Modified Scrambling Based on permutation function Matrix and 2D-DMWT with QPSK System

Samir J. Mohammad **Laith A. Abdul-Rahaim**

Babylon University

Elaf G.Abdul Razak
Kufa University

Abstract

Since an DWT- DMWT based speech scrambler retains aconsiderable residual intelligibility in the scrambled speech; thispaper proposes a new speech-scrambling technique to remove theresidual intelligibility from the scrambled speech. The proposednew technique, based on the combination of an appropriate QPSK mapping method, can scramble speech withoutresidual intelligibility by permuting several frequencycomponents. Without residual intelligibility in the scrambledspeech, the proposed QPSK speech scrambler is secure from frequency domain attacksby eavesdroppers. In addition, the QPSK speech scrambler needs only two 2D(DWT-DMWT) operations insteadof the four required by the 1D(DWT-DMWT)based speech scrambler in systemstructure. Simulation results are also presented to show theeffectiveness of this proposed technique.

الخلاصة

يحتفظ خلط الإشارة الصوتية(Speech Scrambling) المعتمد على (DWT– DMWT) بوضوح متبقي لخلط الإشارة الصوتية. يقترح هذا البحث تقنية جديدة لخلط الإشارة الصوتية لإزالة الوضوحِ المتبقيِ من خلط الإشارة الصوتية. تستطيع هذه التقنية الجديدة المقترحة لخلط الإشارة الصوتية ،المعتمدة على تجميع طريقة ملائمة للتخطيط (QPSK) ، بدون وضوحِ متبقيِ بتبديل عدة مكونات تردد. بدون وضوحِ متبقيِ في خلط الإشارة الصوتية يكون خلط الإشارة الصوتية المقترح (QPSK) امن من هجماتِ مجالِ التردد من خلال المتصنّتين. بالإضافة إلى ذلك ، يحتاج خلط الإشارة الصوتية (QPSK) فقط اثنان عمليات (2D(DWT– DMWT بدلا من أربع عمليات (1D(DWT–DMWTمطلوبة لخلط الإشارة الصوتية في هيكلية النظام. وتعرض أيضا نتائج المحاكاة لإظهار مدى فعالية هذه التقنية المقترحة.

1.Introduction

SPEECH encryption has always been a very important part of military communications**.** Today, due to the fast development of computer technologies, microprocessors, integrated circuits, **LSI** and **VLSI,** modem cryptography, etc., speech encryption techniques have entered a completely new era. Technically speaking, digital encryption of speech is always the best approach, in which the original speech signal **x** is first digitized into a sequence of bits, x (k) which are then encrypted digitally into a different sequence of bits, y (k) before transmission.Digital transmission is always much more efficient than analog transmission, and it is much easier for digital encryption techniques to achieve a very high degree of security. Of course, this type of technique is still not quite compatible with today’s technical environment, i.e., most of the telephone systems are still analog instead of digital; most practical speech digitizers still require a relatively high bit rate which cannot be transmitted via standard analog telephone channels; and low bit-rate speech digitizers still imply relatively high complexity and poor quality. Furthermore, almost all techniques of this type require accurate synchronization between the transmitter and the receiver, i.e., exactly the same block of bits has to be processed by the encryption and decryption devices for signal recovery. The synchronization problem becomes the essential part of the implementation of such techniques. This not only tremendously worsens the complexity, but makes the transmission much more sensitive to channel conditions because slight synchronization error due to channel impairment can completely break the transmission. There is another type of speech encryption technique called scrambling. The original speech signal **x** is scrambled directly into a different signal y(t) in analog form before transmission. The encryption is represented by the transformation between **x(t)** and **y(t)** regardless of digitization. Since the scrambled signal is analog, with similar bandwidth and characteristics as the original speech signal, this type of technique is more compatible with today's technical environment, i.e., can be easily used with existing analog telephone systems. Some conventional techniques of this type, such as frequency inversion and band splitting, do not require synchronization at all for transmission. Although they have been very useful historically, these not true any longer, lately due to the low degree of security achievable. A new series of techniques of this type, the sample data scrambling, have been developed and used extensively in recent years, since it can preserve the advantages of scrambling techniques while tremendously improving the degree of security. The original speech **x** is first sampled into a series of sample data, **x(n).** Then scrambled into a different series of sample data, **y (n)** and recovered into a different signal ***y (t)***for transmission. These techniques have a relatively high degree of security and are compatible with today's

technical environment, thus, they are very useful in the present time. However, almost all these techniques also require synchronization between transmitter and receiver, because the transformation from **x (n)** into **y (n)** has to be performed frame by frame, and exactly the same frame of sample data has to be used in the scrambling and descrambling processes for correct signal recovery. This again complicates the implementation and makes, the transmission very sensitive to channel conditions. Recently, two new sample data scrambling techniques have been proposed**.** One scrambles the speech in frequency domain, and the other in time domain; both approaches preserve the advantages of the sample data scrambling, while eliminating the requirement for synchronization. In other words, no synchronization is required in the receiver at all. This not only simplifies the system structure, but significantly improves the feasibility and reliability of sample data scrambling techniques. The basic point here is that the synchronization isnecessary as long as the scrambling and descrambling are performed frame by frame. It becomes unnecessary when "frame" is not defined in the operation. Efficient speech encryption technique is required for recent communication, not only over digital but also analogue data transmission lines without invasion of privacy. Two types of speech encryption scheme have been proposed. The former type is the frequency bands swapping of analogue signal. The method can be used for wide variety of analogue and digital application systems since the method can transmit speech signal over standard telephone line with acceptable speech quality. According to the result of psycho acoustical evaluations, context of speech is suspected due to remained envelop information of speech. The latter method is the digital speech signal encrypted. It is based on redundant bit to protect speech information effectively. Although the method is secure, it is hard to apply the method to conventional analogue transmission line because the bandwidth is wide. In order to reduce the bit rate under the bandwidth for analogue line, a speech encryption system with a low bit rate coding algorithm is necessary.**Speech** can be described as an act of producing voice through the use of the vocal foldsand vocal apparatus to create a linguistic act designed to convey information.

1. Various types of linguistic acts where the audience consists of more than oneindividual, including public speaking, oration, and quotation.
2. The physical act of **speaking**, primarily through the use of vocal cords to producevoice. See phonology and linguistics for more detailed information on the physical actof speaking.However, speech can also take place inside one's head, known as intrapersonalcommunication, for example, when one thinks or utters sounds of approval or disapproval. Ata deeper level, one could even consider subconscious processes, including dreams whereaspects of oneself communicate with each other (see Sigmund Freud), as part of intrapersonalcommunication, even though most human beings do not seem to have direct access to suchcommunication [Hombrebueno D. J. S., elat 2009].

