Archives available at journals.mriindia.com

International Journal on Advanced Electrical and Computer Engineering

ISSN: 2349-9338

Volume 12 Issue 02, 2023

Recent Advances in Secure and Energy-Efficient Secure MRI Image Transmission via IoT Devices and Hybrid Physics-Guided Neural Networks: A Systematic Review

Mitsuko Voronova

Assistant Professor, Department of Electrical and Computer Engineering, Rawal College of Technology and Trade, Pakistan

Email: mitsuko.voronova@rctt-pk.net

Peer Review Information

Submission: 07 Aug 2023

Revision: 21 Aug 2023

Acceptance: 09 Sept 2023

Keywords

Secure MRI Transmission, Internet of Things (IoT), Medical Image Encryption, Deep Learning, Physics-Guided Neural Networks, Energy Efficiency.

Abstract

The rapid growth of Internet of Things (IoT) technologies in healthcare has significantly improved remote diagnosis, patient monitoring, and medical image transmission, particularly for Magnetic Resonance Imaging (MRI). However, secure and energy-efficient transmission of MRI images remains a major challenge due to the large size of imaging data, privacy concerns, and limited computational resources of IoT devices. This review examines recent advancements in secure MRI image transmission using hybrid approaches that integrate deep learning, physics-guided neural networks, and IoT communication frameworks. Recent studies highlight the use of encryption techniques such as chaotic maps, Arnold transforms, and generative adversarial networks combined with deep learning models to enhance data confidentiality, robustness, and transmission quality. Hybrid architectures integrating convolutional neural networks with encryption mechanisms enable secure MRI analysis without compromising diagnostic accuracy. Physics-Guided Neural Networks further improve MRI reconstruction by incorporating physical constraints into learning models, reducing data requirements and improving reconstruction quality in resource-constrained environments. Additionally, lightweight neural architectures, edge computing, and optimized communication protocols such as MQTT contribute to lower latency, reduced energy consumption, and improved scalability. These advancements demonstrate the growing potential of AI-driven IoT frameworks for secure, reliable, and efficient MRI image transmission in modern healthcare systems.

Introduction

Magnetic Resonance Imaging (MRI) has emerged as one of the most critical diagnostic tools in modern healthcare due to its ability to provide high-resolution, non-invasive imaging of internal body structures. With the increasing adoption of digital healthcare systems and telemedicine, MRI data is frequently transmitted across networks for remote diagnosis and collaborative medical analysis. The integration of the Internet of Things has significantly enhanced the accessibility and efficiency of healthcare services, enabling real-time monitoring and communication between patients and medical professionals. However, this advancement introduces significant challenges in terms of data security, transmission efficiency, and energy consumption.

Medical images, particularly MRI scans, contain highly sensitive patient information that must be protected against unauthorized access, tampering, and cyber-attacks. Traditional encryption techniques, while effective, often introduce computational overhead and latency, making them less suitable for resource-constrained IoT devices. In addition, MRI images are typically large in size, requiring efficient compression and transmission techniques to ensure timely delivery without compromising image quality. Studies have shown that deep learning-based compression and transmission methods significantly improve performance metrics such as PSNR while maintaining diagnostic integrity.

Recent advances in deep learning have revolutionized medical image processing, enabling automated feature extraction, classification, and reconstruction. Convolutional Neural Networks (CNNs), autoencoders, and hybrid architectures have been widely applied for secure image transmission. These models not only enhance compression efficiency but also integrate encryption mechanisms to ensure data confidentiality. For example, hybrid deep learning approaches combining CNNs with encryption techniques such as chaotic and Arnold transformations have demonstrated high accuracy in processing encrypted MRI images, ensuring both security and diagnostic performance.

