FPGA Based DNA Cryptography System for Medical Image Data Analysis Process

Fazal Noorbasha, S. Mohit Srinath, SK. Khadir Bhasha, P. Jagadish, K Hari Kishore

Abstract: Field Programmable Gated Array (FPGA) has been utilized for various prototyping and cryptographic algorithm and system applications. Because of the parallel and reprogrammable engineering of FPGAs, the adaptability of cryptographic algorithm can be exploited to accomplish high throughputs to the detriment of very small chip area. New methods have come into the scene to diminish the activity while maintain up the adequate level of security. Partial encryption is one of the methods which specifically encrypt and decrypt the bulky medical images. Meanwhile, if a similar medical image is should have been reused for another diagnosis, at that point it is prescribed to secure the whole medical image. In this research, we propose low cost FPGA based DNA cryptosystem gives high throughput to region proportion for medical data getting to process.

Keywords: FPGA, DNA, Cryptography, Image, Medical.

I. INTRODUCTION

Data security has been an issue of real interest since decades. In the process of communicating data, the systems of data swapping has been reformed consequently the need of data validness and integrity has additionally essential. Different cryptosystems and algorithms have been anticipated in such manner. A cryptosystem is hardware or programming that can change the data from its unique comprehensible form into a mixed form so that the original data can be uncovered to some chosen people only [1]. Cryptosystems have developed throughout the years from Ceaser's figure, which depended on simply moving of letters, to the modern AES (Advanced Encryption Standard) proposed by Vincent Rijmen and Joan Daemen. Cryptographic hardware designs have been one more field of enthusiasm for some analysts [2]. Several of hardware cryptosystems have been implemented in which the inclination of hardware might be microprocessors, microcontrollers, and custom ASICs based cryptosystems [3]. Swift development in the field of information technology and drug has expanded the utilization of digital medical images in a few applications, for example, tele-diagnosis, tele-surgery and so on.

Revised Manuscript Received on April 14, 2019.

Fazal Noorbasha, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India

S. Mohit Srinath, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India

SK. Khadir Bhasha, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India

P. Jagadish, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India

K Hari Kishore, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India

The expensive use of medical image over the open system has made the researchers to carry out intensive research on processing, compacting/compressing and securing the medical images. Cryptography, the field of computer science and mathematics gives various algorithms to overcome the security challenges of a variety of data including text documents, multimedia records and medical pictures [4]. Cryptographic systems have been used for a long time starting now and into the foreseeable future. That is cryptography consists in processing plain data by applying a figure and acquiring encoded output, which would seem meaningless to a third party who does not know anything about the key includes at least one keys.

The quantity of cryptographic algorithm as far as encryption and digital signature has been accounted for in the literature. The traditional encryptions like DES (Date Encryption Standard), AES (Advanced Encryption Standard) as well as Triple DES have done great work over the textual data and digital image. But these techniques cannot be used over medical images because of their several behaviors like bulky data size and high redundancy [5]. Specific images encryption will in general limit the handling time while keeping up the adequate dimension of security. This has attracted researched to develop some specific image encryption schemes especially for securing medical images. These algorithms are helpful in several medical applications like mobile health care and wireless medical networking for securing medical images [6]. FPGA is an incorporated circuit that can be reconfigured by planners themselves. With every reconfiguration, which takes just a small amount of a second, a coordinated circuit can play out a totally different function. FPGA applications incorporate DSP applications, imaging, discourse acknowledgment, cryptography, equipment imitating and for some other application explicit employments. We proposed a DNA based cryptosystem to be the rising field for encoding the digital images. The mainly advantage of DNA based algorithm are monstrous/massive parallelism, extremely low power utilization, large data storage and offers unbreakable cryptosystem.

II. DNA BASED ENCODING AND KEY GENERATION PROCESS

DNA means deoxyribonucleic acid formed using 4 basic nucleic acids namely Adenine (A), Cytosine (C), Guanine (G), Thymine (T), the pairs as (A,T) as well as (C,G) are complement each other. Figure 1 shows the structure of DNA and Binary values assigned to A, C, G and T.

