Secure Medical Image Encryption and Decryption using AES algorithm

[1]Mrs. T T Mathangi, [2]J S Prathusha Devi, [3]S Pooja, [4]P Loganayagi

[1]Assistant Professor, [2,3,4] UG Students
Information Technology,
K.L.N. College of Engineering, Pottapalayam, India

***Abstract*— Encryption of medical images is an effective way to prevent medical images from threats. Image encryption is a procedure that converts a plain image to an encrypted image by employing a secret key. The decryption process decrypts the cipher image into the original image by employing the secret key. In this proposed system medical image encryption and decryption are done by using the AES algorithm. The overall structure of AES focuses particularly on the four steps used in each round of AES - byte substitution, shift rows, mix columns, and add round keys. Since the image is encrypted using AES, it is more secure than the DES and triple DES as the key size is 192 bits, which makes the encryption and decryption more secure.**

***Key Words*— Advanced Encryption Standard (AES), Encryption, Decryption, Encoding, Decoding.**

I. INTRODUCTION

The image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. Image encryption, video encryption, chaos-based encryption has applications in many fields including the internet communication, transmission, medical imaging, Tele-medicine and military Communication, etc. The evolution of encryption is moving towards a future of endless possibilities. The image data have special properties such as bulk capability, high redundancy and high correlation among the pixels. Encryption is the process by which a readable message is converted to an unreadable form to prevent unauthorized parties from reading it. Decryption is the process of converting an encrypted message back to its original (readable) format. The original message is called the plaintext message. Encryption techniques are very useful tools to protect secret information. Encryption will be defined as the conversion of plain message into a form called a cipher images that cannot be read by any people without decrypting the encrypted images. Decryption is the reverse process of encryption which is the process of converting the encrypted images into its original plain images, so that it can be read. Encryption of data has become an important way to protect data resources especially on the internet, intranets and extranets. Encryption is the process of applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code. The main goal of security management is to provide authentication of users, integrity, accuracy and safety of data resources. Many encryption methods have been proposed in literature, and the most common way to protect large multimedia files is by using conventional encryption techniques.

Images are a significant source of information. Images have various applications in a variety of fields such as storing patient medical information, capturing aerial images by satellite imagery, capturing interplanetary motion images by telescopes, storing an individual's identity in the form of fingerprints, or iris images, etc. Cryptography is an efficient way to safeguard sensitive information. Cryptography is a method of storing and transmitting data in a form intended for reading and processing the information. Cryptographic Algorithm uses a set of keys with the different characters for both encryption and decryption. By using key the plain text is converted to the cipher text and decryption is done by converting back the plaintext from the cipher text. Cryptography is a process of transmitting and storing data in a form that it is read only by authorised users. Cryptography is a science of protection of data by encoding it into unreadable form. Data Confidentiality, Data Integrity, Authentication and Non-repudiation these are four principles of cryptography. It is useful way of protecting the important sensitive information by using mathematical form algorithm for both encryption and decryption process. The encryption and decryption process depend on the key value. The strength of the algorithm is how difficult it is to determine the key value and get the original text. The algorithm is majorly divided into two types symmetric and asymmetric depending on the keys. If same keys are used for both encrypting and decrypting then it is called symmetric algorithm. Symmetric algorithm is further divided into stream and block ciphers. A stream cipher is done on the single byte of data, whereas the block a cipher is done on the block of data. Asymmetric algorithm uses two different keys one for encryption and both for decryption. The key should be kept secret so that the message should be not be decrypted. The purpose of cryptography is to provide Authentication (proving the one's identity), Non-repudiation (the receiver should know the sender should not be faking), Integrity (data should be correct, accuracy, and trustworthiness), and Privacy/confidentiality (message is read by only the intended receiver).

The advancement of encryption and decryption leads to an infinite future. As a result, the safety of image data from unauthorized access is crucial at the hands of user. Image encryption plays a significant role in the field of information hiding.

