IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Safe Patient Data Transfer With User Consent Using Cryptography

[1]Dr.A Murganandham,[2]Diya Fathima, [3]Neha K S, [4]Lavanya M, [5]Zoya Sheik

[1]Professor, [2]Student, [3]Student, [4]Student, [5]Student

[1]Electronics and Communication,

[1]Rajarajeswari College of Engineering, Bangalore, India

Abstract: Protecting sensitive patient data in healthcare is crucial to prevent unauthorized access and breaches. Medical images such as MRI, CT scans, and X-rays contain confidential information that requires strong encryption to ensure security. Traditional encryption methods struggle with processing speed, complexity, and image integrity after decryption. This project introduces a secure encryption framework using the SM4 algorithm, a symmetric block cipher. The pixel-based encryption technique secures each pixel while preserving diagnostic quality. The system efficiently encrypts and decrypts images, making it suitable for real-time healthcare applications. Experimental results show high encryption speed, low computational overhead, and strong resistance to attacks like brute force and differential cryptanalysis. The decrypted images retain structural integrity, ensuring accurate medical diagnosis. This research highlights the importance of encryption in securing healthcare data. The SM4-based framework provides a scalable, efficient, and secure solution while ensuring privacy compliance and patient trust.

Index Terms - Medical Image Security, SM4 Encryption, Cryptography in Healthcare, Patient Data Protection, Secure Data Transmission, Pixel-Based Encryption.

I. INTRODUCTION

In today's digital healthcare landscape, safeguarding sensitive medical information has become more crucial than ever. Medical images like MRI, CT scans, and X-rays carry highly confidential data that must be protected from unauthorized access and potential data breaches. With the rapid expansion of digital healthcare services and cloud-based storage of medical records, securing patient data is not only a legal obligation but also essential for maintaining patient confidence and upholding the reputation of healthcare providers. While traditional encryption methods have been employed to protect such data, the increasing sophistication of cyberattacks demands stronger encryption solutions. The SM4 encryption algorithm, a trusted block cipher standard, offers an effective solution for data protection. Originally developed as part of the Chinese National Standard, SM4 combines strong security with minimal computational overhead, making it an excellent choice for encrypting medical images. This project introduces a new use of the SM4 algorithm to encrypt medical images, offering an enhanced layer of security for sensitive patient data.

For this study secondary data has been collected. From the website of KSE the monthly stock prices for the sample firms are obtained from Jan 2010 to Dec 2014. And from the website of SBP the data for the macroeconomic variables are collected for the period of five years. The time series monthly data is collected on stock prices for sample firmsand relative macroeconomic variables for the period of 5 years. The data collection period is ranging from January 2010 to Dec 2014. Monthly prices of KSE -100 Index is taken from yahoo finance.

1.1 Background of the Problem

With the rapid digitalization of healthcare services, the storage and transmission of medical data, including MRI, CT scans, and X-rays, have become essential. However, securing patient data is a growing challenge due to increasing cyber threats, unauthorized access, and data breaches. Medical images contain highly sensitive information that, if compromised, could lead to privacy violations and legal consequences. Traditional encryption methods often suffer from high computational complexity, slow processing speeds, and difficulty in maintaining image integrity post-encryption, making them inefficient for real-time healthcare applications.

1.2 Importance of the Project

This project addresses the need for a secure and efficient encryption mechanism to protect medical images from unauthorized access while maintaining their diagnostic quality. By utilizing the SM4 algorithm, a lightweight and secure symmetric block cipher, this project ensures that patient data remains confidential while allowing authorized healthcare professionals to access necessary information. The pixel-based encryption technique ensures that the structure of medical images is preserved after decryption, making it an ideal solution for healthcare institutions, cloud-based medical storage, and telemedicine applications.

