The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 3, June 2025
https://doi.org/10.33022/ijcs.v14i4.4891

An Enhanced Model of the Wireless Multicarrier Communication OFDM Systems Applied on the FPGA Platform Based on Steganography system

Ali Y. Jaber[1], Ammar F. Mohammed Ali[2]
[1]ayj72zz@mtu.edu.iq, [2]ammaral-khafaji@mtu.edu.iq
[1]Electrical Technique Dep., Middle Technical University, Baghdad, Iraq
[2]Information and Communication Tech., Middle Technical University, Baghdad, Iraq

Article Information

Received : 27 May 2025
Revised : 1 Jun 2025
Accepted : 23 Jun 2025

Keywords

OFDM, PAPR Reduction, OFDM, IFFT/ FFT, PAPR, FPGA, Steganography

Abstract

OFDM is a promising technology due to its robustness against multipath fading. Multipath fading distorts a signal propagating in free space due to destructive or constructive interference. The evolution of 5G wireless networks has necessitated the integration of high-throughput, low-latency multi-band modulation schemes, such as orthogonal frequency division multiplexing (OFDM), into real-time hardware-optimized platforms. However, challenges related to spectral efficiency, security, and the maximum-to-average power ratio (PAPR) remain, especially when these schemes are implemented on field-programmable gate arrays (FPGAs). Steganography offers increased information security. Therefore, this paper proposes an improved OFDM model for 5G that incorporates advanced data hiding techniques using steganography to embed secure image data within ORFDM subcarriers. The proposed system is implemented on an FPGA platform, leveraging high-speed pipelines and parallelism to achieve real-time performance at a minimal resource cost. Simulation and synthesis results demonstrate significant improvements in reduced PAPR, BER, and device efficiency compared to conventional OFDM applications. The FPGA platform design takes up approximately 20% of the total available space, with very low energy consumption compared to other traditional implementation methods. The results also showed an improvement in the OFDM system's performance by reducing the BER by 30%, indicating the absence of data loss and the effectiveness of the steganography technique in these systems. This results in improved architecture performance in terms of area, power, and speed. Furthermore, the proposed approach has proven its worth in terms of security and permeability.

Attribution-ShareAlike 4.0 International License

A. Introduction

The advent of fifth-generation (5G) wireless networks represents a transformative milestone in communication systems, offering unprecedented data rates, ultra-low latency, and support for massive device connectivity [1]. At the core of 5G's physical layer design is Orthogonal Frequency Division Multiplexing (OFDM), valued for its spectral efficiency, robustness against multipath fading, and ease of integration with MIMO architectures [2]. However, real-time deployment of OFDM in hardware-constrained environments, particularly using Field-Programmable Gate Arrays (FPGAs), necessitates enhanced models that address key performance bottlenecks such as hardware complexity, latency, and power consumption [3]..

Simultaneously, growing concerns over communication security have catalysed the incorporation of information hiding techniques—especially stenographic approaches—within the wireless communication pipeline. These methods facilitate covert data embedding, enabling confidentiality and resilience against interception without requiring additional transmission overhead [4]. By embedding information directly into the OFDM subcarriers, one can achieve not only higher security but also a novel modulation flexibility that leverages both frequency and transform domains.

Steganography is one of the most important data security techniques and algorithms due to its simplicity and invisibility [5]. Steganography requires a secure transmission medium in terms of transmission, robustness, and reliability. This fundamentally impacts data security, and this is the primary purpose of our research, which addresses data security challenges and overcomes communication limitations in OFDM [6]. Many stenographic techniques have been used with OFDM, including frequency-based techniques such as DWT, but they are limited by the storage capacity of the image carrying the data. Another technique, the additive bit inversion map (BIM), is an excellent technique, but it has computational complexity that makes it difficult for real-time operations. One of the most important techniques used is the least significant bit (LSB) technique, which is simple and effective, especially in hybrid systems [7].

Another significant limitation in traditional OFDM systems is the Peak-to-Average Power Ratio (PAPR), which leads to power inefficiency and signal distortion under nonlinear amplification [8]. While PAPR reduction techniques such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) have shown promise, their implementation on real-time platforms often entails trade-offs in complexity and energy consumption. Addressing this, the present research proposes an enhanced 5G multicarrier model that integrates information hiding with PAPR reduction, tailored for FPGA-based realization. The model is designed to embed encrypted data using transform-domain steganography within the OFDM framework and implement it on an FPGA using VHDL or Verilog. This enables parallel and pipelined processing, achieving high throughput, real-time operability, and hardware-level security enforcement. Figure 1 presents the conceptual architecture of the proposed system.

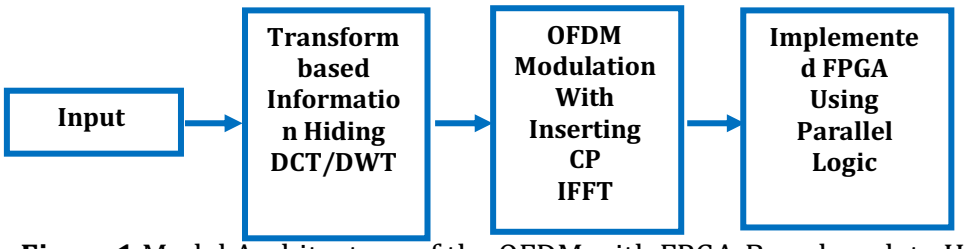

Figure1 Model Architecture of the OFDM with FPGA-Based on data Hiding.

The model is designed to embed encrypted data using transform-domain steganography within the OFDM framework and implement it on an FPGA using VHDL or Verilog. This enables parallel and pipelined processing, achieving high throughput, real-time operability, OFDM modulation is a capable technique for high data rates wireless communication system with multipath fading channel, one of the modulation techniques is multi-carrier (MC). The OFDM signal data consists of several parallel streams in the digital bits form, each modulated with orthogonal subcarriers, which are transmitted to the channel after the DAC unit. [1-4]. In Fourier based OFDM system, inverse fast Fourier transform (IFFT) and fast Fourier transform (FFT) are used at the transmitter (Tx) and receiver (Rx) respectively. cyclic prefix (CP) is added before transmission to mitigate Inter Symbol interference (ISI) and Inter-Channel Interference(ICI) problems. Thus, the delay spread time of the channel becomes longer than the channel impulse response. It is usually 25% of the OFOM symbol period [3]. The limitations of the ISI and ICI are simple to cancel with OFDM technology, which features orthogonal subcarriers and fast IFFT/FFT operations. The advent of high-performance programmable logic devices (PLDs) has made these technologies even more effective in modern communications systems. Recently, OFDM is common used in most 4G wireless communication systems and other applications such IEEE802.11a, b standard systems (Wi-Fi), mobile IEEE802. 16a, e standard systems (WiMAX), and Long Term Evolution (LTE)Systems; OFDM modem essentially was built on an appropriate hardware [9].

The use of programmable electronics, such as FPGAs, in OFDM systems design has led to their rapid spread in wireless communications due to their ease of implementation and the ability to change their functions. System functions can be modified via an easy-to-use API, allowing for control of the FPGA's processing speeds to achieve optimal performance. [10]. Some researchers have proposed implementing software-defined radio (SDR) on the FPGA platform using Xilinx's computer simulation tools by implementing flexible coding schemes [11]. A phase-locked loop (PLL) is designed in the OFDM system to avoid data loss and reduce BER that may result from the synchronization of the orthogonal subcarriers of the transmitter and receiver circuits. In [12], the pioneering Digital Duty Cycle Modulation (DDCM) technology was implemented in converters (DACs) used in the transmitter circuits of the OFDM system within a range of 50 dB and a noise level of 65 dB. These converters were implemented on an FPGA platform and the results were compared with those of single-step converters. In designing a digital-to-analogue converter using Virtex-5 technology, the results were analyzed and compared with their counterparts using computer simulation in MATLAB [13].

This work is timely and significant in the context of secure, real-time 5G applications, including autonomous networks, edge computing, and confidential communications in military and medical domains. Furthermore, when OFDM modem circuit designs are used and implemented on FPGA platforms, they become flexible and reprogrammable designs that can be adapted to the wireless communication application environment, giving designers the ability to make software changes rather than restructuring the design and integrated circuits. Also they can be reprogrammed the FPGA for several times even after publication. LTE wireless communication systems are widely used, featuring high speed, full control over current-generation standards, and full processing capabilities for access to frequency bands. They support high-mobility nodes and the dynamic conditions of data transmission environments across different networks, providing unique performance for these systems [14].

