

Security analysis of encrypted audio based on elliptic curve and hybrid chaotic maps within GFDM modulator in 5G networks

Mohammed Jabbar Mohammed Ameen, Saad S. Hreshee

Department of Electrical Engineering, Collage of Engineering, University of Babylon, Babylon, Iraq

Article Info

Article history:

Received Sep 30, 2022

Revised Dec 16, 2022

Accepted Jan 19, 2023

Keywords:

Audio encryption

Chaotic maps

Elliptic curve-linear

congruential generator

Generalized frequency division

multiplexing

Massive multiple-input-

multiple-output

Parallel spatial modulation

ABSTRACT

Wireless communications face significant security challenges, so there is an ongoing necessity to develop an appropriate security strategy to protect data from eavesdroppers using cryptography based on chaos theory. Generalized frequency division multiplexing (GFDM) is a modern multicarrier waveform adaptable to 5G requirements, but its security issues have not been considered. Therefore, this paper proposed an efficient security technique within the GFDM modulator to protect the audio transmission against eavesdropping in 5G networks. The proposed GFDM is achieved by separating the subsymbols for the subcarrier into real and imaginary parts and combining them using a mixture of elliptic curve-linear congruential generator sequence (EC-LCG) with Ikeda and Tent maps, respectively. After that, the subsymbols of each subcarrier are permuted independently using the Duffing map. The effectiveness of the proposed approach to resist attacks was tested, and findings that were achieved are histogram, signal to noise ratio (SNR=-27.8068), spectral segment SNR (SSSNR=-34.9912), peak SNR (PSNR=0.9142), frequency weighted log spectral distance ($d_{FWLOG}=37.498$), cepstral distance ($d_{CD}=9.0176$), mean square error (MSE=0.82097), key space, and speed. These results show that the proposed model provides a high-security level, high speed in the encryption/decryption, large key space, and high sensitivity to the initial conditions.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Mohammed Jabbar Mohammed Ameen

Department of Electrical Engineering, Collage of Engineering, University of Babylon

60 Road, Hillah, Babylon, Iraq

Email: drmohammedalsalihy@gmail.com

1. INTRODUCTION

The development of 5G wireless communications has resulted in a significant increase in data transfer and massive growth in the number and types of mobile programs. When data are transmitted in the public wireless channel, they are exposed to negative attacks that affect the security of the information represented by the authenticity, confidentiality, and integrity of data, which is a major concern. Consequently, data must be encrypted on many systems before being sent to provide security [1].

Communications security based on chaos theory has emerged as a new subject in wireless communication research in recent years due to it providing the strongest approaches to protect data that travel through insecure channels. The chaos signal is deterministic, aperiodic, nonlinear, and long-term prediction. Since it is highly sensitive to initial conditions and control parameters, no two chaotic systems will develop identically. The chaotic system is classified into one-dimensional and multidimensional based on the number of positive Lyapunov exponents in the chaos system. Multidimensional chaotic systems are more complex and unexpected than one-dimension because of their numerous control parameters and initial conditions [2].

The production of unpredictable amounts, large enough and random enough, is necessary for the security of the majority of known cryptographic systems. Pseudorandom number generators (PRNG) can be generated using elliptic curves (EC). Elliptic curve cryptography (ECC) is a public-key algorithm that is significant in cryptography. Because of the fact of ECC has a small key space and offers a similar level of protection to other public-key algorithms that make use of larger key spaces. Additionally, it provides higher security levels while utilizing less computational power, memory, and bandwidth [3], [4].

Audio-based communication is increasing in the administrative, military, and various aspects of life. Audio has distinct characteristics, structure, and larger file sizes than images and texts. The encryption process guards the data against being accessed or destroyed by unofficial parties. The silent portion of the audio is filled with noise signals during encryption so that only a legitimate receiver can determine the audio content [5].

Massive multiple-input-multiple-output (MIMO) is an interesting wireless technique for meeting 5G requirements by maximizing capacity, throughput, and reliability. In order to improve the spectral efficiency of the transmission system, massive MIMO allows attaching thousands of device antennas to one base station. Also, spatial modulation (SM) scheme is employed with a 5G network to exploit some information resources in transmission [6]. The parallel spatial modulation (PSM) divides the transmitted antennas into subgroups and SM is then carried out independently in each group using similar signal constellations [2].

Furthermore, a massive MIMO must integrate with a multicarrier scheme to deal with the frequency-selective channels in 5G wireless networks. Generalized frequency division multiplexing (GFDM) is a promising new waveform for multicarrier design and is regarded as a generalized form of orthogonal frequency division multiplexing (OFDM) because it is more adaptable to the parameter selection process. Arranging the data in a two-dimensional time-frequency block minimizes the number of cyclic prefixes (CP) compared to valuable information [7]. The combination of massive MIMO-GFDM is very attractive to meet the ever-increasing needs for higher link readability and spectrum efficiency in 5G wireless communication networks [8].

Several audio encryption techniques have been proposed in past studies. Alwabhani and Bashier [9] presented audio encryption using two chaotic maps; a logistic map generates a one-time pad (OTP) for the diffusion phase and a circle map does the confusion phase. Alazawi and Kadhim [10] presented a speech encryption technique based on chaotic Lorenz fractional order. Saad and Hashim [11] introduced a voice encryption system using wavelet transforms and chaotic sequences to perform two-stage of key permutations. A voice encryption technique based on the principles of substitution and permutation by employing 2D logistic, Henon, and Baker maps was suggested in [12]. Mahdi and Hreshee [13] proposed an encryption algorithm to encrypt audio files based on XORed between the voice signal and the binary sequences generated from the chaotic Henon signal. Ismael and Sadkhan [14] presented an audio encryption algorithm using three chaotic maps named Chen, Lorenz, and Henon that mix with audio using a linear and nonlinear function. Kordov [15] suggested a voice encryption scheme based on a circle map and rotation equation to perform permutation and substitution for voice samples. Raheema *et al.* [16] carried out an audio encryption model using Henon and logistic maps for the OFDM technique through the additive white Gaussian noise (AWGN) channel. Raheema *et al.* [17] suggested a voice encryption algorithm for the OFDM waveform using triple chaotic signals named (random logistic map, random Lorenz system, and random Chen system) through the AWGN channel. Abdelfatah *et al.* [18] presented an audio encryption algorithm based on ECC and utilizing a 2D logistic-Lorenz chaotic sequence and hash function. Khoirom *et al.* [19] introduced a voice encryption model using ElGamal encryption algorithm over a finite field.

Through the preceding literature, the classical and contemporary voice encryption techniques do not provide adequate protection, and some modern systems do not yet have protection. In addition, some cryptosystems take a long time to process and leave residue noise in the decrypted audio. In order to overcome these difficulties, in this work, a novel and powerful audio encryption has been proposed, which provides a high level of security to withstand attacks. The main contributions of the proposed cryptosystem in this paper are:

- The encryption process performs inside communication components by securing the GFDM modulator.
- Minimizing residual intelligibility (R.I.) and high reconstructed audio signal quality.
- The subcarriers and subsymbols of GFDM are permuted and substituted using chaotic maps and EC-LCG sequence.
- The Ikeda and Tent map sequences are mixed with the EC-LCG sequence based on the modulo operator and then combined with real and imaginary parts of each subsymbol inside GFDM. The Duffing map sequence is employed to individually randomize the subsymbols in each subcarrier.
- The proposed cryptosystem has good chaotic behaviour, big keyspace, low calculations cost, and high encryption/decryption speed.

