ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206

Volume 8, Issue 8, August 2025

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808190

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

MINIMIZING DATA LEAKAGE IN HEALTH CARE SYSTEMS THROUGH SECURE ENCRYPTION ARCHITECTURES

Dr. Vidya Pol, Srihari A

Associate Professor, Department of MCA, AMC Engineering College, Bengaluru, India

Student, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT: In the digital age, the security and privacy of patient data, particularly medical images, have become paramount due to the increasing threats of data breaches and unauthorized access. This paper presents a novel approach to medical image encryption utilizing the SM4 algorithm, a symmetric block cipher widely used in secure communications. By applying a pixel-based encryption technique using the SM4 algorithm, the proposed encryption framework enhances the security of medical images such as MRI, CT scans, and X-rays. The SM4 algorithm encrypts the pixel values in a highly secure and efficient manner, rendering the images unintelligible without the corresponding decryption key. The medical images and the text information of the patients can be encrypted so that their records are kept safe from any cyber threats. The patient or the hospital staff should use the decryption key to see the details which are encrypted it increases the privacy of the Patients. The efficacy of this approach is evaluated based on various metrics, including encryption speed, computational complexity, and resistance to common cryptographic attacks. Experimental results demonstrate that the proposed method not only preserves the structural integrity and diagnostic value of the images post-decryption but also provides a robust solution to safeguard sensitive patient data.

KEYWORDS: SM4, Encryption, Cipher block, Privacy.

I. INTRODUCTION

It introduces an efficient Encryption frame work to safeguard the Patients health records from cyber threats. The SM4 encryption algorithm, a widely recognized standard for block ciphers, is an effective method for securing data. The System uses SM4 Algorithm for encrypting Medical images and text information also. The system must decrypt encrypted images to restore their original form for diagnostic purposes. The System will generate, store, and transmit encryption keys to the patients and the authorized entities. The system must authenticate users to ensure only authorized patients can access the encrypted images and text related information. This framework employs a pixel-based encryption technique. Using the pixel values of the medical images will encrypt. This Guarantee that if small amount data is Catched it will not get access without decryption key. The SM4 algorithm's symmetric structure allows for rapid encryption and decryption, making it suitable for real-time applications.

II. LITERATURE SURVEY

[1] Electronic health records are normally composed of patient-related information, medical history, symptoms and more information, which are maintained by the involved services in healthcare. Priyanka, Amit Kumar Singh (2022) Proposed a survey, a brief introduction, and the most utilized interesting applications of image encryption. In need of more security for images, the concept of hashing was introduced. It is a one-way function of cryptography that converts any form of data into a unique string of text known as the message digest. The hash method cannot be reversed. Its main contribution is to verify the quality of an image to check any type of alteration or duplicity to the features of an image.

[2] Confidential information in the form of text, pictures, audio, and video are sent over devices. Cryptography is the application of techniques for encrypting data between the sender and receiver so that the receiver can read the data and an adversary cannot. N.S Noor ,D A Hamood ,Al-Naji, Al. Chahl, J. In this work, there are two concepts of image encryption, color mode and color code, that need to be examined in data encryption. Different colors are encoded and mixed to obtain the color required to display the image on the screen or to print it from a printer.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[3] Introduced the use of two chaotic systems (Bernoulli shift map and Zizag map) coupled with DNA coding in an encryption form for medical images in this paper. Dagadu, J.C.; Li, J.-P.; Aboagye, E.O. (2019) introduced of two concepts: Chaotic key generation, DNA diffusion. The message digest algorithm uses five hash function to perform on the plain medical image and the value of hash used in combination with the value of an input ASCII string to develop constraints and boundary for both chaotic systems.

[4]. To safeguard the content of an image is an important issue. Image encryption, which transforms the essential content of an image into noise-like results, is a vital method for protecting images, including medical images. Chen Y, Tang C, et al. (2020) introduced that the cipher image can be fully recovered by attacking using chosen plain image. To increase resistance against such attacks, we propose an improved encryption scheme that performs nonlinear operations on permuted images using an enhanced version of the original algorithm.

[5]. Every 4bit linear relations tested for a particular 4bit crypto S-box.4bit unique linear relations tested for satisfaction of 16- 4 bit unique patterns and for the output bit patterns generated from each index.

EXISTING SYSTEM

Current encryption systems for medical images typically employ standard algorithms like AES (Advanced Encryption Standard) and DES (Data Encryption Standard). While these techniques provide reasonable security, they often come with trade-offs in terms of performance and compatibility with medical imaging formats. With large datasets and real-time medical applications, existing systems struggle to maintain efficiency, leading to latency in healthcare workflows.

