Design, Optimization and Real Time Implementation of a New Embedded Chien Search Block for Reed-Solomon (RS) and Bose-Chaudhuri-Hocquenghem (BCH) Codes on FPGA Board

Azeddine Wahbi[1], Anas El Habti El Idrissi[2], Ahmed Roukhe[3], Bahloul Bensassi[1], Laamari Hlou[2]

[1]Laboratory of Industrial Engineering, data processing and logistic, Faculty of Sciences Ain Chock, University Hassan II, Casablanca, Morocco
[2]Laboratory of Electronic Systems, Information Processing and Energetics, Faculty of Sciences, University Ibn Tofail Kenitra, Morocco
[3]Laboratory of Atomic, Mechanical, Photonics and Energy Faculty of Science, University Moulay Ismail, Meknes, Morocco

***Abstract*:** The development of error correcting codes has been a major concern for communications systems. Therefore, RS and BCH (Reed-Solomon and Bose, Ray-Chaudhuri and Hocquenghem) are effective methods to improve the quality of digital transmission. In this paper a new algorithm of Chien Search block for embedded systems is proposed. This algorithm is based on a factorization of error locator polynomial. i.e, we can minimize an important number of logic gates and hardware resources using the FPGA card. Consequently, it reduces the power consumption with a percentage which can reach 40 % compared to the basic RS and BCH decoder. The proposed system is designed, simulated using the hardware description language (HDL) and Quartus development software. Also, the performance of the designed embedded Chien search block for decoder RS\BCH (255, 239) has been successfully verified by implementation on FPGA board.

***Keywords*:** Embedded Systems, Chien Search Block, Error Locator Polynomial, Hardware Description Language VHDL, FPGA Implementation, RS Codes, BCH codes.

1. Introduction

Embedded systems are widely used these days in most real time applications, especially communications systems [1][2][3]. Due to the growing percentage of people using these technologies, methods are needed to increase the transmission rate without reducing the quality [4] [5]. One of these methods is the Reed-Solomon (RS) and BCH codes which are used to correct errors in many systems such as Vehicular Networks, storage devices (CD, DVD, etc.) and digital video broadcasting (DVB) [6][7][8]. An RS code word is a packet of symbols which are commonly bytes (8-bit symbols), denotes as RS (n, k) where n is the number of the symbols in the encoded message and k is the number of the symbols in the original message as shown in Fig.1.

Each RS code word can correct a maximum of t = (n-k/2) errors in a received packet [9].

The aim of this work is to prove that, it is possible to decrease a large number of hardware resources in the Chien Search Block for RS codes using a new algorithm allowing us to conceive another circuit of Chien Search block with an important number of minimized logic gates.

The paper is structured as follows: In section II, we describe the error locator polynomial. Section III presents the new chien search algorithm and evaluates the performance of the proposed algorithm using a simulation results and comparison between the modified and basic circuits of Chien Search Block. In section IV, we implement the designed embedded block on a Xilinx Spartan 3E-500 FG 320 FPGA (xc3s500e-5fg320) and Section V concludes this paper.

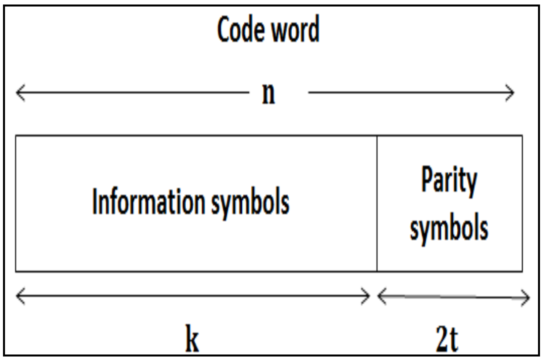

Figure 1. RS code word structure

2. Related Work

2.1 Reed Solomon Code

A Reed-Solomon code is a block code and can be specified as RS (n, k) as shown in Fig. 1. The variable n is the size of the code word with the unit of symbols, k is the number of data symbols and 2t is the number of parity symbols. Each symbol contains m number of bits such as:

- Block length: n= 2^m-1
- Number Of parity check bits r= n-k
- Minimum distance $d_{min} = 2t + 1$

