International Journal of Engineering & Technology, 7 (2.8) (2018) 397-403

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

FPGA implementation of RGB image encryption and decryption using DNA cryptography

Fazal Noorbasha*, K. Suresh

Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
**Corresponding author E-mail: [1]fazalnoorbasha@kluniversity.in*

Abstract

The rapid growth in digitization transmission of information in the form of RGB image. During the process transmission of the image in a channel, some data may be degraded due to noise. At receiver side error in data has to be detected and corrected. Hamming code is one of the popular techniques for error detection and correction. In this paper new algorithm proposed for encryption and decryption of RGB image with DNA cryptography and hamming code for secure transmission, and correction. this algorithm first encodes data to hamming code and encrypted to DNA code. Two-bit error detection and correction for each pixel of the image can be performed.DNA code improves security and use of the Hamming code for error detection and correction. For the image of size 256*256 pixel image, it corrects up to 2*256*256 bits in RGB image. The RGB image encryption and decryption design using Verilog and implemented using FPGA (Field Programmable Gate Array).

Keywords: *RGB Image, Hamming code, DNA cryptography, Error detection and correction.*

1. Introduction

In The recent years, rapid growth in technology in the form of digitization and media. The transmission of information not only in the form of data but also in the form of an image. Mainly images are used in many application such as social media, satellite communication, military, medical imaging and advertising etc. These images are to be transmitted through unsecured channel or platform such as hard drive, emails, server etc, the main issue of protecting privacy, confidentiality, genuineness, and accuracy is a major concern. Information in the form of image exchanged in the presence of third parties. There is a need for algorithms to hide the information for security. There are no of algorithms designed for data security used in cryptography domain. Cryptography technique used to hide the information in the ciphertext or by using the key. cryptography use symmetric and asymmetric algorithms. With the recent growth in DNA cryptography methods applied from text to image.

The digital image is two-dimensional data, each pixel represents different color intensity varies from 0 to 255 values in decimal represented in 8-bit form. Due to the large amount of data conventional encryption methods such as AES and DES etc not used. DNA encryption explained [1-2] using conventional methods. Different encryption methods based on DNA cryptography explained in [3-4]. DNA encryption algorithm using a one-time pad (OTP), the chaotic map used to encrypt images [5],[6] Lorenz system along with DNA cryptography to encrypt color image. RGB image encryption using DNA encoding and elliptic curve Diffie-Hellman cryptography [7].

A. DNA Encoding

DNA means deoxyribonucleic acid formed using 4 basic nucleic acids namely Adenine(A) , Cytosine(C), Guanine(G) , Thymine(T) ,the pairs (A,T) and (C,G) are complement each other Binary values assigned to A,C,G, and T are shown in TABLE:1, Fig1: show structure of DNA .

Table 1: DNA Binary Equivalent Value

A	**00**
C	**01**
G	**10**
T	**11**

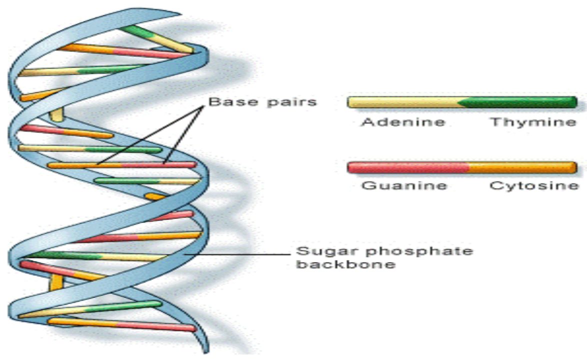

Fig. 1: Structure of DNA

B. Hamming Code

The major issue in communication is the secure transmission of data from a transmitter to the receiver, there are no of technologies used for error correction one is the Hamming code used for error detection and correction. Hamming code is linear block codes improved over parity code method for error detection and correction by using Forward Error Correction (FEC). In digital communication mainly military, security and data compression immune to noise, among various methods FEC is efficient [8,9,10]. Redundant bits are added including parity bit at the transmitter and removed at receiver. Usage of parity enables detecting and correcting single bit error in received messages. For hamming code depend on redundant bits data transmitted, for example, 4 bits of data 3 redundant bits of data are added general formula for representation of hamming code is

$(2^n-1, 2^n-n-1)$,

Where n= no of redundant bits;
2^n-1=block size;
2^n-n-1=no of data bits;

For 4-bit data hamming code represented as (7,4) and extra parity bit added during transmission, by using parity bits hamming code can detect and correct single bit error. (7,4) Hamming code algorithm [11,12,13] implemented using VLSI including error correction explained.