2.Scrambling Based FFTand permutation function Matrix

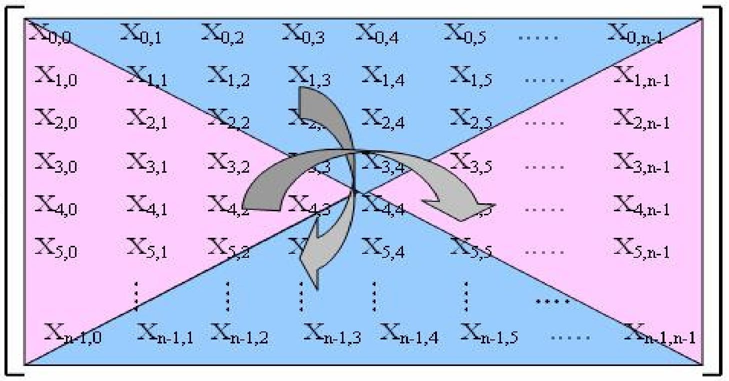
The basic idea of cryptology is hiding information [Roberto C. and García A., 2009], the people who has no authorization cannot know the true information. Encryption is to reverse the information with mathematical tools. The original information is called plaintext; the information enciphered is called cipher text. The process which is from plaintext to cipher text is called encryption; the reverse process is called deciphering. Deciphering is under the control of deciphering key, and the mathematical transformation that is used for deciphering is called data encryption algorithm. Cryptography evaluates the security of systems on the following four attributes: authentication, confidentiality, integrity and availability [Al-Shaer E. 2006, Yuan G., elat 2007]. The term scrambling has been, and still used to describe the encryption process to protect voice communication whether archived by digital or analog means [Ahmed J., elat 2003]. This process is carried out in frequency domain, time-domain as well as two-dimensional (combination of both) [Abdul-Rahaim L. A. 2009]. However, transform-domain data encryption and decryption has sought a significant role in secure communication systems. Among the transform-domain techniques, DCT and DWT have proved to be the best for data encryption [Abbas N. A. 2009].Because the data is stored in the computer transmitted through network in the term of cipher text, if the deciphering is leak out, the person who has no authorization won’t know the true meaning, and then the data can be secure. Meanwhile, anybody who has no authorization can’t forge right cipher text, so the data can’t be changed, then the data is surely safe [Do N. M., elat 2009]. That is why many real world cryptographic implementations use a compression program to reduce the size of the signal before encryption [Brandau M. 2008].Two-dimensional encryption that combines the frequency-domain encryption with the time-domain encryption [Yuan Z. 2003]. Besides, there are many other analogue data encryption methods in the transform domain, e.g., fast Fourier transform, discrete cosine transform and wavelet transform, etc. [Pereira W. 2001]. Recently, some new data encryption methods including chaotic cryptosystem [Gilley J. E. 2003]. In this paper we used hybrid structure of discrete wavelet transform and permutation function matrix as permutation and inverse discrete wavelet transform in building of both Encryption and decryption. The main aim is to investigate the effectiveness of the proposed new data ciphering based on hybrid transformation and its application in wireless OFDM Transceiver [Lee L. S., elat 1983,Gersho A. 1984].

The success of wavelets is mainly due to the good performance for piecewise smooth functions in one dimension. Unfortunately, such is not the case in two dimensions. In essence, wavelets are good at catching zero-dimensional or point singularities, but two-dimensional piecewise smooth signals resembling 2D-signals have one-dimensional singularities. That is, smooth regions are separated by edges, and while edges are discontinuous across, they are typically smooth curves. Intuitively, wavelets in two dimensions are obtained by a tensor-product of one dimensional wavelets and they are thus good at isolating the discontinuity across an edge, but will not see the smoothness along the edge. The properties of the new transform are demonstrated and studied in several applications . As an illustration, consider the 2D-signal denoising problem where there exist other approaches that explore the geometrical`regularity of edges, for example by chaining adjacent wavelet coefficients and then thresholding them over those contours [Gersho A. 1984].

In born of modern cryptography, symmetric cryptosystem gained its popularity in giving security to plaintext messages and data through text ciphering and data encryption. According to Simpson (2006), through symmetric cryptosystem, plaintexts and data can be transformed to unintelligible form using an encryption algorithm and a secret key. In this kind of cryptosystem, the same secret key is used for the decryption process to transform the cipher into its original form. The symmetric cryptosystem is faster compare to other cryptographic schemes based on Hook (2005), making it the best choice for encrypting large bulk of data. On the other hand, symmetric cryptosystem cannot able to verify the real source of the message and its integrity after data transmission as mentioned by Carnegie (2008). Use of symmetric cryptosystem doesn't give further assertion in part of the recipient about the real sender of the message as it doesn't support message non-repudiation. Through this, the sender of the message can able to deny himself as legitimate sender of the message. Another problem arose in the use of symmetric cryptosystem is that cannot able to verify the integrity of the message after the transmission process.

The number of possible permutation of elements is N!. However, all of these permutations cannot be used because some of them do not provide enough security [Cox R. V., elat 1986]. Let P be a set of permutation, and let P^{-1} be the set of inverse permutations corresponding to the permutation in P. The set S has to satisfy the requirement that any permutation in P must not produce an intelligence Encrypted data. It is difficult to evaluate the intelligibility of the Encrypted data signal and the intelligibility of the encrypted data signal by a quantitative criterion because intelligibility is substantially a subjective matter multiplied by a Permutation Function *(PF)* which can be simply generated. It can be seen that the permutation function Matrix is a square matrix with a dimension of N*N points. The permutation function of this matrix will change as the frequency bin of the FFT changes.

The permutation function Matrix is describe as replace upper triangle at lower triangle and left triangle atright triangle of the matrix shown as the following:



$$PFM = \begin{bmatrix} X_{0,0} & X_{0,1} & X_{0,2} & X_{0,3} & X_{0,4} & X_{0,5} & \cdots & X_{0,n-1} \\ X_{1,0} & X_{1,1} & X_{1,2} & X_{1,3} & X_{1,4} & X_{1,5} & \cdots & X_{1,n-1} \\ X_{2,0} & X_{2,1} & X_{2,2} & X_{2,3} & X_{2,4} & X_{2,5} & \cdots & X_{2,n-1} \\ X_{3,0} & X_{3,1} & X_{3,2} & X_{3,3} & X_{3,4} & X_{3,5} & \cdots & X_{3,n-1} \\ X_{4,0} & X_{4,1} & X_{4,2} & X_{4,3} & X_{4,4} & X_{4,5} & \cdots & X_{4,n-1} \\ X_{5,0} & X_{5,1} & X_{5,2} & X_{5,3} & X_{5,4} & X_{5,5} & \cdots & X_{5,n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \\ X_{n-1,0} & X_{n-1,1} & X_{n-1,2} & X_{n-1,3} & X_{n-1,4} & X_{n-1,5} & \cdots & X_{n-1,n-1} \end{bmatrix}$$

If the signal is multiplied by this PF at the transmitter side then it must be multiplied by the *Inverse of* permutation function *Matrix (IPFM)* at the receiver side in order to retrieve it, or in other form:

$$y_{receiver-side} = y_{received} * IPFM \quad (1)$$

Note that the last equation is a general equation, which means it depends on the location of the received signal that must be processed, and the location depends on the transmitter side, because at the receiver the inverse procedure will be done to process the signal.The resizing is very important for the purpose of mapping in the next two sections. Since the data must be converted to a suitable two dimensional matrix before the PFM mapping and then it must be reconverted to a one dimension after mapping to obtain the sub-carrier modulation as seen later. Figure (1) illustrates the main procedure of matrix resizing operations for both **1D** vectorto **2D** matrix and **2D** matrixto **1D** vector [Abdul-Rahaim L. A. 2009].

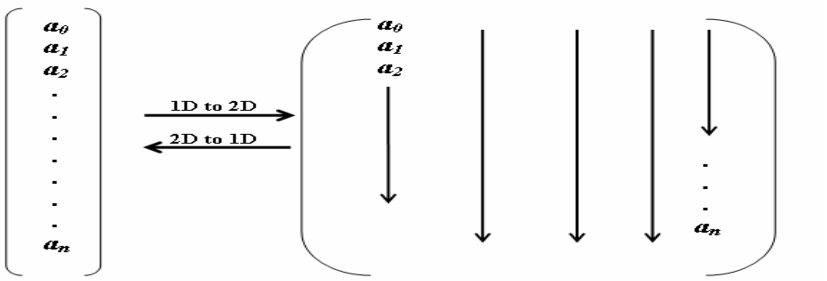


Figure (1) :Graphical illustration of matrix converter operations for both **1D** vectorto **2D** matrix &**2D** matrixto **1D** vector.

