JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

LIGHTWEIGHT BIOMEDICAL IMAGE ENCRYPTION APPROACH

[1]P. Mahesh, [2]N. Chandu, [3]P. Uday Kiran, [4]Mrs. A. Vishalakshi
[1,2,3]UG Scholars, [4]Asst. Professor
[1,2,3,4]Department of Computer Science and Engineering,
Guru Nanak Institutions Technical Campus (Autonomous), Hyderabad, India.

Abstract*: This paper proposes a lightweight image encryption approach for medical Internet of Things (MIoT) networks using compressive sensing and a modified seven-dimensional (MSD) hyperchaotic map. Initially, 7D hyper chaotic map is modified to generate more secure and complex secret keys. SHA-512 is used to create the initial conditions for MSD, which ensures its sensitivity towards input images. Using non sub sampled contourlet transform (NSCT), further improvements in the compressive sensing are achieved, and then the measurement matrices are generated using the secret keys obtained from MSD. Finally, to generate encrypted images, the diffusion and permutation are carried out row and column-wise on compressed images using secret keys obtained from MSD. The comparative analyses verify the performance of the proposed lightweight encryption approach in terms of robustness, security, and statistical analysis.*

***IndexTerms* –** Lightweight Image Encryption, Medical Internet Of Things, Compressive Sensing, Modified Seven Dimensional Hyper Chaotic Map, Robust, Non Subsampled Contourlet transform(NSCT), Security

I. INTRODUCTION

Secure data transmission over the Internet, particularly concerning medical data, is increasingly challenging due to advancements in digital technologies. This is exacerbated by the ease of unauthorized access to medical information, leading to breaches of patient privacy. The convenience of storing and transmitting patient data digitally, including laboratory reports, ECG reports, and medical prescriptions, underscores the need for robust security measures. With more than 90% of medical images processed and stored electronically, ensuring the security and privacy of this data is paramount. The integration of Internet of Things (IoT) systems in medical imaging for remote diagnostics has further highlighted the importance of securing medical data in transit. However, the IoT environment presents vulnerabilities that can be exploited for data manipulation. To address this, security policies and techniques such as steganography and encryption are being integrated into IoT systems to protect sensitive medical data. Traditional encryption techniques, however, may not offer sufficient protection for transmitted data in this context.

