Received: June 17, 2022. Revised: July 20, 2022.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Securing Physical Layer of 5G Wireless Network System over GFDM Using Linear Precoding Algorithm for Massive MIMO and Hyperchaotic QR-Decomposition

Mohammed Jabbar Mohammed Ameen[1]* Saad S. Hreshee[1]

[1]*Department of Electrical Engineering, Collage of Engineering, University of Babylon, Iraq*
* Corresponding author's Email: drmohammedalsalihy@gmail.com

Abstract: This paper introduces a novel voice encryption wireless system, which is based on characteristics of massive Multiple Input Multiple Output (MIMO) wireless channel. By exploiting the Minimum Mean Square Error (MMSE) precoding technique, channel fading values are permutated and substituted using various chaotic generators. The voice samples are mixed with channel values and a chaotic sequence before being transmitted. The proposed model was applied on a 5G network that included Generalized Frequency Division Multiplexing (GFDM), Parallel Spatial Modulation (PSM), and massive MIMO. Two chaotic sequences are generated, the first one used for the substitution stage by QR decomposition for the Henon map and then combining the outcome with Bernoulli and logistic maps to Q and R matrices, respectively. New chaotic signals are added to the real and imaginary parts of the MMSE precoding matrix. The second key is generated by the Tent map to perform the permutation stage for the overall precoding matrix. Several security metrics tests were used to verify effectiveness the of the proposed method resistance against attacks .The obtained tests results are: Signal to Noise Ratio (SNR=-23.1223), Root Mean Square (RMS=0.88565), Crest Factor (CF=10.6717), correlation coefficient (r_xy=0.000471), Linear Predictive Code Distance (dLPC=1.2758), Spectral Segment SNR (SSSNR=-27.6149), Cepstral Distance (dCD=9.4159), number of samples change rate (NSCR=33.334%), unified average changing intensity (UACI=99.9998%), keyspace=2500, key sensitivity, and speed=0.0329.The simulation results show that the proposed scheme has an excellent level of security and resistance to various forms of attacks, which outperforms many recent similar voice encryption methods.

Keywords: Audio encryption, Security analysis, Chaotic maps, Massive MIMO, 5G, PSM, GFDM, MMSE.

1. Introduction

With the rapid evolution of wireless communication networks, security flaws endanger data integrity and pose many challenges, prompting us to design new encryption algorithms to combat attacks. A set of security strategies for more complicated behavior has been developed to protect multimedia data such as text, audio, and image from hackers' dangers that can use various hacks at different levels in network systems [1]. Amongst modern communication's research & design topics, building a secure connection is one of the most important. Conventional cellular communication's security is primarily dependent on higher-layer encryption, while physical (lower) layer data has not been adequately protected. To strengthen security levels, both upper- and lower-layer encryption can be scrambled separately. Cryptography allows the two parties to communicate over a secure wireless channel, preventing the attacker from decrypting the original information. Chaos-based cryptography is implemented at the physical layer, which means that data is encrypted using chaos theory rules prior to transmission. The chaotic sequence properties enhanced this encryption, which is sensitive to initial conditions and parameters affects chaotic map settings. Unauthorized individuals who do not have the secret key will not be able to recover the received signal [2].

The open system interconnect (OSI) paradigm, as depicted in Fig. 1 gives a multilevel security

strategy for achieving private and secure in wireless communications technologies [3].

Audio communications is gaining big popularity in a variety of usages, including administrative and national defense domains. Security has become a serious concern in various fields as the requirement for digital technology has increased. Unauthorized parties cannot read, modify, and damage the original data because encryption safeguards it. Only a lawful recipient may reassemble the content of an audio signal because the quiet part of the communication is filled with noise signals [4].

Numerous governments are already launching fifth-generation (5G) wireless capabilities to be used in Internet of Things (IoT) technologies, including smart cities and self-driving cars. High-level technology such as massive MIMO, beamforming, and millimeter wave (mm wave) is used in the 5G network to provide benefits, including high speeds, low latency, and long battery life [5]. Furthermore, base station signal processing techniques such as precoding help to support 5G technologies. Precoding mixes the input signals in a predetermined fashion and distributes them to the numerous antenna elements in the proper way [6]. In fourth-generation (4G) communications, the orthogonal frequency division multiplexing (OFDM) scheme is the most widely utilized communication method. OFDM offers various advantages, including excellent multipath interference resistance, low inter-symbol interference (ISI), and simplicity of implementation. However, because rectangular pulse filters are used in OFDM, the sidelobes are large, resulting in strong out-of-band (OOB) radiation and a high peak-to-average power ratio (PAPR). OFDM is not suitable for 5G usages for the reasons stated above. To solve the limitations of OFDM in achieving all criteria, so GFDM is a viable waveform for 5G wireless technology. GFDM is a multicarrier modulation technique that uses non-rectangular pulse filters in transmission. By using these filters, it is possible to overcome the problems of high PAPR and OOB values. It is also a versatile scheme that can be tailored to specific uses. Finally, GFDM employs fewer cyclic prefixes (CP), helping to improve spectrum efficiency [5].

2. Literature review

Several algorithms for voice encryption based on chaos have been proposed in previous studies, but it has some shortcomings and limitations, such as inequity between encrypted and recovered voice, an increase value in correlation coefficient, an increased in encryption/decryption period, small key space, high computational processing, high residual intelligibility (R.I.), and slow processing speed. The highlights and evaluation of some literature reviews are as follows:

The authors in [7] suggested that voice encryption utilize XOR operation between input audio and Henon map by using Analog-to-Digital Converter (ADC), threshold, and comparator methods to convert Henon sequence into bits. The comparator method is the best to give more bits and hence more security level. This work presented a good d_{lpc} of about 4.336 and moderate d_{CD} to 7.097 but it has limiting in SSSNR to -4.2272 and low-key space reach to 2^{427}.

The authors in [8] introduced audio encryption algorithm by two-stage permutation. The first permutation is done using two logistic maps to permute the coefficients of Discrete Wavelet Transform (DWT). The second permutation stage is performed after inverse DWT by Arnold cat map. This work offered an appropriate value of d_{CD} reach