The key contributions of this study include development of a novel information-hiding-enhanced OFDM model using DCT/DWT tailored for FPGA. Also, including Bit Error Rate (BER), PAPR, power utilization, and latency under practical conditions. The rest of this paper is structured as follows: Section II reviews recent developments in OFDM enhancement and FPGA communication systems. Section III details the proposed architecture and design methodology. Section IV presents the hardware implementation and simulation setup. Section V analyses the results and benchmarks against existing models. Section VI concludes with implications and future research directions

B. OFDM System Description

The working principle of OFDM technology is to divide the available frequency into a narrow band in which the subcarrier waves are perpendicular to avoid interference and are sent to different communication channels, thus withstanding the harsh conditions of those environments [15]. The block diagram of the OFDM system can be represented as in Figure 2, where the data flow is serial at first and then becomes parallel, and the QAM mechanism is applied. It can be represented mathematically as follows,

$$x(k) = \sum_{n=0}^{N-1} s(n) \sin(\frac{2\pi kn}{N}) - j \sum_{n=0}^{N-1} s(n) \cos(\frac{2\pi kn}{N}) \quad (1)$$

S(n) is the QAM symbols, N is the length IDFT. Cyclic Prefix (CP) of length D implements after Inverse Fast Fourier Transform (IFFT) block, which is valued greater than the channel impulse response in order to mitigate ISI and ICI as,

$$C(t) = [xcp(k)x(k)]^{x(k)} \quad (2)$$

The OFDM signal construction with CP is implemented to parallel to serial converter (PSC) to transmit through a channel *Y (k)* as.

$$Y(k) = x(k) \times h(l) + n(k) \quad (3)$$

Where, *h (l);* channel impulse response, *x(k)*; OFDM signal, *n(k)*; noise

Thus, It is clear that the CP period added to the OFDM signal is shorter than the channel length to avoid interference and obtain optimal performance as follows,

$$n(k) = 10^{-Es/20No} \times AWGA \tag{4}$$

Es/No is the symbol error ratio (SER) and it can be expressed as,

$$(Es/No)dB = (N/N_{cp} + N)dB + (N_{st}/N)dB + (Eb/No)dB \tag{5}$$

N_{cp} represents the length of CP, N_{st} is the number of uses sub-carriers and N is FFT length. Therefore, the signal receives at Rx with consideration it added CP at Tx as.

$$r(k) = \sqrt{\frac{N_{cp} + N}{N}} \times y(k) \tag{6}$$

At the receiver, the reverse stages are applied to received OFDM signal with infrared channel estimation (CE) after FFT stage [16]. Received date is equalized in the frequency domain as.

$$\hat{x}(k) = \frac{y(k)}{H(k)} \tag{7}$$

H (k) is the frequency channel response.

Equalization is equalized OFDM symbols that were faded by channel a result of multipath problem.

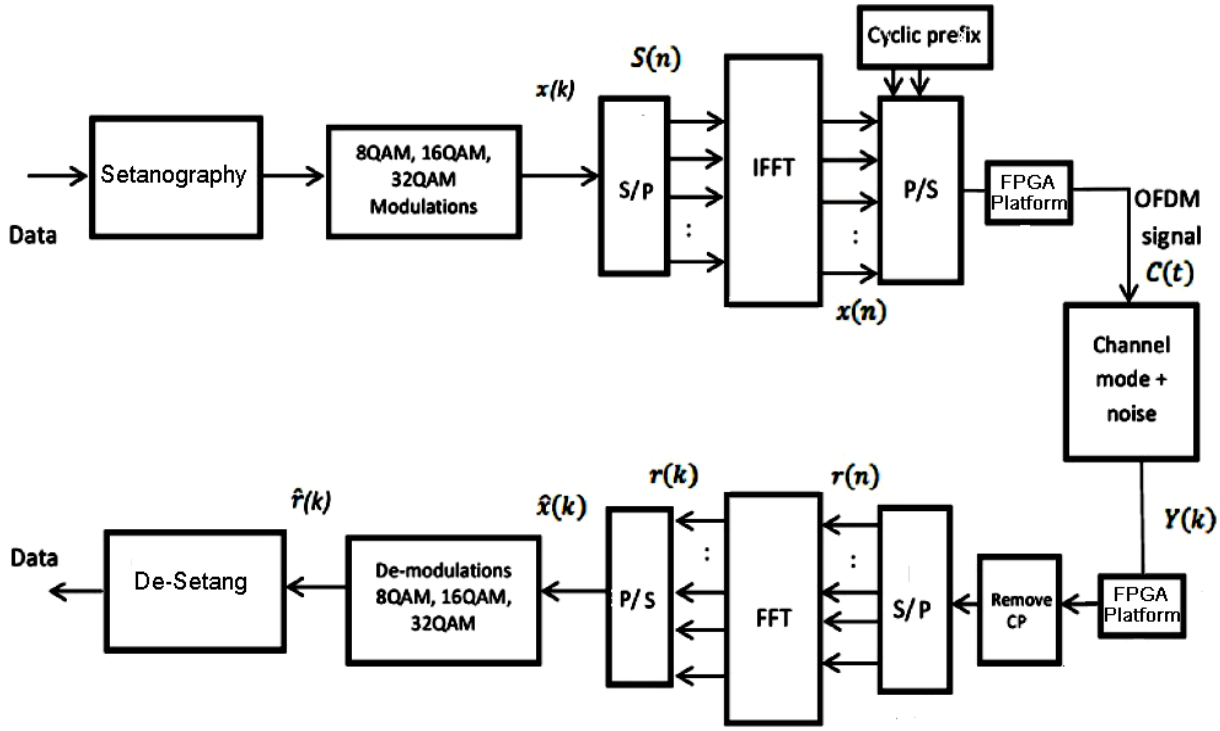

Figure 2 A comprehensive diagram of the OFDM system using FPGA platform

C. Research Method

The proposed system design comprises the following core modules as shown in Figure 3. Also, input Preprocessing, a raw data is divided into secure payload and auxiliary data streams. The payload undergoes preprocessing such as encryption or hashing. Information Hiding Module, the secure payload is embedded into the OFDM subcarriers using transform domain techniques such as LSB. OFDM Modulation, the system follows a traditional OFDM pipeline (serial-to-parallel conversion, IFFT, cyclic prefix insertion). The embedding occurs at the subcarrier level. FPGA Implementation, each module is synthesized and mapped onto FPGA logic using VHDL or Verilog. Design practices include pipelining, parallelism, and clock gating. Transmission and Reception, the transmitted signal is processed by a matched receiver pipeline for synchronization, FFT, subcarrier demapping, and data extraction. Performance Analysis, Bit Error Rate (BER), PAPR, power consumption, resource utilization, and latency are measured

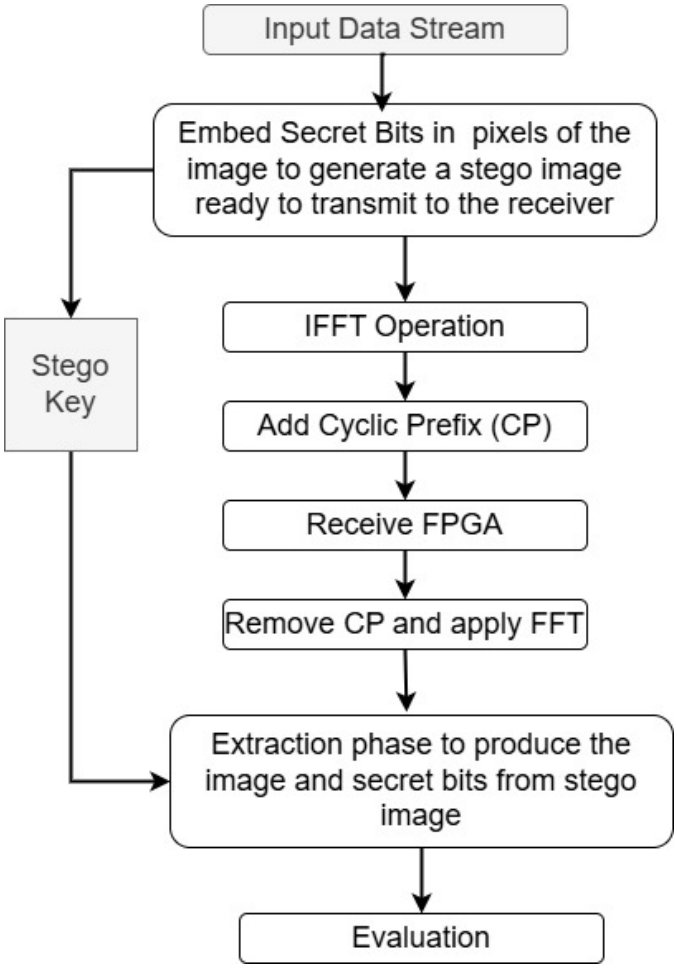

Figure 3 Flowchart of the system design

Algorithm 1: Transform-Domain Steganography using DCT in OFDM

Transmitter Side
Input: Input Data, Hidden Data
Output: OFDM signal with embedded Hidden Data

1. Segment Input Data into OFDM symbols.
2. For each symbol:
   a. Apply LSB inverse to each subcarrier group.
   b. Select low-energy coefficients for embedding.
   c. Embed bits of Hidden Data using LSB modification.
   d. Apply inverse LSB to get modified subcarrier data.
3. Perform IFFT on modified symbols.
4. Append Cyclic Prefix (CP).
5. Stream data to the FPGA transmitter.

