IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 8, August 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308061|

Modified Seven-Dimensional Approach for Lightweight Image Encryption in Medical Internet of Things (MIOT)

M. Kesavamurthi, B.E., Dr. I. Jackson Daniel, M.E., Ph.D.

Department of Electronics and Communication Engineering, Rohini College of Engineering and Technology, Kanyakumari, Tamil Nadu, India

ABSTRACT: Nowadays, secure data transmission over the Internet is a challenging issue due to the unauthorized access of transmission data from various sources of digital technologies and in the Internet. This situation is even worse for medical data transmission. The unauthorized access to medical information over the Internet led to the desecration of patient's rights. The existing system proposed a secure IoT- based healthcare system to handle the security issues associated with conventional techniques. They implemented a KATAN secret cipher algorithm on FPGA hardware platform. This system requires slightly more computational time. This scheme not only increases the transmission risk but also decreases user-friendliness.To overcome the above disadvantages, this project proposes the Lightweight Image Encryption approach for compressive sensing and a modified seven-dimensional (MSD) hyper chaotic map is generated using the applications of Medical Internet of Things (MIoT).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-Subsampled 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

KEYWORDS: KATAN Secret Algorithm, Seven-Dimensional Hyper chaotic map, Non-Subsampled Contourlet Transform.

I. INTRODUCTION

The Internet of Medical Things (IoMT) is the network of Internet-connected medical devices, hardware infrastructure, and software applications used to connect healthcare information technology. Sometimes referred to as IoT in healthcare, IoMT allows wireless and remote devices to securely communicate over the Internet to allow rapid and flexible analysis of medical data. Remote Patient Monitoring: IoT devices enable healthcare providers to remotely monitor patients' vital signs and health parameters in real-time. This can be particularly beneficial for patients with chronic conditions who require continuous monitoring without frequent hospital visits. Data Analytics and Personalized Medicine: The vast amount of data generated by IoT devices can be analysed to identify trends, correlations, and predictive insights.

This data-driven approach facilitates personalized medicine, where treatments and interventions are tailored to individual patient needs and characteristics. Security and Privacy: Given the sensitive nature of health data, ensuring the security and privacy of IoT-enabled healthcare systems is paramount. Robust cybersecurity measures, such as encryption, access controls, and regular security audits, are essential to safeguard patient information and prevent unauthorized access or data breaches. Chaos-based image-encryption technology can be categorized into different types based on various classification methods. One approach is to classify it according to how the original image is processed, which can be divided into chaotic image encryption based on a block cipher and chaotic image encryption based on a stream cipher.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308061|

II. REVIEW OF LITERATURE

Yi Ding et al., (2021) proposed a deep-learning-based image encryption and decryption network for Internet of Medical Things. Internet of Medical Things (IoMT) can connect many medical imaging equipment's to the medical information network to facilitate the process of diagnosing and treating for doctors. As medical image contains sensitive information, it is of importance yet very challenging to safeguard the privacy or security of the patient. In this work, a deep learning-based encryption and decryption network (DeepEDN) is proposed to fulfil the process of encrypting and decrypting the medical image. Specifically, in DeepEDN, the Cycle-Generative Adversarial Network (Cycle-GAN) is employed as the main learning network to transfer the medical image from its original domain into the target domain. Target domain is regarded as a "Hidden Factors" to guide the learning model for realizing the encryption. The encrypted image is restored to the original (plaintext) image through a reconstruction network to achieve an image decryption. In order to facilitate the data mining directly from the privacy-protected environment, a region of interest (ROI)-mining-network is proposed to extract the interested object from the encrypted image. The proposed DeepEDN is evaluated on the chest X-ray dataset. Extensive experimental results and security analysis show that the proposed method can achieve a high level of security with a good performance in efficiency

