SECURE MEDICAL IMAGE TRANSMISSION USING THE RLCD ALGORITHM

G.ANITHA RANI[1]
M.TECH Scholar Department Of Electronics and Communication Engineering
Malineni Lakshmaiah Women's Engineering college
AP, India
anitharanigunja037@gmail.com

Mr .KUNDURTHI RAVI KUMAR[2]
Associate professorDepartment of Electronics and Communication Engineering
Malineni Lakshmaiah Women"s Engineering college
AP, India
kundurthiravikumar1971@gmail.com

Abstract

With the rapid adoption of digital health care platforms, the secure transmission and storage of medical images have become a critical concern. Unauthorized access or tampering of sensitive patient data can lead to severe privacy breaches and compromise clinical decisions. This project introduces an efficient and secure cryptographic framework specifically designed for medical image encryption using Reversible Logic Cryptography Design (RLCD). The proposed system combines Linear Feedback Shift Registers (LFSRs) with XOR gates, enabling high-speed and low-power encryption and decryption operations. By integrating reversible logic gates, the framework significantly reduces energy dissipation while ensuring lossless encryption, preserving the integrity and accuracy of medical images. This feature is particularly important in medical applications,where even minor data alterations can have critical consequences. The design is implemented in Verilog HDL providing a practical and scalable solution for real-world medical imaging systems. Performance analysis demonstrates that the proposed RLCD-based encryption framework achieves a balance between security, speed, and energy efficiency, making it well-suited for modern healthcare environments. Furthermore, this approach addresses the dual challenges of data confidentiality and hardware

Keywords— *Medical Image Encryption, Reversible Logic Cryptography Design (RLCD), Reversible Logic Gates, Linear Feedback Shift Register (LFSR), XOR Gates, VLSI, Verilog HDL.*

I. INTRODUCTION

In the era of data breach, we need to focus on securing the medical images which can led to financial losses, improper treatment, patient privacy, medical identity theft. Image encryption and decryption are methods used to safeguard image data by converting it into an unreadable format through encryption and then restoring it to its original state through decryption. These processes are essential for ensuring that only authorized individuals can access the image, making them critical for the secure transmission of images in areas such as medical imaging, military communications, and cloud storage. Image encryption involves transforming the original image (plaintext) into a scrambled, unreadable version (cipher text) using cryptographic techniques that rearrange pixel values or alter their intensity with the use of a secret key. Imaged ecryption reverses this process, where the encrypted or scrambled image (cipher text) is reverted back to its original form (plaintext) by applying a decryption algorithm and the correct cryptographic key [1].

Image can be secured by various methods like Encryption, Access control and authentication, Watermarking, Secure transmission protocols (HTTP). Here let us discuss about encryption, they are different methods in encryption like RSA, AES, DES, RLCD, Reconfigurable Reversible gates. The major drawback of all these algorithms is heat dissipation in hardware setup, high-power consumption, information loss. In Reversible Logic Cryptography.

In this paper, we will focus on implementing image encryption and decryption using Reversible Logic Circuit Design (RLCD) to address the limitations of existing cryptographic algorithms. The design will be implemented using the Xilinx platform, which allows for efficient hardware synthesis and simulation of reversible logic circuits. By utilizing Xilinx, we aim to demonstrate the practical application of RLCD in a real-world environment, show casing its potential to improve performance, reduce the complexity of hardware, and overcome challenges faced by traditional encryption methods.

CRYPTOGRAPHY AND TYPES

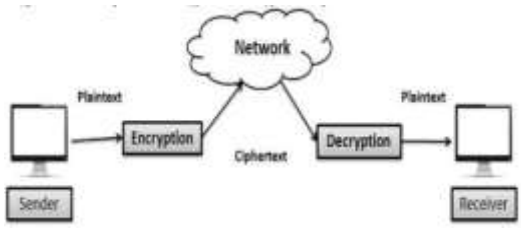

Fig: Encryption And decryption Process

The original message is then encoded using encryption algorithm. This process is called encryption. The reverse process to get back the encrypted data into plain text by using decryption algorithm. This process is called decryption. The process of decryption is reversed to that of encryption.

