Survey on Securing MRI images by Stego-Crypto Lightweight Encryption

Ms. K. R. Nandhashree
Dept. of Cyber Security
SRM Valliammai Engineering College
Kattankulathur, India
nandhashree29@gmail.com

Dr. M. Senthil Kumar
Dept. of Cyber Security
SRM Valliammai Engineering College
Kattankulathur, India
msen1982@gmail.com

M. Abimanyu
Dept. of Cyber Security
SRM Valliammai Engineering College
Kattankulathur, India
abimanyu1452005@gmail.com

B. Hemachandran
Dept. of Cyber Security
SRM Valliammai Engineering College
Kattankulathur, India
chandru20048@gmail.com

K. Surya
Dept. of Cyber Security
SRM Valliammai Engineering College
Kattankulathur, India
soharsurya@gmail.com

 DOA:01.12.2025 / DOP: 10.12.2025 ISSN: 3048-619X
Volume 2 Issue 3 [Sep – Dec 2025] DOI:

***Abstract*—With the evolution of medical imaging technology, protecting privacy, integrity, and security of MRI images has become a significant problem. This work proposes a multi-layer security framework using steganography and triple layering cryptographical encryption (AES-256, ASCON, and ECC) for securing sensitive medical data. First, the system hides the MRI image into a cover image by using the Least Significant Bit (LSB) steganography. Next, three levels of encryption are applied to the stego picture. Users (doctors or patients) need to authenticate themselves using hospital provided credentials, followed by some verification process on the user side of the system to retrieve the image, after which, it restores the original MRI picture while maintaining its security using multi-layer decryptions. The system also provides a robust security approach in the healthcare data management that prevents the data from unauthorized access.**

Keywords— MRI Images, Steganography, Cryptographical Encryption, AES-128, ASCON, ECC, Stego Image

I. Introduction

We are using steganography and triple layer of encryption in this project for securing the medical images to keep the data encrypted to prevent the data from the attackers. The combination of various cryptographic methods to ensure the storage, transfer of data and retrieval of the data which are sensitive. This project uses a triple layer which consists of: AES-128 for robust security, ASCON for lightweight encryption and authentication, ECC for key management. These combined protocols together implemented to provide a layered security approach to secure the data along with consuming less computational power and it is suitable for the medical related IOT systems. Along with these techniques our system uses LSB steganography which hides our source data into normal cover images which provides further protection. This method helps to prevent the manipulation of our data during storage or in transit. After the successful encryption storage of data, it's the time to retrieve it back requires a decryption process. The system only provides decrypted data only to legitimate users who have the correct username and password because medical records are very sensitive data, we should only provide it with the authorized people and restrict the access to others. In order to get the decrypted data, the users have to enter a patient identification number and a one-time password (OTP) which provides additional authentication.

II. Literature Survey

According to the report, lightweight cryptography uses effective security approaches to optimize encryption for low-power devices. ECC's efficient scalar multiplication improves key exchange for secure communication. Steganography conceals encrypted data in images for undetectable transmission. Secure medical data storage ensures protection, authentication, and safe sharing of sensitive records.

A. Lightweight Cryptography

In limited resources scenarios like systems with embedded functionality, implanted medical devices, and Internet of Things devices, lightweight cryptography is essential for secure communication Conventional encryptions are computation heavy and involve heavy computations that can be impractical for low power or small-scale applications. Researchers have proposed optimum implementations of cryptographic algorithms that take into account the trade-off between security and speed-energy efficiency in order to guarantee that the authentication security satisfies the criteria [16]. One important area of development in lightweight cryptography is the hardware-based implementation of encryption protocols. Custom ASIC-based implementations optimize power consumption at the cost of a very high throughput for the encryption [1]. They are predicated on the necessity of using as little memory and logic gates as feasible because these will have very minimal overhead in terms of performance [1]. Particularly, efficient use of lightweight ciphers (such as ASCON) for authenticated encryption offers robust assurances at a minimal resource cost [4]. A further important aspect of lightweight cryptographic design is the optimization of the substitution boxes (S-Boxes) which are part of block ciphers such as AES [18]. Balanced encoding of data ensures identical energy costs when performing arithmetic operations, making assaults via the side channel (such as differential power analysis) much harder [5]. These approaches are especially useful for medical applications where power efficiency and security must complement each other with significance [13]. Additionally, low-area and low-power cryptography modules have been developed for smooth embedded processor integration [15]. The proposed modules use pipelined and parallel processing architectures to accelerate associated encryption with a little higher hardware footprint [11]. For example, threshold versions of

cryptographic algorithms preserve excellent computing efficiency and are more resilient to power analysis [18]. This is important in practical medical imaging and IoT-based healthcare systems where real time data encryption is needed [13]. Accelerators for hardware-based cryptography can also provide secure communication between low-power devices [15]. By removing encryption from general-purpose processors, these accelerators improve performance and lower energy use [15]. Lightweight cryptographic implementations provide reliable and efficient encryption by incorporating hardware-based security mechanisms through applications such as fast access to medical data, channel security of sensors used to communicate medical information, and monitoring of patients through near real- time processing systems [8].

