Received: January 28, 2021. Revised: March 11, 2021. 56

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Low area FPGA Implementation of Secure MIMO OFDM based Wireless ECG Signal Transmission

Santhosh Kumar Kenkere Basavaraj[1]* **Bangalore Ramchandra Sujatha[1]**

[1]*Department of Electronics and Communication Engineering, Malnad College of Engineering, Hassan, India*
* Corresponding author's Email: kbs@mcehassan.ac.in

Abstract: Multiple-Input Multiple-Output Orthogonal Frequency Division Multiplexing (MIMO-OFDM) is widely used to provide high speed data transmission and spectrum efficiency in modern wireless communication systems. Specifically, the transmission of Electrocardiogram (ECG) signal plays a main role in health monitoring systems. The privacy and security of the patient identification and medical records are considered as a main concern in health monitoring systems. In this paper, the Lightweight cryptography (LWC) is proposed to secure the ECG signal transmission from unauthorized users through the MIMO-OFDM system. The LWC is mainly used to minimize the amount of logical elements using the gate level architecture and simple key schedule in the MIMO-OFDM. The turbo code is used in MIMO-OFDM is due to its error correcting capacity that minimizes the amount of error caused during communication under the constraints of burst error and Inter Symbol Interference (ISI). Here, the ECG signals from the MIT arrhythmia database is used to analyse the secure ECG signal transmission of LWC-MIMO-OFDM method. The performance of the proposed LWC-MIMO-OFDM is taken by means of area, delay, power, number of slices, flipflops and LUTs. The LWC-MIMO-OFDM method is compared with Advanced Encryption Standard (AES) to evaluate the efficiency of LWC-MIMO-OFDM. The delay of the LWC-MIMO-OFDM for Virtex 5 device is 13.3ns, it is less when compared to the delay caused by the AES.

Keywords: Electrocardiogram signal, Inter Symbol interference, Lightweight cryptography, Multiple input multiple output, Orthogonal frequency division multiplexing, Turbo code.

1. Introduction

Multi-Input Multi-Output-Orthogonal Frequency Division Multiplexing (MIMO-OFDM) is considered as an evolving technique to support the high performance and higher data rate under diverse fading channel conditions [1, 2]. The MIMO uses multiple antennas in both the transmitter and receiver to deliver high throughput and the throughput of MIMO is high when compared to the single input single output. Subsequently, the OFDM is combined with the MIMO, because of the flat fading feature obtained based on the narrowband sub-carrier signals [3]. Additionally, the OFDM is used to reduce multiuser and inter-carrier interference as well as it provides multi user channel access [4]. The major components in the OFDM are Fast Fourier Transform (FFT) and Inverse FFT (IFFT) which is used to design an appropriate FFT processor. This FFT processor is used to support the different data points (FFT/IFFT sizes) in the MIMO-OFDM wireless communication systems [5]. In time-varying and frequency-selective channel environments, the channel response is precisely estimated by MIMO-OFDM. The spatial domain and frequency-domain diversities are provided by the MIMO-OFDM enhance the spectrum efficiency [6, 7]. But, the main requirement of MIMO-OFDM is precise frequency synchronization among the receiver [8, 9].

In MIMO channel, the theoretical capacity limits are obtained using the capacity-approaching code with turbo decoding in the receiver [10]. In receiver antenna, the transmitted data streams are separated from the received signals using the MIMO decoder at receiver components [11]. The channel coding is generally related to the different configuration options and parameters such as communication

channel, signal-to-noise ratio, frame size and so on [12]. The transmission of ECG signal is important in modern wireless communication system to monitor the patient with cardiovascular diseases [13]. Moreover, the possibility of retrieving the ECG signals by the adversary is high, when the ECG signal is not secured based on the cryptographic processor. Therefore, the ECG signals are encrypted using the dynamic binary key stream that used to obtain secure medical signal transmission [14]. Subsequently, an appropriate security is provided to the communication system using the light-weight block ciphers [15].

The major contributions of this research paper are given as follows:

- The ECG signal transmitted in the MIMO-OFDM is secured using the LWC. Here the LWC is used due to its lesser utilization of logical elements. Thus leads to minimize the area occupied by the overall MIMO-OFDM system.
- The turbo coding method is accomplished in the MIMO-OFDM to overcome the fluctuations caused while transmitting the ECG signal.
- The frequency interleaving and insertion of guard interval are used to overcome the burst error and ISI caused during communication. This helps to minimize the packet loss through the MIMO-OFDM system.

The overall organization of the paper is given as follows: the related works about the FPGA based MIMO-OFDM, secure ECG signal transmission is given in Section 2. The problems identified from the literature survey and solutions to overcome the problem are stated in Section 3. The detailed description about the MIMO-OFDM with turbo coding and LWC cryptography are given in Section 4. The results and discussion of the proposed LWC-MIMO-OFDM are described in Section 5. Finally, the conclusion is made in Section 6.