2. Encryption Process

The RGB image is a combination of three channels as RED, GREEN and BLUE channels, Each channel image combination of pixel values of different levels vary from 0 to 255 in decimal value. DNA cryptography with different algorithms used in digital coding [14,15]. Here in this the process of converting the RGB image into DNA code including hamming code to each pixel of an image. The process of encryption is shown in Fig: 2.

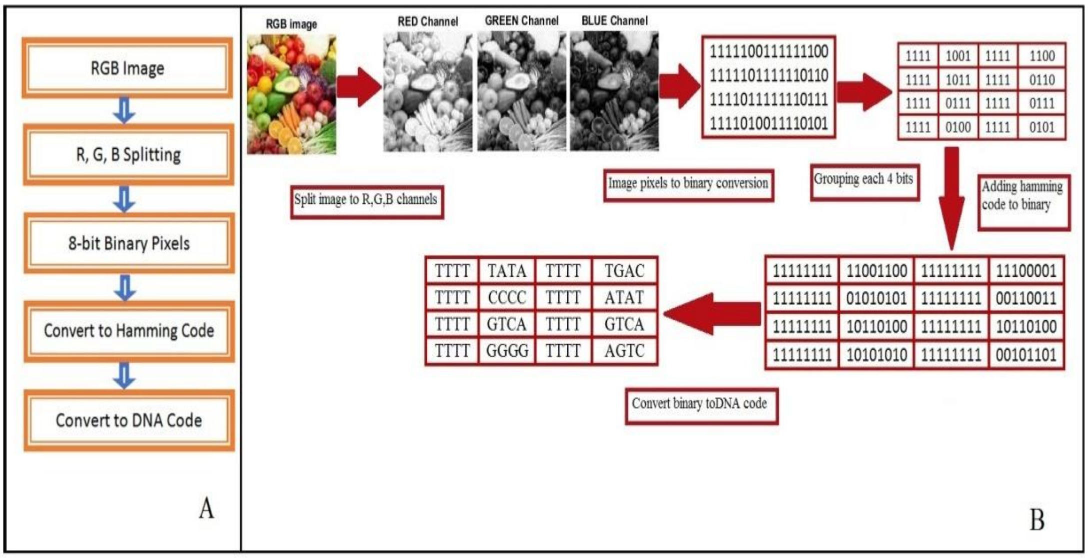

Fig. 2: Encryption process flow A) Flowchart, B) Diagrammatic representation.

As shown in Fig2B: RGB image is taken as input and split the image into Red, Green, Blue channels respectively channel and convert channels to the binary equivalent of pixels and group every 4 bits of binary. Add hamming code including parity to 4bit binary and then encrypt binary data to DNA code, the RGB image is encrypted to DNA code and transmitted as three separate channels i.e Red, Green, Blue channels of DNA encrypted data.

Steps of Encryption process flow :

STEP1: 8-bit RGB image is considered as the input image.

STEP2: Split RGB image into separate Red, Green, Blue channels.

STEP3: Convert each pixel value in decimal into 8-bit binary.

STEP4: Add hamming code to each 4bits of the pixel along with parity bit.

STEP 5: Binary hamming code is converted into DNA code in the form of ACGT, Assign binary values A=00, C=01, G=10, T=11 respectively.

Consider 4 bits of binary data and convert data to hamming code example shown below.

Input data: $D_4D_3D_2D_1$

Code data bits (C1, C2, C3):

$$C1 = D4 \oplus D2 \oplus D1;$$
$$C2 = D4 \oplus D3 \oplus D1;$$
$$C3 = D4 \oplus D3 \oplus D2;$$

Parity bit P=$C1 \oplus C2 \oplus C3 \oplus D4 \oplus D3 \oplus D2 \oplus D1$;

Hamming code = P D_4 D_3 D_2 C3 D_1 C2 C1;

For four-bit data hamming code have length 8bit and code bits are added for 1,2 and 4thbit positions, parity bit added at MSB position.