B. Advanced ECC Implementation

Due to its excellent security and small key sizes, Elliptic Curve Cryptography (ECC) - a method used for digital signatures & secure key exchange [2]. Classic cryptographic techniques like RSA have larger key sizes for the same strength target and are therefore less efficient in resource-constrained use-cases [2]. Studies on speed improvement, latency reduction, and security enhancement have been conducted along with ECC implementations. High performance scalar multiplication is one of the most significant advancements in ECC implementation [11]. The primary operations in ECC are point addition and doubling which are used repeatedly in the scalar multiplication. ECC provides a functional choice for real time applications because of the advanced algorithms such as window based recoding and interleaved multiplication which reduces the time for calculation. We aim to increase the effectiveness of the cryptographic operations in low power devices which contains the resource constraints [15]. Another way to increase the efficiency of ECC based primers is hardware acceleration which means putting a cryptographic engine into silicon. By using the parallel processing methods and improving the efficiency of internal instruction set and architecture, these engines should execute the ECC operations with low latency [15]. The Scientists have integrated ECC modules into the FGPA and ASIC designs to reduce the processing time by making the communication which are suitable for IoT based medical devices [19]. Also, ECC based authentication techniques provides cryptographic procedures only requires low computational cost. ECC based key exchange protocols gives a robust secure channel for communication for the transmission of sensitive data such as the encrypted medical image data [2]. The researchers often use the “forward secrecy” which is a key management technique to ensure that previous communications were protected during the decryption even if the compromise of key occurs [3]. Finally, the cryptographic accelerators work by GPUs and Embedded processors improves the performance of ECC solutions. The encryption and decryption of data using the scalar multiplication technique by low latency window recoding methods increases the speed of the processes [12]. These advanced technologies are particularly required for the fields which requires high protection and robust security measures to protect the sensitive data such as medical imaging where access management and data transfer are crucial. *Steganography*

Steganography is a technique where we can hide the data into images which can be difficult to detect and extract the original data. It makes our data to hide its existence which acts like never been existed of our source content, but the traditional encryption techniques are making the data into an unreadable format. Various types of steganographic techniques are available to improve security of the data by different methods to make the detection of original data more complex [6]. The immune cover techniques were introduced to make the data hiding method more advanced and ensure robust security to prevent from statistical attacks [7]. Using the adaptive algorithms which adapts to the content of the image and only takes bigger entropy regions in the image space makes more difficult for the attackers to detect the existence of original data [10]. These immune systems give an increased security as well as keeping the high quality of the image. Another important approach of steganography involves the usage of the automatic cover image selection techniques [7]. The advanced cover image selection techniques choose the best cover images to reduce the detection of the original data rather than hiding our original data into some random images [14]. These methods are based on the use of generative models and deep learning methods to make steganography images which prevents from the forensic techniques to reveal the original data [14]. The main motive of the image steganography techniques to create secure embedding algorithms which removes the risk of noise, compression and tampering. Advanced methods such as volatility-based steganography uses small pixel variance intensities to add the cipher text data [10]. These techniques guarantee the integrity of data when images face alternate transformations like resizing or format changes. Models in this category sometimes even take advantage of (deep learning) based steganography to make the cover image blend more smoothly with the hidden information [14]. Neural networks that integrate concealed information undetected are used to create deceptive pictures [10]. Such techniques are particularly helpful in the security of medical images, in which, patient’s information can be embedded safely into the diagnostic images to be securely transmitted and stored.