2. Related works

K.S. Pandian, and K.C. Ray [14] presented the Dynamic Hash Key (DHK) using nonlinear feedback function (NLFF) based cipher for protecting the data integrity of ECG signal. The Non-Singular Sequence Folding (NSSF) -based Toeplitz hash function was included in the key generation model. Next, the NSSF based key generation module was used to deliver the dynamic Hash Value (HV) as a master key which used to obtain the key scheduling in RC4. This NLFF based cipher was delivered higher key randomness by using NSSF. However, the NLFF based cipher was required of high amount of logical elements due to the design of NSSF and Toeplitz function.

Z. Haider, K. Javeed, M. Song, and X. Wang [15] developed the integration of low-cost self-test architecture in the PRESENT cipher. The Self-Test PRESENT architecture (STPA) was reduced the hardware overhead by using two different key strategies. At first, the test response compaction was obtained by utilizing the hardware-efficient X-Compactor approach. Next, the PRESENT cipher core was reused as a test pattern generator. But this work was required some additional components such as comparator and Read-Only Memory (ROM) that increased the hardware utilization of the overall STPA architecture.

Delomier [16] presented an effective Low-Density-Parity-Check (LDPC) code by considering the behavioral models. Here, two different types of LDPC model were created for describing the inherent computational parallelism. An extended version of x86 LDPC decoder was the first LDPC decoder model. Moreover, the 1st model was optimized to generate the 2nd model. In 2nd model, the performance of hardware implementation was improved based on the parallelization behavior. The latency of the LDPC code was not minimized, even there was an increment in the operating frequency.

Lin and Shen [17] developed the FFT processor to support the two different sizes of data stream from 64 to 2048 symbols for MIMO-OFDM systems. In MIMO-OFDM, the data-processing sequence was used to process the data stream at time-multiplexing manner. Moreover, the memory elements were shared among the processing stages by using reorder mechanism. The utilization of multipliers was effectively improved based on the data processing technique. The area of the MIMO-OFDM was increased, due to utilization of the high amount of logical elements such as complex multipliers, butterfly unit, dual-port SRAM, two-port register file and shift-and-add circuit.

Lara-Nino [18] developed the architecture of PRESENT that is a standardized lightweight cipher. The developed PRESENT architecture was used to overcome the security issues under highly constrained environments. This work used two different strategies to generate a round-keys such as 1) 80 bit input keys were processed and round keys are produced using the standard logic and 2) 128 bit input keys were processed and round keys were produced by using the standard logic. The maximum frequency for 16-bit architecture with 128-bit keys was less when compared to the PRESENT with 80-bit keys. The key given to the system was manually generated by the generator module and it can be

easily predicted by hackers which affects the system performances.

Anghel [19] developed the FPGA design of the turbo decoder for 3GPP Long-Term Evolution (LTE) standard. Here, the parallel decoding scheme was developed with only one interleaver based on the features of block memory and polynomial interleaver properties of quadratic permutation. Moreover, the latency of the parallel decoding was less, when compared to the serial decoding method. The performance degradation was occurred due to the utilization of parallel decoding in the 3GPP LTE standard.

Kumar and Karthigaikumar [20] presented the modified key expansion architecture in the AES architecture to obtain the encryption and decryption of ECG signals. In modified key expansion architecture, the whole AES was separated into two blocks that are parallely executed to accomplish the encryption process. Moreover, the temporary word was formed in each generation of subkey. The operation of byte transition was provided in the temporary word to improve the security. However, the area and power consumption of the modified and conventional AES architecture was same, because the modified AES architecture was not optimized while delivering the security.

The existing methods has various disadvantages such as higher latency, higher hardware utilization and less security against the attackers. However, the LWC-MIMO-OFDM method uses only less logical elements due to its LWC encryption and decryption process which minimizes the delay during the communication through the MIMO-OFDM system. Additionally, the transmission of ECG signal is secured using the LWC method.

3. Problem Statement

The issues found from the existing researches along with its solution are given as follows:

The latency of the LDPC code is not minimized with the higher operating frequency, which shows the delay of the coding scheme is high while correcting the codes [16]. The MIMO-OFDM system with huge amount of logical elements increases the area occupied by the communication model [17]. The PRESENT architecture is vulnerable by the attackers, due to the manual generation of keys obtained in each clock cycle [18]. The area and power of the modified AES architecture are similar to the conventional AES architecture, due to its parallel execution and key expansion architecture [20]. Therefore, the power consumption of the architecture is high, when the respective architecture contains a huge amount of logical components.

Solution:

In this proposed method, the number of logical elements used in the LWC method is minimized due to its gate level architecture and simple key schedule. The developed LWC method is used to accomplish the secure ECG signal transmission over the MIMO-OFDM system. Here, the secure ECG signal transmission is achieved by alias identity, hash function of LWC and turbo encoder. The lesser hardware utilization in the MIMO-OFDM system minimizes the power and delay during communication.