Jiang et al., (2020) proposed a Toward practical privacy-preserving processing over encrypted data in IoT: An assistive healthcare use case. Future Generation Computer Systems, 107(C), 229–237. With the advancement of Internet of Things (IoT), a large number of electronic devices are connected to the Internet. These connected electronic devices acquire and transmit information, and respond to any received actions. In the medical ecosystem, hospitals can implement medical diagnosis (MD) with medical sensors, especially for remote auxiliary MD. But, in this context, patients' privacy (PP) is of paramount importance, and confidentiality of medical data is crucial. Therefore, the main challenge ahead is how to realize remote auxiliary MD while protecting confidentiality of the medical data and ensuring PP. In this article, based on somewhat homomorphic encryption (SHE) scheme addressed by Junfeng Fan and Frederik Vercauteren (FV), we provide the first instance of a new efficient SHE schemes for homomorphic evaluation over single instruction multiple data (SIMD). We also implement a new set of efficient SIMD homomorphic comparison and division schemes. Based on these findings, we implement efficient privacy preserving and SIMD homomorphic surf and multiretina-image matching schemes.

Yan Qi et al., (2021) proposed a Secured data collection with hardware-based ciphers for IoT-based healthcare. IEEE Internet of Things Journal (Volume: 6, Issue: 1, February 2019) There are tremendous security concerns with patient health monitoring sensors in Internet of Things (IoT). The concerns are also realized by recent sophisticated security and privacy attacks, including data breaching, data integrity, and data collusion. Conventional solutions often offer security to patients' health monitoring data during the communication. However, they often fail to deal with complicated attacks at the time of data conversion into cipher and after the cipher transmission. In this paper, we first study privacy and security concerns with healthcare data acquisition and then transmission. Then, we propose a secure data collection scheme for IoT-based healthcare system named Secure Data with the aim to tackle security concerns similar to the above. Secure Data scheme is composed of four layers: 1) IoT network sensors/devices; 2) Fog layers; 3) cloud computing layer; and 4) healthcare provider layer. We mainly contribute to the first three layers. For the first two layers, Secure Data includes two techniques: 1) light-weight field programmable gate array (FPGA) hardware-based cipher algorithm and 2) secret cipher share algorithm.

N. Saranya et al., (2021) proposed a Secure and efficient data aggregation for IoT monitoring systems. IEEE Internet of Things Journal (Volume: 8, Issue: 10, 15 May 2021). The proliferation of Internet of Things (IoT) as a promising paradigm has contributed enormously to modern technology design. The wireless body sensor network (WBSN) technology is an application of IoT in healthcare, whereas data security and privacy impediments have raised some concerns. The collected data via IoT wireless body sensors is vulnerable to a variety of internal and external attacks. One solution is to encrypt or sign the collected data to provide confidentiality and integrity, but the computational complexity hinders the application in the real IoT-based healthcare devices.

III. PROPOSED SYSTEM

A secure lightweight medical image encryption approach is designed using compressive sensing and a modified seven-dimensional (MSD) hyperchaotic map. MSD is designed by modifying 7D hyperchaotic map to make it more dynamic and complex. The initial conditions for MSD are generated using SHA-512 which assures its sensitivity towards input

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308061|

images. Compressive sensing is further improved by using non-subsampled contourlet transform (NSCT) and measurement matrices are generated using the secret keys obtained from MSD. To generate encrypted images, the diffusion and per- mutation are carried out row and column-wise on com- pressed images using secret keys obtained from MSD. The statistical analysis of the proposed approach is performed using correlation coefficient, histogram analysis, and entropy is utilized to check the randomness of encrypted images. Entropy can be calculated globally as well as locally. The global entropy (GE) evaluates the randomness of the complete image at once. But the evaluation of local entropy (LE) is different than the GE. To evaluate the LE, firstly, an image is decomposed into blocks (Ib) that contain the fixed number of pixels (Fp). Then, each block's entropy is evaluated.

