLUSION

According to the previous summery in table 1 and 2 of the researchers, we think that the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

research [14] has the better results according to the Quality Assurance, Accuracy, and security which overall has the better the outcomes.

Whereas in [13] the authors used a comparison between more than two methods of combination, where they use DCT with Henon, DCT with standard map, and DCT with Baker map. From this, we found that among these combinations the best is the DCT with a Logistic map, and in the secondly the combination of DCT with Baker, and then Henon and Standard respectively.

Where in DCT with Logistic, the SD ((spectral distortion) which represent the far off the spectrum of the encrypted audio speech signal from that of original signal which computed in dB have the best value in encryption (maximum) and in decryption (minimum). And CC (correlation coefficients that evaluate the quality of encryption algorithm i.e. the similarity of samples in original with encrypted sample) in decryption which represent the best value that is the maximum and best LLR(Log Likelihood Ration) which is an important metric to evaluate the quality of signal) in encryption.

In the side of key sensitivity, the combination of DCT with Baker map has the best results where it is more sensitive which reflect the affecting to any changes in the key hence provide better randomness and immunity to attacks. And the reminder combination arranged in the next sorting according to their performance in that side as DCT with a Logistic map, DCT with a standard map and finally with the less key sensitivity is DCT with Henon map.

REFERENCES:

[1] Farsana F J, AnuAssis, K Gopakumar *"Speech Encryption Based on Two Dimensional Maps",* International Journal of Advanced Engineering & Science Research (IJAES), Volume 4, Issue 1, February 2017

[2] Mahmoud Farouk, Osama Faragallah, Osama Elshakankiry, Ahmed Elmhalaway, "*Comparison of Audio Speech Cryptosystem Using 2-D Chaotic Map Algorithms*", Mathematics and Computer Science. Vol. 1, No. 4, 2016, pp. 66-81. October 10, 2016

[3] Pooja Kathil, Sachin Goyal, Ratish Agrawal, " *Survey on various image encryption schemed through Chaotic Maps* ", International Journal of A advanced Research in Computer Science, Volume 8, No. 5, May-June 2017.

[4] J. Gayathri, S. Subashini, " *A survey on security and efficiency issues in chaotic image encryption"*, International Journal of Information and Computer Security, Volume 8 Issue 4, January 2016, Pages 347-38

[5] Priya R Sankpal, P A Vijaya, "*Image Encryption Using Chaotic Maps: A Survey"*, 2014 Fifth International Conference on Signal and Image Processing

[6] Ephin M, Judy Ann Joy, India, N. A. Vasanthi, *" Survey of Chaos based Image Encryption and Decryption Techniques*", Amrita International Conference of Women in Computing (AICWIC'13) Proceedings published by International Journal of Computer Applications (IJCA)

[7] Er. Ankita Gaur, Er. Maneesha Gupta, " *Review: Image Encryption Using Chaos Based algorithms*", Journal of Engineering Research and Applications, Vol. 4, Issue 3(Version 1), March 2014, pp.904-907

[8] Garima Tanwar, Nishchol Mishra, "*Survey on Image Encryption Techniques* ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 12, December 2015 ISSN: 2277 128X

[9] Zankhana Mistry, Hiren V Mer, " *A SURVEY ON ENHANCE SECURITY USING AES WITH MULTIPLE CHAOTIC MAPS*", International Journal of Advanced Engineering and Research Development Volume 2, Issue 1, January -2015

[10] Chetana Singh, Binay Kumar Pandey, DR.H.L.Mandoria, Ashok Kumar, " *A Review Paper on Chaotic Map Image Encryption Techniques"*, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 04 | Apr-2018

[11] Roman Senkerik, Michal Pluhacek, Ivan Zelinka, Donald Davendra, Zuzana Kominkova Oplatkova, *"A Brief Survey on the Chaotic Systems as the Pseudo Random Number Generators*", ISCS 2014: Interdisciplinary Symposium on Complex Systems pp 205-214

[12] Zhaopin Su, Guofu Zhang and Jianguo Jiang (2012). *"Multimedia Security: A Survey of Chaos-Based Encryption Technology",* Multimedia - A Multidisciplinary Approach to Complex Issues, Dr. Ioannis Karydis, (Ed.), ISBN: 978-953-51-0216-8

[13]Mahmoud Farouk, Osama Faragallah, Osama Elshakankiry , Ahmed Elmhala way *"Comparison of Audio Speech Cryptosystem Using 2-D Chaotic Map Algorithms"*, Mathematics and Computer Science Volume 1, Issue 4, November 2016, Pages: 66-81, Oct. 10, 2016.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[14]Emad Mosa, Nagy W. Messiha, Osama Zahran, Fathi E. Abd El-Samie, *"Chaotic encryption of speech signals"*, International Journal of Speech Technology, December 2011.

