Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

EXPLORING A NOVEL STRATEGY FOR ENSURING THE SECURITY OF MEDICAL IMAGES THROUGH ENCRYPTION AND QR ENCODING

J.Rajya Lakshmi, Assistant Professor, Department of Electronics and Communication Engineering, Potti SriRamulu Chalavadi Mallikarjuna Rao College of Engineering and Technology Kothapet, Vijayawada, Krishna District, Andhra Pradesh, India.
P.T.V.S.N.Satyavathi, A.J.R.Sai Vignesh, A.Kumar, D.Anil Kumar Reddy, Y.L.Haneesha, Students, Department of Electronics and Communication Engineering, Potti SriRamulu Chalavadi Mallikarjuna Rao College of Engineering and Technology, Kothapet, Vijayawada, Krishna District, Andhra Pradesh, India.

ABSTRACT

In telemedicine applications, data security is critical for success. Encryption and steganography techniques are employed to maintain the confidentiality and integrity of medical images. QR codes, which can encode more information than traditional barcodes, are used as an additional security layer. The RSA encryption algorithm is used to encrypt medical images, which are then embedded into a cover image to create a stego image. The stego image is then encoded using QR encoding to enhance the system's resilience to malicious attacks. The original medical image can be retrieved by reversing the process, which involves decoding the QR code, obtaining the cipher image, and decrypting it using RSA. The entire process is implemented using the Python programming language.

Keywords—Steganography, Quick Response Code, RSA Encryption and Decryption.

I. INTRODUCTION

Medical imaging has become an essential tool for healthcare professionals, researchers, and remote collaborations. However, transmitting medical images over insecure communication mediums, such as in tele-health applications, raises concerns about the confidentiality and integrity of these images. A breach of confidentiality or integrity could lead to inaccurate diagnoses, which highlights the criticality of securing medical images. Various techniques are used for medical image security, including cryptography, steganography, and watermarking. Our research project aims to bridge communication gaps for individuals with disabilities such as blindness, deafness, and muteness through the development of wearable technology.

Cryptography, which involves secret writing, converts a message from a sensible form (plain text) into an insensible form (cipher text) for secure transmission. Encryption ensures confidentiality and integrity using symmetric or asymmetric approaches. In symmetric encryption, a shared key is used between the sender and receiver, while asymmetric encryption involves a public key known to everyone and a private key only known to the receiver. Steganography, on the other hand, involves embedding secret information into a cover object, such as text, video, image, or audio. Combining cryptography and steganography can create a more secure system. QR codes, which are machine-readable optical labels, can also be used to securely transmit medical images.

In the healthcare sector, there are established standards like the digital imaging and communications in medicine (DICOM) that provide a framework and mechanisms for achieving confidentiality, authentication, and integrity in the transmission of medical images. These standards are designed to ensure that medical images are transmitted securely, offering an additional layer of protection against any unauthorized access or tampering. By following these standards, healthcare professionals can be

confident that patient information is kept confidential and secure during the transmission of medical images.

QR code is a modern term that stands for Quick Response code, and it has become a popular trademark for various business and general purposes. Originally, QR code was designed for the automotive industry in Japan as a type of two-dimensional matrix. It is capable of recording information about an item in the form of a machine-readable label that can be attached to the item. QR code supports four standardized modes of data, including alphanumeric, byte or binary, numeric, and image, which can be used to store or encode information in the QR code.

II. LITERATURE SURVEY

Kalaichelvi et al. have implemented a security system that utilizes CAPTCHA codes to authenticate the intended receiver and prevent unauthorized access by machines. The system generates a randomized CAPTCHA code to establish a secure connection with the authenticated user, and then utilizes Image Steganography for confidentiality. The original message is transmitted via the LSB algorithm, which uses the RGB color spectrum to conceal the image data, providing an additional layer of encryption [1].

Pachiappan et al. proposed Visual cryptographic technique, sharing of images is limited with two shares. Visual secret sharing scheme is used to embed the information. The embedded image constructs the two shared images and have more secured than traditional visual cryptography [2].