2.1.1 Reed Solomon encoder

Reed–Solomon codes are an important group of error-correcting codes systems that were devised to address the issue of correcting multiple errors. Those are an important subset of nonbinary cyclic error correcting code and the most commonly used codes in practice. Reed Solomon describes a systematic way of building codes that could detect and correct multiple random symbol errors. The codes of Reed Solomon are nonbinary BCH (Bose-Chaudhuri-Hocquenghem) codes belonging to the Galois fields GF (q=24). These codes are specified as RS (n, k), with m bit symbols, where n is the size of code word length and k is the number data symbols, n – k = 2t is the number of parity symbols. [10] This means that the encoder takes k data symbols of m bits each, appends n-k parity symbols, and produces a code word of n symbols (each of m bits).

- Polynomial Message

The message that needs to be encoded in one block consists of k information symbols. It can be represented as an information polynomial, M(x), of degree k-1:

$$M(x) = x^{k-1}m_{k-1} + x^{k-2}m_{k-2} + \dots + m_1 + m_0 \quad (1)$$

- Forming The Code word

The process of encoding the message represented in "equation 3" consists of multiplying the information polynomial, m(x), by xn-k and then dividing the result by the code generator polynomial, g(x), Produce a quotient q (x) and a remainder r (x), where r (x) is of degree n-k.

$$C(x) = M(x)x^{n-k} + \left[M(x)x^{n-k} + \text{mod}\, g(x)\right] \quad (2)$$

Where g (x) is the generator polynomial of degree 2t:

$$g(x) = \prod_{i=0}^{2t-1}(x+\alpha^i) \quad (3)$$

Where α is a primitive element in GF (2m)

The scheme of Reed-Solomon encoder is represented in Fig. 2.

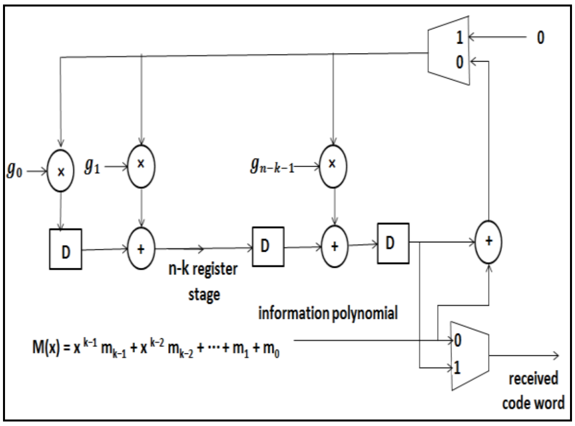

Figure 2. Scheme of a Reed-Solomon encoder

2.1.2 Reed Solomon decoder

The Reed-Solomon decoding is an operation, which is used to detect and correct errors, produced by the transmission channels. T(x) and R (x) represent respectively transmitted code word polynomial and received code word polynomial [11]. The transmitted code word polynomial can be corrupted by channel noise during transmission consequently, the received code word can be wrote as:

$$R(x) = R_{n-1}x^{n-1} + R_{n-2}x^{n-2} + \dots + R_1 + R_0 \quad (4)$$

R(x) = C (x) + E (x), Where E (x) the error polynomial.

The necessary steps used in the Reed-Solomon decoder are :

➢ Syndrome Calculation.
➢ Determine error-location polynomial.
➢ Solving the error locator polynomial.
➢ Calculate error value
➢ Error Correction

All these steps can be represented in figure 3.

➢ Syndrome Calculation.

The first step in decoding the received symbol is to identify the data syndrome. The generator polynomial divides the input symbols received. The remainder must be zero. The parity is placed in the code word to ensure that code is exactly divisible by the generator polynomial. If there is a remainder in the division, then there are errors. The remainder called the syndrome.