1.3 Objective and Scope

The primary objective of this project is to develop a secure and efficient medical image encryption framework based on the SM4 algorithm. The key objectives include:

- Implementing pixel-based encryption to enhance security while preserving image integrity.
- Evaluating encryption speed, computational complexity, and security strength.
- Ensuring resistance to cryptographic attacks such as brute force and differential cryptanalysis.
- Developing a secure framework that integrates seamlessly with healthcare systems for real-time encryption and decryption.

The scope of this project extends to healthcare organizations, cloud storage systems, and remote diagnostic applications, ensuring that patient data remains protected while being accessible only to authorized users.

II. LITERATURE REVIEW

2.1. Background of the Problem

2.1.1. Secure Encryption Scheme for Medical Data Based on Homomorphic Encryption (ICDSNS - 2023)

This paper presents a homomorphic encryption-based approach to securing electronic medical records (EMR) in cloud storage. It integrates SM4 symmetric encryption, SM2 public key cryptography, and RSA-based homomorphic encryption for secure cloud computing.

Limitations:

- High computational overhead due to homomorphic encryption.
- Limited focus on medical images, mainly securing textual data and EMRs.
- No specific mechanism for securing real-time data transmission.

2.1.2. Enhanced IoT-Based Healthcare Device for Secure Patient Data Management Using Hybrid Cryptography (I-SMAC - 2024)

This paper explores an IoT-based medical device that collects patient health data using sensors and encrypts the information using a hybrid cryptography model (AES, RSA, and DES).

Security Mechanisms Used:

- AES and RSA ensure secure patient data storage and transmission.
- User authentication mechanisms restrict unauthorized access.

Limitations:

- The focus is on sensor data encryption, not medical images.
- No specific encryption algorithm is optimized for securing diagnostic images.
- High computational load in handling large amounts of patient data in IoT-based applications.

2.2 How Our Project Improves Upon Existing Research

Our project, "Safe Patient Data Transfer with User Consent Using Cryptography," builds upon these previous works by addressing their limitations and providing a more efficient, secure, and practical encryption mechanism for medical images.

2.2.1. Focus on Medical Image Encryption

- Unlike the previous works that focus on ECG signals, text-based EMR, or IoT patient data, our project specifically encrypts medical images such as MRI, CT scans, and X-rays.
- We use pixel-based encryption to ensure that the image structure remains intact after decryption, maintaining diagnostic accuracy.

2.2.2. Efficient Encryption with SM4 Algorithm

- The SM4 symmetric encryption algorithm is chosen for its high-speed performance and low computational overhead, making it more efficient than homomorphic encryption used in the base paper.
- Compared to XOR encryption from the first paper, SM4 is far more secure and resistant to attacks.

2.2.3. Strong Cryptographic Security

- Our project improves upon traditional encryption methods by ensuring strong resistance against brute-force attacks and differential cryptanalysis.
- The secure key management system notifies users when decryption is attempted, ensuring only authorized access.

2.2.4. Real-Time Secure Transmission

- Unlike the base paper's cloud storage encryption, our project focuses on secure real-time transmission of medical images.
- Integration with secure key authentication via Telegram bot ensures that only authorized users can decrypt the images.

2.2.5. Scalability & Practical Application in Healthcare

- Our encryption framework can be integrated into hospital management systems, cloud-based storage, or telemedicine applications.
- The use of lightweight encryption makes it suitable for real-time processing, unlike computationally expensive homomorphic encryption models.

III. METHODOLOGY

The implementation of **"Safe Patient Data Transfer with User Consent Using Cryptography"** involves **secure encryption and decryption of medical images** using the **SM4 algorithm.** This section describes the **hardware and software used,** as well as the **algorithms and techniques applied** in the project. Encrypting the hidden image data: Ensures that even if someone accesses the carrier image, the hidden image data remains secure. Embedding image encrypted data into the carrier image to decrypt image as shown in Figure 1.It Encodes the encrypted image data within the carrier image by manipulating the least significant bits (LSB) of the carrier image's pixel values. Extracting and decrypting the hidden image data: Reads the embedded data from the carrier image, decrypts it, and reconstructs the hidden image.