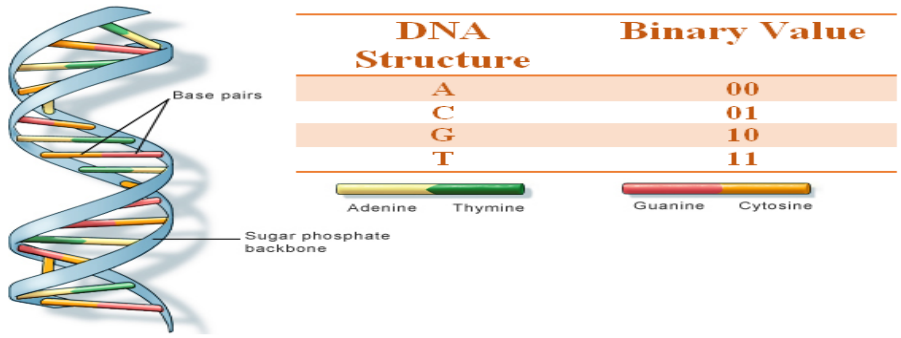

Fig. 1 Structure of DNA and Binary Equivalent Value

By using these DNA bases, one can formulate 24 kinds of encoding rule. But, out of 24 rules, only 8 coding rules which satisfy Watson-Crick complement rule [7]. The 8 encoding rule sets to encode the image pixels as shown in Table 1.

Table. 1 Eight Sets of DNA Encoding Rule

Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7	Rule 8
00-A	00-A	00-T	00-T	00-C	00-C	00-G	00-G
01-C	01-G	01-G	01-C	01-A	01-T	01-A	01-T
10-G	10-C	10-C	10-G	10-T	10-A	10-T	10-A
11-T	11-T	11-A	11-A	11-G	11-G	11-C	11-C

The Advanced Encryption Standard (AES) is 6 times faster than triple DES. A modification for DES was required as its key size was very small. With expanding processing power, it was considered vulnerable against exhaustive key search attach [8]. Triple DES was designed to overcome this drawback but it was found slow. The highlights of AES are symmetric key symmetric block cipher, 128-bit data, 128/192/256-bit keys, Stronger and faster than Triple-DES.
AES is an iterative instead of feistel cipher. It depends on 'substitution– permutation network'. It includes a progression of connected activities, some of which include replacing inputs by explicit yields (substitutions) and others include rearranging bits around (stages). Interestingly, AES performs all its computations on bytes instead of bits. Consequently, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four sections and four columns for handling as a framework [9-10]. Unlike DES, the quantity of rounds in AES is variable and depends upon the length of the key. AES utilizes 10 rounds for 128-piece keys, 12 rounds for 192-piece keys and 14 rounds for 256-piece keys. Every one of these rounds utilizes an alternate 128-piece round key, which is determined from the first AES key.

III. DNA BASED IMAGE ENCRYPTION AND DECRYPTION PROCESS

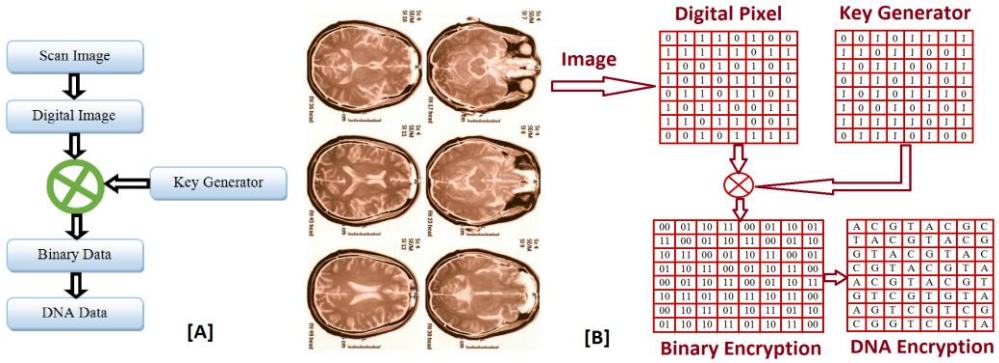

Fig. 2 DNA Encryption process [A] Flowchart and [B] Process Flow

The MRI scan image is converted into pixels and then into binary values and then it is converted into DNA code. The process of encryption is shown in Figure 2A. Figure 2B, shows the Image to DNA encryption cryptography process. The scanned image is converted to pixels using MATLAB and then binary to DNA process.
Steps of involved in the DNA based encryption process:
STEP1: Conversion of analog image into digital pixels
STEP2: Assigning the binary values to each pixel.
STEP3: Binary Key generation (AES algorithm).
STEP4: Encryption: X-OR operation between image binary data and binary key
STEP 5: Binary encryption data is converted into DNA code in the form of A, C, G and T, Assigning binary as A=00, C=01, G=10, T=11 respectively.

