Safeguarding Medical Images Utilizing Biometric-Inspired Robust Security

Ms. Bhavani[1a], Atchaya[2b], Aishwarya[2c], Akshaya[2d], Abinaya[2e], Krishnapriya[2f]
[1] Assistant Professor-Department of Information Technology, Panimalar Engineering College
[2]Second year students-Department of Information Technology, Panimalar Engineering College

Abstract
Protecting sensitive and personal records has gotten challenging as more and more digital data is maintained and shared between users. Privacy is crucial when it comes to clinical data, which contains sensitive patient data. This paper suggests a novel AES-based Base64 encoding method for biometrically driven medical encryption. The suggested solution uses the patient's biometrics to construct a key management system. After that, the medical image is AES-encrypted and ready for safe transmission or storage. The original medical image is then recreated using a reliable decryption approach using the encrypted image.

Keywords: Biometric, Steganography, Image files, AES key, Biometric watermark, Least significant bit(LSB)medical imaging.

1. INTRODUCTION

As more digital data is stored and transmitted between users, maintaining the security of sensitive and secret data has become a challenging problem. Security is undoubtedly critical if there is therapeutic information present that contains important patient data. Medical pictures may be vulnerable to major dangers such as unauthorized alteration, data leakage, and data integrity. The biggest issue emerges when these photos are stored and sent for numerous purposes. The secrecy of medical photographs is a critical problem that must be addressed. To safeguard medical photos, many approaches like as encryption, hashing, steganography, and watermarking have been developed. Of these, encryption is the best approach for ensuring the data's integrity. Due to two intrinsic characteristics of medical images—strong correlation between nearby pixels and redundancy-traditional encryption techniques, such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES), are not suitable for the encryption of medical images.

2. PURPOSE

A very efficient and resilient encryption mechanism is proposed in the suggested system to safeguard medical pictures. The patient goes to the lab for testing and is scheduled for a medical scan. The patient's fingerprint biometrics will be used to encrypt the medical images that were taken in the lab. First, the photos are transformed to bytes using Base64 encoding. The medical picture is then encoded on the biometric image using the image steganography - LSB technique. This method aids in the concealment of one picture within another image with little distortion. The AES technique is then used to seed a key into the embedded image, which is subsequently passed into the embedded image. The status of the test findings and the key will be mailed to the patient, and they will decrypt the photos using their fingerprint, which aids in retrieving the embedded image from storage by comparing the hash value of the image and the seeded key. The medical photos will be securely protected using this technology.

3. ALGORITHM

Any binary information, which is a stream of bytes, can be encoded using the Base64 algorithm into a stream of 64 readable characters. The raw image data is transformed into a stream of bytes for further processing in our proposed system using Base64 encoding. The steps involved in Base64 encoding are as follows:

- Split the input byte stream into three-byte pieces.
- Split each 3-byte block's 24 bits into 4 sets of 6 bits.
- The Base64 set map is used to convert each group of 6 bits to a single printed character.
- Pad the last 3-byte block with two bytes of zero (x0000) if the input file is only one byte long. After encoding it as a conventional block, replace the final two letters with two equal signs (==), letting the decoding process know that two zeros were added to the end as padding.
- Pad the last 3-byte block with 1 byte of zero (x00) if the input file only contains 2 bytes. Replace the final character of the standard block encoding with an equal sign (=), letting the decoding process know that a padding byte of zero was used
- The decoding process ignores carriage return (r) and new line operation (n) that are added into the output character stream.

4. OVERVIEW OF STEGANOGRAPHY

Steganography is the art and science of secret communication. The term steganography is a combination of two Greek words “steganos” and “graphy”, whereby “steganos” means “secret or covered” and “graphy” means “drawing or writing”. Steganography techniques can be divided into various categorized based on cover type, embedding domain, embedding and extraction approaches.

The steganography of medical images requires special caution when embedding extra data inside the medical images, whereby the added information does not impact the image
quality.

4.1 Steganography technique using LSB

Steganography is used in the proposed system to integrate the medical image with the patient's fingerprint image. The Least Significant Bit algorithm is a spatial domain approach in which medical image bits are placed in significant bits of the biometric picture.

