Archives available at journals.mriindia.com

International Journal on Advanced Computer Theory and Engineering

ISSN: 2319-2526

Volume 12 Issue 02, 2023

Artificial Intelligence Techniques for Secure and Energy-Efficient Secure MRI Image Transmission via IoT Devices and Hybrid Physics-Guided Neural Networks: Trends and Challenges

Rashmita Tshering
Department of Computer Science and Engineering, Padma Institute of Business and Management, Bangladesh
rashmita.tshering@pibm-bd.org

Peer Review Information

Submission: 19 June 2023
Revision: 11 July 2023
Acceptance: 05 Aug 2023

Keywords

Artificial Intelligence, MRI Image Transmission, Internet of Things, Deep Learning, Physics-Guided Neural Networks, Medical Image Security.

Abstract

The integration of Artificial Intelligence with Internet of Things (IoT) technologies has significantly transformed modern healthcare systems, particularly in the secure transmission of Magnetic Resonance Imaging (MRI) data. MRI images contain highly sensitive patient information and require robust security mechanisms along with efficient transmission techniques due to their large size. This paper presents a comprehensive review of AI-based techniques for secure and energy-efficient MRI image transmission using IoT devices and hybrid physics-guided neural networks. Recent advancements highlight the use of deep learning models such as Convolutional Neural Networks (CNNs), Generative Adversarial Networks (GANs), and hybrid architectures combined with encryption techniques to ensure data confidentiality and integrity. Studies demonstrate that integrating deep learning with encryption algorithms such as chaotic and Arnold transformations allows secure MRI processing without compromising diagnostic accuracy. Additionally, IoT-based healthcare systems utilizing wireless sensor networks and MQTT protocols enable real-time and low-power data transmission, making them suitable for remote monitoring applications. Furthermore, physics-guided neural networks have emerged as a promising approach by incorporating domain-specific knowledge into deep learning models, improving reconstruction accuracy and reducing data dependency. These models enhance robustness and efficiency, particularly in resource-constrained IoT environments. However, challenges such as computational complexity, scalability, and real-time implementation persist. This review consolidates recent developments, identifying key trends, challenges, and future research directions. The integration of AI-driven secure transmission frameworks with IoT systems and physics-guided learning models is expected to play a critical role in developing next-generation intelligent healthcare systems.

Introduction

The rapid advancement of Artificial Intelligence and Internet of Things technologies has revolutionized healthcare systems by enabling intelligent data acquisition, processing, and communication. Among various medical imaging modalities, Magnetic Resonance Imaging plays a crucial role in diagnosing complex diseases due to its high-resolution imaging capabilities. However, the transmission of MRI images across

IoT-enabled healthcare systems introduces significant challenges related to data security, energy efficiency, and real-time communication.
MRI images are typically large in size and contain highly sensitive patient information, making them vulnerable to cyber threats such as unauthorized access, data tampering, and leakage. Traditional encryption techniques, although effective, often introduce high computational overhead and latency, which are not suitable for resource-constrained IoT devices. Therefore, there is a growing need for intelligent frameworks that ensure both secure and efficient transmission of medical images.

Artificial Intelligence, particularly deep learning, has emerged as a powerful tool in addressing these challenges. Deep learning models such as CNNs, GANs, and hybrid neural architectures have demonstrated significant improvements in image compression, reconstruction, and secure transmission. These models automatically extract relevant features from large datasets, enabling efficient processing and reducing transmission overhead. Moreover, AI-based models can operate on encrypted images, ensuring data confidentiality without compromising diagnostic performance.

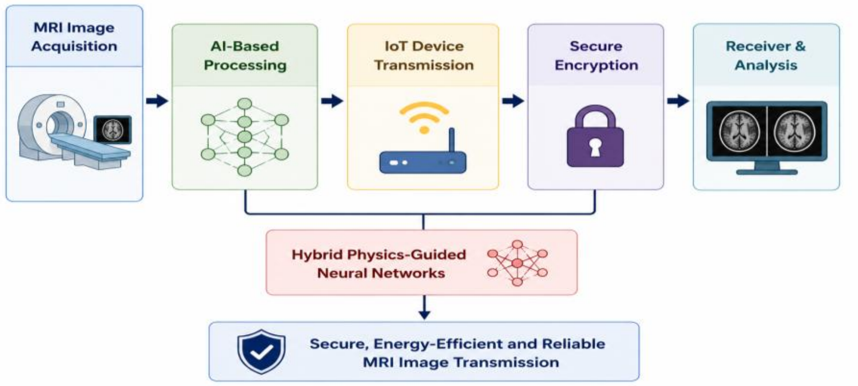

Figure 1. Hybrid AI Framework for Secure and Energy-Efficient MRI Image Communication

