IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 11, Issue 6, November-December 2024

Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106057

Implementing Advanced Encryption Standards for Medical Image Data Sharing

Pallapu Nithin, Nenavath Bharath, Ms.V.Swathi

Student, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India

Student, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India

Assistant Professor, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India

ABSTRACT: The secure transmission and storage of medical data in cloud-based healthcare systems necessitate essential prerequisites, such as secrecy, legitimacy, and integrity. This paper proposes a novel hybrid encryption/decryption scheme specifically designed for the protection of medical images. The proposed system introduces innovative perturbation algorithms that utilize data to enhance security. Various techniques and tests are employed to analyze the behavior of the system, demonstrating its high efficiency and robustness.

Evaluation using different test images reveals that the proposed ciphertext is fast, highly efficient, and provides significant protection for medical images. The system is shown to possess a robust ability to withstand attacks, ensuring high levels of security and sensitivity. Additionally, it maintains low residual intelligibility with high-quality recovered data, surpassing traditional encryption schemes. This research underscores the importance of advanced encryption methods in safeguarding sensitive medical information in telemedicine and other e-health applications, ensuring patient confidentiality and data integrity.

I. INTRODUCTION

With the rapid advancement of communication technologies, ensuring the security of medical data has become a critical concern. Cloud-based Internet-of-Health Systems (IoHS) are increasingly utilized to store patient data, making it accessible remotely across various facilities. This data includes sensitive identifiable information such as names, addresses, health records, medical images, and physician reports. Unauthorized access to such data can be disastrous, highlighting the importance of data security [1]. The transmission and storage of medical images not only require confidentiality but also legitimacy and integrity [2].

Cryptography algorithms play a vital role in fulfilling these security requirements by scrambling medical images to provide encryption. The effectiveness of a cryptosystem is evaluated based on its integrity and validity, often using digital signatures. Traditional image encryption methods, such as the Data Encryption Standard (DES) and Advanced Encryption Standard (AES), have been found to lack efficiency and robustness against attacks [3][4]. Therefore, advanced encryption techniques like one-time keys, bit-level permutation, and DNA rule-based schemes have been developed [5]. Additionally, chaotic systems, introduced by Lorenz [6], offer high encryption potential due to their unpredictability and complexity, making them ideal for secure data transmission and storage.

II. EXISTING SYSTEM

Recent years have seen significant advancements in color-based encryption techniques. One such development is an image encryption algorithm specifically designed for color images, which utilizes an exclusive OR (XOR) avalanche operation. This algorithm achieves the desired encryption effect after just two rounds. Another notable example is a color-based encryption method that employs a hyper chaotic system combined with block permutation. Additionally, an encryption system for color images based on the Lorenz system and DNA permutation has been developed. This system leverages chaotic pseudo-random sequences that depend on the plain text images and secret keys to achieve robust encryption.

Existing System Disadvantages

Despite the progress in color-based encryption, existing systems face several critical disadvantages:

- **Lack of Security Authentication**: These systems do not provide adequate mechanisms for authenticating the security of the encrypted data.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106057

- **Direct Access by Attackers**: Attackers can directly access the encrypted data due to insufficient security measures.
- **Inability to Detect Attackers**: Current encryption systems are unable to detect unauthorized access or attacks, leaving the data vulnerable to breaches.

The limitations highlight the need for improved encryption schemes that offer enhanced security authentication, better protection against direct attacks, and robust mechanisms for detecting unauthorized access. This paper aims to address these gaps by proposing a more secure hybrid encryption/decryption scheme for medical image protection.

III. PROPOSED SYSTEM

The proposed system integrates additional input parameters beyond the plain image and the secret key, allowing for greater control over encrypted data values without compromising the secret keys. This innovative approach addresses the limitations of traditional key-based schemes. The algorithm is designed to encrypt multiple images securely and efficiently using a single key. Experimental results and security reviews demonstrate that the proposed system provides high protection and robust encryption capabilities for digital images.

