Efficient Lossless Medical Image Encryption with Adaptive QCNN and Secure ROI Management for Real-Time Applications

Shaik Neelofar, Dr.N Lakshmi Prasanna, Dr. Ramachandran Vedantam
PG Student, Department of Computer Science and Engineering, VVIT, Guntur, India
Assistant Professor, Department of Computer Science and Engineering, VVIT, Guntur, India
Professor, Department of Computer Science and Engineering, VVIT, Guntur, India

Abstract: **Medical images, which often contain highly sensitive patient data, require effective encryption methods to safeguard against unauthorized access, tampering, or theft. A key challenge in this area is protecting the Region of Interest (ROI)—which holds critical diagnostic data—without degrading the image quality or revealing the location of the ROI during transmission. Many existing encryption techniques struggle to find an optimal balance between security and computational efficiency, especially when handling large medical datasets in real-time environments, such as hospitals. Moreover, ensuring accurate ROI detection and securely managing its position are essential to provide comprehensive protection. Recent methods have leveraged Quantum Cell Neural Network (QCNN) hyperchaotic systems and game theory to encrypt medical images. These approaches focus on pixel-level transformations of the ROI to enable lossless recovery and conceal the ROI's position to prevent exposure. While these methods improve security and accuracy, they introduce substantial computational complexity, making them difficult to deploy in time-sensitive, real-time settings. Additionally, the reliance on precise ROI detection increases the risk of misidentifying critical regions, and the need to conceal the ROI's position further increases data overhead, which can affect transmission efficiency. In response to these challenges, we propose a solution that combines lightweight encryption for non-sensitive regions of the image with adaptive QCNN-based encryption for the ROI, significantly reducing computational load. To improve ROI detection accuracy and reliability, we incorporate machine learning-based techniques and multi-modal image fusion. To manage the hidden position of the ROI, we employ lossless data embedding and differential privacy methods, minimizing overhead and securing the position data without compromising the efficiency of transmission. This integrated approach offers an optimal trade-off between encryption speed, security, and accuracy, making it well-suited for real-time medical applications. This novel encryption scheme ensures the privacy of medical images while enabling their lossless recovery after decryption, providing a comprehensive and secure solution for the protection of sensitive patient information in medical imaging systems.**

Keywords: **Medical Image Encryption, Region of Interest (ROI) Protection, Quantum Cell Neural Network (QCNN), Lossless Encryption, Sensitive Patient Data, Real-Time Medical Applications, Game Theory Optimization, Machine Learning-Based ROI Detection**

1. INTRODUCTION

Medical images have become an indispensable part of modern healthcare, enabling clinicians to diagnose, monitor, and treat patients effectively. These images, often generated through technologies such as X-rays, MRIs, and CT scans, provide critical visual insights into a patient's health status. However, the sensitive nature of the data contained within these images necessitates robust security measures to protect patient privacy and ensure data integrity. Unauthorized access, tampering, or theft of medical image data can result in severe consequences, including compromised patient care, legal liabilities, and breaches of confidentiality. One of the most significant challenges in medical image encryption is safeguarding the Region of Interest (ROI). The ROI represents the specific part of the image that holds critical diagnostic information, such as abnormalities, tumours, or key organs. Protecting the ROI is vital, but it must be done without compromising the image's quality, as any loss of image data could negatively affect clinical decision-making. Additionally, ensuring the secure transmission of medical images—particularly the ROI—presents another layer of complexity, as image transmission often occurs over networks with varying levels of bandwidth, and any delay can compromise timely diagnosis and treatment. Existing encryption techniques for medical images primarily focus on

