Secure Medical Images using Biometric Inspired Robust Security

R. Ramya, T. Sree Hari Priya, R. Deepa
Department of Computer Science and Engineering
B.E Student, Assistant Professor
Prince Dr. K. Vasudevan College of Engineering and Technology, Chennai, India

Abstract:
The protection of sensitive and confidential data become a challenging task in the present scenario as more and more digital data is stored and transmitted between the end users. The privacy is vitally necessary in case of medical data, which contains the important information of the patients. In this article, a novel biometric inspired medical encryption technique is proposed based on newly introduced parameterized all phase orthogonal transformation (PR-APBST), singular value and QR decomposition. 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 experiments on various medical images and security analysis.

I. INTRODUCTION
The modern clinical diagnosis has entered into the digital age due to substantial proliferation in medical research and technology. This paradigm shift leads to fast and better accuracy in the diagnosis and the treatment of the patients. Most of the medical imaging sensors provides the data in the form of digital images such as computed tomography (CT), ultrasound, X-ray, magnetic resonance image (MRI) and positron emission tomography (PET). The medical image data provides valuable information related to position, shape, intensity and scale of the object based on the visual representation of internal structure of the body organs, which is useful in clinical analysis and medical intervention. It helps to detect disease in X-ray, segmenting organs from CT scans and quantifying anomalies in MRI images. Moreover, the medical images such as mammograms can be transformed into a representative image whose pixel value shows the approximate density information. Similarly, other quantitative information about features like shape and scale are useful in tumour and brain cancer detection. Therefore, in essence, medical images contain important confidential and sensitive information related to the patient’s health condition.

The main problem arises during the storage and communication of these images for various purposes. These diagnostics images are generally stored and transmitted across several public channels through internet for various applications such as denoising, compression, segmentation and data hiding. However, due to lack of inherent medical images may be exposed to the serious threats like illegal manipulation, privacy leakage and data integrity. Hence, the stressed motive of this work is to fulfill the requirement of robust encryption technique for medical images with considerably high security.

II. EXISTING SYSTEM
In the existing system, various methodologies have been developed to protect the medical images such as encryption, hashing, stenography and watermarking. Among these, encryption is the most suitable methodology to protect the integrity of the data. However, the conventional encryption techniques such as Advanced Encryption Standard (AES), Data Encryption Standard (DES) and International Data Encryption Standard (IDES) are not suitable for the encryption of medical images due to the integral features of the medical images such as high correlation between neighboring pixels and redundancy.

III. PROPOSED SYSTEM
In the proposed system, a high-efficiency and robust encryption technique to protect medical images is proposed. The patient will register and login and gets a token with which they need to visit hospital. The doctor will register and login to see the patient details. Then the doctor will check the patient and gives the report and asks them to visit the lab for test. The medical images taken in the lab will get encrypted using the fingerprint biometrics of the particular patient. The status of test results will be sent to patient through mail and they will decrypt the images by using the fingerprint by visiting the hospital. By using this technique, the medical images will be secured with robust security.

Figure 1. System Architecture
A. Patient login
The patient is allowed to login by getting all the information of the patient. The major information related to patient are collected. Patient details are rechecked whether the patient is registered earlier. Once checked patient allowed to login by entering the details.

B. Registration
Patient details are registered into hospital login portal. After successful login, details are processed for generation of unique code. According to code patient are directed to doctors. Patient allowed to the concerned doctor, patient directed to lab for scanning process.

C. Medical image generation
As per the doctor’s advice patient directed to medical lab for further scan processing. Medical lab, patient variable medical images as per the doctors consultancy, lab testing's are made. Medical images and their reports are generated.

D. Medical image encryption.
Scanned medical images and reports are encrypted using Parameterized All Phase Orthogonal Transformation (PR-APBST), Singular value and QR decomposition medical encryption techniques. Stored medical images and reports are encrypted using biometrics of patient. Encrypted images are stored and sent via email personals to concerned person mail id.

E. Decryption
Encrypted medical images sent to mail id of patient. Encrypted images are decrypted using reliable decryption method. Decryption can be made only by fingerprint of patient. Once consulting the doctor, images are decrypted securely. It prevents data's more securely.

IV. RESULT 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 experiments on various medical images and security analysis.
ACKNOWLEDGMENT
I would like to express great fullness to U.G..Department of Computer Science Engineering, Prince. Dr. K.Vasudevan College of Engineering and Technology, ponmar.

V. REFERENCES


