International Journal of Engineering Research and Science & Technology

SECURE MEDICAL IMAGE SHARING WITHWATERMARKING IN IMAGE PROCESSING

VANGALA SWATHI [1], A. BHANU CHANDRA PRASAD [2], PILLLAMARI CHANDU [3], KADINGI BHUVAN [4], V. SAI KRISHNA [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— The rapid growth of the Internet and digital healthcare systems, the secure transmission and management of medical particularly medical images have become critical for safeguarding patient privacy and supporting collaborative healthcare delivery. This study explores a range of techniques designed to ensure the confidentiality, integrity, and accessibility of medical data during transmission and storage. We classify these techniques into centralized approaches, including conventional encryption and digital watermarking. Special attention is given to the progression of medical image watermarking methods, focusing on their role in maintaining data security. Traditional watermarking techniques offer simplicity and transparency, making them suitable for regulatory compliance and practical implementation. The study highlights the trade-offs involved in different methods, such as processing overhead, scalability, and resistance to tampering. By presenting a comprehensive classification of current watermarking approaches and suggesting potential areas for refinement, this research contributes to the development of secure, reliable frameworks for medical image sharing in increasingly connected healthcare environments.

Index Terms – Medical Image Sharing, Digital Watermarking, Image Processing, Medical Image Security, Data Integrity, Privacy Preservation, Authentication, Healthcare Systems, Cryptography, Cybersecurity.

I. INTRODUCTION

The healthcare ecosystem manipulates medical data that are of unique and critical importance because of the sensitive nature of

the information it contains. These data encompass not only personally identifiable patient details, but also medical histories, diagnostic images, and other essential information that plays a pivotal role in diagnosing, treating, and monitoring patient health. Given its profound implications for patient care, unauthorized access to or tampering with such data can lead to severe consequences, including misdiagnosis, incorrect treatment, and compromised patient safety [1]. The increasing digitization of healthcare systems, while offering improved efficiency and accessibility, has significantly heightened the risks associated with cyber threats, making the protection of medical data more urgent than ever [2]. Key threats to medical imaging systems encompass ransomware attacks that can encrypt critical medical images, unauthorized access to Picture Archiving and Communication Systems (PACS), and phishing attempts aimed at compromising employee credentials [3]. A prominent example is the WannaCry ransomware incident in 2017, which had a profound impact on healthcare services globally. This attack took advantage of vulnerabilities in outdated Windows systems, encrypting essential data and demanding a ransom for decryption. The incident resulted in the cancellation of numerous medical procedures, emphasizing the necessity of maintaining up-to-date systems and implementing regular backup protocols. Moreover, malware infections pose a risk of data corruption, while breaches due to unsecured servers have led to the exposure of sensitive patient information. For example, researchers uncovered millions of medical images stored on publicly accessible servers without adequate protection, illustrating the dangers of poor security practices. Insider threats also represent a serious concern; in one case, a healthcare worker improperly accessed and disclosed patient information, reinforcing the need for stringent internal access controls and monitoring mechanisms. Additionally, network attacks, like Distributed Denial of Service (DDoS) assaults, can disrupt access to vital imaging systems, causing operational challenges without necessarily resulting in data loss.

II. RELATED WORK

A. Asymmetric healthcare biometric image encryption and watermarking technique using QZ synthesis and QRD algorithm

The research paper introduces an advanced asymmetric biometric image encryption technique that integrates Quasi-Zernike synthesis (QZS), QR algorithm, and hybrid transforms for enhanced security and

integrity. The encryption process incorporates QR decomposition, generating an orthogonal matrix Q that adds obfuscation and randomness to the image representation. QR is also resilient to attacks that exploit vulnerabilities in PTFT-based cryptosystems. QZS further improves security by capturing spatial information and complex features. The use of the compressed sparse row (CSR) format enables efficient storage and secure transmission. This integration provides a robust solution for confidential, secure image communication, applicable in military, surveillance, and sensitive data transfer scenarios. Moreover, watermarking ensures protection from unauthorized access, strengthening security measures. Experimental evaluations demonstrate the proposed algorithm's robustness against common attacks, including noise addition, compression, and filtering. The results showcase high-quality image reconstruction, negligible information loss, affirming the scheme's effectiveness in achieving secure image encryption.