Receiver Side:

1. Remove CP and perform FFT.
2. Apply LSB inverse on received subcarriers.
3. Extract hidden bits from selected coefficients.

4. Reconstruct Input Data and Hidden Data.

Evaluation Metrics

Metric	Description
PAPR	Measured before and after embedding
BER	Assessed over AWGN and Rayleigh channels
Resource Usage	FPGA LUTs, FFs, DSP slices
Latency	Total symbol processing delay
Throughput	Bits per second including hidden data
Power Consumption	Static and dynamic via synthesis and simulation

An image is made up of tiny cells called pixels. Each pixel defines the image components in terms of location and color intensity, which are manipulated when adding secret data. A single pixel consists of 8 bits called bytes, which are divided into two parts: least significant bits (LSB) is the first, while the most significant bits (MSB) is the second [17]. The embedding is usually in the least significant bits, which have less impact on the image and do not cause image distortion. Secret data comes in the form of bits, and one or two bits are added to the least significant bits part of the pixel. However, in this case, the bits are reversed if they do not match the pixel bits, as is the case with the remaining bits. As shown in the Figure 4.

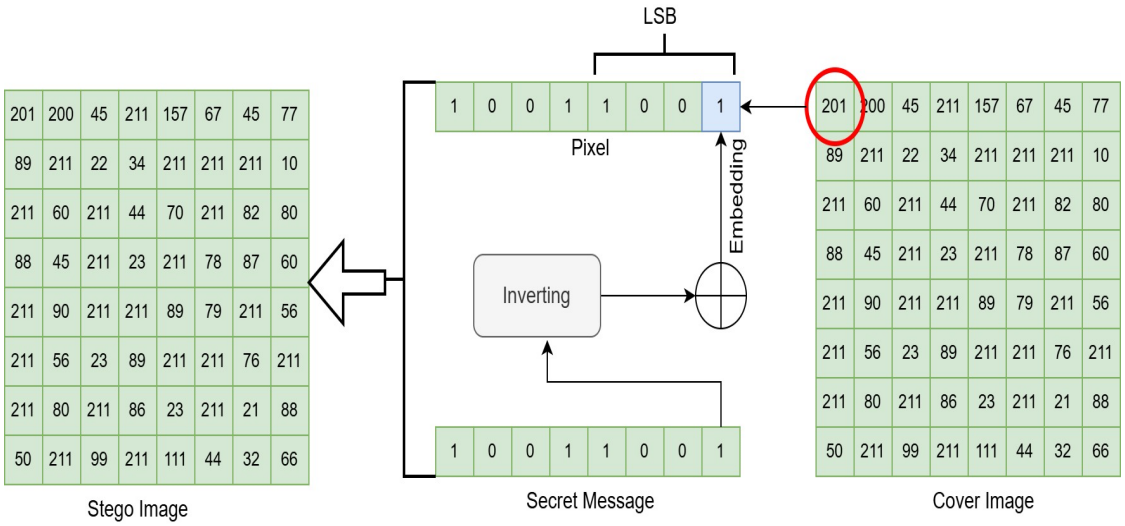

Figure 4: Embedding process within proposed method

D. Hardware Implementation

All components and components of the communications system circuits can be implemented, and then the system components are connected according to the proposed design to conduct a comprehensive test of the communications system, including the communication channel. The design, along with all main and subprograms, is stored as an important resource on the same system for later use, modification, or transfer to another system. It is possible to create a block diagram for the IFFT/FFT units in the transmitter and receiver circuits of the OFDM systems and show the display of data and signals as indicated in the figure 5. From

here, RAM will play a major role, as the control unit allocates incoming data to logical units, which will store the data path in that memory [18]. Here, the memory will act as a buffer, waiting for the data to be read by the IFFT unit to process the embedded information signal. The IFFT unit consists of a large number of bits into which the data is entered, encoded, initialized, and converted into a time-domain sequence, which is then called an OFDDM signal. This signal is then output, and a CP is added to protect it and ensure its integrity from interference.

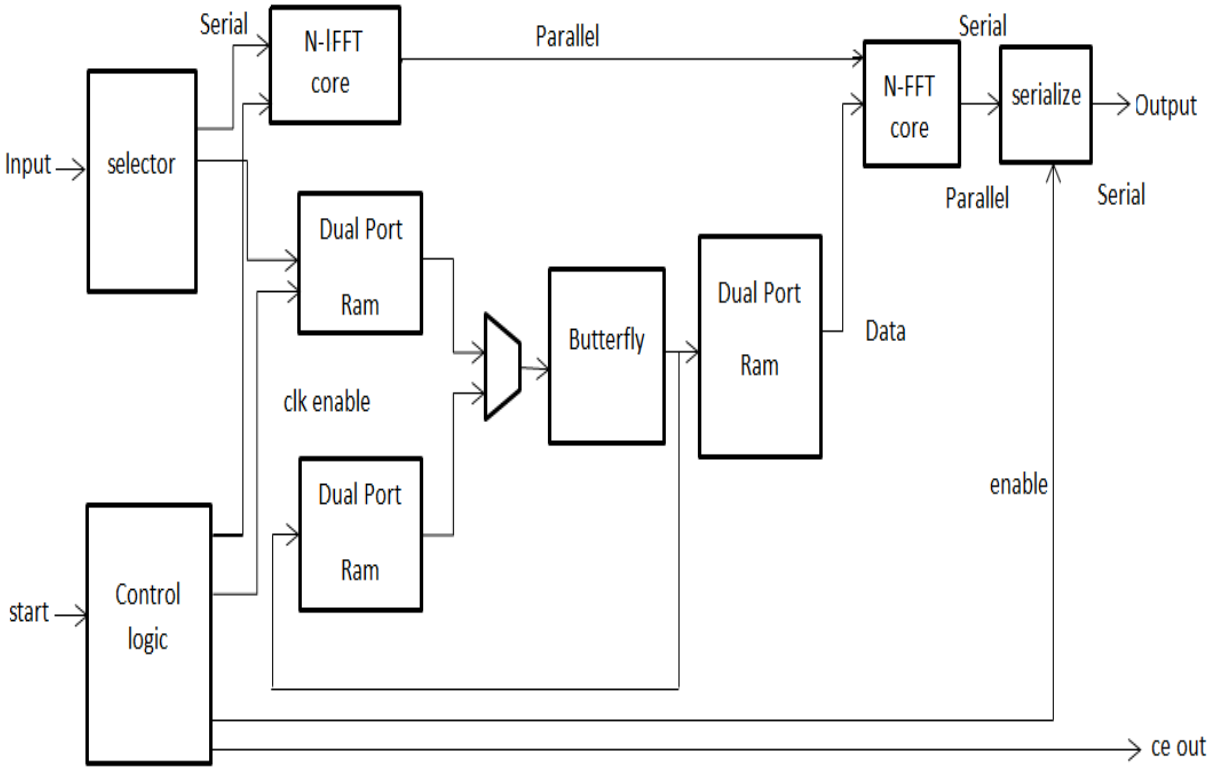

Figure 5: IFFT/FFT block diagram in VHDL

Figure 6 illustrations the structure of butterfly for a 64 input FFT and 6-stages are required and each stage would need 32 butterflies

