Hardware Implementation of Hybrid Model Encryption Algorithm for Secure Transmission of Medical Images

M. Senthil Murugan, T. Sasilatha

Abstract:*The advancement of medical field needs a more secure function for sharing the medical related images in the present environment. For making secure transmission of medical images the best solution is cryptography algorithm. There are many cryptography algorithm existing in the market out of the entire algorithm we are select the best encryption algorithm which is really suitable for medical images transmission. Transmission of data is easy at the same time secure transmission are meet the different challenges. To full fill the all the challenges we concentrating the encryption algorithm which is highly secure. For making more secure transmission hybrid model encryption algorithm support more compare to single encryption algorithm. Its having capable of providing confidentiality, authenticity and integrity services to medical images exchanged in telemedicine applications. The same hybrid model encryption may implement in real time application using FPGA device. While implementing in hardware the following factors need to be concentrate more such as power, area, throughput, PSNR, Sensitivity etc. keeping all the factors in mind the hybrid model encryption algorithm are developed for secure transmission of medical images. The aim of the research is to encrypt and decrypt medical images efficiently and effectively protect the transmitted data. This research paper presents a model for encrypting transmitted medical image data. This model uses the following encryption algorithm such as Advanced Encryption Standard, Rivest Cipher 4.*

Keywords-Hybrid Cryptography algorithm, Advanced Encryption Standard, Rivest Cipher 4, Field Programmable Gate Array, Block Cipher, Stream Cipher.

I. INTRODUCTION

Rapid growth of communication technologies, security and confidentiality has become one of the main concerns for avoid security issues. Cryptography plays an important role to provide privacy, authentication and integrity protection. The cryptosystems are mainly used in different future applications, such as cellular phones, cable/Sat TV broadcasts, radio modems, smart cards, ATM networks, garage door openers, online banking etc. Generally two types of cryptosystems are used, such as symmetric key and public key systems. Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. Public-key cryptography used two different keys for encryption schemes. The most popular traditional symmetric key encryption algorithm is AES [1],

which handle security issues to provide confidentiality, integrity, non-repudiation and authentication.

Revised Manuscript Received on October 12, 2019.

Senthil Murugan M, Research Scholar, Faculty of Electronics, Sathyabama Institute of Science and Technology, Assistant Professor, St. Joseph's Institute of Technology, Chennai

Dr. T. Sasilatha, Dean Academic and Head, Department of Electrical and Electronics Engineering, AMET (Deemed to be University), Chennai, India.

For hardware structure wise, AES available in open literature on both application specific integrated circuit (ASIC) [2–5] and FPGA [6–9] platforms.

AES algorithm is performed by two different approaches, such as substitution box (S-box) and look up tables (LUT) (T-box). In these approaches, all the computational complexities of most critical transforms of AES are replaced by simple LUTs. But encryption and decryption based on these LUTs are not only memory intensive but also asymmetric in nature due to AES operations and sequence of transformations in encryption and decryption. The pipelining based substitution box (S-box) is implement with ROM, block RAM (BRAM) has achieved high throughput rate. The pipelined architecture can be made to togglebetween the encryption and decryption modes without the presence of any dead cycle [6]. Traditional logic elements (LE), such as flip flop and look up tables are also used for speed enhancement process [7-8]. A single s-box of AES can fit in 8 FPGA slices which changes with a sound intertwining of the round and key round functionalities in order to produce encryption and decryption architectures that perfectly fit with the digital cinema initiative specifications [9]. FPGA platforms are ideal for the implementation of cryptographic algorithms. They are reconfigurable that give both time and cost effective solutions as compared to ASICs, that require largest development time and are expensive [10].

FPGAs also provide far better speed performance than software implementations and at the same time can be re-programmed on the fly to store updated encryption standard. Modern generations of FPGA apart from LUTs are now equipped with special embedded features such as multi-mode clock manager (MMCM) and BRAM for the implementation of high-density and high performance designs. An active area of research in optimization of crypto-system on FPGAs focuses not only to use these new embedded features of FPGA but how efficiently and effectively these features are to be used in order to enhance the performance of these crypto-system in terms of both area and speed [11,12]. Encryption and decryption cores are separately implemented and occupied considerable amount of BRAM resources on FPGA [13]. So there is a need to design a unified AES encryption and decryption module to minimize BRAM resources and also to efficiently utilize full memory space of 32 Kb BRAM available in new generations of FPGA devices. The designs target maximizing speed, minimizing area or achieving a trade-off between speed and area, by means of techniques such as loop unrolling, pipelining and data path word length customization.