The remainder of the paper is formatted as follows. Section 2 briefly describes the techniques used, including PSM, GFDM, and massive MIMO. Section 3 introduces the principle of chaos theory in cryptography. Section 4 summarizes EC arithmetic over finite field. Section 5 presents the proposed audio encryption system using secure GFDM. Section 6 presents the performance evaluation and security tests for encrypted audio. Section 7 gives simulation results of the proposed scheme. Section 8 presents a security performance analysis and a comparison study with previous works. Finally, conclusions is in section 9.

2. BASIC PRINCIPLES

2.1. Parallel spatial modulation

The working principle of PSM can be summarized in the steps [7]:

- a. The transmitter antennas are divided into equal groups, each group contains $g=N_t/P$ antenna, where $2 \leq g \leq N_t$, and only one antenna is activated (sends data) per group individually. When $P=1$, this means that $g=N_t$, and therefore we get the conventional SM.
- b. The information bits are divided into $(P+1)$ parts, as seen in Figure 1, the first one part has $\log_2(M)$ bits and the remaining P parts comprise $\log_2(g)$ bits of each.
- c. The first part of information bits is used to modulate signal while the remaining parts is exploited to activate one antenna in each group
- d. The PSM spectrum efficiency in terms of bps/Hz can be expressed as (1):

$$\eta = P \times \log_2(g) + \log_2(M) \tag{1}$$

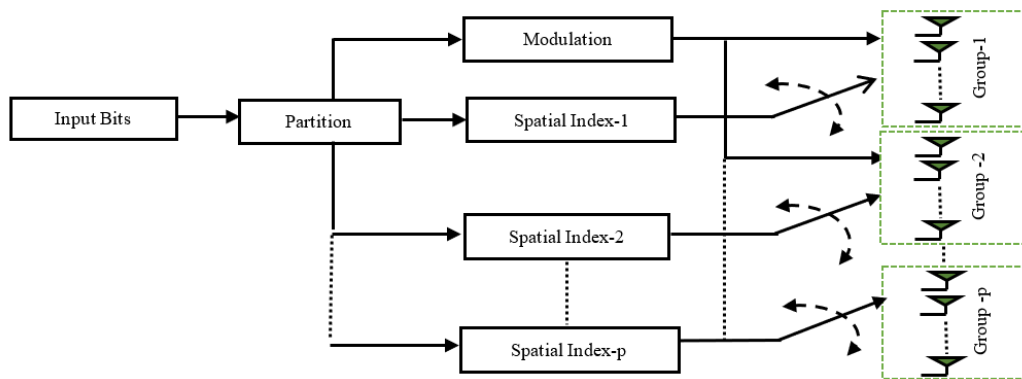


Figure 1. The block diagram of PSM [7]

2.2. Generalized frequency division multiplexing

GFDM is a digital and generic multicarrier modulation technique with pulse shaping, and it satisfies the different requirements of 5G networks. GFDM represents a non-orthogonal modulation method carried out on separate time-frequency blocks, each of which contains a collection of subcarriers in frequency and subsymbols in time. By circularly shifting in the time and frequency domain, the subcarriers on each subsymbol are filtered with applications that require a prototype filter. This approach will eliminate unwanted out-of-band (OOB) radiation and pave the way for spectrum distribution to succeed.

Also, GFDM provides additional properties in terms of reducing inter-carrier and inter-symbol interferences by using CP and pulse shaping. The time-frequency grid layout necessitates highly adaptable sophisticated methods in the receiver to achieve demodulating activities [20]. A single CP is utilized for the whole block in GFDM, even if it contains multiple subsymbols, whereas one CP should be used for every subsymbol in OFDM, as shown in Figure 2(a). OFDM has a considerably high peak-to-average power ratio (PAPR). It could be reduced by raising the subcarrier’s bandwidth and reducing the number of subcarriers. When designing GFDM and OFDM with the same length, the subcarriers become wider, and the block has lower subcarriers, lowering the PAPR in the GFDM block, as shown in Figure 2(b) [21]. The time-frequency resource grid of GFDM consists of K and M , which denote the numbers of subcarriers and subsymbols, respectively. There are KM sample locations in each resource block. As a result, if $KM=N$ is met, the quantity of information transmission by GFDM will equal the amount of transmission data for OFDM across the same symbol time and bandwidth. A pulse-shaping filter is used to identify the position of each resource block. The mathematical formula for the GFDM signal is as (2):

$$\begin{aligned}
 X[n] &= \sum_{k=0}^{K-1} \sum_{m=0}^{M-1} (d_{k,m} \delta[n - mk]) * g[n \bmod N] e^{j2\pi \frac{nk}{K}} \\
 X[n] &= \sum_{k=0}^{K-1} \sum_{m=0}^{M-1} d_{k,m} * \tilde{g}[n - mk] e^{j2\pi \frac{nk}{K}} \\
 X[n] &= \sum_{m=0}^{M-1} \tilde{g}[n - mk] \underbrace{\sum_{k=0}^{K-1} d_{k,m} e^{j2\pi \frac{nk}{K}}}_{IDFT}
 \end{aligned}
 \tag{2}$$

The convolution functions are represented by where (*). In (2), $\tilde{g}[n - mk] \triangleq g[(n - mk) \bmod N]$ is the pulse shaping filter with mK time-shifting, the mod operator is equal to the tail-biting procedure that makes a circular convolution filter. In (2) can simplify to OFDM when $M=1$ and the rectangular pulse shaping filter is used. Similarly, in (2) can convert to the single-carrier transmission in the case of $K=1$; therefore, this method is known as GFDM. The GFDM modulator is as described in Figure 3 [22].