3.ScramblingQPSK System Based On Permutation Function Matrix and 2D-DWT.

In this section, the permutation function matrix and 2D-DWT and 2D-FFT which are presented in the previous section are proposed here as a new Encryption technique for the realization of QPSK transceivers. These transform will be used throughout the following sections as a data mapper to obtain a constellated data symbols prior to the sub-carrier modulation. The modified Encryption is proposed as a new Encryption in the communication systems as shown in Figure(2). The basic building blocks in the implementation of OFDM system after some important modification as it can be seen in the next section. In this model each MATLAB function was designed to simulate a specific part of obtaining the modifiedEncryption of a frame-based input data after achieving the necessary frame resizing according to the algorithm given in the previous section.

The procedure that illustrates the realization steps is shown in Figure (3), a signal flow diagram that explains the proposed Encryption QPSK transmitter [Abbas N. A. 2009].After converting the input data streams from serial to parallel form to construct a one dimensional vector that contains the data symbols to be transmitted,

$$d = (d_1 d_2 \ldots\ldots\ldots\ldots d_{N^2})^T \quad (2)$$

where, N is the specified frame length, and N should be power of 2 numbers. Then convert the data packets which are represented by the vector d from one-dimensional vector to an $N \times N$ two dimensional matrix D, according to the matrix resize operation.

Then take the proposed Encryption method to the matrix D to obtain the matrix *R* of dimensions *N*×*N*. The first step in computing the modified Encryption using DWT is computed 2D-FFT for the matrix *D*. The procedure of computing 2D-FFT is given in [Yeen L. and Fettweis G. -1993, Sadkhan S.B. el at 2004]. The output matrix will be dimensions of *N*×*N*. Then computing permutation function matrix of *N*×*N* then multiplying the input matrix by the permutation function matrix. After this step 2D-IDWT will be computed for the matrix, and the procedure of computing 2D-IDWT is given in [Al-Shaer E. 2006].The modification made on data dimensions in the end of calculation the modified Encryption matrix coefficients is *R*

$r = (r_1\, r_2 \ldots\ldots\ldots\, r_{N\times N})^T$(3)

At the end of this step, the propose encryptionis done and the complex valued symbols are now ready to send through.

After Modified Encryption based on 2D-DWT and permutation function matrix has been done,a pilot-carrier (training sequence) is generated which is a bipolar sequence {± 1}.The receiver will be informed about this sequence previously. The training sequence will be inserted in a parallel with data. The two sequences {data+training} take the QPSK*Tx* for the vector, (*r*) to obtain the sub-channel modulation [Abdul-Rahaim L. A. 2009].

Finally, the two sequences (training plus data) will be converted to one sequence, and P/S converts the signal from parallel form to a serial form (convert the vector(*s*) to serial data symbols): $s_1, s_2, \ldots\ldots\ldots\ldots\ldots, s_{2(N\times N)}$

The transmitted signal (***S***) will be transferred through the channel to the receiver**.**Each MATLAB function with this model was designed to perform a specific part of the system.

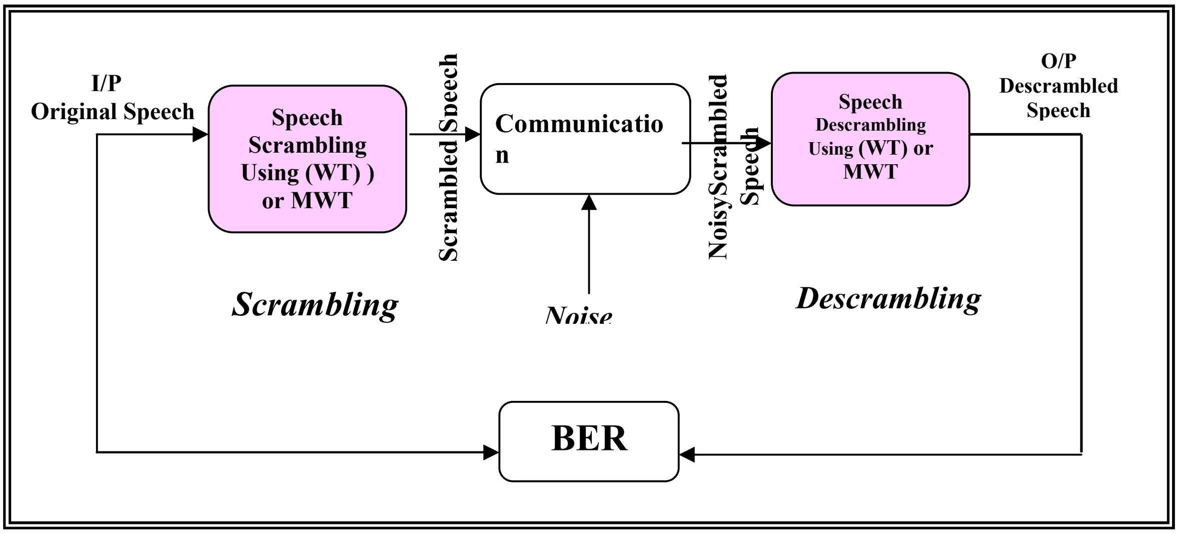


Figure (2) : Block Diagram of The Proposed Speech Scrambling System**.**

Figure(3) represents the procedure for the receiver to retrieve the transmitted data. In the receiver side the procedure is reversed as it can be noticed. Also one can take a close look to see how the data dimensions are changing suitably throughout the blocks. When the signal received in the receiver, S/P converts the received sequence to a parallel form; also the separation of the two sequenceswill be done. The received signal will be input to the OFDM Demodulator (*S*). After that the values corresponding to the zeros pad are removed, therefore the signal at the output of this step represents {data+training}. The training sequence will be used to estimate the channel frequency response as follows:

$$H(k) = \frac{\mathrm{Re}ceived\ \ Training\ \ Sample(k)}{Transmitted\ \ Training\ \ Sample(k)}, k = 1,2....,N \quad (4)$$

The channel frequency response which is found in the last step will be used to compensate the channel effects on the data, and the estimated data can be found using the following equation:

$$Estimate.data(k) = H_{estimate}^{-1}(k) * \mathrm{Re}ceived.data(k) \quad (5)$$
$$, k = 1,2....,N \times N$$

The output of channel compensator will be passed through the signal modified decryption. The reversed procedure of modified Encryptions used in the transmitter as can be noticed in figure (4). The last step is the P/S which converts the parallel form of the signal to a serial form.