Example: Input data =1101;

Code bits are C1=1 0 1=0;
C2=1 1 1 =1;
C3=1 1 0=0;
P=1 1 0 0 1 1 0 =0;

Hamming code =01100110;

After adding hamming code to each 4bit of pixel each pixel 8bit is converted to 16 bit data .

Fig:3 shows pixel value converted to hamming code and then to DNA encrypted code.

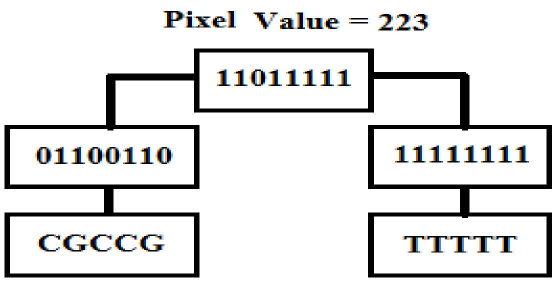

Fig. 3: Pixel value to DNA code conversion

3. Decryption Process

At receiver end during decryption process encrypted DNA code of Red, Green, Blue channels is taken as input. Complete flow for decryption process shown in fig:4.

DNA code is converted to binary hamming code, then to equivalent decimal and combines to get RGB image [16].

As shown in fig:4B) Received DNA code is decrypted to hamming code and then converted to four bit binary equivalent and group binary values to get image for channels and combine channels to get RGB image.

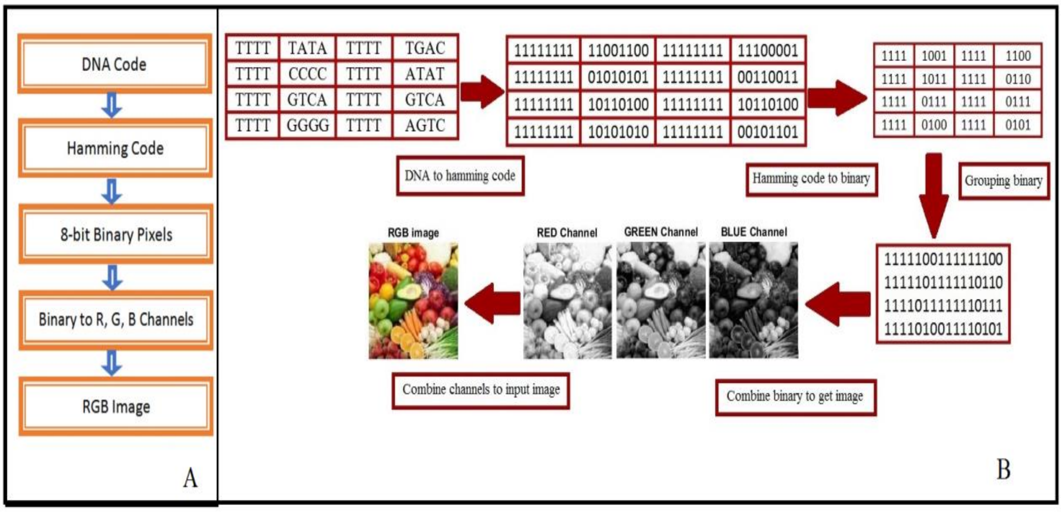

Fig. 4: Decryption process of RGB image. A) Flowchart, B) Diagrammatic representation of flow

Steps of decryption process:
STEP1: Encrypted DNA code of R, G, and B channels are taken as input.
STPE2: Convert DNA code to equivalent binary data of hamming code.
STEP3: Hamming code for the 8-bit binary pixel value conversion. During conversion process error detection by using check bits in hamming code and data can be corrected.
STEP4: Pixel value in binary to Decimal equivalent of Red, green, Blue channels.
STEP5: Combine three (RED, GREEN, BLUE) channels to get RGB image.

4. Simulation Results

RGB image encrypted to DNA code conversion process explained in fig: 2 conversion of each pixel value of the image to equivalent binary and add hamming code including parity bit to every 4 bits of the pixel, binary data converted to DNA code in the form of A, C, G and T values. Simulation results for encryption how RGB image split into three channels shown in Fig:5 and binary pixel values of Red, Green and Blue channels converted to DNA encryption output shown in fig:6. Encrypted data is transmitted to the transmitter as three separate channels.