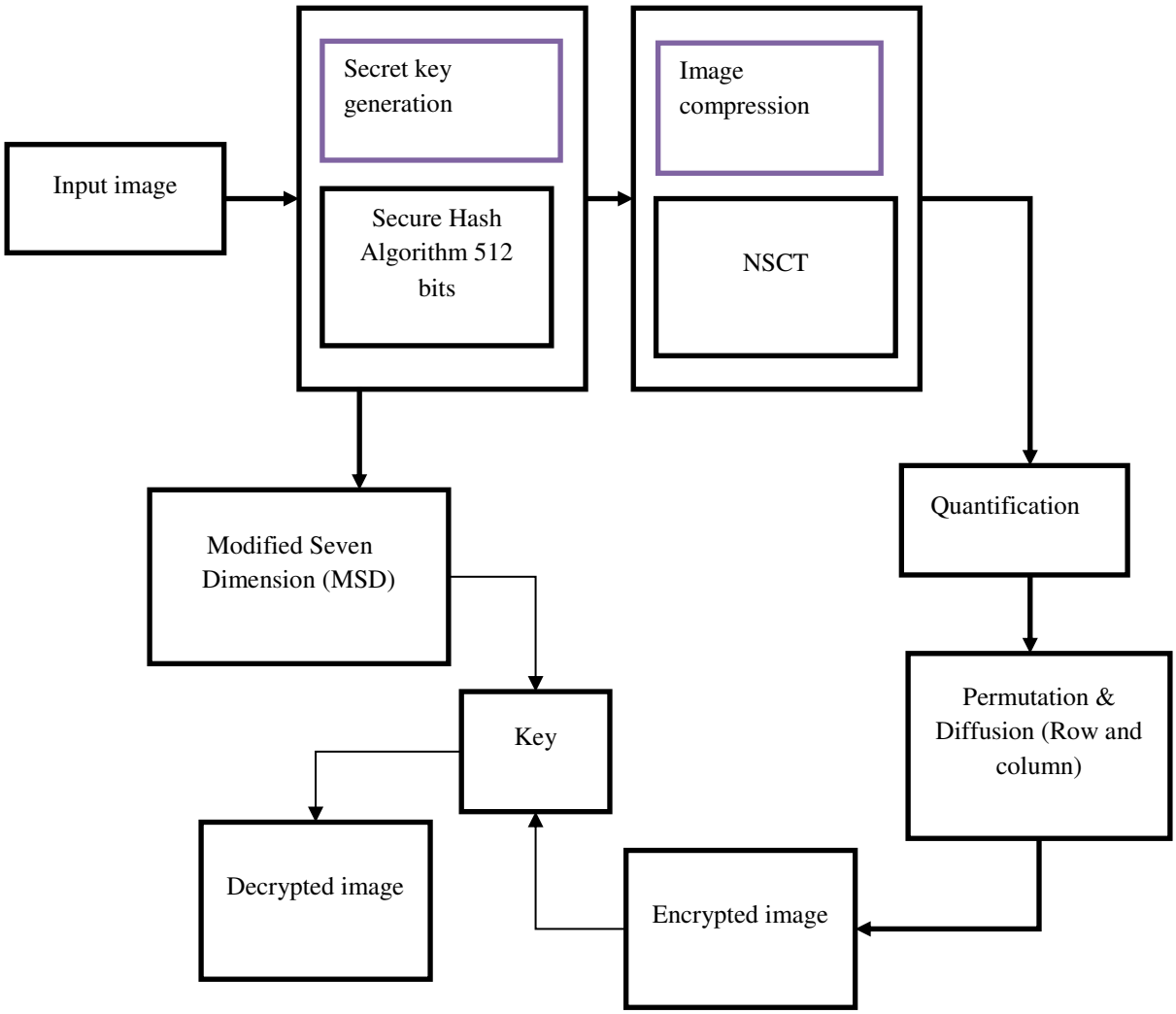

Fig 3.1 Block diagram

IV. RESULT AND DISCUSSION

The input image is biomedical images. These include magnetic resonance imaging (MRI), computed tomography (CT), positron emission tomography (PET), and ultrasound imaging. The input image is show in figure 4.1.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308061|