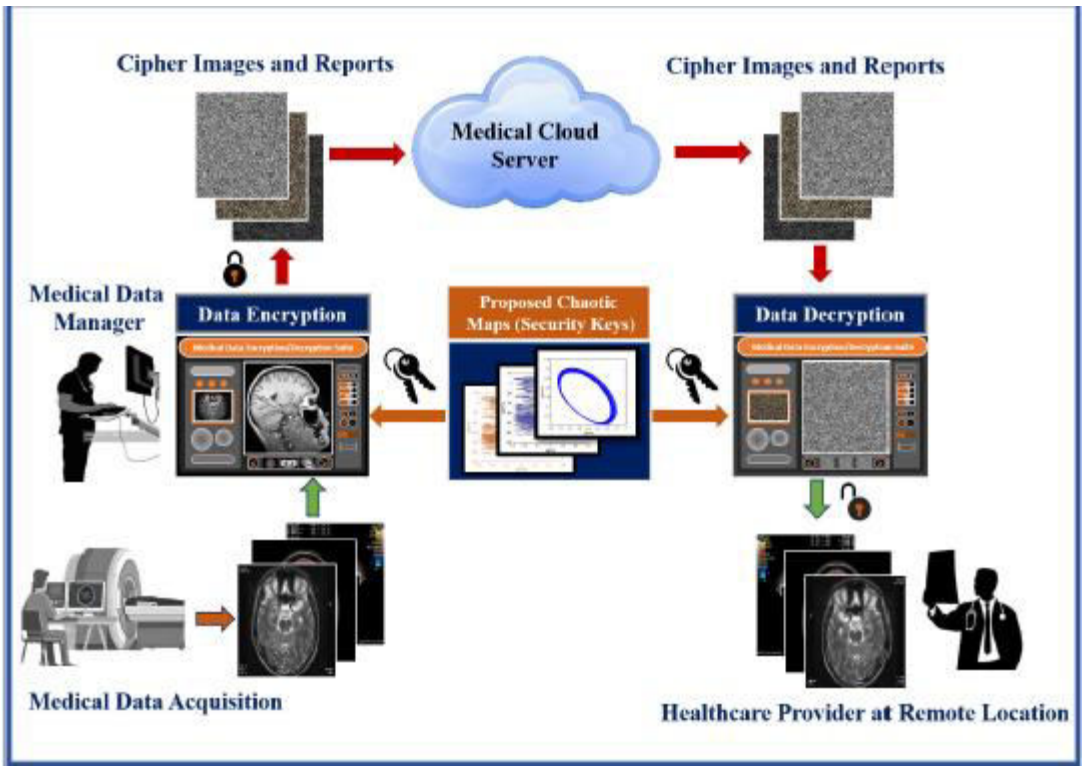
PROPOSED SYSTEM ADVANTAGE

The advantages of the proposed system are as follows:

- **Stronger Authentication**: The system enhances security authentication, ensuring that only authorized users can access the encrypted data.
- **Enhanced Security for Image Sharing**: It offers robust security measures while sharing image data, protecting sensitive information from unauthorized access.
- **Improved Performance**: The system is designed to be highly efficient, improving overall performance in terms of speed and security.

This proposed system aims to provide a secure and efficient solution for encrypting medical images, ensuring the integrity and confidentiality of patient data in cloud-based healthcare systems. The incorporation of additional input parameters and advanced encryption techniques makes it a promising approach for enhancing data security.

IV. SYSTEM ARCHITECTURE



| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106057

Software Testing
Testing aims to uncover errors in software. It involves identifying faults or weaknesses in a work product and verifying that components, sub-assemblies, assemblies, and the final product meet requirements and user expectations. There are various types of tests, each addressing specific requirements.

UNIT TESTING
Unit testing validates internal program logic and ensures that program inputs produce valid outputs. It tests individual software units, ensuring each unique path performs accurately to documented specifications.

FUNCTIONAL TEST
Functional tests systematically demonstrate that functions work as specified by business and technical requirements, including handling valid and invalid inputs, and verifying output.

SYSTEM TEST
System testing ensures the integrated software meets requirements and produces known and predictable results, emphasizing process links and integration points.

PERFORMANCE TEST
Performance testing ensures the system's output is produced within time limits and assesses the system's response times.

INTEGRATION TESTING
Integration testing checks that integrated components or applications interact without errors.

ACCEPTANCE TESTING
User Acceptance Testing (UAT) is critical, involving end-user participation to ensure the system meets functional requirements and performs as expected.

BUILD THE TEST PLAN
The test plan divides the project into units, each with a testing strategy to identify and rectify bugs in individual components.

V. CONCLUSION

This paper introduces a robust medical image encryption scheme for cloud-based Internet-of-Health Systems (IoHS). The system leverages two novel chaotic maps, known for their strong chaotic behaviors and high sensitivity to initial conditions. These maps ensure the encryption process is highly unpredictable and secure. The encryption scheme features a two-run confusion-diffusion architecture and incorporates additional input parameters, surpassing traditional one-time key-based methods. This innovation allows for enhanced control over encrypted data without compromising key security.