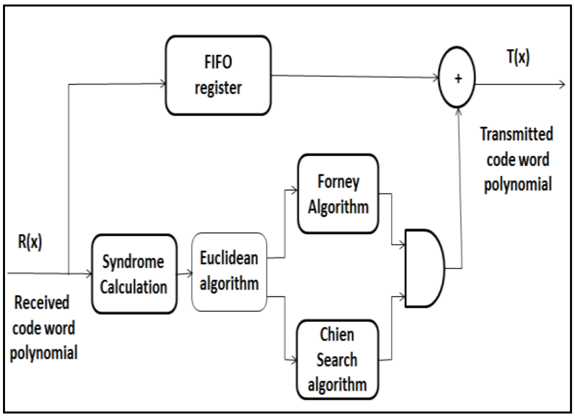

Figure 3. Scheme of a Reed-Solomon decoder

➢ Determination of error-locator polynomial

After counting the syndrome polynomial, next step is to calculate the error values and their respective locations in code. This stage involves the solution of the 2t syndrome polynomials from the previous step.

➢ Solving the error locator polynomial:

Once the ability to determine the error locations and values of a polynomial error, the next step is to evaluate the polynomial error and get the roots. The roots that obtained will now point to error location in the received message. RS decoding generally implements the Chien search algorithm to implement the same.

➢ Calculate error value

Once the errors are located, the next step is to use the syndromes and the error polynomial roots to derive the error values. Forney's Algorithm is used for this purpose. It is an efficient way of performing a matrix inversion, and it involves two main stages.

➢ Error correction

If the error symbol has any set bit, it means that the corresponding bit in the received symbol is having an error, and must be inverted. To automate this correction process each of the received symbols is read again, and at the each error location the received symbols are XORed with the error symbols. Thus the decoder corrects any errors as the received word is being read out from it.

2.2 BCH Code

The BCH code is characterized as (n, k, t), where n is the code length, k is the data length, and t is the error correction capability. The n-bit code word (r0, r1, …, rn-1) can be interpreted as a received polynomial.

2.2.1 BCH encoder

BCH (Bose – Chaudhuri - Hocquenghem) Codes form a large class of multiple random error correcting codes. BCH Code is a generalized form of Hamming Code. The possible BCH codes for m>=3 and t<2^m-1 are:

Block length: n=2^m-1
Parity check bits: n-k<=mt
Minimum distance: d>= 2t+1

2.2.2 BCH decoder

Decoding process for BCH codes is the same one used in the Reed-Solomon decoding which can be represented in three steps:

Step1: Computation of syndromes.
Step2: Berlekamp-Massey algorithm.
Step3: Detection of error position using Chien Search Block.

3. The Proposed Methodology

3.1 Error Locator Polynomial

For the process of RS and BCH decoders, the error locator polynomial is evaluated by introducing only the terms that correspond to errors, it is given as:

$$E(x) = Y_1 x^{e_1} + Y_2 x^{e_2} + \ \dots \ + Y_v x^{e_v} \quad (5)$$

Here, {e₁, … ,eᵥ}, are called the locations of the errors in the code.

word, it is considered as the corresponding powers of x, and $Y_1, \dots, Y_v$ represent the error values at those locations [12].

Then, the error locator polynomial, Λ (x), has a degree of $v \leq t$ and can be expressed as:

$$\begin{aligned} \Lambda\,(x) &= \prod_i^v (1 + X_i x) \\ &= X_1(x + X_1^{-1})\, X_2(x + X_2^{-1})) \end{aligned} \quad (6)$$

Where $X_1 = \alpha^{e1}$, $X_2 = \alpha^{e2} \dots Xv = \alpha^{ev}$

In addition, the function value will be zero if $x = \alpha^{-e1}$, $x = \alpha^{-e2} \dots x = \alpha^{-ev}$

3.2 Proposed Algorithm for New Search Block

For this study, we focused on the Euclidean algorithm to determine the error locator polynomial Λ (x). This algorithm can detect the error position by calculating $\Lambda(\alpha^{-i})$ where $0 \leq i \leq n-1$. For the RS (n, k) or BCH (n, k) codes we must calculate the following terms of Λ (x):

$\Lambda(\alpha\text{-}^{(n-1)})$, $\Lambda(\alpha\text{-}^{(n-2)}) \dots \Lambda(\alpha^{-1})$, $\Lambda(\alpha^{-0})$

However, if the expression reduces to 0, $\Lambda(\alpha^{-i}) = 0$, then that value of x is a root and identifies the error position else the position does not contain an error.

