

Hyperchaotic Modulo Operator Encryption Technique for Massive Multiple Input Multiple Output Generalized Frequency Division Multiplexing system

Mohammed Jabbar Mohammed Ameen and Saad Saffah Hasson Hreshee

Department of Electrical Engineering /Collage of Engineering/University of Babylon/Iraq
drmohammedalsalihy@gmail.com, mohammedalsalihy@uobabylon.edu.iq

Abstract: Fifth generation (5G) wireless communications technology has great challenges to ensure security. Therefore, required a suitable approach to provide security. Using chaos theory in cryptosystems is one of these ways. In this paper, a new approach was proposed for audio encryption in wireless communication based on multiple chaotic maps. The maps used include Bernoulli, Standard, and Bogdanov maps which are combined with audio based on the modulo operator. The initial condition and the controlling parameters of these maps are used as a secret key. The proposed technique was implemented with a 5G infrastructure that contains Generalized Frequency Division Multiplexing (GFDM), Parallel Spatial Modulation (PSM), and massive Multiple Input Multiple Output (MIMO). The strength of the proposed method against attacks has been verified using histogram, spectrogram, Signal to Noise Ratio (SNR), Spectral Segment SNR (SSSNR), Peak SNR (PSNR), percentage of Difference (P. Diff), Mean Square Error (MSE), Correlation Coefficients (R_{xy}), Entropy (H), Linear Predictive Code (d_{LPC}), Log Spectral Distance (d_{LOG}), Frequency Weighted Log Spectral Distance (d_{FWLOG}), number of samples change rate (NSCR) and the unified average changing intensity (UACI), key space, and key sensitivity. The results show that the effectiveness of the proposed audio encryption technique is secure enough to resist various common eavesdroppers. Furthermore, the encryption-decryption process takes a short computational time, making it suitable for real-time communication.

Keywords: Audio Encryption, Security, Chaotic Maps; massive MIMO; 5G; PSM; GFDM

1. Introduction

Audio-based communication is becoming increasingly popular in a variety of scenarios, including the organizational and military domains. With the increasing demand for information technology, security has become a major concern in these domains. Encryption protects the original data from being accessed or destroyed by unauthorized parties. The study of information security, such as data integrity, authentication using scientific methods or well-defined techniques, is known as cryptography. Audio encryption involves filling the quiet part of a communication with noise signals in such a way that only a legal recipient can reconstruct the message's content. Decryption is the process of reassembling an encrypted message into its original form [1].

The use of chaos theory in encrypting data is attracting a growing amount of attention from researchers throughout the last decades. In truth, chaotic systems offer unique and advantageous characteristics, such as high sensitivity to both the beginning conditions and the parameters of the system, totally arbitrarily behavior, highly secure, and efficiency [2]. There are many different types of chaotic system, ranging from one-to-many dimensions. Due to the various parameters in high-dimensional chaotic systems, they are more unexpected. On the other hand, it has drawbacks such as high computing cost and implementation complexity. While, one-dimension chaotic system has a simple chaotic structure and are straightforward to design, but they have restricted to number of chaotic variables and are subjected to attack [3]. Many countries are already using fifth-generation (5G) wireless communications to be used in Internet of Things (IOT) applications such as smart cities and autonomous vehicles, etc. The 5G network employs high-level technology such as massive MIMO, beamforming, and

Received: March 15th, 2022. Accepted: May 22nd, 2022

DOI: 10.15676/ijeel.2022.14.2.4

millimeter wave (mm wave) to provide benefits such as high data rates, low latency, and low power consumption. The orthogonal frequency division multiplexing (OFDM) technique is the considerable commonly used communication in fourth-generation (4G) wireless communication. OFDM has several benefits, such as high resist to multipath interference, good intersymbol interference (ISI) resistance, and ease of execution. OFDM have large sidelobes because of the use of rectangular pulse filters which lead to high out-of-band (OOB) radiation and high peak to average power ratio (PAPR). For the reasons mentioned above, OFDM is not suitable for 5G applications. GFDM is a promising waveform for 5G wireless communications to overcome the difficulties of OFDM in meeting all requirements. GFDM is a type of multicarrier modulation scheme that employs non-rectangular pulse filters in transmission, so the uses of non-rectangular filters, it can avoid the drawbacks faced including high PAPR and high OOB. Furthermore, it is a flexible scheme that can be adapted according to applications. Finally, GFDM uses fewer cyclic prefixes (CP), improving spectrum efficiency to a degree [4]. Several audio encryption techniques based on chaotic systems have been proposed in the literature. An encryption algorithm was proposed by [5] to encrypt audio files based on XORed between the input voice signal and the binary sequences that generated from chaotic signal. In [6], the authors suggested secure audio based on wavelet transforms and chaotic signals with two-stage of key permutation. In [7] an audio encryption scheme based on the cosine number transform has been introduced. An audio encryption scheme using confusion and diffusion based on a multi-scroll chaotic system and one-time key has been presented in [8]. Chen, Lorenz, and Henon have been used to generate a secret key for audio encryption in [9]. An approach based on stream-cipher for selective speech encryption has been introduced in [10]. Speech encryption scheme based on the principle of substitution and permutation by using 2D Logistic map, Henon map, and Baker maps has been introduced in [11]. In [12], an audio encryption scheme using combination between block cipher and chaotic maps has been proposed. In [13] the chaotic audio encryption technique has been introduced using a permutation substitution principle with a chaotic circle map. According to the studies mentioned above, its have some drawbacks and limitations including inequitable between encrypted and decrypted audio, increasing in correlation coefficient, and raise encryption /decryption time, small key space, high computational complexity and low speed of processing. As a result, there is a perceived absence of a complete solution to address the weak points of prior systems. Therefore, a strong audio encryption algorithm that are suitable to the needs of 5G wireless technology should be explored in order to achieve a high level of security and high speed while maintaining the outstanding audio quality of the decrypted audio signals. The main contributions in this work can be highlighted as follow:

- Protect massive MIMO - GFDM system from eavesdroppers.
- Bernoulli, Standard, and Bogdanov chaotic maps are mixed with audio using modulo operator to achieve encryption process.
- Also, the system has good chaotic characteristics, greatly increases the keyspace, reduces the calculation cost, low computational time, high quality in decrypted signals, and low residual intelligibility.

The rest of this paper is organized as follows. The massive MIMO channel is briefly explained in Section 2. PSM is discussed in Section 3. The GFDM is described in depth in Section 4. The chaotic system was introduced in Section 5 along with its properties. The proposed audio encryption technique is presented in Section 6. The performance evaluation and security testing for proposed model in tables are presented in Section 7. The simulation results are shown in Section 8. In section 9, a comparison with previous works is done. Finally, in Section 10, some concluding observations are offered.

2. Massive MIMO System Model

The point-to-point (P2P) massive MIMO system can be described briefly using N_t as the number of transmit antennas and N_r for receive antennas, as illustrated in Figure 1. At the receiver base station, the received signal y can be expressed in a matrix expression as:

$$Y = Hx + n \tag{1}$$

Where $x \in C^{N_t \times 1}$ refers to the signals transmitted from each antenna, $n \in C^{N_r \times 1}$ is denotes to the additive white Gaussian noise (AWGN) and each of its elements being identical and independently distributed random variable with zero mean and σ variance, $H \in C^{N_r \times N_t}$ is the channel matrix between the transmit and receive antennas. On the receiver part, minimum mean square error estimation (MMSE) techniques is exploited to decode and equalize the received signal [14].