[15] Rosa A Asmara, Reza Agustina, Hidayatulloh, *"Comparison of Discrete Cosine Transforms (DCT), Discrete Fourier Transforms (DFT), and Discrete Wavelet Transforms (DWT) in Digital Image Watermarking"*, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 2, 2017

[16] Zeeshan Habib, Jan Sher Khan, Jawad Ahmad, Muazzam A. Khan, Fadia Ali Khan, *"Secure speech communication algorithm via DCT and TD-ERCS chaotic map"*, 2017

[17] Farsana F J, Gopakumar K, *"A Novel Approach for Speech Encryption: Zaslavsky Map as Pseudo Random Number Generator"*, 6th International

Table1: comparison of the researches [1, 3, 5, and 6]

Conference on Advances In Computing & Communications, ICACC 2016, 6-8, September 2016, Cochin, India

[18] Rana Saad Mohammed, Sattar B. Sadkhan, *"Speech scrambler based on Proposed Random Chaotic Maps*", 2016 Al-SadeqInternational Conference on Multidisciplinary in IT andCommunication Science and Applications (AIC-MITCSA) – IRAQ (9-10) May

[19] Sattar B. Sadkhan, RanaSaad Mohammed, *" A Proposed Voice Encryption Based on Random Lorenz Map with DCT Permutation"*, International Journal of Advancements in Computing Technology (IJACT), Volume 7, Number 3, May 2015

[20] SaadNajim Al Saad, Eman Hato, *"A Speech Encryption based on Chaotic Maps "*, International Journal of Computer Applications (0975 – 8887) Volume 93 – No 4, May 2014

[21] E. Dawson, *"Design of a Discrete Cosine Transform Based Speech Scrambler",* Electronics Letters 28th Vol. 27 No, March 1991.

[22] Dalila Slimani, FatihaMerazka *" Encryption of speech signal with multiple secret keys",* International Conference on Natural language and Speech Processing, ICNLSP 2015.

[23] Jithin James, Vinod J Thomas, *" A Comparative Study of Speech Compression using Different Transform Techniques"*, International Journal of Computer Applications (0975 – 8887) Vol. 97– No.2, July 2014.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Features and security values

Features	1	14	16	17
Security	High	**More high**	secure enough	High
Cryptanalysis Attack Prevention	Brute force attack	Known plaintext attack.	brute force attack	brute force attack
Application Area	Cryptographic applications.	Cryptographic applications	Cryptographic applications	Cryptographic applications
Implementation of Algorithm	Simple	Simple	-	Simple
Used technique	DCT & Tinkerbell map	DCT & Baker map	DCT & TD-ERCS chaotic map	DCT & Zaslavsky map and Cat map transform
The dimensions of maps	2D Tinkerbell map	2 D Baker map	1D TD-ERCS chaotic map	2D Zaslavsky map and 1D Cat map transform
Efficiency/Reliability	Good	Good	-	Good
Methodology/Environment	Matlab	-	Matlab *2012b*	MATLAB R2013
Accuracy (SNR)	Good	Good	-	Good
Key length or key space	Large key space	Variable key length	-	large key space
Quality Assurance	Good	High	**Excellent**	Good

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table2: comparison of the researches[18, 19, 20, and 13]

Features	18	19	20	13
Used technique	DCT & Lorenz, Chen chaotic maps	DCT & Lorenz	DCT & The logistic map, Arnold cat map	DCT & logistic
				DCT & Henon
				DCT &standard
				DCT & Baker
Security	Good	Good	**Very good**	Very good
				Good
				Intermediate
				Enough
Cryptanalysis Attack Prevention	brute force attack	brute force attack	brute-force attack	-
Application Area	Cryptographic applications.	Cryptographic applications	Cryptographic applications	Cryptographic applications
The dimensions of maps	3D Lorenz,3D Chen chaotic maps	3D Lorenz	1D logistic map, 2D Arnold cat map	2D_ logistic
				2D_ Henon
				2D_ standard
				2D_ Baker
Efficiency/Reliability	Good	Good	High	High
				Good
				Intermediate
				Enough
Methodology/ Environment	MATLAB (R2013a)	*MATLAB (R2013a)*	-	MATLAB (R 2010a)
Accuracy (SNR)	Good	Good	High	-
The key length or key space	-	Large key space	Large key space	-
Quality Assurance	Good	Good	Very Good	Very good
				Good
				Intermediate
				Enough