II. LITERATURE SURVEY

Architecture Design and VLSI Hardware Implementation of Image Encryption/ Decryption System

Doi:10.48047/ijiee.2026.16.2.55

Using Re-configurable 2-D Von Neumann Cellular Automata by Rong-Jian Chen, Yi-TE Lai, Jui-Lin Lai

The first architecture design and VLSI hardware implementation of image encryption/decryption system using re-configurable two-dimensional (2-D) von Neumann cellular automata (CA) is presented in this paper. Its encryption scheme is based on replacement of the pixel values using a progressive cellular automata (CA) substitution. In our scheme, we used the re-configurable 2-D von Neumann CA to generate high quality random sequence as key stream. To enhance the flexibility of our system, we used 16 x 16 re-configurable 2-D von Neumann CA which produces 1 set (256) CA or concurrently produces 4 sets (64/set) 8 x8 CA and 16 sets (16/set) 4x4 CA, respectively. We have accomplished simulations of our image encryption/decryption system by using CADENCE tools. We also have completed the circuit synthesis using the SYNOPSYS tools with the T SMC 0.18um cell-library. The area size was 15.6816 MM, and the maximum operation frequency was 100 MHz with 27.74 MW total dynamic power. It shows that the architecture of the proposed image encryption/decryption system is suitable for VLSI realization.

A Nonlinearequation-based cryptosystem for image encryption and decryption by Rithmi Mitter, M. Sridevi Sathya Priya.

III. EXTISING SYSTEM AND METHODOLOGY

DES is a secret-key archetypal block cipher with block size of 64 bits. DES encrypts a block of 64-bit plaintext into 64-bit cipher text using 64-bit secret key (Left most bit of a block is bit one). Block diagram of the DES algorithm is shown in Figure 1.

DES adopted in 1977 by the National Bureau of Standards now the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46).

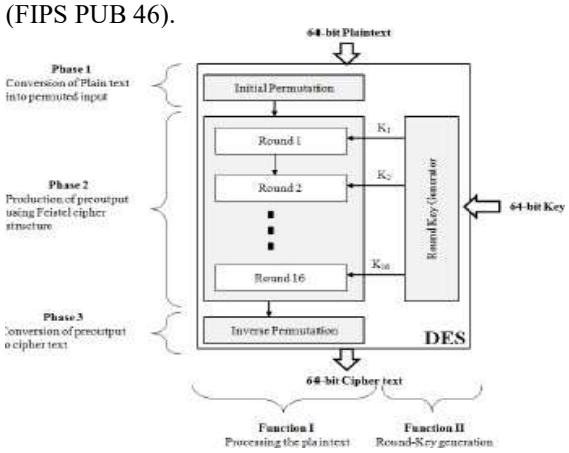

Figure 2:General block diagram of DES algorithm

ADES key consists of 64 binary digits ("0"sor"1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits a reset to make the parity of each 8-bit byte of the keyodd, i.e., there is an odd number of "1"s in each 8-bit byte. A TDEA key consists of three DES keys, which is also referred to as a key bundle. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it. The encryption algorithms specified in this standard are commonly known among those using the standard. The cryptographic security of the data depends on the securityprovided for the key used to encipher and decipher the data.Data can be recovered from cipher only by using the same key used to encipher it.

Unauthorized recipients of the cipher who know the algorithm but do not have the correct key cannot derive the original data algorithmically. However, it may be feasible to determine the key by a brute force "exhaustion attack."Also, anyone who does have the key and the algorithm can easily decipher the cipher rand obtain the original data. A standard algorithm based on a secure key thus provides a basis for exchanging encrypted computer data by issuing the key used to encipher it to those authorized to have the data.

1. Toffoli gate

Any reversible gate must have the same number of input and output bits, by the pigeon hole principle. For one input bit, there are two possible reversible gates. One of them is NOT. The other is the identity gate which maps its input to the output unchanged. For two input bits, the only non-trivial gate is the controlled NOT gate which XORs the first bit to the second bit and leaves the first bit unchanged.