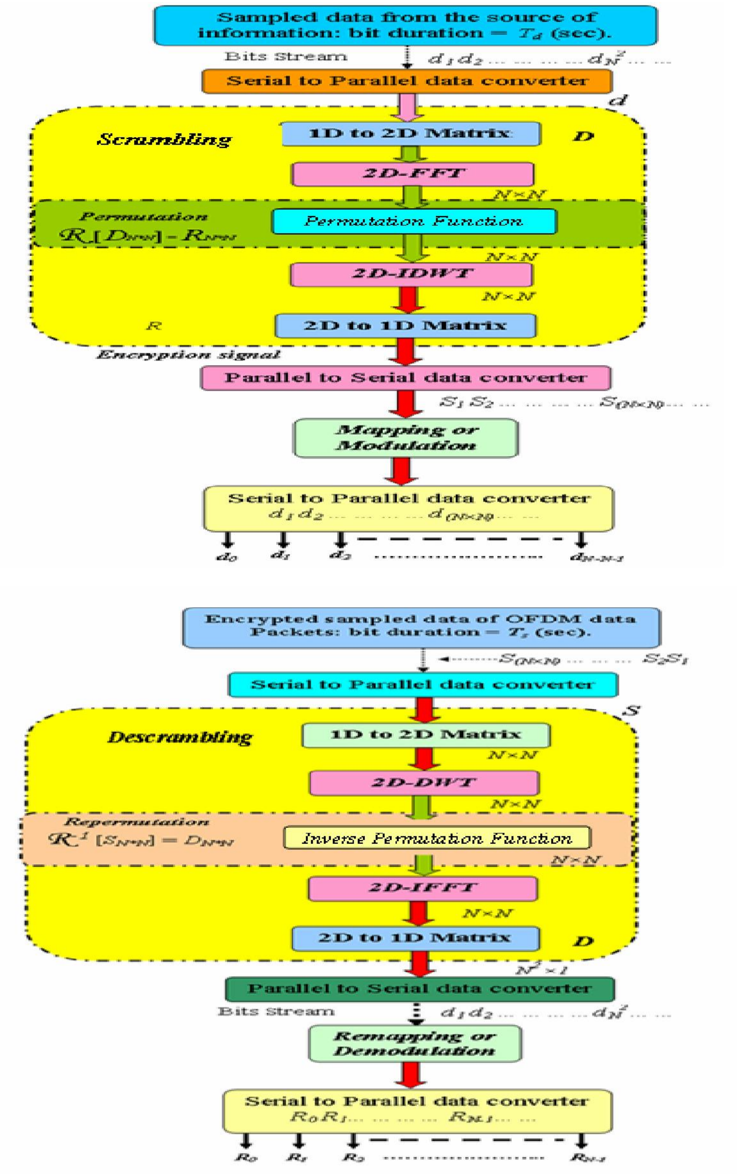

Sampled data from the source of information: bit duration = T_d (sec).
Bits Stream
$d_1 d_2$ ... ... d_{N^2} ... ...
Serial to Parallel data converter
d
Scrambling
1D to 2D Matrix
D
2D-FFT
N×N
Permutation
$\mathcal{R}[D_{N\times N}] = R_{N\times N}$
Permutation Function
N×N
2D-IDWT
N×N
R
2D to 1D Matrix
Encryption signal
Parallel to Serial data converter
$S_1 S_2$ ... ... $S_{(N\times N)}$ ... ...
Mapping or Modulation
Serial to Parallel data converter
$d_1 d_2$ ... ... $d_{(N\times N)}$ ... ...
d_0
d_1
d_2
$d_{N\cdot N-1}$
Encrypted sampled data of OFDM data Packets: bit duration = T_s (sec).
$S_{(N\times N)}$ ... ... $S_2 S_1$
Serial to Parallel data converter
S
Descrambling
1D to 2D Matrix
N×N
2D-DWT
N×N
Repermutation
$\mathcal{R}^{-1}[S_{N\times N}] = D_{N\times N}$
Inverse Permutation Function
N×N
2D-IFFT
N×N
2D to 1D Matrix
D
$N^2 \times 1$
Parallel to Serial data converter
Bits Stream
$d_1 d_2$ ... ... d_{N^2} ... ...
Remapping or Demodulation
Serial to Parallel data converter
$R_0 R_1$ ... ... $R_{N\cdot 1}$ ... ...
R_0
R_1
R_2
R_{N-1}

Figure (4): Schematic diagram for the procedure of the proposed

4. Simulation Results

In the proposed WT scrambling system, speech has been recorded with sampling frequency 11.025 KHz as wav files. The speech in Arabic or English, this speech may be spoken by a man or woman. At the scrambler, the sample speech signal is converted into frames with each frame containing 64 samples and then the Wavelet Transformation is performed on each frame. After that, the transform coefficients are permuted. The resulting scrambled speech signal is saved in a wave file. At the descrambler, frame by frame of length 64 samples are descrambled and saved in wave file. The proposed system investigate one type of Wavelet (Daubechies 4), with one level.

Two types of tests have been used to examine the performance of the simulation, these are :

1. **Subjective Test :**In which the scrambled speech files have been played back to a number of listeners to measure the residual intelligibility, subjectively. For all cases, the judge is that the files contain noise only, which means that the residual intelligibility is very low. The analog descrambled speech files have been tested in a similar way to measure the quality of the descrambled speech files, the judge is that the files are exactly the same as the original copies.
2. **Objective Test :** Is test to the quality of the descrambled speech, and is used to quantify the difference between original speech and descrambled speech. Generally, thebyte error rate is high (large value) which means that the quality is low, and thebyte error rate is law (law value) which means that the quality of the descrambled speech is high.

The proposed speech scrambling system have been tested under two states of the simulation free channel simulation and noisy channel simulation.

1. Free Channel Simulation

In the proposed WT scrambling system, speech have been recorded with sampling frequency 11.025 KHz as wav files. The speech in Arabic or English, this speech may be spoken by a man or woman. At the scrambler, the sample speech signal is converted into frames with each frame containing 64 samples and then the Wavelet Transformation is performed on each frame. After that, the transform coefficients are permuted . The resulting scrambled speech signal is saved in a wave file. At the descrambler, frame by frame of length 64 samples are descrambled and saved in wave file. The proposed systems investigate one type of Wavelet (Daubechies 4), with one leveland DMWTCS. Two types of tests have been used to examine the performance of the simulation, these are :

1. **Subjective Test :**In which the scrambled speech files have been played back to a number of listeners to measure the residual intelligibility, subjectively. For all cases, the judge is that the files contain noise only, which means that the residual intelligibility is very low. The analog descrambled speech files have been tested in a similar way to measure the quality of the descrambled speech files, the judge is that the files are exactly the same as the original copies.
2. **Objective Test :** Is test to the quality of the descrambled speech, and is used to quantify the difference between original speech and descrambled speech. Generally, thebyte error rate is high (large value) which means that the quality is low, and thebyte error rate is law (law value) which means that the quality of the descrambled speech is high.

The proposed speech scrambling systems have been tested under two states of the simulation free channel simulation and noisy channel simulation.

1. Free Channel Simulation

Simulation results of typical experiments with the scrambler, and the descrambler for an Arabic word spoken bywomen's voice"إيلاف ", usingDaubechies 4 Wavelet and one level.

a. Testing Arabic word spoken by woman's voice "إيلاف " as shown in Figure (5), is the original speech signal after apply scrambling result is shown in Figure (6), and reconstruct the original speech signal after apply descrambling result is shown in Figure (7).

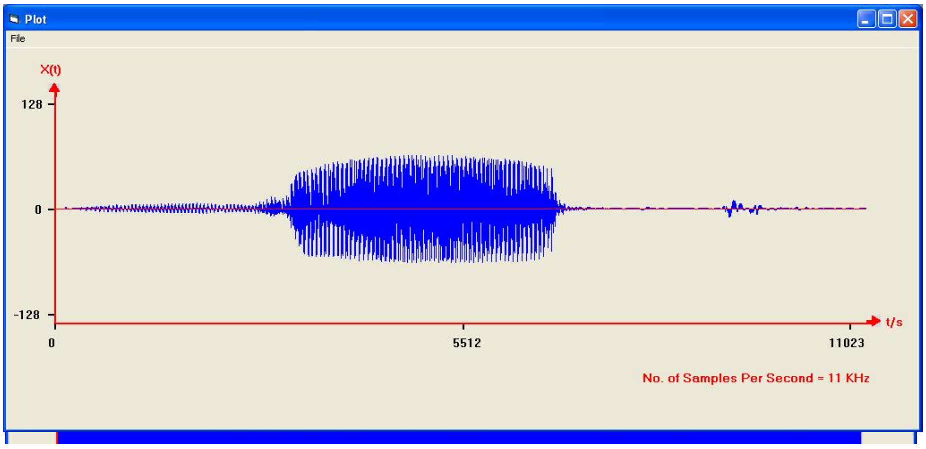


Figure (5) : Original Speech Signal.