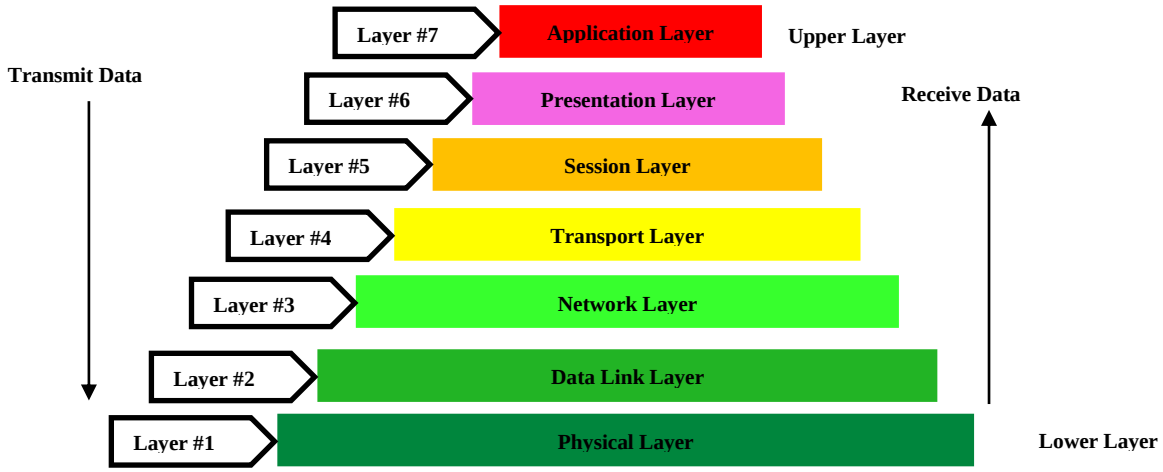

Figure. 1 Open system interconnect layout [3]

to 8.21462 but very low values in SNR at -2.61635 and SSSNR to -2.4587.

In [9], the researchers suggested a dual-channel voice encryption algorithm that uses a chaotic sequence with variable multi-scroll to produce key streams that confuse and diffuse voice data. The one-time keys, such as initial values of state variables, scroll numbers, and initial iteration times of the chaotic system, are dependent on both external keys and the hash value of the voice to increase the randomness of the chaotic trajectory. The system is characterized by a modest correlation coefficient at 0.004, low keyspace reaches 2^{268}, and no taking into account encryption/decryption time.

The authors in [10] introduced audio encryption using Chen, Lorenz, and Henon chaotic maps. Each of these maps is converted to the digital domain by an IEEE 754 converter before being combined using linear and nonlinear functions to provide the secret key needed to encrypt the clear audio. The highest confusion of the speech signal is caused by the use of three chaotic maps to construct the secret key. This work has key space=2^{480}, correlation coefficients = 0.38339 and SSSNR=-16.723 which can be considered as a low security level compared to our study.

The authors [11] in presented audio encryption algorithm using substitution and permutation principles. The audio samples were transformed using the discrete sine/cosine transform (DST/DCT). The 2D logistic and Henon maps used to substitute coefficients of DST/DCT, while, the Baker map performs permutation process. The cryptosystem was limiting in SNR to -3.025 and d_{lpc} to 0.7253.

In [12], a voice encryption system based on a combination of block cipher and chaotic maps was proposed. The cryptosystem divided the voice into blocks with size of 625 bytes and each of them passes through three stages: Permutation, XOR-Adding, and Substitution. The permutation is permuted using Tent map. Then the resulted block is XORed with the key block that generated by Chebyshev polynomial and the final stage is to substitute the block based on the multiplication inverse. This cryptosystem presented a good Correlation coefficient with a low keyspace 2^{319} and very slow speed of encryption reach to 10.4.

The authors in [13] introduced an audio encryption algorithm based on permutation-substitution by pseudo-random generators that generated using a combination of chaotic circle map and rotation equations. In this work, a good speed of encryption, but there is a limitation in keyspace = 2^{149}, SNR = -16.04 and correlation coefficient = 0.004794 that can consider an insufficient security level.

According to the literature mentioned above, there is a perception that there is a lack of a comprehensive solution to overcome the drawbacks of previous systems. Therefore, a powerful audio encryption technique that is suited for the needs of 5G wireless technology should be investigated to achieve a high level of security and high speed while maintaining the excellent audio quality of the decrypted audio signals.

3. Work contributions

The work findings are presented as:

- Enhance security of massive MIMO -PSM-GFDM wireless system from hackers.
- A new pseudorandom number generator (PRNG) was proposed named Hyperchaotic QR Decomposition pseudorandom number generator (HQRPRNG) using QR-decomposition for the Henon map and then combining Bernoulli and logistic maps to Q and R port, respectively.
- The Minimum Mean Square Error (MMSE) precoding matrix is substituted and permuted using chaotic secret keys. The substitution was performed using the HQRRPNG sequence, while the permutation process was done using the tent map.
- The suggested system has many advantages, including excellent chaotic properties, a large keyspace, low calculation cost, fast processing, high signal recovered quality, and low R.I.

4. Key technologies of 5G networks

4.1 Point to point (P2P) massive MIMO link

In this system configuration, each (Nt) transmitter antenna will only connect with one (Nr) receiving antenna, where $Nr \leq Nt$. To enhance the data rate without increasing the bandwidth, the transmitter and receiver base station is equipped with a large number of antennas.

In most P2P systems, frequency-flat and slow-fading channels are considered [14]. As shown in Fig. 2, a massive MIMO downlink (DL) system model is illustrated. According to channel reciprocity in the time division duplexing (TDD) mode, downlink (DL) transmission has the same channel matrix fading (H) as uplink (UL) transmission in the channel coherence time. The channel matrix $H \in C^{Nr \times Nt}$ can be written as:

$$H = \begin{bmatrix} h_{1,1} & \cdots & h_{1,Nr} \\ \vdots & \ddots & \vdots \\ h_{1,Nt} & \cdots & h_{Nr,Nt} \end{bmatrix} \quad (1)$$

An M-ary constellation modulates the arriving bitstream, which is subsequently processed through a precoding process at the transmitter. After precoding and reshaping into vectors, the transmitter antennas send as $x = [x_1, x_2, \ldots, x_{Nt}]^T$, x $\in$ $c^{Nt\times 1}$,to the Nr-received side via wireless channel. The received vector $y = [y_1, y_2, \ldots, y_{Nr}]^T$, y $\in$ $c^{Nr\times 1}$,which is impacted by channel fading and additive white Gaussian noise (AWGN) which can be depicted by:

$$y = Hx + n \quad (2)$$

where n is AWGN, n ∈ C $^{Nr\times 1}$, Equation (1) is made up entirely of complexed normal distributions.

The precoding technique converts the complex processing of the system from the receiver side to the transmitter by employing powerful signal processing algorithms at the base station, which is one of the major principles in massive MIMO systems. In an actual wireless transmission scenario, obtaining a reliable channel-state-information (CSI) is generally difficult, as the efficiency of DL transmission is heavily reliant on it. Precoding technology can be used to deal with CSI that isn't imperfect. The MMSE algorithm is used to minimize the error filtering between the sent symbols from the BS and the receiving side by employing the mean square error procedure in the signal. The formula for the MMSE precoding matrix is:

$$P_{MMSE} = \sqrt{\beta}\, H^*(\lambda I_{Nr} + H^T H^*)^{-1} \quad (3)$$

where β is a scaling power factor, λ is the noise variance, and I_{Nr} is the identity matrix [15].

4.2 Parallel spatial modulation (PSM)

PSM functioning concept can be summed up in the following stages [16]:

I. The set of antennae at the transmitter is split into P equal subsets, each having g=Nt/P size, where each set has $2 \leq g \leq N_t$, and a single antenna is activated in each subset.