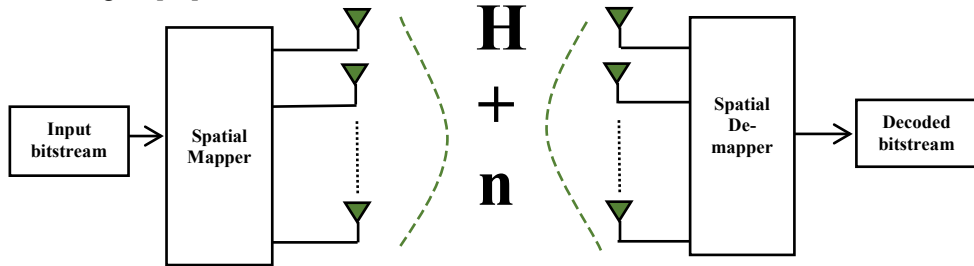


Figure 1. The general model of a massive MIMO system [14]

3. Parallel Spatial Modulation (PSM)

The working principle of PSM can be summarized into steps below [15]:

1. The antennas of the transmitter are partitioned into P equal-sized groups, the size of each one $g=N_t/P$, where $2 \leq g \leq N_t$ and only one transmitter antenna is activated for each group individually. Therefore, SM can be regarded as a special case of PSM when $P=1$ ($g=N_t$).
2. As illustrated in Figure 2, the information to be transmitted is divided into (P+1) sets of bits, with the first part consisting of $\log_2(M)$ bits, and the subsequent P parts consisting of $\log_2(P)$ bits.
3. The signal constellation is achieved by applying the first part of the bits. Then, SM is applied in parallel for each of the groups independently, with the same signal constellation being used.
4. The spectrum efficiency of the PSM scheme in terms of bps/Hz can be represented by:

$$\eta = P \times \log_2(g) + \log_2(M) \tag{2}$$

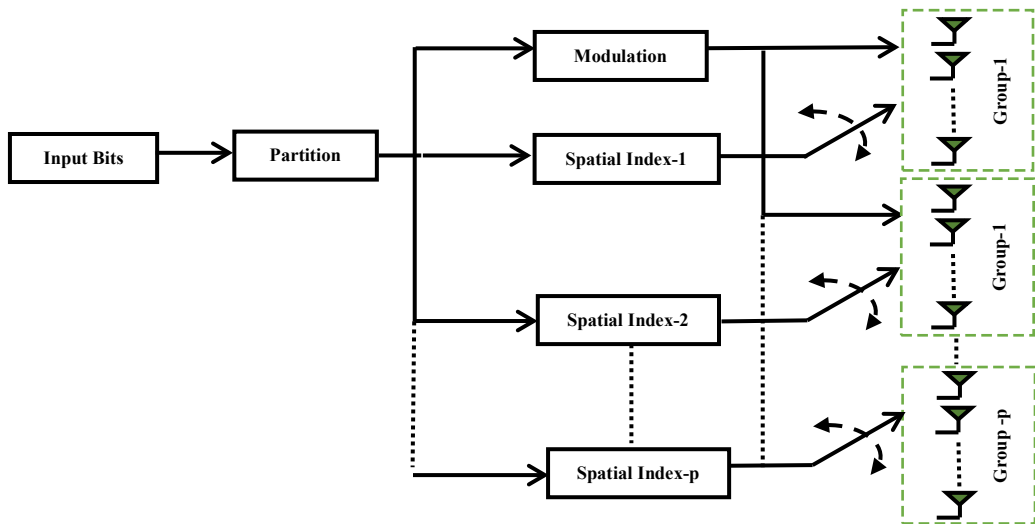


Figure 2. The block diagram of PSM [15]

4. Generalized Frequency Division Multiplexing (GFDM) Technology

GFDM is a non-orthogonal multi-carrier modulation method that allows for adjustable waveform shaping to meet the needs of 5G wireless communications [16]. The transmitting data in GFDM are divided into subblocks and subcarriers to form two-dimensional (time and frequency domain) structure. The prototype filter is used to filter each subcarrier, which has merit in reducing OOB and PAPR. The feature of freely choosing number of subcarriers and subblocks permits the scheme to use the spectral resources more flexibly. Figure 3 shows the structure of GFDM modulation; for each GFDM symbol, one CP is added at the beginning of it [17].

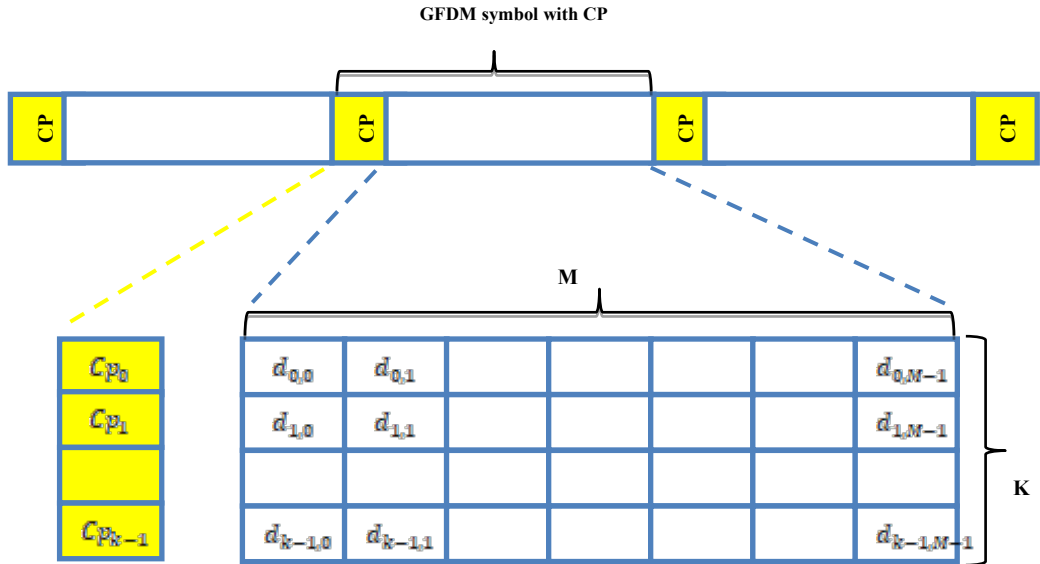


Figure 3. The structure of GFDM data block [17]

A. GFDM Transmitter

The digital data are first modulated to complex symbols before being separated into sequences of $K \times M$ using a serial to parallel converter. Where K and M represent subcarriers and time slots, respectively, also, each sequence characterizes by vector $d[l], l = 0, 1, \dots, KM - 1$. The represented of data by using a block structure, as seen in Figure3, which can be defined in the equations below:

$$D = [d_0, d_1, \dots, d_{k-1}]^T \quad (3)$$

$$D = \begin{bmatrix} d_0[0] & \dots & \dots & d_0[M-1] \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ d_{k-1}[0] & \dots & \dots & d_{k-1}[M-1] \end{bmatrix} \quad (4)$$

where $d_0[m]$ indicate to the symbol in the K^{th} subcarriers and in the m^{th} time slots. In the K^{th} subcarrier at the transmitter, the symbols $d_k[m], m = 0, 1, \dots, KM - 1$ are sampled by factor N , therefore result:

$$d_k^N[n] = \sum_{m=0}^{M-1} d_k[m] \delta[n - mN], n = 0, 1, \dots, KM - 1 \quad (5)$$