This buried data is then recovered using the appropriate decoding algorithm. The main idea of this technique is to directly alter some LSB of the cover image with the secret data. The essential drawback of the available LSB techniques is that increasing the capacity of the stegno image leads to decreasing its quality.

5. LITERATURE AND REVIEW

The broad application of artificial intelligence techniques in medicine is currently hindered by limited dataset availability for algorithm training and validation, due to the absence of standardized electronic medical records, and strict legal and ethical requirements to protect patient privacy. In medical imaging, harmonized data exchange formats such as Digital Imaging and Communication in Medicine and electronic data storage are the standard, partially addressing the first issue, but the requirements for privacy preservation are equally strict. To prevent patient privacy compromise while promoting scientific research on large datasets that aims to improve patient care, the implementation of technical solutions to simultaneously address the demands for data protection and utilization is mandatory.

Artificial intelligence (AI) in medical imaging is a potentially disruptive technology. An understanding of the principles and application of radiomics, artificial neural networks, machine learning, and deep learning is an essential foundation to weave design solutions that accommodate ethical and regulatory requirements, and to craft AI-based algorithms that enhance outcomes, quality, and efficiency. Moreover, a more holistic perspective of applications, opportunities, and challenges from a programmatic perspective contributes to ethical and sustainable implementation of AI solutions.

6. MATERIALS AND METHODS

A. AES Algorithm

AES is a symmetric block encryption designed to replace DES as the accepted standard in the variety of applications. The construction of AES and most symmetric cyphers is quite sophisticated when compared to public-key cyphers like RSA. After the image is incorporated in our system, a key is seeded using AES and transferred into the medical image. The seeded key is also delivered to the patient's email, where it is used to decrypt the photographs.

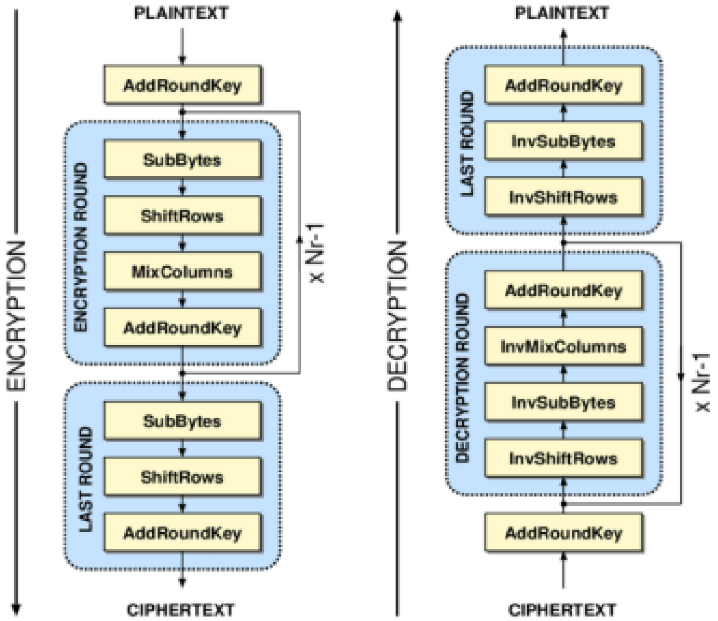


Figure1: AES algorithm for encryption and decryption

B. Biometric watermark

Watermarking is the process of concealing, verifying the validity or integrity of data, or revealing its owners' identities. The name biometric watermarking is offered since we employ the patient's fingerprint for concealing, encrypting, and decrypting medical images by authenticated patients. Watermarking is a technology in which data carrier identification information is embedded with methods that can be difficult to notice and do not affect data use. Watermarking technology usually protects multimedia data copyright like the authentication of banknotes to prevent attackers from damaging watermarking

