***[1]Rupa Kumar Dhanavath,**
[2]Dr. Gopiya Naik S

Design of Flexible Floating Point Processing Element (FFPPE) Based Fingerprint Authentication Model for Error Detection and Correction

Abstract— In communication systems, a proposed FPGA-based authentication setup utilizes an advanced version of the Golay alongside a Flexible Floating Point Processing Element (FFPPE) architecture to enhance fingerprint authentication accuracy. This study features a GOLAY code-integrated FFPPE design comprising various stages, including Timestamp (TS) output with a time to digital converter (TDC), a random number generator, and error correction components involving extended encoding and decoding processes, as well as fingerprint verification techniques. A novel compact integrated circuit (IC) is designed using FFPPE, which plays a key role in operations like multiplication, addition, and subtraction via an Arithmetic Logic Unit (ALU). The binary data structure is built on a Cyclic Redundancy Check (CRC) framework, using both encoders and decoders. This architecture enhances system security while optimizing circuit complexity. Within the error correction module, a polar code decoder tailored for extended Golay code is presented specifically for the fingerprint authentication system. The performance metrics are assessed in terms of look-up table (LUT) optimization, area, power, speed, circuit complexity, power consumption, slice count, clock frequency, false rejection rate (FRR), false acceptance rate (FAR), and total success rate (TSR), and these are compared against existing fingerprint authentication systems. A comparative evaluation between the proposed and existing methodologies is conducted based on multiple parameters to validate the efficacy of the proposed approach. Results indicate that the proposed approach surpasses traditional techniques in bolstering system security. Additionally, FPGA synthesis analysis is carried out across different FPGA families, including Virtex4, Virtex5, and Virtex7.

***Index Terms*—** GOLAY Code, CRC, FFPPE, LUT, Slice Count and Bit Error Rate, Fingerprint authentication, Golay code, encoder, and decoder.

I. INTRODUCTION

In wireless communication and embedded systems, developing a cost-effective biometric authentication system has drawn many researchers' attention. This initiative aims to satisfy the diverse needs of contemporary embedded systems related to cost, speed, power efficiency, minimum bit rate, and bandwidth [1], among other factors. Daily applications like identity verification, e-commerce, and access control depend on these embedded systems to ensure secure and confidential data [2]. Similarly, protecting user information in smart settings is essential to bolster security. However, current technologies are often unreliable due to their susceptibility to duplication, forgery, forgetfulness, misuse, or loss [3-4].

- **Extended Binary GOLAY Code**: This code encrypts 12 bits of data within a 24-bit word. It can correct up to 3-bit errors and recognize any 7-bit errors.
- **Perfect Binary GOLAY Code**: This code has a length of 23, derived from the comprehensive binary GOLAY code by removing one coordinate position.

Currently, polar codes stand out as the most effective error-correcting codes due to their channel attributes [5]. The advantages of this channel are achieved asymptotically through polar coding. There is a need

[1]*aResearch Scholar, PET Research Center, PES College of Engineering, University of Mysore (UOM), Manda, Karnataka 571401, India.
bAssistant Professor, Department of Electronics and Communication Engineering,
Marri Laxman Reddy Institute of Technology and Management, Hyderabad, Telangana 500043, India.
[2]Professor, Department of Electrical and Electronics Engineering, PES College of Engineering, Mandya, Karnataka 571401, India.
*Email: rupakumardhanavath@outlook.com
*[1]Assistant Professor, Electronics and Communication Engineering, pallavi engineering college, Hyderabad.
[2]Associate professor, dept. of Electrical and Electronics Engineering at PESCE, Mandya, Karnataka.
*Corresponding mail: rupadhanvanth135@outlook.com

for further improvement in error correction performance. The fundamental channel capacity of polar codes is obtained through asymptotic properties, and the performance of error correction gets enhanced when codes are extended. However, long polar codes may face challenges related to hardware and extended potential.

Consequently, a strong security method with high protective measures is essential. In today's landscape, the Fingerprint Authentication Model (FAM) is regarded as a leading security mechanism [6]. Unlike ID cards and PINs, which typically consist of fewer combinations, fingerprints possess 16 unique characteristics for each individual. This makes the FAM a more accurate [7] and reliable option for identity verification and management due to its outstanding speed and precision.

False Acceptance (Type I Error) happens when the system mistakenly identifies an unauthorized user as an enrolled member, leading to security threats by allowing unauthorized access. Conversely, Type II errors, or false rejections, occur when the system fails to recognize a legitimate user, preventing them from using the system. This situation can be frustrating for authorized users and may limit system usability. An improper selection of the matching score threshold can lead to a discrepancy between the rates of false acceptance and false rejection [8].