II. The data to be transmitted are separated into (P+1) subsets of bits, the first portion comprising of $\log_2 M$ bits and the remaining portions comprising of $\log_2 P$ bits, as shown in Fig. 3.

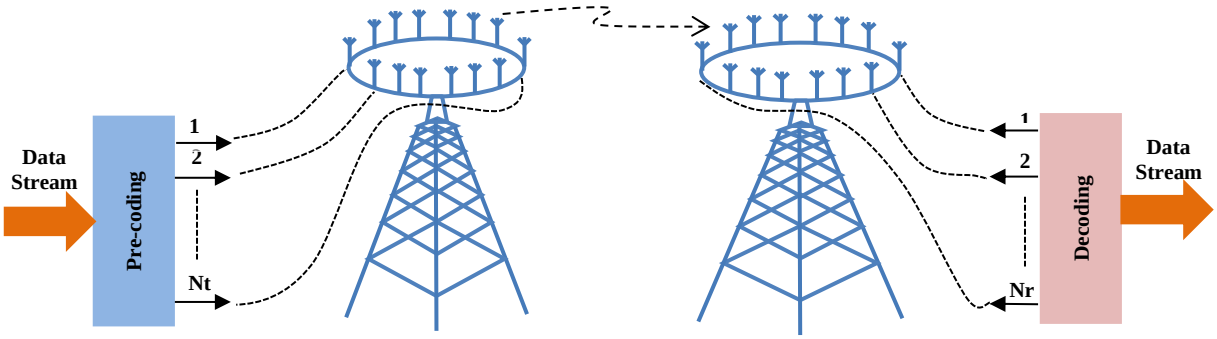

Figure. 2 Basic model of P2P-DL massive MIMO link [14]

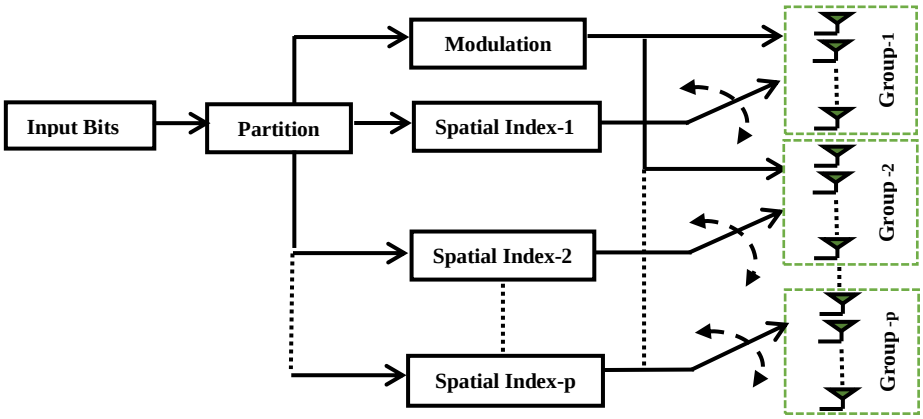

Figure. 3 The block diagram of PSM [16]

III. The first subset ($\log_2 M$ bits) is modulated and then spatial modulation is applied to the reminding subsets ($\mathrm{P}\log_2 P$ bits) independently with same signal constellation.

IV. The spectrum efficiency of the PSM technique in bps/Hz can be expressed as follows:

$$\boldsymbol{\eta = P \times log_2(g) + log_2(M)} \tag{4}$$

4.3 GFDM modulation

The GFDM waveform is a preferred modulation for multi-carrier designs and considered non-orthogonal scheme because of samples distribution method. As a result, GFDM modulation is performed on discrete time-frequency blocks, which includes a group of subcarriers and subsymbols in the frequency and time domains, respectively. The subcarriers are filtered using prototype filters by circularly shifting in both time and frequency domains. This strategy will remove unnecessary OOB radiation and flatten the road for a successful spectrum distribution. Accordingly, GFDM scheme can represent a promising technique for 5G wireless communication systems due to its features and flexibility. The CP and filtering used minimize intercarrier (ICI) and intersymbol interference (ISI) [17]. In GFDM, a one CP is used for the entire block, while, a single CP is employed for each subsymbol in OFDM. Also, the peak-to-average power ratio (PAPR) of OFDM is particularly high, and it can be lowered by increasing the bandwidth of the subcarrier and reducing the number of subcarriers. In case of designing the GFDM and OFDM with same block length, the number of subcarriers become fewer, resulting minimize in PAPR in the GFDM waveform [18]. Fig. 4, illustrates the GFDM time-frequency resources configuration, where K and M represent the number of subcarriers and subsymbols, respectively. Each resource block contains KM sample locations. Furthermore, if KM=N is satisfied, the amount of data transmitted by GFDM is equal to the amount of data transmitted by OFDM over the same symbol time and bandwidth. The location of each resource block is determined using a pulse-shaping filter. The GFDM signal is expressed as follow:

$$\left.\begin{aligned} \boldsymbol{X[n]} &= \sum_{k=0}^{K-1}\sum_{m=0}^{M-1}\left(\boldsymbol{d_{k,m}\delta[n-mk]}\right) \\ &\qquad * \boldsymbol{g[n \bmod N]e^{j2\pi\frac{nk}{K}}} \\ \boldsymbol{X[n]} &= \sum_{k=0}^{K-1}\sum_{m=0}^{M-1}\boldsymbol{d_{k,m} * \tilde{g}[n-mk]e^{j2\pi\frac{nk}{K}}} \\ \boldsymbol{X[n]} &= \sum_{m=0}^{M-1}\boldsymbol{\tilde{g}[n-mk]}\underbrace{\sum_{k=0}^{K-1}\boldsymbol{d_{k,m}e^{j2\pi\frac{nk}{K}}}}_{\boldsymbol{IDFT}} \end{aligned}\right\} \tag{5}$$

Here, (*) is used to describe the convolution operations. In Eq. (5) above, $\boldsymbol{\tilde{g}[n-mk]} \triangleq \boldsymbol{g[(n-mk) \bmod N]}$ is the pulse shaping filter with mK time-shifting and the MOD factor is equal to the tailbiting method that constructs a circular