4. Proposed System

In this proposed method, a secure ECG signal transmission is accomplished through the MIMO-OFDM system. The LWC based encryption and decryption is developed to avoid the access of ECG signal by unauthorized user. The design of the LWC

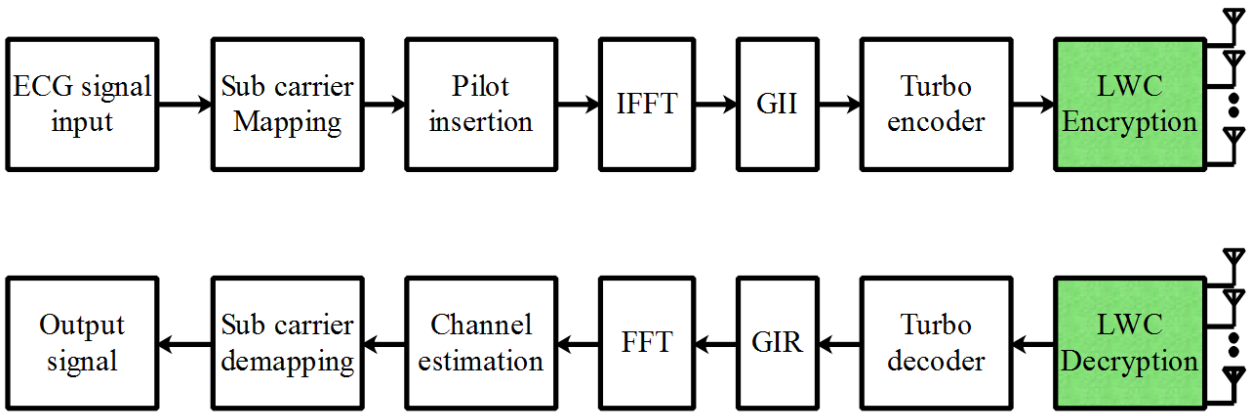

Figure. 1 Block diagram of the proposed method

is used to minimize the amount of logical elements in the MIMO-OFDM. The amount of error caused in ECG signal is minimized by using the turbo coding method. Moreover, frequency interleaving and guard interval are used to avoid the burst error and ISI during the communication. The block diagram of the proposed method is presented in the Fig. 1.

4.1 System model

In the MIMO-OFDM, the OFDM bandwidth is separated into P_{FFT} sub bands for P_{FFT} sub-carriers, where the size of Fast Fourier Transform (FFT) for OFDM demodulation is specified as P_{FFT}. The received signal vector of each sub-carrier for MIMO-OFDM is expressed in the Eq. (1).

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

where, the input signal vector (i.e., ECG signal) is represented as $x = [x_1, x_2, \dots, x_P]^T \epsilon\, A^P$ as well as the input signal is transmitted by P amount of antennas and it is faded by the $P \times Q$ MIMO channel of H. The constellation points generated by Quadrature Amplitude Modulation (QAM) modulation scheme is represented as$A$. Where, $A = \left\{\pm\frac{1}{2}a, \dots, \pm\frac{\sqrt{M}-1}{2}a\right\}$ is the constellation points for M-QAM modulation and a is the power normalization factor. Moreover, the binary error caused in the MIMO-OFDM system is n along with the variance of $\sigma^2 \epsilon \mathbb{C}^Q$, where $\mathbb{C}$ represents the complex number. The received signal vector obtained by the Q receiving antenna is $y = [y_1, y_2, \dots, y_Q]^T \epsilon\, \mathbb{C}^Q$.

The main steps processed in the LWC-MIMO-OFDM are given as follows:

4.1. Initially, the ECG signal from the MIT arrhythmia database [21] is converted into .txt file using MATLAB and this .txt file is loaded in the memory of the VLSI architecture.

4.2. The ECG samples from the .txt file are read and it is converted into serial to parallel as 8 bits. Then the converted 8 bit data are given to the mapper for accomplishing the sub carrier modulation.

4.3. The mapped data is given to the frequency interleaver to overcome the burst error. Because the user data is completely lost by burst error, when all user data are modulated and transmitted on the same wireless channel. This frequency interleaving is carried out for all users in the MIMO-OFDM.

4.4. After performing the frequency interleaving, the pilot insertion is used to identify the user's transmitted channel in the receiver.

4.5. The pilot inserted data is processed through the IFFT to convert the signal into the time domain. This time domain conversion is used to retrieve the data, even when the MIMO-OFDM is processed under fast and slow fading.