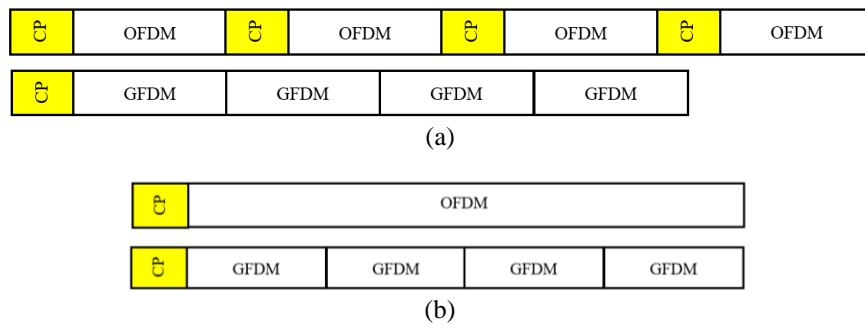


Figure 2. The comparison between OFDM and GFDM block (a) CP saving by GFDM and (b) lowering PAPR in GFDM more than OFDM [22]

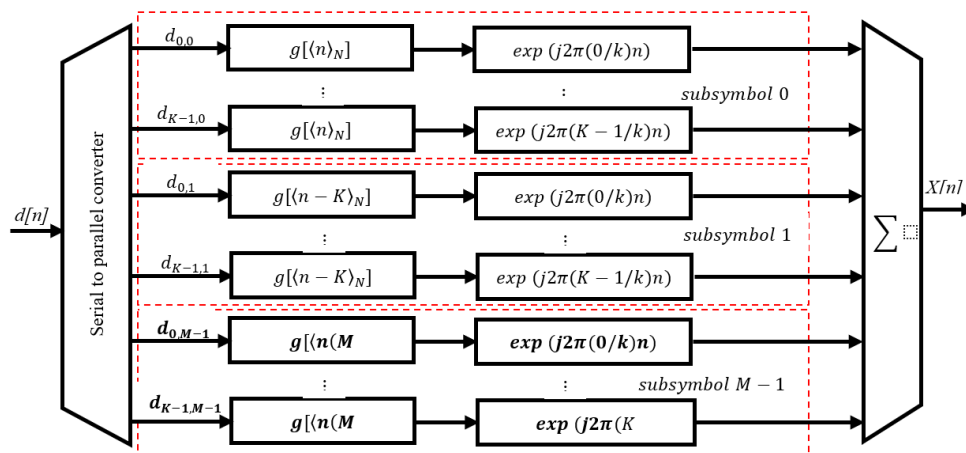


Figure 3. Detail of the GFDM modulator [23]

2.3. Configuration of massive multiple-input-multiple-output system

This paper’s point-to-point massive MIMO transceiver system comprises the number of N_t and N_r antennas at the transmitter and receiver, respectively. The received signal $Y=[y_1, y_2, \dots, y_{N_r}]$ at the base station can be estimated using the formula $Y=Hx+n$ and the received signal in matrix form as (3):

$$\begin{bmatrix} y_1 \\ \vdots \\ y_{N_r} \end{bmatrix} = \begin{bmatrix} h_{1,1} & \dots & h_{1,N_t} \\ \vdots & \ddots & \vdots \\ h_{N_r,1} & \dots & h_{N_r,N_t} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_{N_t} \end{bmatrix} + \begin{bmatrix} n_1 \\ \vdots \\ n_{N_r} \end{bmatrix}
 \tag{3}$$

Where $X=[x_1, x_2, \dots, x_{N_t}]$ indicates the transmitted signals by each antenna, $n=[n_1, n_2, \dots, n_{N_r}]$ mean the AWGN that has zero mean and σ variance of each, and the channel matrix $H \in \mathbb{C}^{N_r \times N_t}$ represents the

fading between the antennas. Minimum means square error estimation (MMSE) algorithms are used to equalize the received signal [24].

3. CRYPTOGRAPHY SYSTEM BASED ON CHAOS THEORY

Chaos theory is a mathematical field that studies nonlinear, dynamical, and complex systems that are apparently random but deterministic. Chaos theory deals with the study of deterministic difference-differential mathematical equations that exhibit sensitive dependence on initial conditions (SDIC) by producing time pathways that appear random. This means that even a tiny variation in measuring the system's state can cause a significant change in its future behavior. This makes it impossible to predict the system's long-term behavior with any accuracy.

Chaos theory has been applied to cryptography to create innovative encryption techniques for audio, image, video, text, data, and watermarking encryption. Cryptography can use a pseudo-chaotic system that is based on chaos theory. Chaos initial conditions and parameters can be utilized as a cryptographic key. Cryptography use diffusion, representing the sensitivity of chaotic parameters to the initial condition. The initial state of the chaos sequence can be mixed with the plaintext to produce keys in cryptography. The final state of the chaos sequence represents ciphertext in cryptography. Asymptotic independence of initial and final states in chaos can be employed as confusion in cryptography.

The chaotic systems used in cryptography can be classified into two categories: maps and flows. Maps are represented by difference equations and are often referred to as discrete systems. Flows are represented by differential equations and are often referred to as continuous systems. Chaotic system dynamics behavior is described using the time domain called time series or in phase space called a strange attractor.

Within this taxonomy, chaotic maps are graded from one-dimensional to multidimensional depending on the number of variables in the equations of the chaotic maps. When mixing two or more types of chaotic maps, a chaotic hybrid map can be created with a more complicated chaotic property than the majority of single chaotic maps and more SDIC. This is because the hybrid approach takes advantage of all the strengths of the combined chaotic maps and attempts to reduce the weakness of one of the weak chaotic maps. Table 1 outlines discrete maps which are used in this paper [7], [25]-[27].

Table 1. List of chaotic maps used

Chaotic maps	Time domain	Equations	Number of space dimensions	Parameter values and initial condition
Duffing map	Discrete	$X_{n+1} = Y_n$ $Y_{n+1} = -bX_n + aY_n - Y_n^3$	2	$a = 2.75; b = 0.2$ $X_d(0) = -1.7$ $Y_d(0) = -1$
Ikeda map	Discrete	$X_{n+1} = 1 + u(X_n \cos t_n - Y_n \sin t_n)$ $Y_{n+1} = u(X_n \sin t_n + Y_n \cos t_n)$ $t_n = 0.4 - \frac{u}{1 + X_n^2 + Y_n^2}$	2	$X_i(0) = 0.527,$ $Y_i(0) = -0.5271$ $u = 0.708$
Tent map	Discrete	$X_{n+1} = \begin{cases} \mu X_n, & X_n < 0.5 \\ \mu(1 - X_n), & X_n \geq 0.5 \end{cases}$	1	$X_i(0) = 0.4$ $\mu = 1.9$

4. CURVE ARITHMETIC OVER FINITE FIELD

For a given prime number p, suppose Fp represents the finite field of p, so the EC over Fp can be defined by the relation in (4):

$$y^2 = x^3 + ax + b \tag{4}$$

where the coefficients a, b ∈ Fp and should be satisfied by (5):

$$4a^3 + 27b^2 \neq 0 \tag{5}$$

Scalar multiplication is necessary to perform point multiplication on EC. The fundamental operations of EC are point addition and point doubling. By assuming there are two points, P (x1, y1) and Q (x2, y2), belonging to Fp, the coordinate addition P+Q yields the third point, R (x3, y3), satisfying the EC equation as in (6)-(8):

$$x_3 = [\lambda^2 - x_1 - x_2] \text{ mod } p \tag{6}$$

$$y_3 = [\lambda(x_1 - x_3) - y_1] \bmod p \tag{7}$$

$$\lambda = \begin{cases} \left(\frac{y_2 - y_1}{x_2 - x_1} \right) \bmod p & \text{when } P \neq Q \\ \left(\frac{3x_1^2 + a}{2y_1} \right) \bmod p & \text{when } P = Q \end{cases} \tag{8}$$