B. *Security of end-to-end medical images encryption system using trained deep learning encryption and decryption network*

The Internet of Medical Things (IoMT) links medical devices and wearable, enhancing healthcare. To secure sensitive patient data over the IoMT, encryption is vital to retain confidentiality, prevent tampering, ensure authenticity, and secure data transfer. The intricate neural network architecture of deep learning models adds a layer of complexity and non-linearity to the encryption process, rendering it highly resistant to plaintext attacks. Specifically, the Cycle_GAN network is used as the leading learning network. This work suggests deep learning-based encryption for medical images using Cycle_GAN, a Generative Adversarial Network. Cycle_GAN changes images without paired training data that improves quality and feature preservation. Unlike conventional image-to-image translation techniques, Cycle_GAN doesn't require a dataset with corresponding input–output pairs. Traditional methods typically needs paired data to learn the mapping between input and output images.

C. *Optical image authentication and encryption scheme with computational ghost imaging*

Considering the necessity of identity authentication in most scenarios, a dual-

channel (digital channel and optical channel) image encryption and authentication algorithm with computational ghost imaging (CGI) is proposed. The entire encryption process is governed by the pseudo-random sequences obtained by the 4D chaotic system and the Logistic map. During the digital channel encryption, the confusion and diffusion of the plaintext image are achieved by random scrambling and DNA computing, respectively. To alleviate the burden of key transmission and storage in the CGI encryption system, the speckle measurement matrices are constructed with the pseudo-random numbers obtained by the Logistic map. Additionally, a nonlinear encryption operation is carried out to compensate the linear vulnerability of CGI encryption.

III. PROPOSED METHODOLOGY

Widely used to protect medical data during transmission and storage. Ensures confidentiality by transforming images into unreadable formats unless decrypted with a secure key.

Data remains on local servers; only encrypted metadata or models are shared. Reduces data exposure and complies with privacy.

A study proposed a blockchain-based system for managing medical data, ensuring not only the immutability of results but also giving patients full control over their personal health records.

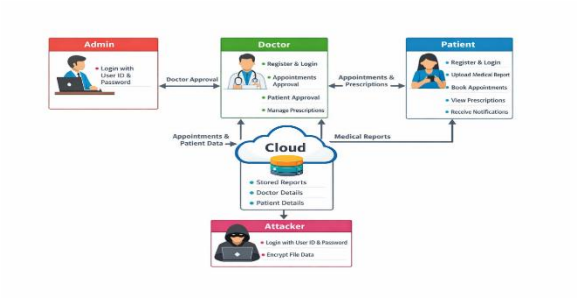


Fig. 1: System Overview

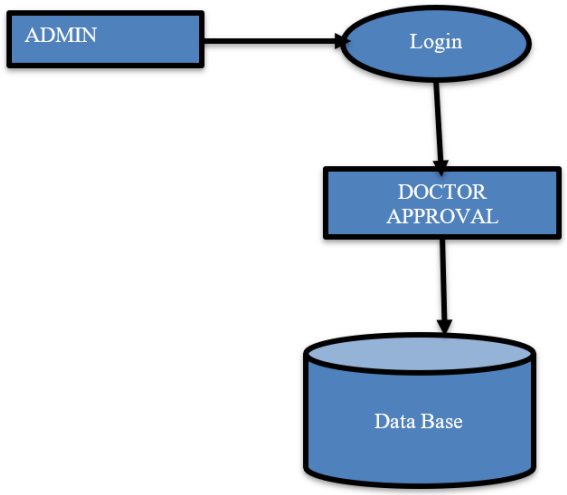
1. Admin

In this system, the Administrator plays a central role in managing and controlling overall operations. The admin logs into the system using a valid user ID and password, ensuring secure authentication and restricted access to administrative features. This login mechanism protects sensitive system controls from unauthorized users and maintains system integrity. Once authenticated, the administrator gains access to a dedicated dashboard that provides management and monitoring capabilities.