3.3 Chien Search Algorithm

The main idea of the proposed algorithm is to applied a specific factorization of the error locator polynomial such as the condition (x_n, where n = 2) must be respected in this factorization. Besides, we can conceive a new algorithm of the Chien Search Block i.e. we can minimize a large number of the logic gates and hardware resources. Therefore, we will have a low complexity compared to the basic and others algorithms [13][14] [15]. If we take the case of RS (255, 239), the error locator polynomial is mathematically represented as follows

$$\begin{aligned} \Lambda\,(x) = &A X^8 + B X^7 + C X^6 + D X^5 + E X^4 \\ &+ F X^3 + G X^2 + HX + I \end{aligned} \quad (7)$$

It is a polynomial of degree 8, we factorize the equation (7), we find:

$$\begin{aligned} \Lambda(X) &= X(A X^7 + B X^6 + C X^5 + D X^4 \\ &\quad + E X^3 + F X^2 + G X^1 + H) + I \\ &= X\ (X\ (A X^6 + B X^5 + C X^4 + D X^3 \\ &\quad + E X^2 + FX + G) + H) + I \qquad (8) \\ &\quad \dots\dots\dots \\ &= X\ (X\ (X\ (X\ (X\ (X\ (X(AX+B) \\ &\quad +C) + D) + E) + F)\ +G)\ +H) + I \end{aligned}$$

4. Simulation and Experimentation Results

4.1 Simulation Results

The basic and the modified circuits as shown respectively in Fig. 4 and Fig. 6 have been designed and simulated using Quartus II development software. The algorithm based on a new Embedded Chien Search Block has been developed, then applied to the proposed RS and BCH codes. The obtained simulation results from the proposed method will be discussed in this section.

For equation (4), the basic circuit corresponding is represented in Fig.4. Therefore, the simulation of the basic circuit (equation 4) using Quartus software is represented in Fig.6.

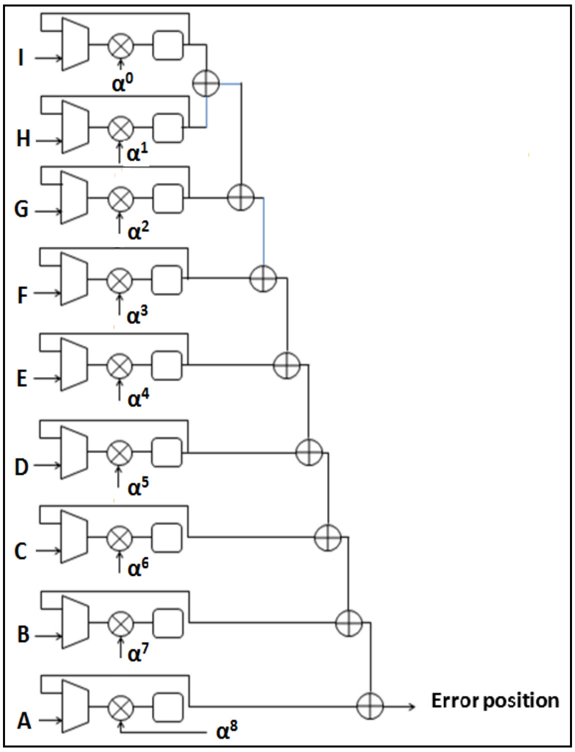

Figure 4. Basic circuit of Chien Search Block

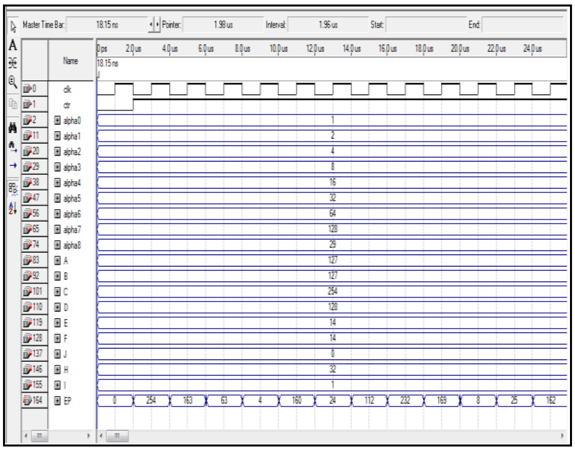

Figure 5. Simulation of the basic circuit (equation 4) using Quartus software.