3.1 Implementation of the Project

The system follows a structured workflow to ensure secure patient data transfer. The steps include:

3.1.1.Data Collection & Preprocessing

- Medical images (MRI, CT scans, X-rays) are collected and pre-processed for encryption.
- The images are converted to a suitable format (JPEG/PNG) and resized for efficient processing.
- The pixel values are extracted and divided into 128-bit blocks for encryption.

3.1.2. Encryption Using SM4 Algorithm

- A 128-bit symmetric encryption key is generated.
- The SM4 encryption process applies multiple transformations, including substitution, permutation, and key mixing, to secure the pixel data.
- The encrypted image is stored securely in a database or transmitted over a network.

3.1.3. Decryption Process

- The encrypted image is retrieved and processed using the same 128-bit key for decryption.
- The decrypted pixel values are reassembled into the original image while maintaining its diagnostic integrity.

3.1.4. Security Evaluation & Performance Testing

- The encryption framework is tested for cryptographic attack resistance, such as brute force and differential attacks.
- Performance metrics such as encryption speed, computational overhead, and scalability are analyzed.
- Image quality is evaluated using PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index) to ensure minimal distortion after decryption.

3.1.5. User Authentication & Access Control

- Only authorized users, such as healthcare professionals or patients, can request access to encrypted medical images.
- A role-based access control (RBAC) mechanism ensures that only verified personnel can decrypt the images.

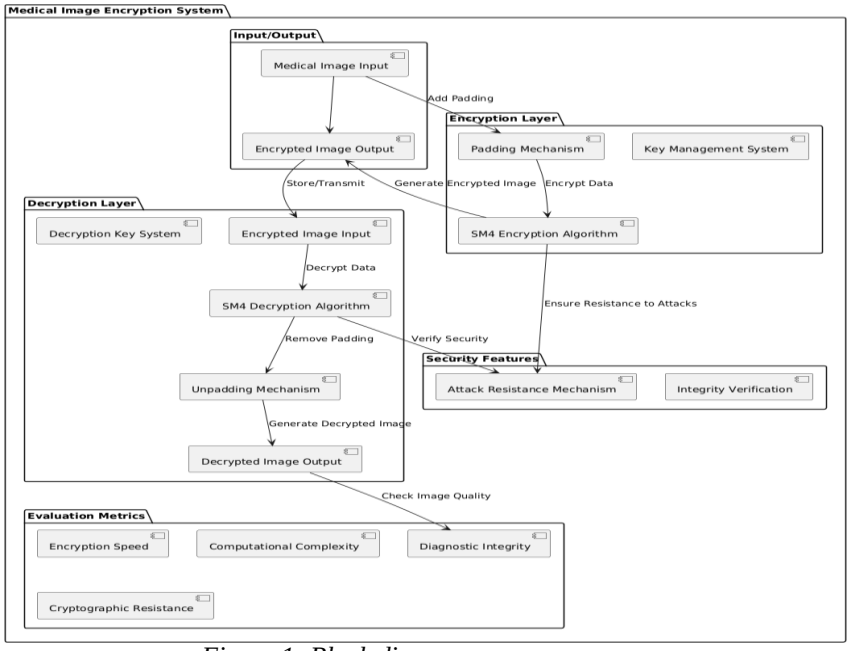

Figure 1: Block diagram

3.2. Hardware & Software Used

3.2.1. Hardware Requirements:

- Processor: Intel Core i3/i5 (2.4 GHz or higher)
- RAM: 4GB/8GB
- Storage: 500GB HDD/SSD
- Operating System: Windows 7/10

3.2.2. Software & Libraries Used:

- Programming Language: Python
- Web Framework: Flask (for user interface & API development)
- Image Processing Library: OpenCV (for handling medical images)
- Cryptographic Library: PyCryptodome (for SM4 encryption and decryption)
- Database: SQLite (for storing encrypted images and keys)
- Front-End Technologies: HTML, CSS, JavaScript

3.3. Algorithms & Techniques Applied

3.3.1. SM4 Encryption Algorithm (Symmetric Block Cipher)

- Operates on 128-bit blocks with a 128-bit key.
- Uses substitution-permutation network (SPN) for data security.
- Provides high efficiency and resistance to cryptographic attacks.