securing the entire image. Methods such as Quantum Cell Neural Networks (QCNN) with hyperchaotic systems and approaches based on game theory have been proposed to enhance the security of these images, offering pixel-level transformations that protect the ROI from unauthorized access. Despite their effectiveness, these techniques often introduce significant computational challenges, requiring high processing power and time, which makes their use in real-time healthcare environments—such as hospitals and emergency care settings—difficult. Furthermore, these approaches may struggle with the management of hidden ROI positions within an image, as securely embedding this information without adding excessive data overhead or compromising transmission efficiency is a key challenge. The goal of this paper is to address these challenges by introducing a novel encryption scheme that ensures the security and confidentiality of sensitive medical image data, particularly the ROI, while also maintaining computational efficiency and facilitating real-time applicability. The proposed scheme integrates several innovative features, including hybrid encryption, machine learning-based ROI detection, and differential privacy to provide a comprehensive solution for medical image protection. Our approach leverages lightweight encryption for non-sensitive regions of the image, reducing computational burden, while applying an adaptive, hardware accelerated QCNN encryption to the ROI to ensure strong protection for the critical areas without excessive resource consumption. Additionally, machine learning algorithms are employed to detect the ROI with high accuracy, reducing the risks associated with misidentifying sensitive regions. To address the challenge of securely managing the hidden position of the ROI, the proposed method utilizes lossless data embedding and differential privacy to maintain the confidentiality of the ROI's location without compromising transmission performance. This hybrid approach aims to strike a balance between speed, security, and accuracy, making it highly suitable for real-time medical applications. By ensuring the lossless recovery of encrypted images, our scheme preserves the diagnostic value of the images, making it a viable solution for secure, efficient, and accurate handling of medical image data in healthcare environments. In summary, this research presents a comprehensive solution to the challenges faced by existing encryption methods, particularly in terms of computational complexity, ROI detection, and real-time applicability. By addressing these limitations, we aim to enhance the security of medical image data while facilitating faster and more efficient image transmission, critical for timely decision-making in clinical settings.

2. LITERATURE SURVEY

Basit et.al [1] integrated Singular Value Decomposition (SVD) and the Discrete Wavelet Haar Transformation (DWT) for data embedding, while encryption is performed using a standard cipher key. At the recipient's end, the embedded image and concealed data are retrieved using SVD, DWT, and the encryption key. Comprehensive simulations conducted in MATLAB evaluate performance metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Bit Error Rate (BER), and robustness under various conditions. The results demonstrate the effectiveness of our method in ensuring both data imperceptibility and robustness, making it a promising solution for secure data embedding in medical imaging.

Magdy et.al [2] provides a comprehensive review of current approaches to ensuring medical data security and highlights the challenges associated with these methods. It offers a detailed examination of security techniques, including cryptography, steganography, and watermarking, along with an extensive survey of recent advancements in these areas. The paper aims to evaluate and compare various algorithms within these approaches based on key performance metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Bit Error Rate (BER), and Normalized Correlation (NC).

Zerva et.al [3] introduces an advanced medical image compression technique based on color wavelet difference reduction. The method extends the traditional wavelet difference reduction (WDR) approach by employing the mean co-located pixel difference to determine the optimal set of color images with the highest spatial and temporal similarity. Images with significant spatiotemporal coherence are grouped and encoded as a single volume, with performance evaluated using Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM). The proposed technique is applied in the field of histopathological microscopy image analysis, utilizing 31 colorectal cancer slides. Results demonstrate exceptionally high perceptual quality, with PSNR improvements of up to 22.65 dB

over JPEG 2000 and up to 10.33 dB compared to a discrete wavelet transform (DWT)-based method. This advancement supports the development of a mobile and web-based platform for real-time compression and transmission of microscopic medical images.

Rajesh et.al [4] proposed a model that integrates the reversible data hiding with visual cryptography to ensure the secure exchange of medical images. Using a Hadamard matrix, the cover image is divided into non-overlapping secret shares. A secret Digital Imaging and Communications in Medicine (DICOM) image is encoded through a deep learning model and embedded within these secret shares to facilitate secure sharing. The DICOM image and cover image can then be fully recovered without any loss. Visual cryptography is employed to protect the embedded secret shares. Performance metrics such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Normalized Correlation (NC) are analyzed and compared with existing research to assess the effectiveness of the proposed method.

Tamboli et.al [5] proposed framework begins with image segmentation, achieved using an Optimized Active Contour Model (OACM). The segmentation process is fine-tuned with a Modified Marriage in Honey Bees Optimization (MMBO) algorithm, which adjusts the weighting factor and maximum iterations of the Active Contour Model. This segmentation divides the input image into regions of interest (ROI) and non-ROI areas. The ROI regions are encoded using an ISPIHT-based lossy compression method, while the non-ROI areas are compressed using a DCT-based lossy compression technique. The outputs of both the ISPIHT algorithm and the DCT model are then combined to produce the compressed image. During decompression, bit streams are segregated and processed separately for ROI and non-ROI areas using an ISPIHT decoder and DCT decompression. This process reconstructs the original image. Comparative analysis indicates that the proposed method outperforms existing techniques in terms of PSNR, SSIM, and compression ratio (CR). The PSNR improvement of the proposed model is approximately 0.22, translating to performance enhancements of 26%, 50%, 60%, and 55% over traditional methods such as MFO, LA, MBO, and JCF-LA, respectively.