The function $\delta[\cdot]$ represents the Dirac Delta. As a result, $d_k^N[mN] = d_k[m]$ and $d_k^N[n] = 0$ for $n \neq mN$. The data are processed by the pulse shaping filter $g[n]$ before being converted to digital subcarriers. Therefore, the yield subcarriers signal $x_k[n]$ is described by:

$$X_k[n] = (d_k^N \square g)[n] * W^{Kn} \quad (6)$$

where \square indicates the circular convolution and $W^{Kn} = e^{i2\pi\frac{nk}{N}}$ is a twiddle factor. The following block structure can be used to represent the transmission signal:

$$X = [x_0, x_1, \dots, x_{K-1}]^T \quad (7)$$

$$X = \begin{bmatrix} x_0[0] & \dots & \dots & x_0[NM-1] \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ x_{k-1}[0] & \dots & \dots & x_{k-1}[NM-1] \end{bmatrix} \quad (8)$$

The total signal is obtained by summing all subcarrier data together in accordance with

$$X[n] = \sum_{k=0}^{K-1} x_k[n] \quad (3)$$

The GFDM modulation block according to above equations are as illustrated in Figure 4

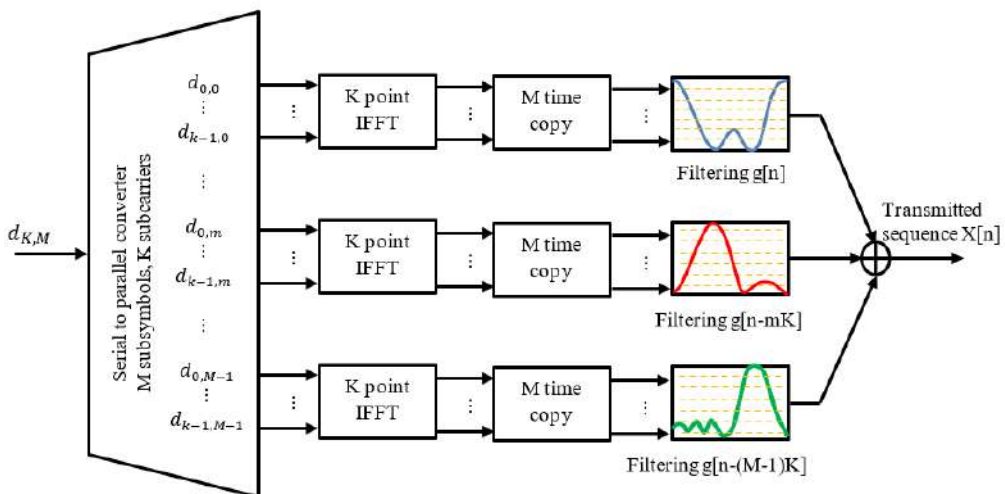


Figure 4. GFDM Modulator[18]

B. GFDM Receiver

The received GFDM signal $y[n]$ can be obtained using expression as in equation (1). This signal is transformed to digital and then converted to parallel data structure. Now channel estimation is applied to get $\hat{y}[n]$. The final received signal is given as:

$$\hat{y}[n] = y[n] * W^{-Kn} \quad (10)$$

$$d_k^N[n] = (\hat{y} \square g)[n] \quad (11)$$

In order to recover the original signal, downsampled and serialized data are used. The GFDM demodulation block according to the above equations is illustrated in Figure 5[18, 19].

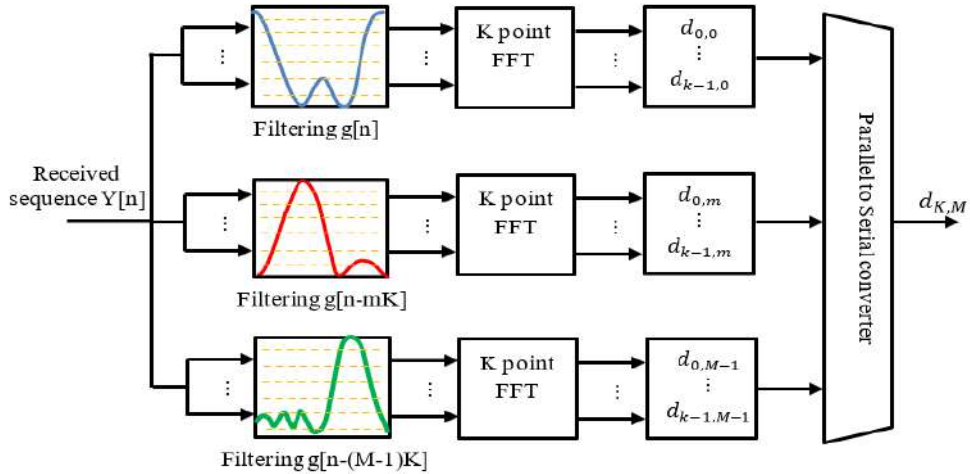


Figure 5. GFDM Demodulator [18]

5. Preliminary of Chaos Theory Based Cryptography

Chaos is a natural phenomenon with a variety of fascinating qualities. Sensitivity Dependent on Initial Conditions (SDIC) is one of the most essential of them. Chaos occurs in numerous non-linear dynamical systems. These systems in fact are deterministic, the initial conditions are unpredictable as well as the output is never repeated. The desired properties of chaos such as ergodicity, broad spectrum, and SDIC can be used in communication systems as a perfect choice for encryption data. Chaos properties are directly related to confusion and diffusion in cryptographic principles. Chaotic signals also feature low correlation coefficients and excellent randomization characteristics. As a result, a variety of chaos-based cryptosystems have been created for wireless communication applications[20]. Table 1 and Figure 6 below briefly introduces the Bernoulli, Standard, and Bogdanov maps, which are used for the proposed model.

Table 1. List of Chaotic Maps used

Chaotic Maps	Time domain	Equations	Number of space Dimensions	Parameter values and Initial condition
Bernoulli [21]	Discrete	$X_{n+1} = \begin{cases} 2\mu X_n, & 0 \leq X_n < 0.5 \\ 2\mu(1 - X_n), & 0.5 \leq X_n < 1 \end{cases}$	1	$X_b(0) \in [0 - 1]$ $\mu_b \in [0 - 1]$
Standard [22]	Discrete	$P_{n+1} = P_n + K \sin(\theta) \text{Mod}(2\pi)$ $\theta_{n+1} = \theta_n + P_{n+1} \text{Mod}(2\pi)$	2	$P(0) = 0; \theta(0) = 0.$ $K \in [0 - 5.19]$
Bogdanov [23]	Discrete	$X_{n+1} = Y_{n+1} + X_n$ $Y_{n+1} = Y_n + \varepsilon Y_n + kX_n(X_n + 1) + \mu X_n Y_n$	2	$X_{bog} = 0.9;$ $Y_{bog} = 0.37;$ $\mu_{bog} = -0.02;$ $\varepsilon = -0.17; k = 1$