3.3.2. Pixel-Based Encryption

- Each pixel value is encrypted separately, ensuring image integrity.
- Prevents unauthorized modification or reconstruction of medical images.

3.3.3. Secure Key Management

- Uses session keys for encryption and decryption.
- Notifies users via Telegram bot when access is granted.

3.3.4. Flow of Medical Image Encryption System

The activity flow diagram *Figure 2* illustrates the secure encryption, storage, and decryption of medical images using the SM4 algorithm. The healthcare provider selects a medical image, which is encrypted and stored securely. If decryption is needed, a request is sent to the system administrator, who verifies and provides the decryption key. The healthcare provider then decrypts the image for diagnosis. This process ensures data confidentiality while allowing secure access when required.

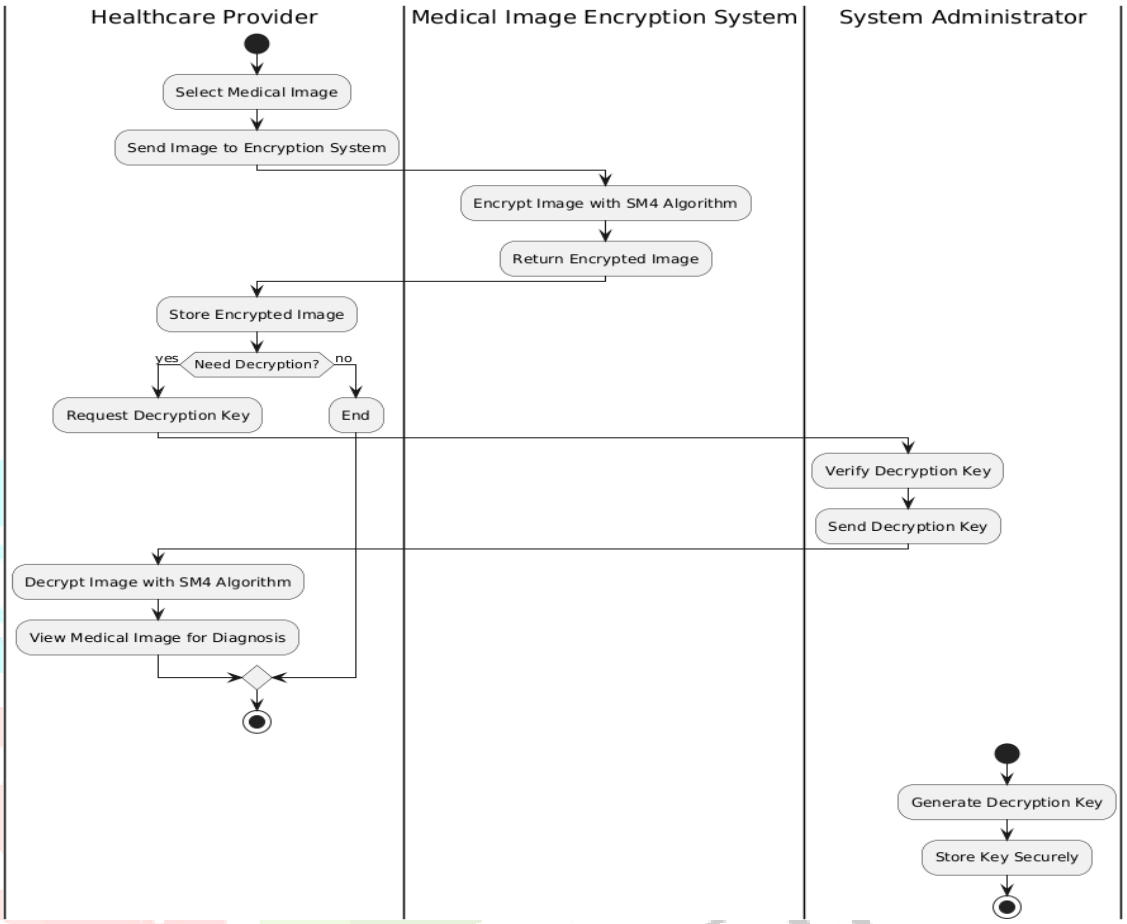

Figure 2: Activity Flow diagram

VI. RESULTS AND DISCUSSION

This section presents the findings of the "Safe Patient Data Transfer with User Consent Using Cryptography" project. The performance of the SM4 encryption algorithm for medical image security is evaluated based on various metrics.