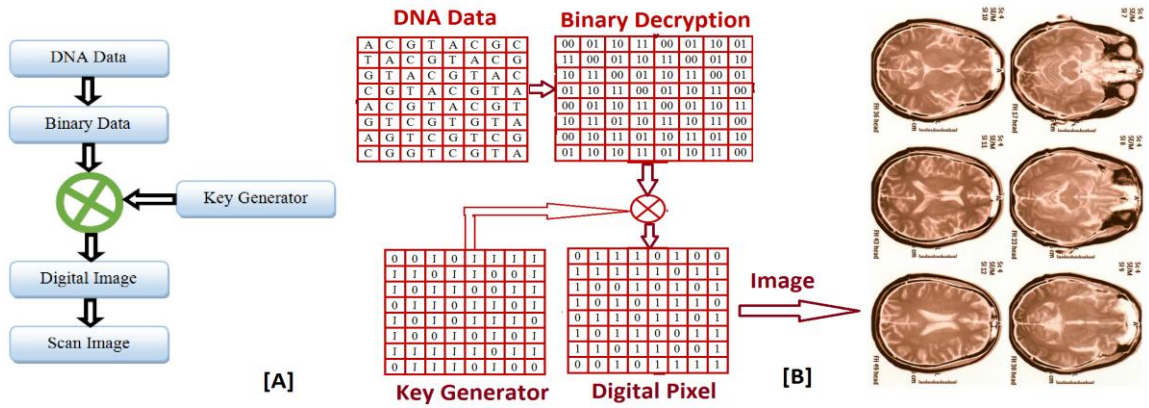

Fig. 3 Decryption process of RGB image. A) Flowchart B) Diagrammatic representation of flow

At receiver end during decryption process encrypted DNA code of MRI image is taken as input. Complete flow for decryption process shown in Figure 3A and 3B. DNA code is converted to binary code, then to equivalent decimal and combines to get image.

IV. FPGA SYNTHESIS ANALYSIS AND SIMULATION RESULTS

FPGAs are becoming a major part of every system. For this DMA cryptography design we used Xilinx (Spartan-3). We developed hardware part by using Verilog HDL code. Figure 4 and Figure 5 are shows the RTL (FPGA) schematic view of Encryption and Decryption modules. The encryption and decryption FPGA device utilization is used as LUTs are 96, input buffers are 84, output buffers 72, number of slices 30 and Global Clocks (GCLKs) are 1. The average connection delay for encryption is 4.8ns. The average connection delay for decryption design is 3.5ns. The total power consumed at encryption side is 11.493 W. The total power consumed at the decryption side is 3.619 W. Figure 6 and Figure 7 shows the simulation timing results of encryption and decryption modules. Table 2 gives the device utilization report.