C. Medical data storage & transmission

The necessity of keeping and distributing medical data securely new encryption and authentication methods are needed to safeguard medical records from the security risks presented by existing storage systems [8]. Data confidentiality, integrity, and availability are the focus of many cryptographic approaches proposed so far. One of these developments for protecting medical data is the use of memory encryption with lightweight ciphers [16]. Hostile software cannot access or change the confidential medical data stored in memory thanks to these encryption mechanisms. In addition to protecting sensitive data at extremely fast rates, these hardware-based encryption systems also safeguard medical records, even in the event that the device is hacked [13]. If you want to safeguard the confidentiality of medical data, secure authentication techniques are also essential. Rather, this security solution enables only authorized users to access encrypted medical data by combining several authentication techniques and key

exchange protocols [3]. Data security is further increased through secure key exchange protocols, including authenticated key agreements, which protect encryption keys from being intercepted [3].Adversarial attack detection on federated learning models is another crucial field of study that needs to develop. Federated Learning used by hospitals to build the AI models which enables the usage of Artificial Intelligence in the medical imaging without the exchange of raw patient data [8]. These models having the risk at malicious attacks that alters the training data so there is a chance to compromise the security. Scientists have developed more effective ways to prevent from the attacks and avoid the threats. Finally, safe communication protocols for medical image security ensures the confidentiality of the encrypted data [12]. The keys used for encryption secures the communication channels to ensure the encrypted data could not be intercepted or eavesdropped. The lightweight authentication protocol also has the ability to maintain integrity by using the authentication tags which provides advance security of data in being storage or in transit [4]. These advanced features protect the patient privacy and increases the security standards in the healthcare management in an effective way. This combination of approaches such as cryptographic techniques, steganography and authentication methods to protect the sensitive medical information in healthcare management increases the confidentiality, integrity and reliability of the data.

III. Discussion

Using Steganography, Elliptic Curve Cryptography(ECC) and lightweight cryptography such as ASCON in the health care management field, our project architecture enables a fast and reliable security approach that will must be employed to provide complete protection of crucial data. This requires a low processing performance as well as maintaining robust security measure which is suitable for the Internet of Things(IoT) based medical instruments. Elliptic Curve Cryptography improves communication security and ensures the confidentiality of data by using minimum computing resources and offers efficient key exchange. Moreover, Steganography gives an additional layer of protection, which reduces the data interception, and it is difficult to detect our original data. Data integrity and privacy are also maintained since private patient information and sensitive medical images are securely stored to avoid unauthorized access. By combining these tactics, a multi-layered defence against common cyberthreats including illicit access, data tampering, and eavesdropping is provided. All cryptographic algorithms are of lightweight design (enough for one usage of an implantable medical device and an Internet of Things (IoT) network), and this results in both secured and efficient part. It meets the high demands of the modern world and the emerging need of medical applications for better security of data, focusing on protecting sensitive health information in various stages of the data lifecycle (gathering, transferring, and storing) without sacrificing medical equipment' computational and energy efficiency.

IV. Conclusion

To put it simply, methods that use advanced key management, light cryptography, data embedding for security, and embedded storage all help to improve security implementations in modern settings. To attain a high level of security, Ascon uses a variety of techniques, including lightweight encryption and the S-Box modified AES. ECC offers a strong method for exchanging keys that enables reduced computing cost and safe communication. This is an additional security measure because the transported encrypted information is embedded in seemingly harmless cover images and so is difficult to detect and degrade. Also, implementation of secure authentication methods and encrypted storage also ensures that sensitive information, such as medical records and IoT data, can be kept safe from unauthorized access. These technologies work together to provide a robust security architecture that successfully strikes a balance between integrity, efficiency, and secrecy. Using these innovations, organizations can accelerate cybersecurity, protect sensitive data, and respond to new risks, particularly in medical, IoT and other high-risk use cases.

References

[1] K. -D. Nguyen, T. -K. Dang, B. Kieu-Do-Nguyen, D. -H. Le, C. -K. Pham and T. -T. Hoang, 'ASIC Implementation of ASCON Lightweight Cryptography for IoT Applications,' in IEEE Transactions on Circuits and Systems II: Express Briefs, Vol. 72, No. 1, pp. 278-282, 2025.

[2] J. Zhang et al., 'High-Performance Elliptic Curve Scalar Multiplication Architecture Based on Interleaved Mechanism,' in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 33, No. 3, pp. 757-770, March 2025.

[3] G. Yu, Q. Li, H. Mao, A. A. A. El-Latif and J. J. P. C. Rodrigues, 'A Multi-Scenario Authenticated Key Exchange Scheme With Forward Secrecy for Fog-Enabled VANETs,' in IEEE Transactions on Vehicular Technology, Vol. 74, No. 1, pp. 831-846, Jan. 2025.

[4] D. Xu, X. Wang, Q. Hao, J. Wang, S. Cui and B. Liu, 'A High-Performance Transparent Memory Data Encryption and Authentication Scheme Based on Ascon Cipher,' in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 32, No. 5, pp. 925-937, May 2024.