The multiple encryption algorithms are combined to form new security scheme called hybrid cryptosystems [14-16], which screw something up than to get any meaningful security gain with little bit tricky. It is also used for compression, encryption and secured session key exchange along with the transmission. The data is encrypted by performing XOR operation on the shuffled data and diffusion template. The cryptosystem takes lesser time and is found to be safe from any of the cryptanalytic attacks. Further elliptic curve cryptography (ECC) is used for secure transfer of private key [14].The modern ciphers appear to be effectively unbreakable; if that's correct, multiple encryptions is possible and it is required. Key encapsulation mechanism (KEM) works just like a public key encryption scheme, except that the encryption algorithm takes no input other than the recipient's public key. The encryption algorithm can only be used to generate and encrypt a key for a symmetric-key encryption scheme. A secure KEM, combined with an appropriately secure symmetric-key encryption scheme, yields a hybrid encryption scheme which is secure in the sense of IND-CCA [15]. A hybrid homomorphic encryption combines public-key encryption (PKE) and somewhat homomorphic encryption (SHE) to reduce the storage requirements of most somewhat or fully homomorphic encryption (FHE) applications [16].

II. RELATED WORKS

Asif et al. [17] have proposed a residue number system (RNS) based apparatus framework of an ECC processor over prime field. The processor figures point development in Jacobian makes by a joined spreading out of point replicating and point advancement. Serial-parallel isolated spoil building is proposed for an adjusted execution of the processor to the degree time and zone. Overhauled reviewed diminishment building is in like way showed that accomplishes a low zone by pulling back the RNS modulo in unimportant parties and structures the get-togethers one by one. A joined arranging of the ECPD and ECPA is utilized to decrease the required number of particular assignments on the focal way and updates the measure of clock cycles for one ECPM by around 17%. The system blended, and executed on the Virtex-7 and Virtex-6FPGAs and shows execution to the best in class parallel and RNS based ECC processors.

Shahbazi et al. [18] have proposed 32-bit ASIP-based crypto processor for AES, IDEA, and MD5. This chart has nine most far away point units and two information transports. It has other than two sorts of 32-bit run packs for executing memory reference, select reference, and information/yield reference headings. The encoded yield possible consequences of the encryption course of action of a 128-piece input square are gotten after 122, 146 and 170 clock cycles for AES-128, AES-192, and AES-256, in a manner of speaking. It takes 95 clock cycles to encode or unscramble a 64-bit input hose by utilizing IDEA. The MD5 hash check requires 469 clock cycles to pass on the coded yields for a square of 512 bits. The execution of the proposed processor is showed up especially in relationship with some past and best in class utilize like speed, progressiveness, throughput, and versatility.

Lee et al. [19] have proposed heterogeneous twofold preparing portion (twofold PE) format and a need dealt with booking of sensible to-left twofold and-circuit reliably EC scalar multiplication (ECSM) with randomized controlling technique. The equipment execution is capable paying little character to the way that the ECC plots are secure at cryptanalysis, the private educational assembling constantly in an unprotected gadget contraption will be removed by physical strikes. It accomplishes a power-examination safe dual-field ECC (DF-ECC) processor. A memory levels of advancement with neighborhood memory synchronization plot is utilized to enhance the information trade speed. The blueprint finished in UMC 90-nm CMOS process with 0.41 mm2 center zone over GF (P^{160}) and GF (2^{160}).

III. HARDWARE IMPLEMENTATION

EDGE Artix 7 FPGA Development board is the feature rich development board with Artix 7 FPGA, SPI FLASH, SRAM, HDMI, Micro SD, Wi-Fi, Bluetooth, ADC, DAC, LCD, 7 segment Display, VGA, , Stereo Jack, buzzer, Push Button, Slide Switch, LED, Temperature Sensor and LDR. The Board also provides additional interface like CMOS Camera and TFT Display at the expansion connectors.

Fig 1.EDGE Artix 7 FPGA Development board

IV. EXPERIMENTATION TESTBEDS:

The experimental setup has been designed based on the ARTIX-7 EDGE Family of the processors in which properties are listed below

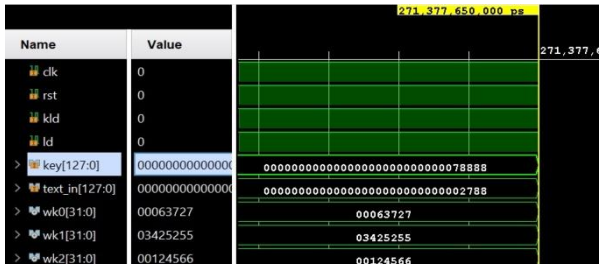
ARTIX-7 Family Used:xc7a200tffg1156 Speed =-1 package = ffg1156

The MRI brain Images are used for testing the proposed algorithm , the MRI brains are then converted into bit maps has been stored in memory of the FPGA and using the constraint files are then ported into the FPGA for further transmission and analysis.