2.Fredkin gate

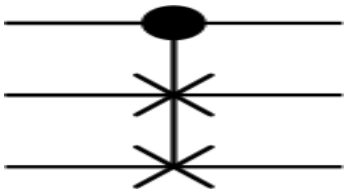

Fig 3: Circuit representation of Fredkin gate

The Fredkin gate (also CSWAP gate) is a computational circuit suitable for reversible computing, invented by Ed Fredkin. It is universal, which means that any logical or arithmetic operation can be constructed entirely of Fredkin gates. The Fredkin gate is the three-bit gate that swaps the last two bits if the first bit is 1.

3.Feynman gate

Feynman gate is a 2*2 one through reversible gate as shown in figure 1. The input vector is I(A, B) and the output vector is O(P, Q). The outputs are defined by P=A, Q=A⊕B.Quantum cost of a Feynman gateis1. Feynman Gate (FG) can be used as a copying gate. Since a fan out is not allowed in reversible logic this gate is useful for duplication of the required outputs.

Fig4: Feynman Gate

Doi:10.48047/ijiee.2026.16.2.55

IMPLEMENTATION

XILINX

It requires Xilinx ISE 14.7 version of software where Verilog source code can be used for design implementation.

Introduction to XILINXISE:

This instrument can be utilized to make, execute, reenact, and integrate Verilog outlines for usage on FPGA chips.

ISE: Insstegrated Software Environment

Environment for the improvement and trial of computerized systems configuration focused to FPGA or CPLD.

Integrated gathering of apparatuses available through a GUI Based on an intelligent combination motor (XST: Xilinx Synthesis Technology)

XST under pins diverse dialects:

Verilog VHDL

XST create a net rundown incorporated with requirements Supports everyone of the means required to finish the plan: Translate, guide, place and course

Bitstream era

For this situation, it is conceivable to utilize Verilog to compose a test seat to confirm the usefulness of the outline utilizing documents on the host PC to characterize jolts, to interface with the client, and to contrast comes about and those normal.

A Verilog show is converted into the "doors and wires" that are mapped onto a programmable rationale gadget, for example, a CPLD or FPGA ,and after that it is the real equipment being designed ,instead of the Verilog code being "executed" as though on some type of a processor chip.

Implementation:

Synthesis (XST)

-Produce anetlist file starting from an HDL description Translate (NGD Build) Converts all input design netlists and then writes the results into a single merged file that describes logic and constraints.

Mapping (MAP)

Maps the logic on device components.

Takes a netlist and groups the logical elements into CLBs and IOBs (components of FPGA).

Place And Route (PAR)

Place FPGA cells and connects cells. Bit stream generation

XILINX Design Process:

Step1:Design entry

HDL(Verilog or VHDL, ABEL x CPLD), Schematic Drawings, Bubble

Diagram

Step 2:Synthesis

Translates .v, .vhd ,.such files into anetilist file (.ngc)

Step 3: Implementation

FPGA: Translate/Map/Place & Route, CPLD: Fitter

Step 4: Configuration/Programming

Download a BIT file into the FPGA Program JEDEC file into CPLD Program MCS file into Flash PROM Simulationcanoccuraftersteps1,2,3.

The tools used in this thesis are XILINX ISE 14.7 for simulation and Synthesis. The programs are written in verilog language.

Xilinx Tools is a suite of software tools used for the design of digital circuits implemented using Xilinx Field Programmable Gate Array (FPGA) or Complex Programmable Logic Device (CPLD). The design procedure consists of (a) design entry, (b) synthesis and implementation of the design, (c) functional simulation and (d) testing and verification. Digital designs can be entered in various ways using the above CAD tools: using a schematic entry tool, using a hardware description language (HDL)– Verilog or VHDL or a combination of both. In this thesis we will only use the design flow that involves the use of Verilog HDL.

IV. RESULTS

The Proposed System Uses RLCD with LFSR and reversible gates for encryption and decryption. The process consists of three main stages

1. Image conversion
2. Encryption
3. Decryption

ENCRYPTION: The process of converting readable data (plaintext) into unreadable, scrambled format (cipher text) using algorithms and cryptographic keys.