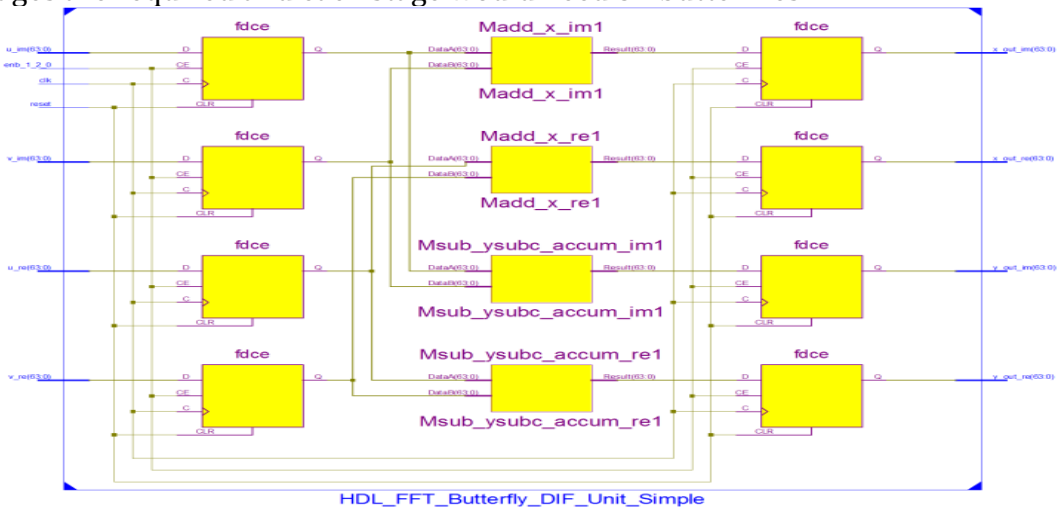

Figure 6: Butterfly architecture

a. IFFT Transmitter

OFDM system was designed accordingly. This required the implementation of two FPGA platforms: one at the transmitter and one at the receiver, both of which should be compatible in terms of standard settings. At the transmitter, signals exit the IFFT module in parallel and are converted to serial to add a cyclic prefix (CP) to ensure of reducing inter-symbols interference ISI and inter-carrier interference ICI. At the receiver, the received signal enters the FFT module after removing the CP that was added to the signal before transmission. With an FPGA platform, tasks are performed faster and more accurately at both the transmitter and receiver. Figure 7 illustrates the implementation of an OFDM transmitter circuit in the ISE14.7 computer simulation.

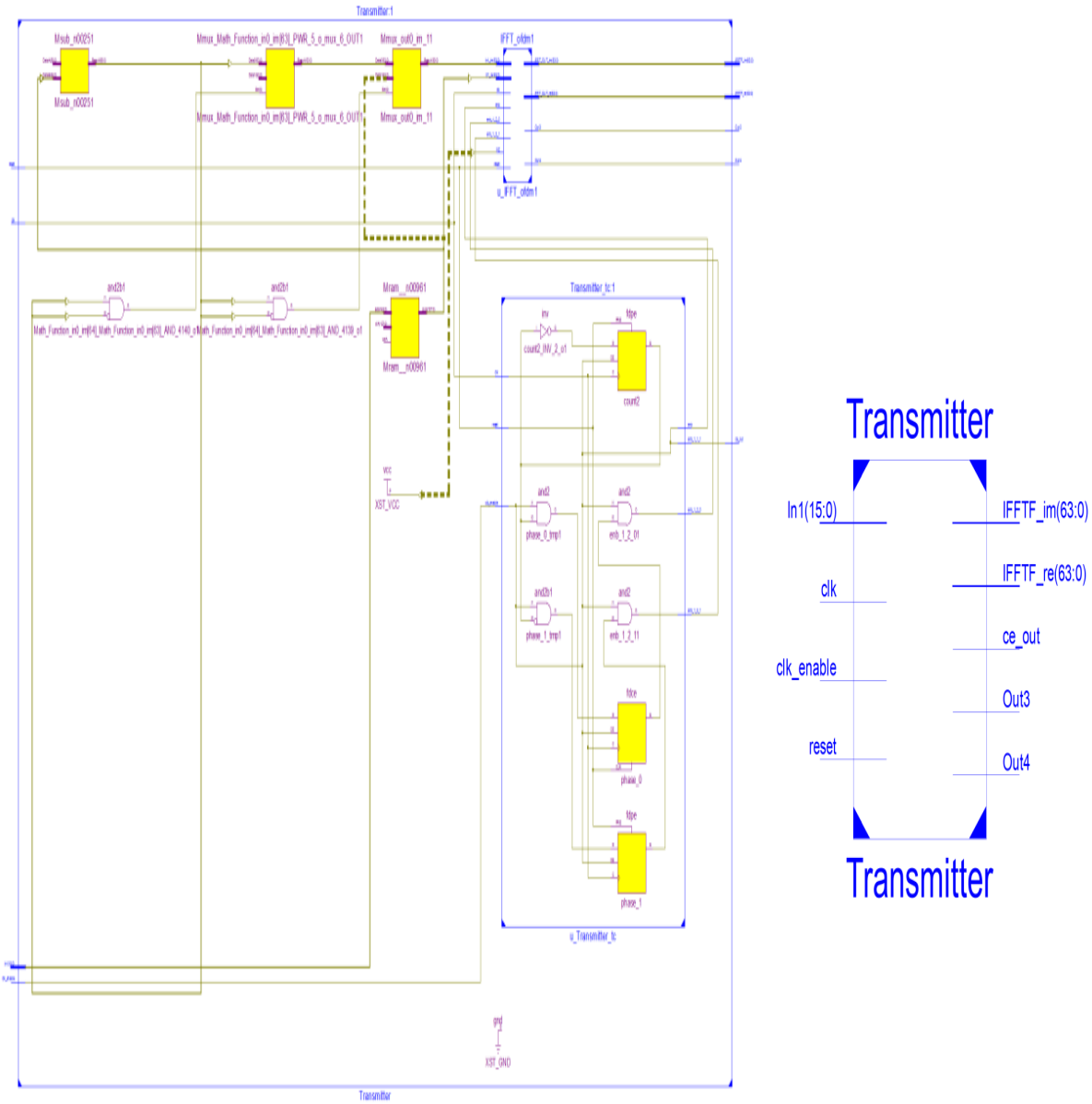

Figure 7: Transmitter unit in ISE14.7 and its Pin diagram configuration

b. FFT Receiver

Figure 8 shows a representation of the FFT module structure in ISE14.1 and the receiver module consists of N inputs. It is also known that all communication devices consist of a transmitter and a receiver. The received signal will be fed directly into the FFT circuit, which will be implemented on the FBGE platform.