The encryption task involves distorting the pixel intensity of the image input to create a cipher image that is completely different from the image input. Using the secret keys, the receiver decrypts the images and returns the original image. There are various private keys used by the sender and receiver in asymmetric key cryptography which are further used to generate the shared secret key. On the other hand, symmetric-key cryptography involves encryption and decryption with a single key that the sender and receiver are

secretly known to have. Most common processes involve symmetric approaches such as AES cipher, etc. to protect the information stored in the images.

II. RELATED WORKS

1. S.S. Bhuyan, U. Y. Kabir, J. M. Escareno, K. Ector, S. Palakodeti, D. K. Wyant, S. Kumar, M. Levy, S. Kedia, D. Dasgupta, and A. Dobalian, "Transforming healthcare cybersecurity from reactive to proactive: Cur- rent status and future recommendations," J. Medical Syst., vol. 44, no. 5, p. 98, 2020.

The recent rise in cybersecurity breaches in healthcare organizations has put patients' privacy at a higher risk of being exposed. Despite this threat and the additional danger posed by such incidents to patients' safety, as well as operational and financial threats to healthcare organizations, very few studies have systematically examined the cybersecurity threats in healthcare. To lay a firm foundation for healthcare organizations and policymakers in better understanding the complexity of the issue of cybersecurity, this study explores the major type of cybersecurity threats for healthcare organizations and explains the roles of the four major players (cyber attackers, cyber defenders, developers, and end-users) in cybersecurity. Finally, the paper discusses a set of recommendations for the policymakers and healthcare organizations to strengthen cybersecurity in their organization.

2. L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," Maturitas, vol. 113, pp. 48–52, 2018.

Electronic healthcare technology is prevalent around the world and creates huge potential to improve clinical outcomes and transform care delivery. However, there are increasing concerns relating to the security of healthcare data and devices. Increased connectivity to existing computer networks has exposed medical devices to new cybersecurity vulnerabilities. Healthcare is an attractive target for cybercrime for two fundamental reasons: it is a rich source of valuable data and its defences are weak. Cybersecurity breaches include stealing health information and ransomware attacks on hospitals, and could include attacks on implanted medical devices. Breaches can reduce patient trust, cripple health systems and threaten human life. Ultimately, cybersecurity is critical to patient safety, yet has historically been lax. New legislation and regulations are in place to facilitate change. This requires cybersecurity to become an integral part of patient safety. Changes are required to human behaviour, technology and processes as part of a holistic solution.

3. M. Alawida, J. S. Teh, A. Samsudin, and W. H. Alshoura, "An image encryption scheme based on hybridizing digital chaos and finite state machine," Signal Process., vol. 164, pp. 249–266, 2019.

Image encryption protects visual information by transforming images into an incomprehensible form. Chaotic systems are used to design image ciphers due to properties such as ergodicity and initial condition sensitivity. A chaos-based cipher derives its security strength from its underlying digital chaotic map, thus a more complex map leads to higher security. This paper introduces an enhancement to a tent map's chaotic properties by hybridizing it with a deterministic finite state machine. We denote the resulting digital one-dimensional chaotic system as TM-DFSM. Chaotic analyses indicate that the new chaotic system has higher nonlinearity, sensitivity to initial condition, and larger chaotic parameter range than other recently proposed one-dimensional chaotic systems. We then propose a new image encryption scheme based on TM-DFSM, capable of performing both confusion and diffusion operations in one pass while also having a flexible key space. The encryption operations are designed to achieve maximal confusion and diffusion properties. Changing a single bit of the plainimage or secret key will result in an entirely different cipherimage. The proposed cipher has been analyzed using histogram analysis, contrast analysis, local Shannon entropy, resistance against differential cryptanalysis, and key security. Performance comparison with other recent schemes also depicts the proposed cipher's superiority.