Shafai et.al [6] introduces a robust cryptosystem for securing medical images by leveraging the combined strengths of deoxyribonucleic acid (DNA) encoding and chaotic maps. The proposed system employs a logistic chaos map, a piecewise linear chaotic map (PWLCM), and DNA rules. The PWLCM generates a secret key image, which is then encoded using DNA rules alongside the input plain image, processed row by row with the logistic chaos map. Subsequently, a logistic map creates an intermediate image that acts as an additional secret key to apply DNA operations row-by-row on the encoded image. This intermediate image undergoes decoding, and the process is repeated column-wise to achieve optimal encryption. Experimental results demonstrate that the proposed cryptosystem ensures high security, efficient processing, and strong resistance against various attacks, including known-plaintext and chosen-plaintext attacks.

Chen et.al [7] presents WMNet, a deep learning-based model designed for accurate identification of watermark copyrights. Traditionally, building deep learning models required extensive amounts of training data. To address this, WMNet utilizes a simulated process to generate numerous distorted watermarks, creating a comprehensive training dataset. However, not all watermarks in the dataset effectively provide copyright information. To enhance learning, the dataset is categorized based on predefined criteria, enabling WMNet to focus on extracting and identifying copyright information embedded in the watermarks. Even when the retrieved watermark data is partially incomplete, the model can still interpret the copyright details accurately and objectively. The experimental results confirm that the proposed approach is both efficient and effective for copyright verification.

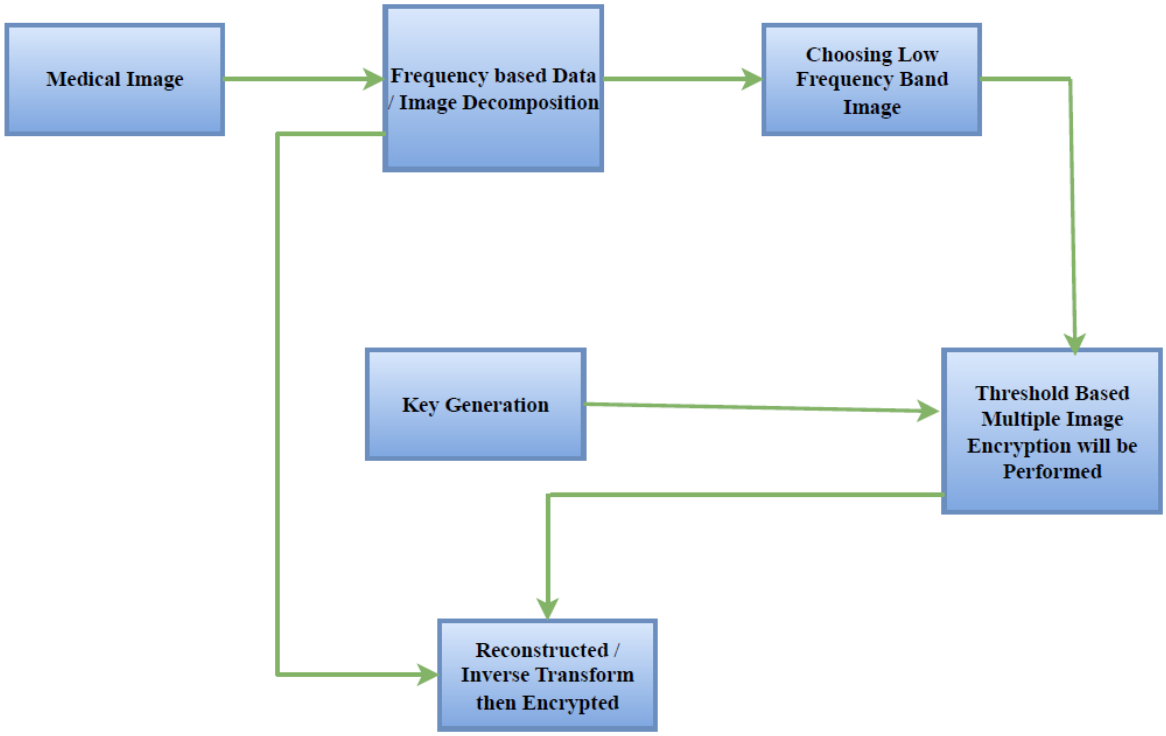
Afthab et.al [8] developed an ROI-based compression method for MR images that effectively addresses the frequency components within the medical image. The Fuzzy C-Means clustering technique is utilized to differentiate the region of interest (ROI) from the non-region of interest (non-ROI). Compression of the non-ROI is achieved using a capsule autoencoder, while the ROI is compressed using Discrete Cosine Transform (DCT) combined with Huffman Run-length encoding. The compression process is evaluated using metrics such as Peak Signal-to-Noise Ratio (PSNR) and Compression Ratio (CR). The analysis demonstrates that the proposed approach outperforms existing methods, offering enhanced performance.