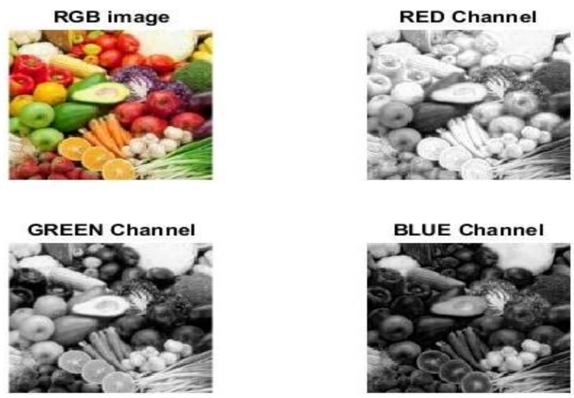

Fig. 5: Split RGB image into three channels.

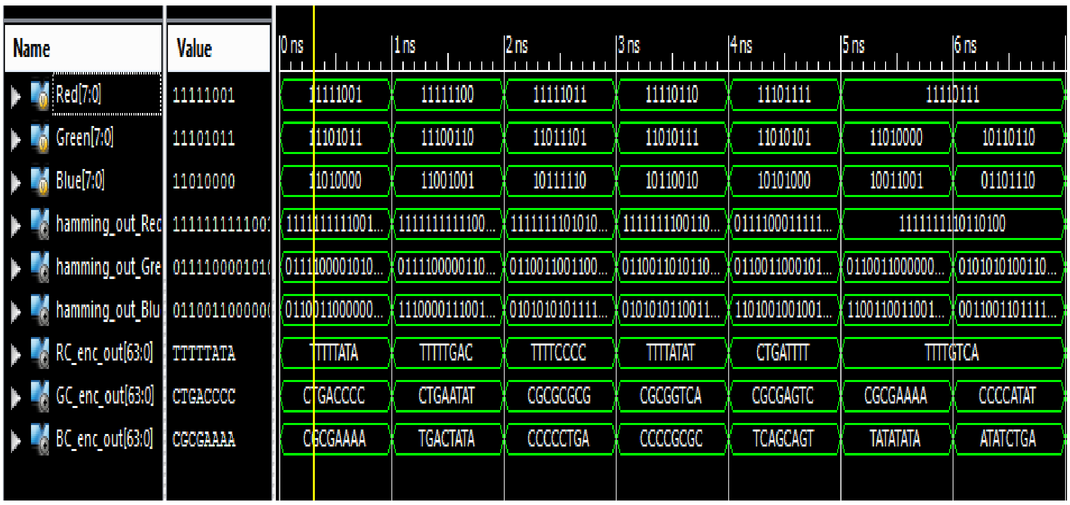

Fig. 6: DNA encryption of RGB image.

At receiver during decryption process conversion of DNA to image flow explained in Fig: 4. At the receiver end, it can detect an error occurred in pixels value by using check bits at receiver. The conversion of DNA code to binary pixel values shown in Fig:7.

An error has occurred can be checked during transmission by using check bits for hamming code, If check bit value is zero then received data has no error. If check bit is not zero depending on check bit value receiver can predict the position of error and it can be corrected. Decryption of image, DNA code converted to pixel value shown in fig:7. Recovered pixel values are converted to red, green and blue channels and combine channels to get RGB image is shown in fig:8.