4.6. Next, the guard interval insertion is performed on the data to overcome the Inter

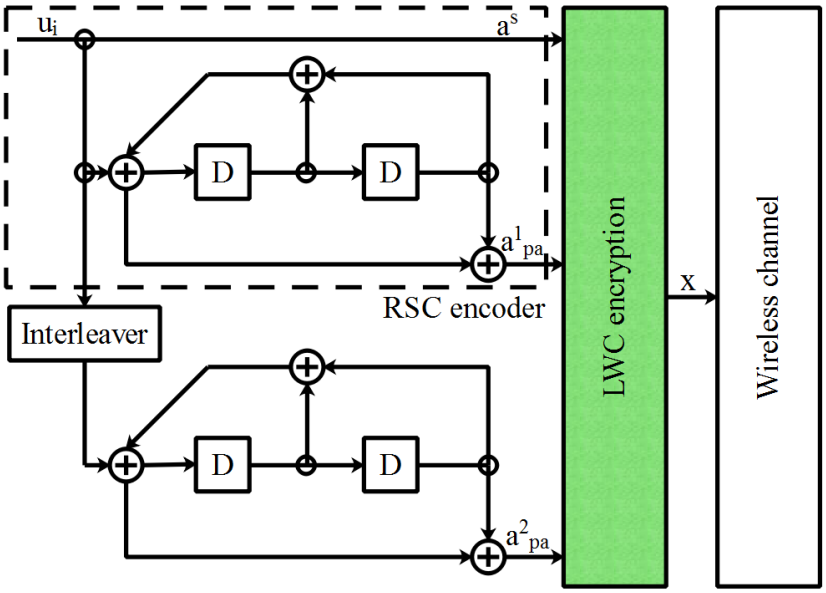

Figure. 2 Architecture of Turbo encoder

Symbol Interference (ISI). This ISI is caused when there is a packet collision in MIMO-OFDM and this ISI creates the packet loss.

4.7. The signal is again converted into parallel to serial and the converted data is given to the turbo encoder. The encoded data is encrypted using the LWC method that used to avoid the access of unauthorized user.

4.8. The encrypted data are transmitted to the receiver through the MIMO-OFDM system. Subsequently, the inverse processes such as LWC decryption, turbo decoding, Guard Interval Removal (GUR), FFT, channel estimation and sub carrier demodulation is carried out to obtain original ECG signal given on input.

4.2 Turbo encoder

After performing the guard interval insertion, the data (u_i) is given as input to the turbo encoder to obtain error correction. The turbo encoder designed in this proposed method produces 11-bit output along with the 7-bit input. The main component of turbo encoder is the parallel concatenation of two Recursive Systematic Convolutional (RSC) encoders.

The component codes of the encoder are divided by using the interleaver. In input, the symbol sequences ordering is permuted based on the interleaver and this interleaver generates the identical symbols with different temporal order. The error correction feature of the turbo encoder is improved by increasing the amount of parity bits at the output. The output of the turbo encoder is one systematic bit (a^s) and two parity bits (a_{pa}^1, a_{pa}^2). Then the output of the turbo encoder is concatenated as a single value and it is given as input to LWC based encryption as shown in Fig. 2.

4.3 Encryption using lightweight cryptography

The LWC based encryption is used in the MIMO-OFDM secure ECG signal. The encoded data from the turbo encoder such as a^s, a_{pa}^1 and a_{pa}^2 are concatenated and given as input to LWC encryption. The encryption of encoded data is carried out in two phases such as setup and authentication phase.

4.3.1. Setup phase

The setup phase operation for the LWC is performed through the secure channel. Initially, the device (P_i) in the MIMO-OFDM system transmits the device identity along with the response generated from the PUF. The random number $(rand)$ is used as input to obtain the response (Re) from the PUF which is shown in Eq. (2).

$$Re = PUF_{P_i}(rand) \tag{2}$$

Subsequently, a one-time alias identity (AID) generated by the server is shown in Eq. (3). The secret key (K_{ds}) is considered as 1st authentication factor to validate the authentication of the device M_i in the MIMO-OFDM system.

$$AID = h(Re||MK) \tag{3}$$

where, $h(.)$ represents the one way hash function and MK is the server's master key. The generated AID and K_{ds} are transmitted to the device P_i.

4.3.2. Authentication phase

The steps processed in the authentication phase to encrypt the ECG signal are given as follows:

4.3.2.1 Request for communication

Initially, the device selects the alias identity (AID), when the device (P_i) is required to communicate with the receiving antenna. The random number N_d is generated and calculates the $N_d^* = N_d \oplus K_{ds}$. Subsequently, the request message (Me_1) is composed by the device and it is transmitted to the receiving antenna for accomplishing the communication.

4.3.2.2 Response from server

The receiving antenna locates the AID, when the authentication request message (Me_1) is received in the MIMO-OFDM system. The server nonce N_e is generated and calculates the $N_e^* = K_{ds} \oplus N_e$ as well as the key hash response (i.e., encrypted data of turbo coder) is generated by using the Eq. (4).

$$x = h(N_d||K_{ds}||N_e^*||a) \tag{4}$$

where, the encoded data bit from the turbo encoder is represented as a. The response message (Me_2) is transmitted to the device, once the key hash response is generated in the receiver. The encrypted data of the turbo encoder are transmitted by using the MIMO-OFDM system.

