Grenze International Journal of Engineering and Technology, June Issue

Diversity DNA Encryption in Layered PTS with FBMC OQAM Systems

K. Ayappasamy[1], G. Nagarajan[2] and R. Senthil Kumaran[3]
[1-2]Puducherry Technological University/Department of ECE, Puducherry, 605014, India.
Email: ayappasamypec@gmail.com, nagarajanpec@pec.edu
[3]IFET College of Engineering/Department of ECE, Villupuram- 605108, India.
Email: sen19841@gmail.com

***Abstract*— In Multi-carrier modulations, the Partial Transmit Sequence (PTS) is a useful way for achieving a low Peak to Average Power Ratio (PAPR). The Filter Bank Multi-carrier with Offset Quadrature Amplitude Modulation (FBMC/OQAM) approach has been shown to be a promising technology in advanced wireless communication. The DFT spread Layered PTS (LPTS) method effectively condenses the PAPR of the FBMC/OQAM signal. In addition, a diversity deoxyribonucleic acid (DNA) chaotic encryption approach is presented in conjunction with the layered PTS scheme to improve the physical layer security of the FBMC/OQAM system. Following encryption of the input original binary bit stream, it is modulated with FBMC/OQAM. The bit data encryption process is dynamically regulated by chaotic sequences which are created by a hybrid chaotic system. It is built with improved-Logistic systems which increase the resilience against harmful attacks by unlawful attackers. The results demonstrate that the Layered PTS approach based on diversity DNA encryption may successfully assure the security of transmitted data.**

***Index Terms*— DFT, DNA, Encryption, FBMC-OQAM, Layered PTS and PAPR.**

I. INTRODUCTION

In modern wireless communication technology, an effective handling capacity of frequency selective channels, for progressive technology [1–3], the Filter Bank Multi-carrier addition with Offset Quadrature Amplitude Modulation technique (FBMC-OQAM) is appealing for 5G wireless communication [4], [5]. This is well-structured, with digital filters constructed for each separate sub-channel [6]. The technique employs a windowing type digital prototype filter [7], [8]. Furthermore, the FBMC-OQAM system employs prototype filters to ensure orthogonality for neighboring sub channels, allowing it to avoid asynchronous signal misinterpretation in head-to-head bands [9], [10]. This multicarrier system is similar to the OFDM system in that it suffers from high PAPR [11], [12], and [13], which cause the Q-point of power amplifiers in the final stage of the transmitter and delivers aberrant BER findings [14]. The FBMC/OQAM technology is built with a good prototype filter, which removes the requirement for Cyclic Prefix (CP) and guard intervals in the system [15]. It has the benefits of resilience against narrowband interference and smaller side lobes, and FBMC/OQAM achieves excellent spectral efficiency as a non-CP-OFDM system [16]. In advanced digital filtering technology, FBMC/OQAM plays a significant role. Because of multicarrier system, the high peak-to-average power ratio (PAPR) of the broadcast signal causes the system performance. To fully exploit the benefits of FBMC/OQAM technology, it is suggested

Grenze ID: 01.GIJET.8.2.511_1

physical layer encryption technique does not cause system damage. In this study, a diversity DNA chaotic encryption scheme is suggested for the first time based on research on existing encryption methods. To produce chaotic sequences and regulate the encryption stages, it also employs an improved-Logistic and Delayed Tent Sine (DTS) hybrid chaotic system. The findings demonstrate that the suggested diversity DNA chaotic encryption approach may successfully enhance the physical layer security of the transmission system, effectively fight unauthorized receivers and improve the security of the FBMC/OQAM system without sacrificing the signal's PAPR performance. The following are the crucial charities of this paper: Section II describes about system model of basic FBMC/OQAM. Section III deals with the conventional PAPR reduction techniques. The proposed diversity DNA encryption in layered PTS is detailed in Section IV. Section V elucidates Numerical simulation results and comparisons with the existing systems and Section VI concludes the work.