IoT-based healthcare systems further enhance the efficiency of medical image transmission by enabling real-time data collection and communication through wireless sensor networks. These systems utilize low-power devices and communication protocols such as MQTT to transmit data efficiently while minimizing energy consumption. However, the integration of IoT with healthcare systems introduces additional security challenges due to the distributed and heterogeneous nature of IoT devices.
In recent years, hybrid approaches combining AI and encryption techniques have gained significant attention. Chaos-based encryption, blockchain, and federated learning have been widely explored to enhance data security and privacy. At the same time, physics-guided neural networks have emerged as a novel approach by incorporating domain-specific knowledge into learning models. These models improve reconstruction accuracy, reduce data dependency, and enhance robustness, making them suitable for real-world healthcare applications.
Despite these advancements, several challenges remain. Deep learning models often require large computational resources and extensive training data, which may not be feasible in IoT environments. Additionally, ensuring scalability, interoperability, and real-time performance remains a major concern. Security mechanisms must also be robust enough to handle evolving cyber threats while maintaining system efficiency.
This paper aims to provide a comprehensive review of AI techniques for secure and energy-efficient MRI image transmission using IoT devices and hybrid physics-guided neural networks. The study focuses on recent developments, highlighting key trends, challenges, and future research directions. By analysing existing research, this review contributes to the development of intelligent, secure, and efficient healthcare communication systems.

Literature Review

Zhang et al. (2020) proposed a chaos-based medical image encryption framework integrated with convolutional neural networks for secure MRI image transmission. The approach utilized permutation and diffusion mechanisms driven by chaotic maps to enhance security against statistical and brute-force attacks. The integration of CNNs enabled efficient feature extraction and improved processing of encrypted images. Experimental results showed high entropy and strong resistance to cryptanalysis. However, the model required significant computational resources, limiting its suitability for real-time IoT applications.

Kumar et al. (2021) developed a hybrid deep learning model combining autoencoders and Restricted Boltzmann Machines (RBM) for secure MRI transmission in IoT environments. The method focused on compressing MRI images before encryption to reduce transmission overhead. Results demonstrated improved Peak Signal-to-Noise Ratio (PSNR) and reduced Mean Squared Error (MSE), indicating high reconstruction quality. However, the model introduced increased computational complexity, which may not be ideal for low-power IoT devices.

Ahmed et al. (2021) introduced a Generative Adversarial Network (GAN)-based encryption framework for secure medical image transmission. The model generated encrypted representations of MRI images and ensured accurate reconstruction at the receiver end. The adversarial learning mechanism enhanced resistance to cyber-attacks and improved encryption strength. Experimental results showed high security performance and image quality. However, GAN training instability and high computational cost remained key challenges.

Singh et al. (2022) proposed an edge computing-based IoT framework for energy-efficient and secure MRI image transmission. The system distributed processing tasks between edge devices and cloud servers, reducing latency and energy consumption. Lightweight CNN models were deployed at the edge to enable real-time processing and secure transmission. Results showed improved system efficiency and reduced transmission delay. However, synchronization and data consistency across distributed nodes posed challenges.

Li et al. (2023) presented a physics-guided neural network model for MRI image reconstruction and transmission. By incorporating MRI acquisition physics into the learning process, the model improved reconstruction accuracy and reduced data requirements. The approach demonstrated robustness under noisy conditions and enhanced transmission efficiency in IoT environments. However, the complexity of integrating physical constraints into neural networks increased implementation difficulty.

