Received: August 28, 2022. Revised: September 24, 2022. 563

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Hybrid Ciphering and Frequency Domain Scrambling for Secure Speech Transmission through MIMO-OFDM System

Hussein A. Hussein Al-Delfi[1] Fadhil Sahib Hasan[1]*

[1]*Mustansiriyah University, Electrical Engineering Department, Baghdad, Iraq.*
* Corresponding author's Email: fadel_sahib@uomustansiriyah.edu.iq

Abstract: This paper suggests the transmission of secure speech signals through the MIMO-OFDM system over a doubly selective fading channel. The two-dimensional chaotic map like logistic (TDLM), standard (TDSM), and triangle function combination discrete chaotic map (TD-TFCDM) are used to generate pseudo-random bit generator (PRBG) and index permutation (IP) to encrypt the information based on ciphering and scrambling techniques. Different speech quality and residual intelligibility measures including log-likelihood ratio (LLR), frequency-weighted segmental signal-to-noise ratio (fwSNRseg), signal-to-noise ratio loss (SNRLOSS), correlation coefficient (CC) and spectrogram measures as well as Bit Error Rate (BER) performance are used to test the performance of the proposed security system. The simulation results show that the speech signal over the MIMO-OFDM system behaves well with high security. Also, the speech encryption system using TDSM and TD-TFCDM outperforms TDLM in most residual intelligibility measures.

Keywords: Speech encryption, Multi input multi output, Orthogonal frequency division multiple (MIMO-OFDM), Doubly selective fading channel, Two-dimensional chaotic map, Pseudo random bit generator, scrambling.

1. Introduction

The protection of speech transmission in a wireless mobile communication system is the most challenging today with the rapid increase in information technology [1], [2]. Orthogonal frequency division multiplexing (OFDM) is widely used today in mobile communication systems due to having high bandwidth efficiency and mitigates the effect of multipath fading channels [3].

Combining the MIMO system with the OFDM system provides more enhancement to channel capacity and bandwidth efficiency compared with single input single output (SISO) system [4]. The growing demand for MIMO-OFDM systems in mobile communication systems has put a demand for increasing the security level of information transmitted through this system. The reliability of information transmission depends on the authentication of information, confidentiality, safety and availability to save the information from the third parties and attacks [5]. To provide the information security against the third party, the information must be protected. The most famous method of speech encryption methods is the scrambling technique [6], [7], in which either the speech signal is scrambled in the time domain or frequency domain or both the time and frequency domain. Another method to encrypt the speech signal is ciphering method [8-11], in which the stream cipher of the speech sequence is XORed with a pseudo-random bit generator (PRBG). The third method is the masking method [12, 13] in which the scrambled speech signal is obtained by adding the speech signal with the chaotic signal. Also, a hybrid between these methods is applied to increase the security of the speech signal [14, 15]. The following literature survey is focused on combining the encryption techniques with the OFDM communication system and employing them for secure speech transmission.

2. Literature survey

In [16, 17] speech signal is transmitted through the OFDM communication system without security.

Therefore, the eavesdropper can recover the data without any attack or difficulty. In [1], hybrid permutation and ciphering techniques are proposed to encrypt the digitized speech signal over the OFDM system. In the first, the speech signal is permutated using a seed and then XORed with the seed value. After that, QAM mapping is applied and passed through IFFT and cyclic prefix guard to produce the OFDM transmitted signal. The securely transmitted signal is sent through Rayleigh and Rician fading channels. In this paper, only 16 QAM are examined and the permutation is not implemented by the chaos system. Also, MIMO system is not combined with this system making the capacity of this system very low. Furthermore, the objective quality of speech signal depends on PESQ only. In [18], secure speech through a communication system was designed and implemented using the TMS320C6711 DSP starter kit. The speech signal is sampled using an 8 kHz sampling frequency and taking Discrete Cosine Transform (DCT) to the frame of 256 samples of the quantized signal. The frequency-domain signal was scrambled using 256 pseudo-random values and then taken Inverse DCT (IDCT) to obtain the transmit time domain of the scrambled speech signal. In this paper, the pseudo-random sequence was not designed with high security, and only the real part of the spectrum was presented. In [19], transmit scrambled voice signals through MIMO NOMA communication systems. The system is incorporated with LDPC channel coding and the enhanced ML decoder depends on QR channel factorization over Raleigh fading channel. In this paper, only the scrambling technique was used to encrypt the speech signal and the objective quality measures were not included. In [2], the secure audio signal is transmitted through coded mmWave massive MIMO FBMC under a 5G communication system. The secure audio signal is generated by converted into an image signal and XORed with a two-dimensional random sequence generated by a two-dimensional discrete chaotic map. In this paper, only one level of security was included with one type of map and no objective measures were included to test the intelligibility of speech signal. In [20], secure speech sending over the OFDM communication system was proposed. The original speech signal is recorded at an 8 kHz sampling rate and converted into stream bits. The stream bits are XORed with pseudo-random bits generated by both Henon or Logistic chaotic map, and then the ciphered message is transmitted through the OFDM system under the AWGN channel. In this paper, the system is not studied under fading channel and only SISO system is included. Also, one level of security was proposed for an OFDM system. In [21], secure audio transmitted through an OFDM system using different 2D chaotic maps was proposed. 2D Baker, 2D Logistic, and 2D Standard map are used either as masking signal or permutation index to encrypt the audio signal. In the first, the audio signal is converted to a 2D signal and then masked by adding it to one of the 2D chaotic maps and clipping the resulted signal by two values. After that, the 2D signal is permutation using the 2D chaotic map and quantized to generate the binary stream that is transmitted through the OFDM system and AWGN channel. The results show that the 2D standard chaotic map has the best performance in terms of objective quality measures than other chaotic maps. In this paper, only AWGN channel is used to SISO OFDM system. In [22], the speech scrambling based on 3D-Lorenz-logitic chaotic map is proposed. The scrambling is made in the frequency domain and the transmission through communication system is not included. In [23], encrypted speech is sending over 3G cellular network and Voice over IP (VoIP). A novel Data over Voice (DoV) depends on a codebooks of short harmonic waveforms and principles of Linear Predictive Coding (LPC) are introduced. In this paper, the information is not sending though MIMO-OFDM system and not applied for wireless channel. In our paper, the speech signal is transmitted over a secure MIMO-OFDM system over a doubly selective fading channel. To our knowledge, there are no papers that studied the encrypted speech signal through a doubly selective fading channel. Two levels of security are applied to the system based on ciphering and scrambling techniques. At the ciphering level, the stream bits of the digitized speech signal is XORed with a pseudo-random bit generator (PRBG), while at the scrambling level the QAM mapped signals are permutated based on index permutation (IP). Both PRBG and IP are designed using two-dimensional chaotic map (TDCM). Different types of TDCM including TD logistic map (TDLM), TD standard map (TDSM), and TD triangle function combination discrete chaotic map (TD-TFCDM) are designed to generate PRBG and IP. Furthermore, PRBG is designed using Three Dimensional Chaotic Map (3DCM). Two types of 3DCM are studied including 3D lgistic map (3D-LM) and 3D Piecewise-henon map (3D-PHM). Different speech quality and residual intelligibility measures including Log-likelihood ratio (LLR), Frequency-weighted segmental signal-to-noise ratio (fwSNRseg), Signal-to-noise ratio loss (SNRLOSS), Correlation coefficient (CC) and spectrogram are used to test the performance of speech encryption system as well as bit error rate (BER) performance

test. The rest of the paper is organized as follows: Section 3 presents the two-dimensional chaotic maps based on pseudo-random bit generator, index permutation and three dimensional chaotic map based PRBG. Section 4 presents the structure model of secure speech transmission through the MIMO-OFDM system. Section 5 presents speech quality and residual intelligibility measures. Section 6 presents the simulation results. Sections 7 and 8 presents the comparisons with other works and conclusions, respectively.

3. Two-dimensional chaotic maps based PRBG and IP

In this section the three types of two dimensional chaotic maps which are TDLM, TDSM and TD-TFCDM are explain in briefly and used to generate PRBG and IP.

3.1 Two-dimensional chaotic maps

A. TD logistic map (TDLM)

The discrete TDLM can be expressed as [21], [24]:

$$\begin{aligned} x_{i+1} &= \alpha\,(3y_i + 1)x_i(1 - x_i) \\ y_{i+1} &= \alpha\,(3x_i + 1)y_i(1 - y_i) \end{aligned} \tag{1}$$

where α is chaotic system parameters which must be positive real value. The chaotic sequences, x_i and y_i, have the range [0, 1].