For the equation (5), the modified circuit using the factorization method is represented in Fig.5. Therefore, the simulation of the modified circuit (equation 5) using Quartus II software is represented in Fig.7.

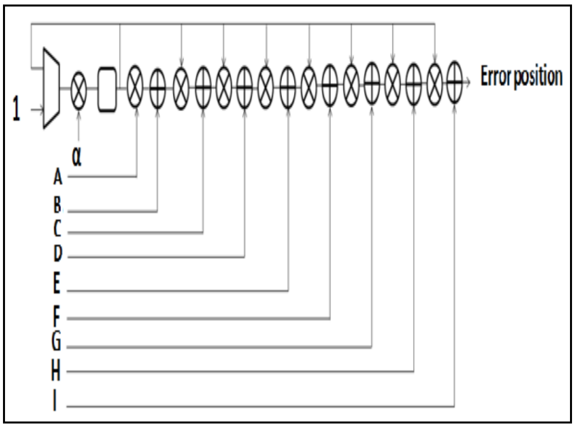

Figure 6. Modified circuit of Chien Search Block

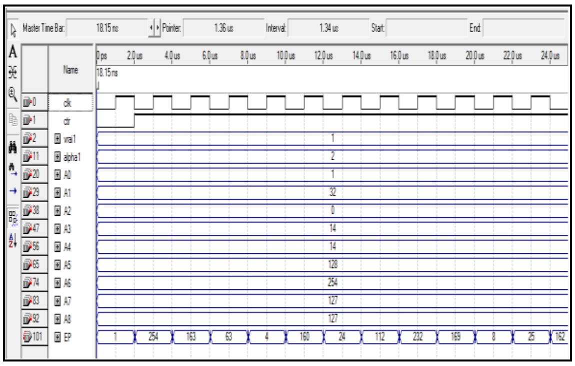

Figure 7. Simulation of the Modified circuit (equation 5) using Quartus software

4.2 Analysis and Discussion of Simulation Results

In order to evaluate the performances of the proposed deign, we carried out a series of tests in context of embedded chien search block for codes. To demonstrate the advantages of the factorization method, different error locator polynomials is tested.

Simulation results were evaluated by BER (Bit Error Rate) and number of minimized logic gates criteria, respectively. Table I show the comparative analysis of different designs is done by comparing the BER values and minimization rate (Number of minimized logic gates). These are tested for different error locator polynomials using this factorization method.

Table 1. Comparison of the BER values and minimization rate of the different locator polynomials based the adopted factorization method for the modified design

Error locator Polynomial Degree	basic design N_b	Modified design	Number of minimized logic gates N_m	Minimization rate %	BER 10^{-5}
2	11	7	4	36,36	6,3
3	15	9	6	40	6
4	19	11	8	42	5,8
5	23	13	10	43,5	5,6
6	27	15	12	44,4	5,56
7	31	17	14	45	5,5
8	35	19	16	45,7	5,4

The evolution curves of minimization rate and BER in dB are also plotted in Fig. 8 and Fig. 9 respectively.

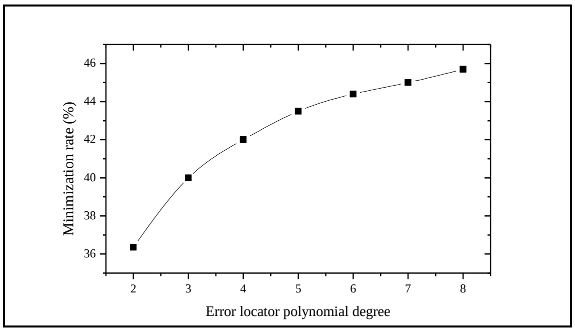

Figure 8. Evolution of the minimization rate depending on the degree of the error locator polynomial