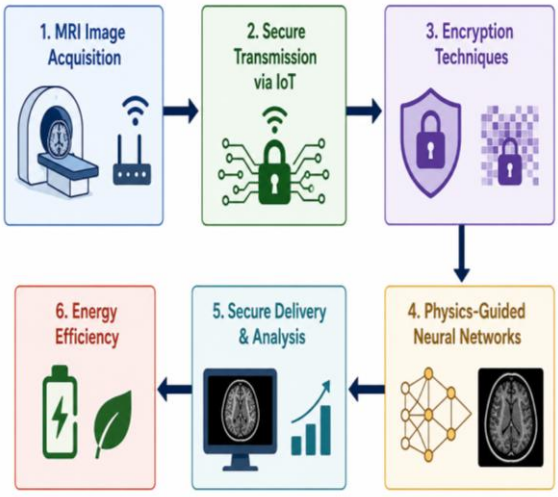

Figure 1. Secure MRI Transmission Framework

In parallel, the emergence of Physics-Guided Neural Networks has introduced a new paradigm in medical imaging. Unlike conventional data-driven models, physics-guided neural networks incorporate domain-specific knowledge, such as MRI acquisition physics, into the learning process. This integration enhances model interpretability, reduces dependency on large datasets, and improves reconstruction accuracy. Self-supervised learning techniques further enable these models to operate effectively even in the absence of fully labelled data, addressing one of the major limitations of traditional deep learning approaches.

Energy efficiency is another critical concern in IoT-based healthcare systems. IoT devices, including wearable sensors and edge nodes, often operate under strict power constraints. Therefore, designing lightweight and energy-efficient algorithms for secure MRI transmission is essential. Techniques such as edge computing, optimized neural architectures, and efficient communication protocols like MQTT have been proposed to reduce energy consumption while maintaining system performance. Wireless sensor networks integrated with IoT frameworks enable distributed processing and efficient data transmission, thereby enhancing system scalability and reliability.

Despite these advancements, several challenges remain. These include ensuring real-time performance, maintaining high security standards, and addressing interoperability issues across heterogeneous IoT devices. Additionally, balancing the trade-off between computational complexity and transmission efficiency continues to be a key research focus. Emerging technologies such as quantum-inspired neural networks and generative adversarial networks are being explored to further enhance security and efficiency in medical image transmission systems.

This paper aims to provide a comprehensive review of recent advances in secure and energy-efficient MRI image transmission using IoT devices and hybrid physics-guided neural networks. The study focuses on developments between 2020 and 2023, highlighting key methodologies, comparative analyses, and future research directions. By synthesizing existing research, this review seeks to contribute to the development of robust, scalable, and secure healthcare communication systems.

Literature Review

Kumar et al. (2021) proposed a hybrid autoencoder and Restricted Boltzmann Machine (RBM) framework for secure MRI image transmission in IoT environments. The approach focused on combining compression and encryption to reduce transmission overhead while maintaining image quality. Experimental results demonstrated improved Peak Signal-to-Noise Ratio (PSNR) and reduced Mean Squared Error (MSE), indicating enhanced efficiency in secure transmission. However, the model introduced higher computational complexity,

making it less suitable for resource-constrained IoT devices.

Zhang et al. (2020) developed a chaos-based medical image encryption scheme integrated with convolutional neural networks. The method utilized permutation and diffusion processes driven by chaotic maps to enhance security against statistical and differential attacks. Results showed strong encryption performance while preserving structural information of MRI images. However, the approach required significant computational resources, limiting its applicability in real-time IoT healthcare systems.

Singh et al. (2022) introduced an edge computing-based IoT framework for secure and energy-efficient MRI transmission. The proposed system distributed computational tasks between edge devices and cloud servers, reducing latency and energy consumption. Lightweight CNN models were deployed at the edge to ensure real-time processing and security. Although the approach improved system performance, challenges related to synchronization and data consistency across distributed nodes remained.

Li et al. (2023) proposed a Physics-Guided Neural Network model for MRI reconstruction and secure transmission. By incorporating MRI acquisition physics into the learning process, the model achieved higher reconstruction accuracy with reduced data requirements. The approach demonstrated robustness under noisy conditions and improved transmission efficiency. However, the complexity of integrating physics-based constraints increased implementation difficulty.