Zhou et.al [9] introduces a novel lossless medical image encryption method that leverages game theory

with optimized ROI parameters and concealed ROI positions. During encryption, the ROI undergoes pixel-level transformation to ensure the image can be fully decrypted without any loss, safeguarding the integrity of medical image information. Simultaneously, the position of the ROI is effectively concealed, preventing any leakage of location data during transmission. Additionally, a quantum cellular neural network (QCNN) hyperchaotic system generates random sequences to scramble and diffuse the ROI, enhancing security. A quantitative analysis of ROI parameters is conducted, utilizing game theory to achieve an optimal balance between encryption speed and security performance. Simulation results and numerical evaluations confirm that the proposed approach provides efficient, lossless encryption and decryption, offering robust and adaptable protection for medical images of varying types and structures against different attacks.

Sreenivasulu et.al [10] presents a lossless medical image compression technique based on wavelet transform and advanced encoding methods. The system is divided into three key stages: (i) segmentation, (ii) image compression, and (iii) image decompression. Initially, the input medical image is segmented into the region of interest (ROI) and non-region of interest (non-ROI) using an enhanced region growing algorithm. The ROI is then compressed using the discrete cosine transform (DCT) combined with set partitioning in hierarchical tree (SPIHT) encoding, while the non-ROI is compressed using discrete wavelet transform (DWT) with a merging-based Huffman encoding technique. The final compressed image is formed by merging the compressed ROI and non-ROI. During decompression, the original image is reconstructed by reversing the compression process. Experimental evaluations conducted on various medical images demonstrate that the proposed method delivers superior performance compared to other existing techniques.

3. METHODOLOGY



The block diagram discribes a secure encryption process specifically designed for medical images. The process begins by breaking down the medical image into its frequency components through a decomposition technique, such as a Fourier or wavelet transform. From these components, the low-frequency band—representing the most critical and informative part of the image—is selected for further processing. Next, a cryptographic key is generated, which serves as the foundation for the encryption process. Using a threshold-based multiple image encryption method, the selected low-frequency band is securely encrypted. This technique ensures that the most vital portions of the medical image are

adequately protected. Following the encryption of the low-frequency band, the encrypted data is reconstructed to reassemble the image. To strengthen security further, an additional layer of encryption is applied to the reconstructed image, creating a multi-tiered security framework. This layered approach is designed to protect sensitive medical information from unauthorized access while ensuring data integrity and confidentiality.

4. PARAMETERS

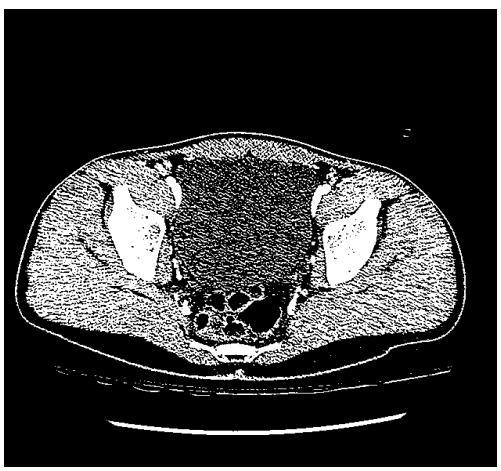
Sl.No	Parameter	Formula
1	Mean Square Error (MSE)	$\frac{1}{n}\sum_{i=1}^{n}\left(Y_i - \hat{Y}_i\right)^2$
2	Peak Signal to Noise Ratio (PSNR)	$10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$
3	Structural similarity Structural similarity index measure (SSIM)	S S I M (x, y) = [l (x, y)] α · [c (x, y)] β · [s (x, y)] γ where
4	Entropy	$\Delta S_{system} = \frac{q_{rev}}{T}$