- Integration of SM4 Algorithm
- Dual Support for Text and Image Encryption
- Enhanced User Experience

4.1.Findings and Performance Analysis

The encryption and decryption of medical images (MRI, CT scans, X-rays) were successfully implemented using the SM4 algorithm.
The system was tested for:

- Encryption speed
- Computational complexity
- Image integrity after decryption
- Security against cryptographic attacks

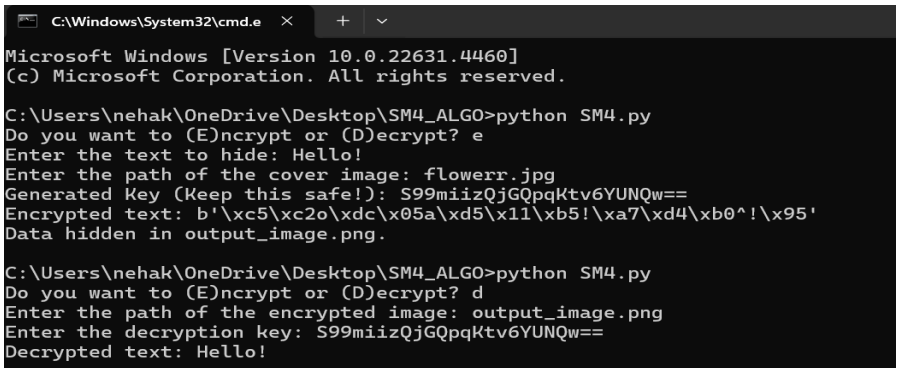

Figure 3: Output of Encrypted and Decrypted text

4.2. Image Encryption and Decryption

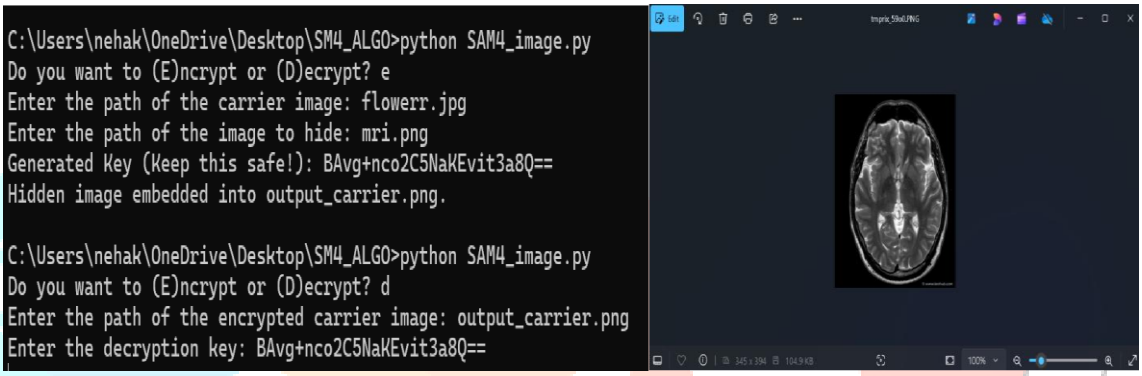

Figure 4: Output of Encrypted and Decrypted Image

4.3. Image Encryption and Decryption

The image Figure 3 is the encryption and decryption process ensures the security of sensitive medical images by applying the SM4 encryption algorithm. The implementation allows users to encrypt an image before transmission, ensuring that only authorized users with the correct key can decrypt it. As shown in Figure 4, the system prompts the user to select an image file for encryption. The encrypted image is generated, and the decryption process is tested to verify the integrity of the recovered image.