4.4 Decryption using lightweight cryptography

The data bit y is received by using the Q amount of receiving antennas which are installed in the receiver end. If the response message (Me_2) is

received, the device acquires the PUF output and evaluates the key hash response. The decryption protocol is terminated, when the key hash response is not valid over the MIMO-OFDM system. if not, the receiving antenna is authenticated by the device and decodes the $N_e = K_{ds} \oplus N_e^*$. The decrypted value of encoded data of turbo encoder is shown in the Eq. (5).

$$b = h(N_e||k||R_{new}^*||hd^*||y) \tag{5}$$

where, key element is $k = FE.Rec(R, hd)$, $FE.Rec$ represents the reconstruction algorithm; helper data is $hd = h(K_{ds}||N_e) \oplus hd^*$; $R_{new}^* = k \oplus R'_{new}$, $R'_{new} = PUF_{P_i}(rand_{new})$, $rand_{new} = h(rand||K_i)$. After decoding the received data, it is given as input to the turbo decoder to obtain the input data bit given to the turbo encoder.

4.5 Turbo decoder

The output from the LWC decryption (b) is given to turbo decoder and it has 2 constituent Soft-In and Soft-Out (SISO) decoders in the serial concatenation scheme Moreover, the turbo decoding is performed by using the maximum a posteriori (MAP) algorithm. In two SISO decoder, the first SISO decoder is operated in sequential order (Phase1) and 2nd SISO decoder is operated in interleaved order (Phase2). The SISO decoder used in the turbo decoder is separated using the interleaver and deinterleaver. The input data are divided into three parts such as one systematic bit (b^s), parity bits (b_{pa}^1, b_{pa}^2) and output from previous decoder (L). The systematic bit is given as the first input, which is multiplied using the channel's reliability value. Similarly, the 2nd input i.e., parity-check bits also multiplied by using the channel's reliability value. The iterative decoding of turbo decoder is used to improve the error correcting performance. The Log Likelihood Ratio (LLR) and extrinsic information are the output of the turbo decoder. Next, the original data encoded by the turbo decoder are reconstructed based on the hard decision evaluated from the LLR of the second SISO decoder. The architecture of turbo decoder is shown in the Fig. 3.

4.5.1. MAP algorithm

The MAP algorithm used in the turbo decoder is formulated based on the Bayers rule and Markov model to calculate the decoded bit's reliability namely LLR. The LLR calculated from the MAP algorithm is expressed in the Eq. (6).

$$L(u_i) = \log\left(\frac{p(u_i = +1|\underline{b})}{p(u_i = -1|\underline{b})}\right) \tag{6}$$

where, the input data of the turbo encoder is u_i and the output data of turbo decoder is b. This MAP algorithm is used to obtain the original information bits, because the transmitted data bits using MIMO-OFDM is affected by the channel noise.

5 Results and discussion

The results and discussion of the proposed LWC-MIMO-OFDM method is described in this section. The LWC-MIMO-OFDM method is implemented and simulated in the Xilinx 14.4 software.

Additionally, the ECG signal acquisition and conversion of ECG signal into .txt file are done using the MATLAB 2018a software. The ECG signals used in this communication are acquired from the MIT arrhythmia database. The simulation parameters

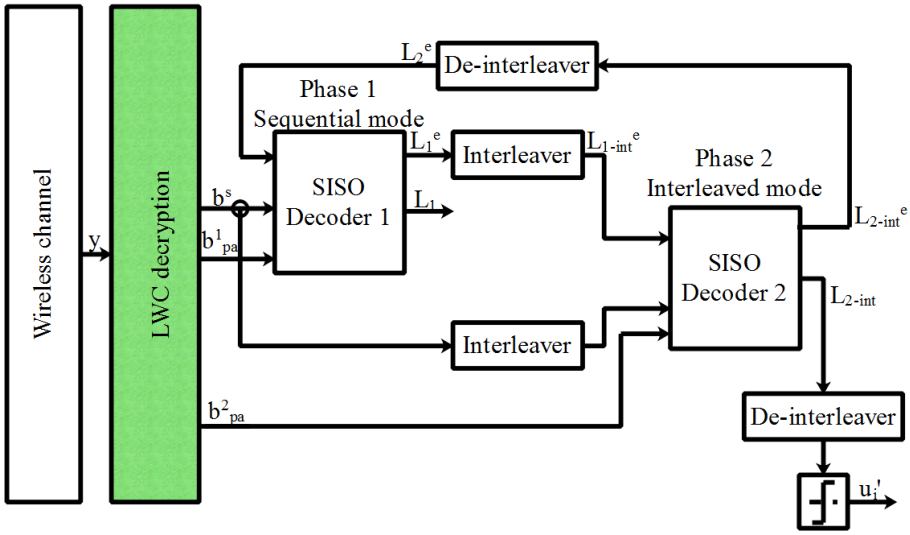

Figure. 3 Architecture of turbo decoder

Table 1. Simulation parameters

Parameter	Value
Number of transmitting antennas	4
Number of receiving antennas	4
FFT length	64
Cyclic prefix	64
Constellation mapping	QAM16
Symbols	64
Simulation time	10000ns