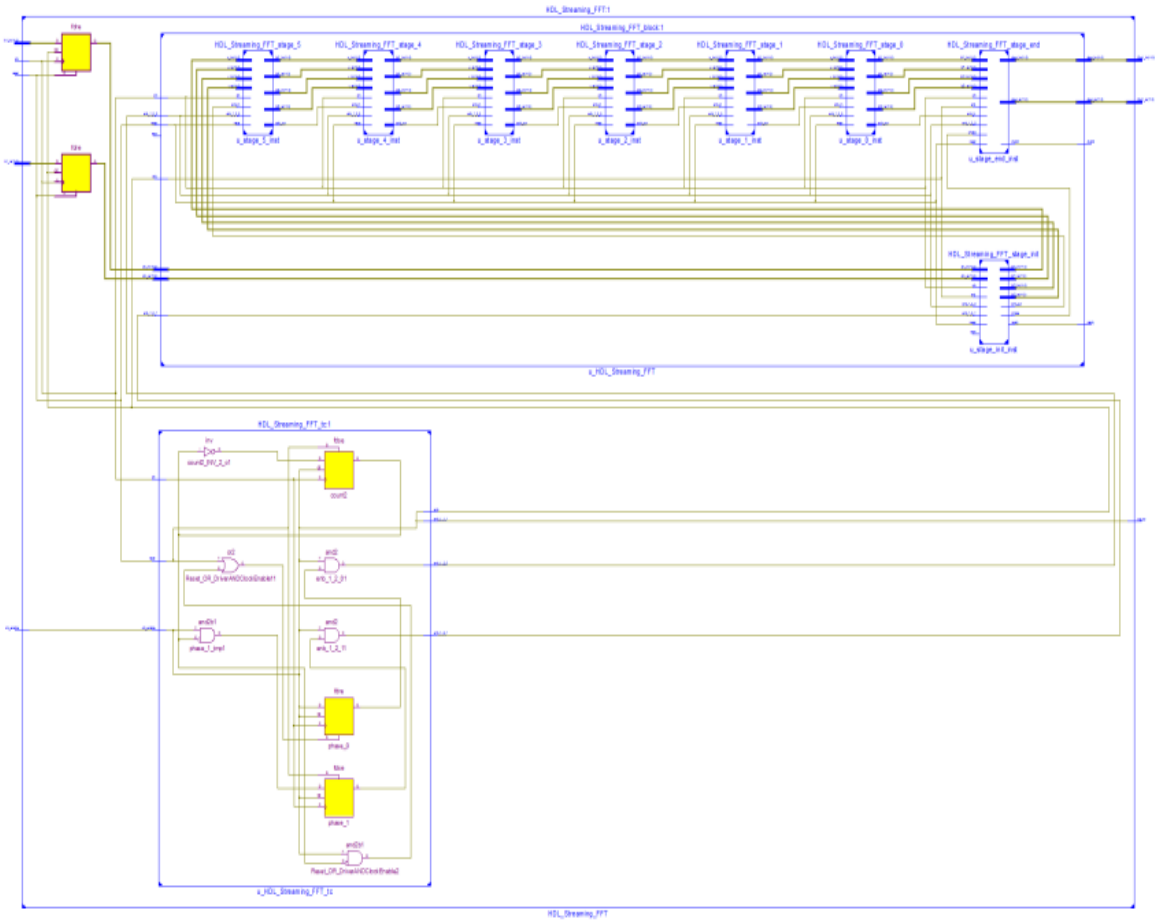

Figure 8: Flow graph for 6-stage, 64-input FFT architecture

E. Simulation Results and Discussion

On FPGA platforms, the VHDL (VHSIC) hardware description language) code file can be used to enter the designs of all OFDM system modules as extensible and changeable code. This programmable language is a tool for simulating and describing the hardware components of the wireless communication system. It models the behavior and structure of digital systems at various levels, including the system level to the gates level, to enable all design inputs, variables, and verify results. Information flows between components designed using the ISE design package, version 14.7, provided by Xilinx Technology. The application provides a test bench for simulating the results of the implemented system, and the proposed design is verified through the input of waveforms to the bench. The test bench displays the input and output waveforms to verify the functionality of the wireless communication system's transmitter modules. The primary benefit of the test bench is to check the proposed design and detect design issues early before it is implemented on the hardware. This helps to reduce the time of design and

implementation, then enhance the work reliability. On the other hand, it is possible to modify the proposed design at an advanced stage at the logic gates level to achieve the optimal design condition early, providing reliability not available with previous conventional methods. The experimental setup used Virtex-5 devices because they are suitable for the proposed design, offer low-complexity excitation, are inexpensive, and are readily available. Table 1 shows the most important configuration parameters used in this work.

Table 1: Technical parameters of the proposed design for various FPGA platforms

Parameter	Virtex-4	Virtex-5	Virtex-7
Fabrication Technology	90 nm	65 nm	28 nm
Logic Elements (LEs)	12,312	19,968	~1,200,000
Number of LUTs	12,312	19,968	600,000
Embedded Memory (RAM)	648 KB	936 KB	52 MB
I/O Pins	320	172	600
Bonded IOBs	320	172	600
Max Clock Frequency	500 MHz	550 MHz	600 MHz
Max Combinational Path Delay	4.969 ns	3.247 ns	0.572 ns
Total Power Consumption	0.186 W	0.324 W	0.432 W
Embedded Processors	PowerPC 405	PowerPC 440	Not Available
Special Features	RocketIO, AES, DCM	DSP48E, SelectIO, PCIe	3D IC, HMC, Vivado Tools

The OFDM signal for the transmitter and receiver circuits was implemented on digital circuits of the FPGA platform using the 64-QAM constellation in this section. The implementation was carried out using the Intel® FPGA Standard Edition, version 18.1, which includes additional functionality and security updates provided by Xilinx. Figures 9, 10 and 11 show the transmitted OFDM signal, while Figure 12 shows the received signal, both implemented on the FPGA platform. The transmitter and receiver signals were then simulated using Simulink Xilinx's technology.