Fig3. Hardware Setup for the Interfacing Techniques

Fig.4 Transmitter Side mechanism

SL.NO	VLSI families	Fmax(mhz)	Throughput(Gbps)
1	Xc7at200tffg-1	250	30.334
2	Xc7at200ff-1.2	150	34.783
3	Xc7at150tffg-1	100	36.904
4	Xc7at155tffg-2	300	29.98
5	Xc7at1000tffg-2	200	34.589
6	Xc7at250tffg-2	125	33.9



5.Analysis Side Interfaced with the System for Analysis.

AREA UTILIZATION SUMMARY:

SL.NO	VLSI families	LUT	Slices	DRAM	DSP
1	Xc7at200tffg-1	574	376	6.5	0
2	Xc7at200ff-1.2	574	378	6.5	0
3	Xc7at150tffg-1	300	236	7	0
4	Xc7at155tffg-2	234	200	8	0
5	Xc7at1000tffg-2	452	300	7.2	0
6	Xc7at250tffg-2	345	300	9	0

V. EXPERIMENTAL SETUP DETAILS:

Fig6. Encrypted test Data for the Image From the FPGA Analysis

THROUGHPUT ANALYSIS :

Throughput has been analyzed by the following expression

Throughput = (FmaxX latency) /Slices

VI. AVALANCHE EFFECT ANALYSIS AND SENSITIVITY MECHANISM

Avalanche Effect: The strength of the cryptosystem is tested on the basis of Strict Avalanche Criterion (SAC). SAC is said to be satisfied whenever complementing a single input bit results in change of each of the output bits with a 50% probability. The 128 bit image sections and key each of 128-bit are the inputs to the AES algorithm. Thus, with a single bit complemented in plaintext or key, the cipher text should change with a probability of 50% known as Avalanche Effect.

Sl.no	Algorithms	No of bits taken	Avalanche Effect
01	Algorithm proposed by Qiang-2015	128 bits	50%
02	Algorithm proposed by Harshali Zodpe-2018	128 bits	51% to 63%
03	Proposed algorithm	128 bits	55% to 65%

From the above table, it is clear that the proposed algorithm has the 55% to 65% in avalanche effect and whereas the other algorithm consumes the 50 % to 63% .

VII. SENSITIVITY ANALYSIS:

In this analysis, we have introduced the attacks -brutal force attacks in the data , in which the encrypted image has been transmitted in an IoT environment /WIFI and received at the receiver side. the same hardware has been used for the receiver side . the sensitivity has been analyzed by the formula

NPCR = $\{[\sum_i d(i)]/m\}x100\%$

The NPCR and entropy conditions were calculated at the different cases which is mentioned above and tabulated in the table

Sl.No	Changes in data position bit	NPCR	Entropy
01	5%	99.8%	1.2
02	10%	99.75%	1.4
03	25%	99.8%	1.45
04	50%	99.8%	1.34
05	75%	99.8%	1.39
06	100%	99.8%	1.40

From the above table ,Clearly states that the sensitivity analysis has been calculated on the basis of one-bit change in the receiver side and hence then the output has been calculated based on the above formula.

VIII. COMPARATIVE ANALYSIS:

Sl.no	Algorithm	Family Tested	Throughput (Gbps)	LUT	SLICES	A.E	Pipelining
1	Algorithm proposed by Qiang-2015	Spartan-6	3.45	5688	5688	50%	Non
2	Algorithm proposed by Harshali Zodpe-2018	Spartan6	30	3788	3788	51% to 63%	6
3	Proposed Algorithm	Artix-7/Spartan-6	33.97	378	456	53% to 65%	6

From the above table, we have compared the proposed algorithm with the algorithms in which performance in terms of area and throughput has increased when compared with other existing algorithms and finds it suitability for the IoT based Medical Image Processing.

IX. CONCLUSION

Hardware implementation of hybrid model encryption algorithm proposed for secure transmission of medical images. For making hybrid model from the symmetric key algorithm modified Advanced Encryption Standard and Rivest Cipher 4 were used. Avalanche effect is more percentage compare to existing method. Here the sensitivity of the data also compared with the previous algorithm. While looking the parameter such as throughput, LUT, Slices this proposed model having better performance. All the parameter tested with hardware with support of Artix 7 board of FPGA device.