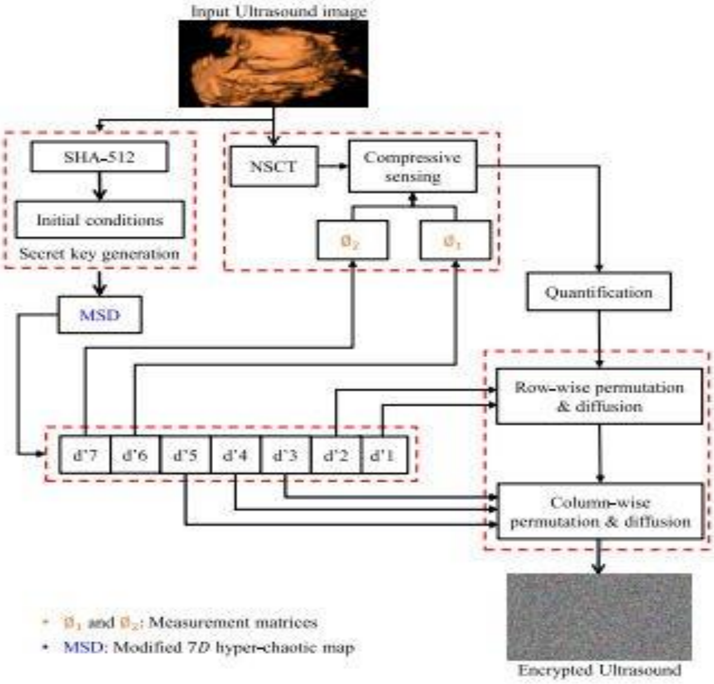
LITERATURE REVIEW

Medical images possess significant importance in diagnostics when it comes to healthcare systems. These images contain confidential and sensitive information such as patients’ X-rays, ultrasounds, computed tomography scans, brain images, and magnetic resonance imaging. However, the low security of communication channels and the loopholes in storage systems of hospitals or medical centres put these images at risk of being accessed by unauthorized users who illegally exploit them for non-diagnostic purposes. In addition to improving the security of communication channels and storage systems, image encryption is a popular strategy adopted to ensure the safety of medical images against unauthorized access. In this work, we propose a lightweight cryptosystem based on Henon chaotic map, Brownian motion, and Chen’s chaotic system to encrypt medical images with elevated security. The efficiency of the proposed system is proved in terms of histogram analysis, adjacent pixels correlation analysis, contrast analysis, homogeneity analysis, energy analysis, NIST analysis, mean square error, information entropy, number of pixels changing rate, unified average changing intensity, peak to signal noise ratio and time complexity. The experimental results show that the proposed cryptosystem is a lightweight approach that can achieve the desired security level for encrypting confidential image-based patients’ information.

II. RESEARCH METHODOLOGY

.

The complete architecture diagram is shown as



.

III. TECHNIQUE USED OR ALGORITHM USED

3.1 EXISTING TECHNIQUE: -

DNA Cryptography

DNA cryptography utilizes DNA molecules' storage and coding capabilities for encryption, treating adenine (A), cytosine (C), guanine (G), and thymine (T) as binary digits. Encoding converts binary data into DNA sequences, leveraging DNA's dense storage and parallelism. Decryption involves reverse transcription, translating DNA back into binary. This approach benefits from DNA's robustness, resistance to cyberattacks, and data-handling capabilities, making it an emerging field with significant potential for secure data storage and transmission.

3.2 PROPOSED TECHNIQUE USED OR ALGORITHM USED:

SHA-512

The proposed system offers both low computational cost and low power consumption. Beugnon et al. introduced a secret 3-D object sharing scheme to protect image content, focusing on safeguarding geometrical distortions through a unique sharing mechanism. Kamal et al. devised an image splitting technique with a logistic map (ISTLM) to secure medical images, utilizing random permutation, rotation, and zigzag patterns to scramble image blocks. Secret keys generated from the logistic chaotic map were used to diffuse the scrambled blocks. Akkasaligar et al. employed a dual hyper chaotic map and (DDNA) for medical image encryption.

IV. IMPLEMENTATION

In this project, Secure data transmission over the Internet is increasingly challenging due to digital advancements, particularly concerning medical data. Unauthorized access to such data has compromised patient rights, as medical information like laboratory reports and ECG data are stored digitally, making them convenient yet vulnerable. The rise of IoT systems in medical imaging exacerbates this vulnerability, requiring integration with information security policies for data privacy. Encryption and steganography are employed to protect sensitive patient information, with medical data encrypted through sensors and decrypted by medical practitioners for diagnosis. Cloud servers are also used for supplementary diagnoses, utilizing encrypted patient data. Traditional encryption methods, however, may not be sufficient for direct encryption of transmitted data. This paper proposes a lightweight image encryption methodology for Medical Internet of Things (MIoT) networks, aiming to enhance the security and efficiency of encrypting medical images. The approach modifies a seven-dimensional (7D) hyper chaotic map to generate more secure secret keys and utilizes cryptographic techniques like SHA-512 to enhance overall security in this project.