4. A. Abusukhon, Z. Mohammad, and A. Al-Thaher, "An authenticated, secure, and mutable multiple-session-keys protocol based on elliptic curve cryptography and text-to-image encryption algorithm," Concurr. Comput. Pract. Exp., vol. 34, no. 4, 2022

Most of the key agreement protocols (e.g., Menezes–Qu–Vanstone [MQV] family) generate one common key per session. This leaves the session key vulnerable against various attacks. This article proposed an enhanced multiple session key (EMSK) protocol which is based on the elliptic curve Diffie–Hellman (ECDH), HMQV, and the YAK protocols. The EMSK generates multiple session keys per session. Unlike the MQV protocol, the EMSK needs only two messages to be exchanged in order to create nine session keys. However, the MQV requires 18 messages to be exchanged in order to produce these nine session keys. In EMSK, one of the session keys is used to encrypt the plaintext using the one-time pad cipher. The encrypted message is then embedded in an RGB-image in order to provide confidentiality service of communication. The EMSK is evaluated theoretically against various types of attacks and practically using the Scyther simulator. The results from the simulator showed that the EMSK protocol withstand various types of attacks on the MQV, HMQV, and the YAK protocols, and provided perfect forward secrecy. In addition, the EMSK provides a digital signature feature which validates the authenticity and integrity of a digital message using the zero knowledge prove.

III. PROBLEM STATEMENT

Sending medical images over the network requires a strong encryption algorithm such that it is resistant against cryptographic attacks. Therefore, we have proposed this System, Secure medical Image Encryption and decryption using AES algorithm.

IV. METHODOLOGY

In the proposed system, secure medical image encryption and decryption are performed by using the AES algorithm. The AES algorithm is widely used in applications in daily life, such as smart cards, cell phones, automated teller machines, and WWW servers. AES encrypts the original image to a cipher image, which can be decrypted to the original image using a common private key. The cipher image is in a different form, so it has no idea of the original image. For image encryption and decryption, the AES encrypts the image in a different form using the key, which has no idea of the original form. After decrypting it, it will be in its original form. In the implementation, the sender can choose the image and request a key from admin. An admin can view the requested list to generate a key. Then the key is generated and sent to the sender. The sender gets a key and encrypts the entire image. The receiver can view the encrypted image for decryption. And get a key for the image, and the multiple encrypted medical images will be decrypted once at a time. Both encrypted and decrypted multiple medical images are stored.

V. IMPLEMENTATION

AES Algorithm

AES performs operations on bytes of data instead of performing operations in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time. The number of rounds depends on the key length. 128 bit key is used for 10 rounds, 192 bit key is used for 12 rounds and 256 bit key is used for 14 rounds.

Creation of Round keys :

All round keys are generated from the key using the Key Schedule algorithm. Hence, several different round keys that will be used in the corresponding round of the encryption are created using the original key.

Encryption

AES considers each block as a 16 byte (4 byte x 4 byte = 128) grid in a column. Each round consists of 4 steps such as, Substitute Bytes, Shift Rows, Mix Columns and Add Round Key.

Substitute Bytes : This stage puts the substitution into action. Each byte is replaced with another byte in this phase. The S-box, another name for the lookup table used, is employed. A byte is never replaced by itself or by a byte that is a complement of the current byte because of the manner this substitution is carried out. This process yields the same 16-byte (4 x 4) matrix.

Shift rows: This step is just as it sounds. Each row is shifted a particular number of times.

Mix columns: This step essentially involves multiplying matrices. Each column is multiplied by a particular matrix, which changes the order of each byte in the column.The final round omits this stage.

Add Round Keys: The output from the previous stage is now XORed with the appropriate round key. In this case, the 16 bytes are simply regarded as 128 bits of data and not as a grid.

Decryption

The steps in the rounds are simple to reverse because they each contain an opposite that, when used, undoes the modifications. Depending on the key size, each of the 128 blocks is processed via 10, 12, or 14 rounds.Each round of decryption consists of, Add round key, Inverse Mix Columns, Shift Rows and Inverse Substitute Byte.

Inverse MixColumns : This step is similar to the encryption's MixColumns step, but it uses a different matrix to carry out the operation.

Inverse SubBytes : During decryption, bytes are substituted using the Inverse S-box as a lookup table.

Encoding and Decoding

Image encoding is necessary as a means of compressing an image in order to reduce it's bandwidth and be able to transmit it. Image decoding is the process of converting the encoded image back to a uncompressed bitmap which can then be rendered on the screen. This involves the exact reverse of the steps involved in encoding the image.