Table 2. Hardware utilization for Spartan 6 device

Family and Package: XC6SLX4 & TQG144			
Performances	**Available resources**	**Occupied resources**	**% of utilization**
Slice registers	11440	378	3%
Slice LUT	5720	1659	29%
Slices	1430	577	40%

Table 3. Hardware utilization for Virtex 4 device

Family and Package: XC4VFX12 & SF363			
Performances	**Available resources**	**Occupied resources**	**% of utilization**
Slice registers	10944	396	3%
Slice LUT	10944	1622	14%
Slices	5472	938	17%

Table 4. Hardware utilization for Virtex 5 device

Family and Package: XC5VLX20 & FF323			
Performances	**Available resources**	**Occupied resources**	**% of utilization**
Slice registers	12,480	475	3%
Slice LUT	12480	1180	9%
Slices	3120	376	12%

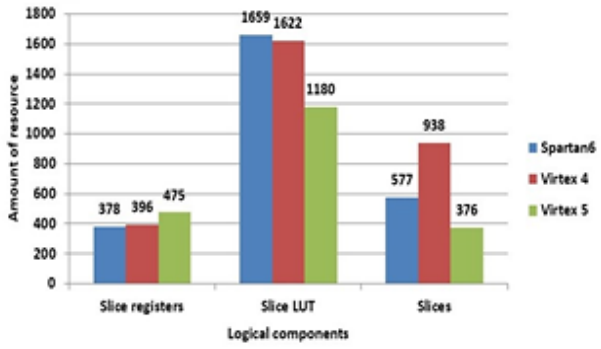

Figure. 4 Graphical illustration of Hardware utilization

considered for this MIMO-OFDM system is given in the Table 1.

5.1 Performance analysis

The secured ECG signal transmission is analysed with 4×4 MIMO-OFDM configuration. This shows LWC-MIMO-OFDM method analysed with 4 transmitting antennas and 4 receiving antennas

Table 5. Frequency, delay, and power analysis for different FPGA devices

FPGA device	Frequency (MHz)	Delay (ns)	Power (W)
Spartan 6	49.656	20	1.57
Virtex 4	71.898	13.9	1.42
Virtex 5	74.750	13.3	1.31

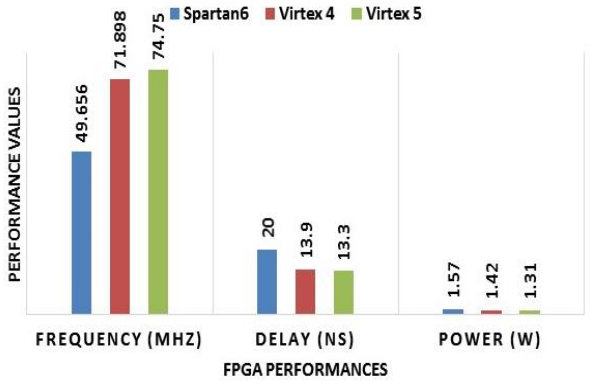

Figure 5. Graphical illustrations of frequency, delay, and power

for communication. The performance analysis of the proposed LWC-MIMO-OFDM method is analysed for three different FPGA devices such as Spartan 6, Virtex 4 and Virtex 5. These FPGA device family and packages are mentioned in Table 2, 3, and 4. The LWC-MIMO-OFDM method is evaluated by means of slice registers, slice LUT, Slices, frequency, and delay.

Fig. 6 shows the output waveform of LWC-MIMO-OFDM method which is obtained from the Modelsim software. The important signals present in the output waveform are *desired_in*, *signal_in* and *signal_out*. The signal given to the MIMO-OFDM transmitter is *desired_in* which is already modulated, encoded and encrypted ECG signal. Next, the data transmitted and received by the MIMO-OFDM receiver is *signal_in* . This *signal_in* is processed through the LWC based decryption, turbo decoder and QAM demodulation to generate the *signal_out* (i.e., Output signal). Additionally, the control signals used in the LWC-MIMO-OFDM method are *clk*, *rst* and *enable*.