V. RESULTS

The proposed lightweight image encryption methodology for Medical Internet of Things (MIoT) networks addresses the challenges of secure data transmission, particularly for medical data, over the Internet. With the increasing digitalization of patient information, protecting data privacy and preventing unauthorized access and manipulation have become critical issues. This methodology aims to enhance the security and efficiency of encrypting medical images transmitted over MIoT networks, which often operate under resource constraints. The approach involves modifying a seven-dimensional (7D) hyper chaotic map to generate more secure and complex secret keys, thereby bolstering the encryption process. Additionally, cryptographic techniques, such as SHA-512, are leveraged to ensure the sensitivity of the chaotic system to input images, enhancing overall security. By integrating information security policies and utilizing steganography and encryption approaches, sensitive patient diagnostic information can be effectively protected in the IoT environment. This methodology not only enhances the security of medical data transmission but also ensures the privacy and integrity of patient information in digital form.

Results of bas

VI. CONCLUSION

In Medical Internet of Things (MIoT) networks, the transmission of biomedical images over the Internet poses security risks. To address this, a lightweight biomedical image encryption approach was developed using Modified Seven-Dimensional (MSD) hyperchaotic map and compressive sensing. MSD was enhanced for dynamism and complexity, with SHA-512 generating initial conditions. Compressive sensing was improved with NSCT, generating measurement matrices using MSD keys. Encryption involved diffusion and permutation on compressed images with MSD keys. Performance analysis showed better robustness, security, and speed compared to existing methods, with improvements in entropy, NPCR, UACI, and PSNR.

VII. FUTURE ENHANCEMENTS

Future enhancements to the proposed lightweight image encryption approach for medical Internet of Things (MIoT) networks include integrating adaptive key management mechanisms for dynamic encryption parameter adjustment based on network conditions and security requirements. Error correction coding techniques can be incorporated to enhance data transmission robustness, reducing the risk of data loss or corruption. Advanced image fusion techniques can integrate multi-modal medical imaging data while preserving data integrity and confidentiality. Hardware acceleration techniques such as field-programmable gate arrays (FPGAs) or graphics processing units (GPUs) can significantly improve the computational efficiency of the encryption process, making it more suitable for resource-constrained MIoT devices.

VIII. REFERENCES

[1] Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, M. Cao, and Z. Qin, ‘‘DeepEDN: A deep- learning-based image encryption and decryption network for Internet of Medical Things,’’ IEEE Internet Things J., vol. 8, no. 3, pp. 1504–1518, Feb. 2021.

[2] L. Jiang, L. Chen, T. Giannetsos, B. Luo, K. Liang, and J. Han, ‘‘Toward practical privacy-preserving processing over encrypted data in IoT: An assistive healthcare use case,’’ IEEE Internet Things J., vol. 6, no. 6, pp. 10177–10190, Dec. 2019.

[3] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, ‘‘Secured data collection with hardware-based ciphers for IoT-based healthcare,’’ IEEE Internet Things J., vol. 6, no. 1, pp. 410–420, Feb. 2019.

[4] F. Rezaeibagha, Y. Mu, K. Huang, and L. Chen, ‘‘Secure and efficient data aggregation for IoT monitoring systems,’’ IEEE Internet Things J., vol. 8, no. 10, pp. 8056–8063, May 2021.

[5] D. Wang, T. Song, L. Dong, and C. Yang, ‘‘Optimal contrast grayscale visual cryptography schemes with reversing,’’ IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 2059–2072, Dec. 2013.

[6] B. Ferreira, J. Rodrigues, J. Leitão, and H. Domingos, ‘‘Practical privacypreserving content-based retrieval in cloud image repositories,’’ IEEE Trans. Cloud Comput., vol. 7, no. 3, pp. 784– 798, Jul. 2019.

[7] Q. Yang, D. Zhu, and L. Yang, ‘‘A new 7D hyperchaotic system with five positive Lyapunov exponents coined,’’ Int. J. Bifurcation Chaos, vol. 28, no. 5, May 2018, Art. no. 1850057.

[8] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, ‘‘Securing data in Internet of Things (IoT) using cryptography and steganography techniques,’’ IEEE Trans. Syst., Man, Cybern. Syst., vol. 50, no. 1, pp. 73–80, Jan. 2020.