C. System Overview

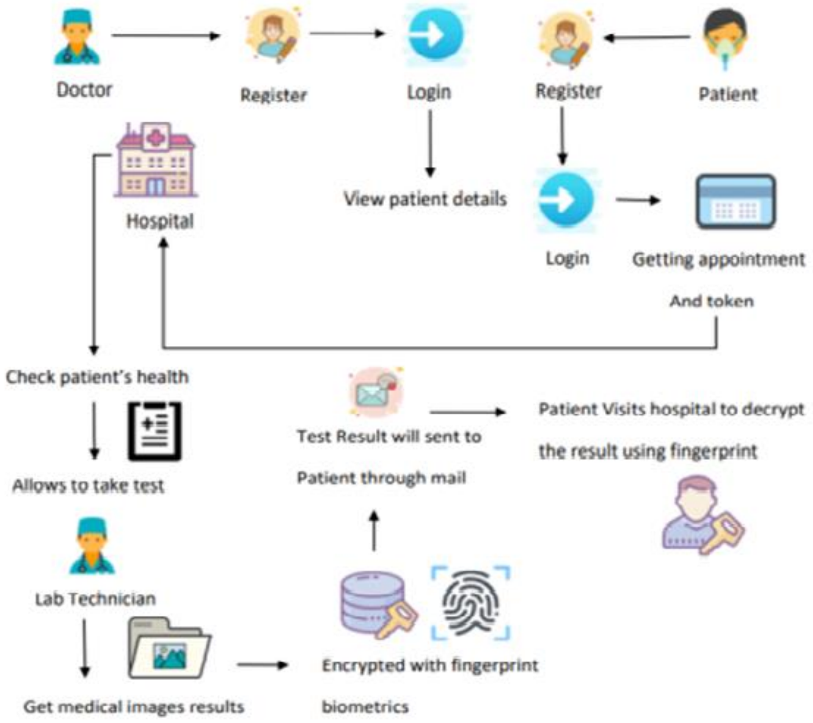


Fig.2: Overview of the proposed system

6.1 Doctor's Registration and Login

The physician will sign up and log in later to access the patient's details.

6.2 Patient's Registration and Login

Token The patient will register and login to get appointment to visit the hospital.

6.3 Generation and allow patient to take test

Each patient will receive a special token. The doctor will next examine *the patient and* the go-ahead to take tests. The patient will next proceed to the laboratory's scanning procedure.

6.4 Encrypting / decrypting medical images with fingerprint

At the lab, the patient will be scanned, and the scanned medica*l pictures will be* encrypted with that patient's fingerprint and a key will be supplied to the image, which will be seeded using the AES technique. This outcome will be provided to the patients through email. The medical picture can be accessed once it has been encrypted by using his or her fingerprint and inputting the AES key.

7.ADVANTAGES

- Paper based patient registration can be time consuming, and there are a chances for error. Alternatively, biometric registration can lead to more accurate and easy patient registration.
- Faster authentication, accuracy, scalability.
- When a child has a chronic disease or a form of cancer, medical imaging is essential not only at initial diagnosis, but for monitoring how the disease is responding to treatment or if the disease is progressing, and when a treatment plan might be stopped or adjusted.

8.DISADVANTAGES

- Cost-significant investment is needed in biometric pages for security.
- Data breaches-biometric data bases can still be hacked.
- Tracking and data-biometric devices like fingerprint, facial recognition systems can limit privacy for user

9.RESULTS AND DISCUSSION

The proposed technique utilizes the biometrics of the patient/owner to generate a key management system to obtain the parameters involved in the proposed technique. The medical image is then encrypted employing PR-APBST, QR and singular value decomposition and is ready for secure transmission or storage. Finally, a reliable decryption process is employed to reconstruct the original medical image from the encrypted image. The validity and feasibility of the proposed framework have been demonstrated using an extensive experiment on various medical images and security analysis. Moreover, in order to achieve confidentiality and security in the sharing of patient's information in biometric and medical image steganography requires an emphasis on other essential criteria such as privacy and authentication