Fig 5: encryption of medical image

Fig 6: decryption of medical image

Doi:10.48047/ijiee.2026.16.2.55

Fig 7: decryption power consumption

V. CONCLUSION

The proposed RLCD-based encryption framework successfully demonstrates an efficient, secure, and fully reversible method for protecting medical images in modern healthcare systems. By combining reversible logic gates such as CNOT, HNG, and PEARS with an LFSR-driven key generator, the system achieves high-speed and low-power encryption while maintaining complete information integrity. The use of reversible logic ensures that no data is lost during processing, enabling perfect reconstruction of medical images during decryption—an essential requirement in clinical applications where diagnostic accuracy cannot be compromised. Hardware implementation using Verilog HDL further verifies that the design is scalable, energy-efficient, and suitable for real-time medical imaging environments.

The proposed framework can be further extended to support larger image sizes and higher-resolution medical formats such as MRI, CT, and ultrasound data sets. Future enhancements may explore integrating more advanced reversible gates, optimizing the LFSR for stronger key unpredictability, or combining RLCD with lightweight block ciphers for layered security. The system can also be implemented on FPGA or ASIC platforms to evaluate performance under real clinical workloads. Additionally, in corporating machine-learning-based anomaly detection can strengthen security by identifying potential tampering or unauthorized access. With these extensions, the RLCD-based encryption scheme has strong potential to evolve into a robust and sustainable security solution for next-generation medical data management systems.

REFERENCES

[1] [1] Gordon E. Moore, " Craming more components onto integrated circuits," Electronics, pp.114-117, April 1965.

[2] Rolf Landauer, Irreversible and heat generation in the computing process, IBM Research and Development, vol.5, pp.183–191, July 1961.

[3] C.H. Bennett, "Logical reversibility of computation" IBM Research and Development, vol.17, pp.525–532, 1973.

[4] Saranya Karunamurthi, Vineyakumar Krishnasamy Natarajan, "VLSI implementation of reversible logic gates cryptography with LFSR key," Microprocessors and Microsystems, Elsevier, vol. 69, pp.68–78, September 2019.

[5] Mehran Mozaffari Kermani, Kaj Reza Azarderakhsh, Siavash Bavat Sarmadi, "Fault resilient light weight cryptography block cipher for secure embedded systems," in IEEE Embedded System Letters, vol. 6, no. 4, pp.89–92, Dec. 2014.

[6] Shikha Kuchhal , Rakesh Verma, "Security design of DES using reversible logic," Int. J. Compute. Sci. Newt. Security, vol. 15, no. 9,pp. 81–84, September 2015.

[7] Z. H. A. O. Guosheng, W. A. N. G. Jain, "Security analysis and enhanced design of a dynamic block cipher," China Commun., vol. 13, pp. 15–160, January 2016.

[8] Srivatsam Subramanian, Mehran Mozaffari Kermani, Reza Azarder akhsh, Mehrdad Nojoumaian, "Reliable hardware architectures for cryptographyic block ciphers LED and HIGHT," in IEEE Trans. Comput. Aided Des. Integr. Circuits Syst., vol. 36, no.10, pp. 1750-1758, Oct.2017.

[9] Raghava Garipelly, P.MadhuKiran, A.Santhosh Kumar, " A review on reversible logic gates and their implementation," in International Journal of Emerging Technology and Advanced Engineering, vol. 3, no. 3, March 2013.

[10] Abduullah Bamatraf, Rosziati Ibrahim, Mohd. Najib. B, Mohd. Salleh, "Digital watermarking algorithm using LSB," in 2010 International Conference on Computer Applications and Industrial Electronics, Kuala Lumpur, pp. 155-159, 2010.

[11] MeenalDadhe,Prof. Anup.R.Nage, " Design of high speed VLSI architecture for LFSR with maximum length feedback polynomial," in International Journal for Scientific Research & Development, vol .3, no.5, 2015.

[12] Y. G. Praveen Kumar, B. S. Kriyappa, M. Z. Kurian, "Implementation of power efficient 8-bit reversible linear feedback shift register for BIST," in 2017 International Conference on Inventive Systems and Control, Coimbatore, 2017.

.

Doi:10.48047/ijiee.2026.16.2.55