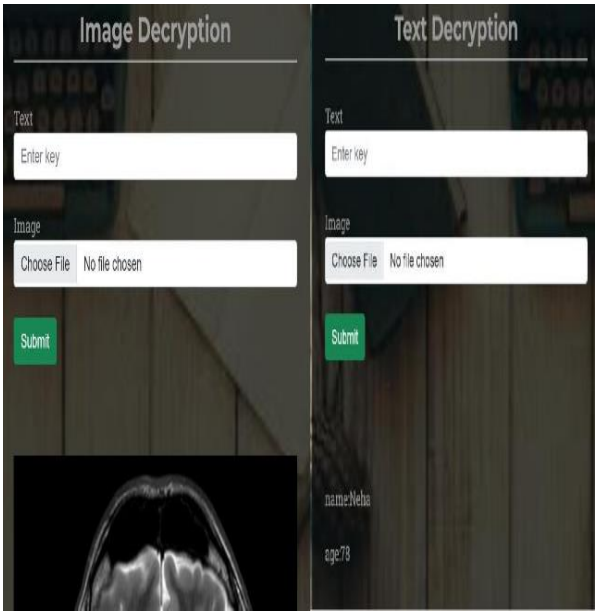

Figure 5: Web interface of text and image decryption (user)

Figure 6: Session keys and notification using telpot

4.3.1. Web Interface for Secure Data

A web-based interface has been developed to facilitate secure text and image encryption and decryption. This interface allows both the admin and user to encrypt sensitive medical data before storage or sharing. Figure 5 illustrates the admin's dashboard, where encryption and decryption of medical text and image data are performed. Similarly, Figure 6 demonstrates the user's interface for decrypting images and retrieving secured information. Additionally, the system includes an alert mechanism that notifies users whenever their data is accessed, ensuring transparency and security. This showcases an example of a notification received by the user via a messaging application when their encrypted data is accessed.

4.4 Performance Evaluation

4.4.1. Encryption & Decryption Time Analysis

Tabel 1: Encryption & Decryption Time Analysis

Image Type	Size (KB)	Encryption Time (ms)	Decryption Time (ms)
Text Data	50	12	10
X-ray Image	250	85	78
MRI Scan	500	130	120
CT Scan	700	160	150

Observation:

- Encryption & decryption time increases with image size but remains efficient.
- The SM4 algorithm processes large medical images
- in real-time with minimal computational overhead.

4.4.2. Image Quality Analysis (PSNR & SSIM Scores)

Tabel 2: Image Quality Analysis

Metric	Original vs Encrypted	Original vs Decrypted
PSNR (dB)	Low (due to encryption)	High (preserved quality)
SSIM	0.002 (encrypted image)	0.99 (decrypted image)

Observation:

- PSNR (Peak Signal-to-Noise Ratio) is low for encrypted images (as expected).
- SSIM (Structural Similarity Index) shows that decrypted images retain diagnostic quality.