B. TD Standard map (TDSM)

The discrete TDSM can be expressed as [21, 25]:

$$\begin{aligned} x_{i+1} &= (x_i + y_i) \bmod N \\ y_{i+1} &= \left(y_i + \gamma sin\left(\frac{N x_{i+1}}{2\pi}\right)\right) \bmod N \end{aligned} \tag{2}$$

where γ is chaotic system parameters which must be positive integer value and N is the length of chaotic sequence. The chaotic sequences, x_i and y_i, have the range (0, N).

C. TD triangle function combination discrete chaotic map (TD-TFCDM)

The TD-TFCDM can be expressed as [26]:

$$\begin{aligned} x_{i+1} &= \mu_1 cos(x_i + y_i) \\ y_{i+1} &= \mu_2 cos(x_i - y_i) \end{aligned} \tag{3}$$

where μ_1 and μ_2 are the chaotic system parameters, here $\mu_1 = 8$ and μ_2=0.5 [26]. The chaotic sequences, x_i and y_i, have the range (-8,8x).

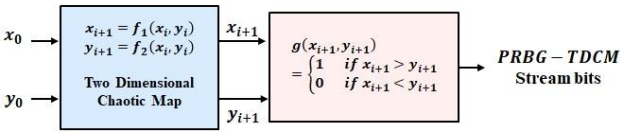

Figure. 1 PRBG based on TDCM

3.2 Two-dimensional chaotic map based PRBG

Pseudo random bit generator (PRBG) is the main core of the stream cipher system in which the stream insecure data is XORed with PRBG to produce the ciphered sequence [10, 26]. Different techniques are used to design PRBG using chaotic system. In [10, 11] Hasan et al. generates PRBG using fixed point chaos system and combined two or more PRBGs with XOR function to produce new version of PRBG with high security. In [26] Patidar et al. used two logistic maps with different initials to generate PRBG by comparing them with each other. While in [28] mixing 3D Chen system is used with chaotic Tactics to produce new PRBG. This system has highly complexity comparing with chaotic map. In this paper, two-dimensional chaotic maps are designed to produce new PRBG with simple and good security. The proposed PRBG based on TDCM is illustrated in Fig. 1. This system is similar to the Patidar model in [27] but is used TDCM instead of one-dimensional logistic map. Starting from the random initial values x_0 and y_0 the two-dimensional sequence x_{i+1} and y_{i+1} are generated by:

$$\begin{aligned} x_{i+1} &= f_1(x_i, y_i) \\ y_{i+1} &= f_2(x_i, y_i) \end{aligned} \quad , i = 0,1,..,N-1 \tag{4}$$

The stream bits of PRBG, K_i, are produced by comparing x_{i+1} and y_{i+1} according to:

$$K_i = g(x_{i+1}, y_{i+1}) = \begin{cases} 1 & if\ x_{i+1} > y_{i+1} \\ 0 & if\ x_{i+1} < y_{i+1} \end{cases} \quad , i = 0,1,..,N-1 \tag{5}$$

3.3 Two-dimensional chaotic maps based IP

Fig. 2 shows the Index permutation based on TDCM. In the first, the two-dimensional sequences x_{i+1} and y_{i+1} are converted into one dimensional sequence v_j using concatenation function, $v_j = [x_{i+1}, y_{i+1}]$, $i \in [0, N)$, $j \in [0,2N)$. Framing the sequence and then sorting using sort function, s[v_s π_j]=sort(v), where v_s is the sequence after sorting and $\pi_j, j = 1,..,2N$, is the index permutation.

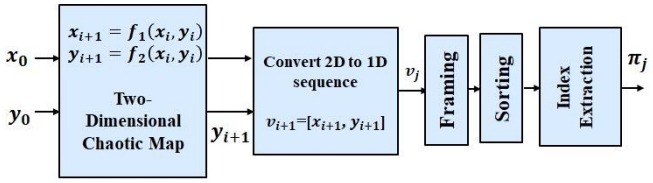

Figure. 2 Index permutation based on TDCM

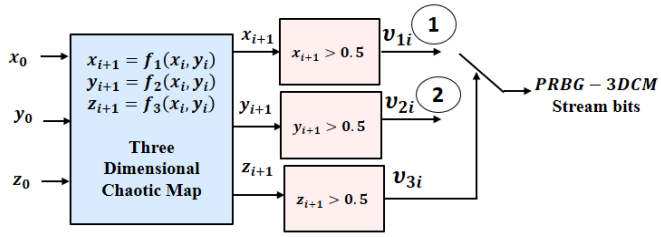

Figure. 3 PRBG based on 3DCM.

3.4 Three-dimensional chaotic maps based PRBG

PRBG can be generated using three-dimensional chaotic maps (3DCM) instead of TDCM. Two maps are suggested that are 3D logistic map (3D-LM) [29] and 3D piecewise-henon map (3D-PHM) [30] that are expressed respectively as:

$$\begin{aligned} x_{i+1} &= a_1 x_i(1-x_i) + b_1 y_i^2 x_i + c_1 z_i^3 \\ y_{i+1} &= a_1 y_i(1-y_i) + b_1 z_i^2 x_i + c_1 x_i^3 \\ z_{i+1} &= a_1 z_i(1-z_i) + b_1 x_i^2 x_i + c_1 y_i^3 \end{aligned} \quad (6)$$

where x_i, y_i and z_i are initial values of the chaotic system in the range [0, 1]. a_1, b_1, c_1 are control parameters with the range of [3.53, 3.81], [0, 0.022], [0, 0.015], respectively.

$$\begin{aligned} x_{i+1} &= \left(|1 - a_2 x_i| + (y_i + 1 - b_2 z_i^2)\right) mod 1, \\ y_{i+1} &= \left(|1 - a_2 y_i| + (z_i + 1 - b_2 x_i^2)\right) mod 1, \\ z_{i+1} &= \left(|1 - a_2 z_i| + (x_i + 1 - b_2 y_i^2)\right) mod 1, \end{aligned} \quad (7)$$

where a_2 and b_2 are control parameters that are set to 15 and the range of x_i,y_i and z_i is [0,1].

Fig 3 shows the proposed PRBG based on 3D-chaotic map (3DCM). In the first, the initial values x_0,y_0,and z_0 are entered to the 3DCM system to generate the next *i*-th samples x_i,y_i, and z_i iteratively. Each sample is passed through thresholding to generate the *i*-th bit in each sample $(v_{1i}, v_{2i}, v_{3i}) \in \{0,1\}$ and then the stream bits of PRBG-3DCM is generated by select either v_{1i} or v_{2i} depends on the i-th v_{3i} bit. When $v_{3i} = 0$ the output is taken from position 1 (v_{1i}) and $v_{3i} = 1$ the output is taken from position 2 (v_{2i}).

4. Secure speech transmission through MIMO-OFDM syste

4.1 Transmitter model

Fig. 4 shows the block diagram of the proposed MIMO-OFDM system at the sender side. Firstly, the analogue speech signal is digitized with sampling frequency (f_s) = 8 KHz and resolution bits (n)=16. The digitized speech signal (s) converted to positive normalized sequence (sn) in the range 0 to (2^{16}-1) according to [11]:

$$sn = fix\left((2^{16} - 1)\left(\frac{s - s_{min}}{s_{max} - s_{min}}\right)\right) \quad (8)$$

where *fix* (.) is round function to a nearest integer toward zero. s_{max} and s_{min} are the largest and lower value of s, respectively. The positive sequence is then converted to *j*-th stream bits, $\underline{u}_j$, and then converted to parallel two bits, $u_{1,j}$ and $u_{2,j}$, using serial to parallel converter. After that, the *j*-th two stream bits are XORed with the two keys $k_{1,j}$ and $k_{2,j}$ to produce the *j*-th two ciphered sequences $c_{1,j}$ and $c_{2,j}$, respectively according to:

$$c_{l,j} = u_{l,j} \oplus k_{l,j} \quad , l = 1,2 \quad (9)$$

where $k_{1,j}$ and $k_{2,j}$ are the PRBG generated by the same type of TDCM or 3DCM but with different initial values, i.e. the initial values $(x_{1,0}, y_{1,0})$ and $(x_{2,0}, y_{2,0})$ are used for the first and second key respectively for TDCM. The *l*-th sequences $c_{l,j} \in \{0,1\}$ are the first level security. The ciphered sequences are then mapping using QAM modulation and framing into *M* samples to produce the length *M* symbol at the *l*-th transmit antenna $q_{l,m} \in \mathbb{C}^{2\times M}$, *l*=1,2 and *m*=0,..,*M*-1. The second level security is applied to the two mapped block signals, in which $q_{l,m}$ is permutated by the index permutations $\pi_{l,m}$, *l*=1,2 and m=0,..,*M*-1. The two index permutations are generated from the same type of TDCM with different initial value, i.e. the initial values $(x_{1,0}, y_{1,0})$ and $(x_{2,0}, y_{2,0})$ are used for the first and second key respectively. The *m*-th scrambled signal of the *l*-th transmitted antenna, $qs_{l,m}$ is expressed as:

$$qs_{l,m} = q_{l,m}(\pi_{l,m}) \quad l=1,2 \text{ and } m=0,1,..,M-1 \quad (10)$$