One of the important responsibilities of the admin is handling doctor approvals stored in the database. When a doctor registers in the system, their details such as name, specialization, contact information, and

credentials are stored in the database with a pending approval status.

If approved, the doctor's status in the database is updated to "Approved," granting them access to system features and services. If rejected, the status is marked accordingly, preventing system access. This approval process ensures that only verified and authorized doctors are allowed to operate within the system. Overall, the admin login and doctor approval mechanism enhances security, maintains data accuracy, and ensures controlled access management within the platform.



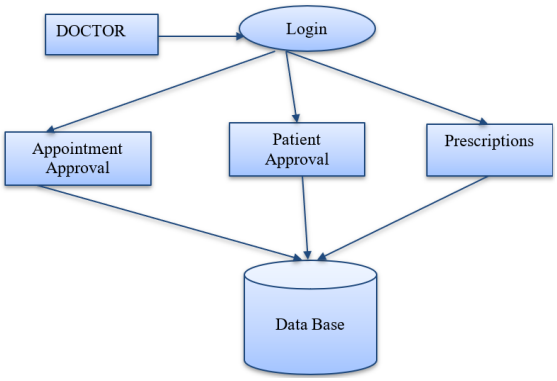
2.Doctor

In this system, the Doctor plays an important role in managing patient care and medical services. First, the doctor must register by providing required details such as name, specialization, contact information, qualifications, and login credentials. After successful registration and approval (if required), the doctor can log into the system securely using a user ID and password. This authentication process ensures that only authorized medical professionals can access sensitive patient information and system features.

Once logged in, the doctor has the ability to manage appointment approvals. When patients request appointments, the requests are stored in the system with a pending status.

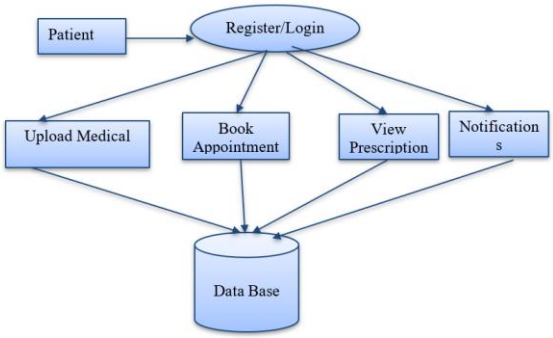
The doctor also has the authority to approve patients within the system. This may include verifying patient registration details or confirming consultation eligibility. After consultation, the doctor can create and manage prescriptions for patients. Prescription details such as medicines, dosage, instructions, and follow-up recommendations are recorded and stored securely in the database. Overall, the doctor module ensures secure access, efficient appointment handling, patient management, and accurate prescription generation within the healthcare system.

International Journal of Engineering Research and Science & Technology



3.Patient

In this system, the Patient module is designed to provide secure and convenient access to healthcare services. First, the patient must register by entering required personal details such as name, age, contact information, medical history, and login credentials. After successful registration, the patient can log in using a valid user ID and password. This authentication process ensures that only authorized patients can access their personal medical information. Once logged in, the patient can upload medical reports such as lab results, scan reports, or previous prescriptions. These reports are securely stored in the database and can be accessed by the doctor during consultation. The patient can also book appointments by selecting an available doctor and choosing a suitable date and time. The appointment request is then sent to the doctor for approval. After consultation, the patient can view prescriptions provided by the doctor. Prescription details such as medicines, dosage instructions, and follow-up dates are displayed in the patient dashboard. Additionally, the system provides notifications to inform patients about appointment approvals, prescription updates, or important messages from doctors. Overall, the patient module ensures secure access, efficient communication, and organized management of medical records and appointments.