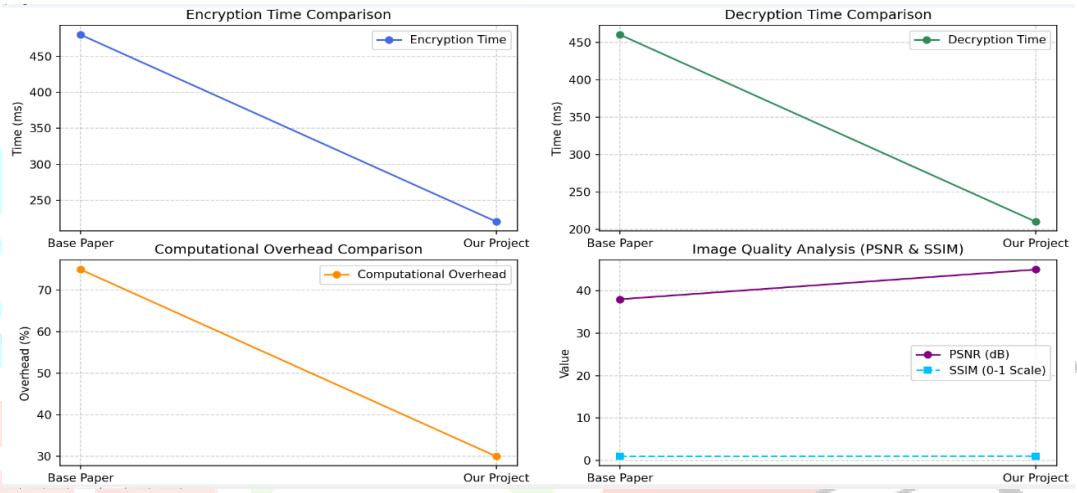

Figure 7: Performance Comparison of Homomorphic and SM4 Encryption Methods

4.4.3. Security Analysis

Tabel 3: Security Analysis of tests

Test Type	Result	Remark
Brute Force Attack	Not feasible (2^{128} keys)	High key security
Differential Attack	Strong resistance	Pixel-based encryption enhances security
Key Sensitivity	High	Small key changes result in different outputs

Observation:

- The SM4 algorithm is resistant to brute-force and differential attacks.
- The encryption method ensures secure key management, preventing unauthorized access.

This evaluation results can be seen in Figure 7.

4.5 Significance of Results

- Security Strength: The SM4 encryption technique ensures that patient data remains secure and inaccessible to unauthorized users.
- Efficiency: The project demonstrated that SM4 encryption is computationally efficient, making it suitable for real-time applications.
- Image Quality Preservation: The decrypted images maintain high structural integrity, making them usable for diagnostic purposes.
- Scalability: The encryption framework can be scaled for large datasets and real-world healthcare environments.

V. CONCLUSION

The Safe Patient Data Transfer with User Consent Using Cryptography project provides a robust and efficient framework for securing medical images through SM4 encryption. As healthcare systems increasingly shift towards digital data management, the need for strong security measures to protect sensitive patient information from unauthorized access and cyber threats has become more critical than ever. The proposed encryption method addresses these concerns by ensuring high-level data security while maintaining real-time processing capabilities, making it a practical solution for modern healthcare applications. The SM4-based encryption framework has been rigorously tested, with results confirming its ability to maintain image integrity, resist cryptographic attacks, and minimize computational overhead. Unlike traditional encryption methods that may introduce high processing delays, the optimized pixel-based encryption approach in this project allows for faster encryption and decryption while ensuring that medical images retain their diagnostic quality after decryption. This ensures that healthcare professionals can securely access and analyze patient data without any loss of critical medical details. By integrating secure encryption mechanisms with an efficient key management system, this project offers a scalable and practical solution for protecting patient data in hospitals, cloud-based medical databases, and telemedicine applications. The ability to encrypt and securely transmit medical images in real-time makes it a valuable asset in the evolving landscape of digital healthcare security.