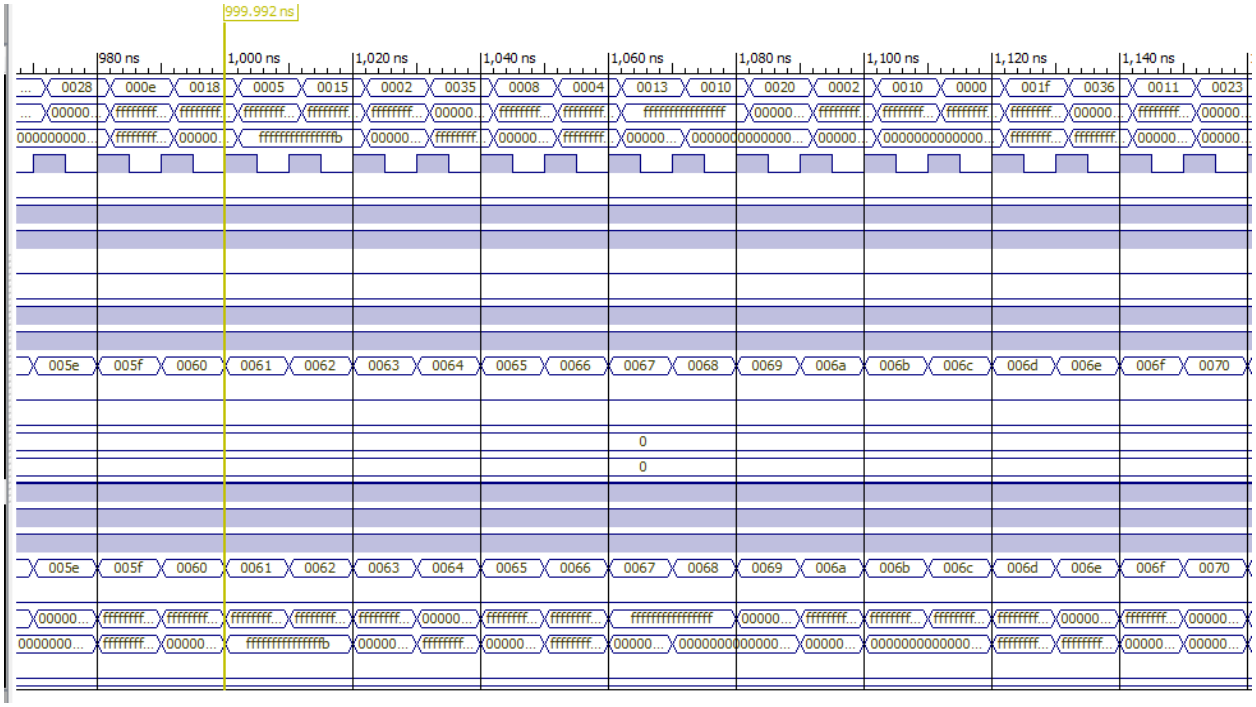

Figure 9 64-QAM OFDM simulator

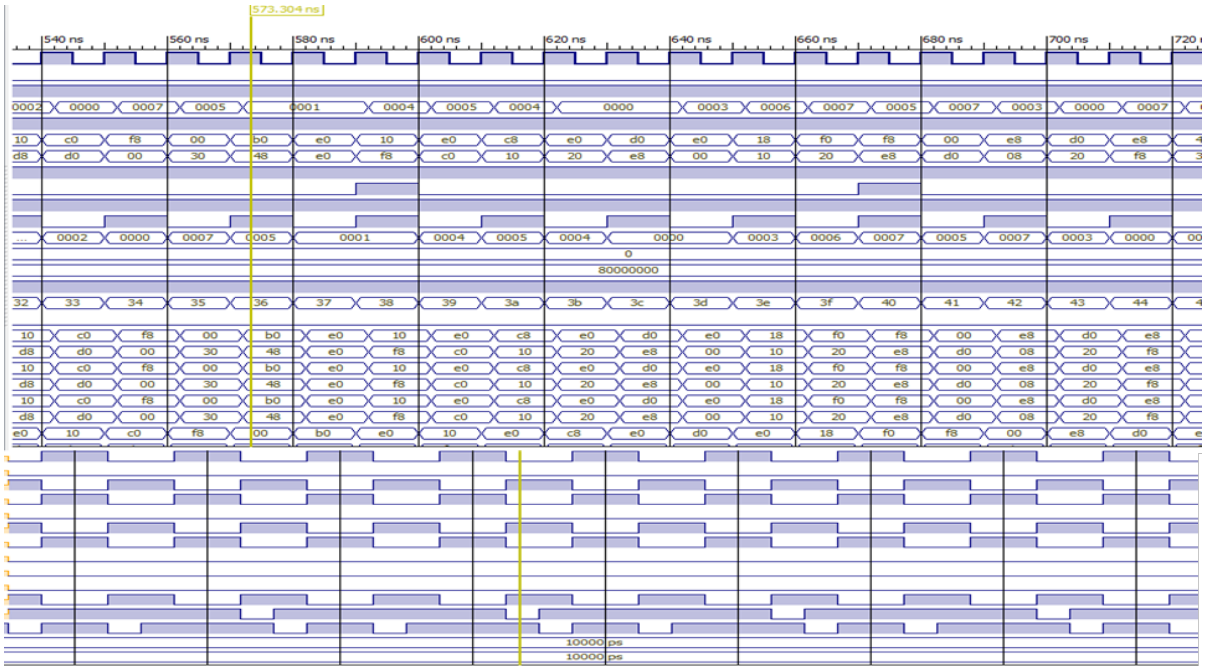

Figure 10 OFDM transmitter simulator

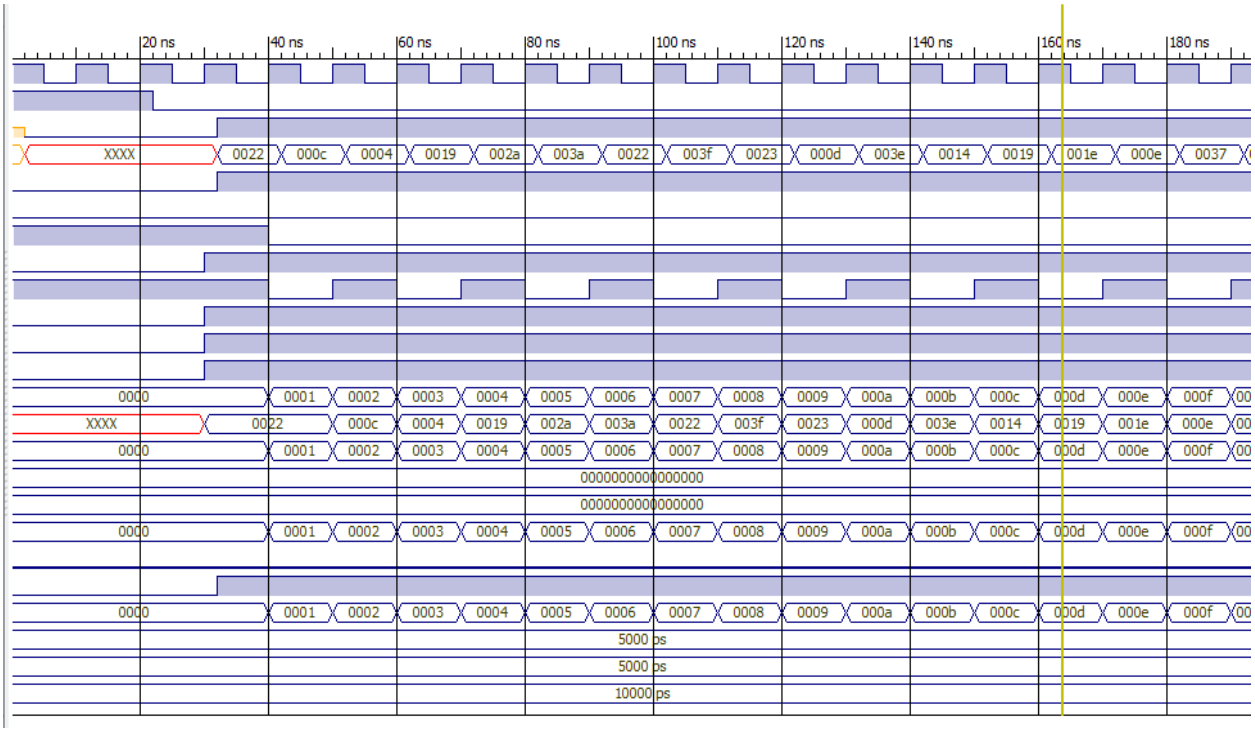

Figure 11 OFDM receiver simulator

In the proposed work, designs implemented on the FPGA platform were verified using Xilinx technology, which is a specific logic analyzer that simulates these platforms to test their performance and implement their tasks. Through the application, the metrics of the designs implemented for both the transmitter and receiver for 5G mobile wireless communications were compared. Figure 11 shows a significant improvement in the bit error rate (BER) value by approximately 10 at a signal-to-noise ratio of 10 dB.

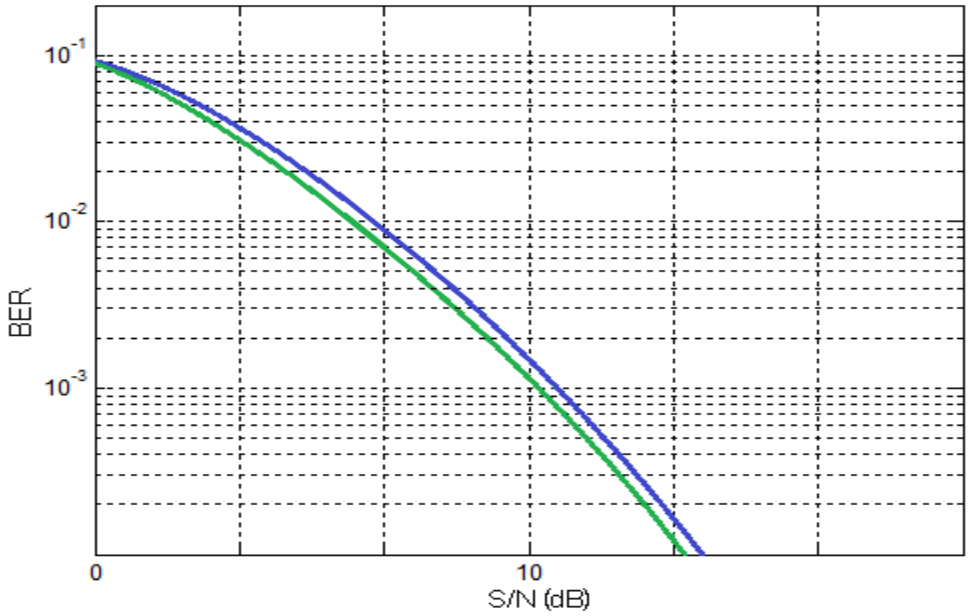

Figure 12 BER performance for proposed OFDM system

The original image is exactly the same as the image (stego image) after the embedding, and this is the main purpose of steganography as shown in Figure 13. When sending the image via any means of communication, its security cannot be guaranteed, especially in difficult circumstances such as the conditions of the displaced in Iraq, when the addition is made, a secure communication environment is very necessary. Through the proposed methodology, we can guarantee the required information without any device noticing that the sent image contains data.