[5] S. Lee and J. -N. Kim, 'Balanced Encoding of Near-Zero Correlation for an AES Implementation,' in IEEE Transactions on Information Forensics and Security, Vol. 19, pp. 6589-6603, Dec. 2024.

[6] Y. Chen, H. Wang and W. Li, 'Constructing Immune-Cover for Improving Holistic Security of Spatial Adaptive Steganography,' in IEEE Transactions on Dependable and Secure Computing, Vol. 21, No. 6, pp. 5403-5419, Dec. 2024.

[7] J. Yu, J. Zhang, Z. Wang, F. Li and X. Zhang, 'Cover Selection in Encrypted Images,' in IEEE Transactions on Circuits and Systems for Video Technology, Vol. 34, No. 12, pp. 13626-13641, Dec. 2024.

[8] E. Darzi, F. Dubost, N. M. Sijtsema and P. M. A. van Ooijen, 'Exploring Adversarial Attacks in Federated Learning for Medical Imaging,' in IEEE Transactions on Industrial Informatics, Vol. 20, No. 12, pp. 13591-13599, Dec. 2024.

[9] Z. Yang, K. Chen, K. Zeng, W. Zhang and N. Yu, 'Provably Secure Robust Image Steganography,' in IEEE Transactions on Multimedia, Vol. 26, pp. 5040-5053, March 2024.

[10] J. Zhang, K. Chen, W. Li, W. Zhang and N. Yu, 'Steganography With Generated Images: Leveraging Volatility to Enhance Security,' in

IEEE Transactions on Dependable and Secure Computing, Vol. 21, No. 4, pp. 3994-4005, Aug. 2024.

[11] J. Zhang, Z. Chen, M. Ma, R. Jiang, H. Li and W. Wang, 'High-Performance ECC Scalar Multiplication Architecture Based on Comb Method and Low-Latency Window Recoding Algorithm,' in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 32, No. 2, pp. 382-395, Feb. 2024.

[12] J. Feng, Y. Wei, F. Zhang, E. Pasalic and Y. Zhou, 'Novel Optimized Implementations of Lightweight Cryptographic S-Boxes via SAT Solvers,' in IEEE Transactions on Circuits and Systems I: Regular Papers, Vol. 71, No. 1, pp. 334-347, Jan. 2024.

[13] A. Wu et al., 'Design and Construction of a Low-Cryogen, Lightweight, Head-Only 7T MRI Magnet,' in IEEE Transactions on Applied Superconductivity, Vol. 34, No. 5, pp. 1-5, Aug. 2024.

[14] K. Chen, H. Zhou, Y. Wang, M. Li, W. Zhang and N. Yu, 'Cover Reproducible Steganography via Deep Generative Models,' in IEEE Transactions on Dependable and Secure Computing, Vol. 20, No. 5, pp. 3787-3798, Oct. 2023.

[15] J. Dong, P. Zhang, K. Sun, F. Xiao, F. Zheng and J. Lin, 'EG-FourQ: An Embedded GPU-Based Efficient ECC Cryptography Accelerator for Edge Computing,' in IEEE Transactions on Industrial Informatics, Vol. 19, No. 6, pp. 7291-7300, June 2023.

[16] P. Rosa, A. Souto and J. Cecílio, 'Light-SAE: A Lightweight Authentication Protocol for Large-Scale IoT Environments Made With Constrained Devices,' in IEEE Transactions on Network and Service Management, Vol. 20, No. 3, pp. 2428-2441, Sept. 2023.

[17] J. Cui et al., 'Lightweight Encryption and Authentication for Controller Area Network of Autonomous Vehicles,' in IEEE Transactions on Vehicular Technology, Vol. 72, No. 11, pp. 14756-14770, Nov. 2023.

[18] J. Song, K. Lee and J. Park, 'Low Area and Low Power Threshold Implementation Design Technique for AES S-Box,' in IEEE Transactions on Circuits and Systems II: Express Briefs, Vol. 70, No. 3, pp. 1169-1173, March 2023.

[19] M. Zeghid, H. Y. Ahmed, A. Chehri and A. Sghaier, 'Speed/Area-Efficient ECC Processor Implementation Over GF(2m) on FPGA via Novel Algorithm-Architecture Co-Design,' in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 31, No. 8, pp. 1192-1203, Aug. 2023.

[20] X. Li et al., 'LIGHT: Lightweight Authentication for Intra Embedded Integrated Electronic Systems,' in IEEE Transactions on Dependable and Secure Computing, Vol. 20, No. 2, pp. 1088-1103, April 2023.