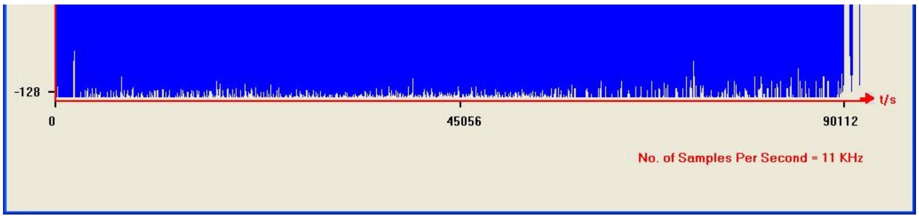


Figure (6) : Scrambled Speech Signal Using Daubechies 4 Wavelet With Level 1.

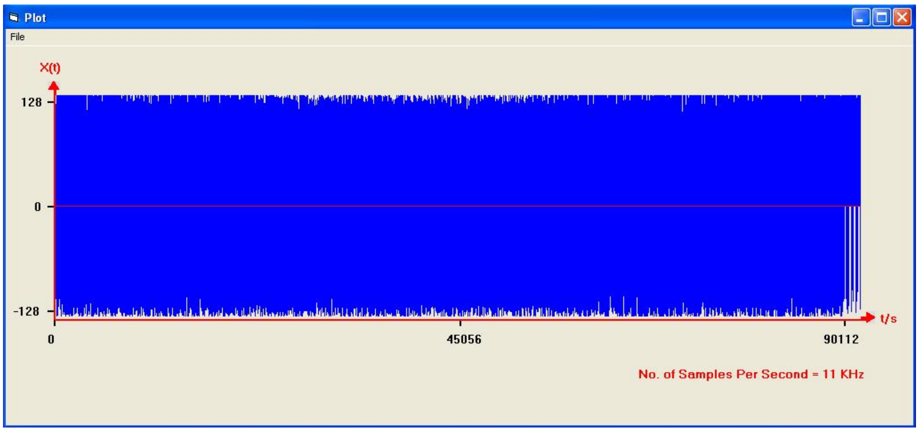


Figure (7) : Scrambled Speech Signal Using Multiwavelet.

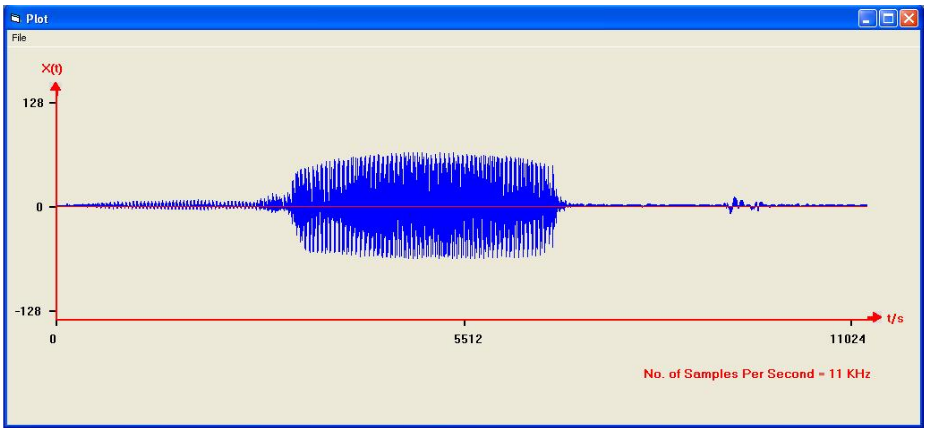


Figure (8) : Descrambled Speech Signal Using Daubechies 4 Wavelet With Level 1.

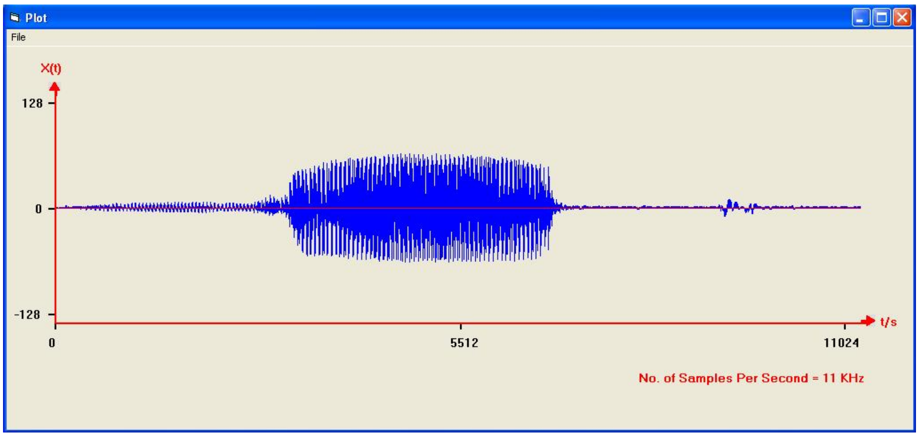


Figure (9) : Descrambled Speech Signal Using Multiwavelet

5. Simulation Results of QPSK with proposed Scrambler:

System parameters that will be used through the simulation are; T_d=*0.1µsec*; modified Scrambler window: 8×8; DWT bins= 64; Guard interval: Cyclic prefix approach with 26 symbol is added to the frame; Pilot-assisted channel estimator. The output of modified Scrambler is (16×6), and then the frame that will be sub carrier modulation of length 64×2 after the training is inserted into to the frame before sending through channel, while different types of channel models are taken into account during the simulation. First, an AWGN channel is considered with several SNR values. Then, multi-path Raleigh distributed fading channels are considered with two scenarios; Flat and multi-path selective fading cases. Fig.(3) is schematic block diagrams for the proposed QPSKtransceiver. The pilot-assisted channel estimator is proposed here to combat the fading effects as it was explained earlier in the previous section. It was found to be an efficient method especially for slow fading channels.

5.3 Simulation Results of QPSKwith proposed Scrambler:

In time-domain they are simply drawn as discrete-time signals but in frequency domain the distribution of energy is not as genuine as before the application of Scrambler process. Secondly, the spectrum is inverted altogether which flips the distribution of energy level as a function of frequency. Thirdly, signal is multiplied in frequency domain which is tantamount to convolution in time-domain. As the transmitted signal is in time-domain so any unauthorized person who wants to decrypt the signal without the knowledge of scheme, would have to convolve in time-domain which, unquestionably a very time consuming process in real-time systems. Further, he doesn't know the permutation order of the system that's why he would have to apply on each frame that will ideally take infinite time.These parameters are shown in table (1)

Table (1) Simulation Parameters

25 MHz	Bandwidth
AWGN	Channel model
Flat fading+AWGN	
Frequency selective fading+AWGN	

We have conducted an extensive exercise of experiments over a long period of time. These experiments including original, scrambled and descrambled speech were carried out using various speech segments of different time periods and genders. Since the residual intelligibility and quality of the recovered speech are largely subjective quantities; the scrambling and descrambling techniques are evaluated on the average results given by the trained listeners. In this regard, many subjective tests were conducted by using the methods adopted by [Gersho A., 1984] with the help of wave files. In a view to make these tests easily understandable for listeners, the wave files of said speech signals were played and heard by the trained listeners. In this exercise, thirty trained listeners who were all listened to these recorded 50 scrambled speech segments. Each segment consisted of the digits 0 to 9 spoken in group of four digits. Further, the tests were not confined to digits only but sentences and conversational segments were also used. In order to make tests stringent and more result-oriented, although it was laborious and time-consuming, all the tests were carried out in English, languages. The repetition of the digits on the same position is strictly avoided. The tests were made more inflexible than carried out by [Do N. M., elat 2007] by:

(i) Isolating the digits that were spoken by not only male but female as well.