The IFFT is applied for the *l*-th antenna scrambled data symbol according to [31]:

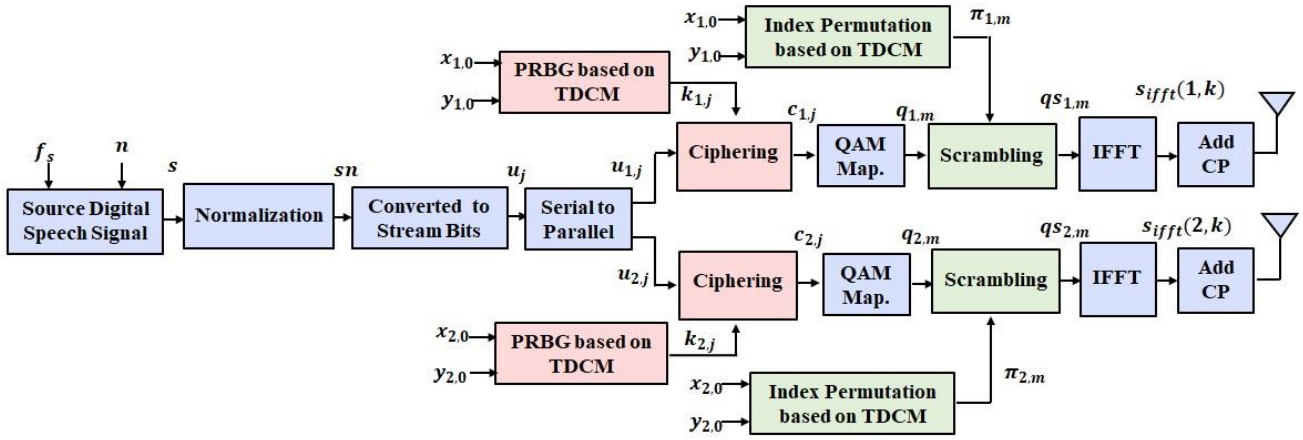

Figure. 4 Proposed the MIMO-OFDM communication system at transmitter side based on TDCM

$$s_{ifft}(l,k) = \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} \hat{q}_{l,m} e^{\frac{j2\pi mk}{M}}, \quad 0 \le k \le M-1 \tag{11}$$

where $s_{ifft}(l,k)$ is the k-th IFFT signal of the l-th transmitted antenna. Eq. (4) can be rewritten in matrix form as [32]:

$$\boldsymbol{s}_{ifft,l} = \mathbf{G}\, \boldsymbol{qs}_l \tag{12}$$

where $\mathbf{G} \in \mathbb{C}^{M\times M}$ is transmitted matrix which depends on the twiddle factors $\frac{1}{\sqrt{M}} e^{j2\pi mk/M}$. A guard interval depends on a cyclic prefix (CP) is added to the OFDM modulated signal to eliminate the effects of the channel multi-path delay spread. Also, CP will eliminate the inter-symbol interference (ISI) and maintain the orthogonality between the subcarriers [31].

4.2 Receiver model

Fig. 5 shows the block diagram of the proposed MIMO-OFDM system at the reception side. At the reception, after remove CP, the received signal at ρ-th reception antenna, $\boldsymbol{r}_\rho \in$ is written by [31, 32]:

$$\boldsymbol{r}_\rho = \sum_{l=1}^{2} \boldsymbol{H}_{\rho,l}\, \mathbf{G}\, \boldsymbol{qs}_l + \boldsymbol{w}_\rho, \quad \rho = 1,2 \tag{13}$$

where $\boldsymbol{w}_\rho \in \mathbb{C}^{M\times 1}$, $\rho = 1,2$, is the ρ-th additive white Gaussian noise vector with zero mean and power spectral density $N_0/2$ and $\boldsymbol{H}_{\rho,l} \in \mathbb{C}^{M\times M}$, $\rho = 1,2$ and $l = 1,2$, is the time variant convolution matrix of the doubly selective fading channel, which is modeling using Nissel depends on Jakes' model [28].The ρ-th received signal $\boldsymbol{r}_\rho$is multiplying by $\mathbf{G}^{\mathrm{H}}$ and obtain the OFDM demodulation, $\mathbf{G}^{\mathrm{H}}$ is equivalent to FFT transform. Thus, the ρ -th demodulated 2×2 MIMO-OFDM signal $\boldsymbol{s}_{ifft,\rho} \in \mathbb{C}^{M\times 1}$ can be expressed as [31, 32]:

$$\boldsymbol{s}_{fft,\rho} = \sum_{l=1}^{2} \mathbf{G}^H \boldsymbol{H}_{\rho,l}\, \mathbf{G}\, \boldsymbol{qs}_l + \mathbf{G}^H \boldsymbol{w}_\rho, \quad \rho = 1,2 \tag{14}$$

where H is Hermitian operation and real orthogonality in OFDM implies that $\mathcal{R}\{\boldsymbol{G}^H\boldsymbol{G}\} = \boldsymbol{I}_M$ [31]. where $\mathcal{R}\{.\}$ is the real part of the complex signal. Define $\boldsymbol{s}_{fft} = \begin{bmatrix} \boldsymbol{s}_{fft,1} \\ \boldsymbol{s}_{fft,2} \end{bmatrix}$, $\boldsymbol{D} = \begin{bmatrix} \boldsymbol{G}^H\boldsymbol{H}_{1,1}\boldsymbol{G} & \boldsymbol{G}^H\boldsymbol{H}_{1,2}\boldsymbol{G} \\ \boldsymbol{G}^H\boldsymbol{H}_{2,1}\boldsymbol{G} & \boldsymbol{G}^H\boldsymbol{H}_{2,2}\boldsymbol{G} \end{bmatrix}$, $\boldsymbol{qs} = \begin{bmatrix} \boldsymbol{qs}_1 \\ \boldsymbol{qs}_2 \end{bmatrix}$, then the ρ-th output of full block MMSE equalizer, $\widetilde{\boldsymbol{qs}}_l$, ρ =1,2, is expressed as [32]:

$$\begin{bmatrix} \widetilde{\boldsymbol{qs}}_1 \\ \widetilde{\boldsymbol{qs}}_2 \end{bmatrix} = \begin{bmatrix} \mathcal{R}\{\boldsymbol{D}\} \\ \Im\{\boldsymbol{D}\} \end{bmatrix}^T \left(\begin{bmatrix} \boldsymbol{G}^H\boldsymbol{H}_{1,1}\boldsymbol{G} & \boldsymbol{G}^H\boldsymbol{H}_{1,2}\boldsymbol{G} \\ \boldsymbol{G}^H\boldsymbol{H}_{2,1}\boldsymbol{G} & \boldsymbol{G}^H\boldsymbol{H}_{2,2}\boldsymbol{G} \end{bmatrix}^T + \boldsymbol{\Gamma} \right)^{-1} \begin{bmatrix} \mathcal{R}\{\boldsymbol{s}_{fft}\} \\ \Im\{\boldsymbol{s}_{fft}\} \end{bmatrix} \tag{15}$$

where $\Im\{.\}$ is the imaginary part of the complex signal and $\boldsymbol{\Gamma}$ is the noise matrix that is given by [32]:

$$\boldsymbol{\Gamma} = \frac{\boldsymbol{N_0}}{\boldsymbol{2}} \begin{bmatrix} \mathcal{R}\{\boldsymbol{\Omega}\} & -\Im\{\boldsymbol{\Omega}\} \\ \Im\{\boldsymbol{\Omega}\} & \mathcal{R}\{\boldsymbol{\Omega}\} \end{bmatrix} \text{ with } \boldsymbol{\Omega} = \begin{bmatrix} \boldsymbol{G}^H\boldsymbol{G} & 0 \\ 0 & \boldsymbol{G}^H\boldsymbol{G} \end{bmatrix} \tag{16}$$

The following step is descrambling stage that is applied to the output of MMSE equalizer using the identical index permutation at the transmitter side to obtain the ρ -th descrambled signal, $\widetilde{\boldsymbol{q}}_\rho$, ρ =1,2, according to:

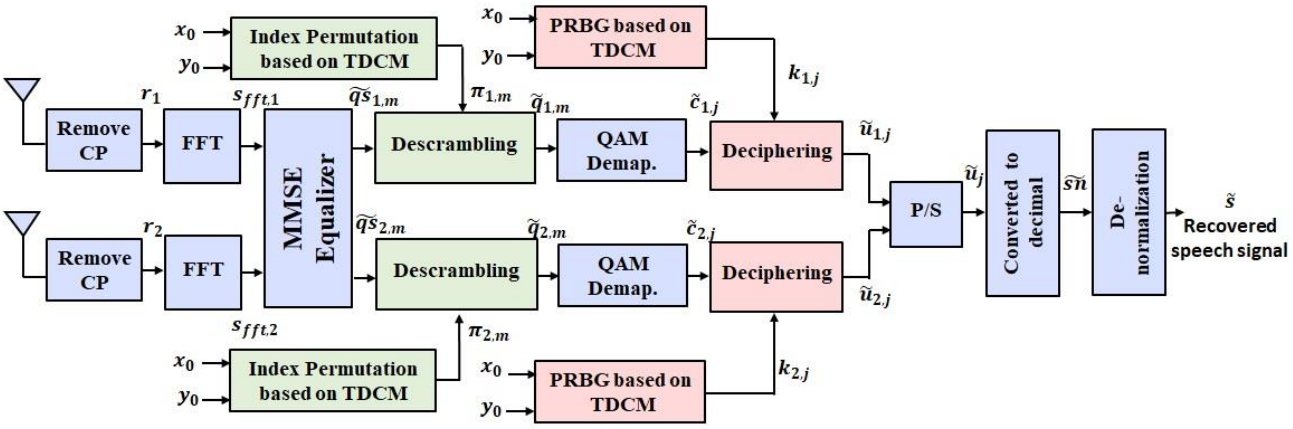

Figure 5. Proposed the MIMO-OFDM communication system at receiver side based on TDCM

Table 1. Simulation parameters

QAM order	64, 256
Subcarrier Numbers	24
FFT size	256
Subcarrier spacing (kHz)	15
Cyclic Prefix length	4.7619 $\boldsymbol{\mu sec}$
Channel	Doubly selective fading channel + AWGN (Vehicular A)
Velocity (km/h)	200, 500
Carrier frequency(GHz)	2.5
SNR [dB]	0-45
Chaotic	TDLM, TDSM, TD-TFCDM
Performance measure	LLR, SNRLOSS, fwSNRseg, CC

$$\tilde{q}_{\rho,m}(\pi_{\rho,m}) = \widetilde{qs}_{\rho,m} \ , \ \rho = 1,2 \text{ and } m = 0,1,..,M\text{-}1 \quad (17)$$

The m-th detected of the ρ-th received antenna is obtained using QAM demapping and converted to stream bits to get the ρ-th stream bits at the j-th time, $\tilde{c}_{\rho,j}, \rho = 1,2$. The ρ-th deciphered sequence, $\tilde{u}_{\rho,j}$ is obtained by XORed $\tilde{c}_{\rho,j}$ with the ρ-th identical PRBG key at the transmitter side according to:

$$\tilde{u}_{\rho,j} = c_{\rho,j} \oplus k_{\rho,j} \qquad , \rho = 1,2 \quad (18)$$

The parallel sequence are converted to serial bits, $\tilde{u}_j$ and then the stream bits are converted into decimal format after taking framing of n bits, $\widetilde{sn}$. Finally, the recovered speech signal is obtained by applying de-normalization function to $\widetilde{sn}$ according to:

$$\tilde{s} = \frac{\widetilde{sn}(s_{max} - s_{min})}{2^{16}-1} + s_{min} \quad (19)$$

5. Speech quality and residual intelligibility measures

In this paper, log-likelihood ratio (LLR) [10, 13, 33], frequency-weighted segmental signal-to-noise ratio (fwSNRseg) [10, 33], signal-to-noise ratio loss (SNR_{LOSS}) [10, 34] and correlation coefficients (CC) [7, 21] measures are used to test the performance of speech signal over secure MIMO-OFDM system.

6. Simulation results

In this simulation, three TD chaotic maps including TDLM, TDSM, and TD-TFCDM have been used either as PRBG or Index permutation and applied to secure speech transmitted over MIMO-OFDM with two levels of security. The speech signal is recorded with a 16 kHz and a 16 bits resolution with a total length of 47880 samples (3 sec). Table 1 illustrates the main parameters of the proposed MIMO-OFDM system. In all PRBGs generated by the TD and 3D chaotic maps, statistical randomness measures depicted in [35] are used to test the randomness of PRBGs. The results show all PRBGs are passed the tests with a P-value greater than 0.01threshold level for all tests.

6.1 Decryption simulation results

In this simulation, the BER and speech Quality performance of the decrypted speech signal over MIMO-OFDM system are presented. The comparisons are investigated for different QAM level (64 and 256 QAM) and different velocities (200 and 500 km/h). In this experiment, TDLM is used to generate both PRBG and index permutation. Two stages of encryption including ciphering and

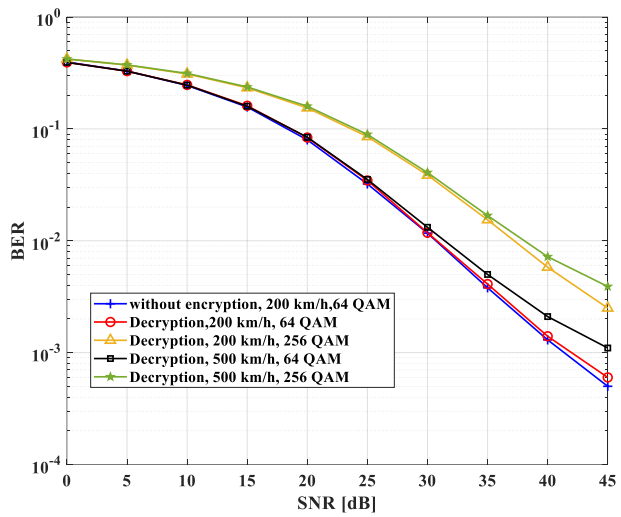

Figure. 6 The BER performance of decrypted speech signal through MIMO-OFDM system

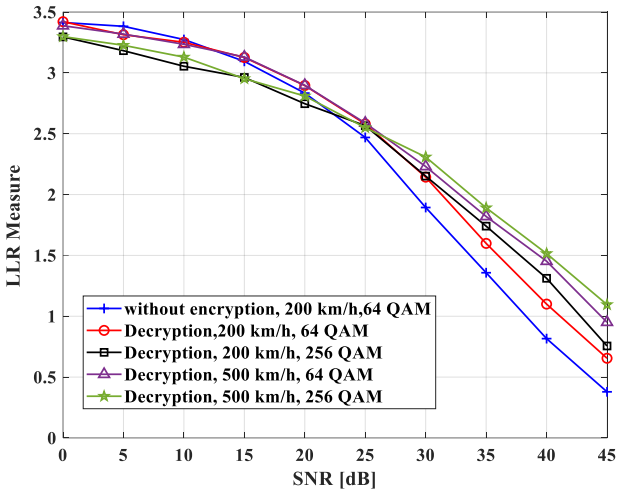

Figure. 7 The LLR performance of decrypted speech signal through MIMO-OFDM system

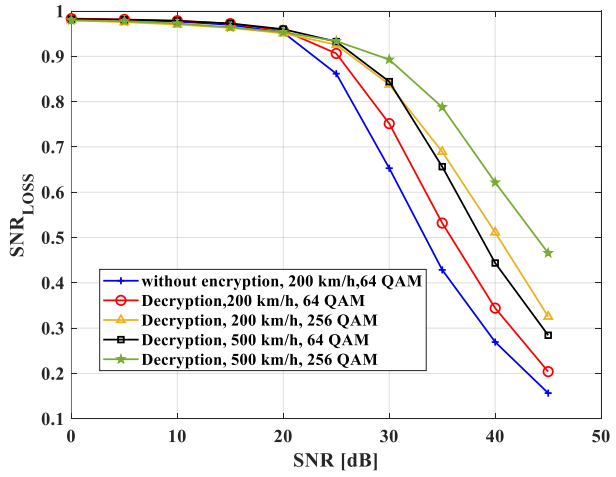

Figure. 8 The SNR_{LOSS} performance of decrypted speech signal through MIMO-OFDM system

scrambling stage are used in this simulation. Fig. 6 shows the BER performance of decrypted speech signal through MIMO-OFDM system for various QAM levels and velocities. The speech signal is recovered with the correct keys for the two stage levels of security. The results are compared with the system without adding any encryption stages. The results show that the BER performance for the system without encryption is approximately the same for the system with decryption. Also, increased either the level of QAM or velocities will degrade the BER performance of the system.