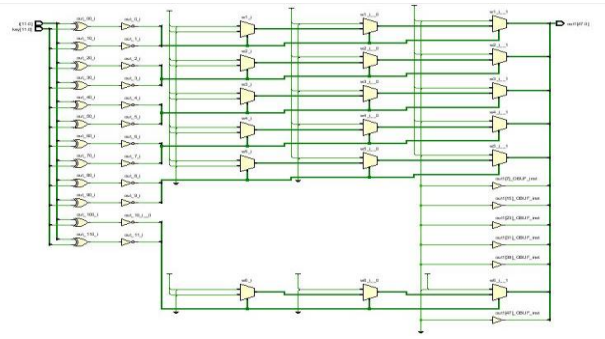

Fig. 4 RTL Schematic of Encryption module

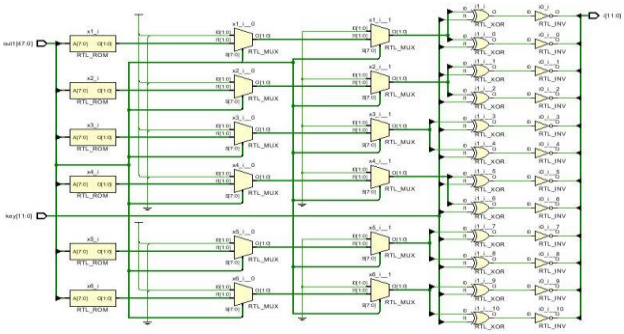

Fig. 5 RTL Schematic of Decryption module

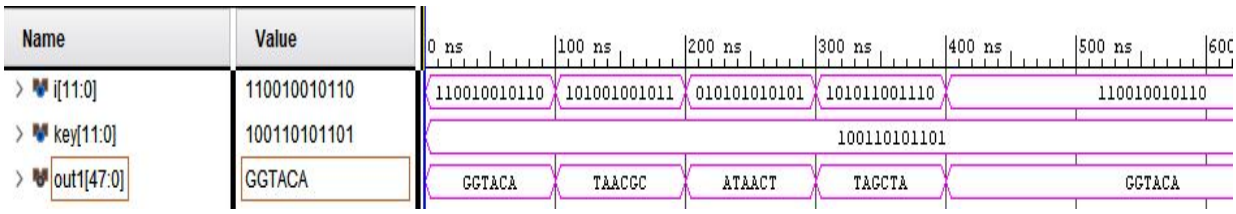

Fig. 6 DNA encryption of MRI image

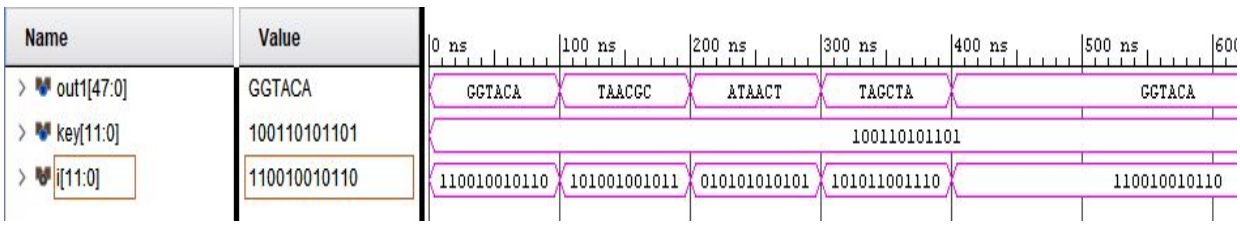

Fig. 7 Decryption of DNA code to pixel values of the image

Table. 2 Device Utilization report

Name of the Device	Encryption Module	Decryption Module
No. of LUT's	24	72
No. of Input Buffer	24	60
No. of Output Buffer	60	12
No. of Slices	12	18

V. CONCLUSIONS

We have proposed a DNA based cryptography algorithm using AES key, that increase complexity in each round thus it can increase the security. So that it increases the efficiency and gives high accuracy. By using same security algorithm, we are optimizing the resource utilization. To implement this designed we have used Verilog HDL. The total process is tested on FPGA Spartan 3 Kit. The total power consumed by encryption module is 11.493 W. The total power consumed by decryption module is 3.619 W. The memory utilization of encryption module is 682.5 MB with the gain of 383.3 as well as for the decryption module the memory utilization is 685.7 MB with the gain of 386.3. For medical images data analysis this algorithm secures the data. New methodologies can help this algorithm in future to diminish the activity while keeping up the adequate level of security.