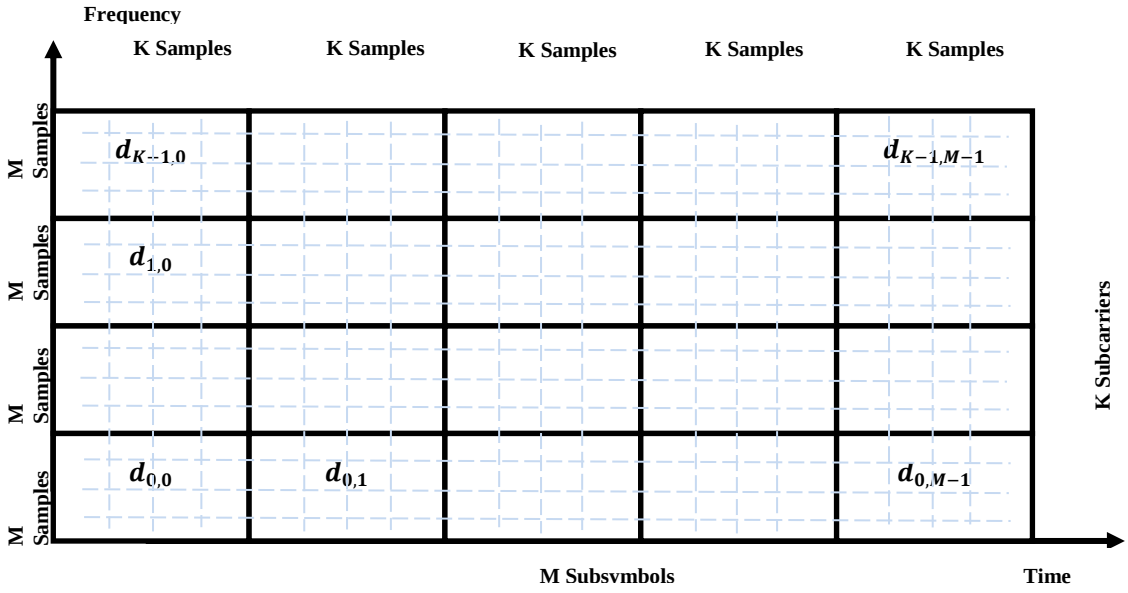

Figure. 4 GFDM symbol mapping structure

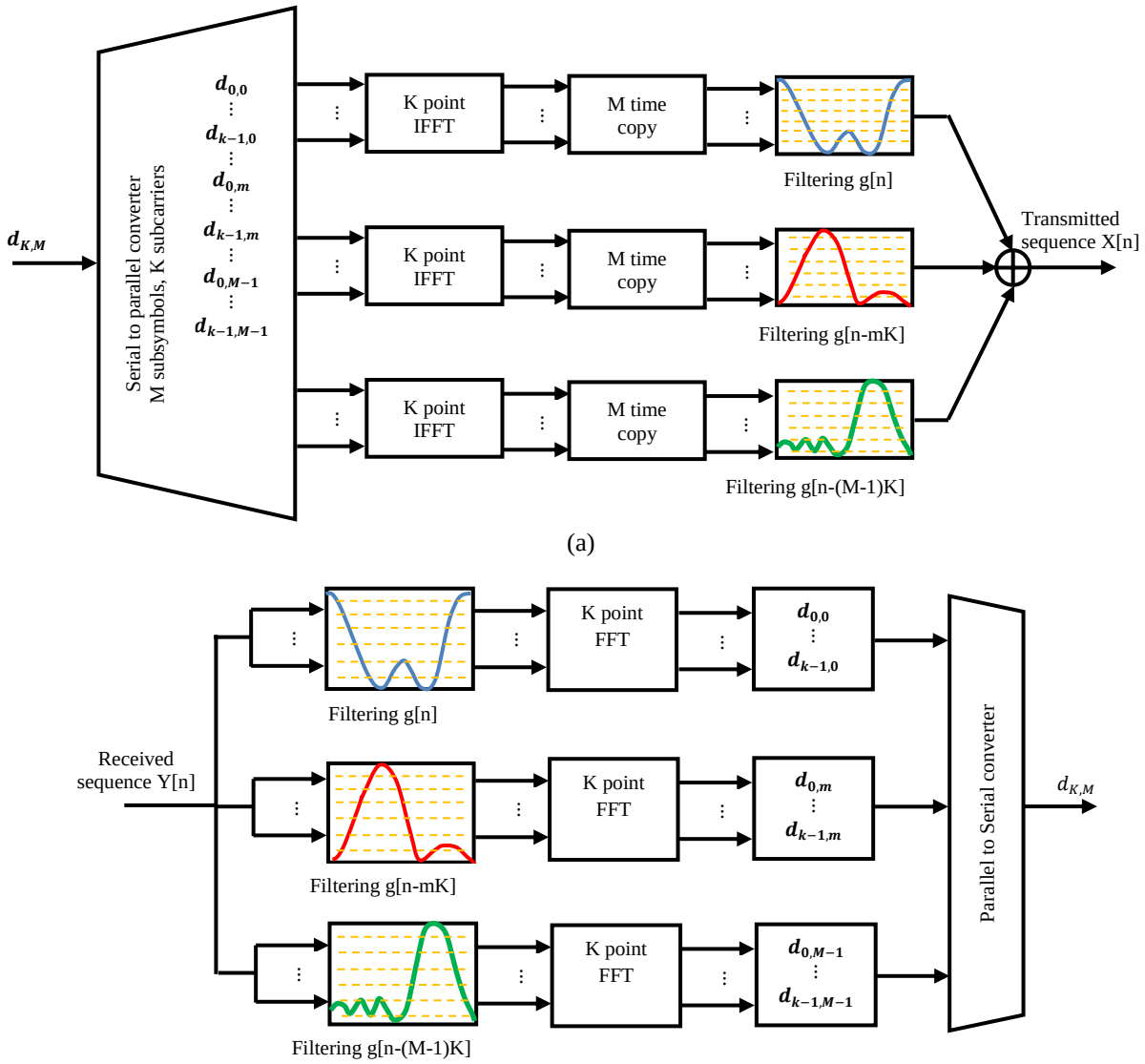

Figure. 5 GFDM scheme structure [19]: (a) GFDM modulator and (b) GFDM demodulator

convolution filter. The GFDM modulator and demodulator are as described in Fig. 5. Finally, Eq. (5) can converted to OFDM waveform when M = 1 and rectangular pulse shaping filter is used ,also, it is equal to the single-carrier transmission in the case of K = 1 [19].

5. Introductory chaos theory-based cryptography

Wireless networking security based on chaos theory is an approach that tries to provide protection, secure wireless communications, and is capable of providing confidentiality. Also, modern cryptography to security solutions is focused on the behavior of non-linearity systems. Chaos signals have a deterministic, nonlinear, irregular, long-term prediction, and sensitivity to initial conditions, which are all attractive properties. Audio encryption has become more important in wireless communication due to the high volume of sensitive voice information passing across open telecommunication networks. The behavior of chaotic maps varies quickly when a slight modification in the control parameter and/or initial condition (Which represents secret keys) happens [20]. Table 1 summarizes well-known discrete chaotic maps, which will be employed in this paper.

6. The proposed PRNG based on QR decomposition

The non-linear behavior of one-dimension chaotic maps is less. Therefore, it can be improved by increasing the number of dimensions of the chaotic map. This paper proposed a new two chaotic map using the QR decomposition technique of one chaotic map.