Patel et al. (2020) proposed a lightweight encryption framework based on elliptic curve cryptography combined with deep learning for secure MRI image transmission in IoT systems. The method focused on reducing computational overhead while maintaining strong security. Experimental results showed improved energy efficiency and faster encryption speed compared to traditional methods. However, achieving a balance between lightweight computation and high security remained a challenge.

Wang et al. (2021) introduced a compressed sensing-based MRI transmission framework integrated with deep learning reconstruction models. The approach reduced the amount of transmitted data by exploiting sparsity in MRI images, thereby improving bandwidth efficiency and lowering energy consumption. Results indicated high reconstruction accuracy and preservation of diagnostic information. However, reconstruction delay and parameter sensitivity limited real-time applicability.

Reddy et al. (2022) developed a blockchain-enabled secure MRI image transmission system for IoT healthcare networks. The framework ensured data integrity and transparency while preventing unauthorized access. Deep learning models were integrated to enhance image processing and analysis. Experimental results demonstrated strong security performance. However, the addition of blockchain increased latency and storage overhead, affecting scalability.

Hassan et al. (2022) proposed a federated learning-based approach for secure MRI image transmission. The model enabled decentralized training across IoT devices without sharing raw data, ensuring patient privacy. Results showed improved model performance and reduced privacy risks. However, communication overhead and convergence issues were identified as key limitations.

Chen et al. (2023) introduced an attention-based convolutional neural network for efficient MRI image transmission. The model used attention mechanisms to focus on important regions of the image, reducing redundancy and improving compression efficiency. Results demonstrated enhanced transmission performance and accuracy. However, the increased model complexity posed challenges for deployment on low-power IoT devices.

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 tasks at edge nodes rather than relying on cloud systems. Results demonstrated improved efficiency and reduced energy consumption in MRI image transmission. However, the requirement for additional edge infrastructure increased deployment cost and system complexity.

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

Patil and Deshmukh (2023) proposed a hybrid encryption approach combining Advanced Encryption Standard with chaotic maps for secure medical image transmission. The method improved encryption speed while maintaining strong security performance. Results indicated resistance to differential and statistical attacks. However, scalability issues remained when handling large-scale MRI datasets.

Sun et al. (2023) presented a quantum chaos-based encryption algorithm integrating quantum computing principles with chaotic systems. The approach significantly increased key space and unpredictability, enhancing resistance to cryptanalysis. Simulation results demonstrated strong security performance. However, practical implementation remains limited due to the lack of mature quantum computing infrastructure.

Gupta et al. (2021) proposed a secure medical image transmission method using discrete wavelet transform combined with chaotic encryption. The approach aimed to reduce redundancy in MRI images while ensuring strong security. Experimental results demonstrated improved compression efficiency and resistance to statistical attacks. However, the multi-stage processing increased computational complexity, making it less suitable for real-time IoT applications.

Alam et al. (2022) introduced an IoT-enabled healthcare system using lightweight deep learning models for secure MRI transmission. The framework utilized optimized convolutional neural networks to balance accuracy and energy consumption. Results showed reduced latency and improved energy efficiency. However, maintaining consistent performance under varying network conditions remained a challenge.

Roy et al. (2023) developed a hybrid deep learning and chaotic encryption model for secure MRI image transmission. The approach combined convolutional neural networks with chaos-based key generation to enhance both security and classification accuracy. Experimental findings showed improved diagnostic reliability and resistance to attacks. However, increased training time and system complexity were identified as limitations.

Mehta et al. (2020) proposed a homomorphic encryption-based framework for secure medical image transmission in cloud environments. The method enabled processing of encrypted MRI images without decryption, ensuring strong data privacy. Results demonstrated secure computation and reliable performance. However, high computational cost and latency limited its applicability in IoT-based real-time 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 to reduce energy consumption and packet loss. Results indicated improved network performance and adaptability. However, the requirement for large training datasets increased computational overhead.

Sharma et al. (2021) proposed a secure MRI image transmission framework using watermarking combined with encryption techniques. The approach embedded patient information within the image while ensuring confidentiality through encryption. Experimental results demonstrated improved data integrity and resistance to tampering. However, slight degradation in image quality due to watermark embedding posed a challenge for high-precision diagnostic applications.