Jiang et al. proposed a novel approach for securing medical images that combines the RSA algorithm, logistic chaotic encryption algorithm, and steganography technique. This approach employs a two-step encryption process where a medical image is first encrypted using a chaotic sequence generated by a logistic map. Next, the initial value of the chaotic sequence is encrypted using the RSA algorithm to ensure secure transmission of the image data. The decryption process involves legitimate users obtaining the necessary parameter information to decrypt the image data and obtain the original medical image. This approach provides enhanced security measures to prevent unauthorized access to sensitive medical information [3].

Soualmi et al. introduced a new technique for blind medical image watermarking, which involves two main processes: embedding the watermark data in the DWT- Schur coefficients and then extracting the watermark using the same steps as the embedding process. This technique allows the watermark to be extracted without the original or watermarked image, ensuring better privacy and security of the medical information. The method was evaluated experimentally and proved to maintain goodrobustness while preserving high image quality [4].

Maurya et al. introduces an innovative Extended Visual Cryptography Technique (EVCT) to secure medical images, where the image is first encrypted and then embedded into three cover images. On the receiver side, the secret image is reconstructed by combining the three shares (meaningful) and subsequently decrypting the image. The encryption and embedding techniques used in this process are lossless and low in complexity, making the approach more efficient [5].

Ali Al-Haj et al. proposed a region-based crypto- watermarking algorithm that can ensure authenticity by embedding robust watermarks in non-interest regions of the image using the Singular Value Decomposition (SVD) in the Discrete Wavelet Transform (DWT) domain. The algorithm offers two levels of integrity protection, one by using a cryptographic hash watermark and the other by employing an encryption-based tamper localization scheme. The algorithm also provides confidentiality by hiding sensitive patient data within the image. This approach offers enhanced security measures to safeguard medical images against unauthorized access and tampering[6].

Srivastava et al. introduced a technique that involves encrypting the confidential section of an

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

image by embedding it in non-salient pixel locations within the same image, ensuring secure image transfer. To achieve the encryption and subsequent recovery, a seeded one-time pad is utilized [7].

In this system a Microcontroller, Raspberry Pi is used and found that model has a web interface which helps the user to operate from his location remotely by using the functionality needed to operate the system [8].

Salameh et al. proposed a secure system for managing medical images and patient information using a sharing approach. The system generates two shares: the first share represents the encrypted medical image using MJEA, while the second share contains all the patient's information embedded in the medical image and encrypted using MJEA. To further enhance security, the two shares are mixed together using a scrambling algorithm before transmission. This approach ensures the confidentiality of both the medical image and patient's information during transmission and storage [9].

Abd El-Latif et al. have introduced an algorithm that employs gray code and a chaotic map to encrypt quantum images. The quantum gray code is used to scramble the image, and then the image is encrypted using a quantum XOR operation with a key generated by the logistic-sine map. This approach ensures a robust and efficient encryption process for quantum images and outperforms the classical encryption methods [10].

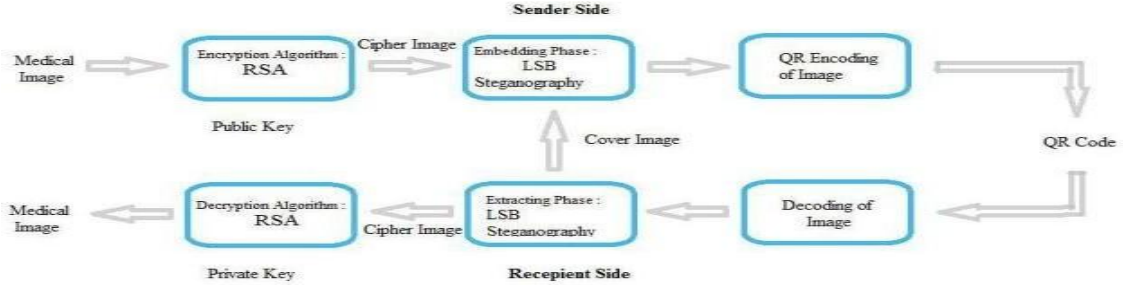
III. THE PROPOSED METHODOLOGY

The protection of medical images is essential in the healthcare industry to maintain confidentiality and integrity, especially when transmitting images through insecure communication channels like telehealth applications. The proposed system aims to provide a secure and reliable solution by utilizing encryption techniques and steganography. While the current system uses one-time padding and steganography techniques, it has limitations that make it unsuitable for modern applications. Therefore, the proposed system employs the RSA encryption algorithm to overcome these limitations.

