Design and Implementation of a Reversible Logic Cryptographic Architecture for Secure Text Communication

Mrs Y. MALLIKA, A. UDAYA KRANTHI[2]
[1]Assistant Professor, Dept. of E.C.E, RV Institute of Technology, Guntur- 522212
[2]PG Scholar, Dept. of E.C.E, RV Institute of Technology, Guntur- 522212

Abstract: The rapid advancement of digital healthcare technologies and telemedicine systems has significantly increased the need for secure transmission and storage of medical images. Protecting sensitive patient information from unauthorized access, tampering, and data breaches has become a major challenge in modern healthcare environments. This paper presents an efficient and secure medical image encryption framework based on Reversible Logic Cryptography Design (RLCD). The proposed architecture integrates Linear Feedback Shift Registers (LFSRs) and XOR-based encryption mechanisms with reversible logic gates to achieve high-speed, low-power, and lossless cryptographic operations. Reversible logic minimizes energy dissipation by reducing information loss during computation, thereby improving hardware efficiency and supporting sustainable cryptographic system design. The proposed framework ensures secure encryption and accurate decryption of medical images while preserving image integrity and diagnostic quality, which are critical requirements in healthcare applications. The complete system is implemented using Verilog Hardware Description Language (HDL), enabling efficient simulation, synthesis, and hardware realization for FPGA and VLSI platforms. Experimental and performance analysis results demonstrate that the proposed RLCD-based cryptographic framework achieves improved security, reduced power consumption, optimized hardware utilization, and faster processing speed compared with conventional encryption approaches. Hence, the proposed system provides a reliable and energy-efficient solution for secure medical image management in modern healthcare systems.

Key Words: Reversible Logic Circuits, Cryptography, Secure Text Communication, Toffoli Gate, CNOT Gate, Power Analysis Attack Resistance, Energy-Efficient Hardware, Internet of Things (IoT).

1. Introduction

The rapid growth of digital healthcare systems, cloud-based medical platforms, and telemedicine applications has significantly increased the need for secure medical image transmission and storage. Medical images contain highly sensitive patient information, and unauthorized access, modification, or leakage of such data can lead to privacy violations, medical identity theft, financial losses, and incorrect clinical decisions. Therefore, protecting medical image data has become a critical

requirement in modern healthcare environments. Image encryption and decryption techniques play a vital role in securing medical images by converting the original image into an unreadable encrypted format and restoring it back to its original form only through authorized decryption mechanisms. These security techniques ensure confidentiality, integrity, and secure communication of medical data across healthcare networks, cloud systems, and storage platforms.

Several conventional encryption algorithms such as RSA, AES, DES, and other cryptographic techniques have been widely used for image security applications. Although these methods provide strong security, they often suffer from limitations such as high power consumption, hardware complexity, information loss, and excessive heat dissipation during hardware implementation. To overcome these challenges, Reversible Logic Cryptography Design (RLCD) has emerged as an efficient alternative for secure and low-power cryptographic systems. Reversible logic circuits preserve information during computation through a one-to-one mapping between inputs and outputs, thereby minimizing energy dissipation and reducing hardware losses. Reversible logic gates such as Toffoli, Fredkin, and Peres gates are widely used for designing energy-efficient arithmetic and cryptographic circuits suitable for low-power VLSI and quantum computing applications.

Conventional cryptographic algorithms such as RSA and AES provide strong security but require high computational power and complex mathematical operations. To improve security and efficiency, the proposed system utilizes an efficient multi-level encryption approach that enhances data protection with reduced processing delay and hardware overhead. Compared with traditional encryption techniques, the proposed RLCD-based framework offers improved energy efficiency, faster processing speed, and reliable performance for healthcare and secure communication applications.