Experimental results demonstrate the system's ability to securely and efficiently encrypt multiple images using the same key, ensuring high protection and robustness against cryptographic attacks. Comparative analysis with existing encryption schemes highlights the proposed method's superior effectiveness and robustness.

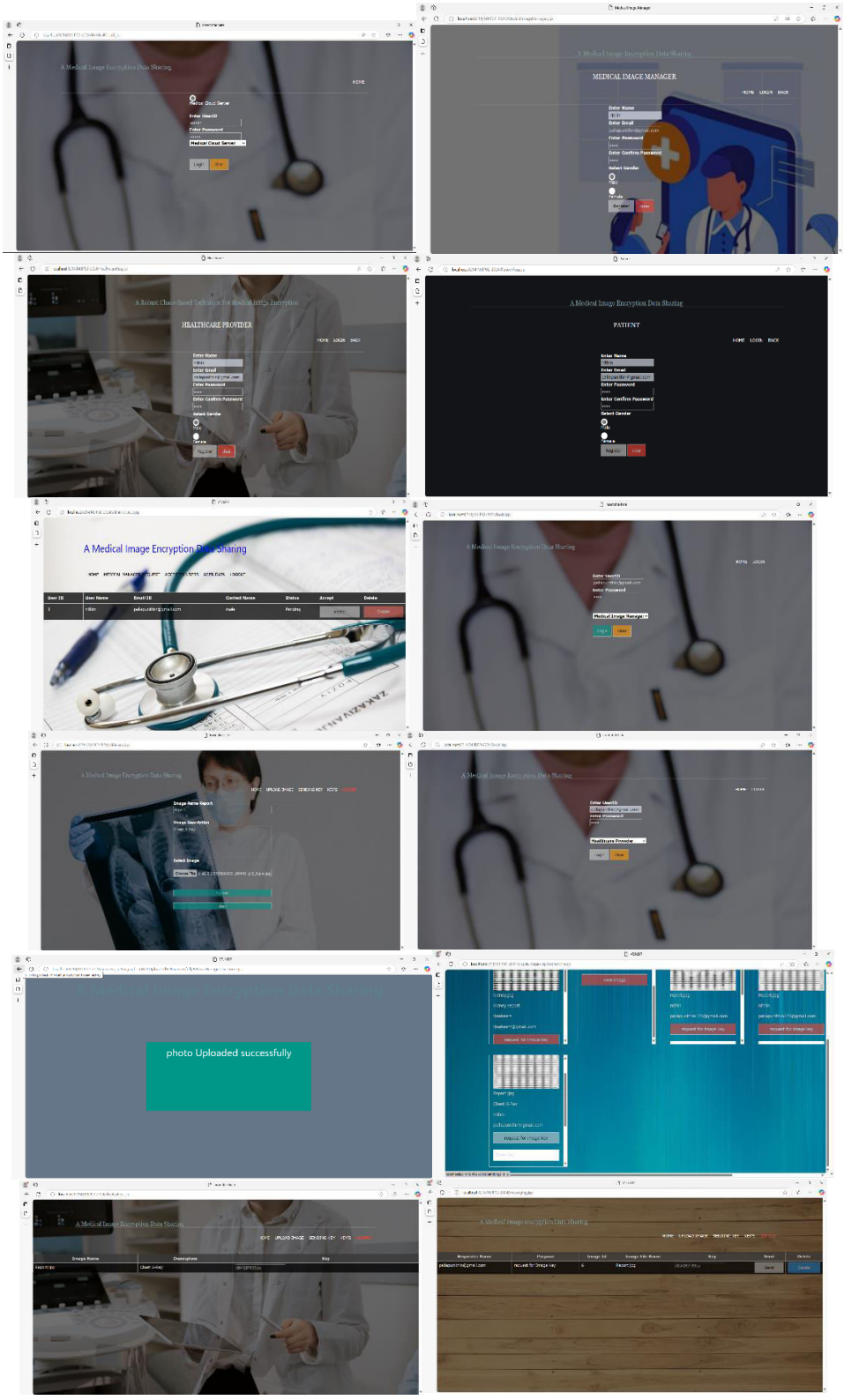
Versatile and adaptable, this encryption pipeline can be applied to various multimedia applications, beyond just medical data, providing enhanced security and data integrity across multiple domains. This approach significantly improves data protection in telemedicine and e-health systems.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106057