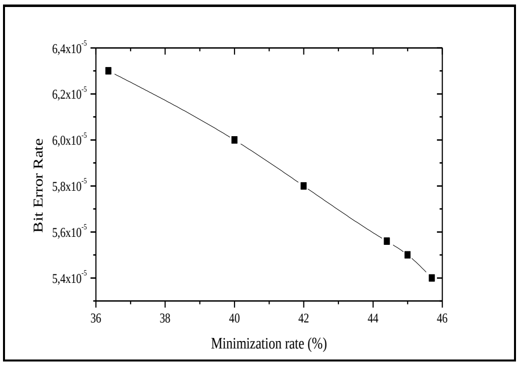

Figure 9. Evolution of the bit error rate BER depending on the minimization rate

Commensurate with the basic design, the simulation result is plotted in Fig. 5, the obtained result is similar to that of the new proposed algorithm as shown in Fig. 7, but we can say the decreased number of hardware resources. The adopted factorization method offers a very important decreasing of the power consumption with a percentage which can reach approximately 40 % compared to the basic algorithm [16] [17]. Also, it offers better BER values.

4.3 Experimentation Results

The workstation is equipped with the following items: Personal computer with Intel Dual-core processor 2.30 GHz and 4 GB RAM, Xilinx software and Xilinx Spartan 3E-500 FG 320 FPGA (xc3s500e-5fg320) as shown in Fig.10.

Figure 10. A typical station setup

At experimentation level, A Xilinx ISE (Integrated Synthesis Environment) software and Hardware Description Language (HDL) are used for developing and implementing the embedded block for RS or BCH decoder as shown in Fig.11.

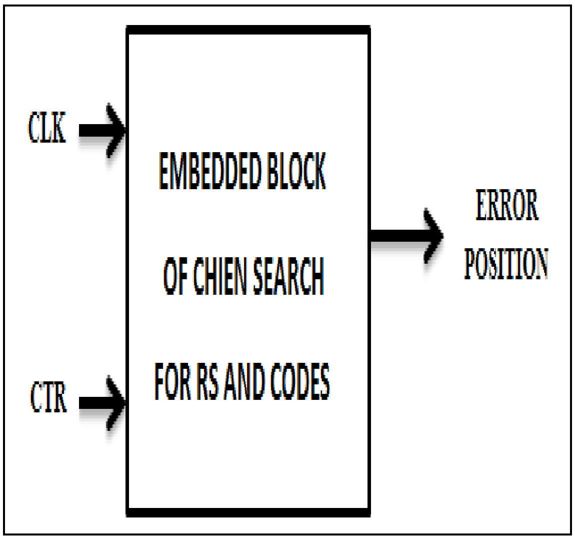

Figure 11. Embedded Block diagram of Chien Search

The proposed Chien Search Block consists of a global 'Clk' and the error detection process is initiated by an 'Input', the 'Error position' can be obtained immediately after entering input.

Also, the proposed system is designed, implemented and executed on a Xilinx Spartan 3E-500 FG 320 FPGA (xc3s500e-5fg320). This FPGA ensures the reconfiguration of its architecture for each new design. Especially, error correcting codes. It is highly used for compute intensive designs demanding very large amount of hardware resources [18] [19] [20].

For testing and verifying the theoretical results, effectiveness and robustness of our improved algorithm, we validated it by considering a concrete scenario, so this is a specified Code for DVB-T according to the following specifications:

The DVB-T standard specifies a (255, 239, t=8) Reed-Solomon code, shortened to form RS (204, 188, t=8) code, so that the 188 bytes of the input packet will be extended with parity bytes to produce a coded block length of 204 symbols [21]. For this code, the Galois field has 256 elements (m=8) and the polynomial representation of a field element is:

$$a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x^1 + a_0 \quad (9)$$

Corresponding to the binary numbers 00000000 to 11111111. Alternatively, we can use the decimal equivalents 0 to 255. The specification also mentions the field generator polynomial, given as:

$$P(x) = x^8 + x^4 + x^3 + x^2 + 1 \quad (10)$$

For the case of RS (255, 239) used in DVB-T standard, the decoder can detect 16 errors and correct 8 errors.

Fig.12 shows the experimentation results. Notice that when the proposed system was implemented and exceeded on FPGA board. In addition, a comprehensive testing environment was developed to test the implemented algorithm [22] [23] [24].

From Fig.12 (a), it is clear that the non-zero result shows that this position does not contain an error, On the other hand in Fig.12 (b) the value is equal to zero, so this position contains an error. Thus, experimental results on the tested scenario show that the proposed system is very effective and achieves high performance in the detection of errors.