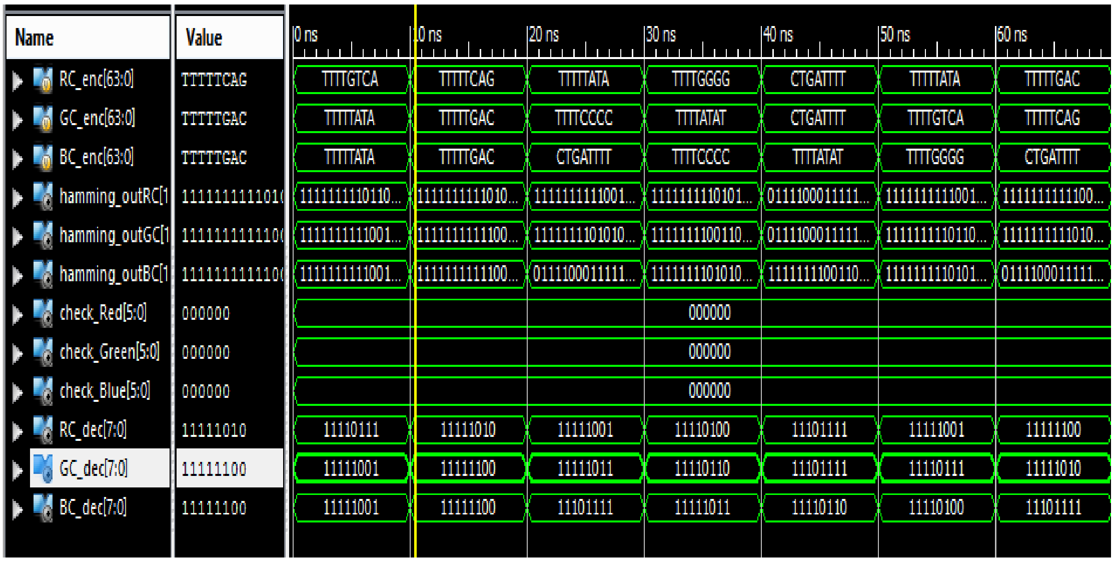

Fig. 7: Decryption of DNA code to pixel values of the image.

Fig. 8: Decryption of RGB image.

5. Error Detection and Correction

A. Error Detection

Hamming code used for the variable length of data, In this paper, perform hamming code for 4bits of the pixel. During encryption process code bits are added for hamming code discussed during the encryption process. By using check bits receiver can check data received correctly or not, If data received correctly the value of check bits are 000 else data received have some error, Depend on the value of check bits position of error can be known.

Check data (3 bit)A:

$A1 = C1 \oplus D4 \oplus D2 \oplus D1;$

$A2 = C2 \oplus D4 \oplus D3 \oplus D1;$

$A3 = C3 \oplus D4 \oplus D3 \oplus D2;$

Received end check bit data generated using received hamming 8-bit code including parity. If A=000 no error, if it is having some value then there exists an error by changing value 0 to 1 or 1 to 0. error detection for using hamming code check bits shown in TABLE 1.

Table 1: Error Detection Using Check bits

Check data A3A2A1	Error bit position	Corrected data	
000	0	No change	
001	1	0 to 1	1 to 0
010	2	0 to 1	1 to 0
011	3	0 to 1	1 to 0
100	4	0 to 1	1 to 0
101	5	0 to 1	1 to 0
110	6	0 to 1	1 to 0
111	7	0 to 1	1 to 0

Error Detection for hamming code using check bits for received data is shown in fig: 9.