In the subtraction case, the sign inversion of the y-coordinate of the second point is needed and solved as (9):

$$P(x_1, y_1) - Q(x_2, y_2) = P(x_1, y_1) + Q(x_2, -y_2) \tag{9}$$

Point multiplication calculations can be improved by effectively using point addition and doubling operations. Point multiplication can be calculated as many points are added together. For instance, when one needs to estimate nP, where n is a positive integer, then:

$$nP = P + P + \dots, n = 1, 2, \dots \tag{10}$$

The PRNG can be generated based on the group of points of an EC defined over a prime finite field. This work uses a linear congruential generator on elliptic curve (EC-LCG), a type of PRNG sequence. The EC-LCG sequence for a given U_0 and $G \in F_p$, where G represents the generating point, and U_0 represents the initial value (seed), is defined as (11):

$$U_n = U_{n-1} + G = nG + U_0, n = 1, 2, \dots \tag{11}$$

The initial value $U_0 = (x_0, y_0)$, and the constants $G, a,$ and b can be taken as secret keys in the cryptographic algorithm [19], [27], [28]. In this work, the parameter values used are $p=4,093, a=9, b=7, G=(4,1110)$, and $U_0 = (332,1395)$. Therefore, the keyspace of the EC-LCG sequence is 2^{60} by assuming a and b are constant.

5. THE PROPOSED SECURE GFDM SYSTEM

The proposed GFDM modulator is described in detail in this section, as shown in Figure 4. The proposed secure model depends on substitution and permutation principles. Three chaotic and EC-LCG sequences are mixed separately with the data inside GFDM. Substitution is performed inside the GFDM system by separating subsymbols into real and imaginary parts. Then the result of the modulo operation between the Ikeda map and the x-coordinate of EC-LCG is combined with the real part of the GFDM subsymbol. Similarly, the result of the modulo operator between the Tent map and the y-coordinate of EC-LCG is combined with the imaginary part of the GFDM subsymbol.

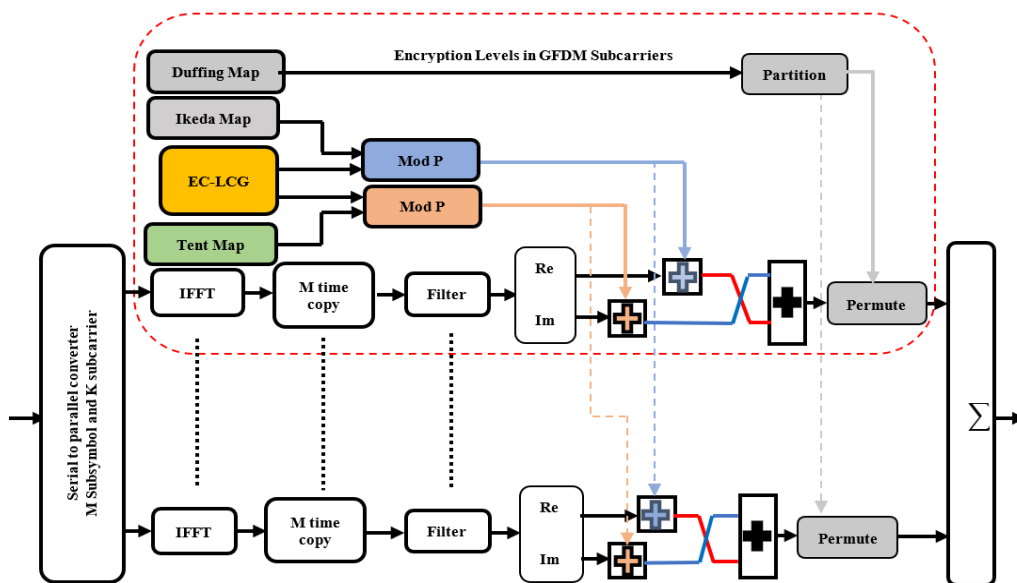


Figure 4. Block diagram of the proposed GFDM

After that, the real and imaginary parts are swapped and reconstructed data again to complex-valued. For permutation operation, the data index is randomized using the Duffing map. Now, the proposed GFDM is being implemented onto 5G wireless communication networks architecture that consists of massive MIMO and PSM; the details of each part are illustrated in Table 2 and Figure 5. On the transmitter side, the original audio is sampled at a frequency of 8 kHz and saved in WAV audio format. Then, an analogue-to-digital converter (ADC) is used to convert the audio into a binary system. In order to satisfy the PSM requirement, the incoming bitstream is partitioned into six groups, each with 4 bits, one group used for 16 quadrature amplitude modulation (QAM) modulation, and the remaining groups used for antenna index. The outputs of each PSM group are modulated using the proposed GFDM and then transmitted using multiple antennas through the fading channel. On the receiver side, the decrypting process can be completed successfully by performing procedures similar to the transmitter but in the opposite direction and generating the same secret key and its positions.

Table 2. Simulation parameters

Parameter	Value
Number of subcarriers (K)	16
Number of time slots (M)	5
Pulse shaping filter	Raised cosine filter
Roll-off factor	0.2
Modulation scheme	16-QAM
Length of cyclic prefix (CP)	20
Number of transmit antennas (N _t)	80
Number of receive antennas (N _r)	80
Channel fading	Rayleigh
Number of group (p)	5
Group size (g)	16

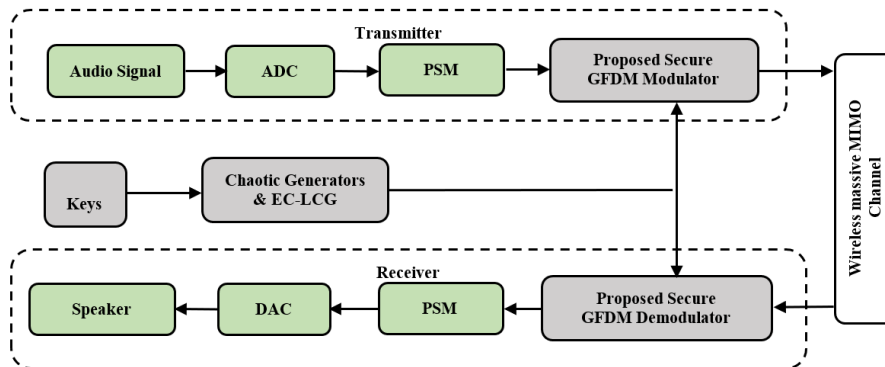


Figure 5. Block diagram of the proposed cryptosystem

6. SECURITY ASSESSMENT KEYS

The encryption algorithm must effectively protect audio transmitted on the public wireless channel and be impervious to eavesdropping techniques. A valuable indicator for considering and establishing a system's security needs is R.I. If the audio's R.I. is low, the audio is indistinct (high-security level) [2]. The proposed cryptosystem algorithm's R.I. was evaluated using the following tests.

6.1. Signal to noise ratio

SNR can be used to assess the audio encryption/decryption waveform quality. When the SNR is low, this means a good encryption algorithm. The encrypted audio SNR values are calculated as (12):

$$SNR = 10 \log_{10} \frac{\sum_{i=1}^N x_i^2}{\sum_{i=1}^N (x_i - y_i)^2} \tag{12}$$

where x_i and y_i are original and encrypted audio samples, respectively.