The comparative analysis of the LWC-MIMO-OFDM method with existing AES [20] is described in the section. The AES [20] is designed and simulated for three different FPGA devices such as Spartan 6, Virtex 5 and Virtex 7. Here, the Table 6 shows the delay comparison of AES [20] with LWC-MIMO-OFDM for Spartan 6, Virtex 5 and Virtex 7 FPGA devices. Next, the graphical illustration of

Figure 6. Output waveform of LWC-MIMO-OFDM method

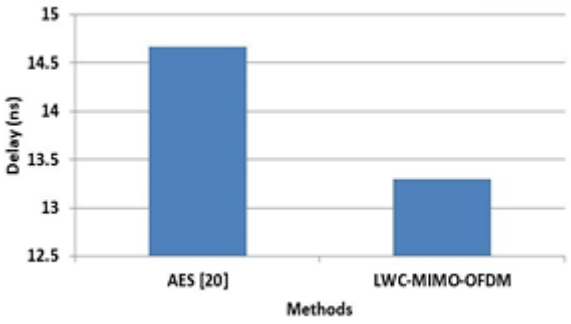

Figure 7. Graphical illustration of delay comparison

Table 6. Comparative analysis of delay

FPGA device & family	Methods	Delay (ns)
Virtex 5 XC5VLX20	AES [20]	14.668
	LWC-MIMO-OFDM	13.3
Spartan 6 & XC6SLX4	AES [20]	23.48
	LWC-MIMO-OFDM	20
Virtex 7 & XC7VX485	AES [20]	12.71
	LWC-MIMO-OFDM	10.25

Table 7. Comparative analysis of FPGA performances

FPGA device and family	Method	LUT	FF	Slices	Frequency (MHz)	Delay (ns)	Power (W)
Virtex 5 & XC5VLX20	DHK [14]	16201	4178	4195	68.47	14.974	1.62
	LWC-MIMO-OFDM	1180	475	376	74.75	13.3	1.31
Spartan 6 & XC6SLX4	STPA[15]	3890	1690	1330	33.24	25.43	1.81
	LWC-MIMO-OFDM	1659	577	378	49.65	20	1.57
Virtex 7 & XC7VX485	LDPC[16]	4142	5805	1647	94.21	13.75	1.46
	LWC-MIMO-OFDM	1014	414	345	105.42	10.25	1.05

delay for AES [20] with LWC-MIMO-OFDM analysed in the Virtex 5 is shown in the Fig. 7. The comparison shows that the delay of LWC-MIMO-OFDM method for Virtex 5 is 13.3ns, which is less when compared to the AES [20].

The AES [20] based ECG signal encryption and decryption obtains higher delay of 14.668ns due to the utilization of higher logical elements during implementation. The delay of the LWC-MIMO-OFDM method is less when compared to the AES [20] due to its less logical elements. Consequently, the lesser logical elements of the LWC-MIMO-OFDM method helps to increase the overall speed during secure ECG signal transmission.

The comparative analysis of hardware utilization is given in Table 7. In the comparison, DHK, STPA, and LDPC method results have been tabulated. These DHK, STPA and LDPC are designed and simulated in three different FPGA devices such as Spartan 6, Virtex 5 and Virtex 7. These conventional design contains more logical elements which increase the hardware utilization of the entire architecture. Due to

the usage of optimal turbo encoder and decoder, the LWC-MIMO-OFDM method is occupied less hardware utilization than conventional designs. The operating frequency of the all the design results are given in Table 7. The operating frequency of DHK, STPA, and LDPC becomes less due to the increase in delay. However, the LWC-MIMO-OFDM method achieves higher operating frequency because of its lesser delay obtained during ECG signal transmission.

6 Conclusion

MIMO-OFDM based ECG signal transmission is accomplished in health monitoring systems. In this research paper, the LWC is used to achieve the secure ECG signal transmission in the MIMO-OFDM system. The turbo encoding and decoding is used in the MIMO-OFDM for correcting the errors occurred due to the fluctuations caused while transmitting the data packets. The burst error and ISI are overcome by using the frequency interleaving insertion of the guarded interval through the MIMO-OFDM system. The utilization of logical elements is reduced by using the LWC for securing the ECG signal from the unauthorized users. Moreover, the power and delay of the MIMO-OFDM system during ECG signal transmission are reduced by decreasing the logical elements. The delay of the LWC-MIMO-OFDM method is 13.3 ns that is less when compared to the delay of the AES method. In Virtex 5 FPGA, LWC-MIMO-OFDM method is occupied 1180 LUTs, 475 FFs, and 376 Slices which are less compared to DHK method. Similarly, LWC-MIMO-OFDM method synthesised in Virtex 7, and Spartan 6 devices where the hardware utilization of LWC-MIMO-OFDM method is less compared to STPA and LDPC designs. In future, the optimal coding and encryption method can be used to minimize the hardware utilization for secure medical signal transmission.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

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

References

[1] A. Agarwal, and S. N. Mehta, "Development of MIMO–OFDM system and forward error correction techniques since 2000s", *Photonic Network Communications*, Vol. 35, No. 1, pp. 65-78, 2018

[2] J. S. Park and T. Ogunfunmi, "Efficient FPGA-based implementations of MIMO-OFDM physical layer", *Circuits, Systems, and Signal Processing*, Vol. 31, No. 4, pp. 1487-1511, 2012.