REFERENCES

1. Muhammad Sohail Ibrahim, Irfan Ahmed , M. Imran Aslam, Muhammad Ghazaal, Muhammad Usman, Kamran Raza and Shujaat Khan, "A Low Cost FPGA based Cryptosystem Design for High Throughput Area Ratio" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 2, 2017, PP. 385-393.
2. M. Ebrahim, S. Khan, and U. B. Khalid, "Symmetric algorithm survey: A comparative analysis," International Journal of Computer Applications, Vol. 61, No. 20, 2014, PP. 12-19.
3. Nisar Ahmed, Hafiz Muhammad Shahzad Asif and Gulshan Saleem, "A Benchmark for Performance Evaluation and Security Assessment of Image Encryption Schemes", I. J. Computer Network and Information Security, Vol. 8, No. 12, 2016, PP.18-29.
4. 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.
5. 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
6. Fazal Noorbasha, C.H. Vainatheyi, R. Goutham, P. Raviteja, B. Karthik, "Implementation of Image Secured Hybrid AES - DNA Algorithm Using Verilog HDL", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 02-Special Issue, 2018, PP. 452-458.
7. G Divya, Fazal Noorbasha, "Implementation of DNA Based Cryptography Using OTP Random Key Generation Process", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 02-Special Issue, 2018, PP. 481-490.
8. Ali Al-Haj, Hiba Abdel-Nabi, "Digital image security based on data hiding and cryptography", 3rd International Conference on Information Management , 21-23 April 2017, PP. 437-440.
9. Dilovan Asaad Zebari, Habibollah Haron, Subhi R. M. Zeebaree, Diyar Qader Zeebaree "Multi-Level of DNA Encryption Technique Based on DNA Arithmetic and Biological Operations", International Conference on Advanced Science and Engineering (ICOASE), Vol.978(1), PP.312-317, 2018.
10. Wenting Yuan, Xuelin Yang, Wei Guo, Weisheng Hu, "A double-domain image encryption using hyper chaos" 19th International Conference on Transparent Optical Networks (ICTON), 2017, PP. 1-4.
11. Yadlapati, A., Kakarla, H.K. An Advanced AXI Protocol Verification using Verilog HDL (2015) Wulfenia, 22 (4), pp. 307-314.
12. Bindu Bhargavi, K., Hari Kishore, K. Low Power Bist on Memory Interface Logic (2015) International Journal of Applied Engineering Research, 10 (8), pp. 21079-21090.
13. Charan, N.S., Kishore, K.H. Recognization of delay faults in cluster based FPGA using BIST (2016) Indian Journal of Science and Technology, 9 (28).
14. Hari Kishore, K., Aswin Kumar, C.V.R.N., Vijay Srinivas, T., Govardhan, G.V., Pavan Kumar, C.N., Venkatesh, R.V. Design and analysis of high efficient UART on spartan-6 and virtex-7 devices (2015) International Journal of Applied Engineering Research, 10 (9), pp. 23043-23052.
15. Kante, S., Kakarla, H.K., Yadlapati, A. Design and verification of AMBA AHB-lite protocol using Verilog HDL (2016) International Journal of Engineering and Technology, 8 (2), pp. 734-741.
16. Bandlamoodi, S., Hari Kishore, K. An FPGA implementation of phase-locked loop (PLL) with self-healing VCO (2015) International Journal of Applied Engineering Research, 10 (14), pp. 34137-34139.
17. Murali, A., Hari Kishore, K., Rama Krishna, C.P., Kumar, S., Trinadha Rao, A. Integrating the reconfigurable devices using slow-changing key technique to achieve high performance (2017) Proceedings - 7th IEEE International Advanced Computing Conference, IACC 2017, art. no. 7976849, pp. 530-534.
18. A. Surendar, K. H. Kishore, M. Kavitha, A. Z. Ibatova, V. Samavatian "Effects of Thermo-Mechanical Fatigue and Low Cycle Fatigue Interaction on Performance of Solder Joints" IEEE Transactions on Device and Materials Reliability, P-ISSN: 1530-4388, E-ISSN: 1558-2574, Vol No: 18, Issue No: 4, Page No: 606-612, December-2018.
19. N Bala Dastagiri K Hari Kishore "A 14-bit 10kS/s Power Efficient 65nm SAR ADC for Cardiac Implantable Medical Devices" International Journal of Engineering and Technology (UAE), ISSN No: 2227-524X, Vol No: 7, Issue No: 2.8, Page No: 34-39, March 2018.
20. 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.
21. 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.
22. 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.
23. 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 and Soft Computing,ISSN:978-1-4799-3486-7/14,pp.248-251,August 2014.
24. 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.
25. Avinash Yadlapati, Hari Kishore Kakarla "Design and Verification of Asynchronous FIFO with Novel Architecture Using Verilog HDL" Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No: 14, Issue No: 1, Page No: 159-163, January 2019.