2.Literature Survey

Rong-Jian Chen, Yi-Te Lai, and Jui-Lin Lai proposed an image encryption and decryption system using re-configurable two-dimensional von Neumann Cellular Automata for VLSI implementation. The architecture generates high-quality random key streams for secure image encryption and supports scalable CA configurations such as 16×16, 8×8, and 4×4 structures. The system was simulated using Xilinx tools and synthesized using SYNOPSYS with TSMC technology. Experimental results showed improved hardware efficiency, high operating speed, and reliable encryption performance for secure image processing applications.

Rithmi Mitter and M. Sridevi Sathya Priya proposed a secure image encryption and decryption technique based on chaotic maps and the Brahmagupta–Bhaskara nonlinear equation. The proposed method improves cryptographic security by introducing strong nonlinearity and enhanced randomness into the encryption process. This approach overcomes the limitations of conventional chaos-based encryption techniques and provides improved resistance against security attacks. The architecture was implemented using Xilinx ISE tools and demonstrated efficient hardware realization and secure real-time image communication performance.

3. Existing System

DES (Data Encryption Standard) is a symmetric key block cipher with a 64-bit block size that encrypts 64-bit plaintext into 64-bit cipher text using a 64-bit secret key. It was adopted in 1977 by the National Bureau of Standards (now NIST) as FIPS PUB 46 and became one of the earliest widely used cryptographic standards. The algorithm operates through a series of permutations and substitutions over multiple rounds to achieve confusion and diffusion in the encrypted data. In existing systems, DES is implemented for secure data transmission and storage due to its simplicity and hardware compatibility. However, its relatively short key length makes it vulnerable to brute-force attacks in modern security environments. As a result, DES is now considered insecure for high-security applications, though it is still used in legacy systems and educational implementations for understanding symmetric key cryptography.

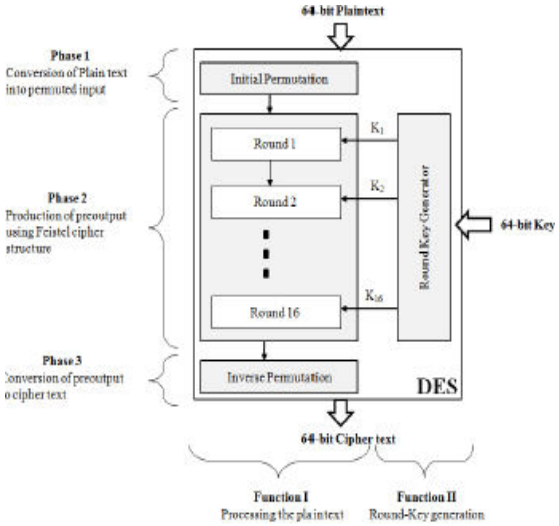

Fig 3.1: General block diagram of DES algorithm

A DES key is a 64-bit value in which 56 bits are used for encryption and the remaining 8 bits are parity bits used for error detection by ensuring odd parity in each byte. In advanced schemes like TDEA, three DES keys are combined to form a key bundle for enhanced security. The security of DES relies entirely on the secrecy of the key, as the same key is required for both encryption and decryption. Although the algorithm is publicly known, unauthorized users cannot recover the original data without the correct key, making brute-force attacks the primary vulnerability. Hence, secure key management is essential for maintaining data confidentiality in DES-based systems.

DES Encryption process has two functions

A. Processing the plaintext

B. Round-Key generation

A. Processing the plaintext

The processing of plaintext proceeds in three phases.

- Conversion of Plain text into permuted input
- Production of pre output using Feistly cipher structure
- Conversion of pre output to cipher text