6.2. Peak signal to noise ratio

The mean square error of the original (x_i) and encrypted (y_i) audio can be estimated as (13):

$$MSE = \frac{1}{N} \sum_{i=1}^N (x_i - y_i)^2 \quad (13)$$

Then, peak signal to noise ratio (PSNR) can be determined using (14):

$$PSNR = 10 \log_{10} \left(\frac{MAX^2}{MSE} \right) \quad (14)$$

Where MAX denotes the maximum value of the encrypted audio. Lower PSNR implies that the audio has a high amount of noise, indicating that the encryption technique is good and resistant to attacks [7].

6.3. Spectral segment signal to noise ratio

The SSSNR is abbreviated as in (15):

$$SSSNR = 10 \log \left[\frac{\sum_{i=0}^{N-1} |x_i|^2}{\sum_{i=0}^{N-1} (|x_i| - |y_i|)^2} \right] \quad (15)$$

where x_i and y_i are DFT of clean and encrypted audio samples respectively.

6.4. Cepstral distance

The cepstral distance (d_{CD}) is written as (16):

$$d_{CD} = 10 \log \sqrt{2 \sum_{i=1}^p (C_x(i) - C_y(i))^2} \quad (16)$$

Where $C_x(i)$ and $C_y(i)$ are the cepstral coefficient of original and encrypted audio respectively. Also, the linear predictive coding (LPC) coefficient can be used to calculate the d_{CD} [13].

6.5. Frequency weighted log spectral distance (d_{FWLOG})

It is possible to understand audio with a frequency band of 300-500 Hz. In other words, the audio R.I. components are found within this frequency band. As a result, distance measures more appropriate for cryptanalysis of transform domain audio encryption would prefer accurate coefficient reposition in this frequency band. One method is to mask elements of the original and cryptanalysis audio signal spectrum to zero, restricting distance measurements to the 300-500 Hz region. A masking window can be applied to the spectrum of the two frames to compare these frequencies as (17):

$$d_{FWLOG} = \frac{1}{n} \sum_{f=a}^b |\log(s(f)) - \log(s'(f))|^p, f = a, a+1, \dots, b \quad (17)$$

where a and b are the index of upper and lower frequency spectral coefficients, and $n=b-a+1$ [7].

7. SECURITY ASSESSMENT KEYS

7.1. Histogram analysis

The quality of scrambled audio can be determined using histogram analysis, which is a simple and practical approach. The original audio converts to random-like noise with an approximately flat sample value distribution to be a more secure encryption method. Figures 6(a)-(c) show the histogram of the original, encrypted, and decrypted audio, respectively.

7.2. Key space and sensitivity analysis

Keyspace and key sensitivity are major factors that affect audio encryption efficiency. Keyspace refers to the collection of secret keys used in audio encryption. When there is a small change in the encryption key, audio decryption is impossible, which means key sensitivity. Powerful audio encryption must have a large keyspace and great sensitivity to be secure against attacks [29]. Table 3 shows the keyspace of each chaotic map employed in the proposed system.

Assuming that the precision of the calculation in MATLAB R2020a is about (10^{-15}) , meaning that there are $(10^{15} \approx 2^{50})$ values for each secret key that can choose, then the overall secret keys space of the proposed model is 2,510. In order to examine the key sensitivity of the proposed system, one key is changed by a very small value, while the remaining keys are unaltered during implementation [5]. The statistical

measurements to show the sensitivity key is the percentage of difference (P. Diff.), d_{CD} , d_{FWLOG} , MSE, SNR, PSNR, and SSSNR, as illustrated in Table 4. When the values of P. Diff. MSE and d_{CD} are high, and the values of SNR, PSNR, and SSSNR are small is means a large key sensitivity of the proposed system. The proposed system's secret keys are a, b, $X_d(0)$, $Y_d(0)$, u, $X_i(0)$, $Y_i(0)$, $X_t(0)$, and μ for chaotic maps and p, X_o , Y_o , G_x , and G_y for EC-LCG. The following factors should be considered when evaluating the proposed system from a statistical point of view: i) minimizing SNR, SSSNR, and PSNR values implies the reduction of R.I. in encrypted audio (high-security level) and ii) the increased d_{FWLOG} , d_{CD} , and MSE values mean a low R.I. of audio.

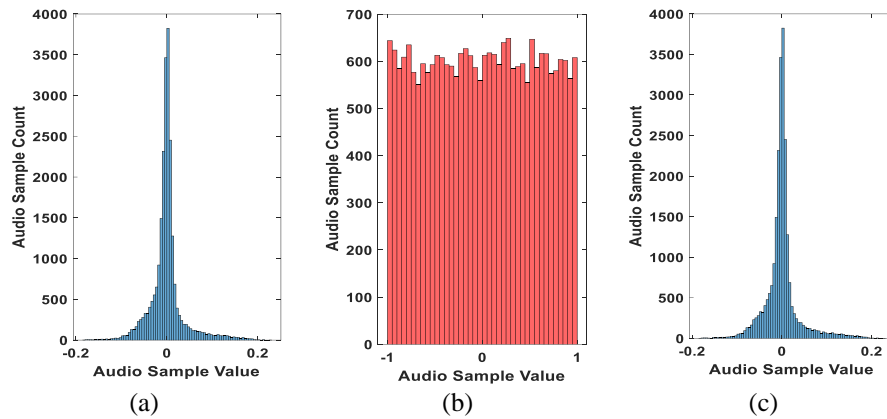


Figure 6. Histogram of audio-2: (a) original, (b) encrypted, and (c) decrypted

Table 3. Key space of proposed cryptosystem

Chaotic maps	Number of control parameters	Number of initial conditions	Keyspace
Duffing	2	2	$(10^{15})^4 \approx 2^{200}$
Ikeda	1	2	$(10^{15})^3 \approx 2^{150}$
Tent	1	1	$(10^{15})^2 \approx 2^{100}$
EC-LCG	3	2	$(2^{12})^5 \approx 2^{60}$

Table 4. Key sensitivity examination of the proposed cryptosystem using audio-2 with a duration of 3 second

Map	Change key value	MSE	d_{CD}	d_{FWLOG}	SSSNR	SNR	PSNR	P. Diff (%)
Duffing	a + 10^{-8}	0.77512	9.0176	32.8403	-34.7283	-27.6171	1.1039	100
	b + 10^{-8}	0.73861	8.8635	34.2837	-34.4992	-27.4854	1.2356	100
	$X_d(0)+10^{-8}$	0.74226	8.9897	32.4557	-34.5244	-27.6421	1.0789	100
	$Y_d(0)+10^{-8}$	0.82097	8.9547	34.7219	-34.9912	-27.8068	0.9142	100
Ikeda	u + 10^{-8}	0.71348	6.9245	34.11	-34.1827	-27.2366	1.4844	99.982
	$X_i(0)+10^{-8}$	0.70772	7.0754	34.2933	-34.1328	-27.2201	1.5009	99.987
	$Y_i(0)+10^{-8}$	0.71526	6.9862	33.9975	-34.1996	-27.2760	1.445	99.987
Tent	$X_t(0)+10^{-8}$	0.71542	6.9466	33.8375	-34.2445	-27.257	1.464	99.975
	$\mu+10^{-8}$	0.72796	6.9208	33.4152	-34.3351	-27.3442	1.3768	99.983
EC-LCG	P+1	0.65034	2.2799	36.6504	-33.7564	-26.8838	1.8372	99.995
	Xo+1	0.63268	2.4718	34.9047	-33.5828	-26.726	1.995	99.995
	Yo+1	0.62573	2.4039	36.9023	-33.4724	-26.6888	2.0322	99.983
	Gx+1	0.63191	2.3286	37.498	-33.6108	-26.75	1.971	99.995
	Gy+1	0.64307	2.3771	36.0941	-33.6649	-26.8428	1.8782	99.995