REFERENCE:

1. NIST -Advanced Encryption Standard, National Institute of Standards and Technology, FIPS-197, 2001.
2. M.-Y.Wang, C.-P.Su, C.-L.Horng, C. Wu, C.-T.Huang, Single and multi-core configurable AES architectures for flexible security, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 18 (4) (2010) 541–552. ISSN 1063-8210.
3. H. Li, Efficient and flexible architecture for AES, IEE Proc. Circuits Devices Syst. 153 (6) (2006) 533–538.
4. A. Hodjat, I. Verbauwhede, Area-throughput trade-offs for fully pipelined 30 to 70 Gbits/s AES processors, IEEE Trans. Comput. 55 (4) (2006) 366–372. ISSN 0018- 9340.
5. T. Good, M. Benaissa, 692-nW advanced encryption standard (AES) on a 0.13-um CMOS, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 18 (12) (2010) 1753–1757.
6. G. Saggese, A. Mazzeo, N. Mazzocca, A. Strollo, An FPGA-based performance analysis of the unrolling, tiling, and pipelining of the AES algorithm, in: Field Programmable Logic and Application (FPL 2003), in: LNCS, vol. 2778, Springer, Berlin, Heidelberg, Lisbon, Portugal, 2003, pp. 292–302. ISBN 978-3-540-40822-2.
7. S. Drimer, T. Güneysu, C. Paar, DSPs, BRAMs, and a pinch of logic: extended recipes for AES on FPGAs, ACM Trans. Reconfigurable Technol. Syst. 3 (1) (2010) 3:1–3:27. ISSN 1936–7406.
8. P. Bulens, F.-X. Standaert, J.-J.Quisquater, P. Pellegrin, G. Rouvroy, Implementation of the AES-128 on Virtex-5 FPGAs, in: Progress in Cryptology, AFRICACRYPT 2008, in: LNCS, vol. 5023, Springer, Berlin, Heidelberg, 2008, pp. 16–26. ISBN 978-3- 540-68159-5.
9. A. Aziz, N. Ikram, A Look-Up Table implementation of AES, in: International Conference on High Performance Computing, Networking and Communication Systems (HPCNCS-07), Orlando, Florida, USA, 2007, pp. 187–191.
10. F.R. Henrquez, A.D. Prez, N.A. Saqib, C.K. Koc, Cryptographic Algorithms on Reconfigurable Hardware, Signals and Communication Technology, Springer, 2007.
11. D.-S. Kundi, A. Aziz, N. Ikram, Resource efficient implementation of T-boxes in AESon Virtex-5 FPGA, Inf. Process. Lett. 110 (10) (2010) 373–377. ISSN 0020-0190.
12. K. Latif, A. Arshad, A. Mahboob, Optimal utilization of available reconfigurablehardware resources, Comput. Electr. Eng. 37 (6) (2011) 1043–1057.
13. L. Ali, I. Aris, F.-S. Hossain, N. Roy, Design of an ultra-high speed AES processor fornext generation IT security, J. Comput. Electr. Eng. 37 (6) (2011) 1160–1170.
14. K. Gupta and S. Silakari, "Novel Approach for fast Compressed Hybrid color image Cryptosystem", Advances in Engineering Software, vol. 49, pp. 29-42, 2012.
15. J. Herranz, D. Hofheinz and E. Kiltz, "Some (in) sufficient conditions for secure hybrid encryption", Information and Computation, vol. 208, no. 11, pp. 1243-1257, 2010.
16. S. Priya, P. Karthigaikumar, N. Siva Mangai and P. Kirti Gaurav Das, "An Efficient Hardware Architecture for High Throughput AES Encryptor Using MUX Based Sub Pipelined S-Box", Wireless PersCommun, 2016.
17. A. Hodjat and I. Verbauwhede, "Area-throughput trade-offs for fully pipelined 30 to 70 Gbits/s AES processors", IEEE Transactions on Computers, vol. 55, no. 4, pp. 366-372, 2006.
18. Hua Li and Jianzhou Li, "A high performance sub-pipelined architecture for AES", 2005 International Conference on Computer Design.
19. U. Farooq and M. Aslam, "Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA", Journal of King Saud University - Computer and Information Sciences, 2016.

AUTHORS PROFILE

Senthil Murugan M obtained his Bachelor's degree in Electronics and Communication Engineering from University of Madras, 2003. Then he obtained his Master's Degree in Applied Electronics from Anna University, Chennai, 2005. Currently he is pursuing Ph.D. in Sathyabama Institute of Science and Technology, Chennai and working as an Associate Professor in the department of Electronics and Communication Engineering, St. Joseph's Institute of Technology, Chennai. His specializations include Wireless Network, Network Security and VLSI Design

Dr.T.Sasilathareceived her B.E Degree in Electronics and Communication Engineering from Government College of Engineering, Tirunelveli, Tamil Nadu, India in 1995 and M.E degree from Anna University, Chennai, India in 2003. She has completed her Ph.D. in VLSI Design from Anna University Chennai, India in February 2010. She has about 22 Years of experience in teaching and currently she is working as a Dean Academic and Head in the department of Electrical and Electronics Engineering, AMET (Deemed to be University), Chennai, India. She has published about 75 papers in both national, international journals and conferences. She is guiding more than 20 research scholars in various universities. Her research area includes Low power RF circuit design, ASIC design, VLSI signal processing and Wireless Sensor Networks.