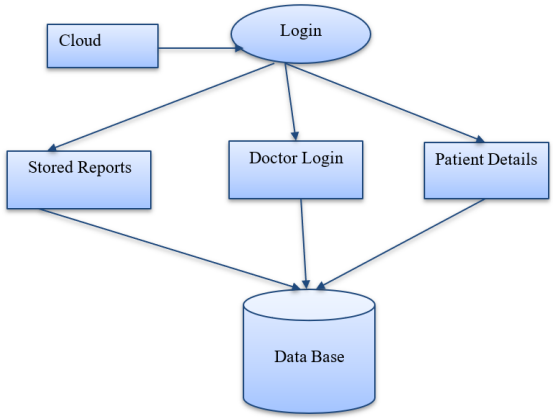


4.CLOUD

In this healthcare system, the Cloud module functions as a centralized and secure data management platform. The cloud administrator or authorized cloud service logs into the system using a valid user ID and password. This authentication process ensures that only permitted entities can access sensitive healthcare information stored within the cloud environment. Secure login mechanisms help protect the system from unauthorized access and potential security threats.

Once logged in, the cloud is responsible for storing medical reports uploaded by patients. These reports may include lab results, diagnostic scans, medical histories, and treatment records. The cloud ensures that all uploaded data is securely stored and properly organized for easy retrieval by authorized users such as doctors and administrators.

In addition to medical reports, the cloud also maintains doctor details, including their personal information, specialization, qualifications, and approval status. Similarly, it stores patient details such as registration information, appointment records, prescriptions, and uploaded documents.



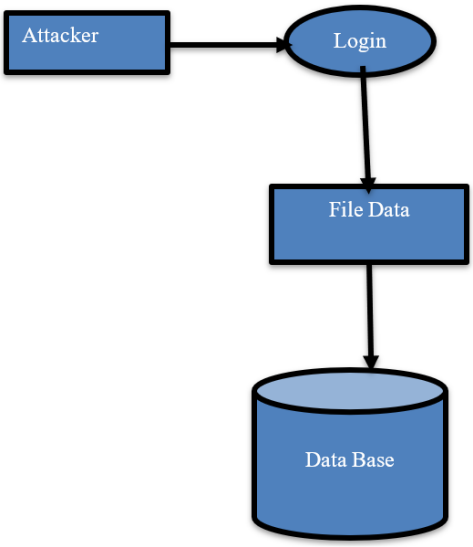
4. ATTACKER

In this system, the Attacker module represents an unauthorized or malicious user attempting to gain access to sensitive data. The attacker may try to log into the system using a user ID and password, either by guessing credentials, using stolen login details, or exploiting security vulnerabilities. This highlights the importance of strong authentication mechanisms, secure password policies, and additional security measures such as encryption and access control to prevent unauthorized entry.

If the attacker gains access to file data, the system ensures that the stored information is protected through encryption. In this case, the file data is converted into an encrypted image format or encrypted data form. Encryption transforms the original readable data into an unreadable format using a specific key or algorithm. Without the correct decryption key, the attacker cannot interpret or misuse the encrypted content.

By encrypting files and storing them securely, the system minimizes the risk of data breaches and protects sensitive information even if unauthorized access occurs. This approach ensures confidentiality and data security.

International Journal of Engineering Research and Science & Technology



IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the watermarking method successfully embedded authentication and ownership information into medical images while preserving the diagnostic quality of the original images.

The analysis showed that the proposed approach achieved high robustness against common image processing attacks such as compression, noise addition, filtering, cropping, and image enhancement operations.