7.3. Time analysis

The speed with which a powerful encryption technique executes is an important quality factor. The encryption/decryption time is the duration required to complete the encryption/decryption technique procedures. This time is proportional to the length of the audio [30]. Accordingly, the proposed algorithm is implemented in MATLAB R2020a under Windows 10, using a PC with Intel(R) Core (TM) i7-7500U @ 2.70 GHz 2.9 GHz, 8 GB RAM, and 64-bit operating system. Two audio files of different lengths were used. The computational time and speed can be summarized in Table 5. The model waveforms data are exhibited in Figures 7 and 8. The approach turns the original audio into practically noise-like encrypted audio.

Table 5. Time analysis

Audio file	Duration (sec)	Size (KB)	Total time (sec)	Speed (sec/KB)
Audio-1	2	32.0	0.79	24.7×10^{-6}
Audio-2	3	48.0	1.15	24×10^{-6}

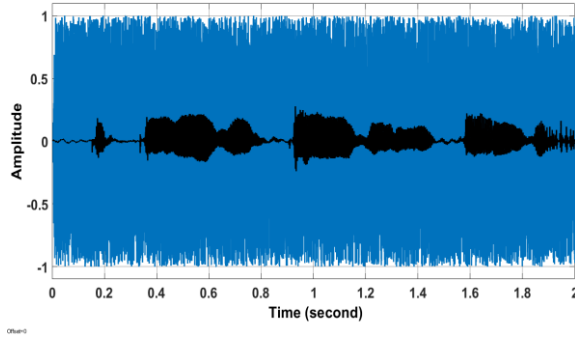


Figure 7. Audio encryption waveforms results for audio-1

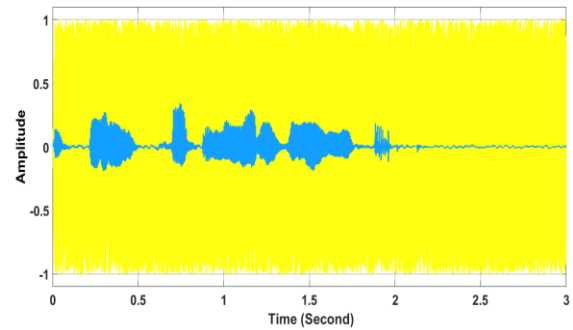


Figure 8. Audio encryption waveforms results for audio-2

7.4. Noise effect

In this part of the simulation results, the impact of noise on the recovered audio at the receiver was examined. This was done by calculating several metrics, including SSSNR, PSNR, d_{FWLOG} , d_{CD} , and MSE, which measure the quality of the audio. These calculations were performed between the original audio and the recovered audio of the proposed secure GFDM system at different SNR values. The results are presented in Figures 9-13, providing a comprehensive analysis of the system's performance under varying noise conditions.

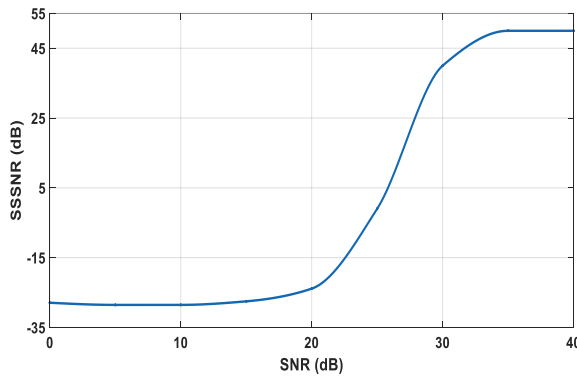


Figure 9. SSSNR variation of the recovered audio

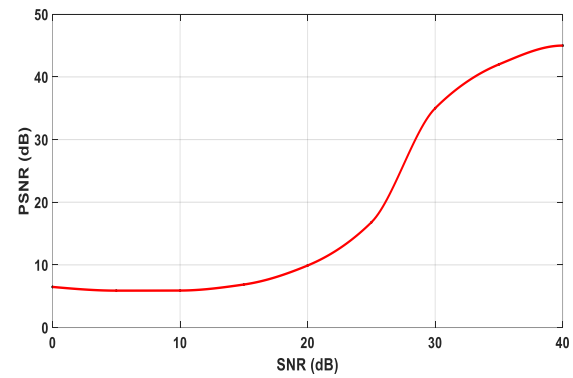


Figure 10. PSNR variation of the recovered audio

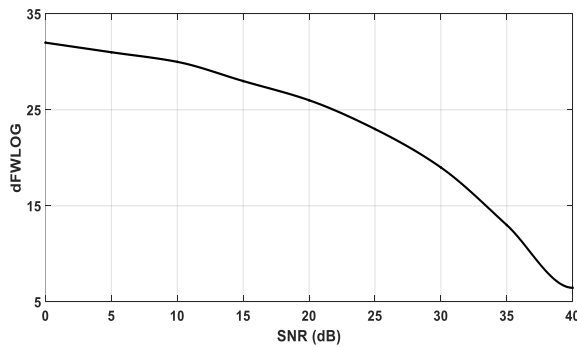


Figure 11. d_{FWLOG} variation of the recovered audio

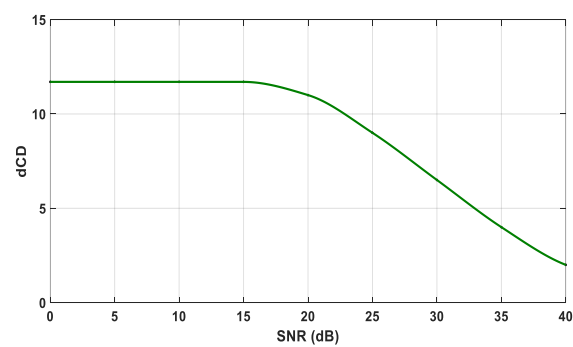


Figure 12. d_{CD} variation of the recovered audio

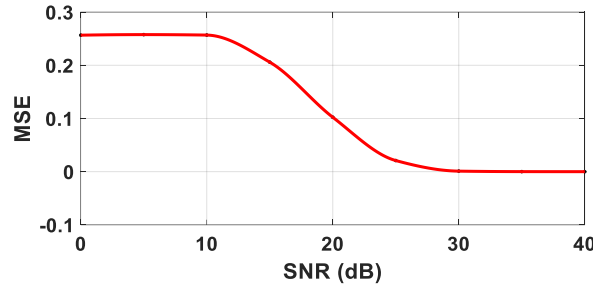


Figure 13. MSE variation of the recovered audio

8. SECURITY PERFORMANCE ANALYSIS

The investigation of the security performance in terms of the bit error rate (BER) was achieved, as shown in Figure 14. The BER of the authorized receiver and the eavesdropping receiver without knowing the secret keys for chaotic and EC-LCG sequences were tested. The plot shows that the eavesdropper could not retrieve the information without the secret keys due to the high BER of around 0.5. However, the legitimate receiver could obtain the information with an acceptable BER.