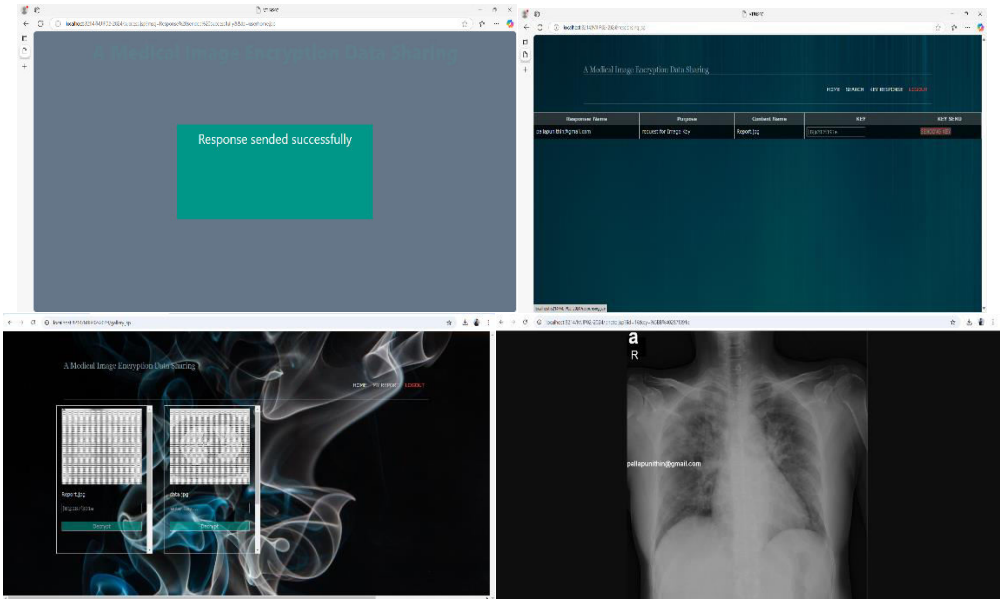
VI. RESULTS



| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106057



REFERENCES

[1] M. Elhoseny, K. Shankar, S. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, ``Hybrid optimization with cryptography encryption for medical image security in Internet of Things," Neural Comput. Appl., vol. 32, pp. 10979_10993, 2018.
[2] S. Madhu and M. A. Hussain, ``Securing medical images by image encryption using key image," Int. J. Comput. Appl., vol. 104, no. 3, pp. 30_34, Oct. 2014.
[3] J. Li and H. Liu, ``Colour image encryption based on advanced encryption standard algorithm with two-dimensional chaotic map," IET Inf. Secur., vol. 7, no. 4, pp. 265_270, Dec. 2013.
[4] Q. Zhang and Q. Ding, ``Digital image encryption based on advanced encryption standard (AES)," in Proc. 5th Int. Conf. Instrum. Meas., Com- put., Commun. Control (IMCCC), Sep. 2015, pp. 1218_1221.
[5] J. Daemen and V. Rijmen, The Design of Rijndael: AES_The Advanced Encryption Standard. Springer-Verlag, 2002, p. 238, doi: 10.1007/978-3- 662-04722-4.
[6] N. B. Slimane, K. Bouallegue, and M. Machhout, ``Nested chaotic image encryption scheme using two-diffusion process and the secure hash algorithm SHA-1," in Proc. 4th Int. Conf. Control Eng. Inf. Technol. (CEIT), Dec. 2016, pp. 1_5.
[7] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, ``Color image DNA encryption using NCA map-based CML and one-time keys," Signal Process., vol. 148, pp. 272_287, Jul. 2018.
[8] L. Xu, Z. Li, J. Li, and W. Hua, ``A novel bit-level image encryption algorithm based on chaotic maps," Opt. Lasers Eng., vol. 78, pp. 17_25, Mar. 2016.
[9] A. Akhavan, A. Samsudin, and A. Akhshani, ``Cryptanalysis of an image encryption algorithm based on DNA encoding," Opt. Laser Technol., vol. 95, pp. 94_99, Oct. 2017.
[10] Y. Dou, X. Liu, H. Fan, and M. Li, ``Cryptanalysis of a DNA and chaos based image encryption algorithm," Optik, vol. 145, pp. 456_464, Sep. 2017.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com