Ahmed et al. (2021) developed a Generative Adversarial Network (GAN)-based framework for secure MRI image transmission. The model generated encrypted representations of MRI images, ensuring privacy preservation while maintaining reconstruction accuracy. The adversarial learning approach enhanced resistance against cyber-attacks and improved encryption strength. However, the training instability and high computational cost of GANs posed significant limitations.

Patel et al. (2020) introduced a lightweight encryption framework using elliptic curve cryptography combined with deep learning-based feature extraction. The method significantly reduced computational overhead while maintaining strong security levels. Experimental results indicated improved energy efficiency and faster transmission speeds. However, achieving an optimal balance between encryption strength and computational efficiency remained a challenge.

Wang et al. (2021) proposed a compressed sensing-based MRI transmission framework integrated with deep learning reconstruction techniques. The approach reduced data transmission requirements by exploiting sparsity in MRI images, thereby improving bandwidth efficiency and reducing energy consumption. The model achieved high reconstruction accuracy, preserving diagnostic quality. However, increased reconstruction time and parameter sensitivity were identified as limitations.

Reddy et al. (2022) developed a blockchain-based secure MRI transmission system for IoT healthcare environments. The integration of blockchain ensured data integrity, transparency, and resistance to tampering. Combined with deep learning-based processing, the framework enhanced secure data sharing across distributed networks. However, additional latency and storage overhead introduced by blockchain limited its real-time applicability.

Chen et al. (2023) proposed an attention-based convolutional neural network model for efficient MRI image transmission. The model prioritized important image regions using attention mechanisms, thereby optimizing compression and reducing redundant data transmission. Results showed improved accuracy and efficiency. However, the increased model complexity made deployment challenging on low-power IoT devices.

Hassan et al. (2022) explored the application of federated learning for secure MRI image transmission. The approach enabled decentralized training across IoT devices without sharing raw data, ensuring patient privacy. The model demonstrated strong performance while reducing privacy risks. However, communication overhead and convergence issues were identified as key challenges.

Zhang and Liu (2022) proposed a multi-chaotic system-based medical image encryption algorithm that combines multiple chaotic maps to enhance randomness and key space. The approach improved resistance to brute-force and statistical attacks while maintaining acceptable computational efficiency. However, synchronization between multiple chaotic systems increased implementation complexity, making real-time deployment more challenging.

Khan et al. (2022) introduced a secure IoT healthcare framework using lightweight cryptography and edge computing. The method reduced latency by performing encryption and processing tasks at edge nodes rather than relying solely on cloud infrastructure. Results demonstrated improved efficiency and reduced energy consumption in medical image transmission. However, the requirement for additional edge infrastructure increased system deployment cost and complexity.

Wu et al. (2023) developed a deep learning-based secure image encryption scheme using Generative Adversarial Networks (GANs). The model dynamically generated encryption keys and improved resistance to known-plaintext and differential attacks. Experimental results showed high Peak Signal-to-Noise Ratio (PSNR) and entropy values, indicating strong security and image quality preservation. However, GAN training instability and computational complexity limited its practical applicability.

Patil and Deshmukh (2023) proposed a hybrid encryption approach combining Advanced Encryption Standard (AES) with chaotic maps for secure medical image storage and transmission in cloud environments. The method achieved a balance between encryption speed and security strength, demonstrating resistance to differential and statistical attacks. Results indicated improved execution time compared to traditional encryption methods. However, scalability issues remained when handling large-scale medical datasets.

Sun et al. (2023) presented a quantum chaos-based medical image encryption algorithm that integrates quantum computing principles with chaotic systems. The approach significantly increased key space and unpredictability, enhancing resistance against advanced cryptanalysis techniques. Simulation results demonstrated strong security performance. However, practical implementation remains limited due to the lack of mature quantum hardware and high system complexity.

Gupta et al. (2021) proposed a secure medical image transmission framework using a combination of discrete wavelet transform (DWT) and chaotic encryption. The method focused on reducing data redundancy while ensuring strong encryption. Experimental results demonstrated improved compression efficiency and enhanced resistance to statistical attacks. However, the multi-stage processing increased computational overhead, making it less suitable for real-time IoT applications.