Let Xh_{n+1} be a Henon signal was reshaped to matrix Z_{n+1}, $Z_{n+1} \in C^{w \times w}$, $w \geq MK$, where K and M denote the numbers of subcarriers and subsymbols of GFDM modulation, respectively. Then factorization process is taken to matrix Z_{n+1} with linear independent columns is decomposed to give an orthogonal matrix Q, an upper triangular matrix R, as in equation below:

$$\boldsymbol{Z_{n+1} = Q_{n+1} \times R_{n+1}} \quad (6)$$

Then after convert Q_{n+1} *and* R_{n+1} to vector again, combining it with Bernoulli and Logistic maps respectively, as in equations:

$$\boldsymbol{Q_{Chaotic} = Xb_{n+1} + Q_{n+1}} \quad (7)$$

$$\boldsymbol{R_{Chaotic} = Xl_{n+1} + R_{n+1}} \quad (8)$$

The schematic diagram of new PRBG sequence is shown in Fig. 6. It's clear that two PRNG was construct using triple chaotic maps mixed together using QR factorization, called Hyperchaotic QR Decomposition (HQRPRNG).

7. The proposed audio encryption system based on the MMSE precoding matrix technique

In this part of the work, a novel approach to protect audio will be formulated based on HQRPRBG sequence to substitute and permute the precoding matrix at the base station. The proposed audio transmission system comprisis of massive MIMO, PSM, and GFDM, the details of each part are illustrated in Table 2 and Fig. 7. There are own series for each chaotic map and it is known in both sender and receiver.At the transmitter side,the original audio is sampled with a frequency of 8 kHz and saved as WAV audio format and (double) data type, resulting in a cryptosystem with an excellent security level and low R.I.

The algorithm of transmitter side for the proposed audio encryption can summarized in the following steps:

Step1: Segmentation and reshape the input audio into a 2-D block:

1. Read audio signal .wav.
2. Sample rate =8 KHz.
3. Samples per audio channel=16.

Table 1. Chaotic maps generator

Chaotic Maps	Time domain	Equations	Number of space Dimensions	Parameter values and Initial condition
Henon [21]	Discrete	$\boldsymbol{Xh_{n+1} = 1 + Y_n - a_h Xh_n^2}$ $\boldsymbol{Yh_{n+1} = b_h Yh_n}$	2	a_h = 1.4, b_h = 0.3 and Xh (0)= Yh (0)=0
Logistic [21]	Discrete	$\boldsymbol{Xl_{n+1} = rXl_n(1 - Xl_n)}$	1	3.57≤ r ≤4 and 0.5< xl(0) <1
Bernoulli [22]	Discrete	$\boldsymbol{Xb_{n+1} = \begin{cases} 2\mu Xb_n, & 0 \leq X_n < 0.5 \\ 2\mu(1 - Xb_n), & 0.5 \leq X_n < 1 \end{cases}}$	1	$X_b(0) \in [0 - 1]$ $\mu_b \in [0 - 1]$
Tent [23]	Discrete	$\boldsymbol{X_{n+1} = \begin{cases} \mu X_n, & X_n < 0.5 \\ \mu(1 - X_n), & X_n \geq 0.5 \end{cases}}$	1	$X_n(0) = 0.4$ $\mu = 1.9$

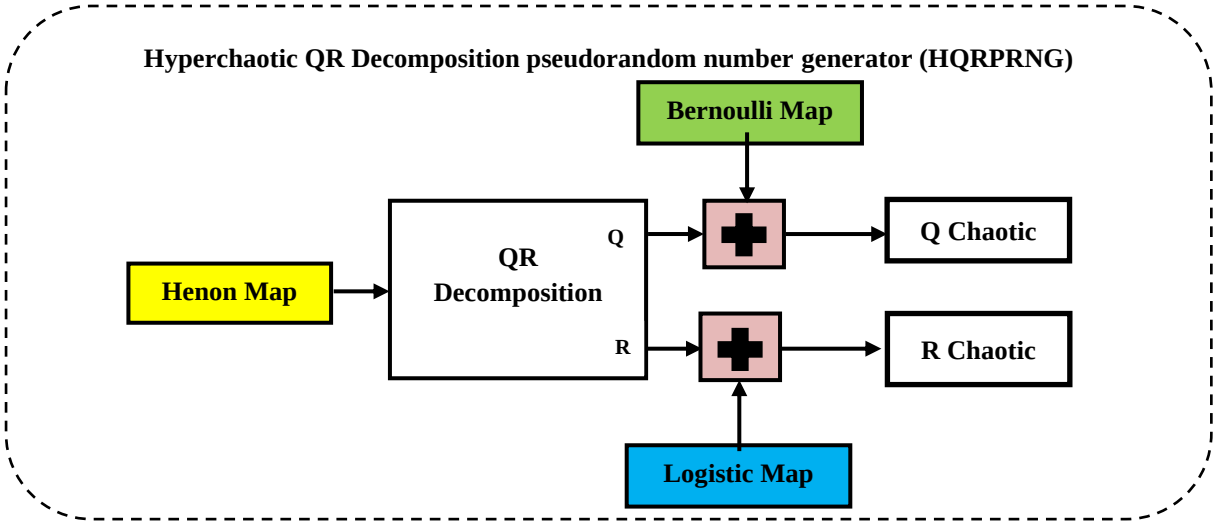

Figure. 6 The block diagram of HQRPRBG sequence

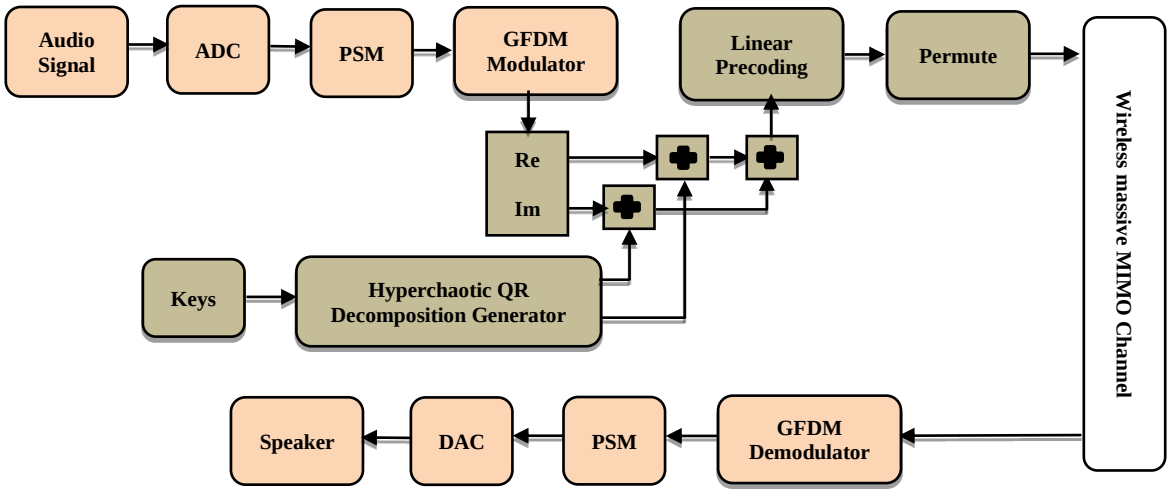

Figure. 7 Encryption block diagram of the proposed system

Table 2. Simulation parameters

Scheme	Parameter	Value
GFDM parameters	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
Massive MIMO	Number of transmit antennas (N_t)	80
	Number of Receive antennas (N_r)	80
	Channel Fading	Rayleigh
PSM	Number of group (p)	5
	Group size (g)	16

4. Convert audio to binary form using ADC.
5. divides bits into 24 bits per frame

Step2: PSM procedure

1. Divide the incoming bits from **Step1** into subframes with 4 bits
2. apply the 4:16 line decoder
3. Apply 16-QAM

Step3: GFDM modulator procedure

1. The incoming data are divided into five subsymbols, and each subsymbol has sixteen subcarriers.
2. Apply IDFT and filtering
3. Add cyclic prefix.
4. Reshape into a 2-D block.