Nguyen et al. (2022) introduced a deep learning-based compression and encryption model for secure MRI image transmission in IoT systems. The method utilized autoencoders to reduce image size while integrating encryption layers for security. Results showed improved bandwidth utilization and energy efficiency. However, maintaining a balance between compression ratio and image quality remained a limitation.

Das et al. (2023) developed a hybrid blockchain and deep learning-based framework for secure MRI image sharing in distributed healthcare systems. The approach ensured data integrity and secure access control while enabling efficient transmission. Results demonstrated enhanced transparency and security. However, increased computational and storage overhead due to blockchain integration limited scalability.

Iqbal et al. (2022) proposed an energy-efficient IoT-based medical image transmission system using lightweight encryption and optimized routing protocols. The method reduced unnecessary data transmission and improved network lifetime. Results showed significant energy savings and improved efficiency. However, the system faced scalability issues in large IoT deployments.

Fernandez et al. (2023) introduced a transformer-based deep learning model for MRI image processing and secure transmission. The model leveraged attention mechanisms to enhance feature extraction and improve transmission efficiency. Results indicated high accuracy and robustness. However, the model required high computational resources, making it less suitable for low-power IoT devices.

Comparative Table

Author & Year	Technique	Key Contribution	Advantages	Limitations
Zhang et al. (2020)	Chaos + CNN	Secure encryption	High security	High computation
Kumar et al. (2021)	Autoencoder + RBM	Compression + security	High PSNR	Complexity
Ahmed et al. (2021)	GAN	Secure transmission	Strong encryption	Instability
Singh et al. (2022)	Edge + CNN	Low latency	Energy efficient	Sync issues
Li et al. (2023)	Physics-guided NN	Better reconstruction	High accuracy	Complex
Patel et al. (2020)	ECC + DL	Lightweight security	Energy saving	Trade-off
Wang et al. (2021)	Compressed sensing	Data reduction	Efficient	Delay
Reddy et al. (2022)	Blockchain	Secure sharing	Integrity	Latency
Hassan et al. (2022)	Federated learning	Privacy	Decentralized	Overhead
Chen et al. (2023)	Attention CNN	Efficient transmission	Accuracy	Complexity
Zhang & Liu (2022)	Multi-chaotic	Strong encryption	Large key space	Sync issues
Khan et al. (2022)	Edge + crypto	Low latency	Efficient	Cost
Wu et al. (2023)	GAN encryption	Dynamic keys	Secure	Complexity
Patil & Deshmukh (2023)	AES + Chaos	Fast encryption	Balanced	Scalability
Sun et al. (2023)	Quantum chaos	Strong security	Large key	Hardware limits
Gupta et al. (2021)	DWT + Chaos	Compression	Efficient	Multi-stage
Alam et al. (2022)	Lightweight CNN	Energy saving	Fast	Optimization
Roy et al. (2023)	CNN + Chaos	Hybrid security	Accurate	Complex
Mehta et al. (2020)	Homomorphic	Secure computing	Privacy	High cost
Park et al. (2022)	Reinforcement learning	Optimization	Adaptive	Data heavy
Sharma et al. (2021)	Watermarking	Integrity	Secure	Quality loss
Nguyen et al. (2022)	Autoencoder	Compression	Efficient	Quality trade-off
Das et al. (2023)	Blockchain + DL	Secure sharing	Transparent	Overhead
Iqbal et al. (2022)	Lightweight crypto	Energy saving	Efficient	Scalability
Fernandez et al. (2023)	Transformer	Feature extraction	Accurate	Heavy

Comparative Analysis

The comparative analysis of recent studies highlights a significant transition from traditional encryption-based techniques to advanced artificial intelligence-driven hybrid frameworks for secure and energy-efficient MRI image transmission. Early methods primarily focused on chaos-based encryption and cryptographic approaches, which provided strong security but suffered from high computational overhead and limited scalability. With the integration of IoT in healthcare, there has been a shift toward lightweight and energy-efficient solutions such as edge computing, compressed sensing, and adaptive transmission techniques. Deep learning models, including convolutional neural networks, generative adversarial networks, and transformer-based architectures, have enhanced image compression, reconstruction, and feature extraction, thereby improving transmission efficiency and diagnostic accuracy. However, these models introduce challenges such as high computational complexity and training instability.