Generally, the embedded systems are affected by harsh environments such as space and area. The functionality of the circuits is also disrupted by the radiation, and various errors occur. Error correction codes (ECC) [9] are often used to avoid such corruption of the stored memory data. To identify and fix errors, ECCs include parity check bits to every word of memory. This necessitates a decoder to identify and fix errors when reading from memory and an encoder to compute these bits when writing to memory [10]. To reduce this kind of problems, the Golay code (23, 12, 7) was developed by the author [12, 13], with a minimum spacing of 7. FPGA [11] has become an emerging area that focuses on real-time implementation at the system level. Compared to microcontrollers [12, 13], FPGAs enable parallel processes that execute multiple inputs with one FPGA without encountering a bottleneck problem. One can achieve a fast authentication approach with minimal hardware resource requirements by considering appropriate authentication on FPGA [14]. FPGAs have the ability to simulate other hardware components as they are considered special integrated circuits while being reprogrammable in the field [15]. In this research, the fingerprint authentication system is carried out with an error correction process using FPGAs. In this research, the proposed system works in three stages: timestamp generator, random number generator (RNG), fingerprint verification (FPV) and error correction.

II. RELATED WORK

The Golay code plays an important role in communication systems, and it is used in forward error correction applications with a perfect linear error correction code. In this research, Rupa Kumar Dhanavath and Gopiya Naik Sevyanaik [16] developed a novel compact integrated chip (IC) based on the Flexible Floating Point Processing Element (FEPPE). FEPPE is also considered an important unit for carrying out additions, subtractions and multiplications. The encoder and decoder structure are used by the cyclic redundancy check method used in binary data architecture. The GOLAY Code Encoder Architecture (GCEA) is implemented on FPGA devices in the Xilinx ISE 14.2 simulator. The performance of the system is analyzed based on area, power consumption, speed, clock frequency, slice count and circuit complexity. The communication system can also be affected by crosstalk and channel noise. Therefore, it is important to retrieve the sender's data to detect and resolve anomalies in the received data. Most data transfer methods utilize the CRC method in the communication system. Rupa Kumar Dhanavath and Gopiya Naik Sevyanaik [17] performed the demodulation of Quadrature Amplitude Modulation (QAM) using a code phrase.

The data symbols are converted into signal waveforms through QAM. Within a Rayleigh fading channel, data loss occur due to noise and interference. To enhance security in the encoder-decoder setup while minimizing circuit complexity, a Golay coding approach combined with CRC is employed. Recent advancements in microelectronics—from the micrometer to the deep submicrometer range—have led to the emergence of multiple cell upset (MCU) in modern memory systems. Error correction codes (ECC) help reduce the effects of MCUs while maintaining simpler designs. In their research, Raj Kumar Maity et al. [18] introduced a high-performance T-bit Burst Error Correcting (BEC) code. Additionally, they proposed a streamlined decoding technique that offers improved area efficiency and power usage. Furthermore, the paper [19] presented an encoding method utilizing cyclic redundancy checks and introduced effective strategies for encoding. Algorithms for both the binary GOLAY and extended binary GOLAY codes were developed within an FPGA prototype. Without depending on

a linear feedback shift register(LFSR), the architecture for the GOLAY encoder in the Virtex 4 FPGA was designed for maximum speed and minimal latency. This work optimized the decoding architecture based on the imperfect extreme possibility decoding structure, focusing on reduced complexity. Compared to existing approaches, this proposed architecture utilizes a smaller area and achieves lower latency. While this module improved forward error correction in communication links, the system speed was relatively low [19]. In a similar vein, one article explored a low-complexity soft-decision decoding architecture design. An appropriate algorithm was created that leverages the code properties to streamline the decoding process. Simulation results indicated that the proposed algorithm successfully minimized costs. The decoder architecture was outlined, and results from the VLSI synthesis were obtained [20]. Furthermore, this study focused on a reconfigurable coding system that adapts according to user requirements, determining whether the process involves the decoder, encoder, or both. The reconfigurable system was proposed using the GOLAY code, implemented on the SPARTAN-3 FPGA, and its performance was evaluated both with and without the reconfigurable architecture [21].

III. PROPOSED MEET OUT

- To create a fingerprint authentication system that utilizes FPGA technology, featuring an area-delay efficient architecture for the extended Golay code encoder and an optimized arithmetic unit for generating codewords.
- To design a decoder based on adaptive polar codes within the extended Golay code framework for error correction in the fingerprint authentication system.
- To develop a decoding process for the Golay Code that minimizes complexity and area while achieving the Maximum Combinational Path Delay (MCPD).
- To ensure reliable authentication with the proposed error correction technique, improving the dependability of the biometric system while reducing power consumption, leakage levels, delay times, and enhancing the speed of both encoding and decoding processes.
- To showcase the entire simulation using Xilinx Verilog coding and validate the functionality of the proposed approach by comparing it to existing methods.