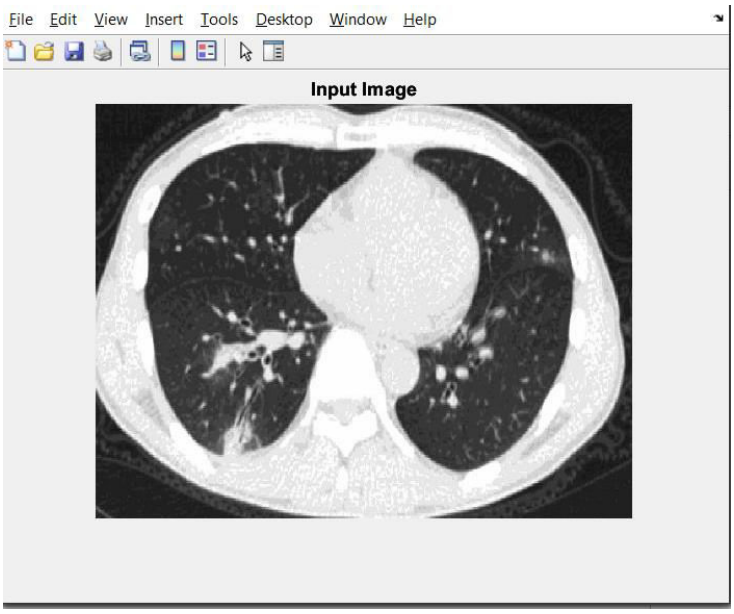

Fig. 4.1 Input image

The compression technique used in this project is NCST. The NSCT (Non-Subsampled Contourlet Transform) is a type of image transform that has been explored for image compression. The image is shown in the figure 4.2.

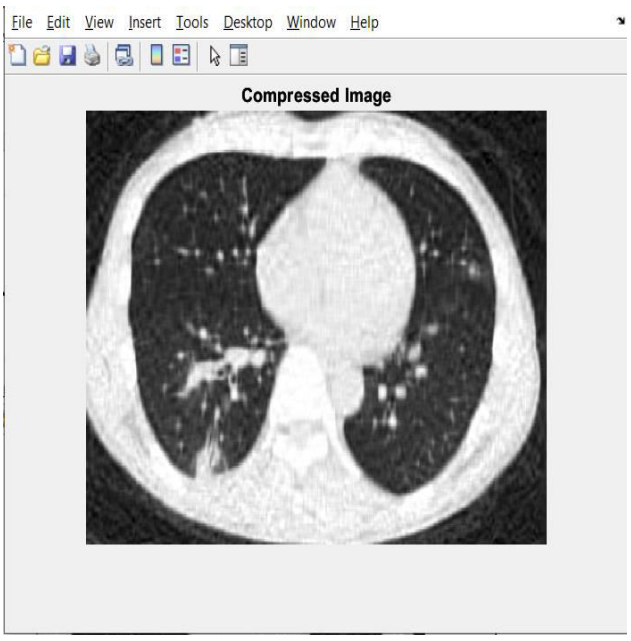

Fig 4.2 Compressed image

Quantization refers to the process of reducing the number of distinct colours or intensity levels in an image. This is typically done to reduce the amount of data required to represent the image or to simplify the image for further processing. The quantized image is shown in figure 4.3

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308061|

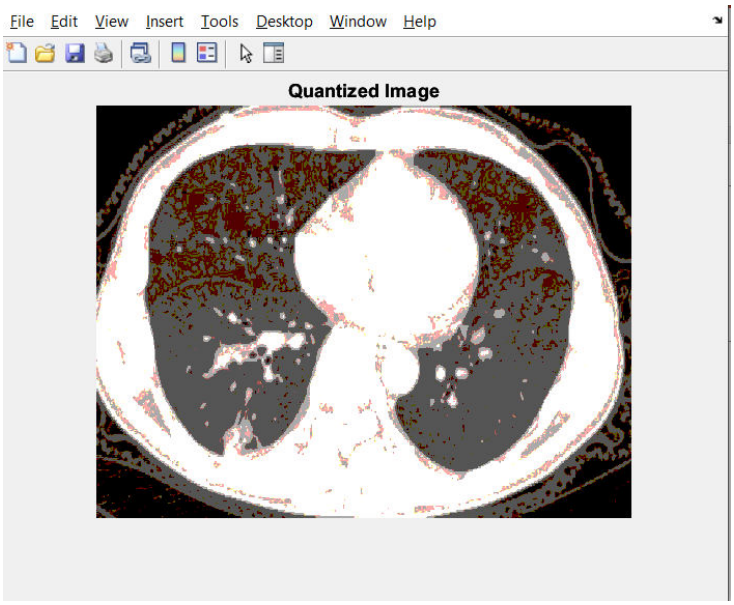

Fig 4.3 Quantized image

Permutation involves rearranging the pixels of an image according to a specific permutation key or algorithm. Diffusion is a technique used to embed a hidden information into the image. The image is shown in figure 4.4.