(ii) Tests are not limited to digits only, sentences are also included. These segments are recorded.

(iii) Further, conversational segments are also carried out in three languages by both genders.

Some of the results conducted on proposed system using Matlab-7.4 are demonstrated in this paper. The close analysis of these signals and their subsequent transformation into frequency domain leave very remarkable and noteworthy observations. In time-domain they are simply drawn as discrete-time signals but in frequency domain the distribution of energy is not as genuine as before the application of Scrambler process. Secondly, the spectrum is inverted altogether which flips the distribution of energy level as a function of frequency. Thirdly, signal is multiplied in frequency domain which is tantamount to convolution in time-domain. As the transmitted signal is in time-domain so any unauthorized person who wants to decrypt the signal without the knowledge of scheme, would have to convolve in time-domain which, unquestionably a very time consuming process in real-time systems. Further, he doesn't know the permutation order of the

system that’s why he would have to apply on each frame that will ideally take infinite time.

A. The Scrambler-QPSKin AWGN Channel:

A program of MATLAB V7.4 was used to simulate the proposed modified Scrambler- QPSKtransceiver shown in Fig. (3). Several MATLAB functions were programmed to simulate the transceiver shown in Fig. (3).These include frame resizing, modified Scrambler-description, pilot carriers insertions-removing, etc. the result of the simulation for the proposed Scrambler-QPSKsystem is calculated and shown in Fig.(10), and which gives the BER performance of Scrambler-QPSKusing DWT and QPSK in AWGN channel. It is shown clearly that the Scrambler-QPSKusing 2D-DMWT Scrambler is much better than QPSK transceiver and the Scrambler of 2D-DWT QPSK .

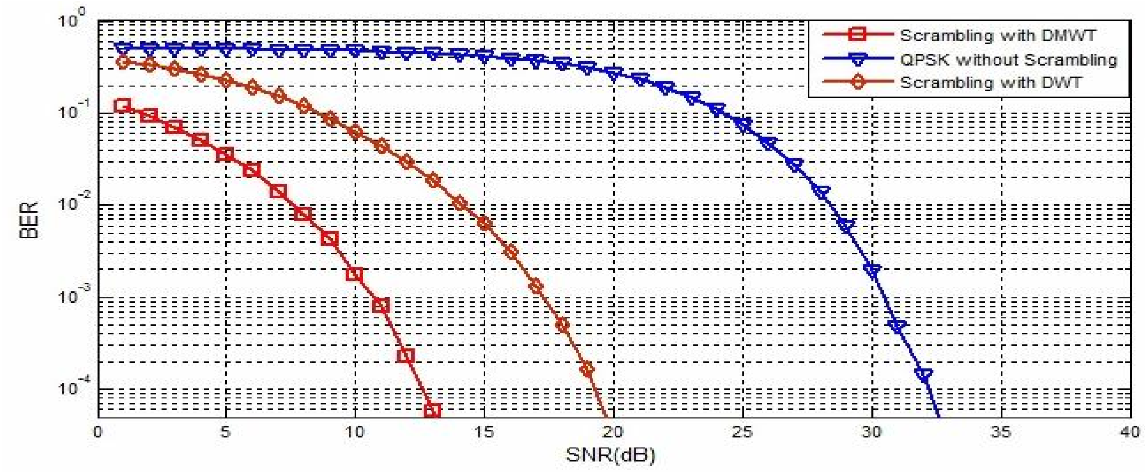


Fig ..(10)BER performance of proposed Scramblers in AWGN channel model

B. The Scrambler-QPSKin Flat fading channel

The same MATLAB V7.4 program that simulated in Fig. (3) is used here to simulate the results in flat fading channel with AWGN except a flat fading channel is added to the channel model. In this type of channel, the signal is affected by the flat fading with addition to AWGN; in this case all the frequency components in the signal will be affected by a constant attenuation and linear phase distortion of the channel, which has been chosen to have a Rayleigh's distribution. A Doppler frequency of 10 Hz is used in this simulation. From Fig (5.8), it can be seen that for BER=10^{-4} the SNR required for Scrambler-QPSKusing 2D-DMWT Scrambler is about 17dB, while in QPSK transceiverthe SNR is about 36dB,and for 2D-DWT scrambling QPSK transceiver about 23dB. The same thing are shown in from fig.(5.9) and fig.(5.10), therefore from fig.(11) fig.(12) and fig.(13) a gain of 19dB and 6dB for the Scrambler-QPSKusing 2D-DMWT Scrambler against QPSK 2D-DWT Scrambler transceivers are obtained respectively. Therefore the Scrambler-QPSKusing 2D-DMWT Scrambler outperforms significantly system for this channel model.

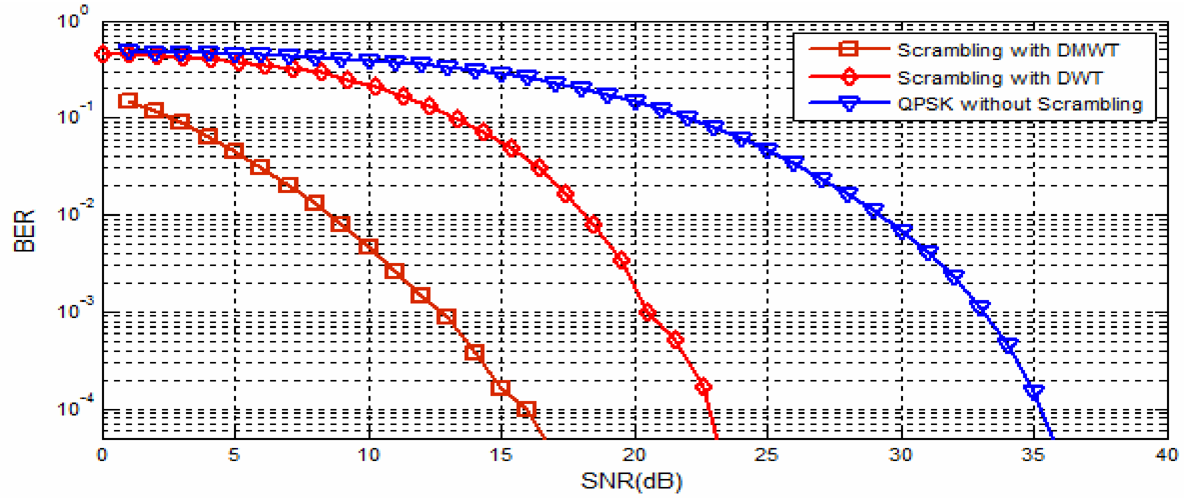


Fig. .(11). BER performance of Scrambler using modified Scrambler in Flat Fading Channel at Max Doppler Shift=10Hz.