Step4: HQRPRBG generation

1. Generate key1 sequence using Henon map.
2. Generate key2 sequence using the Bernoulli map.
3. Generate key3 sequence using Logistic map
4. Generate key4 sequence using Tent map
5. key1 is convert into a 2-D block and factorize to Q, R matrices.
6. Reshape Q and R to vector
7. Add Q to key2 and add R to key3 to produce $Q_{chaotic}$ and $R_{chaotic}$ respectively.

Step5: Encryption procedure within precoding matrix

1. The incoming symbols from GFDM modulator Separate into the real and imaginary values.
2. Add $Q_{chaotic}$ to real part and add $R_{chaotic}$ imaginary part to form new complex vector.
3. Multiply complex vector from **Step5-2** by MMSE precoding matrix.
4. Permute new precoding matrix using key4.

Step6: 80 antennas send data via a wireless channel.

The decryption method is very similar to that of encryption. The original audio can be recovered by executing the inverse process on the encrypted audio.

8. Security metrics

In order to be resistant to all eavesdropping processes, the encryption algorithm must be powerful in protecting multimedia types broadcasted on the public wireless channel. R.I. is a useful metric for evaluating and determining the security requirement of a system. When the R.I. of the audio is low, it indicates that the audio is unclear (more security) [20]. R.I of the proposed algorithm was assessed based on the following tests:

8.1 Signal to noise ratio (SNR)

Simply, SNR is estimate as follow:

$$\boldsymbol{SNR = 10\, log_{10} \frac{\sum_{i=1}^{N} x_i^2}{\sum_{i=1}^{N} (x_i - y_i)^2}} \quad (9)$$

Where x_i, y_i are original and encrypted audio sample respectively.

8.2 Root mean square (RMS) and crest factor (CF) tests

The average amplitude of audio determines the RMS value, which is calculated as follows:

$$\boldsymbol{RMS} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}|A_i|^2} \tag{10}$$

CF can be defined as the ratio between the peak and effective values of audio, CF is estimated by the following:

$$\boldsymbol{CF} = \mathbf{20}\log_{10}\frac{|V_{peak}|}{V_{RMS}} \tag{11}$$

8.3 Correlation analysis

The correlation coefficient (r_{xy}) is a proper metric for measuring the strength of a cryptographic against various attacks. It calculates the correlation between similar segments of the original and encrypted audio. An effective audio encryption algorithm changes audio into a noisy signal with a low r_{xy} difference between the original and encrypted audio. The following formula can be used to calculate r_{xy}:

$$\boldsymbol{r_{xy}} = \frac{\boldsymbol{cov(x,y)}}{\boldsymbol{\sigma_x\sigma_y}} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y))}{\sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2}\sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i-E(y))^2}} \tag{12}$$

$$\boldsymbol{d_{LPC}} = \boldsymbol{ln}\left(\frac{cVc^T}{dVd^T}\right) \tag{13}$$

$$\boldsymbol{SSSNR} = \mathbf{10}\,\boldsymbol{log}\left[\frac{\sum_{i=0}^{\frac{N}{2}-1}|x_i|^2}{\sum_{i=0}^{\frac{N}{2}-1}(|x_i|-|y_i|)^2}\right] \tag{14}$$

Where, N : audio samples, x_i and y_i :clear and encrypted audio samples, $E(x)$ and $E(y)$: clear and encrypted audio expected value, $\sigma_x, \sigma_y \neq 0$: represent clear and encrypted audio standard deviation, and $cov(x, y)$ is the covariance between two audios [21].

8.4 Linear predictive code distance (dLPC)

The d_{Lpc} can be written as follows:

Where $c = [1, c_1, c_2, \cdots, c_p]$ is the LPC coefficients estimated from clean voice, $d = [1, d_1, d_2, \cdots, d_p]$ is the LPC coefficients calculated from distorted voice, V=V(i,j) , i1, j = 0, 1, … . , p, is the autocorrelation matrix computed from distorted audio, and p represent the filter order.

8.5 Spectral segment SNR (SSSNR)

The SSSNR is briefing as:

Where $\boldsymbol{x_i}$ and $\boldsymbol{y_i}$ are DFT of clean (original) and encrypted (distorted) voice samples.

8.6 Cpestral distance (dCD)

The d_{CD} is abbreviated as:

$$\boldsymbol{d_{CD}} = \mathbf{10}\,\boldsymbol{log}\sqrt{\mathbf{2}\sum_{i=1}^{p}(\boldsymbol{CC_x(i)} - \boldsymbol{CC_y(i)})^2} \tag{15}$$

Where $CC_x(i)$ and $CC_y(i)$ are the Cpestral coefficient of clear and distorted voice samples [7].

8.7 UACI and NSCR analysis

The ability to withstand a variety of threats is a key measure of encryption effectiveness. The least significant bit of the sample is inverted to create modified audio to evaluate this amount of resistance. The clear and altered audios are both encrypted using the same secret key, resulting in two encrypted audios. The encrypted audio signals are then compared using the number of samples change rate (NSCR) and the unified average changing intensity (UACI):

$$\boldsymbol{NSCR} = \sum_i \frac{\boldsymbol{P_i}}{\boldsymbol{N}} \times \mathbf{100}\%\,,$$
$$\boldsymbol{P_i} = \begin{cases} \mathbf{1}, \boldsymbol{X_i \neq X_i'} \\ \mathbf{0}, \boldsymbol{otherwise} \end{cases} \tag{16}$$

$$\boldsymbol{UACI} = \frac{1}{N}\left[\sum_i \frac{|X_i - X_i'|}{65535}\right] \tag{17}$$

Where X and X' represent the encrypted audio and modified version which has a difference in one sample between them. N indicates the number of samples in audio. The typical values of NSCR and UACI are 100 % and 33.3 %[24].