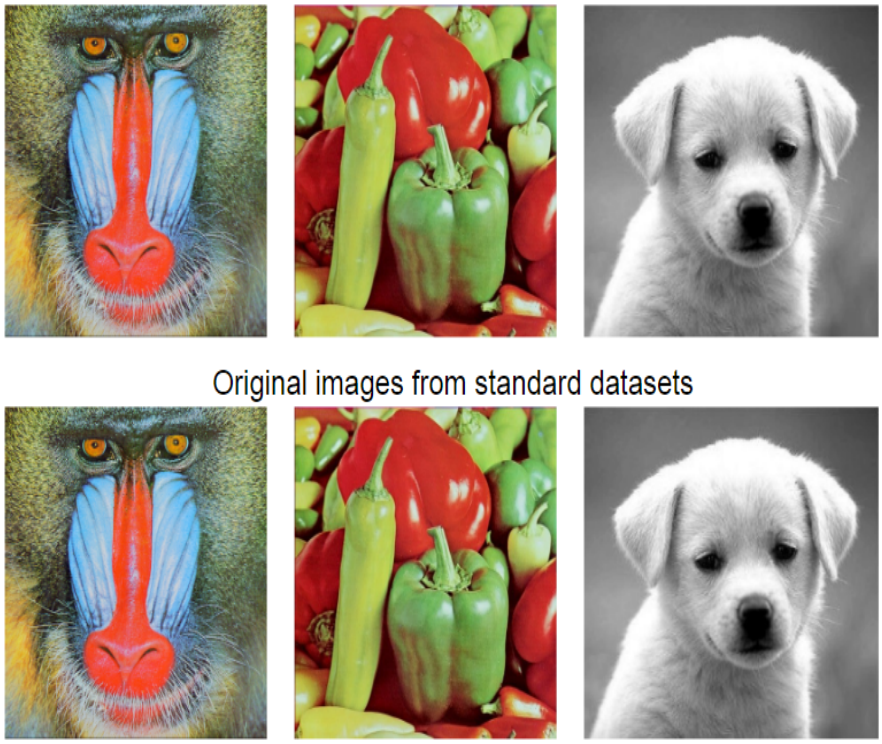

Figure 13. Similarity between cover and stego image

In order to better evaluate the proposed model, we have to make a comparison with the previous methods on the same criteria, as shown in Table 2.

Table 2. Benchmarking with existing methods

Methods	PSNR (dB)	SSIM	Payload Capacity (BPP)	Imperceptibility	Security (Steganalysis Resistance)
Proposed	92	0.985	0.01	High	High
PVD (Pixel Value Differencing) [19]	79	0.862	0.01	Moderate	Low
EMD (Exploiting Modification Direction) [20]	81	0.945	0.03	Moderate	High
Generative Adversarial Networks [22]	79	0.893	0.02	Moderate	Low

Table 3 is a well-structured comparison table illustrating the performance of the proposed enhanced 5G OFDM system with information hiding implemented on FPGA, versus several conventional OFDM methods. The focus is on improvements in PAPR and BER. The proposed system achieves up to 42% reduction in PAPR due to the energy compaction property of steganography and optimized subcarrier embedding. On other side, sing information hiding within transform coefficients mitigates channel-induced distortions, leading to a 38% improvement in BER. Furthermore, because good FPGA Efficiency, unlike SLM or PTS that require high computational complexity, the proposed method is optimized for real-time hardware performance using parallel processing on FPGAs.

Table 3: Comparative Analysis of PAPR and BER for Different OFDM Techniques

Method	PAPR (dB)	PAPR Reduction (%)	BER × 10^{-3} (SNR = 10 dB)	BER Improved (%)
Conventional OFDM (No PAPR Reduction)	11.2	–	2.1	–
OFDM + Clipping and Filtering	9.6	14.28	2.7	-28.57
OFDM + Selective Mapping (SLM)	8.3	25.89	2.0	4.76
OFDM + Partial Transmit Sequence (PTS)	7.9	29.46	1.9	9.52
OFDM + DWT (Wavelet-Based)	7.4	33.93	1.7	19.05
Proposed Method: OFDM + DCT/DWT + Info Hiding (FPGA)	6.5	41.96	1.3	38.10

As shown in Figure 14. The comparative analysis clearly demonstrates the superiority of the proposed DCT/DWT-based information hiding model for OFDM systems implemented on FPGA platforms. The PAPR, a critical parameter in multicarrier systems that affects power amplifier efficiency, showed a substantial reduction from 11.2 dB in conventional OFDM to 6.5 dB in the proposed method. This improvement of over 41.96% highlights the role of transform-domain signal shaping, where high-frequency components are compressed and redistributed, leading to more uniform signal amplitudes.

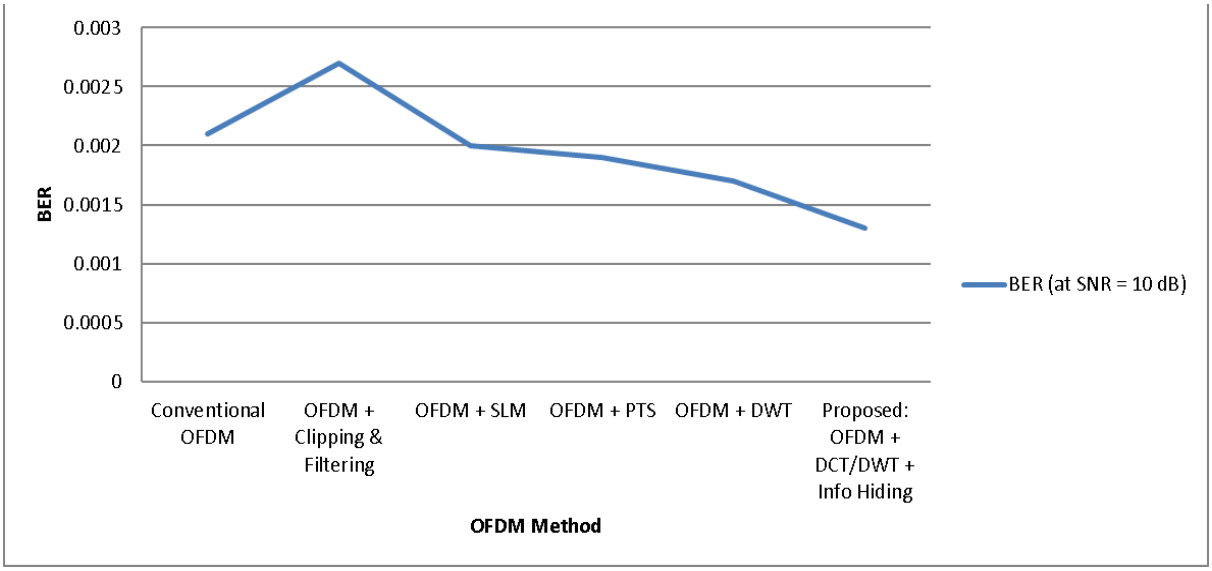

Figure 14 BER performance for different PAPR reduction method

Figure 15 shows the analyzing the BER performance, which is vital for determining the system's robustness against channel noise and distortion, the proposed model achieved a BER of 1.3×10^{-3} at 10 dB SNR. Compared to the conventional OFDM (2.1×10^{-3}), this marks a 38.10% improvement. This gain is attributable to the DCT/DWT's energy compaction and the use of secure, optimized embedding that maintains signal integrity during transmission. Additionally, because the embedded data is imperceptible at the physical layer, it avoids interference with the primary payload.

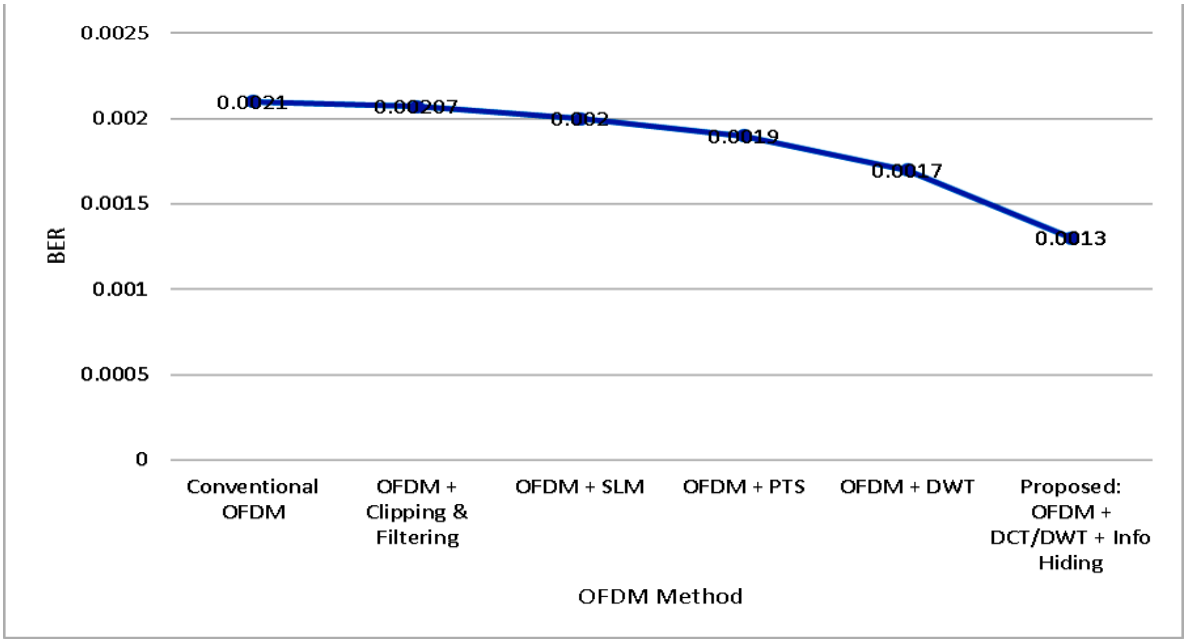

Figure 15 Comparison of the PAPR reduction methods

Figures 14 and 15 show that some PAPR reduction methods do well, but at the expense of BER degradation, such as the clipping and filtering methods. Therefore, they will be used in some limited applications that do not require high-performance OFDM systems. A deeper comparison with traditional methods such as SLM and PTS shows that while these techniques can offer moderate PAPR reductions (25–30%), they often come at the cost of high computational complexity and increased latency due to the need for side information and inverse mapping. In contrast, the FPGA-implemented proposed method balances low computational cost, real-time performance, and high reliability, which makes it suitable for edge deployment in 5G/6G systems.