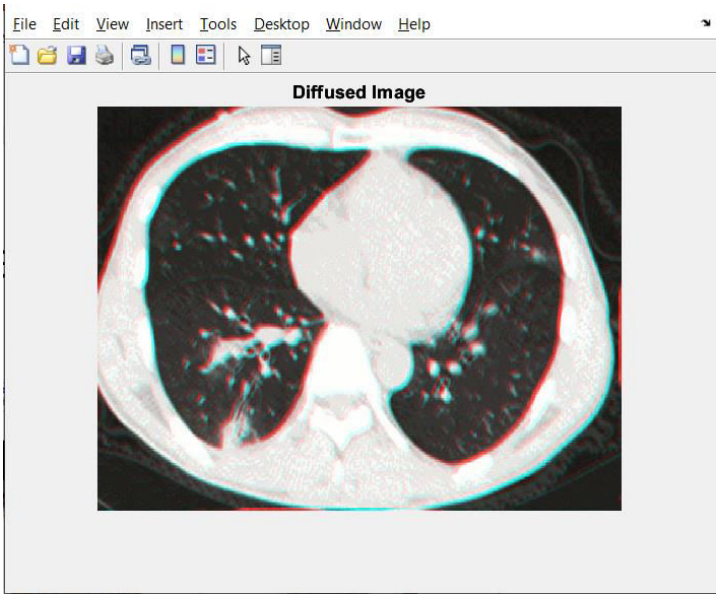

Fig 4.4 Diffused image

The image encryption approach is considered to be effective when it generates a random-like encrypted image. A random like encrypted image should not contain any pixel pattern like input biomedical. The encrypted image is shown in figure 4.5

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308061|

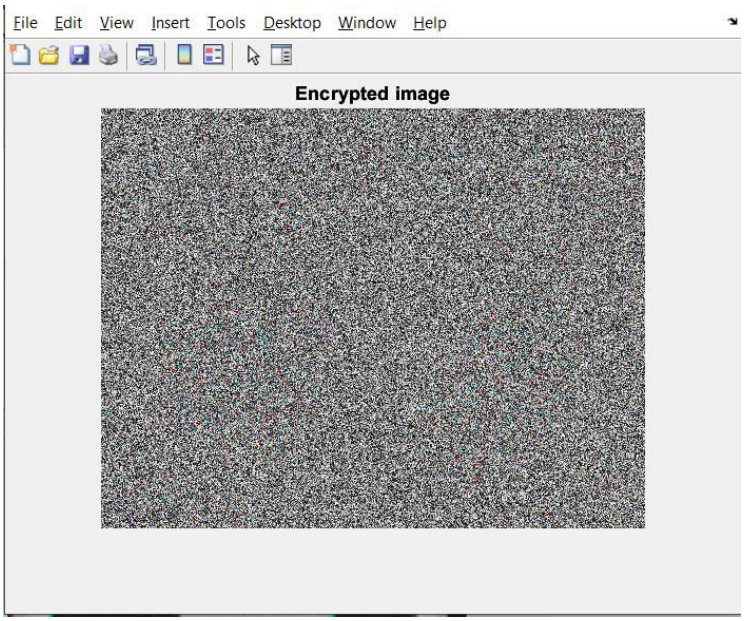

Fig 4.5 Encrypted image

An image histogram is a Gray-scale value distribution showing the frequency of occurrence of each Gray-level value. Histogram image is shown in figure 4.6.