Figs. 7-10 show the LLR, SNRLOSS, fwSNRseg and CC quality measure, respectively for decrypted speech signal through MIMO-OFDM system for different QAM levels and velocities. For all measures it can be noticed that increase SNR will improve the quality of decrypted speech signal. At high SNR when SNR greater than 25 dB, for LLR, SNR_{LOSS}, fwSNRseg and CC measures there are a values less than 0.5, 0.1, 10 dB and 0.4, respectively between the systems without encryption and decryption at 200 km/h and 64 QAM i.e. the quality of speech signal at the receiver will little affected when combined an encryption system with a MIMO-OFDM system. Also, the quality measure affected by the QAM level and velocity where any increase in the level or velocity will decrease the quality of the speech signal at the receiver side

6.2 Encryption simulation results

In this simulation, the BER and speech residual intelligibility performance of the encrypted speech signal over the MIMO-OFDM system is presented. The comparisons are investigated for 64 QAM and 200 km/h. In this experiment, TDLM is used to generate both PRBG and IP. The encryption is made by only ciphering, scrambling, or combined methods and tests the performance of the system. Fig. 11 shows the BER performance of encrypted speech signals through the MIMO-OFDM system for 64 QAM and 200 km/h velocity. The speech signal is recovered with incorrect keys for all scenarios of the security. The results show that the BER performance of the system using ciphering algorithm has less value compared with both scrambling and combination algorithms, which means that the 3rd party has the chance to detect the speech signal for ciphering method greater than scrambling and combination methods.

Figs. 12-15 show the LLR, SNR_{LOSS}, fwSNRseg, and CC residual intelligibility measure, respectively for encrypted speech signal through MIMO-OFDM system with 64 QAM and velocity 200 km/h. For LLR measure result, ciphering method appears to be

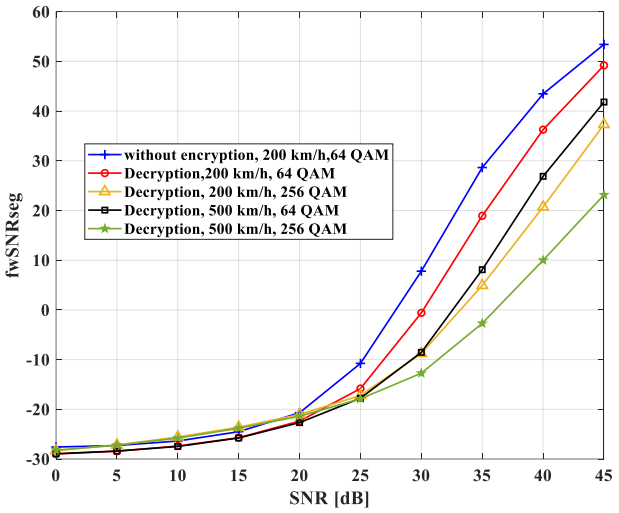

Figure. 9 The fwSNRseg performance of decrypted speech signal through MIMO-OFDM system

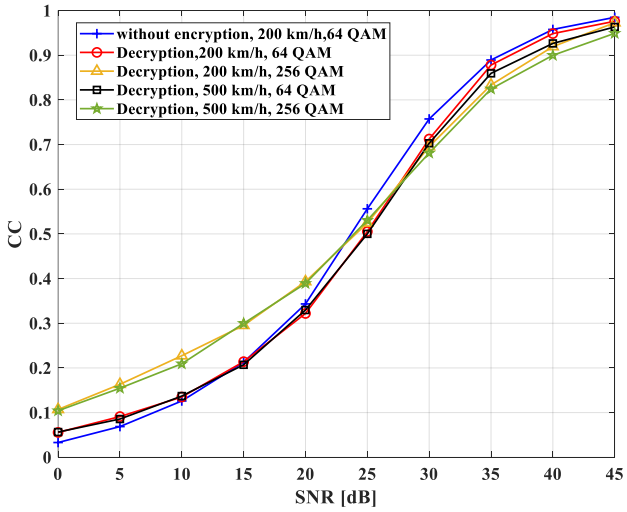

Figure. 10 CC performance of decrypted speech signal through MIMO-OFDM system

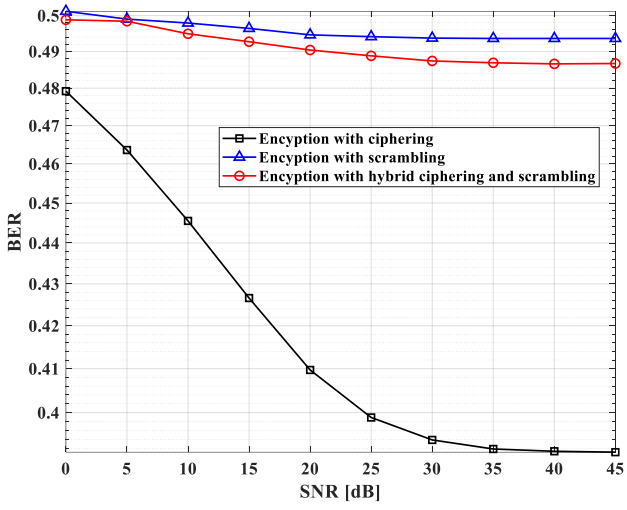

Figure. 11 The BER performance of encrypted speech signal through MIMO-OFDM system

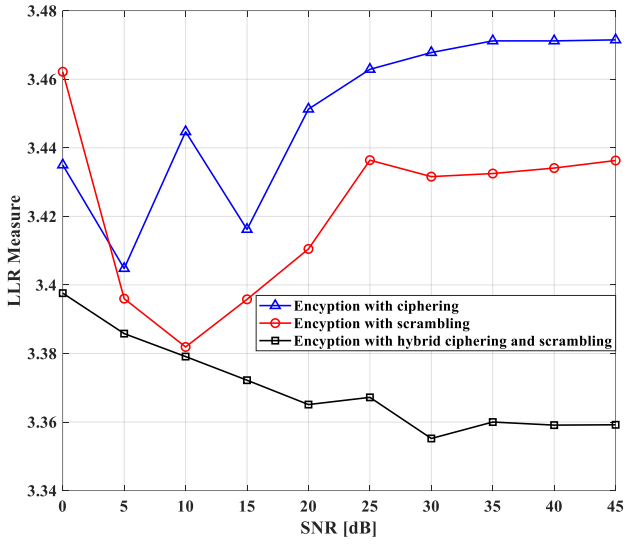

Figure. 12 LLR performance of encrypted speech signal through MIMO-OFDM system

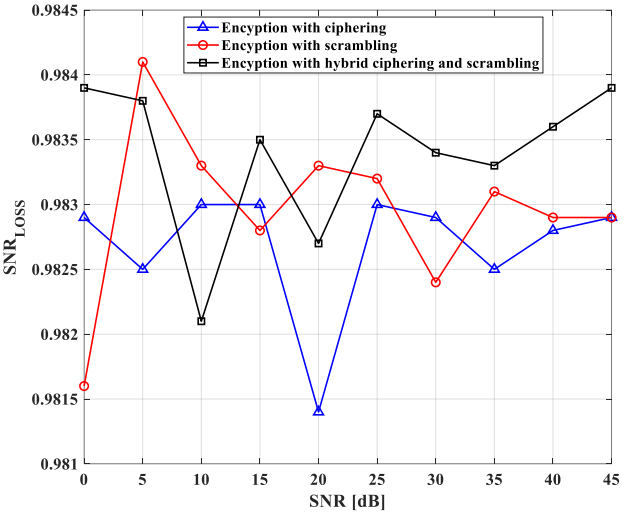

Figure. 13 SNR_{LOSS} performance of encrypted speech signal through MIMO-OFDM system

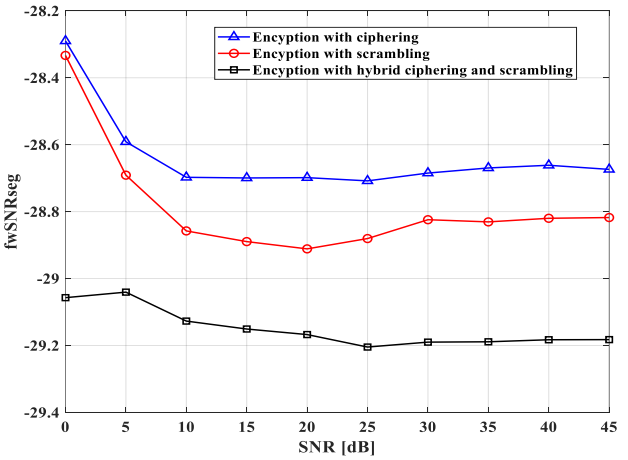

Figure. 14 fwSNRseg performance of encrypted speech signal through MIMO-OFDM system