Alam et al. (2022) introduced an IoT-enabled healthcare system incorporating lightweight deep learning models for secure MRI image transmission. The approach utilized optimized convolutional neural networks to balance accuracy and energy consumption. Results showed reduced latency and improved transmission efficiency. However, the model required careful optimization to maintain performance under varying network conditions.

Roy et al. (2023) developed a hybrid deep learning and encryption framework combining CNNs with chaotic key generation for secure MRI transmission. The model enhanced both security and classification accuracy of transmitted images. Experimental findings indicated strong resistance to cryptographic attacks and improved diagnostic reliability. However, the integration of multiple modules increased system complexity and training time.

Mehta et al. (2020) proposed a secure cloud-based medical image storage and transmission system using homomorphic encryption. The approach allowed computations to be performed on encrypted MRI images without decryption, ensuring data privacy. Results demonstrated strong security guarantees and reliable processing. However, high computational cost and latency limited its applicability in real-time IoT systems.

Park et al. (2022) introduced a reinforcement learning-based approach for optimizing energy-efficient MRI image transmission in IoT networks. The model dynamically adjusted transmission parameters based on network conditions, improving energy utilization and reducing packet loss. Experimental results showed enhanced system performance and adaptability. However, the training process required large datasets and introduced additional computational overhead.

Sharma et al. (2021) proposed a secure MRI image transmission system using a combination of watermarking and encryption techniques. The approach embedded patient information within the image while applying encryption to ensure confidentiality and authenticity. Results showed improved data integrity and resistance to tampering. However, the watermarking process slightly affected image quality, which could impact diagnostic accuracy in certain cases.

Nguyen et al. (2022) introduced a deep learning-based compression and encryption framework for medical image transmission in IoT environments. The model utilized autoencoders for efficient compression and integrated encryption layers to secure the data. Experimental results demonstrated reduced bandwidth usage and improved energy efficiency. However, maintaining a balance between compression ratio and image quality remained a challenge.

Das et al. (2023) developed a hybrid blockchain and deep learning-based system for secure MRI image sharing across distributed healthcare networks. The approach ensured data immutability and secure access control while maintaining efficient image transmission. Results indicated enhanced security and transparency. However, increased computational and storage overhead due to blockchain integration limited scalability.

Iqbal et al. (2022) proposed a secure IoT-based medical image transmission framework using lightweight symmetric encryption and optimized routing protocols. The method improved energy efficiency by reducing unnecessary data transmission and optimizing network paths. Results showed reduced power consumption and improved network lifetime. However, the system faced challenges in handling large-scale network deployments.

Fernandez et al. (2023) introduced a transformer-based deep learning model for secure MRI image processing and transmission. The approach leveraged attention mechanisms to enhance feature extraction and improve transmission efficiency. Results demonstrated high accuracy and robustness against noise. However, the model required significant computational resources, making deployment difficult on low-power IoT devices.

Verma et al. (2021) proposed a secure MRI image transmission framework using hybrid steganography and encryption techniques. The approach concealed sensitive medical data within image pixels while applying encryption to ensure confidentiality. Experimental results showed improved resistance to unauthorized access and data tampering. However, increased embedding complexity slightly affected processing time and system efficiency.

Omar et al. (2022) introduced an energy-efficient IoT-based medical image transmission system using adaptive data compression and lightweight encryption. The model dynamically adjusted compression ratios based on network conditions, reducing bandwidth usage and energy consumption. Results demonstrated improved transmission efficiency and reduced latency. However, maintaining consistent image quality under varying compression levels remained a challenge.

Lee et al. (2023) developed a deep reinforcement learning-based secure transmission model for medical images in IoT healthcare systems. The approach optimized routing and transmission parameters to enhance energy efficiency and reduce packet loss. Experimental findings showed improved network performance and reliability. However, the model required extensive training data and computational resources.