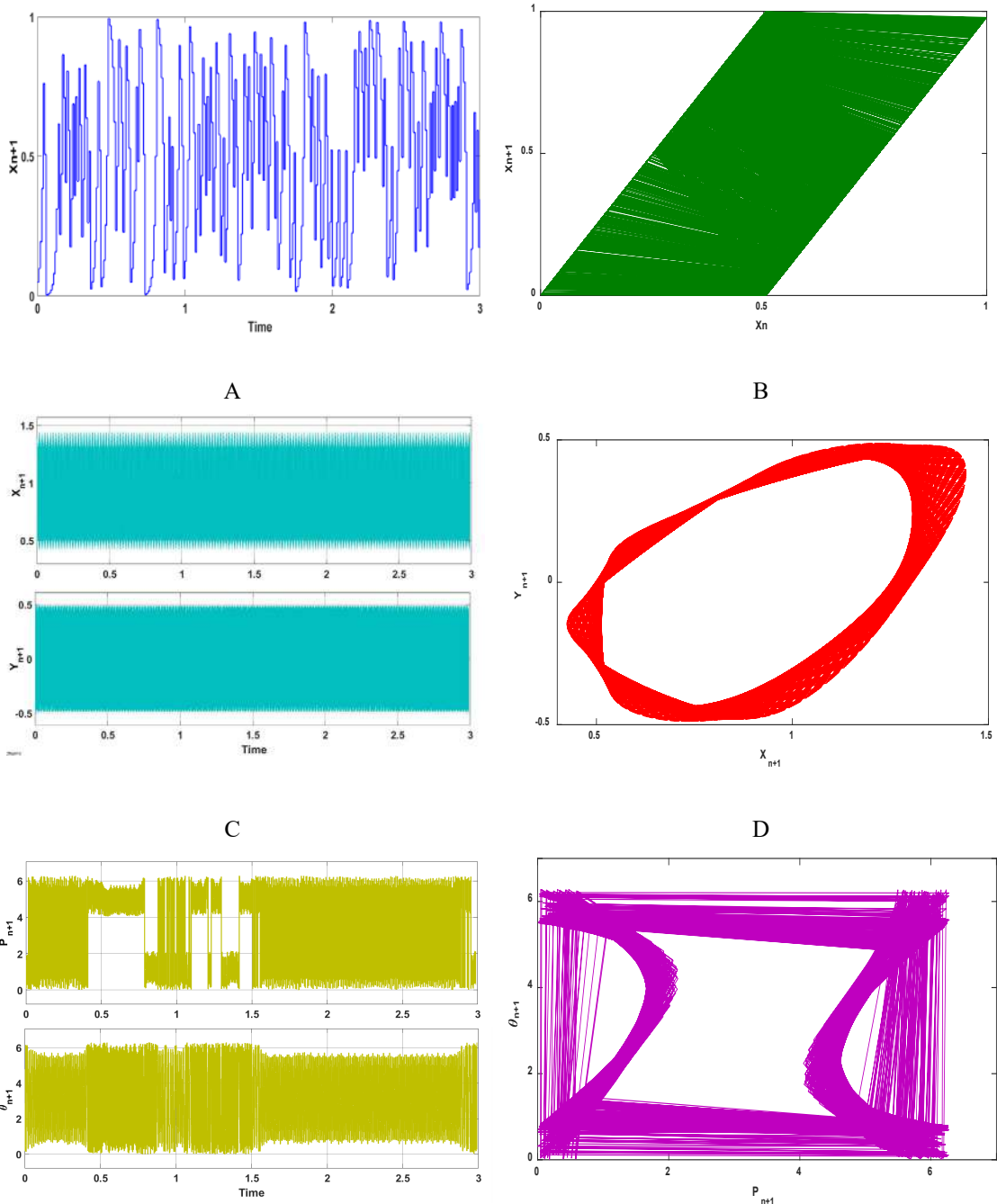


Figure 6. Behavior of chaotic maps [(A), (C), (E)] time series, [(B), (D), (F)] attractor of Bernoulli, Standard, and Bogdanov maps respectively

6. The Proposed Audio Encryption Model

In this part of the work, a novel approach to protect audio will be formulated based on triple chaotic maps utilized as a secret key generator (pseudo-random number generators (PRNG)). The proposed hyperchaotic Modulo operator comprises of massive MIMO, PSM, and GFDM, the details of each part are illustrated in Table 2 and Figure 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 (int16) data type in order not to cause loss of voice data when it is converted to binary bits and reconverted to original data. The generated PRNGs are utilized to directly encrypt audio using the modulo principle to generate a hyperchaotic Modulo operator as demonstrated in Figure 8, resulting in a cryptosystem with the excellent security level and low residual intelligence (RI). The mathematical representation of encryption process is as following:

$$A \text{ mod } B = (R, Q) \tag{4}$$

where A is the dividend (Audio), B is the divisor (Bogdanov Map), Q is the quotient and R is the remainder. To rebuild (A) again, use the following formula:

$$A = R + Q \cdot B \tag{5}$$

By adding PRNGs for each part of above equation to achieve audio encryption results:

$$A_{\text{encrypted}} = (R + \text{PRNG}_{\text{Bernoulli}}) + (R + \text{PRNG}_{\text{standard}}) \times \text{PRNG}_{\text{Bogdanov}} \tag{6}$$

After the encryption process is completed, an analog to digital converter (ADC) is used to convert the audio to a binary system. In order to satisfy the PSM requirement, the incoming bitstream is partitioned into six groups and each has 4 bits, one group used for 16-QAM modulation, and the remaining groups used for antenna index. At the receiver side, the decryption process can perform as shown in Figure 9 below, using equation:

$$A_{\text{decrypted}} = (R - \text{PRNG}_{\text{Bernoulli}}) + (R - \text{PRNG}_{\text{standard}}) \times \text{PRNG}_{\text{Bogdanov}} \tag{7}$$