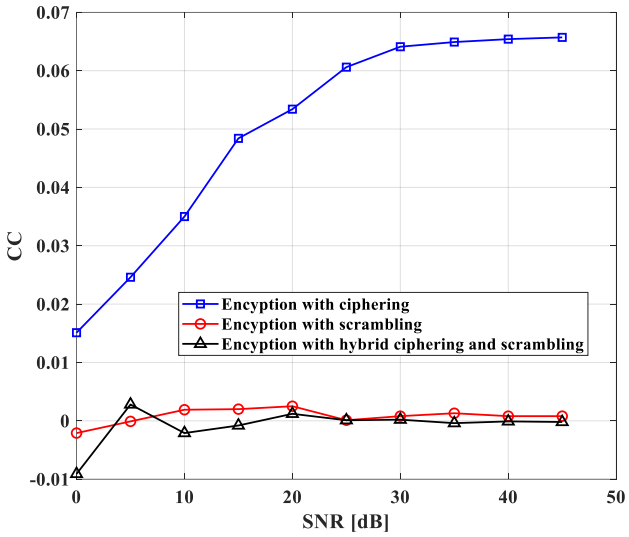

Figure. 15 CC performance of encrypted speech signal through MIMO-OFDM system

the best performance comparing with scrambling and combination. Also, for all SNR, LLR values greater than 3.35 for all methods. For SNRLOSS, fwSNRseg and CC, it is clearly that the performance of combined ciphering and scrambling together outperform both ciphering and scrambling alone. Also, scrambling method has performance better than ciphering method except LLR measure that appears the performance of ciphering method better than scrambling method for all SNR by gain not greater than 0.03.

6.3 Two dimensional chaotic simulation results

In this simulation, the BER and speech residual intelligibility performance are comparison for three types of TDCM that are TDLM, TDSM and TD-TFCDM. The comparisons are investigated for 64 QAM and 200 km/h. Combination of ciphering and scrambling method are used where PRBG and index permutation are generated by the same type of TDCM. Fig. 16 shows the BER comparisons between TDCM types where the data is recovered with the incorrect keys. The results show that the BER performance of TDSM has the highest BER values followed by TD-TFCDM. In general, all chaotic map has BER greater than 0.48 even though SNR is high.

Figs. 17-20 show the LLR, SNR_{LOSS}, fwSNRseg and CC residual intelligibility measure comparisons, respectively between different types of TDCM. For LLR results, TD-TFCDM has high security comparing with others followed by TDSM. For SNR_{LOSS} measure, the performance is fluctuation while TDSM appears the best performance. For fwSNRseg measure, TDLM has the best performance

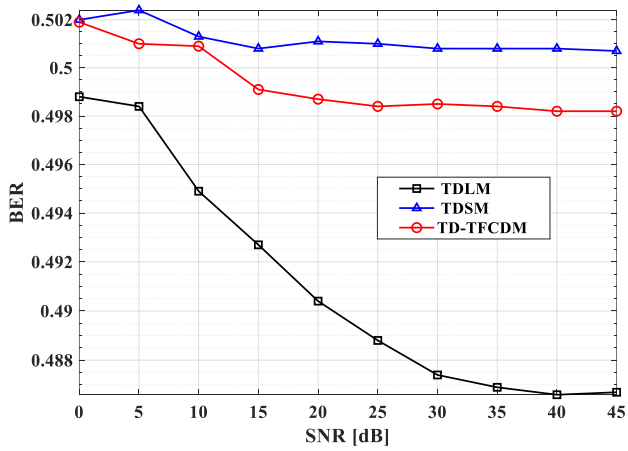

Figure. 16 BER comparisons of encrypted speech signal for different types of TDCM

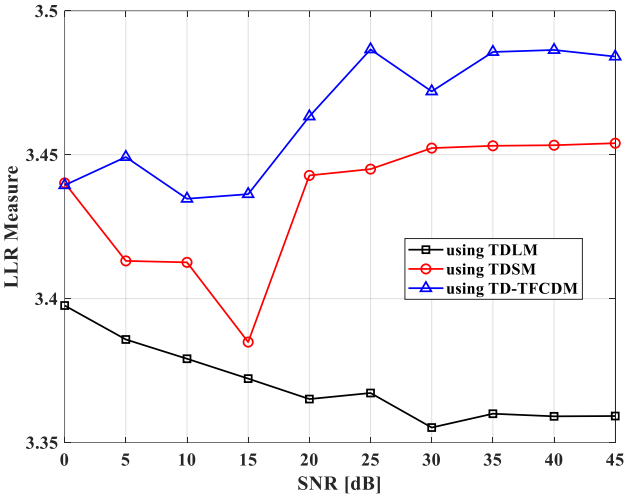

Figure. 17 LLR measure comparisons of encrypted speech signal for different types of TDCM

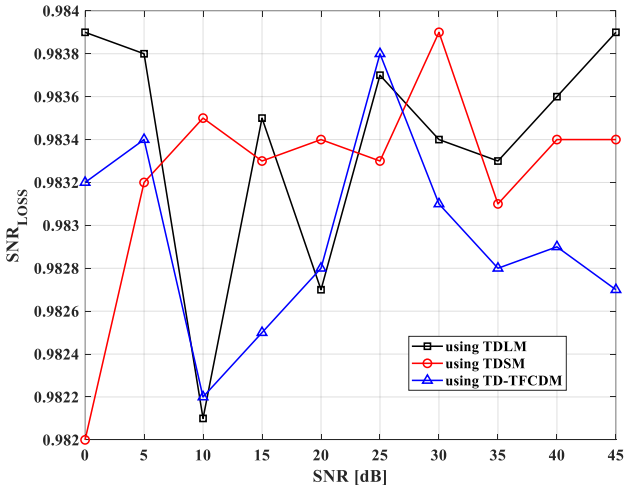

Figure. 18 SNR_{LOSS} measure comparisons of encrypted speech signal for different types of TDCM

when SNR <12 dB. When SNR>12 dB, TD-TFCDM becomes the best (high security). CC measure shows

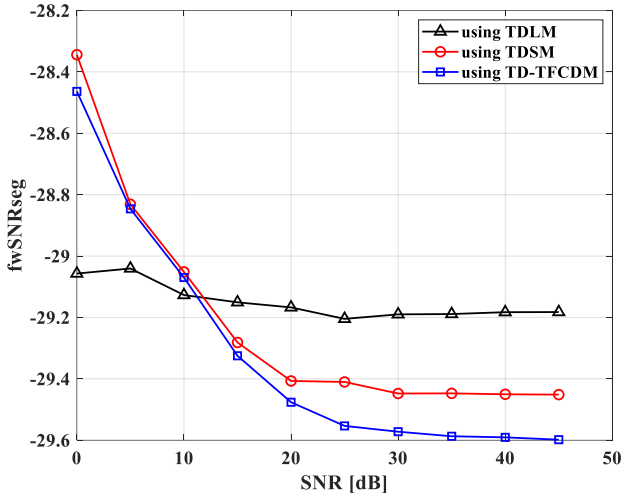

Figure 19 fwSNRseg measure comparisons of encrypted speech signal for different types of TDCM

.

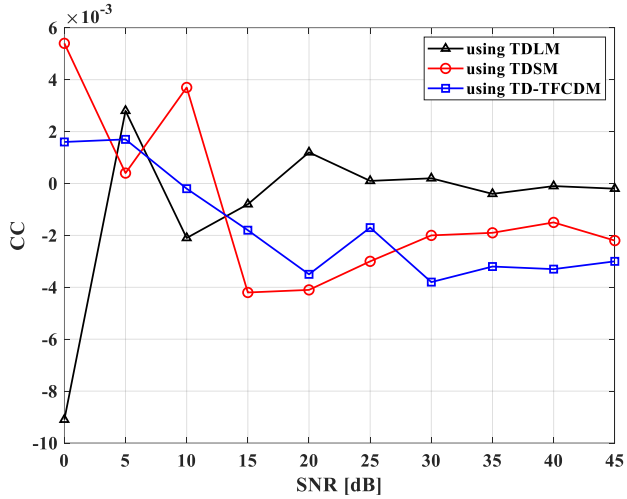

Figure. 20 CC measure comparisons of encrypted speech signal for different types of TDCM

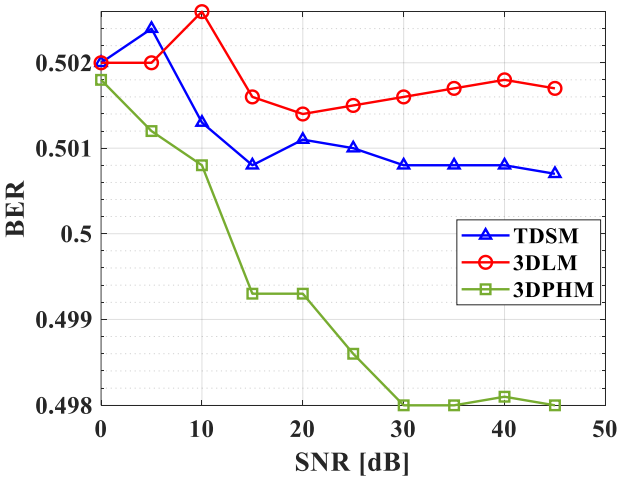

Figure. 21 BER comparisons of encrypted speech signal for different types of 3DCM

that TDSM and TD-TFCDM has better performance than TDLM.