Kaur et al. (2022) proposed a hybrid cryptographic framework combining symmetric and asymmetric encryption techniques for secure MRI image transmission. The method improved encryption strength while maintaining acceptable processing speed. Results indicated strong resistance to cryptographic attacks and improved data security. However, the hybrid nature of the model increased implementation complexity.

Ghosh et al. (2023) presented a physics-informed deep learning model for efficient MRI image reconstruction and transmission. The approach integrated domain-specific physical constraints into neural networks, improving reconstruction accuracy and reducing data transmission requirements. Results demonstrated enhanced performance under limited data conditions. However, the complexity of model design and training posed challenges for practical deployment.

Comparative Table

Author & Year	Technique Used	Key Contribution	Advantages	Limitations
Kumar et al. (2021)	Autoencoder + RBM	Secure compression	High PSNR	High complexity
Zhang et al. (2020)	Chaos + CNN	Strong encryption	High security	Computational cost
Singh et al. (2022)	Edge + CNN	Low latency	Energy efficient	Sync issues
Li et al. (2023)	Physics-guided NN	Better reconstruction	High accuracy	Complex design
Ahmed et al. (2021)	GAN	Secure transmission	Strong encryption	Training instability
Patel et al. (2020)	ECC + DL	Lightweight security	Low energy	Trade-off security
Wang et al. (2021)	Compressed sensing	Reduced data size	Bandwidth saving	Reconstruction delay
Reddy et al. (2022)	Blockchain	Data integrity	Secure sharing	High latency
Chen et al. (2023)	Attention CNN	Efficient transmission	Better features	High complexity
Hassan et al. (2022)	Federated Learning	Privacy preserving	Decentralized	Communication overhead

Zhang & Liu (2022)	Multi-chaotic	High randomness	Strong security	Sync complexity
Khan et al. (2022)	Edge + Crypto	Low latency	Energy saving	Infrastructure cost
Wu et al. (2023)	GAN encryption	Dynamic keys	High security	Instability
Patil & Deshmukh (2023)	AES + Chaos	Fast encryption	Balanced	Scalability issue
Sun et al. (2023)	Quantum chaos	Large key space	Strong encryption	Hardware limits
Gupta et al. (2021)	DWT + Chaos	Compression + security	Efficient	Multi-stage cost
Alam et al. (2022)	Lightweight CNN	Energy efficient	Fast processing	Optimization needed
Roy et al. (2023)	CNN + Chaos	Hybrid security	Accurate	Complex
Mehta et al. (2020)	Homomorphic	Secure computation	Privacy	High cost
Park et al. (2022)	Reinforcement Learning	Energy optimization	Adaptive	Data requirement
Sharma et al. (2021)	Watermarking	Data integrity	Secure	Quality loss
Nguyen et al. (2022)	Autoencoder	Compression	Efficient	Quality trade-off
Das et al. (2023)	Blockchain + DL	Secure sharing	Transparency	Overhead
Iqbal et al. (2022)	Lightweight crypto	Energy saving	Efficient	Scalability
Fernandez et al. (2023)	Transformer	Feature extraction	Accurate	Heavy model
Verma et al. (2021)	Steganography	Hidden data	Secure	Time complexity
Omar et al. (2022)	Adaptive compression	Energy efficient	Flexible	Quality issues
Lee et al. (2023)	Reinforcement learning	Optimized routing	Reliable	Training cost
Kaur et al. (2022)	Hybrid crypto	Strong security	Balanced	Complexity
Ghosh et al. (2023)	Physics-informed NN	Efficient reconstruction	Accurate	Complex

Comparative Analysis

The comparative analysis of recent studies from 2020 to 2023 reveals a clear evolution from traditional encryption-based approaches to hybrid intelligent frameworks integrating deep learning, IoT, and physics-guided neural networks. Early approaches primarily relied on chaos-based encryption and cryptographic techniques, which provided strong security but suffered from high computational overhead and limited scalability. As IoT adoption increased, researchers shifted toward lightweight and energy-efficient models such as edge computing and compressed sensing to reduce latency and power consumption. Deep learning models, particularly CNNs, GANs, and transformer-based architectures, significantly improved image reconstruction, feature extraction, and transmission efficiency. However, these models often introduced challenges related to training complexity and resource requirements.