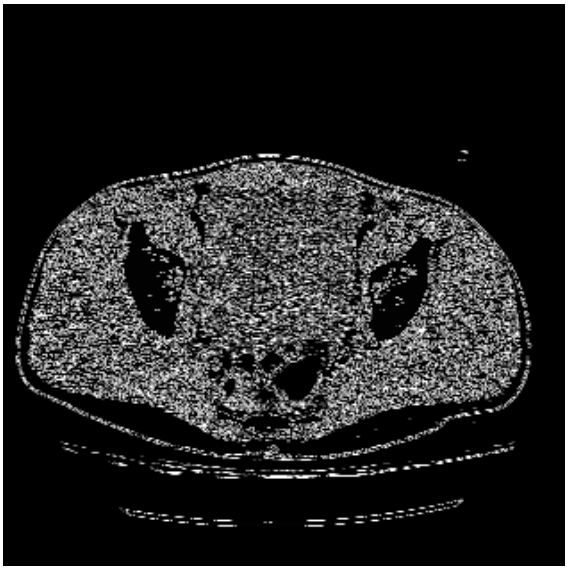
5 PERFORMANCE ANALYSIS

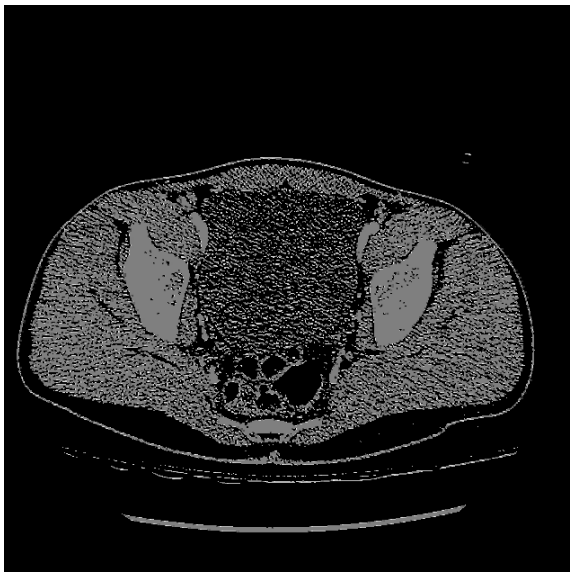
Sl.No	Parameter	Existing	Extension
1	Mean Square Error (MSE)	8.68	6.7
2	Peak Signal to Noise Ratio (PSNR)	32.46	42.85
3	Structural similarity Structural similarity index measure (SSIM)	8.632	8.97
4	Entropy	7.2	7.56

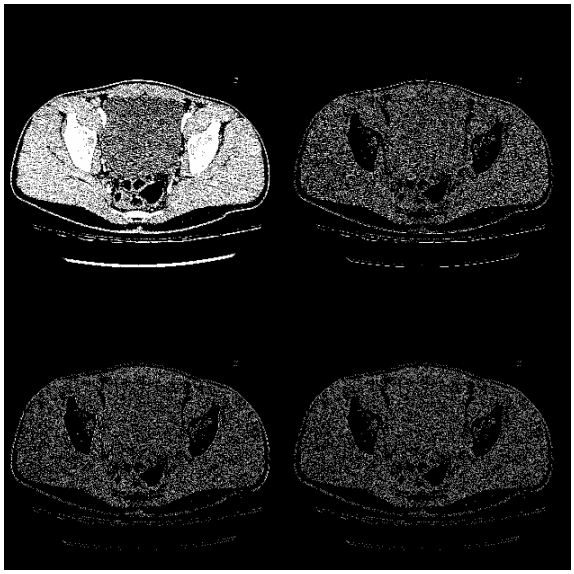
4. RESULTS

Metric	Existing Approach	Proposed Approach
MSE	High (due to image degradation and encryption artifacts)	Low (lossless recovery with hybrid encryption)
PSNR	Low (degradation due to pixel-level encryption)	High (due to lossless recovery and high-quality encryption)
SSIM	Low (visible distortion due to pixel-level encryption)	High (structural similarity maintained)
Entropy	High (increased randomness due to encryption)	High (due to encryption, but more balanced)