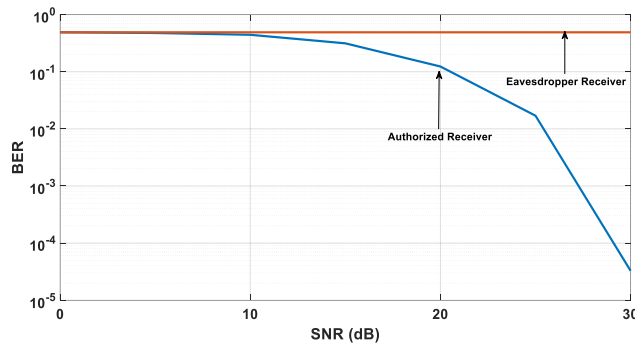


Figure 14. BER of authorized and eavesdropper receiver

In addition, to evaluate the weakness and strong points of the proposed cryptosystem, the suggested audio encryption technique’s performance is compared to other related techniques. Keyspace, SNR, PSNR, SSSNR, P.Diff., d_{CD} , d_{FWLOG} , MSE, and speed are the security metrics considered for this comparison, as shown in Table 6. This comparison shows that the proposed method provides better results than existing works and is compatible with the requirements of 5G networks.

Table 6. Security metric comparison with previous techniques

Ref.	Keyspace	SNR	PSNR	SSSNR	P. Diff (%)	d_{CD}	d_{FWLOG}	MSE	Speed
[16]	-	-	-	-28.22	-	8.987	20.9976	-	-
[9]	2^{280}	-14.0093	-	-	99.92	-	-	-	-
[13]	2^{427}	-	-	-4.2272	-	7.097	-	-	-
[10]	-	-	-	-19.6325	-	4.2037	-	-	-
[17]	-	-	-	-22.6783	-	-	-	0.4175	-
[14]	2^{480}	-	-	-16.723	99.14	7.2274	-	-	-
[7]	2^{500}	-20.971	4.746	-29.703	100	10.9592	22.1612	0.3352	0.0045
[5]	2^{600}	-25.9956	2.5998	-31.901	100	9.6945	-	0.54973	0.7690
[2]	2^{500}	-23.1223	-	-27.6149	100	9.4159	-	-	0.0329
This work	2^{510}	-27.8068	0.9142	-34.9912	100	9.0176	37.498	0.63191	24×10^{-6}

9. CONCLUSION

This paper proposed a novel audio encryption approach by employing several chaotic maps and EC arithmetic to encrypt audio in the massive MIMO-GFDM transmission system. This approach is based on chaotic maps of Ikeda, Tent, Duffing, and EC-LCG for the permutation and substitution processes inside

GFDM. The security analysis results show that very low values were obtained for SNR, PSNR, and SSSNR, which means high noise levels in encrypted audio. Also, high values for d_{CD} , d_{FWLOG} and MSE were obtained, indicating low R.I. The large key space and high sensitivity of the secret keys satisfy the required security level against various attacks. Ultimately, the proposed secure GFDM modulation is a powerful and suitable cryptosystem for 5G wireless networks. Moreover, the high speed obtained for the encryption/decoding process allows the proposed approach for real-time applications. In the future, it is important to determine whether the encryption using subcarrier locations of secure GFDM impacts security levels.