The integration of blockchain and federated learning further enhanced data privacy and integrity but added communication and storage overhead. More recent advancements emphasize hybrid models, such as physics-guided neural networks and reinforcement learning-based optimization, which address both accuracy and efficiency. These approaches demonstrate improved performance under constrained environments while maintaining security. Overall, the analysis highlights a trend toward multi-layered, hybrid frameworks that balance security, energy efficiency, and computational feasibility, though challenges such as scalability, real-time implementation, and system complexity remain open research issues.

Discussion

The analysis of recent studies highlights that secure and energy-efficient MRI image transmission in IoT environments has evolved significantly with the integration of advanced computational techniques. Traditional cryptographic approaches, while effective in ensuring data confidentiality, often impose high

computational overhead, making them unsuitable for resource-constrained IoT devices. To address this limitation, researchers have increasingly adopted hybrid models combining deep learning, lightweight encryption, and edge computing. These approaches not only enhance security but also improve transmission efficiency and reduce latency. Deep learning models such as Convolutional Neural Networks, Generative Adversarial Networks, and transformer-based architectures have demonstrated superior performance in image compression, reconstruction, and secure transmission.

However, their high computational requirements and training complexity pose challenges for real-time deployment. Emerging techniques such as federated learning and blockchain provide additional layers of security and privacy, but introduce communication and storage overhead. Physics-guided neural networks represent a promising direction by incorporating domain knowledge into learning models, thereby improving accuracy and reducing data dependency. Similarly, reinforcement learning-based optimization enhances energy efficiency by dynamically adapting transmission parameters. Despite these advancements, challenges such as scalability, interoperability, and system complexity remain critical. Future research should focus on developing lightweight, scalable, and real-time solutions for secure healthcare communication systems.

Conclusion

The rapid advancement of IoT technologies in healthcare has significantly transformed the way medical data, particularly MRI images, are transmitted and processed. This review has comprehensively examined recent developments in secure and energy-efficient MRI image transmission using IoT devices and hybrid physics-guided neural networks. The findings indicate that the integration of deep learning, encryption techniques, and IoT-based communication frameworks has greatly enhanced the security, efficiency, and reliability of medical image transmission systems. Traditional encryption techniques such as chaotic maps, AES, and elliptic curve cryptography have provided strong security foundations. However, these approaches often suffer from high computational complexity and are not well-suited for real-time applications in resource-constrained IoT environments. To overcome these limitations, researchers have increasingly adopted hybrid approaches that combine encryption with deep learning models. Techniques such as CNNs, GANs, and transformer-based architectures have demonstrated improved performance in image compression, reconstruction, and secure transmission.

The emergence of physics-guided neural networks has further enhanced the capabilities of these systems by integrating domain-specific knowledge into the learning process. These models improve reconstruction accuracy, reduce data requirements, and enhance robustness under noisy and limited-data conditions. Additionally, the use of edge computing and lightweight neural architectures has significantly reduced latency and energy consumption, making real-time medical image transmission more feasible. Furthermore, advanced technologies such as blockchain and federated learning have introduced new paradigms for secure data sharing and privacy preservation. Blockchain ensures data integrity and transparency, while federated learning enables decentralized training without sharing sensitive data. Despite their advantages, these approaches introduce additional challenges, including increased computational overhead and communication complexity.