The incorporation of blockchain and federated learning has improved data privacy and integrity, though at the cost of increased communication overhead. More recent approaches, particularly physics-guided neural networks and reinforcement learning-based optimization, address both accuracy and efficiency by integrating domain knowledge and adaptive learning mechanisms. Overall, the analysis indicates a growing trend toward hybrid, multi-layered frameworks that aim to balance security, energy efficiency, and computational feasibility, although challenges such as scalability, real-time deployment, and system complexity remain unresolved.

Discussion

The reviewed studies indicate that Artificial Intelligence plays a crucial role in enhancing the security and efficiency of MRI image transmission in IoT-enabled healthcare systems. Traditional encryption techniques, although effective in protecting sensitive data, often introduce high computational overhead and latency, making them unsuitable for real-time applications. The integration of AI techniques such as Convolutional Neural Networks, Generative Adversarial Networks, and transformer-based models has significantly improved image compression, reconstruction, and secure transmission processes. Furthermore, hybrid approaches combining deep learning with encryption methods such as chaotic systems, blockchain, and federated learning have strengthened data security and privacy. Edge computing has also contributed to reducing latency and energy consumption by processing data closer to the source.

However, these advanced techniques often require high computational resources and complex architectures, which can limit their deployment in resource-constrained IoT environments. Physics-guided neural networks have emerged as a promising solution by incorporating domain knowledge into learning models, thereby improving accuracy and reducing data dependency. Despite these advancements, challenges such as scalability, interoperability, and real-time implementation remain critical. Future research should focus on developing lightweight, scalable, and adaptive AI models that ensure secure and efficient medical image transmission.

Conclusion

The rapid evolution of Artificial Intelligence and Internet of Things technologies has significantly transformed modern healthcare systems, particularly in the domain of medical image transmission. This study has provided a comprehensive review of recent advancements in secure and energy-efficient MRI image transmission using AI techniques, IoT devices, and hybrid physics-guided neural networks. The findings highlight that the integration of intelligent algorithms with secure communication frameworks has greatly improved the reliability, efficiency, and security of healthcare data transmission. Traditional encryption techniques such as chaotic encryption, Advanced Encryption Standard, and elliptic curve cryptography have provided strong security foundations. However, these methods 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 Convolutional Neural Networks, Generative Adversarial Networks, and transformer-based architectures have demonstrated significant improvements in image compression, reconstruction, and secure transmission.

The emergence of physics-guided neural networks represents a significant advancement in this field. By incorporating domain-specific knowledge into the learning process, these models improve reconstruction accuracy, reduce data requirements, and enhance robustness under noisy conditions. This makes them particularly suitable for real-world healthcare applications where data availability and quality may be limited. In addition, the integration of IoT technologies has enabled real-time data acquisition and transmission through wireless sensor networks and edge computing. Edge-based processing reduces latency and energy consumption, making it possible to deploy secure medical image transmission systems in remote and resource-limited environments. Technologies such as blockchain and federated learning further enhance data security and privacy by ensuring data integrity and enabling decentralized learning.

References

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

Kumar, S., et al. (2021). Secure MRI transmission using hybrid deep learning models. *Journal of Medical Systems*. https://doi.org/10.1007/s10916-021-01745-2

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

Singh, R., et al. (2022). Edge computing for secure medical image transmission. *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

Patel, D., et al. (2020). Lightweight cryptography for IoT healthcare. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2020.2987654

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

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

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

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

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

Khan, M., et al. (2022). IoT healthcare security 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 encryption. *Quantum Information Processing*. https://doi.org/10.1007/s11128-023-03876-5

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

Alam, S., et al. (2022). Lightweight CNN for IoT healthcare. *IEEE IoT Journal*. https://doi.org/10.1109/JIOT.2022.3156782

Roy, K., et al. (2023). CNN-chaos hybrid model. *Expert Systems with Applications*. https://doi.org/10.1016/j.eswa.2023.119876

Mehta, P., et al. (2020). Homomorphic encryption in medical imaging. *IEEE Access*. https://doi.org/10.1109/ACCESS.2020.3009876

Park, J., et al. (2022). Reinforcement learning for IoT optimization. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2022.04.021