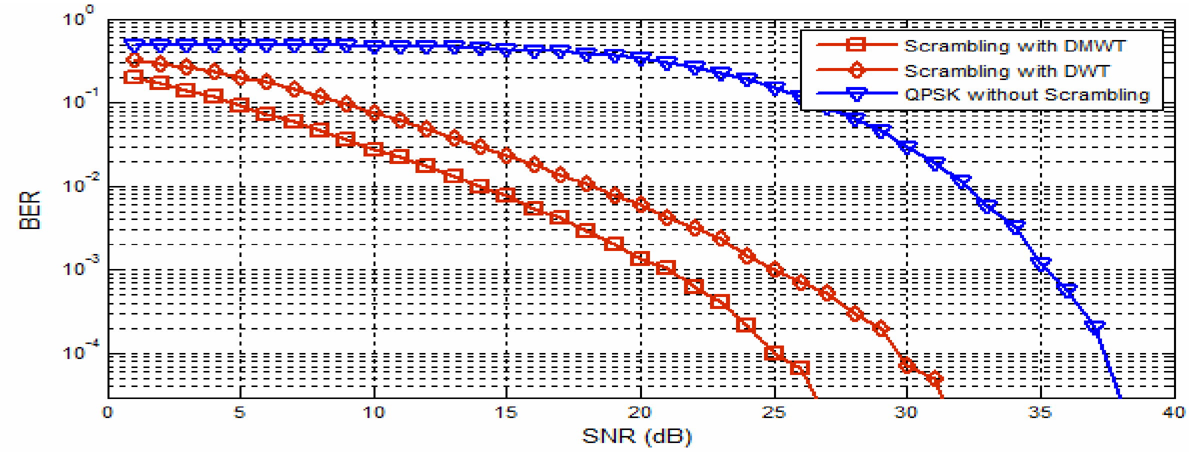


Fig..(12)BER performance of Scrambler using modified Scrambler in Flat Fading Channel at Max Doppler Shift=100Hz.

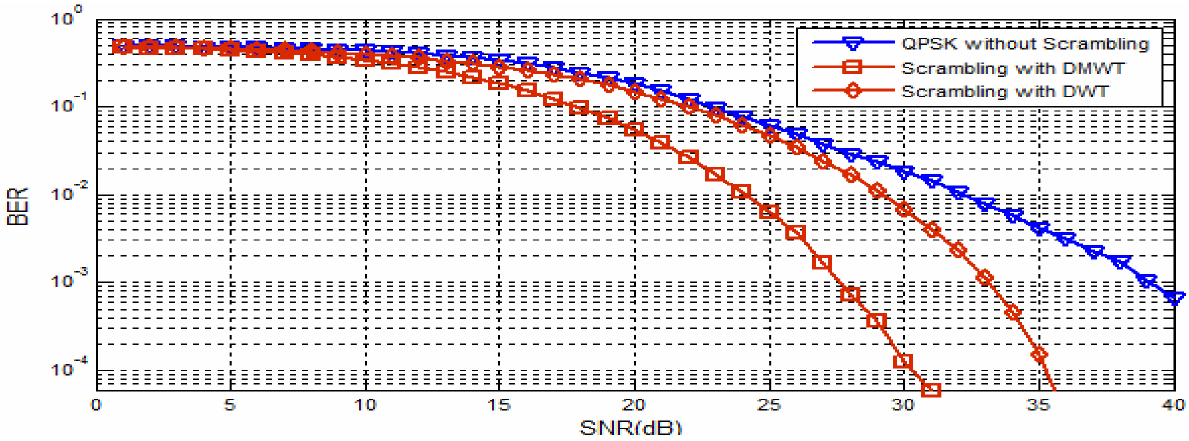


Fig..(13)BER performance of Scrambler using modified Scrambler in Flat Fading Channel at Max Doppler Shift=500Hz.

C. The Scrambler-QPSKin Frequency Selective fading channel:

In this section, BER performances of modified Scrambler-QPSKusing 2D-DWT and phase matrix are simulated in a multi-path frequency selective Rayleigh distributed channels with AWGN. Two ray channel is assumed here with a second path gain of -8dB, at a maximum delay from the second path of $\tau_{max}=0.1\mu sec$ for several values of SNR [4]. Fig. (14) Shown simulation results at maximum Doppler shift, f_{Dmax}=10Hz. It's clearly seen from this figure the performance for BER=10^{-4} the SNR required for Scrambler-QPSKusing 2D-DMWT is about 19dB, while in Scrambler-QPSKusing 2D-DWT and QPSK transceivers, the SNR are about 31dB and 37dB respectively. Therefore from figs.(14)a gain of 18dB for the Scrambler-QPSKusing 2D-DMWT against QPSK transceiver is obtained. In Figs(15),(16) the same thing can noted that Scrambler-QPSKusing 2D-DMWT Scrambler system outperforms significantly for this channel model.The results present in this sections are summarized in Table (2), and these results were computed after test the system by transferring about 1M symbols. The table present the SNR that get BER of (10^{-4}).

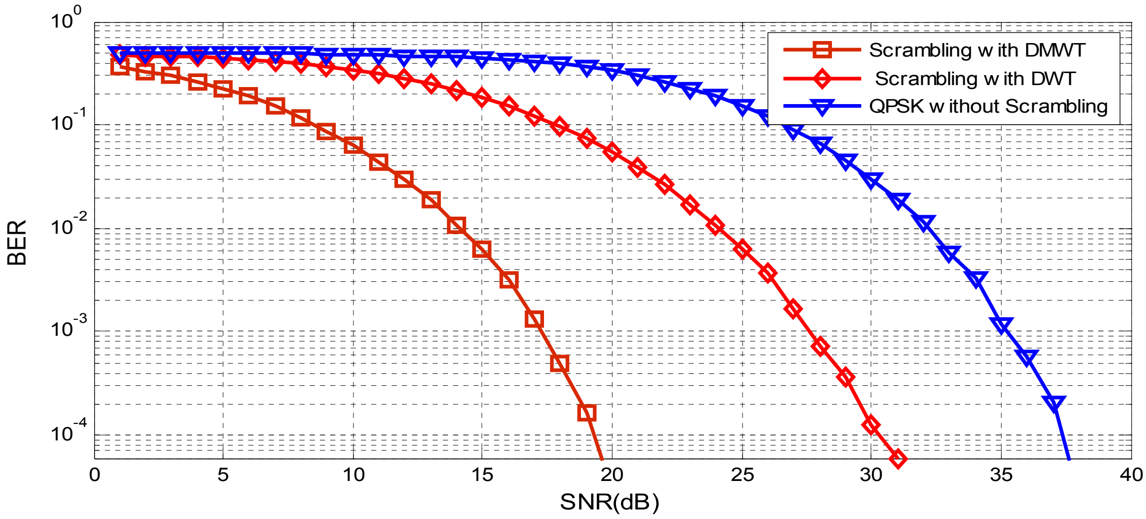


Fig .(14)BER performance of Scramblerusing modified Scrambler in Selective Fading Channel at Max. Doppler Shift=10Hz.