[3] Y. Huang, and J. Wang, "Multiple ldpc-encoder layered space-time-frequency architectures for ofdm mimo multiplexing", *Wireless Personal Communications,* Vol. 63, No. 4, pp. 995-1012, 2012.

[4] B. Pandya, F. K. Chuang, C. H. Tseng, and T. D. Chiueh, "An energy-efficient communication system using joint beamforming in multi-hop health monitoring sensor networks", *EURASIP Journal on Wireless Communications and Networking*, Vol. 2017, No. 1, pp. 1-16, 2017.

[5] K. Elango and K. Muniandi, "VLSI implementation of an area and energy efficient FFT/IFFT core for MIMO-OFDM applications", *Annals of Telecommunications*, pp. 1-13, 2019.

[6] W. Y. Chen, C. F. Liao, and Y. H. Huang, "Hardware-Efficient Interpolation-Based QR Decomposition and Lattice Reduction Processor for MIMO-OFDM Receivers", *Journal of Signal Processing Systems*, Vol. 88, No. 3, pp. 411-423, 2017.

[7] S. K. Singh, A. P. Rathkanthiwar, and A. S. Gandhi, "New algorithm for time and frequency synchronization in MIMO-OFDM systems", *Wireless Personal Communications,* Vol. 96, No. 3, pp. 3283-3295, 2017.

[8] N. Kirubanandasarathy and K. Karthikeyan, "Design of MOD-R2MDC FFT for MIMO OFDM in wireless telecommunication system", *Telecommunication Systems*, Vol. 63, No. 3, pp. 457-463, 2017

[9] T. H. Pham, I. V. McLoughlin, and S. A. Fahmy, "Robust and efficient OFDM synchronization for FPGA-based radios", *Circuits, Systems, and Signal Processing*, Vol. 33, No. 8, pp. 2475-2493, 2014.

[10] W. Wang, X. Gao, X. Wu, X. You, C. Zhao, and K. K. Wong, "Dual-turbo receiver architecture for turbo coded MIMO-OFDM systems", *Science China Information Sciences,* Vol. 55, No. 2, pp. 384-395, 2012.

[11] M. L. Mohamed, K. Mohammed, and B. Daneshrad, "Energy efficient programmable MIMO decoder accelerator chip in 65-nm

CMOS", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 22, No. 7, pp. 1481-1490, 2013.

[12] V. Lapotre, G. Gogniat, A. Baghdadi, and J. P. Diguet, "Dynamic configuration management of a multi-standard and multi-mode reconfigurable multi-ASIP architecture for turbo decoding", *EURASIP Journal on Advances in Signal Processing*, Vol. 2017, No. 1, pp. 35, 2017.

[13] B. Venkataramanaiah and J. Kamala, "ECG signal processing and KNN classifier-based abnormality detection by VH-doctor for remote cardiac healthcare monitoring", *Soft Computing*, pp. 1-10, 2020.

[14] K. S. Pandian and K. C. Ray, "Dynamic Hash key-based stream cipher for secure transmission of real time ECG signal", *Security and Communication Networks*, Vol. 9, No. 17, pp. 4391-4402, 2017.

[15] Z. Haider, K. Javeed, M. Song, and X. Wang, "A Low-Cost Self-Test Architecture Integrated with PRESENT Cipher Core", *IEEE Access*, Vol. 7, pp. 46045-46058, 2019.

[16] Y. Delomier, B. Le Gal, J. Crenne, and C. Jego, "Model-Based Design of Flexible and Efficient LDPC Decoders on FPGA Devices", *Journal of Signal Processing Systems*, pp. 1-19, 2019.

[17] H. J. Lin, and C. A. Shen, "The Architectural Optimizations of a Low-Complexity and Low-Latency FFT Processor for MIMO-OFDM Communication Systems", *Journal of Signal Processing Systems*, pp. 1-12, 2019.

[18] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Lightweight hardware architectures for the present cipher in FPGA", *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 64, No. 9, pp. 2544-2555, 2019.

[19] C. Anghel, C. Stanciu, and C. Paleologu, "LTE turbo decoding parallel architecture with single interleaver implemented on FPGA", *Circuits, Systems, and Signal Processing*, Vol. 36, No. 4, pp. 1455-1475, 2017.

[20] T. M. Kumar and P. Karthigaikumar, "FPGA implementation of an optimized key expansion module of AES algorithm for secure transmission of personal ECG signals", *Design Automation for Embedded Systems*, Vol. 22, No. 1-2, pp. 13-24, 2018.

[21] G. B. Moody and R.G. Mark, "The MIT-BIH arrhythmia database on CD-ROM and software for use with it", In: *Proc. of Computers in Cardiology*, pp. 185-188, 1990.