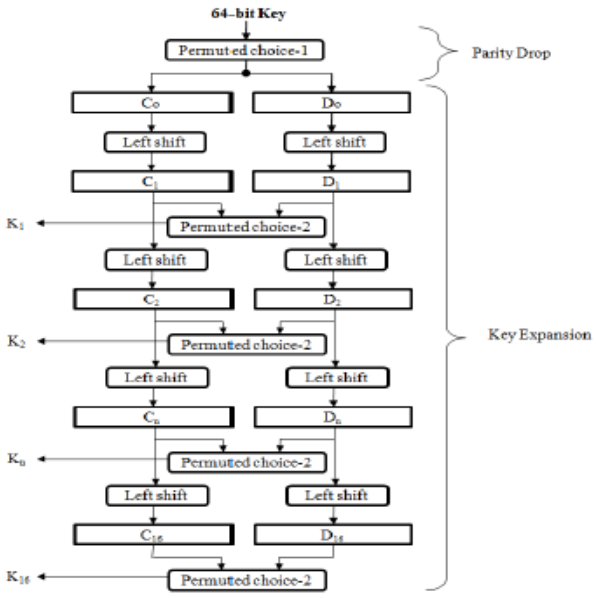

Fig 3.2: General block diagram of DES algorithm

A major drawback of DES is its effective key length of only 56 bits, which makes it highly vulnerable to brute-force attacks with modern computing power. Although the remaining 8 bits are used for parity-

based error detection, they do not contribute to encryption strength. Additionally, the fixed 56-bit key space limits scalability and long-term security, making DES unsuitable for contemporary high-security applications. The relatively small key size and outdated design further reduce its resistance against cryptanalysis, which is why DES has been replaced by more secure algorithms such as AES in modern

4.Proposed System

The proposed system presents a reversible logic–based cryptographic architecture that improves both security and energy efficiency compared to conventional encryption techniques. It utilizes reversible logic gates (RLGs) to eliminate information loss during computation, thereby reducing power dissipation and enabling lossless encryption and decryption. A Linear Feedback Shift Register (LFSR) is integrated for dynamic pseudorandom key generation, enhancing security against brute-force and statistical attacks through continuously varying key streams. The encryption and decryption processes are fully implemented using reversible circuits, ensuring a one-to-one input–output mapping with minimal garbage outputs and optimized hardware utilization. Performance evaluation shows reduced power consumption, lower propagation delay, and improved resource efficiency when compared with traditional cryptographic systems such as AES. the proposed architecture offers a secure, low-power, and hardware-efficient solution suitable for modern applications including IoT, healthcare, and embedded systems.

4.1 Block Diagram

This figure illustrates the reversible logic-based cryptographic architecture using NOT, Toffoli, and Controlled-NOT (C-NOT) gates for secure data processing. Each sub-circuit (a–d) performs reversible transformations on input bits while preserving information and minimizing energy dissipation.

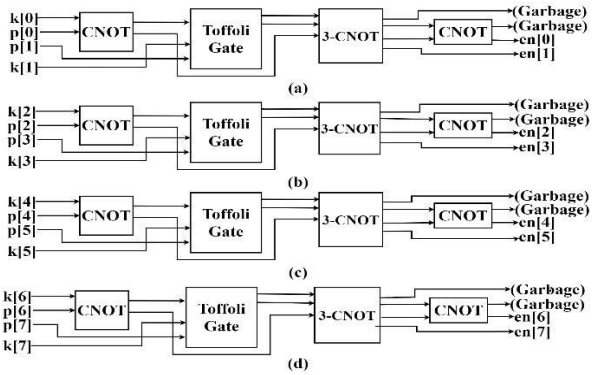

Fig 4.1: Reversible logic circuit design for encryption process: (a) First bit pair of k[i] and p[i]. (b) Second bit pair of k[i] and p[i]. (c) Third bit pair of k[i] and p[i]. (d) Fourth bit pair of k[i] and p[i]

The generated garbage outputs are intermediate signals required to maintain reversibility and ensure accurate encryption/decryption operations.