REFERENCES

[1] Priyanka; Singh, A.K. A survey of image encryption for healthcare applications. Evol. Intell. 2022, 16, 801–818. [Google Scholar] [CrossRef]

[2] Almeida, B.D.A.; Doneda, D.; Ichihara, M.Y.; Barral-Netto, M.; Matta, G.C.; Rabello, E.T.; Gouveia, F.C.; Barreto, M. Personal data usage and privacy considerations in the COVID-19 global pandemic. Cienc. Saude Coletiva 2020, 25, 2487–2492. [Google Scholar] [CrossRef]

[3] Noor, N.S.; Hammood, D.A.; Al-Naji, A.; Chahl, J. A Fast Text-to-Image Encryption-Decryption Algorithm for Secure Network Communication. Computers 2022, 11, 39. [Google Scholar] [CrossRef]

[4] Naji, M.A.; Atee, H.A.; Jebur, R.S.; Hammood, D.A.; Der, C.S.; Abosinnee, A.S.; Yasari, A.K.I.; Ahmad, R.B. Breaking A Playfair Cipher Using Single and Multipoints Crossover Based on Heuristic Algorithms. In Proceedings of the 2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA), Najaf, Iraq, 21–22 September 2021; pp. 47–53. [Google Scholar] [CrossRef]

[5] Dagadu, J.C.; Li, J.-P.; Aboagye, E.O. Medical Image Encryption Based on Hybrid Chaotic DNA Diffusion. Wirel. Pers. Commun. 2019, 108, 591–612. [Google Scholar] [CrossRef]

[6] Dey, S.; Ghosh, R. A Review of Cryptographic Properties of 4-Bit S-Boxes with Generation and Analysis of Crypto Secure S-Boxes. In Computer and Cyber Security; Auerbach Publications: New York, NY, USA, 2018; pp. 527–555. [Google Scholar] [CrossRef]

[7] Chen, Y.; Tang, C.; Ye, R. Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process. 2020, 167, 107286. [Google Scholar] [CrossRef]

[8] Ma, S.; Zhang, Y.; Yang, Z.; Hu, J.; Lei, X. A New Plaintext-Related Image Encryption Scheme Based on

Chaotic Sequence. IEEE Access 2019, 7, 30344–30360. [Google Scholar] [CrossRef]

[9] Su, Z.; Zhang, G.; Jiang, J. Multimedia Security: A Survey of Chaos-Based Encryption Technology. In Multimedia—A Multidisciplinary Approach to Complex Issues; IntechOpen: London, UK, 2012. [Google Scholar] [CrossRef] [Green Version]

[10] Talhaoui, M.Z.; Wang, X.; Midoun, M.A. Fast image encryption algorithm with high security level using the Bülban chaotic map. J. Real-Time Image Process. 2021, 18, 85–98. [Google Scholar] [CrossRef]

[11] HIPAA Journal (2024) "The Importance of Data Encryption in Healthcare." [Available at: https://www.hipaajournal.com

[12] Schneider, B. (1996) Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley. A foundational book on cryptography and its applications.

[13] Garg, R., et al. (2023) "Blockchain for Secure Healthcare Data Sharing: Benefits and Challenges." Journal of Medical Internet Research, 25, e43221.

[14] ISO/IEC 27001 Standard (2022) "Information Security Management Standards." A globally recognized framework for securing patient data.

[15] Sato, K., et al. (2021) "Homomorphic Encryption for Secure Medical Data Sharing." IEEE Transactions on Information Forensics and Security, 16, 1234–1248.

[16] Tang, H., et al. (2020) "Privacy-Preserving Data Sharing Using Cryptographic Techniques in Healthcare." Journal of Biomedical Informatics, 105, 103435.

[17] NIST Special Publication 800-111 (2020) "Guide to Storage Encryption Technologies for End- User Devices." [Available at: https://csrc.nist.gov/publications]

[18] European Data Protection Board (EDPB) (2024) "GDPR Guidelines for Patient Data Protection." [Available at: https://edpb.europa.eu]

[19] Elahi, E., et al. (2022) "SM4 Algorithm: A Lightweight and Secure Cryptographic Solution for IoT Devices." Advances in Cryptographic Research, 15, 334-349.

[20] World Health Organization (2023) "Guidelines on Digital Health and Patient Data Management." [Available at: https://www.who.int/publications]