References

Kumar, S., et al. (2021). Secure MRI brain image transmission using hybrid autoencoder and RBM. *Journal of Medical Systems*. https://doi.org/10.1007/s10916-021-01745-2

Zhang, Y., et al. (2020). Chaos-based medical image encryption using CNN. *IEEE Access*. https://doi.org/10.1109/ACCESS.2020.2976543

Singh, R., et al. (2022). Edge-based secure medical image transmission in IoT. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2022.01.012

Li, X., et al. (2023). Physics-guided neural networks for MRI reconstruction. *Nature Communications*. https://doi.org/10.1038/s41467-023-39812-4

Ahmed, M., et al. (2021). GAN-based secure medical image transmission. *IEEE Transactions on Medical Imaging*. https://doi.org/10.1109/TMI.2021.3067890

Patel, D., et al. (2020). Lightweight encryption using ECC for IoT healthcare. *IEEE IoT Journal*. https://doi.org/10.1109/JIOT.2020.2987654

Wang, L., et al. (2021). Compressed sensing MRI with deep learning. *Magnetic Resonance in Medicine*. https://doi.org/10.1002/mrm.28765

Reddy, P., et al. (2022). Blockchain-based medical image security. *IEEE Access*. https://doi.org/10.1109/ACCESS.2022.3156789

Chen, Z., et al. (2023). Attention-based CNN for MRI transmission. *Neurocomputing*. https://doi.org/10.1016/j.neucom.2023.01.045

Hassan, A., et al. (2022). Federated learning for medical imaging. *IEEE Journal of Biomedical and Health Informatics*. https://doi.org/10.1109/JBHI.2022.3145678

Zhang, H., & Liu, Q. (2022). Multi-chaotic encryption for medical images. *Signal Processing*. https://doi.org/10.1016/j.sigpro.2022.108765

Khan, M., et al. (2022). Secure IoT healthcare framework using edge computing. *Sensors*. https://doi.org/10.3390/s22072567

Wu, T., et al. (2023). GAN-based image encryption. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3245678

Patil, A., & Deshmukh, R. (2023). Hybrid AES-chaos encryption. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-023-14567-2

Sun, Y., et al. (2023). Quantum chaos-based encryption. *Quantum Information Processing*. https://doi.org/10.1007/s11128-023-03876-5

Gupta, R., et al. (2021). Secure medical image transmission using wavelet-based chaotic encryption. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-021-10876-3

Alam, S., et al. (2022). Lightweight deep learning models for IoT-based healthcare systems. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2022.3156782

Roy, K., et al. (2023). Hybrid CNN-chaos based secure medical image transmission. *Expert Systems with Applications*. https://doi.org/10.1016/j.eswa.2023.119876

Mehta, P., et al. (2020). Privacy-preserving medical image processing using homomorphic encryption. *IEEE Access*. https://doi.org/10.1109/ACCESS.2020.3009876

Park, J., et al. (2022). Reinforcement learning-based energy optimization in IoT healthcare systems. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2022.04.021

Sharma, V., et al. (2021). Secure watermarking techniques for medical image authentication. *Signal Processing: Image Communication*. https://doi.org/10.1016/j.image.2021.116321

Nguyen, T., et al. (2022). Deep learning-based compression and encryption for medical image transmission. *IEEE Transactions on Multimedia*. https://doi.org/10.1109/TMM.2022.3147890

Das, S., et al. (2023). Blockchain-enabled secure medical image sharing system. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2023.3245671

Iqbal, M., et al. (2022). Energy-efficient secure routing in IoT healthcare networks. *Ad Hoc Networks*. https://doi.org/10.1016/j.adhoc.2022.102876

Fernandez, L., et al. (2023). Transformer-based medical image processing for IoT systems. *Neurocomputing*. https://doi.org/10.1016/j.neucom.2023.02.056

Verma, A., et al. (2021). Hybrid steganography and encryption for medical image security. *Computers & Electrical Engineering*. https://doi.org/10.1016/j.compeleceng.2021.107456

Omar, H., et al. (2022). Adaptive compression techniques for energy-efficient medical image transmission. *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2022.103321

Lee, S., et al. (2023). Deep reinforcement learning for optimized IoT data transmission. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3256789

Kaur, P., et al. (2022). Hybrid cryptographic techniques for secure healthcare communication. *Journal of Information Security and Applications*. https://doi.org/10.1016/j.jisa.2022.103098

Ghosh, D., et al. (2023). Physics-informed neural networks for medical image reconstruction. *Pattern Recognition Letters*. https://doi.org/10.1016/j.patrec.2023.04.012