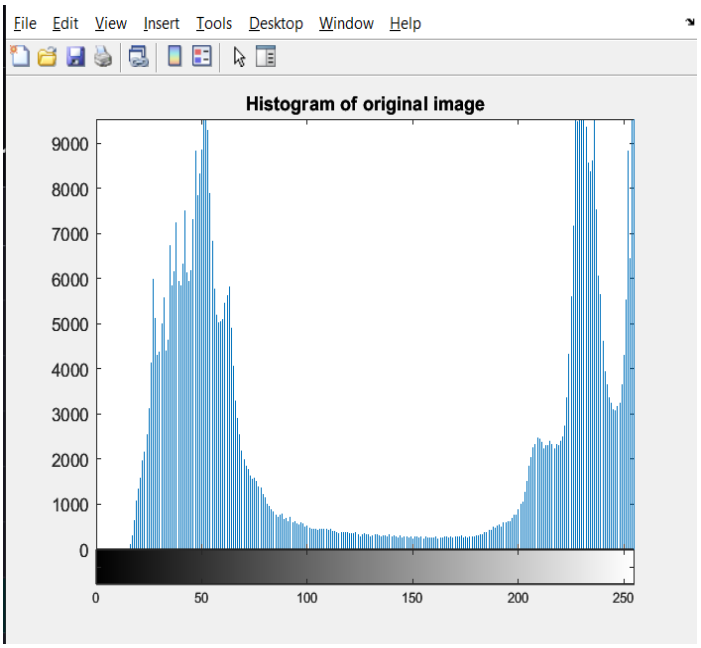

Fig 4.6 Histogram of original image

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308061|

Histograms are utilized to analyse the pixel distribution the histogram of encrypted image is shown in figure 4.7.

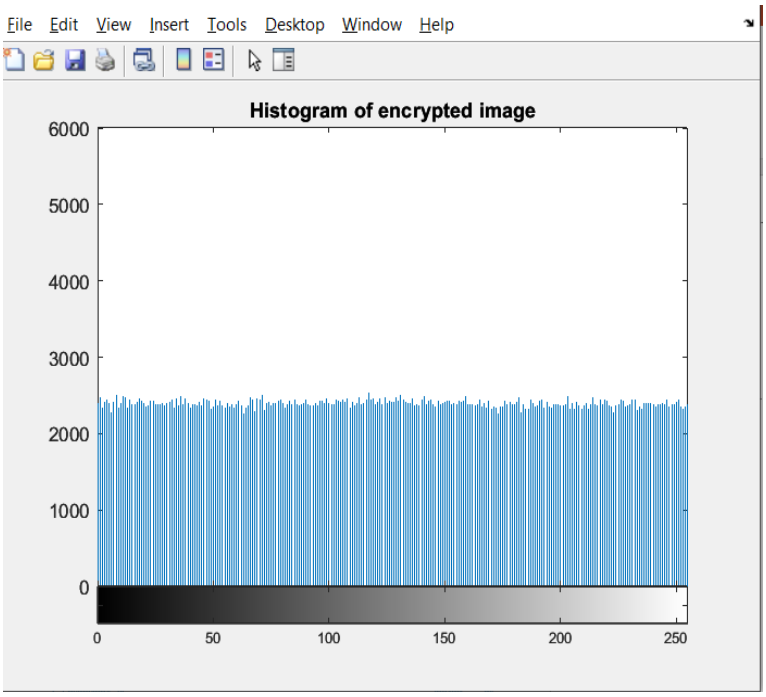

Fig 4.7 Histogram of encrypted image

The image is decrypted based on key generated. The decrypted image is shown in figure 4.8.