II. System Model

A. FBMC/OQAM Systems

Fig. 1 establishes a structure of FBMC-OQAM scheme that comprises a transceiver [5]. The N sub stream of carriers are unruffled with OQAM symbols which results are given as $S_m = [s^0_m, s^1_m, \cdots, s^{N-1}_m]^T$, when n varies from 0 to N which is converted from sequence to parallel. The divided actual and unreal incoming sequences are given as,

$$s^n_m = a^n_m + jb^n_m \tag{1}$$

The counts of incoming sequences are denoted as M. a^n_m and jb^n_m are the complex values of the m^{th} sequences on the n^{th} sub stream of carrier.

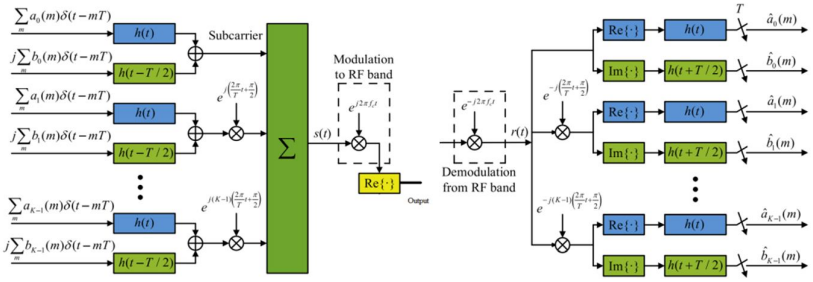


Fig. 1. Model of FBMC/OQAM Transmitter and Receiver system

III. Conventional Systems

A. Genetic Algorithm based Layered PTS FBMC/OQAM Systems

The GA-based Layered PTS scheme is proposed, and the GA-LPTS scheme block diagram is depicted in Fig. 2. This scheme takes advantage of the overlapping structure of the FBMC/OQAM signal and it is sufficient for PAPR minimization in the FBMC/OQAM signal with four up-sampling. The scheme's goal is to reduce the search complexity of the conventional PTS scheme with the help of the prototype filter, but not at the expense of system performance. As shown in Fig. 2, the data block S_m containing M overlapping FBMC/OQAM data is divided into V sub blocks using the adjacent partition method and $0 \le m \le M-1$, that is

$$s_m = \sum_{v=1}^{v} s_m^v \tag{2}$$

Combining the candidate vector of phase factors $b_m = [\, b^{\sim 1}_m, \cdots, b^{\sim v}_m, \cdots, b^{\sim V}_m]$ with the corresponding V sub blocks in the layer 2, the PAPR minimization problem of the FBMC/OQAM signal is then written as $P2$.

$$P2 = \min_{b_m} \{\max_k 1 \, |\bar{s}_m \, [k]|^2\} \tag{3}$$

$$\tilde{s}_m \, [k] = \sum_{v=1}^{v} \tilde{b}^v_{m1} \, s^v_m \, [k] \tag{4}$$

IV. Proposed Diversity DNA Encryption with Layered PTS Scheme

Fig. 3 depicts the principle of the diversity DNA chaotic encryption approach. The DSP-generated pseudo-random binary sequence (PRBS) is utilized as the original input data in the FBMC/OQAM system's transmitter.

To begin, serial/parallel (S/P) converts the PRBS to create a matrix. Each of the matrix's three components is separated into a group to generate N/313/row vector blocks, where N is the number of bits in PRBS. After picking one of these row vector blocks as the beginning point, the row vector blocks are mapped to construct a new matrix using the provided rule. The mapped data is then encoded into base sequences using two alternative encoding techniques and the base sequence is encrypted using the chaotic scrambling method. There are three scrambling rules which are given as addition, subtraction and XOR. Chaotic sequences are utilized to choose particular rules for base scrambling. To construct chaotic sequences K_1, K_2, K_3, K_4, the DTS chaotic method is used which are stated as

$$X_{i+1} = \sin(\pi(T(r, x_{i-m}))) + s(1 - r, x_{i-m}) \begin{cases} \sin(\pi(2rx_{i-m} + Q) & x_i < 0.5 \\ \sin(\pi(2r(1 - x_{i-m}) + & x_i < 0.5 \end{cases} \quad (5)$$