Objective

This research presents a FAM that is based on the architecture of GOLAY code decoders and encoders utilizing the CRC processing technique. This technique simplifies the circuit design, facilitating efficient data communication. A novel compact integrated circuit (IC) is created using FFPPE, which serves as the key component for arithmetic operations such as subtraction, addition, multiplication, binary data manipulation, and the ALU approach.

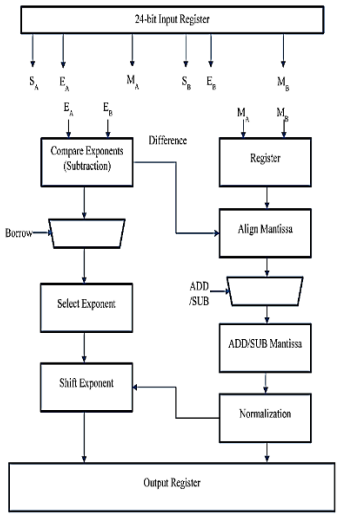

Figure.1. Architecture design FFPPE system

Figure 1 illustrates a 24-bit input register. Various operations are carried out as depicted in the flowchart to achieve the output register. The CRC method is one of the techniques used for error detection in data encryption and decryption. This study primarily focuses on separating input data bits and generating key bits. It aims to enhance the architecture involved in the division process for decoding and encoding purposes. A Priority Based Encoder (PBE) has been developed to implement the XOR gate method in the subtraction operation. This design aims to analyze the subtraction of data bits while increasing the number of zero bits to reduce the overall complexity of the division architecture. The encoding algorithm for this code is based on the CRC generation process, converting the BGC into EGC. An example for the Check Bit Generation (CBG) is illustrated in Figure 2.

Figure 2 represents the data encoding process, using 456h as the Example data. In this example, a polynomial P(X) = AE3h is utilized. Furthermore, modulo-2 division is employed to produce the check bit. Consequently, a twelve-bit message is taken, and eleven check bits are added to obtain the GOLAY code word. This is achieved through the modulo-2 division technique in conjunction with CRC. Thus, the binary GOLAY code word is generated. Therefore, the CRC for the data 456H with the polynomial AE3H results in 1C8H.

```
101011110011 ) 010001010110000000000 ( 000001110110
-----------------------------------
  101011110011
  --------------------
  0011100110000000
  001011110011
  --------------------
  011110010000
  01011110011
  --------------------
  10001100000
  101011110011
  --------------------
  0111001000
  00000000000
```

Figure.2. Check-bit generation example

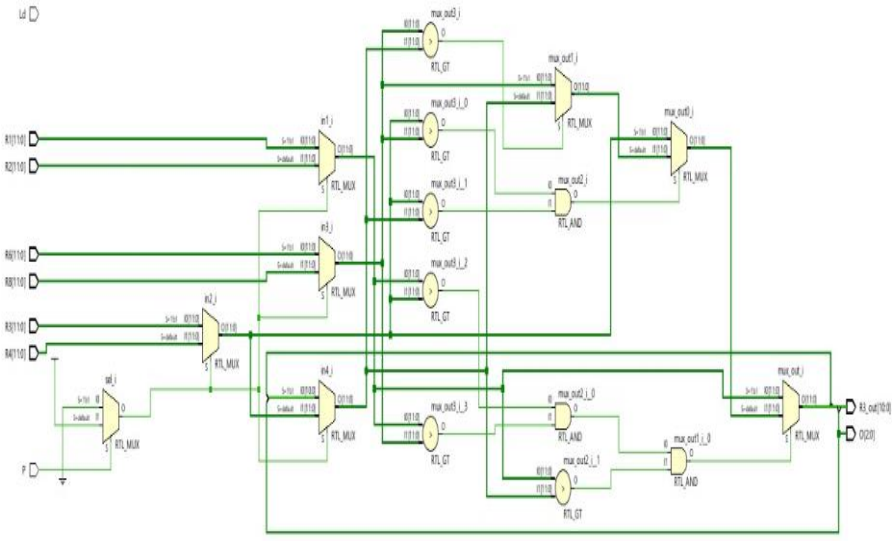

Figure.3. RTL schematic of FFPPE circuit for FAM

Figure. 3. shows the Register Transfer Level (RTL) implementation of the priority encoder. It consists of the following components:

Input Registers:

- R1, R2, R3, R4, R6, R8: These registers store the 12-bit input values.

Control Logic:

- The control logic, implemented using multiplexers, selects the input pairs based on the P signal.