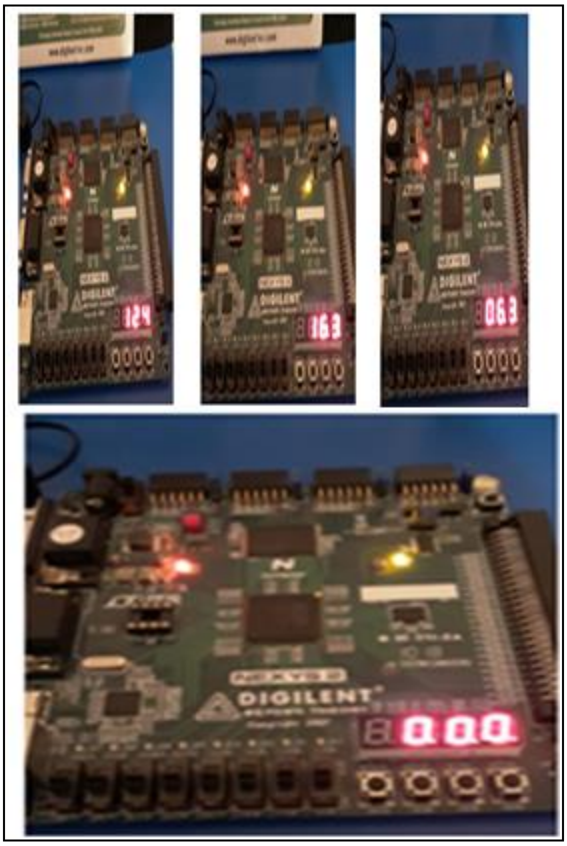

Figure 12. Values of Chien search block for RS (255, 239) codes

4.4 Discussion of Experimentation Results

Real time Implementation of the improved and basic system of RS (255, 239) was effected on Xilinx Spartan 3E-500 FG 320 FPGA (xc3s500e-5fg320) devices. Also, a Xilinx ISE software version 14.1 is used. The synthesis results of the two architectures are shown in Table 2. This table shows the slices and input-output blocks used in this architecture.

Thus, the proposed algorithm presents a low complexity and a very good performance compared to the basic one.

Table 2. Comparison Report of Implemented Algorithm for RS (255, 239)

Hardware Recources requirement	Proposed improved design	Basic design
Number of occupied Slice	90	119
Number of LUT Flip Flops pairs used	39	95
Number of 4 input LUTs	504	196
Number of used as logic	504	196

5. Conclusion

This research paper aims to present an efficient optimized new algorithm of Embedded Chien Search Block for RS and BCH codes. This algorithm is based on a new technique of factorization for error locator polynomial so as to reduce the number of minimized logic gates. This algorithm reduces the power consumption with a percentage which can reach 40% compared to the basic one. The proposed algorithm has been generated and simulated using the hardware description language VHDL and Quartus, then implemented on a Xilinx Spartan 3E-500 FG 320 FPGA (xc3s500e-5fg320). The results show that the proposed algorithm requires reduced hardware resources compared to the basic algorithm.

References

[1] M. Alam et al., “Real Time Modeling and Processing for Communication Systems,” Lecture Notes in Networks and Systems, 2018.

[2] Christos Koulamas and Mihai T. Lazarescu , “Real-Time Embedded Systems: Present and Future,” Electronics, vol. 7, no. 9, 205, 2018.

[3] Sasirekha GVK, Gangaraju KM, “Forward Error Correcting System for Wireless E1 ATM Links”, International Journal of Computer Science, vol. 35, no. 3, pp 1534-1539, 2008.

[4] Haesik Kim, Wireless Communications Systems Design, 1st Edition, John Wiley and Sons Ltd, 2015.

[5] John G. Proakis and Masoud Salehi, “Digital Communications,” 5th Edition, McGraw-Hill Education, 2007.

[6] Irina Bocharova et al., “Low Delay Inter-Packet Coding in Vehicular Networks,” Future Internet journal, vol. 10, no. 10, 2019.

[7] A. Alotaibi, “Implementation of (255, 223) Reed Solomon Code Encoder /Decoder,” California State University, Northridge, 2012.