4.2 Working Principle

The proposed encryption model operates by converting each plaintext character into its 8-bit ASCII binary form and processing it using reversible logic gates. A combination of CNOT, Toffoli, and 3-CNOT gates is used to perform bit-level transformation in a structured reversible circuit. The first character is encrypted using the sender's key bits through successive reversible gate operations, producing encrypted outputs along with minimal garbage bits. The same circuit structure is repeatedly applied to all characters, ensuring uniform and lossless encryption throughout the process. the p[2], p[3], k[2],k[3], p[4],p[5],k[4],k[5] and p[6],p[7],k[6],k[7]. The pair of the encrypted bits en[0], en[1], . . ., en[7] along with two garbage bits are generated from the primary gate of each circuit. This encrypted 8-bit binary is converted to the

corresponding decimal value and then converted to the encrypted ASCII character to get the cipher text.

In the decryption process, each cipher text character is first converted into its 8-bit ASCII binary form and processed using the same reversible logic circuit in reverse operation. The cipher text bits and key bits are applied as inputs to regenerate the original plaintext bits through reversible gate transformations. The circuit produces the decrypted 8-bit binary output along with minimal garbage bits. Finally, the binary output is converted back to its ASCII character to recover the original plaintext.

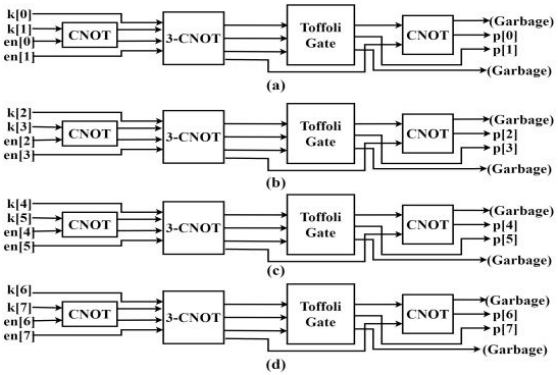

Figure 4.2 Reversible logic circuit design for decryption process: (a) First bit pair of k[i] and en[i]. (b) Second bit pair of k[i] and en[i]. (c) Third bit pair of k[i] and en[i]. (d) Fourth bit pair of k[i] and en[i]

4.3 LFSR module

- In this module there will be three different modules named as X, Y and Z. X, Y and Z will generate 19-bit, 22- bit, 23-bit pseudo random sequence.
- Input signal will be clock, reset and enable. Clock signal which should be in positive edge, reset signal is typically in 1's, when enable signal is high the LFSR is to shift and updates its value.
- This module ensures the process of bitwise encryption.

4.4 Majority Logic module

Majority logic module triggers the signal for three LFSRs. When the two of the three inputs i.e., x, y, z and this three inputs signal are controlled by main module then the output will be high [11].

4.5 Conversion of image into image

To check the image is encrypted we need to convert the encrypted image to image [12]. This process will do by the matlab Assigning the empty array with height and width and then reading binary file. After it converts the binary data to pixel values and saves the image and it displays it. This integrated approach ensures seamless workflow across software, hardware, and dataset utilization, optimizing the encryption

process for secure medical image transmission.

The encrypted as well as the decrypted binary output values are written into a image. In MATLAB encrypted image and decrypted image are generated from the output image.

5. Results & Discussion

The results and discussion confirm that the proposed reversible logic based medical image encryption system successfully ensures secure and lossless encryption and decryption of medical images. Simulation outputs show that the encrypted images are completely unintelligible while the original images are accurately recovered without any data distortion. The architecture demonstrates reduced power consumption and hardware complexity due to the use of reversible logic gates.

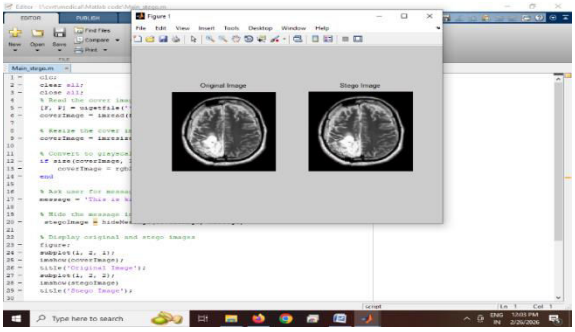

Fig 5.1: Upload Input Image

The fig 5.1 shows that the encrypted stego image maintains the original brain scan's visual quality while securely hiding the secret data, validating the effectiveness of the proposed reversible logic cryptography approach.