Comparator:

- Compares the selected input pairs and selects the larger one.
- This process is repeated to select the largest value among all inputs.

Priority Encoder:

- Encodes the 12-bit output from the comparator into a 4-bit output.

Output Registers:

- R3_out: Stores the selected 11-bit value.
- O: Stores the 3-bit priority output.

Data Encoder Architecture

The Golay encoder architecture is a function and is outlined for modifying the general structure of encoder. It undertakes key updation for data transmission. The encoder architecture comprises of a GF field function based LFSR result equation, CRC design, and the architecture of GOLAY code. The data encoder operation helps in the bit addition of input message, output bits corresponding to CRC and the design of GOLAY code based on majority bits for sending the data bits in the encoder architecture. Moreover, the design of priority encoder is shown in the below figure.4.

The data encoder operation helps in the bit addition of input message, output bits corresponding to CRC and the design of GOLAY code based on majority bits for sending the data bits in the encoder architecture.

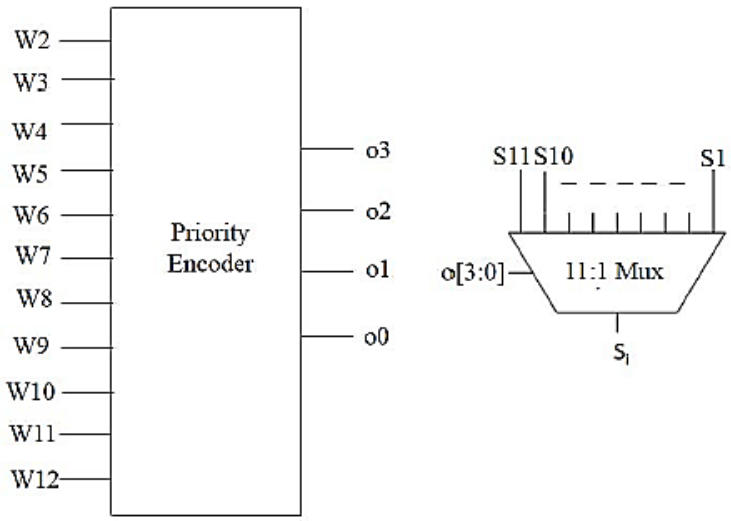

Figure.4. Design of priority encoder

Data decoder architecture

Initially, the data output which are received by modifying decoder architecture with support of EGC. This design is to check the whole output data encoder. The majority output data bits are then examined thus to relate the data

bit location of GOLAY code architecture. The CRC key data bits are checked so that it is possible to relate the process CRC calculation and solving the '0' level final data bit. Moreover, the Design of priority decoder is shown in the below figure.5.

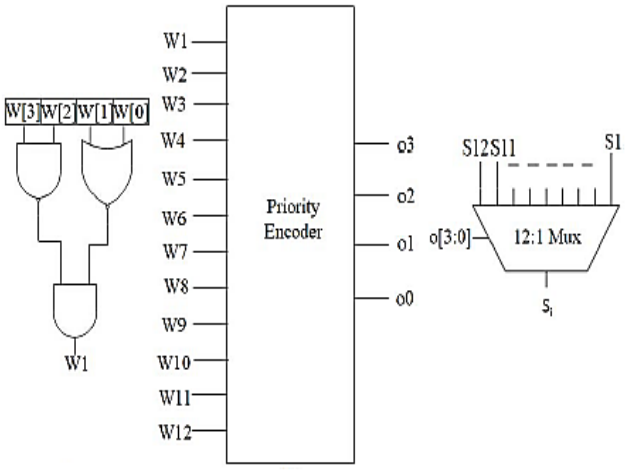

Figure.5. Design of priority decoder

Timestamp (TS) output with time to digital converter (TDC)

The binary fine time stamp signal is produced by a time stamp generator (TSG) in the FPGA-based Fingerprint identification system.

The FPGA architecture of TSG employs several blocks, namely, coarse generator, tuned sampling time to digital logic (TDL), and combinational encoder for counters with ones and zeros. The coarse time signal is generated by the coarse generator. The carry chain blocks (Carry4) are used to construct the delay line and allow multiplexers to propagate the input signal. A TDL with 192 delay cells and a clock frequency of 250 MHz is used in this design. The largest time interval covered is 262.14, depending on the clock frequency and the quantity of coarse counter bits.