[8] Mohamed Haj Taieb, Jean-Yves Chouinard and Demin Wang , “Low Complexity Rate Estimators for Low Latency Wyner-Ziv Video Decoders,” Engineering Letters, vol. 21, no. 1, pp 1-9, 2013.

[9] A. Al Azad, MI. Shahed, “A Compact and Fast FPGA Based Implementation of Encoding and Decoding Algorithm Using Reed Solomon Codes,” International Journal of Future Computer and Communication, vol. 3, no .1, pp. 31–35, 2014.

[10] Asif Muhammad and Shah, Tariq, “BCH Codes with Computational Approach and its Applications in Image Encryption,” Journal of Intelligent & Fuzzy Systems, vol. 37, no. 3, pp. 3925–3939, 2019.

[11] Martin Tomlinson et al., “Error-Correction Coding and Decoding: Bounds, Codes, Decoders, Analysis and Applications,” 1St Edition. Kindle Edition, 2017.

[12] V. Tilavat, Y. Shukla, “Simplification of Procedure for Decoding Reed-Solomon Codes using various Algorithms: An introductory Survey,” International Journal of Engineering Development and Research, vol. 2, no. 1, pp. 279–283, 2014.

[13] R. Huynh, G. Ning and Y. Huazhung, “A Low Power Error Detection in the Syndrome Calculator Block for Reed-Solomon Codes RS: (208,188) ,” J. Tsinghua Science and Technologie, vol. 14, no. 4, 474–477, 2009.

[14] Anna-Lena Horlemann-Trautmann and Margreta Kuijper, “A Module Minimization Approach to Gabidulin Decoding via Interpolation,” J. Algebra Comb. Discrete Appl, vol. 5, no. 1, pp. 29-43, 2018.

[15] Saïd Nouh et al., “Decoding of Block Codes by using Genetic Algorithms and Permutations Set,” International Journal of Communication Networks and Information Security (IJCNIS), Vol 5, No. 3,pp. 201-209, 2013.

[16] H. Bartz and V. Sidorenko, “On Syndrome Decoding of Punctured Reed-Solomon and Gabidulin Codes,” Electronic Notes in Discrete Mathematics, vol. 57, pp. 33–38, 2017.

[17] Jiongyue Xing et al., “Progressive Algebraic Soft Decoding of Reed-Solomon Codes Using Module Minimization,” in IEEE International Symposium on Information Theory (ISIT), 2018, pp. 11-15.

[18] Anas EL HABTI, Azeddine WAHBI, Rachid EL GOURI, Laamari HLOU, “Energy Efficient of Error Detection in the Chien Search Block for Reed-Solomon Codes with Hardware Implementation on FPGA Card,” in 4th Mediterranean Congress of Telecommunications (CMT’14), Mohammedia, Morocco, Mai 2014.

[19] D. Chaudhari, M. Bhujade, P. Dhumal, “VHDL Design and FPGA Implementation of Reed-Solomon Encoder and Decoder for RS (7, 3),” International Journal of Science, Engineering and Technology Research, vol. 3, no. 3, pp. 563–566, 2014.

[20] Manju Mangtani, “Implement Reed Solomon Encoder/ Decoder Using Spartan FPGA,” Journal of Research in Engineering and Applied Sciences, vol. 1, no. 4, pp. 199-205, 2016.

[21] BBC Research and Develompment, “Reed-Solomon Error Correction,” British Broadcasting Corporation, Research & Development, 2002.

[22] A. El Habti, R. El Gouri,A. Lichioui, H. Laamari, “Performance Study and Synthesis of New Error Correcting Codes RS, BCH and LDPC Using the Bit Error Rate (BER) and Field-Programmable Gate Array (FPGA) ,” International Journal of Computer Science and Network Security, vol. 16, no. 5, pp. 21-28, 2016.

[23] Wali Ullah Khan, Furqan Jameel, Muhammad Ali Jamshed, Haris Pervaiz, Shafiullah Khan, JuLiu, Efficient power allocation for NOMA-enabled IoT networks in 6G era, Physical Communication, Vol. 39, April 2020.

[24] M. Sohail, S. Khan, R. Ahmad, D. Singh, J. Lloret, Game Theoretic Solution for Power Management in IoT-Based Wireless Sensor Networks, Sensors, 19(18), 2019.