Key Generator

Key generation is the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted. A device or program used to generate keys is called a key generator.

FIGURES

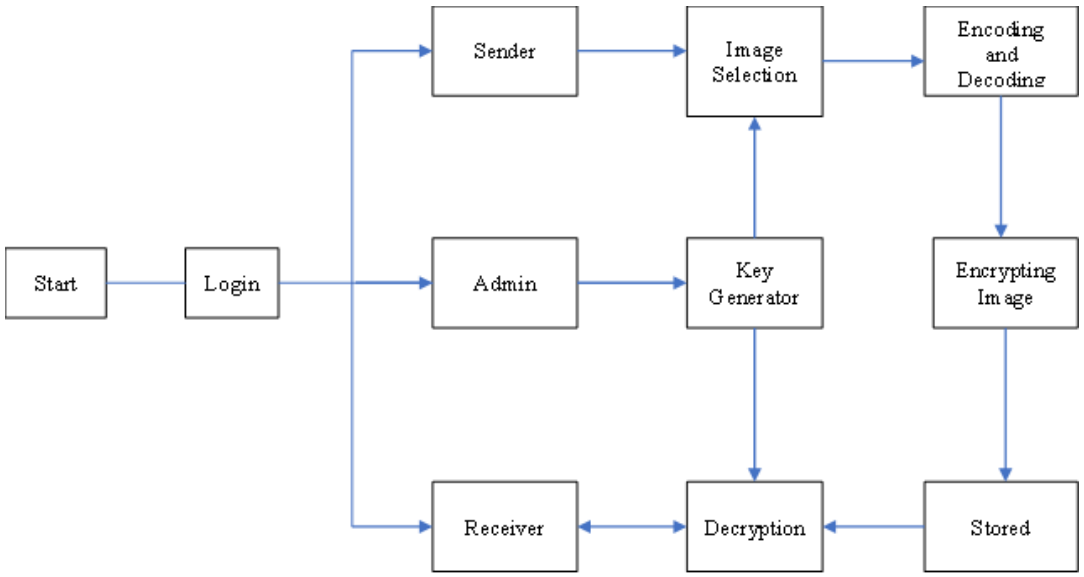

Fig. 1 System Architecture

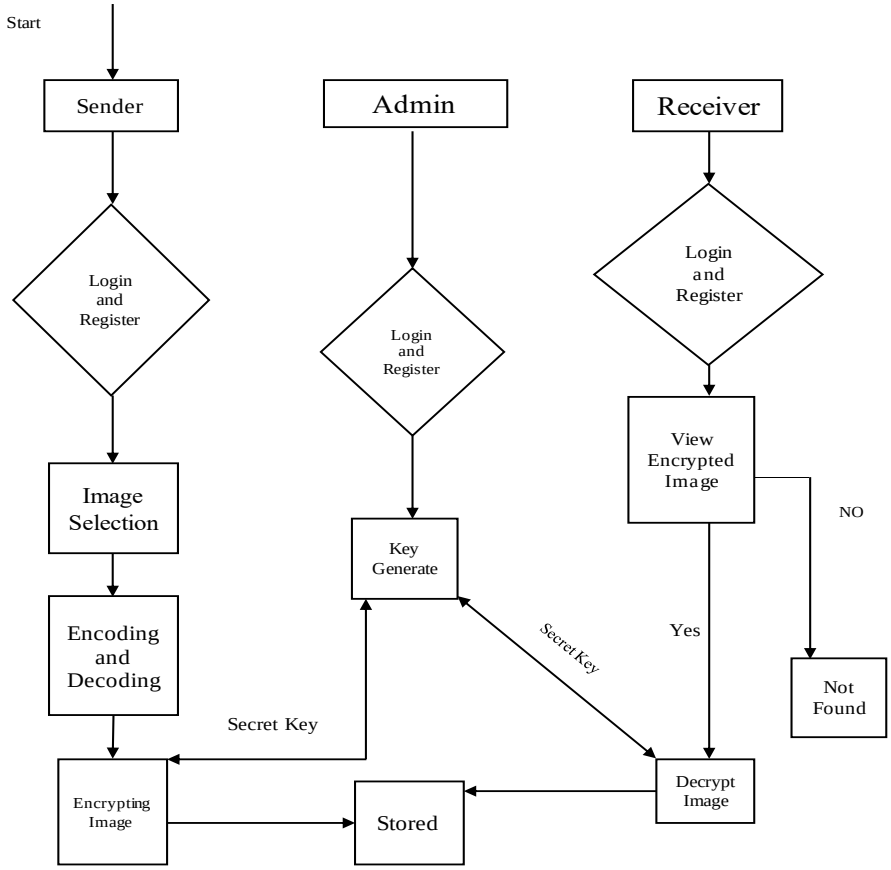

Fig. 2 Flow Diagram

VI. Result And Conclusion

To ensure the security of medical images, this paper proposes a solution for secure healthcare. Since the image is encrypted using AES, it is more secure than the DES and triple DES as the key size is 192 bits, which makes the encryption and decryption more secure. This system protects the medical images from illegal copying and distribution. Thus the proposed system improves the cyber security of the medical images against various attacks when transmitting data in wireless medium.

VII. Future enhancement

In our proposed system we have secured the medical images alone using AES algorithm. In future we will encrypt and decrypt all the medical data also and guarantee confidentiality, integrity and availability of the medical data.

REFERENCES:

[1] S.S. Bhuyan, U. Y. Kabir, J. M. Escareno, K. Ector, S. Palakodeti, D. K. Wyant, S. Kumar, M. Levy, S. Kedia, D. Dasgupta, and A. Dobalian, "Transforming healthcare cybersecurity from reactive to proactive: Cur- rent status and future recommendations," J. Medical Syst., vol. 44, no. 5, p. 98, 2020.
[2] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," Maturitas, vol. 113, pp. 48–52, 2018.
[3] M. Alawida, J. S. Teh, A. Samsudin, and W. H. Alshoura, "An image encryption scheme based on hybridizing digital chaos and finite state machine," Signal Process., vol. 164, pp. 249–266, 2019.