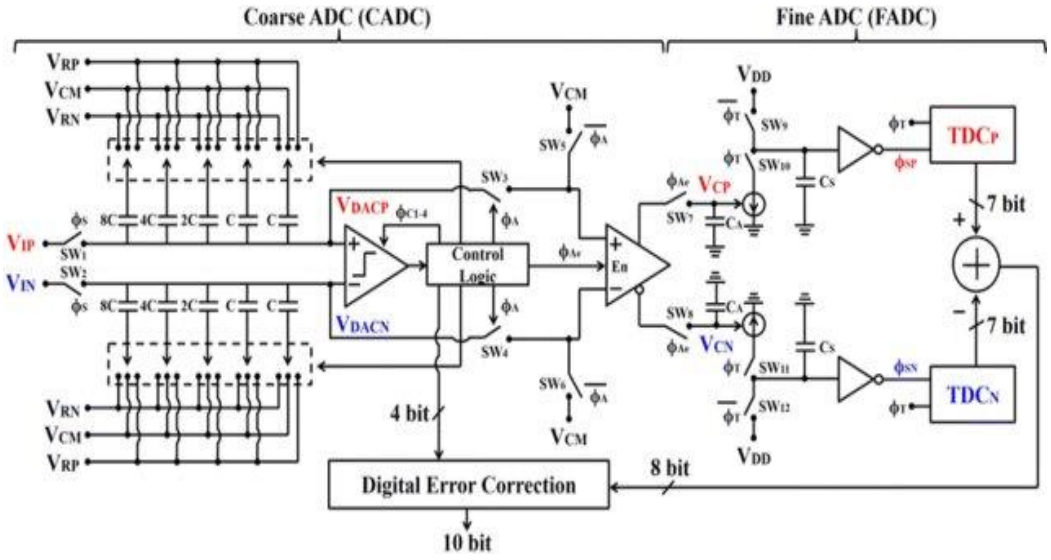

Figure.6. Illustration of time stamp generator

When the hit signal arrives, the state of the delay chains is captured by the D flip-flops. The captured state is then converted into a binary code by the encoders. The coarse and fine counters start counting the clock cycles. The coarse counter counts the number of clock cycles that have passed since the hit signal. The fine counter performs

the counting task of the number of clock cycles within the last coarse counter cycle. The outputs of the coarse and fine counters are added together to produce the final time stamp.

The Figure.7. is to represent a Golay Code Encoder. Golay codes are a type of error-correcting code used in various communication systems to improve reliability. This encoder takes an input bitstream and adds redundancy in the form of parity bits to create a codeword. This codeword can then be transmitted over a noisy channel, and the receiver can use the redundancy to detect and correct errors.

Components and their Functions

- Registers (Rgt 1, Rgt 2, Rgt 3):
  - These registers store the input bits.
  - Rgt 1 holds 22 bits of the input data.
  - Rgt 2 holds 24 bits of the input data, including 2 parity bits.
  - Rgt 3 holds the final 24-bit Golay codeword.
- Logic Gates (L, M, and the Adder Network):
  - The logic gates perform the necessary calculations to generate the parity bits and combine them with the input data.
  - The adder network adds the input bits and parity bits to form the final codeword.
- Extended Golay Code:
  - The final output is a 24-bit extended Golay code, which can correct up to three errors in a codeword.

The input data is stored in Rgt1. The logic gates calculate the parity bits based on the input data. The input bits and parity bits are combined using the adder network to form the 24-bit Golay codeword. The final codeword is stored in Rgt3 and can be transmitted over the channel.

The diagram in figure.8. is a simplified representation of a system that represents the extended Golay code-based FAM implemented with FFPPE architecture. It has three main components:

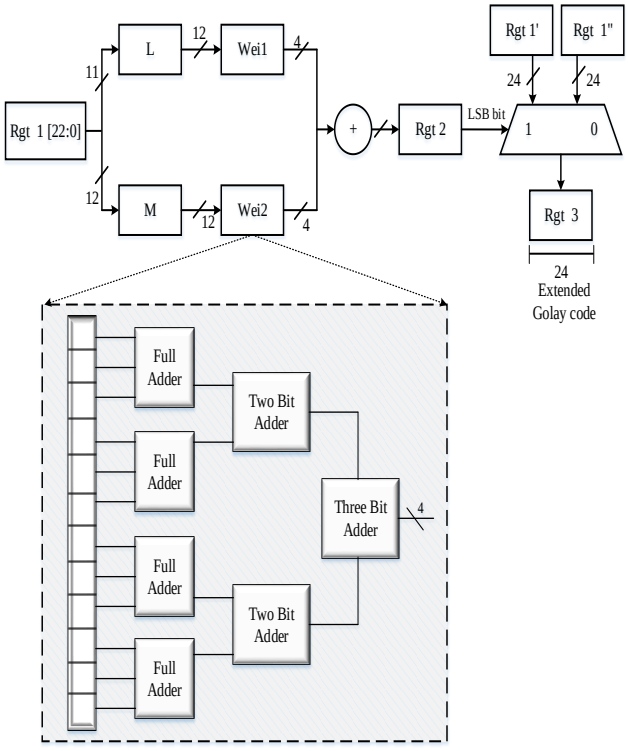

Figure.7. Encoder architecture of Extended Golay code FFPPE based FAM

- Time Stamp Generator (A2) module is responsible for generating timestamps, possibly to associate with data or events.
- Verification (A5) module verifies the integrity or authenticity of data.
- Error Correction (EC1) is responsible for detecting and correcting errors in data.