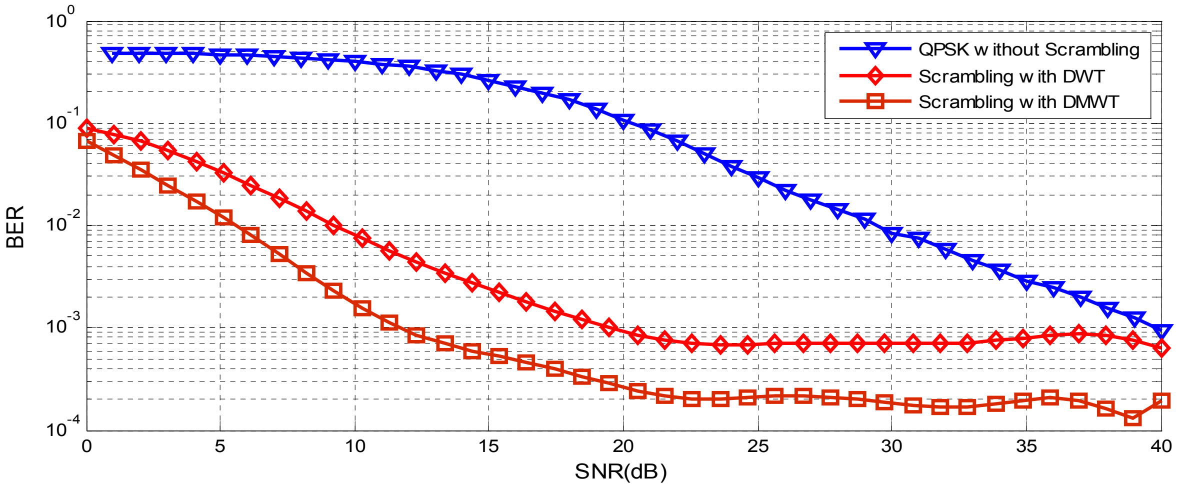


Fig .(15). BER performance of Scrambler using modified Scrambler in Selective Fading Channel at Max. Doppler Shift=100Hz.

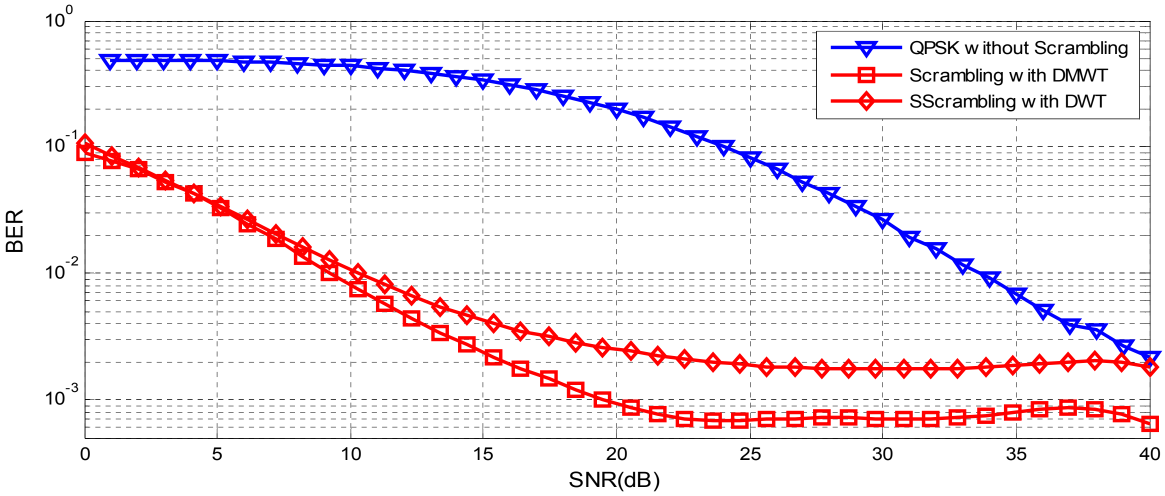


Fig .(16)BER performance of Scrambler using modified Scrambler in Selective Fading Channel at Max. Doppler Shift=500Hz.

Table (2) the results for all systems

System name	*AWGN*	*Flat Fading*			*Selective Fading*		
		Max. Doppler Shift			*Max. Doppler Shift*		
		10 Hz	*100 Hz*	*500 Hz*	*10 Hz*	*100 Hz*	*500 Hz*
QPSK- transceiver	24	31	39	non	35	non	non
2D-DWT SCRAMBLER- transceiver	19	23	29	36	31	non	non
2D-DMWT SCRAMBLER- transceiver	13	17	25	32	19	non	non

7. CONCLUSION

In this work, we proposed a new modified scrambler using 2D-DWT or 2D-DMWT that is easy to configure since it does not require a complex digital signal processing of 2D-DWT or 2D-DMWT algorithms which are available in all common DSP processors. As well it was successfully extended in the implementation of QPSK system. It was found that parameters of the new structure have physical relationship with the communication system performance characteristics which makes the matching very easy. Also it can be concluded that this structure offers more robust performance in many other high rate communication systems, resisting a wide range of changes in system parameters. As a result of applying the modified scrambler, the BER performance was improved significantly, especially in the existence of multi-path fading channels on the average, an SNR gain of 6.5dB is gained to achieve an error of 10-4 in AWGN, flat fading channels respectively. While in multi-path frequency-selective channel SNR gain of 3.5dB is gained to achieve such an error.

References

Hombrebueno D. J. S., Sicat M. G. C. E., Niguidula J.D., Chavez E. P., and Hernandez A.R A.,2009,“Symmetric Cryptosystem Based on Data Encryption Standard Integrating HMACand Digital Signature Scheme Implemented in Multi-Cast Messenger Application”, IEEE Second International Conference on Computer and Electrical Engineering, Vol.2, pp. 327-334.

Al-Shaer E., 2006, “Network Security Policies: Verification, Optimization and Testing”, IEEE/IFIP Network Operations and Management Symposium NOMS, pp. 584-584.

Yuan G., Wang F., and Hao Y., 2007, “Research on Data Encryption Technology Based on Chaos Theory”, IEEE Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Vol.1, pp. 93-98.

Ahmed J., and Ikram N., 2003, “Frequency Domain Speech Scrambling/Descrambling Techniques Implementation and Evaluation on DSP ”, IEEE 7th International Multi Topic Conference, pp.44-48.

Abdul-Rahaim L. A., 2009, “ Proposed Realization of Modified Scrambling using 2D-DWT Based OFDM Transceivers ” , IEEE MASAUM Journal of Computing, Vol. 1, No 2 .

Abbas N. A., 2009, “ Speech Scrambling Based on Principal Component Analysis”, Dept. of Computer Science, University of Babylon, Iraq.

Do N. M., and Vetterli M., 2009, “The Finite Fidgelet Transform for Image Representation”.

Brandau M., 2008,“ Implementation of A real-time Voice Encryption System ”.

Yuan Z., 2003, “ The Weighted Sum of The Line Spectrum Pair for Noisy Speech”, M.Sc. Thesis, Dept. of Electrical and Communications Engineering, Helsinki University of Technology.

Pereira W., 2001,“ Modifying LPC Parameter Dynamics to Improve Speech Coder Efficiency ”, M. Sc. Thesis, Department of Electrical & Computer Engineering, Faculty of Graduate Studies and Research, McGill University.

Gilley J. E., 2003 ,“ Bit-Error-Rate Simulation ”, August .

Breed G., 2003, “Bit Error Rate: Fundamental Concepts and Measurement Issues”.

Lee L. S., and Chou G. C., 1983 ,“ Asynchronous Speech Encryption- Formulation and Simulation ”, IEEE, Dept. of Electrical Engineering , National Taiwan University .

Gersho A., 1984, “Perfect Security Encryption of Analog Signals ”, IEEE Selected Areas in Communications, Vol. Sac-2, No. 3, pp. 460-466.

Cox R. V., Bock D. E., Bauer K. B., Johnston J. D., and Snyder J. H., 1986, “The Analog Voice Privacy System”, IEEE, AT&T Bell Laboratories, ICASSP 86, Tokyo,Vol.11, pp. 341-344.

Matsunaga A., Koga K., and Ohkawa M., 1989, “An Analog Speech Scrambling System Using The FFT Technique With High Level Security ”, IEEE Journal on Selected Areas in Communications, Vol. 7, No. 4, pp. 540-547.