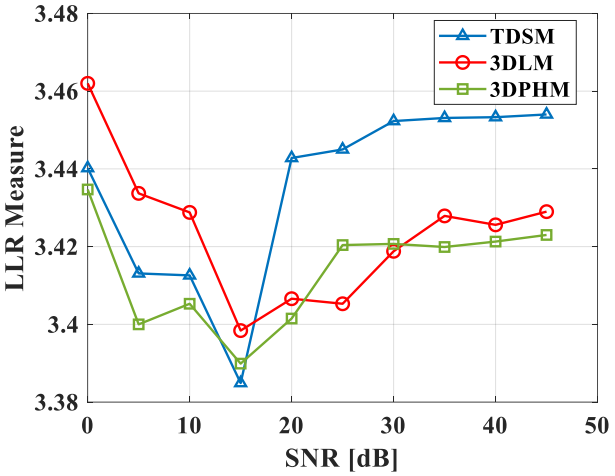

Figure. 22 LLR measure comparisons of encrypted speech signal for different types of 3DCM

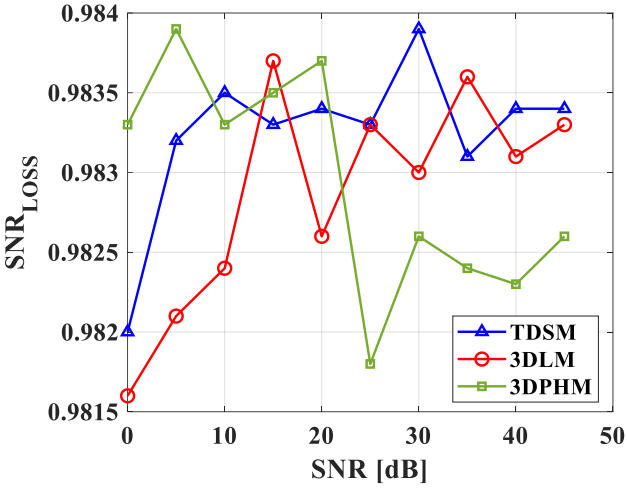

Figure. 23 SNR_{LOSS} measure comparisons of encrypted speech signal for different types of 3DCM

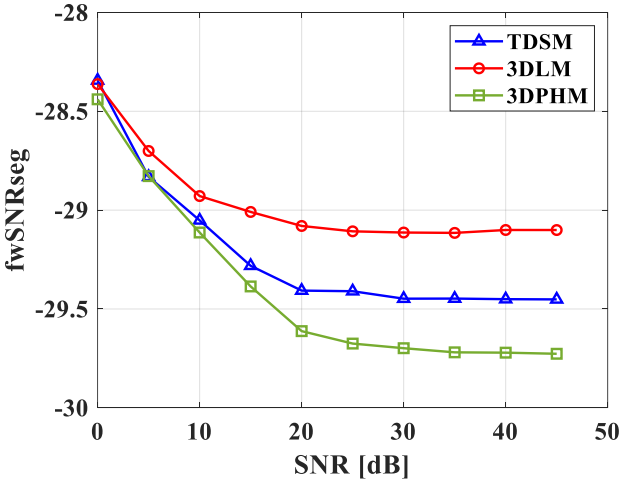

Figure. 24 fwSNRseg measure comparisons of encrypted speech signal for different types of 3DCM

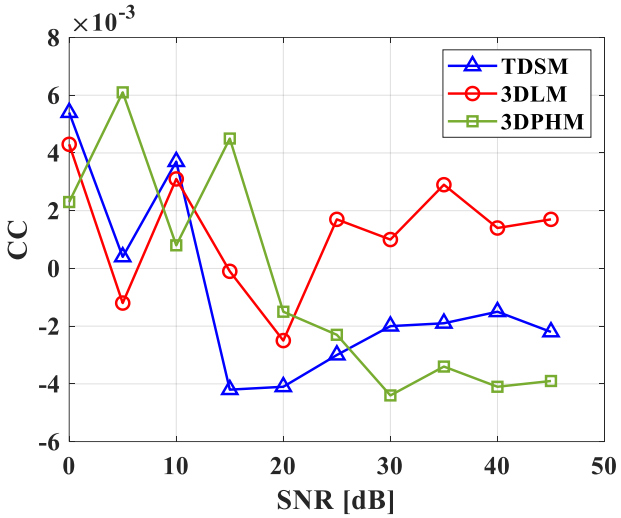

Figure. 25 CC measure comparisons of encrypted speech signal for different types of 3DCM

6.4 Three dimensional chaotic simulation results

In this simulation, the BER and speech residual intelligibility performance are comparison for the two types of 3DCM that are 3DLM, 3DPHM. The comparisons are investigated for 64 QAM and 200 km/h. Combination of ciphering and scrambling method are used where index permutation are generated by TDCM. Fig. 21 shows the BER comparisons between 3DCM types and TDSM where the data is recovered with the incorrect keys. The results show that the BER performance of 3DLM has the high security comparing with other map. In general, all chaotic map has BER greater than 0.49 even though SNR is high.

Figs. 22-25 show the LLR, SNR_{LOSS}, fwSNRseg and CC residual intelligibility measure comparisons, respectively between the two types of 3DCM. For LLR results, 3DLM has better performance than 3DPHM. For SNR_{LOSS} measure, the performance is fluctuation while TDSM and 3DLM appear better than 3DPHM. For fwSNRseg measure, 3DLM has the best results. CC measure shows that 3DPHM has better performance for high SNR (>20 dB).

7. Comparisons with other works

Tables 2 and 3 shows the comparison between previous works for encryption simulation results. From these tables we see that the proposed system outperform other systems.

8. Conclusion

In this paper, secure speech transmission through the MIMO-OFDM system is simulated over the doubly selective fading channel. Two levels of encryption are combined based on ciphering and scrambling methods. The PRBG and IP for ciphering and scrambling technique, respectively are generated using the TDCM. Three types of maps are studied which named TDLM, TDSM, and TD-TFCDM and used for generating PRBG and IP. Different speech quality and residual intelligibility measures including LLR, SNR_{LOSS}, fwSNRseg, and CC are used to test the decryption and encryption performance through the system as well as the BER performance. Furthermore, three dimensional chaotic map named 3DLM and 3DPHM are studied and compared with TDCM. The simulation results show that the speech signal over MIMO-OFDM system behaves well with high security. The encryption system using the TDSM and the TD-TFCDM outperform the TDLM in most residual intelligibility measures. Also, 3DCM enhance the security and key size of the system but increase the complexity and the processing time.

Table 2. BER comparisons at SNR=10 and 15 dB

SNR [dB]	Reference [1]	Reference [19]	Ours TDLM	Ours 3DLM
10	0.4663	0.422	0.4949	0.5009
15	0.407	0.392	0.4927	0.5016

Table 3. Speech residual intelligibility measures comparisons

Measure	Reference [10]	Reference [11]	Ours TDLM	Ours 3DLM
LLR	2.8897	2.9678	3.3651	3.406
SNR_{LOSS}	0.9849	0.9869	0.9827	0.983
fwSNRseg	-22.046	-22.3736	-29.16	-29.08

Conflicts of interest

The authors do not have any conflict of interest.

Author contributions

The first author has the following contribution: the validation and the investigation, writing the review and editing, the formal analysis and the funding acquisition. The second author has the following contribution: the methodology, the software, writing the original draft, supervision and project administration.

Acknowledgements

This work is supported by the college of Engineering/ Mustansiriyah University Iraq, Baghdad. (https://webmail.uomustansiriyah.edu.iq),

References

[1] G. Dhanya and J. Jayakumari, "Secure speech communication using improved OFDM scrambler for next generation mobile communication systems", *American-Eurasian Journal of Scientific Research*, Vol. 11, No. 1, pp. 56-62, 2016.