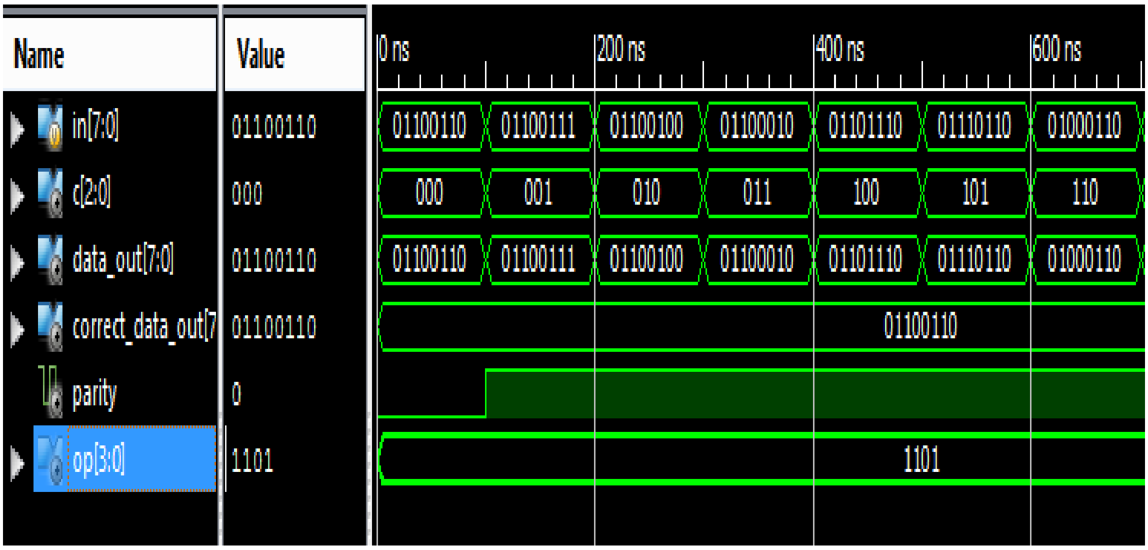

Fig. 9: Error detection using check bit position

B. Error Correction

Error correction for hamming code received data by using check bits and parity bits. Error position in MSB bit i.e 8^{th} bit can be known by using parity for data. Hamming code for 4-bit data given as input and error position detected using check bit and parity. Single bit error correction can be implemented using both check and parity bits, sometimes an error occurs in parity bit position also it cannot be detected by check bits but it can be detected by using parity, Table :2 describe error correction for one bit and more than one bit by using parity and check bit .If more than a one-bit error occurs it can not be corrected. Error correction for one bit shown in Fig10.

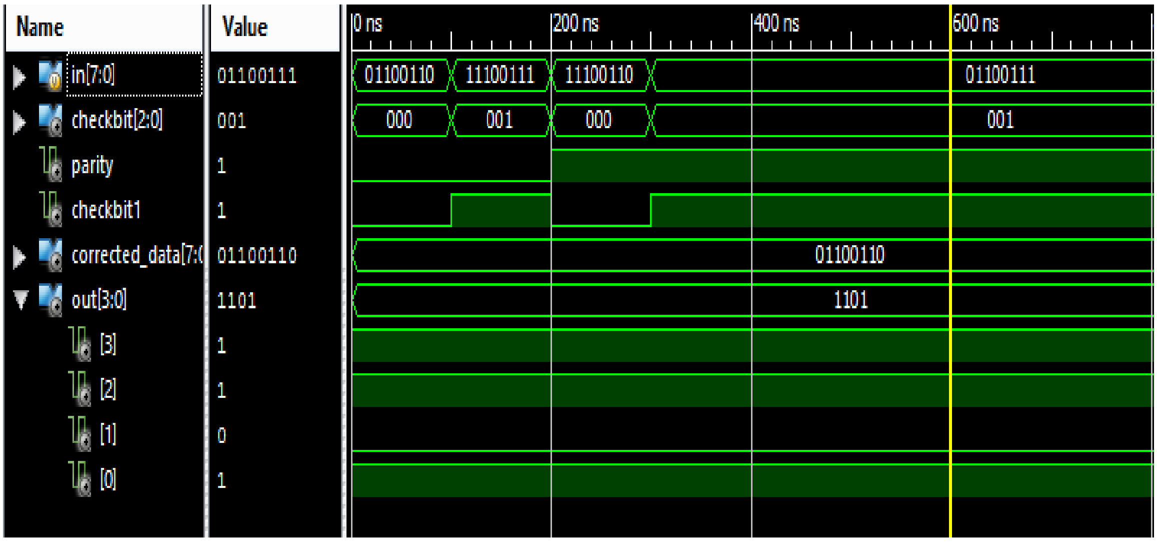

Fig. 10: Error correction for one bit using check bit and parity.

Table 2: Error correction of hamming code data using check bits and parity

Parity	Check bit	No of errors	Description
0	0	0	No error
1	0	0	Error in parity
0	1	1	Correct up to one error
		>1	No error correction
1	1	1	Correct up to one error including parity
		>1	No error correction

Error correction for 4bit data using the hamming code shown in fig:10; For 8-bit pixel data it corrects up to 2bit by performing hamming code for every 4 bit in pixel value. It improves error correction rate when compare to the hamming code applied to 8-bit data.

6. Synthesis Results

Encryption, Decryption and error correction of RGB image designed in Verilog and implemented using FPGA. RTL view of Encryption, Decryption and error correction are shown in fig: 11.