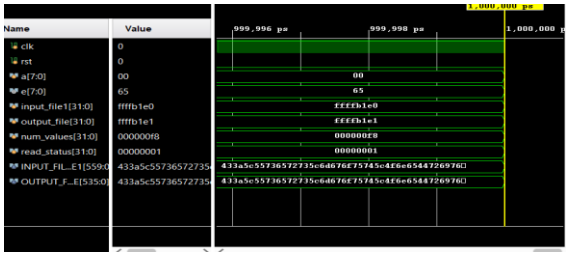

Fig 5.2: Encryption Simulation Result

Fig. 5.2 shows that the encrypted medical image is highly distorted and unreadable, confirming secure protection of sensitive data using LFSR-based encryption.

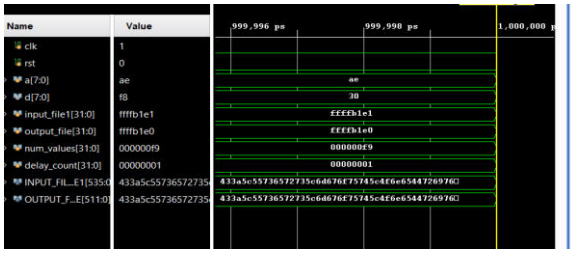

Fig 5.3: Decryption Simulation Result

Fig. 5.3 shows that the decrypted medical image is perfectly restored to its original form without any loss of information, confirming the accuracy and reliability of the proposed LFSR-based system.

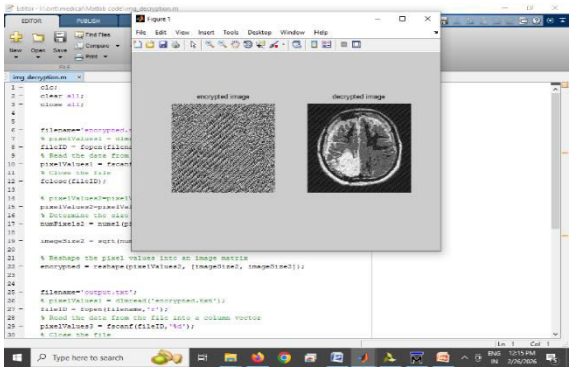

Fig 5.4: Encryption and Decryption Image

Fig. 5.4 shows that the encrypted image ensures confidentiality and the decrypted image successfully restores the original, confirming secure and reliable transmission.

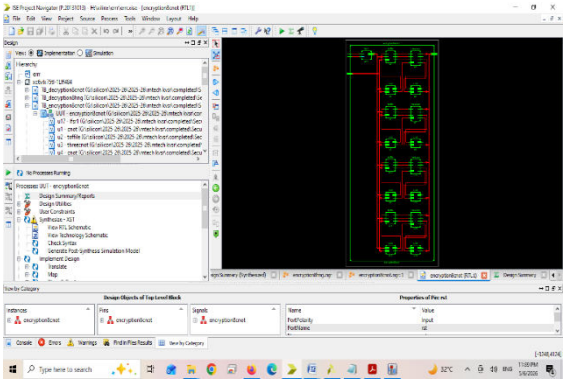

Fig 5.5: RTL schematic of Encryption

Fig. 5.5 shows the RTL schematic of the encryption module, illustrating its internal logic flow and efficient reversible logic-based hardware implementation.