9. Experimental results

9.1 Key space and sensitivity analysis

Keyspace and key sensitivity are two important variables that determine the voice encryption efficiency of the system. Keyspace refers to the collection of secret keys used during the voice encryption process. When there is a small variation

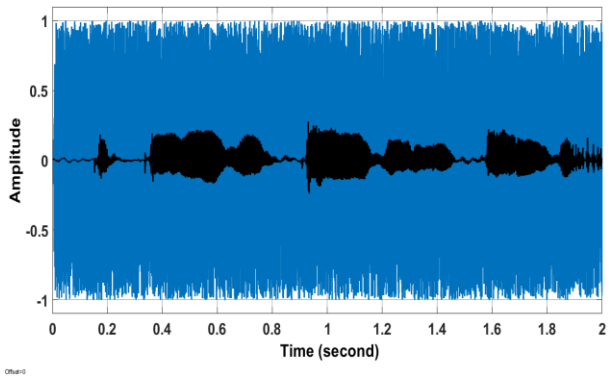

Figure. 8 Audio encryption waveforms results of audio-1

Table 3. Key space of chaotic maps

Chaotic Maps	Number of Control Parameter	Number of Initial conditions	Key space
Bernoulli	1	1	$(10^{15})^2 \approx 2^{100}$
Logistic	1	1	$(10^{15})^2 \approx 2^{100}$
Henon	2	2	$(10^{15})^4 \approx 2^{200}$
Tent	1	1	$(10^{15})^2 \approx 2^{100}$

in the encryption key, the sensitivity of the key indicates that decoding the voice is impossible. Audio encryption with a large keyspace and great sensitivity is required to be a secure system against attacks. Table 3 lists the key Space of each chaotic map used in the proposed system.

If the calculation accuracy of Matlab R2020a is approximately (10^{-15}), this implies that every secret key's available options are ($10^{15} \approx 2^{50}$), then the total keys space of the currently proposed system has ten secret keys $(2^{50})^{10} = 2^{500}$. A slight changeover to one of the keys is performed throughout implementation to test the sensitivity of the proposed system key, while the rest of the parameters stay unaltered [25]. The percentage of Difference (P. Diff.) is used to measure the sensitivity of the key in addition to SNR, RMS, CF, r_{xy}, d_{lpc} , SSSNR, and d_{CD} are illustrated in Table 4. When measured values RMS, CF, d_{lpc} , and d_{CD} are high that means the proposed system has high key sensitivity ,while ,when

Table 5. Time analysis

Audio file	Duration (Sec.)	Size (KB)	Total Time (Sec.)	Speed (Sec./KB)
Audio-1	2	32.0 KB	1.0540	0.0329
Audio-2	3	48.0 KB	1.67	0.0348

Table 6. UACI and NSCR measurements

Audio file	Duration (Sec.)	UACI	NSCR
Audio-1	2	33.3355%	99.9993%
Audio-2	3	33.334%	99.9998%

r_{xy},SNR,SSSNR have low values , this means high key sensitivity. The proposed system's secret keys are: a_h, b_h, $X_h(0)$, $Y_h(0)$, r, $X_l(0)$, $X_b(0)$, μ_b, $X_t(0)$, μ_t When statistical analysis of the proposed model is performed, the following criteria must be taken into account:

• When low SNR, SSSNR, and r_{xy} values are obtained, indicating that the security level has enhanced.

• When increasing the value of d_{CD}, RMS, d_{LPC} and CF, means that the security level has improved.

9.2 Time analysis

The speed with which a robust encryption technique executes is another important criterion. The encryption/decryption period is the amount of time it takes for the encryption/decryption technique to finish its procedure. This time is related to the audio length [24, 26, 27].The suggested algorithm has been implemented in Matlab R2020a under Windows 10 Pro. on a computer with an Intel(R) Core (TM) i7-7500U @ 2.70 GHz 2.9 GHz, 8 GB RAM, and a 64-bit operating system. The computational time can be described in Table 5 by using two audio files. Fig. 8 shows the audio waveform. The method effectively converts the original audio to noise-like encrypted audio.

Table 4. Key sensitivity test of the proposed model using audio-1 with duration 2 second

Map	Change key	d_{CD}	r_{xy}	d_{LPC}	SSSNR	SNR	RMS	CF	P. Diff.
Henon	a_h +10^{-8}	9.3504	-0.0027	1.256	-24.114	-19.735	0.59793	4.4664	100%
	b_h+10^{-8}	9.3863	-0.0136	1.2417	-24.160	-19.800	0.60183	4.4664	100%
	$X_h(0) + 10^{-8}$	9.4159	-0.0073	1.2529	-24.117	-19.746	0.59843	4.4582	100%
	$Y_h(0) + 10^{-8}$	9.3027	-0.015	1.2758	-24.104	-19.741	0.59843	4.4702	100%
Logistic	r+10^{-8}	8.9206	-0.0015	1.2379	-27.608	-23.113	0.8848	1.0329	100%
	$X_l(0) + 10^{-8}$	8.831	-0.0034	1.2601	-27.614	-23.122	0.88565	1.0229	100%
Bernoulli	X_b (0) +10^{-8}	9.3544	0.00335	1.2653	-17.700	-13.684	0.29334	10.652	100%
	μ_b+10^{-8}	9.3493	0.00047	1.2744	-17.680	-13.666	0.29254	10.6717	100%
Tent	X_t (0) +10^{-8}	9.3944	-0.0022	1.2505	-24.022	-19.646	0.59249	4.561	100%
	μ_t+10^{-8}	9.3871	-0.0021	1.261	-24.392	-19.71	0.6039	4.561	100%

Table 7. Comparisons with pervious work

Ref. / Tests	[7]	[8]	[9]	[10]	[11]	[12]	[13]	**Ours**
Keyspace	2^{427}	-	2^{268}	2^{480}	-	2^{319}	2^{149}	2^{500}
SNR	-	-2.61635	-	-	-3.025	-	-16.04	-23.1223
SSSNR	-4.2272	-2.4587	-	-16.723	-3.04	-	-	-27.6149
P. Diff	-		-	99.14%	-	-	-	100%
UACI	-		-	-	-	-	-	33.334%
NSCR	-		-	-	-	-	99.99%	99.9998%
d_{CD}	7.097	8.21462	-	7.2274	-	-	-	9.4159
Speed	-	-	-	-	-	10.4	0.003	0.0329
r_{xy}	-	-	0.004	0.38339	-	-0.00462	−0.004794	0.000471
d_{LPC}	4.336	-	-	-	0.7253	-	-	1.2758

10. Comparative study

In order to evaluate the weakness and strongness points of the proposed cryptosystem, the suggested technique's features will be compared to those of existing competing systems. The most widely utilized security criterion was applied, including SNR, RMS, CF, r_{xy}, d_{LPC}, SSSNR, d_{CD}, NSCR, UACI, keyspace, key sensitivity, P. Diff. and speed. This comparison with different algorithms is shown in Table 7. The results show that the suggested cryptosystem has the lowest value of r_{xy}. It is also evident that, the suggested cryptosystem has the largest key space from all the others, with a value of 2^{500}. The proposed cryptosystem exhibits the most negative SNR and SSSNR values of the previous approaches. Furthermore, the proposed cryptosystem has the highest values of UACI, NSCR, d_{CD}, RMS, and d_{LPC}, among other techniques, so it has the strongest resistance against brute-force attacks.