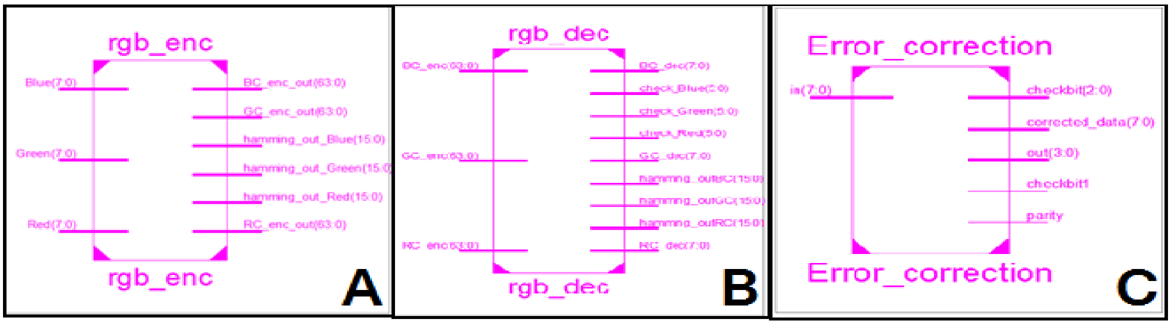

Fig. 11: Synthesis result A) RTL view of Transmitter, B) RTL view of Receiver, C) RTL view of error correction.

After implementation for Encryption, Decryption and Error correction in field programmable gate array (FPGA) device utilization shown in TABLE:
3.

Table 3: Device utilization

Name	Transmitter	Receiver	Error correction
No of LUT	42	42	14
No of slices	114	114	14
IO's	282	72	33
Dleay	6.37ns	5.43ns	2.32ns

7. Conclusions

A secured system designed for Encryption and decryption system for RGB image using DNA cryptography, Hamming code added to every 4 bits of the pixel of the image. It improves error correction up to 2bits for each pixel value, considers 256*256 pixel image get error correction up to 2*256*256 bits. Secured image transmission using DNA cryptography achieved and error detection and correction by using hamming code. It is designed in Verilog and implemented using FPGA maximum delay for implementation of the circuit is 6.37ns.

References

[1] G.Xiao, M.Lu, L.Qin, X.Lai "New field of cryptography: DNA cryptography," Chinese Science Bulletin, vol.51 (10), pp.1139-114, Jun 2006.

[2] Fazal Noorbasha, Harikishore Kakarla, Deekshatha.A, P.G.Mounika, N.Ganga Dheeraj, M. Manasa, "Implementation of Quarter Cycle Key Cryptographic Algorithm Using Verilog HDL", International Journal of Pure and Applied Mathematics, ISSN 1311-8080. Volume115, No.7, 2017, PP. 423-427.

[3] T.Head G.Rozenberg, R.S.Bladegroen , C.K.D.Breek , P.H.M.Lommerese,H.Pspalink, "computing with DNA by operating on plasmids", Biosystems 57(2)(2000) 87-93.

[4] X.DZheng, J.xu.W.Parallel, "DNA arithmetic operation based on n-module set", Applied Mathematics and Computation, 212(1) (2007) PP.173-84.

[5] X.Y Wang, Y.Q, Zhang, X.M Bao, "An oval chaotic image encryption scheme using DNA sequence operations", Optic laser Eng 73(1) (2015) 53-61.

[6] Q.zhang, x.wei," RGB color image encryption method based on Lorenz chaotic system and DNA computation".IETE Rev 30(5) (2013) 404-409.

[7] Manish Kumar, Akhlad Iqbal, Pranjal Kumar,"A new RGB image encryption algorithm based on DNA encoding an elliptic curve Diffie-Hellman cryptography" signal processing 125(2016) 187-202.

[8] Fazal Noor Basha ,Hari Kishore kakarla, Sri Ramya R,"VLSI implementation of Encryption and Decryption system using hamming code algorithm "Int.Journal of Engineering Research and Applications, 4(1)(2014)52-55.

[9] Fazal Noorbasha, G. Jaswanth Varma, B. Ajani Kumar, Harikishore Kakarla, M. Manasa, "Data Security Based On DNA Cryptography Using S-Box Encryption", International Journal of Pure and Applied Mathematics, ISSN 1311-8080. Volume115, No.7, 2017, PP. 429-434.