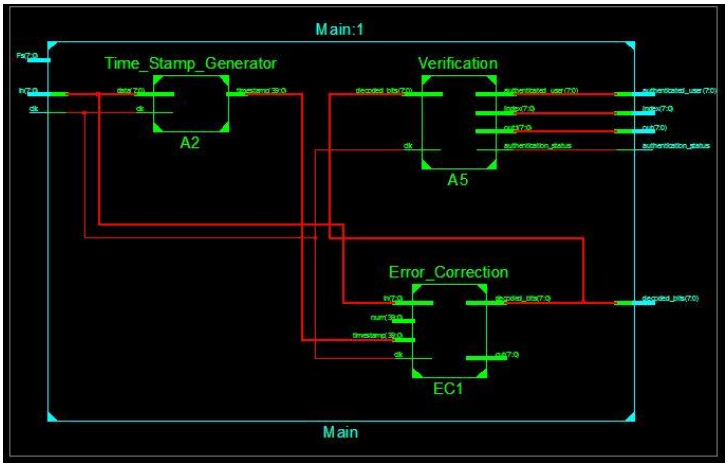

Figure.8. RTL schematic of Integrated FFPPE and FAM

IV. RESULTS AND DISCUSSION

The outputs obtained through the Design of proposed system is elaborated here with performance and comparative analysis.

4.1 Performance Analysis

This section provides the detailed depiction of the performance analysis of the proposed technique.

4.1.1 RTL (Register Transfer Level)

RTL is constructed on synchronous logic, which in turn comprises three primary portions specifically registers which embrace state information, combinatorial logic that describes the next state responses and clocks that regulate once the state fluctuates.

4.1.2 Synthesis report

The synthesis report outlines the overall usage of the system along with the clock frequency output for the implemented system. The synthesis report is illustrated in the figure 9. below.

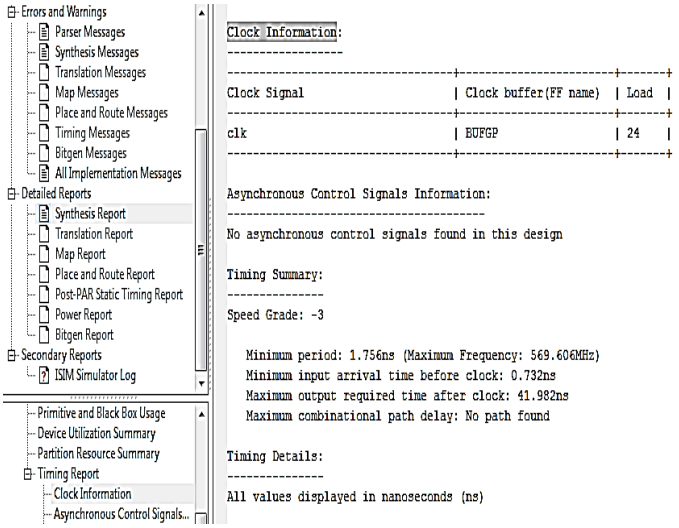

Figure.9. Synthesis Report

From the above figure.9, the clock information, asynchronous control signal information, timing summary and their details are determined through the implementation of the proposed method. It is also evident that the proposed system consumes very minimal time. It is shown in the below table-1.

Table-1. Clock and speed of the proposed system

Minimum period	1.76ns
Minimum input arrival time before clock	0.732ns
Maximum output required time after clock	41.962ns
Speed grade	-3 (no unit)

From the above table-1, the minimum period is found to be at a rate of 1.76ns, Minimum input arrival time before clock is found to be 0.732ns, Maximum output required time after clock is found as 41.962ns and the speed grade is found as -3 (no unit). Thus, the proposed system consumes minimum time to reduce the circuit complication for data communication as well as response practice.

4.2 Comparative analysis

The comparative evaluation of the suggested method and the current technique is presented in the table below, labeled as table-2. The analysis takes into account parameters such as the number of slices, the count of LUTs, delay time in nanoseconds, clock frequency in megahertz, and power consumption in milliwatts.