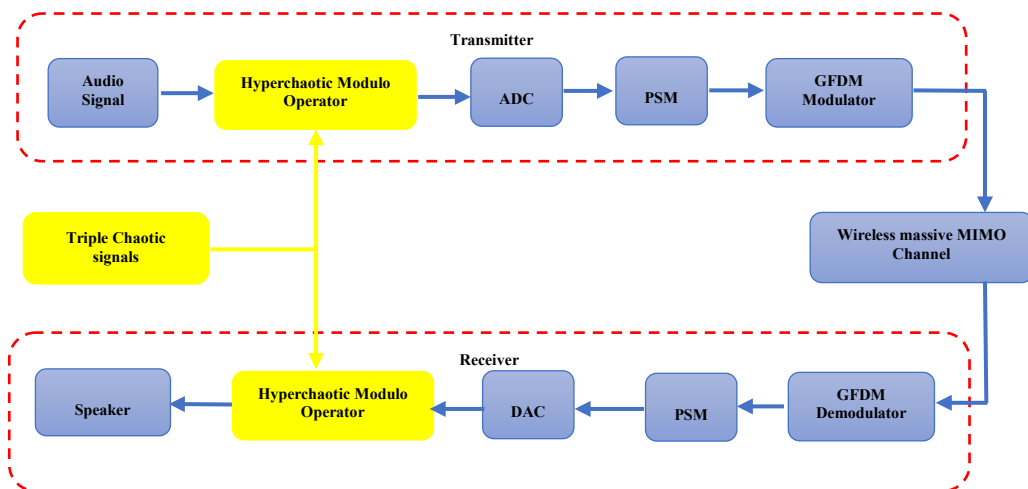


Figure 7. Flowchart of the general proposed system

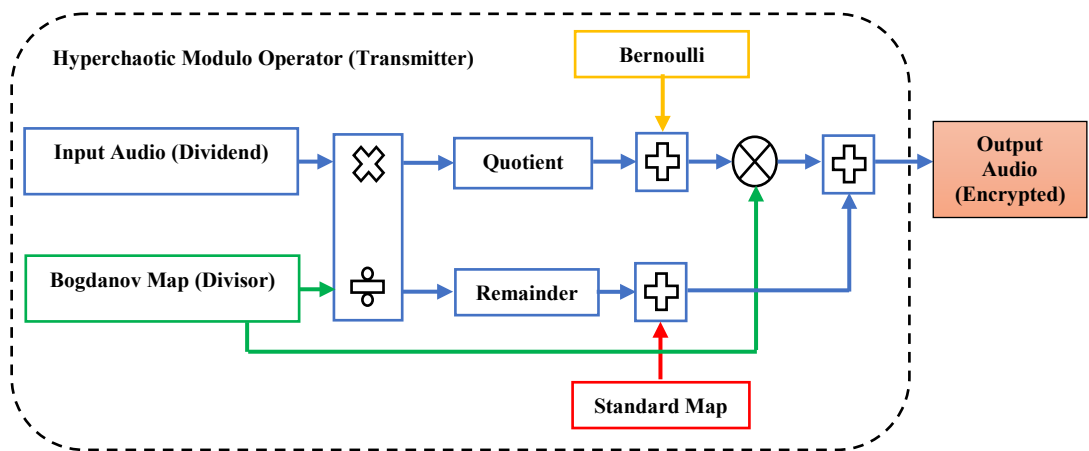


Figure 8. Encryption block diagram of the proposed hyperchaotic Modulo operator

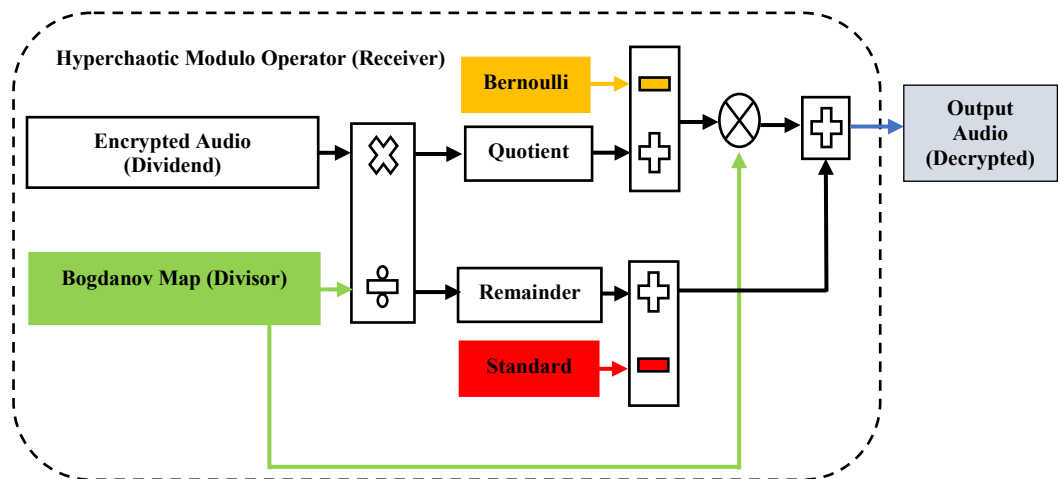


Figure 9. Decryption block diagram of the proposed hyperchaotic Modulo operator

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
Massive MIMO	Length of cyclic prefix (CP)	20
	Number of transmit antennas (N_t)	80
	Number of Receive antennas (N_r)	80
PSM	Channel Fading	Rayleigh
	Number of group (p)	5
	Group size (g)	16

7. Quality Of Encrypted Signal and Security Analysis

When receiving an audio signal, the encryption technique must be effective sufficient to produce an unclear signal. R.I. evaluates the quality of the audio encryption scheme. R.I. referred to redundant data measure in the encrypted audio. Subjective tests can be used to assess the R.I. of the encrypted audio and the quality of the recovered audio. The encrypted audio would have to be heard by a wide number of experienced and untrained human listeners in subjective tests. There are three degrees of R.I in these tests: word, phrase, and digit.

The range of R.I. scores is (0-100) percent and as follows:

- When R.I (0) %, this is a perfect case (good encryption scheme).
- When R.I (1-10) %, this gives a low case
- When R.I (11-30) %, this gives a medium case.
- When R.I (31-50) %, this gives a high case (poor encryption scheme).

These tests have the disadvantages of taking a long time in the laboratory and requiring a big number of audiences. There are other tests that can be used, called objective tests, and they serve as indicators for encrypted audio R.I. and the quality of the retrieved audio [24]. The most popular methods are:

A. Signal to Noise Ratio (SNR)

The SNR is a simple measure for evaluating the quality of the audio encryption algorithm. The noise value in the encrypted audio is high thus; low SNR is required for good encrypted. The SNR values of encrypted audio are estimated as follow:

$$SNR = 10\log_{10} \frac{\sum_{i=1}^N X_i^2}{\sum_{i=1}^N (X_i - Y_i)^2} \quad (8)$$

Where X_i, Y_i are original and encrypted audio sample respectively.

B. Peak Signal to Noise Ratio (PSNR)

The mean square error of original (X_i) and encrypted (Y_i) audio can be estimated as follows:

$$MSE = \frac{1}{N} \sum_{i=1}^N (X_i - Y_i)^2 \quad (9)$$

Then, PSNR can be determined using the following formula:

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

Where MAX represents the maximum value of the encrypted audio samples. Lower PSNR indicates the high noise level in the audio that is means a good encryption algorithm and has resistance against attacks.

C. Correlation Analysis

Correlation coefficient (R_{xy}) is a tool metric for evaluating a cryptographic algorithm against different attacks. Its measures the relationship among similar portions of the original and encrypted audio. A good audio encryption algorithm is one that converts the audio into noisy signal with low value of R_{xy} between original and encrypted audio. In general, original audio has R_{xy} close to one while the encrypted audio has R_{xy} close to zero. R_{xy} can be estimated as following:

$$R_{xy} = \frac{\text{cov}(x, y)}{\sigma_x \sigma_y} = \frac{\frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y))}{\sqrt{\frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2} \sqrt{\frac{1}{N} \sum_{i=1}^N (y_i - E(y))^2}} \quad (11)$$

Where N is the number of audio samples, x_i and y_i are the samples value of the original and encrypted audio respectively, $E(x)$ and $E(y)$ are expected value of the original and encrypted audio samples respectively, $\sigma_x, \sigma_y \neq 0$ are the standard deviation of the original audio and encrypted audio respectively, and $\text{cov}(x, y)$ is the covariance between audios [25]. In Figure 10 below, the scatter plot was presented for audio-2 and the corresponding encrypted audio. It is clear that there is no similarity between the adjacent encrypted samples.

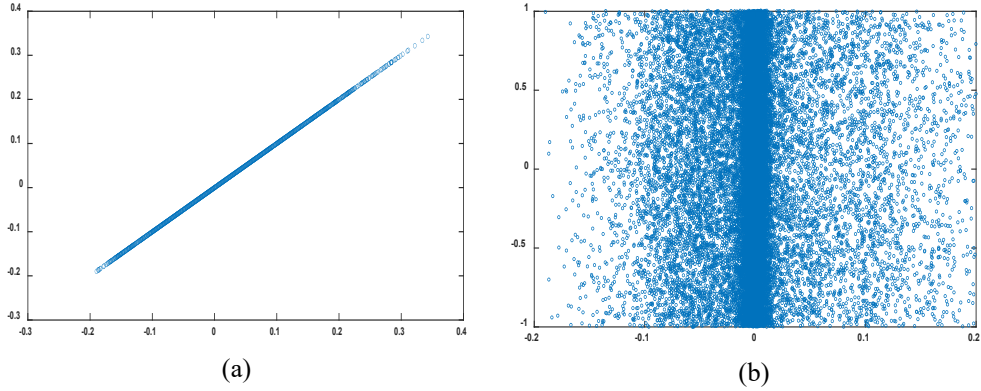


Figure 10. Correlation coefficient result for audio-2: (a) original (b) encrypted

D. Information Entropy Measure (H)

Entropy plays an important measure in determining information's uncertainty and randomization. The entropy $H(m)$ can be estimated as follows [26]:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \times \log_2 \frac{1}{p(m_i)} \quad (12)$$