where $Q = (1\text{-}r) \sin(\pi x_{i-m})$ and $m = 1, 2, \ldots, 8$ is the delay number, and the bifurcation parameter $r = 0.26$. The Delay Tent Sine (DTS) chaotic sequences are obtained by the following calculation:

$$\begin{aligned} K_1 &= \text{ceil (mod ((DTS(x,m))* } 10^5, 2)\text{-1} && m=2 \\ K_2 &= \text{ceil (mod ((DTS(x,m))* } 10^5, 2)\text{-1} && m=3 \\ K_3 &= \text{ceil (mod ((DTS(x,m))* } 10^5, 3)\text{-1} && m=2 \\ K_4 &= \text{ceil (mod ((DTS (x,m)) * } 10^5, 2)\text{- 1} && m=3 \end{aligned} \quad (6)$$

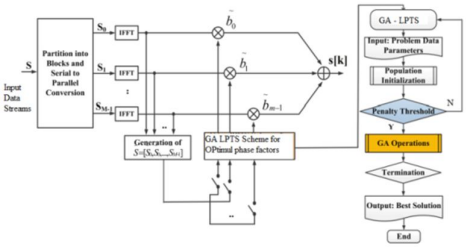


Fig. 2. The Conventional GA-LPTS Scheme

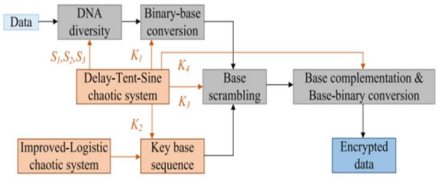


Fig.3. DNA diversity encryption strategy process

The ceil function is used to round numbers to positive infinity and mod is used to perform modulo operations. The chaotic sequences K_1, K_2, K_3 and K_4 is calculated using the abovementioned equations. The improved-Logistic chaotic algorithm generates a binary chaotic sequence LX, which is encoded into a key base sequence. The improved-Logistic method is written as follows:

$$\begin{cases} x_{n+1} = \mu x(1 - x) & x < 0.5 \\ x_{n+1} = \mu x(1 - x) \ \frac{\mu}{4} & x \geq 0.5 \end{cases} \quad (7)$$

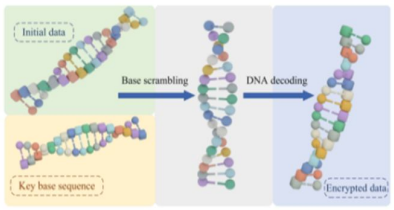


Fig. 4. Diversity DNA encryption schematic diagram

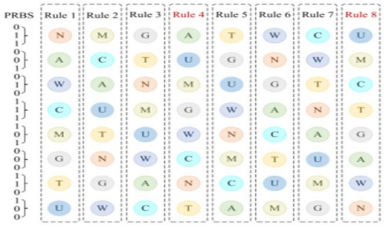


Fig. 5. Base encoding and binary rules

Fig. 4 depicts the diversity DNA encryption process, which includes DNA diversity, binary-base encoding, key base sequence creation, base scrambling, base complementary and decoding into binary symbols. The diversity DNA encryption approach is depicted schematically in Fig. 4. The following rules are used to find out the encrypted output using DNA method.

Rule 1: The cube symbolizes the '0-1' bit row vector block, while the sphere is the foundation. After mapping the DNA diversity, the basic data is encoded as bases and scrambled using key base sequence. To finish DNA diversity encryption, the encrypted bases are decoded into a bit stream. The binary data matrix following S/P is denoted as D, its size is h, p and the sequences are S_1, S_2 and S_3. These are utilized to determine the first row vector block and the DNA diversity mapping rules.S_1, S_2, and S_3 which are calculated in the following manner:

$$S_1 = H.\frac{1}{sort\ (Lx)^T}.Lx.H = [1, 2, \ldots h]$$
$$S_1 = P.\frac{1}{sort\ (Lx)^T}.Lx.P = [1, 2, \ldots p]$$
$$S_1 = \text{mod}\ ((Lx).*10^5.4) + 1 \quad (8)$$

Rule 2: Sort (LX) T is the process of arranging the sequence LX in ascending order and transposing it. The estimated value ranges of the S_1 and S_2 sequences are integers in 1-h and 1-p, respectively. To find the coordinate d_1 of the first row vector block, use the sequences S_1 and S_2. If we denote the picked i^{th} element in S_1 and S_2 as S_1 i and S_2 i, then the coordinate d_1 is (S_1 i, S_2 i).