[10] Fazal Noorbasha, B. Anjani Kumar, G. Jaswanth Varma,Harikishore Kakarla, M. Manasa, "Data Encryption and Decryption Cryptography Using Modified AES Algorithm", International Journal of Pure and Applied Mathematics, ISSN 1311-8080. Volume115, No.7, 2017, PP.435-440.

[11] [11] Fazal Noorbasha, M. Manasa, R. Tulasi Gouthami, S. Sruthi, D. Hari Priya, N. Prashanth, And Md. Zia Ur Rahman, "FPGA Implementation Of Cryptographic Systems For Symmetric Encryption", Journal of Theoretical and Applied Information Technology, 15th May 2017. Vol.95. No 9, PP. 2038-2045, ISSN: 1992-8645.

[12] M. Manasa, Fazal Noorbasha, Ch.L.Sudheshna, M.Santhosh, V.Naresh, Md. Zia Ur Rahman, "Comparative Analysis of CORDIC Algorithm and Taylor Series Expansion ", Journal of Theoretical and Applied Information Technology, 15th May 2017. Vol.95. No 9, PP. 2015-2022, ISSN: 1992-8645.

[13] Upputuri Neelima, Fazal Noorbasha, "Data Encryption and Decryption using Reed-Muller Techniques", International Journal of Engineering and Technology (IJET), ISSN : 0975-4024 Vol 8 No 1 Feb-Mar 2016, PP. 83-91

[14] Dr. Ananathi Shesashaayee, D Sumathy, "OTP Encryption Techniques in Mobiles for Authentication and Transaction Security" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 10, October 2014, PP 6193-6201.

[15] Vishal Krishnan, Hanumesh H, Prateek D Nayak, Krishanmurty M S, "OTP Authenticated and Encrption on Cloud Data", SEA International Journal of Advanced Research in Engineering, Vol. 1, Issue 1, 2016, PP 1- 6.

[16] Ramesh K., Ramesh S., "Implementing One Time Password Based Security Mechanism for securing personal health records in cloud", International conference on control, instrumentation, communication and computational technologies (ICCICCT) 10 Jul - 11 Jul 2014, PP 968 – 972.

[17] Dr. Seetaiah Kilaru, Hari Kishore K, Sravani T, Anvesh Chowdary L, Balaji T "Review and Analysis of Promising Technologies with Respect to fifth Generation Networks", 2014 First International Conference on Networks & Soft Computing, ISSN:978-1-4799-3486-7/14,pp.270-273,August2014.

[18] Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs" Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.

[19] P Bala Gopal, K Hari Kishore, R.R Kalyan Venkatesh, P Harinath Mandalapu "An FPGA Implementation of On Chip UART Testing with BIST Techniques", International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 14 , pp. 34047-34051, August 2015.

[20] A Murali, K Hari Kishore, D Venkat Reddy "Integrating FPGAs with Trigger Circuitry Core System Insertions for Observability

in Debugging Process" Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.11, Issue No.12, page: 2643-2650, December 2016.

[21] Mahesh Mudavath, K Hari Kishore, D Venkat Reddy "Design of CMOS RF Front-End of Low Noise Amplifier for LTE System Applications Integrating FPGAs" Asian Journal of Information Technology, ISSN No: 1682-3915, Vol No.15, Issue No.20, page: 4040-4047, December 2016.

[22] N Bala Dastagiri, Kakarla Hari Kishore "Reduction of Kickback Noise in Latched Comparators for Cardiac IMDs" Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.43, Page: 1-6, November 2016.

[23] S Nazeer Hussain, K Hari Kishore "Computational Optimization of Placement and Routing using Genetic Algorithm" Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.47, page: 1-4, December 2016.

[24] Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs" Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.

[25] N Bala Dastagiri,, K Hari Kishore "Analysis of Low Power Low Kickback Noise in Dynamic Comparators in Pacemakers" Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.44, page: 1-4, November 2016.

[26] S.V.Manikanthan and V.Rama"Optimal Performance of Key Predistribution Protocol In Wireless Sensor Networks" International Innovative Research Journal of Engineering and Technology ,ISSN NO: 2456-1983,Vol-2,Issue –Special –March 2017.

[27] T. Padmapriya, V.Saminadan, "Performance Improvement in long term Evolution-advanced network using multiple imput multiple output technique", Journal of Advanced Research in Dynamical and Control Systems, Vol. 9, Sp-6, pp: 990-1010, 2017.