[4] A. Abusukhon, Z. Mohammad, and A. Al-Thaher, "An authenticated, secure, and mutable multiple-session-keys protocol based on elliptic curve cryptography and text-to-image encryption algorithm," Concurr. Comput. Pract. Exp., vol. 34, no. 4, 2022.
[5] A. Daoui, H. Karmouni, O. E. Ogri, M. Sayyouri, and H. Qjidaa, "Robust image encryption and zero-watermarking scheme using SCA and modified logistic map," Expert Syst. Appl., vol. 190, p. 116193, 2022.
[6] Z. Gu, H. Li, S. Khan, L. Deng, X. Du, M. Guizani, and Z. Tian, "IEPSBP: A cost-efficient image encryption algorithm based on parallel chaotic system for green iot," IEEE Trans. Green Commun. Netw., vol. 6, no. 1, pp. 89–106, 2022.
[7] A. Rajhans, A. Bhave, I. Ruchkin, B. H. Krogh, D. Garlan, A. Platzer, and B. R. Schmerl, "Supporting heterogeneity in cyber-physical systems architectures," IEEE Trans. Autom. Control., vol. 59, no. 12, pp. 3178– 3193, 2014.
[8] S. R. Kessler, S. Pindek, G. Kleinman, S. Andel, and P. E. Spector, "Information security climate and the assessment of information security risk among healthcare employees," Health Informatics J., vol. 26, no. 1, 2020.
[9] A. G. Sreedevi, T. N. Harshitha, V. Sugumaran, and P. Shankar, "Application of cognitive computing in healthcare, cybersecurity, big data and iot: A literature review," Inf. Process. Manag., vol. 59, no. 2, p. 102888, 2022.
[10] G. N. Nguyen, N. H. L. Viet, M. Elhoseny, K. Shankar, B. B. Gupta, and A. A. A. El-Latif, "Secure blockchain enabled cyber-physical systems in healthcare using deep belief network with resnet model," J. Parallel Distributed Comput., vol. 153, pp. 150–160, 2021.