Rule 3: Starting at the top/bottom of d1, work your way clockwise. Choose the ith element in the chaotic sequence S3, and the link between its value and the mapping rule is as follows: 1 indicates clockwise above $S_{1,\ 2}$ means counterclockwise above S_1, 3 means clockwise below S_1 and 4 means counterclockwise below S1 and all are connected by an S-shaped route.

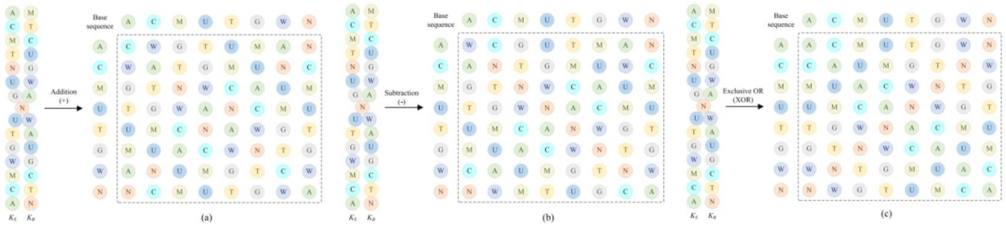
Rule 4: Return to the selected block and map all the blocks in matrix D according to the rule after mapping all the blocks above or below it. At this point, the DNA diversity mapping is accomplished and the new matrix after diversity is indicated as D'.

Rule 5: Adenine (A), guanine (G), cytosine (C) and thymine are the four bases that make up a normal DNA sequence. The Watson-Crick principle states that the basic complimentary pairing rules are A-T and C-G. Encoding two binary bits as one DNA base is typical in DNA encryption; for example, 00, 01, 10, and 11 are used to encode bases A, G, C, and T, respectively. As a result, there are 4! = 24 encoding rules. The diversity DNA encryption approach introduced in this study is expanded to three bits and adds four extra bases based on the normal DNA sequence, which are termed M, W, U, and N, with the base complementary pairing rules being M-W, U-N. Based on this strategy, there are 8! = 40320 encodings of three binary bits as one DNA base.

Rule 6: In binary encoding, 0 and 1 are complementary and the rules are chosen appropriate for this complimentary connection from the 8!. Different types of encoding rules are shown in Fig. 5. In this article, Rules 4 and 8 are encoded.

Rule 7: Each row vector block in the matrix D' is completed as a group, and each group contains three binary values; the chaotic sequence K_1 governs the binary base encoding rule for each group. Rule 4 is used to encode the i^{th} group of binary numbers when the i^{th} element of K_1 is 1, otherwise rule 8 is used, as shown in Fig. 6. The encoded base sequence should be labeled with the letter K_S.

Rule 8: Encode the LX sequence in the key base chain KB.



. (a) Addition (b) Subtraction (c) Exclusive OR

Fig. 6. The base sequences and its Clambering rules

To generate a new base sequence, the chaotic sequence K_3 controls the scrambling rules of the base sequence KS and the base key chain KB. To jumble the bases, it uses three separate rules: 1. addition, 2. subtraction and 3. XOR are illustrated in Fig. 6. The chosen underlying scrambling rules are altered when the value of the chaotic sequence K_3 is getting varies. When the i^{th} element of K_3 is 1, the i^{th} pair of KS and KB is chosen to conduct addition, when the element is 2, subtraction is chosen and XOR is chosen when the element is 3.

V. Performance Evaluation

The performance of an improved DFT spread with genetic algorithm in layered PTS for reduced PAPR FBMC-OQAM system is proposed. It has been evaluated by simulation using the Simulation Tool as MATLAB R 2018a. The proposed system shows improved performance compared to the existing method. Table. I shows the simulation environment for the proposed system.