The RSA encryption algorithm is used to encrypt the medical image in the first step, generating a cipher text. This cipher text is then embedded into a cover image using LSB steganography, where the least significant bits (LSB) of the cover image is replaced with the most significant bits (MSB) of the input image. This process creates a Stego Image, which is then encoded to generate a QR code. The use of QR codes makes the system more user- friendly and accessible to healthcare professionals who require access to medical images.The proposed system provides a comprehensive solution to ensure the confidentiality and integrity of medical images by utilizing advanced encryption techniques and steganography. The system employs the RSA encryption algorithm, which addresses the limitations of the one-time pad method, making it more practical and effective. Additionally, the use of steganography ensures that the image data is secure and inaccessible to unauthorized individuals.

BLOCK DIAGRAM

Fig.1 : Combination of Encryption, Steganography and QR Encoding



Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

Overall, the proposed system offers a robust and reliable solution to protect medical images, which is critical in the healthcare industry. The system's use of advanced encryption techniques and steganography ensures that the images remain confidential and secure, while the QR code makes the system more user-friendly and accessible to healthcare professionals who require access to the images.

IV. OBSERVATION AND RESULTS

The use of encryption and QR encoding to secure medical images is a highly promising technique that can greatly enhance the privacy and security of sensitive patient data. The RSA encryption algorithm plays a crucial role in safeguarding medical images against unauthorized access and tampering during both storage and transmission. Additionally, the use of LSB steganography helps to conceal the encrypted image within a cover image, adding an extra layer of protection and making it difficult to detect by any unauthorized party. Furthermore, encoding the Stego Image into a QR code enhances its security since QR codes are widely used and can be easily scanned using mobile devices. This approach has proven to be reliable and efficient in encrypting and encoding medical images using QR codes. The decryption process is secure, requiring the use of a private key to retrieve the original medical image, ensuring that only authorized personnel can access the sensitive medical data. Overall, this approach offers a practical and feasible solution for protecting sensitive medical data during both storage and transmission. It has the potential to be utilized in various medical applications, including telemedicine, electronic medical records, and remote diagnosis.

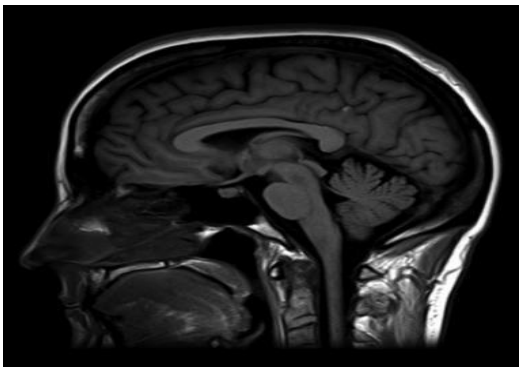


Fig.2 : Input Image

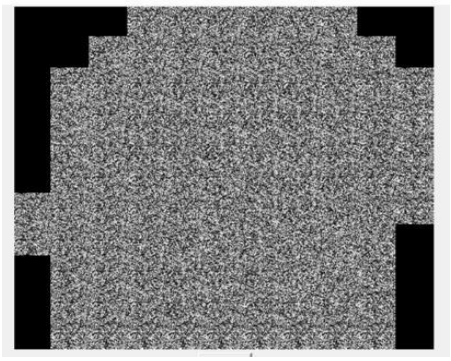


Fig.3 : Cipher Image

V. CONCLUSION

In conclusion, the approach of securing medical images using encryption and QR encoding is a promising technique that can provide robust security measures for sensitive medical data. The use of RSA encryption and LSB steganography ensures that medical images are protected from unauthorized access and tampering during storage and transmission.