The results of the proposed system are discussed

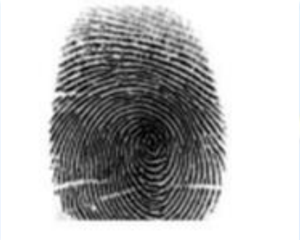


Fig.3: patient's fingerprint

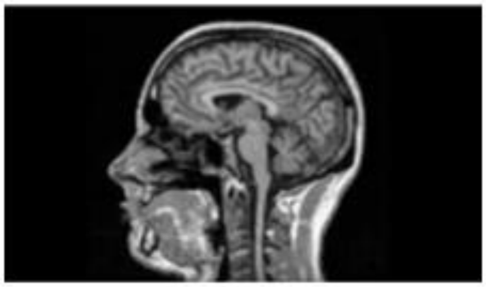
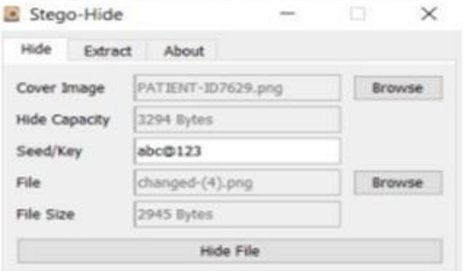


Fig.4: medical image of the patient



Cover Image PATIENT-ID7629.png

Hide Capacity 3294 Bytes

Seed/Key abc@123

File changed-(4).png

File Size 2945 Bytes

Fig.5: medical image and biometric of the patient are embedded and key value seeded.

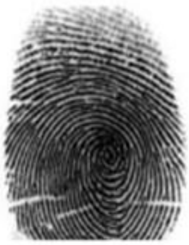
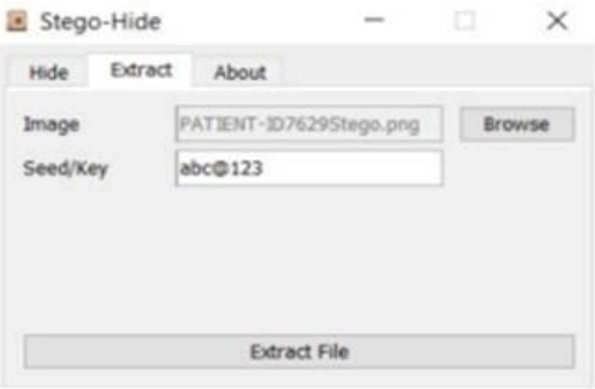


Fig.6: Image after performing steganography



Stego-Hide

Image: PATIENT-ID7629Stego.png

Seed/Key: abc@123

Fig.7: Extraction of medical images from the steganography image by passing the seeded key

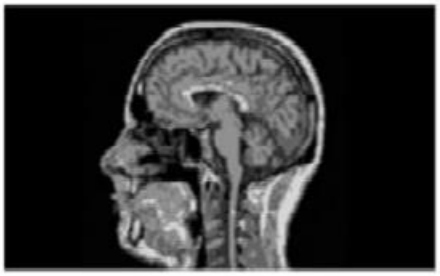


Fig.8: Extracted medical image

10. CONCLUSION

This is an innovative idea that might help to protect medical images stored in a hospital cloud. The most effective technology for preserving the integrity of data is encryption, which is superior to hashing, stenography, watermarking, and stenography. This is included as a key. This technique is resilient because fingerprints have the best statistical features of any biometric. Nevertheless, for intricate photos and high resolution.

Biometric scanners to produce high quality medical images, this system require additional image processing units. If this concept is improved in the future, it will undoubtedly safeguard the personal data of medical photographs, facilitating the processing of medical findings for diverse persons.

Author’s declaration

-Conflict of interest-none

-Funding-the research receive no external funding.

Reference

.[1]Georgios A. Kaissis, Marcus R. Makowski, Daniel Rückert & Rickmer F. Braren,"Secure, privacy preserving and pederated machine learning inmedical imaging", Nature Machine Intelligence volume 2, pages305–311 (2020)

[2]Floridi L, Cowls J, Beltrametti M,et al.AI4People-an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. Minds Mach. 2018;28: 689-707

[3]M. Sumithra and Dr. S. Malathi,"A Novel Distributed Matching Global and Local Fuzzy Clustering (DMGLFC) FOR 3D Brain Image Segmentation for Tumor Detection", IETE Journal of Researchdoi.org/10.1080/03772063.2022.2027284,2021

[4]B.Buvanswari and T.Kalpalatha Reddy,"A Review of EEG Based Human Facial Expression Recognition Systems in Cognitive Sciences"International Conference on Enenrgy,Communication, Data analytics and Soft computing(ICECDS),CFP17M55-PRJ:978-1-5386-1886-8",August 2017.