TABLE I. SIMULATION ENVIRONMENTS

ATTRIBUTES	REMARKS
Simulation Tool	MATLAB R2018a
No of subcarriers (N) assigned	512 and 1024
Subcarrier index	0.5
Phase factors	1 and -1
Overlapping factor (K)	4
No. of filter coefficients	11
Sub-blocks (V)	4, 8
Frequency Band	2.4 GHz
Sub Carrier frequency N=512	4.687 MHz
Sampling frequency for N= 512	10 MHz
Sub Carrier frequency N=1024	2.343 MHz
Sampling frequency for N= 1024	5 MHz
Carrier spacing	30 KHz
Pilot spacing in frequency domain (D)	4
Modulation	16 OQAM
Filter Type	Raised Cosine window type

A. Comparison of PAPR

The PAPR is defined as the ratio of peak power to the average power of all *N* subcarriers and the reduced PAPR provides better performance. It is signified as

$$PAPR = [(Max\left| \{s(n)^2\} \right|) / (E\left| s(n) \right|^2)] \quad (9)$$

where, *Max (s(n))* is peak value and *E(s(n))* is the average power of assigned *N* subcarriers.
The proposed DNA Encryption based Layered PTS (LPTS) method achieves better reduction of PAPR. The proposed scheme offers 2 dB and 2.7 dB at the Complimentary Cumulative Distribution Function (CCDF) of 10^{-4} when the phase rotation vectors (U) are assigned as U= 8 and U= 16 respectively while assigning the subcarrier as N= 512 which is shown in Fig. 7. Also, the Fig. 8 show the proposed simulated results of PAPR while the subcarrier N= 1024. The result obtains, the minimum value of PAPR of 2.2 dB and 2.8 dB when the phase rotation vectors are assigned as U= 8 and U= 16 respectively at the CCDF of 10^{-4}.

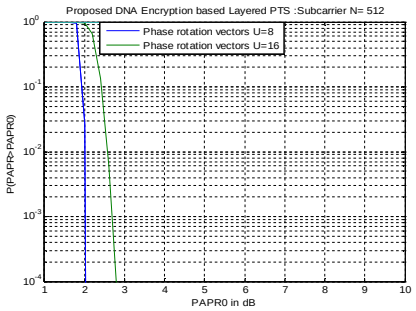


Fig. 7. PAPR for Proposed Scheme when N=512

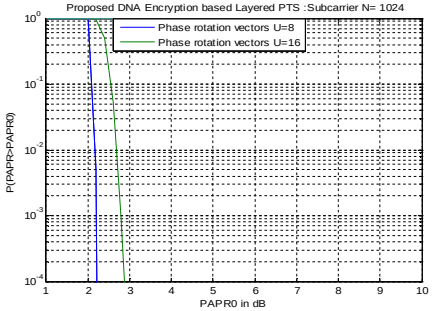


Fig. 8. PAPR for Proposed Scheme when N=1024

B. Comparison of Spectral Efficiency

Fig. 9 and Fig. 10 show the comparison of Spectral Efficiency of the system. The proposed scheme offers 27 bits/sec/Hz and 24 bits /sec/Hz of high spectral efficiency compared to the earlier system which shows the less spectral efficiencies of (21 bits/sec/Hz and 9 bits /sec/Hz) both are simulated for the subcarriers N=512 and N= 1024 respectively which are simulated when the phase rotation vectors are assigned as 16.

C. Computational Copmlexity

Comparison of Relative Computational Complexity of proposed scheme for the subcarriers N=512 and N=1024 as shown in Fig. 11 and Fig. 12 respectively. At first, the results are simulated when the subcarrier *N* is assigned as 512 and phase rotaion vectors *U* are assigned as 8 and 16. As a result, the proposed system proves less relative complexity of 0.0293 and 0.035 when N= 512 and 1024 respectively by assigning
U = 16.