PROPOSED SYSTEM

This System proposes an advanced encryption framework using the SM4 algorithm. The SM4 encryption algorithm is a block cipher that operates on 128-bit blocks, offering a high level of security with lower computational complexity. The System Encrypts the medical images inside another images and the information related to the patient will also be encrypted. The system generates the key and it will be transmitted to the patient. The patient can decrypt the images or text information using the key. The system will authenticate the users to ensure only authorized patients can access the encrypted information. The patient will get notify when the hospital management are trying to access the encrypted data.

III. SYSTEM ARCHITECTURE

The System main goal is to protect the information of patients in the health care industry. The diagnosis information and medical images will be encrypted and the system will generate key. Images will ge encrypted inside an another image and text related information also will be encrypted inside the image. And it will be transmitted to the patients and those patients who have authorization can decrypt the information.

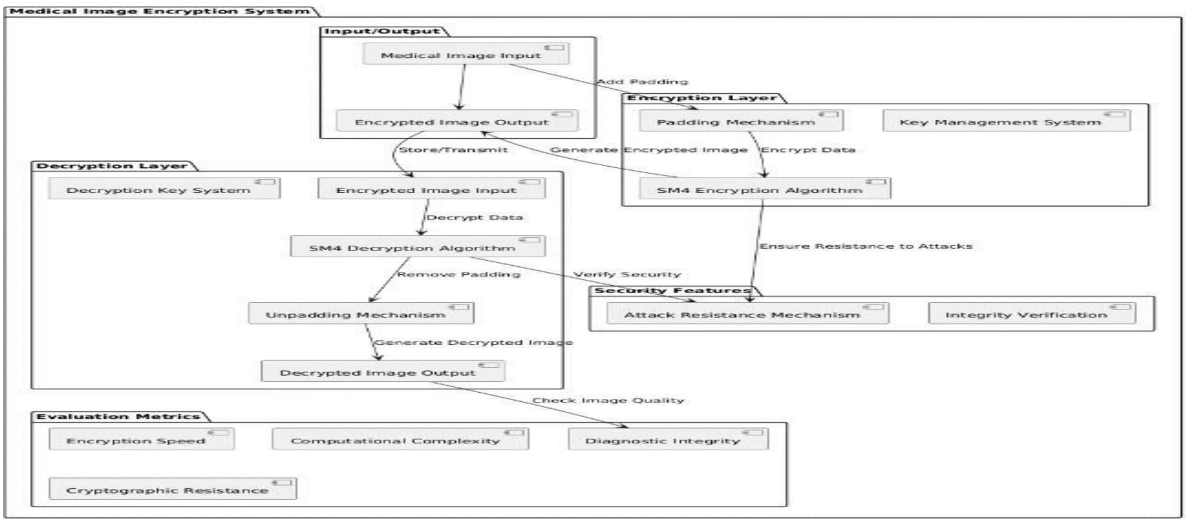


Fig 3.1 System Architecture

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808190

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

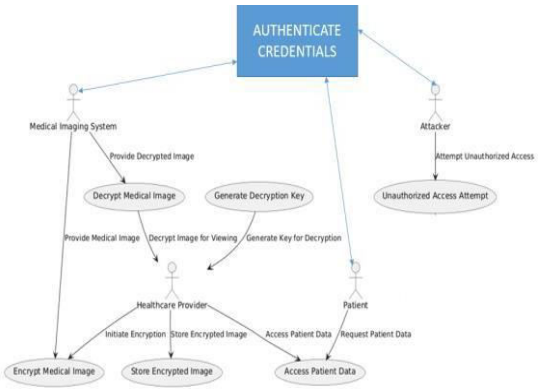
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. METHODOLOGY

The methodology for encrypting medical images using the SM4 algorithm involves several key stages, from data preparation to encryption, decryption, and evaluation. The process ensures the security and privacy of sensitive medical images like MRI, CT scans, and X-rays, while maintaining the image's diagnostic integrity. The first will be image collection and preprocessing. The medical images such as MRI, CT scan images will be collected this image will be input for the encryption process. Images will Checked if it is cooperative with encryption framework. This includes converting images to a suitable format (e.g., PNG, JPEG) and ensuring consistent resolution and size for the encryption algorithm. The pixel values of the images are extracted and treated as data blocks for encryption. A 128-bit symmetric encryption key is generated, which will be used to both encrypt and decrypt the medical images. The encrypted images is split into 128-bit blocks. Each block is decrypted using the SM4 algorithm in ECB mode. The pixel values which are decrypted will be restructured to get the original medical image. The decrypted image should be identical to the original pre-encrypted image.