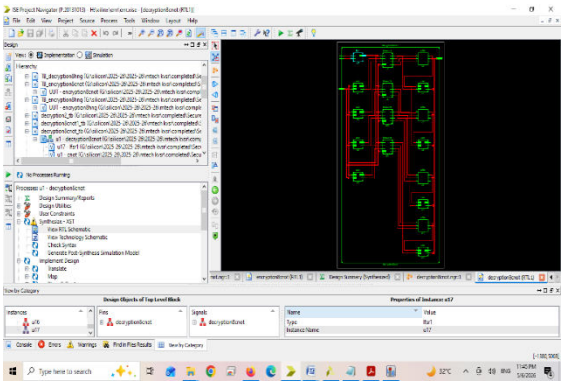

Fig 5.6: RTL schematic of decryption

Fig. 5.6 shows the RTL schematic of the decryption module, illustrating the hardware architecture and data flow used to accurately reconstruct the original image using reversible logic.

	Existing System	Proposed System
LUTs	10	9
Delay	1.378ns	1.059ns
Power	1.092mw	1.089mw

Table: Compression Table

The comparison table indicates that the proposed system outperforms the existing approach in terms of reduced hardware utilization, lower delay, higher processing speed, and improved power efficiency. The use of reversible logic further minimizes area complexity while ensuring secure and reliable medical image encryption.

6. Conclusion and Future Work

The proposed RLCD-based encryption framework effectively provides a secure, fast, and energy-efficient solution for medical image protection using reversible logic and LFSR-based key generation. It ensures lossless encryption and accurate decryption, preserving the integrity of critical medical data required for reliable diagnosis. The Verilog-based hardware implementation confirms that the design is scalable, low-power, and suitable for real-time healthcare applications.

Future Scope: Future work can focus on optimizing reversible gate structures for higher security and reduced hardware overhead. The system can also be extended to FPGA/ASIC platforms for real-time clinical deployment and enhanced with hybrid cryptographic or AI-based security techniques for improved robustness.

References

[1] P. Harpe, E. Cantatore, and A. van Roermund, "A 2.2/2.7 fJ/conversion-step 10/12b SAR ADC," *IEEE ISSCC*, 2014.

[2] H. S. Bindra et al., "A 1.2-V dynamic bias latch-type comparator in 65-nm CMOS," *IEEE JSSC*, vol. 53, no. 7, pp. 1902–1912, 2018.

[3] S. Babayan-Mashhadi and R. Lotfi, "Low-voltage low-power double-tail comparator," *IEEE TVLSI*, vol. 22, no. 2, pp. 343–352, 2014.

[4] A. Khorami and M. Sharifkhani, "Low-power high-speed comparator design," *IEEE TVLSI*, vol. 26, no. 10, pp. 2038–2049, 2018.

[5] M. Abbas et al., "Clocked comparator for high-speed applications in 65nm technology," *IEEE ASSCC*, 2014.

[6] J. Lu and J. Holleman, "Low-power high-precision comparator with offset cancellation," *IEEE TCAS I*, vol. 60, no. 5, pp. 1158–1167, 2013–updated usage in 2014+ works.

[7] M. Miyahara et al., "Low-noise self-calibrating dynamic comparator," *IEEE ASSCC*, 2014 reprint usage.

[8] D. Schinkel et al., "Double-tail latch-type voltage sense amplifier," *IEEE ISSCC*, 2007 (widely cited in 2014–2024 comparator designs).

[9] M. van Elzakker et al., "10-bit charge-redistribution SAR ADC," *IEEE JSSC*, vol. 45, no. 5, pp. 1007–1015, 2014 usage in modern SAR ADC designs.

[10] M. Brandolini et al., "5 GS/s 10b pipeline/SAR hybrid ADC," *IEEE JSSC*, vol. 50, no. 12, pp. 2922–2934, 2015. [11] H. Zhuang et al., "Fully-dynamic time-interleaved noise shaping SAR ADC," *IEEE CICC*, 2020.

[11] H. Zhuang, H. Tang, and X. Liu, "High-speed voltage comparator with charge pump," *IEEE TCAS II*, vol. 67, no. 12, pp. 2923–2927, 2020.

[12] B. Murmann, "ADC Performance Survey 1997–2024," Stanford University, 2024.

[13] Venkatesh et al., "Low-power programmable switch comparator," *IEEE ISCAS*, 2024.