[5]Sumithra and Dr. S. Malathi," Modified Global Flower Pollination Algorithm-based image fusionfor medical diagnosis using computed tomography and magnetic resonance imaging", International Journal of Imaging Systems and Technology, Vol. 31, Issue No.1,pp.223-235, 2021

[6]K. Sridharan, and Dr. M. Chitra "SBPE:A paradigm Approach for proficient Information Retrieval, Jokull Journal" , Vol 63, No. 7;Jul 2013

[7]M. Sumithra and Dr. S. Malathi, "3D Densealex NET Model with Back Propagation for Brain TumorSegmentation", International Journal OfCurent Research and Review, Vol. 13, Issue 12, 2021.

[8]B.Buvaneswari and Dr.T. Kalpalatha Reddy,"EEG signal classification using soft computing techniques for brain disease diagnosis",Journal of International Pharmaceutical Research ,ISSN : 1674-0440,Vol.46,No.1,Pp.525-528,2019.

[9]K. Sridharan, and Dr. M. Chitra "Web Based Agent And Assertion Passive Grading For Information Retervial", ARPN Journal of Engineering and Applied Sciences, VOL. 10, NO. 16, September 2015pp:7043-7048

[10]M. Sumithra and Dr. S. Malathi,"Segmentation Of Different Modalitites Using Fuzzy K-Means And Wavelet ROI", International Journal Of Scientific & Technology Research, Vol. 8, Issue 11, pp. 996-1002, November 2019.

[11]M. Sumithra and S. Malathi,"A Survey of Brain Tumor Segmentation Methods with Different Image Modalitites", International Journal of Computer Science Trends and Technology (IJCST) – Vol. 5 Issue 2, Mar – Apr 2017

[12]B.Buvaneswari and Dr.T. Kalpalatha Reddy,"High Performance Hybrid Cognitive Framework for Bio-Facial Signal Fusion Processing for the Disease Diagnosis", Measurement,ISSN: 0263-2241,Vol.140,Pp.89-99,2019.

[13]M. Sumithra and Dr. S. Malathi,"A Brief Survey on Multi Modalities Fusion", Lecture Notes on Data Engineering and Communications Technologies, Springer, 35, pp. 1031-1041,2020.

[14]M. Sumithra and S. Malathi, "A survey on Medical Image Segmentation Methods with Different Modalitites", International Journal of Engineering Research and Technology (IJERT) – Vol. 6 Issue 2, Mar 2018.

[15]B.Buvaneswari and Dr.T. KalpalathaReddy,"ELSA- A Novel Technique to Predict Parkinson's Disease in Bio-Facial",International Journal of Advanced Trends in Computer Science and Engineering, ISSN 2278-3091,Vol.8,No.1,Pp. 12-17,2019 [16]K.Sridharan, and Dr. M. Chitra, Proficient Information Retrieval Using Trust Based Search On Expert And Knowledge Users Query Formulation System, Australian Journal of Basic and Applied Sciences, 9(23) July 2015, Pages: 755-765.

[17]B.Buvaneswari and Dr.T. Kalpalatha Reddy, "ACPT- An Intelligent Methodology for Disease Diagnosis",Journal of Advanced Research in Dynamical and Control Systems,ISSN:0974-5572,Vol.11,No.4,Pp.2187-2194,2019.

[18]Sumithra, M., Shruthi, S., Ram, S., Swathi, S.,Deepika, T,"MRI image classification of brain tumor using deep neural network and deployment using web framework", Advances in Parallel Computing, 2021, 38, pp. 614–617.

[19]K. Sridharan, and Dr. M. Chitra "RSSE: A Paradigm for Proficient Information Retrieval using Semantic Web",Life Science Journal 2013;10(7s), pp: 418-425