Table-2. Comparative analysis of the proposed and existing system

PARAMETERS	**EXISTING SYSTEM**	**PROPOSED SYSTEM**
SLICES COUNT REGISTERS	972	781
LUT COUNT	333	24
DELAY TIME (ns)	2.305	1.756
CLOCK FREQUENCY (MHz)	433.657	569.606
POWER(mW)	67.9	44

The proposed method yields a slice count of 781, with a LUT count of 24, a delay time of 10756 ns, a clock frequency of 569.606 MHz, and a power consumption of 44 mW. Therefore, when compared to the existing technique, the new method demonstrates superior results, highlighting the effectiveness of the introduced system. In addition, various existing systems are compared with the proposed system in terms of LUT count, area and synthesized frequency. It is shown in the below table-3.

Table-3. Evaluation of the suggested and current [24] techniques regarding different factors.

comparison parameters	FPGA types			
	virtex 5	**virtex 4**	**spartan 3**	**Proposed**
synthesized frequency (MHZ)	197.035	162.425	83.876	245
Number of LUT	151	191	193	84
Number of Slice(Area)	65	102	103	36

From the above table-3, the proposed system is found to be effective than the existing methods with respect to area, LUT count and synthesized frequency. It is shown as graphical form in the below figure.10.

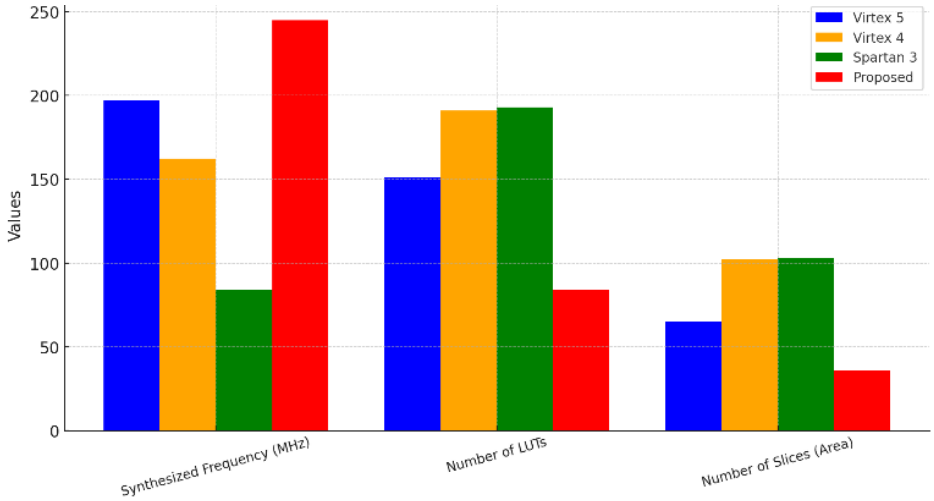

Figure.10. Comparative analysis of the Proposed and existing systems

From the above figure.10, the proposed system is found to show high frequency and minimum LUT and area thereby enhancing the efficacy of the system.

Thus the proposed system is found to be effective than the existing methods in minimizing the circuit complication for data communication in minimum time.

V. CONCLUSION

In this research, a novel compact integrated chip utilizing a Flexible Floating Point Processing Element (FFPPE) for a fingerprint authentication module is introduced, which plays a crucial role in the processes of addition, subtraction, binary data manipulation, and multiplication. Additionally, VHDL is employed on FPGA devices to validate the GCEA (Golay Code Encoder Architecture) within Xilinx ISE 14.2. To address the limitations of current systems, some alterations to the design of this model are proposed. Therefore, the focus of this research is on the effective FPGA implementation of a fingerprint authentication system incorporating an enhanced polar code-based decoder. The proposed method achieves a True Success Rate (TSR) of 98.7% in comparison to existing techniques. Moreover, an analysis of FPGA synthesis is conducted in terms of area, delay, and frequency across various FPGA families. The performance evaluation was carried out, and the findings were compared with those of existing methods concerning synthesized frequency in MHz, LUT count, area, clock speed, and other parameters to demonstrate the effectiveness of the proposed system. The results indicate that the proposed system offers greater efficiency than existing approaches in enhancing security. In future work, the proposed method's

effectiveness and robustness against potential attacks will be showcased as part of a security performance assessment under exhaustive and statistical attack scenarios.

REFERENCES

[1] Y. Wu, X. Gao, S. Zhou, W. Yang, Y. Polyanskiy, and G. Caire, "Massive access for future wireless communication systems," IEEE Wireless Communications, vol. 27, pp. 148-156, 2020.

[2] Prakash AJ, Patro KK, Hammad M, Tadeusiewicz R, Pławiak P. BAED: A secured biometric authentication system using ECG signal based on deep learning techniques. Biocybernetics and Biomedical Engineering. 2022;42(4):1081-93.

[3] Sarkar A, Singh BK. A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimedia Tools and Applications. 2020;79(37):27721-76.