Where $p(m_i)$ is the occurrence probability of the symbol m_i

E. Linear Predictive Code Distance (d_{LPC})

The d_{LPC} can expressed as:

$$d_{LPC} = \ln \left(\frac{CVC^T}{dVd^T} \right) \quad (13)$$

Where $c = [c_1, c_2, \dots, c_p]$ is the LPC coefficients vector estimated from original (clean) audio, $d = [d_1, d_2, \dots, d_p]$ is the LPC coefficients vector calculated from encrypted (distorted) audio, and $V = V(i, j)$, $i, j = 0, 1, \dots, p$, is the correlation coefficients matrix estimated from encrypted audio as:

$$v(i, j) = \frac{1}{p} \sum_{n=i}^{p-i-1} b(n)b(n+i-j) \quad (14)$$

Where p is the filter order

F. Log Spectral Distance Measure (d_{LOG})

The d_{LOG} can be determined using following formulas:

$$v(f) = \log(s(f)) - \log(s'(f)), f = 0, 1, \dots, N-1 \quad (15)$$

Where $s(f)$ and $s'(f)$ represent the power spectrum original and encrypted audio respectively, so

$$d_{LOG} = \frac{1}{N} \sum_{f=0}^{N-1} |v(f)|^p, f = 0, 1, \dots, N-1 \quad (16)$$

Where p is the distance order [27].

G. Frequency Weighted Log Spectral Distance (d_{FWLOG})

Audio with a frequency range of 300-500 Hz can be understood reasonably well. In other meaning, the audio residual intelligibility components are found within the 300-500 Hz frequency range. As a result, distance measurements more suited to the cryptanalysis of transform domain audio encrypted would prioritize proper coefficient relocation in this frequency region. One way to perform this is to mask portions of the spectra of the original and cryptanalyzed audio waveform to zero, limiting the distance measurements to the 300-500 Hz band. Modifying the d_{LOG} would be a useful approach. That is, before using Equation (24) to calculate the d_{LOG} , a masking window can be implemented to the spectra of the two frames to compare only the 300-500 Hz components. The use of such a window permits equation 24 to be simplified to:

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

Where a and b are the index of spectral coefficients of frequencies 300 Hz and 500Hz respectively, and $n=b-a+1$ [28].

H. Spectral Segment SNR (SSSNR)

The SSSNR is abbreviated as:

$$SSSNR = 10 \log_{10} \left[\frac{\sum_{i=0}^{N/2-1} |X_i|^2}{\sum_{i=0}^{N/2-1} (|X_i| - |Y_i|)^2} \right] \quad (18)$$

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

I. Cpestral Distance (d_{CD})

The (d_{CD}) is expressed in the following way:

$$d_{CD} = 10 \log_{10} \sqrt{2 \sum_{i=1}^p (C_x(i) - C_y(i))^2} \quad (19)$$

Where $C_x(i)$ and $C_y(i)$ are the Cpestral coefficient of original and encrypted audio respectively [5].

G. UACI and NSCR Analysis

Resistance against differential threats is a key indicator of encryption strength. To determine this level of resistance, a modified audio is obtained by inverting the least significant bit of the sample. The same secret key is employed to encrypt both the original and modified audio, resulting in two encrypted audios. After that, the encrypted audio signals are then compared by the number of samples change rate (NSCR) and the unified average changing intensity (UACI), they are represented by:

$$NSCR = \sum_i \frac{D_i}{N} \times 100\%, D_i = \begin{cases} 1, A \neq A'_i \\ 0, otherwise \end{cases} \quad (20)$$

$$UACI = \frac{1}{N} \left[\sum_i \frac{|A_i - A'_i|}{65535} \right] \quad (21)$$

Where A and A' are the encrypted of original and modified audio, respectively, which have difference in one sample only. N is representing number of samples in audio. The optimal NSCR and UACI values are 100 % and 33.3 %, respectively [7].

8. Simulation Results

A. Audio Representation

The useful tools for classifying and analyzing audio waveforms are:

A.1. Histogram Analysis

Histogram analysis is a reliable method of determining the quality of encrypted audio. A stronger encryption system should convert the original audio to random-like noise (uniform distribution) with a roughly flat sample value distribution. In addition, the filling the muted portion of audio by noisy signals with approximate similarly values explains that why the histogram of encrypted audio resulting become approximately flat, while, the histogram of the original audio is random and concentrating on zero point. The histogram of the original and corresponding encrypted audio is shown in Figure 11 [25].

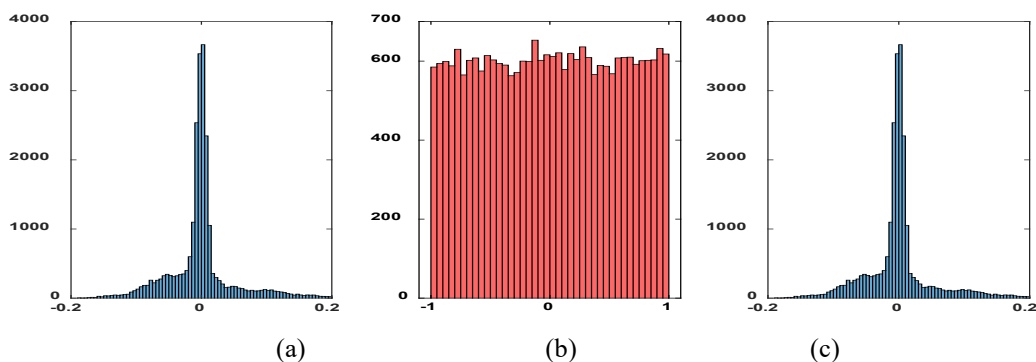


Figure 11. Histogram of Audio-2: (a) Original (b) encrypted (c) decrypted

B. Spectrogram Analysis

The spectrogram is the three-dimensional representation of information using time, frequency, and energy value. The colors describe the value of energy in the audio, and when the color is darker that it refers to a high content of energy. Color gradation start from blue (low energy) to yellow (medium-energy) to red (high energy). The spectrogram of the original and corresponding encrypted audio files is shown in Figure 12 [29].

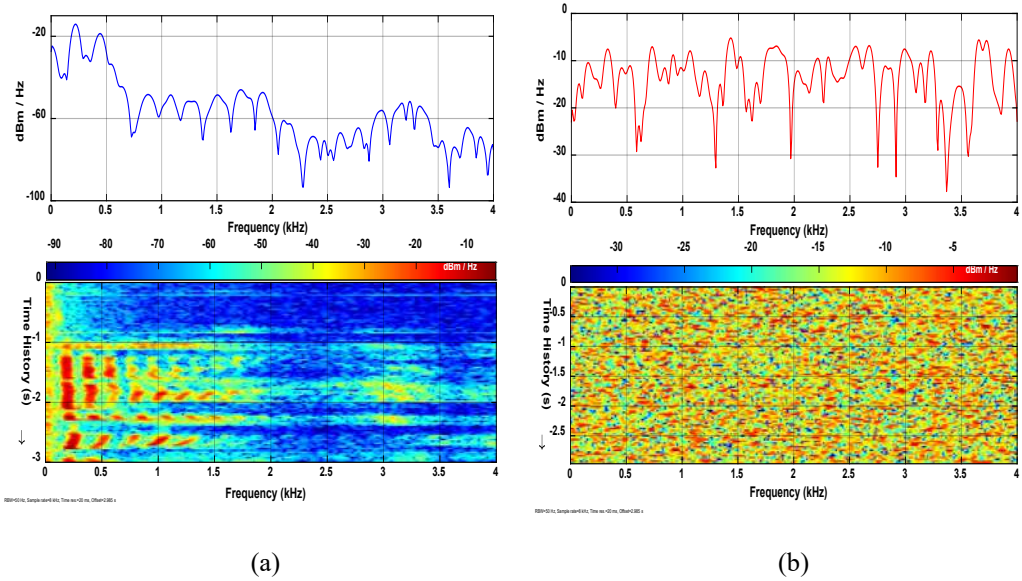


Figure 12. power spectrum density (PSD) and Spectrogram for (a) original and (b) encrypted Audio-2 (3 Sec.)