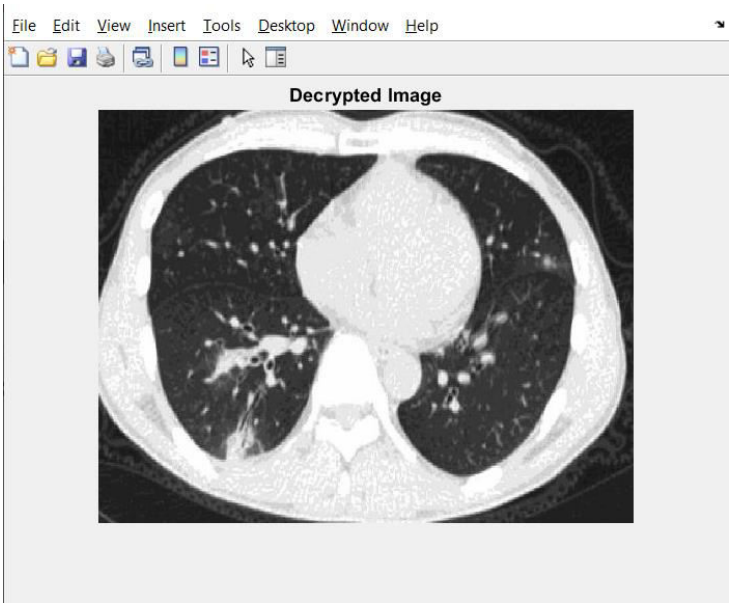

Fig 4.8 Decrypted image

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308061|

V. CONCLUSION AND FUTURE WORK

In MIoT networks, a large number of biomedical images are transmitted over Internet for their storage and analysis on cloud servers. Due to this, biomedical images are vulnerable to numerous security vulnerabilities. Hence, a lightweight biomedical image encryption approach was developed using MSD and compressive sensing. MSD was designed by modifying 7D hyperchaotic map to make it more dynamic and complex. The initial conditions for MSD were generated using SHA-512 which enforce the sensitivity of proposed approach to input images. Compressive sensing was improved by using NSCT and measurement matrices were generated using the secret keys obtained from MSD. Finally, to generate encrypted images, the diffusion and permutation were carried out row and column-wise on compressed images using secret keys obtained from MSD.

The performance analysis proved that the proposed lightweight encryption achieved better performance in terms of robustness, security, and computational speed as compared to the existing approaches. The future work will be focusing on the implementation of hyper chaotic encryption algorithms on the real time medical images.

REFERENCES

[1] L. Bao et al., ‘‘Combination of sharing matrix and image encryption for lossless (k, n)-secret image sharing,’’ IEEE Trans. Image Process., vol. 26, no. 12, pp. 5618–5631, Dec. 2017.
[2] Y. Ding et al., ‘‘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.
[3] B. Ferreira et al., ‘‘Practical privacy preserving content-based retrieval in cloud image repositories,’’ IEEE Trans. Cloud Compute., vol. 7, no. 3, pp. 784–798, Jul. 2019.
[4] V. Itier, et al., ‘‘Recompression of JPEG crypto compressed images without a key,’’ IEEE Trans. Circuits Syst. Video Technol., vol. 30, no. 3, pp. 646–660, Mar. 2020.
[5] L. Jiang et al., ‘‘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.
[6] M. Khari et al., ‘‘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.
[7] K. Lee et al., ‘‘Digital image sharing by diverse image media,’’ IEEE Trans. Inf. Forensics Security, vol. 9, no. 1, pp. 88–98, Jan. 2014.
[8] K. Muhammad et al., ‘‘Secure surveillance framework for IoT systems using probabilistic image encryption,’’ IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3679–3689, Aug. 2018.
[9] F. Rezaeibagha et al., ‘‘Secure and efficient data aggregation for IoT monitoring systems,’’ IEEE Internet Things J., vol. 8, no. 10, pp. 8056–8063, May 2021.
[10] M. Sasaki et al., ‘‘Visual secret sharing schemes encrypting multiple images,’’ IEEE Trans. Inf. Forensics Security, vol. 13, no. 2, pp. 356–365, Feb. 2018.
[11] H. Tao et al., ‘‘Secured data collection with hardware-based ciphers for IoT-based healthcare,’’ IEEE Internet Things J., vol. 6, no. 1, pp. 410–420, Feb. 2019.
[12] D. Wang et al., ‘‘Optimal contrast grayscale visual cryptography schemes with reversing,’’ IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 2059–2072, Dec. 2013.
[13] T. Xiang et al., ‘‘Visual security evaluation of perceptually encrypted images based on image importance,’’ IEEE Trans.Circuits Syst. Video Technol., vol. 30, no. 11, pp. 4129–4142, Nov. 2020.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details