CONCLUSION

In conclusion, the proposed medical image encryption scheme offers a comprehensive solution to the complex challenge of protecting sensitive patient data while ensuring efficient real-time processing in healthcare environments. By combining lightweight encryption for non-sensitive image regions with adaptive Quantum Cell Neural Network (QCNN)-based encryption for critical Regions of Interest (ROI), this approach significantly reduces computational overhead and accelerates encryption times. Additionally, the integration of machine learning for accurate ROI detection, coupled with multi-modal image fusion, ensures precise identification of sensitive areas without compromising diagnostic quality. The use of differential privacy and lossless data embedding techniques for managing ROI positions further enhances security and transmission efficiency, making the system suitable for real-time applications in resource-constrained healthcare settings. With its focus on security, computational efficiency, and lossless image recovery, the proposed approach offers a scalable, practical solution for protecting patient privacy while maintaining high standards of care in modern healthcare systems.

FUTURE SCOPE

The future scope of medical image encryption, especially concerning the protection of Regions of Interest (ROIs), is highly promising as advancements in AI, quantum computing, and cryptography continue to evolve. The proposed hybrid encryption

model offers significant improvements in real-time healthcare settings by balancing the need for robust security with the practical constraints of computational efficiency. As AI-driven techniques for ROI detection and machine learning-based encryption methods mature, the accuracy and speed of identifying sensitive image regions will improve, minimizing the risk of data leakage while reducing processing times. Moreover, ongoing research into quantum-safe encryption methods, along with the integration of blockchain for secure data sharing, could further enhance the privacy and integrity of medical images. The scalability of such systems, along with their adaptability to various medical imaging modalities (MRI, CT, etc.), will enable widespread adoption across healthcare facilities, making real-time secure image transmission a reality. Furthermore, the integration of differential privacy and lightweight encryption methods can help address current challenges related to data overhead, transmission efficiency, and compliance with global privacy regulations, ultimately supporting more efficient and secure healthcare practices in the future.

REFERENCES

[1] Basit, A., Toor, W. T., Saadi, M., Maroof, N., Khan, S. A., & Otaibi, S. A. (2023). Reversible encryption and lossless data hiding for medical imaging aiding smart health care. Cluster Computing, 26(5), 2977-2991.

[2] Magdy, M., Hosny, K. M., Ghali, N. I., & Ghoniemy, S. (2022). Security of medical images for telemedicine: a systematic review. Multimedia Tools and Applications, 81(18), 25101-25145.

[3] M. C. H. Zerva, V. Christou, N. Giannakeas, A. T. Tzallas and L. P. Kondi, "An Improved Medical Image Compression Method Based on Wavelet Difference Reduction," in IEEE Access, vol. 11, pp. 18026-18037, 2023, doi: 10.1109/ACCESS.2023.3246948

[4] Rajesh Kumar, N., Bala Krishnan, R., Manikandan, G., Subramaniyaswamy, V., & Kotecha, K. (2022). Reversible data hiding scheme using deep learning and visual cryptography for medical image communication. Journal of Electronic Imaging, 31(6), 063028-063028.

[5] Tamboli, S. S., Butta, R., Jadhav, T. S., & Bhatt, A. (2023). Optimized active contor segmentation model for medical image compression. Biomedical Signal Processing and Control, 80, 104244.

[6] El-Shafai, W., Khallaf, F., El-Rabaie, E. S. M., & El-Samie, F. E. A. (2021). Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. Journal of Ambient Intelligence and Humanized Computing, 12, 9007-9035.

[7] Chen, Y. P., Fan, T. Y., & Chao, H. C. (2021). Wmnet: A lossless watermarking technique using deep learning for medical image authentication. Electronics, 10(8), 932.

[8] B. P.V. and J. Afthab, "Region of Interest Based Medical Image Compression Using DCT and Capsule Autoencoder for Telemedicine Applications," 2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT), Erode, India, 2021, pp. 1-7, doi: 10.1109/ICECCT52121.2021.9616748.

[9] J. Zhou, J. Li and X. Di, "A Novel Lossless Medical Image Encryption Scheme Based on Game Theory With Optimized ROI Parameters and Hidden ROI Position," in IEEE Access, vol. 8, pp. 122210-122228, 2020, doi: 10.1109/ACCESS.2020.3007550.

[10] Sreenivasulu, P., & Varadarajan, S. (2019). An efficient lossless ROI image compression using wavelet-based modified region growing algorithm. Journal of Intelligent Systems, 29(1), 1063-1078.