C. Key Space and Sensitivity Analysis

There are two factors that affect audio encryption quality which is Keyspace and key sensitivity. The group of secret keys used during audio encryption is known as keyspace. The key sensitivity means that the decryption of the audio cannot be achieved when there is little variation in the secret key. To be a secure system against attacks, powerful audio encryption must have a large keyspace and high sensitivity. The key Space of each chaotic Maps used in the proposed system are listed in Table 3.

Table 3. Key Space of Chaotic Maps

Chaotic Maps	Number of Control Parameter	Number of Initial conditions	Key space
Bernoulli	1	1	$(10^{15})^2 \approx 2^{100}$
Standard	1	2	$(10^{15})^3 \approx 2^{150}$
Bogdanov	3	2	$(10^{15})^5 \approx 2^{250}$

If the computation precision of Matlab R2020a is around (10^{-15}) , which means that the possible values of each secret key can take $(10^{15} \approx 2^{50})$, then the overall keys space of the proposed model has ten secret keys, therefore the overall key space $(2^{50})^{10} = 2^{500}$. To test the sensitivity of the proposed hyperchaotic modulo operator key, a small modification is made to one of the parameter keys, while the rest of the parameters remain unchanged during implementation [24]. The statistical measurements to show the sensitivity key are the percentage of Difference (P. Diff.), CD, MSE, and SSSNR are illustrated in Table 4. When the values of P. Diff. and CD is high and the values of MSE and SSSNR is small that is means a large key sensitivity of the proposed system. The proposed system's secret keys are: $X_b(0), \mu_b, P(0), \theta(0), K, X_{bog}, Y_{bog}, \mu_{bog}, \varepsilon, k$

Table 4. Key sensitivity test of the proposed models using audio-2 with duration 3 second

Map	Change key	MSE	d_{CD}	SSSNR	P. Diff
Bernoulli	$X_b(0)+10^{-8}$	0.33559	10.9425	-29.7173	100%
	μ_b+10^{-8}	0.33314	10.9501	-29.6916	100%
Standard	$P(0)+10^{-8}$	0.33486	11.0079	-29.7024	99.9917%
	$\theta(0)+10^{-8}$	0.33417	10.9733	-29.7002	99.9917%
	$K+10^{-8}$	0.33377	11.0447	-29.6874	99.9833%
Bogdanov	$X_{bog}(0)+10^{-8}$	0.29481	10.988	-28.6032	100%
	$Y_{bog}(0)+10^{-8}$	0.30278	10.9019	-28.8269	99.9958%
	$\mu_{bog}(0)+10^{-8}$	0.33650	10.9523	-29.7067	99.9958%
	$k+10^{-8}$	0.30261	10.9507	-28.7826	100%
	$\varepsilon+10^{-8}$	0.33524	10.9592	-29.7038	99.9917%

D. Security Metrics Test

The capabilities of the proposed scheme can be evaluated in this subsection. By assuming that the eavesdroppers know map type and its position in the transmission system but don't have any initial conditions and control parameters. The most common security test was listed in the Table 5 below.

The following factors should be considered when evaluating the proposed system from a statistical point of view:

- The reduction in SNR, SSSNR, r_{xy} and PSNR value means that the (R.I.) audio encryption procedure is low, thus improving the security level.
- The increasing in d_{CD} , MSE, d_{LPC} , d_{LOG} , and d_{FWLOG} value means low the R.I. of audio.

Table 5. Results of encryption for audio-1 and audio-2

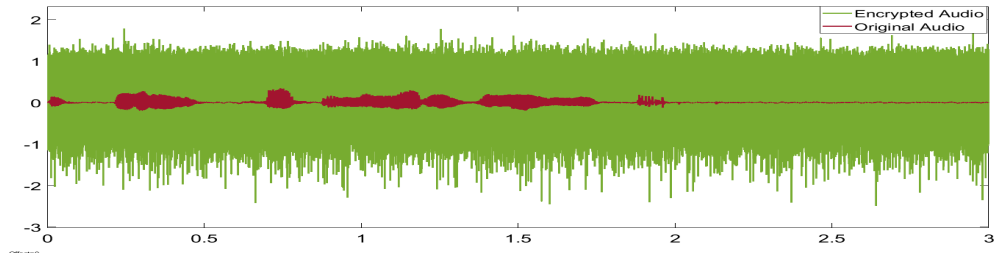
TESTS	Audio-1	Audio-2
Cpectral Distance (d_{CD})	9.4857	10.9592
Spectral Segment SNR (SSSNR)	-23.765	-29.7038
Peak SNR	7.7594	4.7465
Signal to Noise Ratio (SNR)	-19.3936	-20.9716
Mean Square Error (MSE)	0.33424	0.33524
Correlation Coefficients (R_{xy})	-0.01477	-0.002010
Encrypted audio Entropy (H)	13.727	14.2006
Linear Predictive Code (d_{LPC})	1.187	1.7083
Log Spectral Distance (d_{LOG})	20.205	22.3839
Frequency Weighted Log Spectral Distance (d_{FWLOG})	10.2937	22.1612

E. Time Analysis

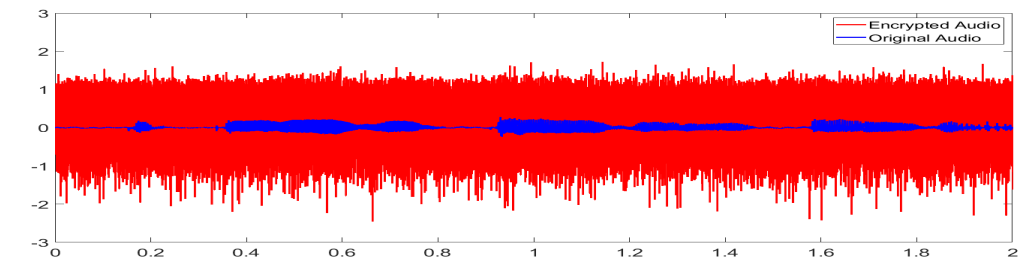
Other crucial features of a strong encryption algorithm are its speed of execution. The encryption/decryption time is the time that the encryption/decryption algorithm takes to complete its process, respectively. This time is proportional to the length of the audio [7, 30, 31]. Consequently, the proposed 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. By using two audio files, the computational time can be summarized in Table 6. Audio waveform are exhibited in Figure 13. The approach clearly turns the original audio into practically noise-like encrypted audio.

Table 6. Time analysis

Audio file	Duration (Sec.)	Size (KB)	Total Time (Sec.)	Speed (Sec./KB)
Audio-1	2	32.0 KB	0.015	4.6875×10^{-4}
Audio-2	3	48.0 KB	0.022	4.5833×10^{-4}



(a)



(b)

Figure 13. Audio encryption Waveforms results (a) Audio-1 (b) Audio-2

F. Resistance against differential attacks

Resistance against differential attacks is a strong indicator of the strength of an encryption algorithm. NSCR and UACI tests are used to evaluate this resistance. Table 7 shows the results of the tests, demonstrating that the suggested system is very resistant to differential attacks.