[2] J. Rahman, J. J. Sadique, M. S. Hossain, and S. E. Ullah, "Secured audio signal transmission in 5G compatible mmWave massive MIMO FBMC system with implementation of audio-to-image transformation aided encryption scheme", *Global Journal of Computer Science and Technology: E Network, Web and Security*, Vol. 18, No. 1, pp.13-17, 2018.

[3] M. G. Rashed, M. H. Kabir, M. S. Reza, M. M. Islam, R. A. Shams, S. Masum, and S. E. Ullah, "Transmission of voice signal: BER performance analysis of different FEC schemes based OFDM system over various channels", *International Journal of Advanced Science and Technology*, Vol. 34, pp. 89-100, 2011.

[4] Y. Xiaoyan, W. Jiaqing, Y. Luxi, and H. Zhenya, "Doubly selective fading channel estimation in MIMO-OFDM systems", *Science in China Series F: Information Sciences*, Vol. 48, pp. 795–807, 2005.

[5] M. A. Khan, M. Asim, V. Jeoti, and R. S. Manzoor, "On secure OFDM system: Chaos based constellation scrambling", In: *Proc. of IEEE International Conference on Intelligent and Advanced Systems*, Kuala Lumpur, Malaysia, pp. 484-488, 2007.

[6] M. S. Ehsani and S. E. Borujeni, "Fast Fourier transform speech scrambler", In: *Proc. of First International IEEE Symposium Intelligent Systems*, Varna, Bulgaria, pp. 248-251, 2002.

[7] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption algorithm using FFT and 3D-Lorenz–logistic chaotic map", *Multimedia Tools and Applications*, Vol. 79, pp. 17817–17835, 2020.

[8] F. J. Farsana and K. Gopakumar, "A novel approach for speech encryption: Zaslavsky map as pseudo random number generator," In: *Proc. of 6th International Conference on Advances in Computing & Communications, ICACC* 2016, Cochin, India, pp. 816-823, 2016.

[9] A. Belmeguenai, K. Mansouri and M. Lashab, "Speech Encryption Using Stream Cipher", *British Journal of Applied Science & Technology*, Vol. 8, No. 1, pp. 107-125, 2015.

[10] F. S. Hasan, "Speech encryption using fixed point chaos based stream cipher (FPC-SC)", *Eng. &Tech. Journal*, Vol. 34, No. A, pp. 2152-2166, 2016.

[11] Zahraa M. Dawood, M. Aboud, and F. S. Hasan, " Speech encryption using finite precision chaotic maps based stream ciphers", In: *Proc. of the International Conference on Information and Communication Technology*, Baghdad, Iraq, pp. 127–133, 2019.

[12] L. J. Sheu, "A speech encryption using fractional chaotic systems", *Springer, Nonlinear Dynamics*, Vol. 65, pp. 103–108, 2010.

[13] M. K. M. A. Azawi, and J. Q. Kadhim, "Speech Scrambling Employing Lorenz Fractional Order Chaotic System", *Journal of Engineering and Development*, Vol. 17, No. 4, 2013.

[14] A. K. Jawad, H. N. Abdullah, and S. S. Hreshee, "Secure speech communication system based on scrambling and masking by chaotic maps", In: *Proc. of International Conference on Advances in Sustainable Engineering and Applications (ICASEA)*, Iraq, pp. 7-12, 2018.

[15] E. M. Elshamy, E. Sayed, M. E. Rabaie, and O. S. Faragallah, "Efficient audio cryptosystem based on chaotic maps and double random phase encoding", *Springer, International Journal of Speech Technology*, Vol. 18, pp. 619–631, 2015.

[16] M. G. Rashed, M. H. Kabir, M. S. Reza, M. M. Islam, R. A. Shams, S. Masum, and S. E. Ullah, "Transmission of Voice Signal: BER Performance Analysis of Different FEC Schemes Based OFDM System over Various Channels", *International Journal of Advanced Science and Technology*, Vol. 34, pp. 89-100, 2011.

[17] N. F. Soliman, S. M. A. Alhalem, Sahar A. E. Rahman, M. M. Fouad, and F. E. A. E. Samie, "Speech transmission with COFDM based on different discrete transforms", *International Journal of Speech Technology*, Vol. 19, pp. 565–576, 2016.

[18] A. Jameel, M. Y. Siyal, and N. Ahmed, "Transform-domain and DSP based secure speech communication system", *Microprocessors and Microsystems*, Vol. 31, pp. 335–346, 2007.

[19] M. H. Kabir, J. Rahman2, and S. E. Ullah, "Secured voice frequency signal transmission in 5G compatible multiuser downlink MIMO NOMA wireless communication system", *International Journal of Networks and Communications*, Vol. 8, No. 4, pp. 97-105, 2018.

[20] A. M. Raheema, S. B. Sadkhan, and S. M. A. Sattar, "Performance comparison of hybrid chaotic maps based on speech scrambling for

OFDM techniques", In: *Proc. of IEEE Third Scientific Conference of Electrical Engineering (SCEE)*, University of Technology, pp.317-321, 2018.

[21] S. F. E. Zoghdy, H. S. E. Sayed and O. S. Faragallah, "Transmission of chaotic-based encrypted audio through OFDM", *Wireless Personal Communications*, Vol. 113, pp. 241–261, 2020.

[22] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption algorithm using FFT and 3D-Lorenz–logistic chaotic map", *Multimedia Tools and Applications*, Vol. 79, pp. 17817–17835, 2020.

[23] P. Krasnowski, J. Lebrun, and B. Martin, "Introducing a Novel Data Over Voice Technique for Secure Voice Communication", *Wireless Personal Communications*, Vol. 124, pp. 3077–3103, 2022.

[24] S. Rajendran and M. Doraipandian, "A nonlinear two-dimensional logistic-tent map for secure image communication", *Int. J. Information and Computer Security*, Vol. 10, No. 2/3, pp. 201-2014, 2018.

[25] E. M. Elshamy, E. M. E. Rabaie, O. S. Faragallah, O. A. Elshakankiry, F. E. A. E. Samie, H. S. Elsayed, et al., "Efficient audio cryptosystem based on chaotic maps and double random phase encoding", *International Journal of Speech Technology*, Vol. 18, No. 4, pp. 619–631, 2015.

[26] P. Li, L. Min, Y. Hu, G. Zhao and X. Li, "Novel two-dimensional discrete chaotic maps and simulations", In: *Proc. of IEEE 6th International Conference on Information and Automation for Sustainability*, Beijing, pp.159-162, 2012.

[27] V. Patidar, K. K. Sud, and N. K. Pareek, "A Pseudo random bit generator based on chaotic logistic map and its statistical testing", *Informatica*, Vol. 33, pp. 441–452, 2009.

[28] X. Huang, L. Liu, X. Li, M. Yu, and Z. Wu, "A New Pseudorandom Bit Generator Based on Mixing Three-Dimensional Chen Chaotic System with a Chaotic Tactics", *Hindawi Complexity*, Vol. 2019, pp. 1-9, 2019.

[29] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, and W. Wang, "A Novel Color Image Encryption Algorithm Based on Three-Dimensional Chaotic Maps and Reconstruction Techniques", *IEEE Access*, Vol. 9, pp. 61334-61345, 2021, doi: 10.1109/ACCESS.2021.3073514.

[30] C. Liu and Q. Ding, "A Color Image Encryption Scheme Based on a Novel 3D Chaotic Mapping", *Hindawi Complexity*, Vol. 2020, p. 20, 2020. Doi: 10.1155/2020/3837209.

[31] Y. Xiaoyan, W. Jiaqing, Y. Luxi and H. Zhenya, "Doubly selective fading channel estimation in MIMO-OFDM systems", *Science in China Ser. F Information Sciences*, Vol. 48, No. 6, pp. 795—807, 2005.

[32] R. Nissel, M. Rupp, and R. Marsalek, "FBMC-OQAM in doubly-selective channels: a new perspective on MMSE equalization", In: *Proc. of IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Sapporo, 2017.

[33] Y. Hu and P. C. Loizou, "Evaluation of Objective Quality Measures for Speech Enhancement", *IEEE Transactions on Audio, Speech and Language Processing*, Vol. 16, No. 1, pp. 229-238, 2008.

[34] J. Ma and P. C. Loizou, "SNR loss: a new objective measure for predicting the intelligibility of noise suppressed speech", *Speech Communication*, Vol. 53, pp. 340-354, 2011.

[35] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications", *National Institute of Standards and Technology (NIST)*, Special Publication 800-22, Revision 1, August 2008.