[4] Lee YK, Jeong J. Securing biometric authentication system using blockchain. ICT Express. 2021;7(3):322-6.

[5] S. M. Abbas, Y. Fan, J. Chen, and C.-Y. Tsui, "High-throughput and energy-efficient belief propagation polar code decoder," IEEE Transactions on very large scale integration (VLSI) systems, vol. 25, pp. 1098-1111, 2017.

[6] Liu G, Xu T, Ma X, Wang C. Your model trains on my data? Protecting intellectual property of training data via membership fingerprint authentication. IEEE Transactions on Information Forensics and Security. 2022;17:1024-37.

[7] Popli A, Tandon S, Engelsma JJ, Namboodiri A. A unified model for fingerprint authentication and presentation attack detection. In Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment 2023:77-99. Singapore: Springer Nature Singapore.

[8] Choi H, Woo SS, Kim H. Blind-Touch: Homomorphic Encryption-Based Distributed Neural Network Inference for Privacy-Preserving Fingerprint Authentication. In Proceedings of the AAAI Conference on Artificial Intelligence 2024;38(20):21976-21985.

[9] Barman S, Shum HP, Chattopadhyay S, Samanta D. A secure authentication protocol for multi-server-based e-healthcare using a fuzzy commitment scheme. IEEE Access. 2019;7:12557-74

[10] kumar Natarajan S, Rathinasabapathy R, Narayanasamy J, Aravind AR, Raghesh A. An Automated Fingerprint Recognition Model With Optimized Deep Learning Model: A Meta-Heuristic Approach. Scandinavian Journal of Information Systems. 2023;35(1):1440-9.

[11] Babaei A, Schiele G, Zohner M. Reconfigurable Security Architecture (RESA) Based on PUF for FPGA-Based IoT Devices. Sensors. 2022;22(15):5577.

[12] Vargas MG, Hoyos FE, Candelo JE. Portable and efficient fingerprint authentication system based on a microcontroller. International journal of Electrical and Computer Engineering. 2019;9(4):2346.

[13] Hersyah MH, Yolanda D, Sitohang H. Multiple laboratory authentication system design using fingerprints sensor and keypad based on microcontroller. In 2020 International Conference on Information Technology Systems and Innovation (ICITSI) 2020:14-19. IEEE.

[14] Oroutzoglou I, Kokkinis A, Ferikoglou A, Danopoulos D, Masouros D, Siozios K. Optimizing Savitzky-Golay Filter on GPU and FPGA Accelerators for Financial Applications. In 2022 11th International Conference on Modern Circuits and Systems Technologies (MOCAST) 2022:1-4. IEEE.

[15] Bakshi A, Panigrahy M, Das JK. FPGA Based Digital Filters Design to Remove Noise from ECG Signal. In 2021 IEEE International Symposium on Smart Electronic Systems (iSES) 2021:236-239. IEEE.

[16] Dhanavath RK, Sevyanaik GN. Design of Flexible Floating Point Processing Element (FFPPE) Architecture Based on Golay Code Strategy. Wireless Personal Communications. 2022;125(2):1783-800.

[17] DHANAVATH RK. An Efficient Technique to Implement Encoder and Decoder in Communication System for Error Detection and Correction Golay CodeUsing Golay code.

[18] Maity RK, Samanta J, Bhaumik J. Construction technique and evaluation of high performance t-bit burst error correcting codes for protecting MCUs. Journal of Circuits, Systems and Computers. 2023;32(09):2350142.

[19] S. Sarangi and S. Banerjee, "Efficient Hardware Implementation of Encoder and Decoder for Golay Code," IEEE Trans. VLSI Syst., vol. 23, pp. 1965-1968, 2015.

[20] P. Adde and R. Le Bidan, "A low-complexity soft-decision decoding architecture for the binary extended Golay code," in Electronics, Circuits and Systems (ICECS), 2012 19th IEEE International Conference on, 2012, pp. 705-708.

[21] S. D. Deshpande and M. Nagachandra, "Error Correcting Code with Reconfigurability for Binary Communication," 2017.

[22] M. Nazeri, A. Rezai, and H. Azis, "An Efficient Architecture for Golay Code Encoder," in 2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT), 2018, pp. 114-117.

[23] M. Sprachmann, "Automatic generation of parallel CRC circuits," IEEE Design & Test of Computers, vol. 18, pp. 108-114, 2001.

[24] G. Campobello, G. Patane, and M. Russo, "Parallel CRC realization," IEEE Transactions on Computers, vol. 52, pp. 1312-1319, 2003.

[25] M.-I. Weng and L.-n. Lee, "Weighted erasure codec for the (24, 12) extended Golay code," ed: Google Patents, 1983.