Table 7. UACI and NSCR analysis

Audio file	Duration (Sec.)	UACI	NSCR
Audio-1	2	33.3354%	99.9937%
Audio-2	3	33.3347%	99.99958%

9. Comparative Study

In this part, the proposed technique features will be compared to those of existing competing systems. Therefore, the most popular security criteria will be used. The results of the comparison in Table 8 show that the proposed system is superior to the previous ones, especially in speed and negative SNR.

Table 8. Comparisons with pervious work

Ref. Tests	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[27]	Ours
Keyspace	2^{427}	-	2^{256}	2^{268}	2^{480}	2^{512}	-	2^{319}	2^{149}	-	2^{500}
SNR	-	- 2.61635	-	-	-	-10.6	-3.025	-	-16.04	-	-20.971
PSNR	-		-	4.5299		47.98	-	4.8069	4.39	-	4.746
SSSNR	- 4.2272	-2.4587	-	-	-16.723	-	-3.04	-	-	-26.506	-29.703
P. Diff	-		-	-	99.14%	-	-	-	-	-	100%
UACI	-		33.29%	-	-	-	-	-	-	-	33.33%
NSCR	-		99.99%	-	-	-	-	-	99.99%	-	99.99958%
d_{CD}	7.097	8.21462	-	-	7.2274	-	-	-	-	8.8503	10.9592
MSE	-	-	-	-	-	-	-	21666	-	-	0.3352
Speed	-	-	-	-	-	-	-	10.4	$3*10^{-3}$	-	$4.583*10^{-4}$
R_{xy}	-	-	0.0021	-	0.38339	-0.0059	-	- 0.00462	-0.004794	-	-0.002010
d_{LPC}	4.336	-	-	-	-	-	0.7253	-	-	0.9741	1.7083
d_{Log}	-	-	-	-	-	-	-	-	-	14.5415	22.3839
d_{FWLOG}	-	-	-	-	-	-	-	-	-	20.9976	22.1612

10. Conclusions





A novel audio encryption system against attacks was developed through use a triple chaotic map as a PRNG to encrypt audio transmitted on massive MIMO-GFDM system. Bernoulli, Standard, and Bogdanov maps are combined with audio using the modulo operator to achieve a cryptosystem. The proposed technique is safe and protected for wireless audio communication based on the different evaluations achieved. The suggested encryption method has a wide keyspace, great sensitivity to secret keys, and invulnerable behavior against various assaults such as noise, according to simulation findings and security studies. In addition, the encryption time is short and suitable for real-time applications. In the future, the hyperchaotic modulo operator can be applied inside the GFDM modulator with a high-dimensional chaotic flow.

11. References





- [1]. 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.
- [2]. S. Kassim, O. Megherbi, H. Hamiche, S. Djenoune, and M. Bettayeb, "Speech encryption based on the synchronization of fractional-order chaotic maps," in *2019 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, 2019: IEEE
- [3]. Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," *Multimedia Tools and Applications*, vol. 78, no. 15, pp. 22023-22043, 2019.
- [4]. F.-B. Ueng, Y.-S. Shen, and D.-C. Lin, "Novel Detectors for Massive MIMO-GFDM Systems," *Wireless Personal Communications*, vol. 121, no. 1, pp. 245-266, 2021.
- [5]. A. Mahdi and S. S. Hreshee, "Design and implementation of voice encryption system using XOR based on Hénon map," in *2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, 2016: IEEE, pp. 1-5.
- [6]. S. N. Al-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.
- [7]. J. B. Lima and E. F. da Silva Neto, "Audio encryption based on the cosine number transform," *Multimedia Tools and Applications*, vol. 75, no. 14, pp. 8403-8418, 2016.
- [8]. 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, 2016.
- [9]. 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 & Communications Technology Applications (NTICT)*, 2017: IEEE, pp. 132-137.
- [10]. A. Belmeguenai, Z. Ahmida, S. Ouchtati, and R. Djemii, "A novel approach based on stream cipher for selective speech encryption," *International Journal of Speech Technology*, vol. 20, no. 3, pp. 685-698, 2017.
- [11]. A. Mostafa, N. F. Soliman, M. Abdallah, and F. E. Abd El-samie, "Speech encryption using two dimensional chaotic maps," in *2015 11th International Computer Engineering Conference (ICENCO)*, 2015: IEEE, pp. 235-240.
- [12]. E. A. Albahrani, "A new audio encryption algorithm based on chaotic block cipher," in *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, 2017: IEEE, pp. 22-27.
- [13]. K. Kordov, "A novel audio encryption algorithm with permutation-substitution architecture," *Electronics*, vol. 8, no. 5, p. 530, 2019.
- [14]. 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, 2018.
- [15]. M. Mohaisen, "Constellation design and performance analysis of the parallel spatial modulation," *International Journal of Communication Systems*, vol. 32, no. 18, 2019.
- [16]. N. Michailow, R. Datta, S. Krone, M. Lentmaier, and G. Fettweis, "Generalized frequency division multiplexing: A flexible multi-carrier modulation scheme for 5th generation cellular networks," in *Proceedings of the German microwave conference (GeMiC'12)*, 2012, vol. 62, pp. 1-4.
- [17]. W. Jinqiu, Q. Gang, and K. Pengbin, "Emerging 5G multicarrier chaotic sequence spread spectrum technology for underwater acoustic communication," *Complexity*, vol. 2018, 2018.
- [18]. 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.

- [19]. 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*, 2020.
- [20]. 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, 2021.
- [21]. R. F. Martínez-González, J. A. Díaz-Méndez, L. Palacios-Luengas, J. López-Hernández, and R. Vázquez-Medina, "A steganographic method using Bernoulli's chaotic maps," *Computers & Electrical Engineering*, vol. 54, pp. 435-449, 2016.
- [22]. S. Sheela, K. Suresh, and D. Tandur, "A novel audio cryptosystem using chaotic maps and DNA encoding," *Journal of Computer Networks and Communications*, vol. 2017, 2017.
- [23]. S. Ayyappan and C. Lakshmi, "Empirical analysis of robust chaotic maps for image encryption," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 9 no. 11, 2020.
- [24]. 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 *Journal of Physics: Conference Series*, 2021, vol. 1804, no. 1: IOP Publishing, p. 012048.
- [25]. R. I. Abdelfatah, "Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic DNA computations," *IEEE Access*, vol. 8, 2020.
- [26]. A. Qayyum *et al.*, "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8, pp. 140876-140895, 2020.
- [27]. A. M. Raheema, S. B. Sadkhan, and S. M. A. Satar, "Performance Enhancement of Speech Scrambling Techniques Based on Many Chaotic Signals," in *2020 International Conference on Computer Science and Software Engineering (CSASE)*, 2020: IEEE, .
- [28]. M. Theberge, "Security evaluation of transform domain speech scramblers," University of British Columbia, 1996.
- [29]. X. Wang and Y. Su, "An audio encryption algorithm based on DNA coding and chaotic system," *IEEE Access*, vol. 8, pp. 9260-9270, 2019.
- [30]. 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.
- [31]. 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.



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 MSc degree in communications engineering from Al-Ahliyya Amman University in 2017, Jordan. He is working as a lecturer in the college of engineering/electrical department 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 & communication security, FEC, and 5G.



Saad Saffah Hasson Hreshee     was born in Baghdad, Iraq, in 1974. He received his BSc degree in Electrical Engineering from the Electrical Engineering Department, College of Engineering, University of Babylon, Iraq, in 1997. He obtained his MSc in Electronic Engineering from the Electrical and Electronic Engineering Department, University of Technology, Iraq, in 2000, while his PhD. in Electronic and Communication Engineering from the Electrical Engineering Department, 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, signal processing, and encryption and communication security.