11. Conclusions

A new voice cryptosystem against hackers was designed through the utilization of three chaotic maps to construct an HQRPRNG sequence. HQRPRNG can be obtained by applying QR-factorization for the Henon map and then adding Bernoulli and logistic maps to Q and R output respectively in order to protect audio broadcast over a massive MIMO-GFDM system. The HQRPRNG sequence performs a substitution process inside the MMSE precoding matrix while the Tent map performs a permutation process. The results demonstrate that the lowest values obtained of SNR is -23.1223 and SSSNR is -27.6149 which means a high level of noise in encrypted voice. The correlation coefficient r_{xy} reaches 0.000471, UACI about 33.334%, and NSCR about 99.9998%, these values indicate that the audio samples are completely different from the corresponding samples, as well as the high quality of the encryption. The key space value is 2^{500} which shows that the necessary level of security against brute-force attacks and key sensitivity analysis shows that even any tiny change of the chaotic parameters and initial condition leads to unsuccessful voice decryption. In addition to the other results obtained, we are able to draw the conclusion that the proposed approach is safe and secure for wireless audio transmission.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper conceptualization, methodology, software, validation, ,formal analysis, resources, data curation, , writing—original draft preparation, writing—review and editing, visualization, supervision, project administration and funding have been done by 1st and 2nd authors.

Reference

[1] K. A. Korba, D. Abed, and M. Fezari, “Securing physical layer using new chaotic parametric maps”, *Multimedia Tools and Applications*, Vol. 80, No. 21, pp. 32595-32613, 2021.

[2] K. Sakoda, H. Hata, and S. Hata, “Chaotic Encryption for Belief Propagation Decoding in Massive MIMO Systems”, *Journal of Communications Technology and Electronics*, Vol. 65, No. 2, pp. 172-178, 2020.

[3] S. Komeylian and S. Komeylian, “Deploying an OFDM physical layer security with high rate data for 5G wireless networks”, In: *Proc. of 2020 IEEE Canadian Conference on Electrical and Computer Engineering*, pp. 1-7, 2020.

[4] F. Farsana and K. Gopakumar, "A novel approach for speech encryption: Zaslavsky map as pseudo random number generator", *Procedia Computer Science*, Vol. 93, pp. 816-823, 2016.

[5] 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, 2022.

[6] D. Subitha and R. Vani, "Analysis of linear precoding techniques for massive MIMO-OFDM systems under various scenarios", In: *Proc. of IOP Conference Series: Materials Science and Engineering*, Vol. 1084, No. 1: IOP Publishing, p. 012053, 2021.

[7] A. Mahdi and S. S. Hreshee, "Design and implementation of voice encryption system using XOR based on Hénon map", In: *Proc. of 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications*, pp. 1-5, 2016.

[8] S. N. A. Saad and E. H. Hashim, "A speech scrambler algorithm based on chaotic system", *Al-Mustansiriyah J. Sci*, Vol. 24, No. 5, pp. 357-372, 2013.

[9] H. Liu, A. Kadir, and Y. Li, "Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys", *Optik*, Vol. 127, No. 19, pp. 7431-7438, 2016.

[10] H. A. Ismael and S. B. Sadkhan, "Security enhancement of speech scrambling using triple Chaotic Maps", In: *Proc. of 2017 Annual Conference on New Trends in Information & Communications Technology Applications*, pp. 132-137, 2017.

[11] A. Mostafa, N. F. Soliman, M. Abdalluh, and F. E. A. El-samie, "Speech encryption using two dimensional chaotic maps", In: *Proc. of 2015 11th International Computer Engineering Conference*, pp. 235-240, 2015.

[12] E. A. Albahrani, "A new audio encryption algorithm based on chaotic block cipher", In: *Proc. of 2017 Annual Conference on New Trends in Information & Communications Technology Applications*, pp. 22-27, 2017.

[13] K. Kordov, "A novel audio encryption algorithm with permutation-substitution architecture", *Electronics*, Vol. 8, No. 5, p. 530, 2019.

[14] N. Hassan and X. Fernando, "Massive MIMO wireless networks: An overview", *Electronics*, Vol. 6, No. 3, p. 63, 2017.

[15] M. A. Albreem, A. H. A. Habbash, A. M. A. Hudrouss, and S. S. Ikki, "Overview of precoding techniques for massive MIMO", *IEEE Access*, Vol. 9, pp. 60764-60801, 2021.

[16] M. Mohaisen, "Constellation design and performance analysis of the parallel spatial modulation", *International Journal of Communication Systems*, Vol. 32, No. 18, p. e4165, 2019.

[17] 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*, pp. 1-31, 2020.

[18] N. Michailow, "Generalized frequency division multiplexing for 5th generation cellular networks", *IEEE Transactions on Communications*, Vol. 62, No. 9, pp. 3045-3061, 2014.

[19] 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, 2016.

[20] S. B. Sadkhan and R. S. Mohammed, "Proposed random unified chaotic map as PRBG for voice encryption in wireless communication", *Procedia Computer Science*, Vol. 65, pp. 314-323, 2015.

[21] R. I. Abdelfatah, "Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic DNA computations", *IEEE Access*, Vol. 8, pp. 69894-69907, 2020.

[22] R. F. M. González, J. A. D. Méndez, L. P. Luengas, J. L. Hernández, and R. V. Medina, "A steganographic method using Bernoulli's chaotic maps", *Computers & Electrical Engineering*, Vol. 54, pp. 435-449, 2016.

[23] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption using chaotic shift keying for secured speech communication", *EURASIP Journal on Audio, Speech, and Music Processing*, Vol. 2017, No. 1, pp. 1-11, 2017.

[24] J. B. Lima and E. F. D. S. Neto, "Audio encryption based on the cosine number transform", *Multimedia Tools and Applications*, Vol. 75, No. 14, pp. 8403-8418, 2016.

[25] H. K. Zghair, S. A. Mehdi, and S. B. Sadkhan, "Speech scrambler based on discrete cosine transform and novel seven-dimension hyper chaotic system", In: *Proc. of Journal of*

Physics: Conference Series, Vol. 1804, No. 1: IOP Publishing, p. 012048, 2021.

[26] M. J. Blakit and Y. Eljaafreh, "Performance analysis of QOSTBC-OFDM system based on FEC codes", *Advances in Natural and Applied Sciences*, Vol. 10, No. 17, pp. 81-89, 2016.

[27] M. J. M. Ameen and H. J. Kadhim, "The efficient interleaving of digital-video-broadcasting-satellite 2nd generations system", *Telkomnika*, Vol. 18, No. 5, pp. 2362-2370, 2020.