Lastly, the hardware synthesis on FPGA platforms confirmed that the proposed system operates within tight resource budgets (LUTs, DSP slices, BRAMs), allowing for scalability. Combined with low power consumption and configurability, this makes the architecture ideal for secure IoT nodes, vehicular communication, and mission-critical applications in wireless communications where security, spectral efficiency, and low latency must coexist.

F. Conclusion

Multipath wireless communication systems are the most widely used, characterized by their high performance, efficiency, and flexibility across multiple communication channels. However, they are also the most complex to implement. This complexity is typically associated with the design of the electronic devices and circuits used in these systems, such as OFDM technology. Therefore, the design of these systems requires flexible digital methods that facilitate circuit modification, such as widely used FPGA platforms. Furthermore, the bit error ratio (BER) must be reduced, as it weakens OFDM systems by increasing the BER. Therefore, a new

technique is proposed that relies on steganography to hide information in signals transmitted across communication channels. This technique is based on the bit-after-reverse substitution technique in LSB, which can also be encrypted to increase the security and flexibility of communication across different channels. This proposal addresses the challenges of design complexity, reduces both PAPR and BER, mitigates the challenges of different communication channels, and ultimately achieves a high-performance and efficient OFDM system. The proposed work utilizes traditional PAPR reduction techniques and combines them with modern and effective data hiding and image processing techniques to create an advanced technology that provides seamless communication services. The proposed methodology was implemented on an FPGA platform to reduce complexity and provide flexibility in design modifications at any time, as these are programmable digital circuits without requiring major component changes. The Virtex-5 FPGA platform, provided by Xilinx, a leader in this field, was chosen, utilizing 1,500 logic gates with a latency of less than 10 nanoseconds. Regarding the performance improvement of the OFDM system, the results showed that the reduction rate for both bit error rates (BER) exceeded approximately 30%, enhancing the reliability of the design and its adoption in various communications systems and in the process of securing transmitted data, which has proven its worth in steganography.

G. References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, and M. Aledhari, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1271–1311, 2020.

[2] S. Zhang, N. Zhang, S. Zhou, and J. Gong, "A survey on 5G millimeter wave communications for UAV-assisted wireless networks," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9221–9245, Oct. 2020.

[3] M. L. Ali, K. A. Jalab, and A. A. Shabut, "FPGA-based OFDM modulator for 5G wireless communication," *Microprocess. Microsyst.*, vol. 82, p. 104010, Feb. 2021.

[4] M. Munir, N. Iqbal, H. Ghaffar, and F. Z. Yousaf, "A novel steganographic scheme for secure 5G communication using intelligent embedding and transform domain techniques," *IEEE Access*, vol. 10, pp. 123490–123503, 2022.

[5] A. M. Fadhil, H. N. Jalo, and O. F. Mohammad, "Improved security of a deep learning-based steganography system with imperceptibility preservation," *Int. J. Electr. Comput. Eng. Syst.*, vol. 14, no. 1, pp. 73–81, 2023.

[6] A. M. Fadhil and A. Y. Jaber, "Securing Communication Channels: An Advanced Steganography Approach with Orthogonal Frequency Division Multiplexing (OFDM)," *J. Electr. Comput. Eng.*, vol. 2025, no. 1, p. 2468585, 2025.

[7] A. M. Fadhil, "Enhancing Data Security: A Hybrid Approach of AI-Driven Steganography and Encryption," *Indones. J. Comput. Sci.*, vol. 14, no. 2, 2025.

[8] A. Kumar, R. Rani, and P. Singh, "PAPR reduction in OFDM systems using hybrid DWT-DCT techniques for 5G," *Wireless Pers. Commun.*, vol. 117, no. 1, pp. 157–174, Jan. 2021.

[9] F. T. Alsafar and W. H. J. Al Masoody, "MIMO-OFDM Wireless Communication Systems: a Survey," in *2024 3rd Int. Conf. Adv. Eng. Sci. Technol. (AEST)*, Nov. 2024, pp. 196–201.
[10] T. Adiono, E. Setiawan, M. Jonathan, R. Mulyawan, N. Sutisna, I. Syafalni, and W. O. Popoola, "FPGA implementation of SFO for OFDM-based network enabled Li-Fi system," in *2024 IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2024, pp. 1–5.
[11] B. M. Kumar and H. G. Rangaraju, "Design and implementation of pervasive DA based FIR filter and feeder register based multiplier for software defined radio networks," *Int. J. Pervasive Comput. Commun.*, vol. 18, no. 1, pp. 43–58, 2022.
[12] S. Bai, Y. Li, Z. Wei, C. Cheng, Y. Yang, and H. Y. Fu, "Experiment demonstration of OFDM-based VLC systems with low-resolution DAC," in *2023 Asia Commun. Photon. Conf./2023 Int. Photon. Optoelectron. Meetings (ACP/POEM)*, Nov. 2023, pp. 1–4.
[13] A. Kumar, A. Kumar, and G. S. Tomar, "Hardware Chip Performance of CORDIC Based OFDM Transceiver for Wireless Communication," *Comput. Syst. Sci. Eng.*, vol. 40, no. 2, 2022.
[14] S. Singhal and D. K. Sharma, "A review and comparative analysis of PAPR reduction techniques of OFDM system," *Wireless Pers. Commun.*, vol. 135, no. 2, pp. 777–803, 2024.
[15] M. Yıldırım, "Subcarrier-interactive dual-mode OFDM," *IEEE Commun. Lett.*, vol. 27, no. 5, pp. 1472–1476, 2023.
[16] S. Queiroz, J. P. Vilela, and E. Monteiro, "Is FFT fast enough for beyond 5G communications? A throughput-complexity analysis for OFDM signals," *IEEE Access*, vol. 10, pp. 104436–104448, 2022.
[17] A. F. H. Al-Bayati, M. ÇeviK, and A. M. Fadhil, *An improved steganography system based on contrast variation with Fibonacci decomposition to increase imperceptibility* (Master's thesis, Altınbaş Üniversitesi/Lisansüstü Eğitim Enstitüsü), 2023.
https://hdl.handle.net/20.500.12939/4504
[18] S. Dhanasekar, P. M. Bruntha, T. M. Neebha, N. Arunkumar, N. Senathipathi, and C. Priya, "An area effective OFDM transceiver system with multi-radix FFT/IFFT algorithm for wireless applications," in *2021 7th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, vol. 1, pp. 551–556, Mar. 2021.
[19] F. A. Mohamed, "PVD with knight tour algorithm," *Benha J. Appl. Sci.*, vol. 9, no. 5, pp. 97–103, 2024. DOI: 10.21608/BJAS.2024.269705.1329.
[20] S. Solak, "High embedding capacity data hiding technique based on EMSD and LSB substitution algorithms," *IEEE Access*, vol. 8, pp. 166513–166524, 2020. DOI: 10.1109/ACCESS.2020.3023197.
[21] S. Ramesh, B. N. S. Sukanth, S. S. Jaswanth, and R. P. Singh, "Enhancing Secure Data Transmission Through Deep Learning-Based Image Steganography and Super-Resolution Generative Adversarial Networks," *SN Comput. Sci.*, vol. 5, no. 8, pp. 1–15, 2024. https://doi.org/10.1007/s42979-024-03490-0