Fig. 2: Homepage

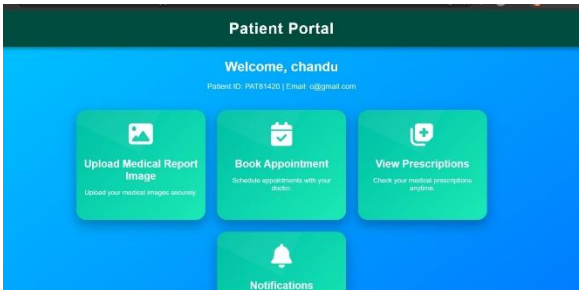


Fig. 3: Dashboard

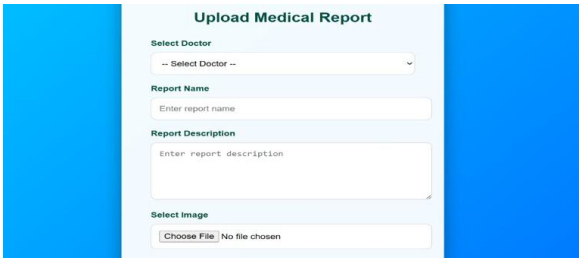


Fig. 4: Upload Medical Record

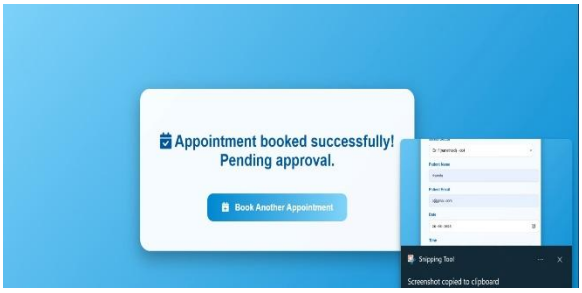


Fig. 5: Appointment booked

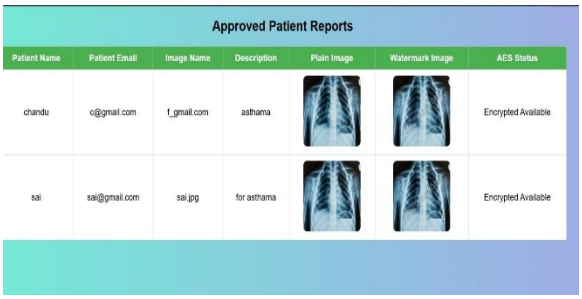


Fig. 6: Approved Records



Fig. 7: Send Prescription

V. CONCLUSION

This thorough study underscores the essential need for secure medical data sharing in healthcare, highlighting the many technologies available along with their relative advantages and disadvantages. Centralized techniques such as encryption and watermarking are essential for safeguarding confidentiality and integrity; however, they encounter issues related to key management and susceptibility to tampering. Decentralized methodologies, including blockchain and federated learning, provide strong alternatives by distributing trust and safeguarding data privacy; however, they require significant resources and encounter threats such as adversarial attacks.

REFERENCES

[1] S. B. Patel, T. B. Mehta, and S. N. Pradhan, ‘‘A unified technique for robust digital watermarking of colour images using data mining and DCT,’’ Int. J. Internet Technol. Secured Trans., vol. 3, no. 1, p. 81, Apr. 2011.

[2] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd ed. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2007.

[3] M. Eichelberg, K. Kleber, and M. Kämmerer, ‘‘Cybersecurity in PACS and medical imaging: An overview,’’ J. Digit. Imag., vol. 33, no. 6, pp. 1527–1542, Dec. 2020.

[4] M. Khatkar, K. Kumar, and B. Kumar, ‘‘An overview of distributed denial of service and Internet of Things in healthcare devices,’’ in Proc. Res., Innov., Knowl. Manage. Technol. Appl. Bus. Sustainability (INBUSH), Feb. 2020, pp. 44–48.

[5] A. K. Singh, B. Kumar, G. Singh, and A. Mohan, Medical Image Watermarking







Techniques: A Technical Survey and Potential Challenges. Cham, Switzerland: Springer, 2017, pp. 13–41.

[6] H. D. Tagare, C. C. Jaffe, and J. Duncan, ‘‘Medical image databases: A content-based retrieval approach,’’ J. Amer. Med. Inform. Assoc., vol. 4, no. 3, pp. 184–198, May 1997.



AUTHORS Profile

Ms. VANGALA SWATHI has received her B.Tech from JNTUH, Hyderabad in 2015, M.Tech degree in Computer science from JNTUH, Hyderabad in 2017. She is dedicated to teaching field from the last 7 years. Her research area Deep Learning. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus ,Ibrahimpatnam, Telangana, India.

Mr. A. BHANU CHANDRA PRASAD pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. PILLLAMARRI CHANDU pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. KADINGI BHUVAN pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. V. SAI KRISHNA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.