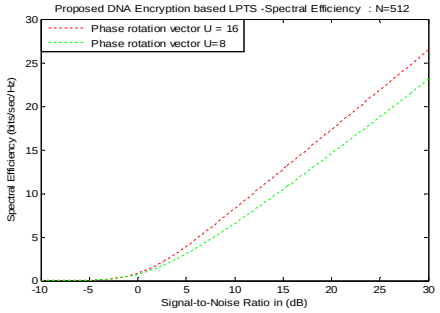


Fig. 9. Spectral efficiency when N= 512

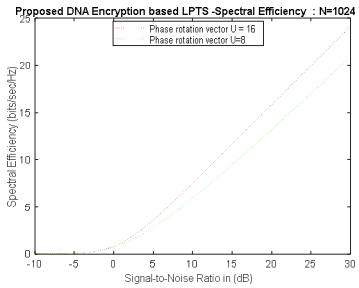


Fig. 10. Spectral efficiency when N= 1024

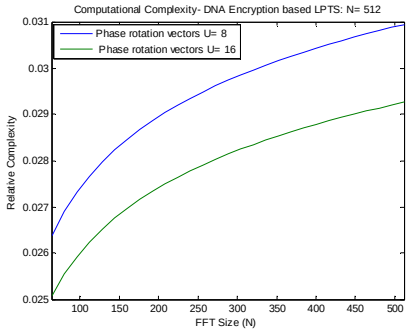


Fig. 11. Computational Complexity when N= 512

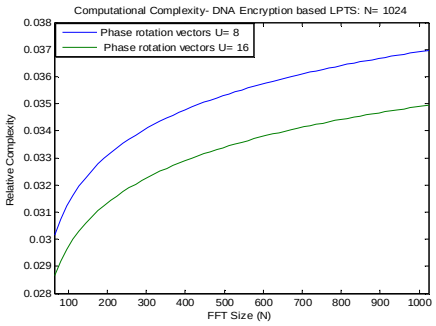


Fig. 12. Computational Complexity when N= 1024

TABLE II. RESULTS COMPARISON

Parameters	Existing Improved DFT spread with GA-LPTS Scheme [2]	Proposed Diversity DNA Encryption based LPTS
PAPR for 10^{-4} CCDF ;N= 512	2.6 dB	2 dB
PAPR for 10^{-4} CCDF; N= 1024	2.9 dB	2.2 dB
Spectral Efficiency N= 512 (30 dB SNR)	21 bits/sec/Hz	27 bits/sec/Hz
Spectral Efficiency N= 1024	19 bits/sec/Hz at (30 dB SNR)	24 bits/sec/Hz at (30 dB SNR)
Computational Complexity N=512	0.0413	0.0293
Computational Complexity N=1024	0.0461	0.035

VI. CONCLUSION

Table.II shows the comparison of offered results in terms of the simulation parameters. The proposed results are compared with existing improved DFT spreading with genetic algorithm based layered Partial transmit sequence. From the result comparison, the proposed diversity DNA encryption based layered Partial transmit sequence in FBMC-OQAM scheme offers reduces PAPR of 2 dB and 2.2 dB at the CCDF of 10^{-4} for N= 512 and 1024 respectively. It is also provides 27 bits/sec/Hz of high spectral efficiency, 0.0293 reduced relative computational complexity. Thus, it is proved that, the proposed method offers better performance compared to the existing method.

REFERENCES

[1] Siying LV, Junhui Zhao and Lihua Yang, "Genetic Algorithm Based Bilayer PTS Scheme for Peak-to-Average Power Ratio Reduction of FBMC/OQAM Signal", *IEEE Access- Special Section On Artificial Intelligence For Physical-Layer Wireless Communications*, Vol.8, Issue. 2, pp. 17945-17955, Jan. 2020.

[2] K. Ayappasamy, G. Nagarajan and P. Arunagiri, "An Improved DFT Spread with Genetic Algorithm in Layered PTS for Reduced PAPR in FBMC OQAM Systems", *7th International Conference on Computations in Engineering and Technology 2022* (*Accepted for Publication in The Institution of Engineering and Technology*).