V. DESIGN AND IMPLEMENTATION

The medical imaging system provides encrypting and decrypting images and text information. The health care Provider will initiate encrypting text into the image and it also encrypts image inside a image. The health care provider can access the data using the key. The patient will receive the decryption key and he can view the information using that key. If an attacker or un authorized person tries to access the information of the patients the system will not give access to the information saying that unauthorized access attempt. The health care provider uploads a medical image through the User Interface. The UI forwards the image to the Encryption Module. The Encryption Module processes the image using the SM4 Algorithm and it will encrypt. The patient requests a decryption through the User Interface. The User Interface sends request to the Decryption Module. The Decryption Module retrieves the encrypted image. The decrypted image is reconstructed and sent back to the User Interface for the user to download or view.



VI. OUTCOME OF THE RESEARCH

This research is to develop an efficient and secure medical image encryption framework based on the SM4 algorithm. Encryption is applied using SM4 it is based on pixel based technique. Evaluating the proposed method's performance based on encryption speed, computational complexity, and resistance to cryptographic attacks. Proving that the encryption framework will maintain the original structure and quality of the medical image. Establishing the feasibility of adopting SM4-based encryption in healthcare systems for real- time and large-scale applications. Encryption ensures that sensitive patient data remains confidential, even if intercepted during transmission. Protection Against Cyberattacks robust encryption minimizes the risk of unauthorized access, ransomware attacks.

VII. RESULT AND DISCUSSION

In this project we have used SM4 algorithm technique for encrypting and decrypting of medical images and the texts of patients. It is a symmetric block cipher it encrypts the medical images as well as patient's information which is in text format. The admin manages the creation and distribution of keys to authorized persons to ensure secure access to the

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

medical information. The sensitive images cannot be accessed with Out decryption key. This method ensures the privacy and security of the patient's data. By using SM4 we can implement pixel form of encryption. The algorithm used preserves the integrity of image diagnostic quality after the decryption also. The algorithm uses a complex key scheduling process making it resistant from key- recovery attacks and brute force attacks. The padding approach is used like PKCS#7 ensures image data aligns with block size. Padding will be removed during Decryption. The SM4 algorithm if fast, securable, and it preserves the image quality efficiently compared to other encryption techniques. The key which is Created will be sent to the patient's device and admin. Whenever the admin who is the hospital staff tries to access the patient's data a notification will be sent to the patient's device. Whenever the admin wants to access the data he should contact the patient for the key. The users who are authorized can only view or download the data and medical images. By this the confidential data of the patients can be kept safe.

VIII. CONCLUSION

In conclusion, the proposed method of encrypting medical images using the SM4 algorithm provides a robust solution to address the growing concerns regarding the security and privacy of sensitive patient data in healthcare environments. With the increasing use of telemedicine, cloud storage, and Electronic Health Records (EHR), safeguarding medical images such as MRIs, CT scans, and X- rays is paramount. By utilizing the SM4 algorithm, this approach offers high security, efficiency. The patient and admin can only access the key .It Protects Patient confidentiality during remote consultations and prevents unauthorized access. The encryption technique ensures that medical images are rendered unintelligible without the corresponding decryption key, preventing unauthorized access while preserving the integrity and diagnostic value of the images after decryption. Additionally, the method is resilient to common cryptographic attacks, making it an ideal choice for protecting sensitive healthcare data. The experimental results have demonstrated that the proposed framework effectively balances security and performance, making it suitable for deployment in real- world healthcare applications.

REFERENCES

[1] Priyanka, Amit kumar Singh. "A survey of image encryption for healthcare applications", Evolutionary Intelligence (**2022)**, doi: 10.1007/s12065-021-00683-x

[2] Noor Sattar Noor et al. "A Fast Text- to-ImageEncryption-DecryptionAlgorithm for Secure network communication", computers,(2022),*11*(3),39;https://doi.org/10.3390/co mputers11030039

[3] Joshua C. Dagadu et al. " Medical Image Encryption Based on Hybrid ChaoticDNADiffusion".Wirelesspersona lcommunications (2019),springer nature volume 108

[4] Yucheng Chen et al. " Cryptanalysis and Improvement of medical image encryption using high speed scrambling and pixel adaptive diffusion" sciencedirect,(2020),volume167,https://doi.org/10.1016/j.sigpro.2019.107286

[5] Sankhanil Dey, Ranjan Ghosh. "A Review of Cryptographic Properties of 4- bit S-Boxes with Generation and Analysis of Crypto Secure" (2018), ebook ISBN: 9780429424878

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com