The process of embedding the cipher image into a cover image and encoding it into a QR code is reliable, efficient, and provides an additional layer of security to the encrypted image. The use of a private key to decrypt the cipher image and retrieve the original medical image guarantees that only authorized personnel can access the medical data. Future research can explore ways to enhance the efficiency and reliability of the encryption and encoding processes. Additionally, further investigations can be done to evaluate the approach's scalability, compatibility, and ease of implementation in different healthcare systems. Furthermore, this approach can be extended to other medical applications, such as securing medical records and protecting patient information. The use of

encryption and QR encoding can provide a practical solution for maintaining privacy and security in healthcare, enabling telemedicine, remote diagnosis, and other digital healthcare services to thrive.

Fig.4 : Stego Image

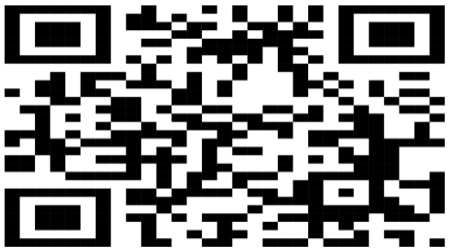


Fig.5 : Encoded Medical Image

Overall, the approach of securing medical images using encryption and QR encoding has significant potential to revolutionize healthcare practices, protect sensitive medical data, and improve patient outcomes.

REFERENCES

[1] Kalaichelvi, T., and P. Apuroop. "ImageSteganography Method to Achieve Confidentiality Using CAPTCHA for Authentication." In 2020 5th International Conference on Communication and Electronics Systems (ICCES), pp. 495-499. IEEE,2020.

[2]] Pachiappan, Kalaivani, S. Annaji, and N. I. T. H.Y. A. Jayakumar. "Security in medical images using enhanced visual secret sharing scheme." Int j sci eng technol res 3, no. 9 (2014): 1642-1645.

[3] Jiang, Tao, Kai Zhang, and Jinshan Tang. "Securing medical images for mobile health systems using a combined approach of encryption and steganography." In International Conference on Intelligent Computing, pp. 532-543. Springer, Cham,2018.

[4] Soualmi, Abdallah, Adel Alti, and Lamri Laouamer. "A blind image watermarking method for personal medical data security." In 2019 International Conference on Networking and Advanced Systems (ICNAS), pp. 1-5. IEEE, 2019.

[5] Maurya, Richa, Ashwani Kumar Kannojiya, and B. Rajitha. "An Extended Visual Cryptography Technique for Medical Image Security." In 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 415- 421. IEEE, 2020.

[6] Al-Haj, Ali, Ahmad Mohammad, and Alaa Amer. "Crypto-watermarking of transmitted medical images." Journal of digital imaging 30, no. 1 (2017): 26-38.

[7] Srivastava, Anushka, Shobhit Kumar Awasthi, Saqib Javed, Shubham Gautam, Naman Kishore, and Rajitha Bakthula. "Seeded one time pad for security of medical images in health information." In 2018 4th International Conference on Computing Communication and Automation (ICCCA), pp. 1-6. IEEE, 2018.

[8] Han, Baoru, Yuanyuan Jia, Guo Huang, and Lisha Cai. "A Medical Image Encryption Algorithm Based on Hermite Chaotic Neural Network." In 2020 IEEE 4th 22 Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), vol. 1, pp. 2644-2648. IEEE, 2020.

[9] Salameh, Jamal N. Bani. "A new approach for securing medical images and Patient's information by using hybrid system."Int J of Computer Sci Netw Secur 19, no. 4(2019): 28-39.

[10] Abd El-Latif, Ahmed A., Bassem Abd-El-Atty, and Muhammad Talha. "Robust encryption of quantum medical images." IEEE Access 6 (2017): 1073-1081.