[3] Da Chen, Tao Jiang and Rui Wang, “Channel Estimation and Pilot Symbol Optimization Based on Intrinsic Interference Utilization for OQAM/FBMC systems,” *IEEE Transactions on Signal Processing*, vol. 8, no. 2, pp. 1-6, Aug. 2021.
[4] Defeng Ren, Jing Li and Guangyue Lu, “Joint Channel Estimation and Equalization Using New AFB Output Signal Models for FBMC/OQAM Systems,” *IEEE Transactions on Communications*, vol. 69, no. 6, pp. 4186 – 4201, Mar. 2021.
[5] Siying LV , Junhui Zhao and Lihua Yang, "Genetic Algorithm Based Bilayer PTS Scheme for Peak-to-Average Power Ratio Reduction of FBMC/OQAM Signal", *IEEE Access- Special Section On Artificial Intelligence For Physical-Layer Wireless Communications*, vol.8, Issue. 2, pp. 17945-17955, Jan. 2020.
[6] Xing Cheng, Wenzhe Shi and Yang Zhao, "A Novel Conversion Vector-Based Low-Complexity SLM Scheme for PAPR Reduction in FBMC/OQAM Systems", *IEEE Transactions on Broadcasting*, Vol.3, pp.1-11, Jan. 2020.
[7] K. Ayappasamy, G. Nagarajan and P. Elavarasan, “Decision Feedback Equalizers and Alamouti Coded DFT Spread for Low PAPR FBMC-OQAM System”, *IEEE International Conference on Emerging Trends in Information Technology and Engineering* (ic-ETITE), *IEEE Explore Digital Library Electronic* ISBN: 978-1-7281-4142-8, (2020).
[8] Siying LV, Junhui Zhao and Lihua Yang, "Genetic Algorithm Based Bilayer PTS Scheme for Peak-to-Average Power Ratio Reduction of FBMC/OQAM Signal", *IEEE Access- Special Section on Artificial Intelligence For Physical-Layer Wireless Communications*, vol. 8, Issue. 2, pp. 17945-17955, Jan 2020.
[9] Da Chen, Rui Wang and Yujuan Mei, “Distribution Line Fitting-Based Channel Estimation Without Guard Symbols for OQAM/FBMC Systems,” *IEEE Transactions on Wireless Communication*, vol.20, no.6, pp. 3659 – 3669, Jan. 2021.
[10] Zhao. J, Ni. S and Yang. L, ‘‘Multiband cooperation for 5G HetNets: A promising network paradigm,’’ *IEEE Vehicular Technology Magazine*, vol. 14, no. 4, pp. 85–93, Dec. 2019.
[11] Farhang-Boroujeny. B, ‘‘OFDM versus filter bank multicarrier,’’ *IEEE Signal Processing Magazine*, vol. 28, no. 3, pp. 92–112, May 2011.
[12] Nadal. J, Nour C. A and Baghdadi. A, ‘‘Design and evaluation of a novel short prototype filter for FBMC/OQAM modulation,’’ *IEEE Access*, vol. 6, pp. 19610–19625, Jun. 2018.
[13] Zhao. J, Ni. S and Gong. Y, ‘‘Peak-to-average power ratio reduction of FBMC/OQAM signal using a joint optimization scheme,’’ *IEEE Access*, vol. 5, pp. 15810–15819, 2017.
[14] Rahim. M. U, Stitz. T. H and Renfors. M, ‘‘Analysis of clipping-based PAPR-reduction in multicarrier systems,’’ *IEEE Vehicular Technology Conference. (VTC) Spring, Barcelona, Spain*, vol. 3, pp. 1–5, Apr. 2009.
[15] Yang. Z, Fang. H and Pan. C, ‘‘ACE with frame interleaving scheme to reduce peak-to-average power ratio in OFDM systems,’’ *IEEE Transactions on Broadcasting*, vol. 51, no. 4, pp. 571–575, Dec. 2005.
[16] LU. S, QU. D AND HE. Y, ‘‘SLIDING WINDOW TONE RESERVATION TECHNIQUE FOR THE PEAK-TO-AVERAGE POWER RATIO REDUCTION OF FBMC-OQAM SIGNALS,’’ *IEEE WIRELESS COMMUNICATION LETTERS*, VOL. 1, NO. 4, PP. 268–271, AUG. 2012.