REFERENCES

- [1] M. F. Haroun and T. A. Gulliver, "Secure OFDM with peak-to-average power ratio reduction using the spectral phase of chaotic signals," *Entropy*, vol. 23, no. 11, pp. 1-15, Oct. 2021, doi: 10.3390/e23111380.
- [2] M. J. M. Ameen and S. S. Hreshee, "Securing physical layer of 5G wireless network system over GFDM using linear precoding algorithm for massive MIMO and hyperchaotic QRDecomposition," *International Journal of Intelligent Engineering and Systems*, vol. 15, no. 5, pp. 579-591, Oct. 2022, doi: 10.22266/ijies2022.1031.50.
- [3] D. Mahto and D. K. Yadav, "Network security using ECC with biometric," in *Quality, Reliability, Security and Robustness in Heterogeneous Networks: 9th International Conference, QShine 2013*, 2013, vol. 115, pp. 842-853, doi: 10.1007/978-3-642-37949-9_73.
- [4] O. Reyad and Z. Kotulski, "Statistical analysis of the chaos-driven elliptic curve pseudo-random number generators," in *Communications in Computer and Information Science (CCIS)*, vol. 448, pp. 38-48, 2014, doi: 10.1007/978-3-662-44893-9_4.
- [5] M. J. M. Ameen and S. S. Hreshee, "Hyperchaotic based encrypted audio transmission via massive MIMO - GFDM system using DNA coding in the antenna index of PSM," in *IICETA 2022 - 5th International Conference on Engineering Technology and its Applications*, May 2022, pp. 19-24, doi: 10.1109/IICETA54559.2022.9888569.
- [6] R. Chataut and R. Akl, "Massive MIMO systems for 5G and beyond networks—overview, recent trends, challenges, and future research direction," *Sensors*, vol. 20, no. 10, pp. 1-35, May 2020, doi: 10.3390/s20102753.
- [7] M. J. M. Ameen and S. S. Hreshee, "Hyperchaotic modulo operator encryption technique for massive multiple input multiple output generalized frequency division multiplexing system," *International Journal on Electrical Engineering and Informatics*, vol. 14, no. 2, pp. 311-329, Jun. 2022, doi: 10.15676/ijeei.2022.14.2.4.
- [8] R. Zayani, H. Shaiek, and D. Roviras, "PAPR-aware massive MIMO-OFDM downlink," *IEEE Access*, vol. 7, pp. 25474-25484, 2019, doi: 10.1109/ACCESS.2019.2900128.
- [9] S. M. H. Alwabhani and E. B. M. Bashier, "Speech scrambling based on chaotic maps and one time pad," in *Proceedings - 2013 International Conference on Computer, Electrical and Electronics Engineering: "Research Makes a Difference", ICCEEE 2013*, Aug. 2013, pp. 128-133, doi: 10.1109/ICCEEE.2013.6633919.
- [10] M. K. M. Alazawi and J. Q. Kadhim, "Speech scrambling employing Lorenz fractional order chaotic system," *Journal of Engineering and Development*, vol. 17, no. 4, pp. 195-211, 2013.
- [11] S. N. A. -Saad and E. H. Hashim, "A speech scrambler algorithm based on chaotic system," *Al-Mustansiriyah Journal of Sciences*, vol. 24, no. 5, pp. 357-372, 2013.
- [12] A. Mostafa, N. F. Soliman, M. Abdallah, and F. E. Abd El-Samie, "Speech encryption using two dimensional chaotic maps," *2015 11th International Computer Engineering Conference: Today Information Society What's Next?, ICENCO 2015*, pp. 235-240, 2016, doi: 10.1109/ICENCO.2015.7416354.
- [13] A. Mahdi and S. S. Hreshee, "Design and implementation of voice encryption system using XOR based on Hénon map," in *Al-Sadiq International Conference on Multidisciplinary in IT and Communication Techniques Science and Applications, AIC-MITCSA 2016*, May 2016, pp. 82-86, doi: 10.1109/AIC-MITCSA.2016.7759915.
- [14] H. A. Ismael and S. B. Sadkhan, "Security enhancement of speech scrambling using triple Chaotic Maps," in *2017 Annual Conference on New Trends in Information and Communications Technology Applications, NTICT 2017*, Mar. 2017, pp. 132-137, doi: 10.1109/NTICT.2017.7976141.
- [15] K. Kordov, "A novel audio encryption algorithm with permutation-substitution architecture," *Electronics*, vol. 8, no. 5, pp. 1-15, May 2019, doi: 10.3390/electronics8050530.
- [16] A. M. Raheema, S. B. Sadkhan-Smieee, and S. M. A. Satar, "Performance enhancement of speech scrambling techniques based on many chaotic signals," *Proceedings of the 2020 International Conference on Computer Science and Software Engineering, CSASE 2020*, pp. 308-313, 2020, doi: 10.1109/CSASE48920.2020.9142062.
- [17] A. M. Raheema, S. B. Sadkhan, and S. M. Abdul Sattar, "Performance evaluation of voice encryption techniques based on modified chaotic systems," in *2020 6th International Engineering Conference "Sustainable Technology and Development" (IEC)*, Feb. 2020, pp. 135-140, doi: 10.1109/IEC49899.2020.9122933.
- [18] R. I. Abdelfatah, M. E. Nasr, and M. A. Alsharqawy, "Realization of audio encryption using elliptic curve," *CiiT International Journal of Digital Signal Processing*, vol. 13, no. 6, pp. 89-99, 2021.
- [19] M. S. Khoirom, D. S. Laihrakpam, and T. Tuithung, "Audio encryption using ameliorated ElGamal public key encryption over finite field," *Wireless Personal Communications*, vol. 117, no. 2, pp. 809-823, Mar. 2021, doi: 10.1007/s11277-020-07897-9.
- [20] M. Gupta, A. S. Kang, and V. Sharma, "Comparative study on implementation performance analysis of simulink models of cognitive radio based GFDM and UFMC techniques for 5G wireless communication," *Wireless Personal Communications*, vol. 126, no. 1, pp. 135-165, Sep. 2022, doi: 10.1007/s11277-020-07561-2.
- [21] N. Michailow *et al.*, "Generalized frequency division multiplexing for 5th generation cellular networks," *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3045-3061, Sep. 2014, doi: 10.1109/TCOMM.2014.2345566.
- [22] H. Shimodaira, J. Kim, and A. S. Sadri, "Enhanced next generation millimeter-wave multicarrier system with generalized frequency division multiplexing," *International Journal of Antennas and Propagation*, vol. 2016, pp. 1-11, 2016, doi: 10.1155/2016/9269567.
- [23] A. Kumar and M. Magarini, "Improved Nyquist pulse shaping filters for generalized frequency division multiplexing," in *2016 8th IEEE Latin-American Conference on Communications (LATINCOM)*, Nov. 2016, pp. 1-7, doi: 10.1109/LATINCOM.2016.7811588.
- [24] S. Wang, W. Li, and J. Lei, "Physical-layer encryption in massive MIMO systems with spatial modulation," *China Communications*, vol. 15, no. 10, pp. 159-171, Oct. 2018, doi: 10.1109/CC.2018.8485478.




- [25] B. Stoyanov and T. Ivanova, "Novel implementation of audio encryption using pseudorandom byte generator," *Applied Sciences*, vol. 11, no. 21, pp. 1-12, Oct. 2021, doi: 10.3390/app112110190.
- [26] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption using chaotic shift keying for secured speech communication," *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 20, pp. 1-12, Dec. 2017, doi: 10.1186/s13636-017-0118-0.
- [27] J. Gutierrez, "Attacking the linear congruential generator on elliptic curves via lattice techniques," *Cryptography and Communications*, vol. 14, no. 3, pp. 505-525, May 2022, doi: 10.1007/s12095-021-00535-6.
- [28] O. Reyad and Z. Kotulski, "On pseudo-random number generators using elliptic curves and chaotic systems," *Applied Mathematics and Information Sciences*, vol. 9, no. 1, pp. 31-38, Jan. 2015, doi: 10.12785/amis/090105.
- [29] H. K. Zghair, S. A. Mehdi, and S. B. Sadkhan, "Bifurcation of novel seven-dimension hyper chaotic system," *Journal of Physics: Conference Series*, vol. 1804, no. 1, pp. 1-13, Feb. 2021, doi: 10.1088/1742-6596/1804/1/012051.
- [30] H. K. Zghair, S. A. Mehdi, and S. B. Sadkhan, "Speech scrambler based on discrete cosine transform and novel seven-dimension hyper chaotic system," *Journal of Physics: Conference Series*, vol. 1804, pp. 1-14, Feb. 2021, doi: 10.1088/1742-6596/1804/1/012048.

BIOGRAPHIES OF AUTHORS



Mohammed Jabbar Mohammed Ameen    was born in Hillah-Iraq. He received a B.Sc. degree in Electrical Engineering from the University of Babylon in 2007 and M.Sc. degree in Communications Engineering from Al-Ahliyya Amman University in 2017, Jordan. He is working as a lecturer in the College of Engineering/Department of Electrical at Babylon University. He is currently working on his Ph.D. degree in Electrical Engineering. His research interests include IoT, massive MIMO, OFDM, GFDM, encryption and communication security, FEC, and 5G. He can be contacted at email: drmohammedalsalihy@gmail.com, mohammedalsalihy@uobabylon.edu.iq.



Prof. Dr. Saad S. Hreshee    was born in Baghdad, Iraq, in 1974. He received B.Sc. degree in Electrical Engineering from the Department of Electrical Engineering, College of Engineering, University of Babylon, Iraq, in 1997. He obtained M.Sc. in Electronic Engineering from the Department of Electrical and Electronic Engineering, University of Technology, Iraq, in 2000, while his Ph.D. in Electronic and Communication Engineering from the Department of Electrical Engineering, College of Engineering, University of Basrah, Iraq, in 2007. Since 2001, he has been with the staff of the Department of Electrical Engineering, College of Engineering, University of Babylon. His main research interests are antenna propagation, encryption, and communication security. He can be contacted at email: eng.saad.saffah@uobabylon.edu.iq.