The Original

SECURED AI-ENABLED FRAMEWORK FOR MRI SCANNER HEALTH MONITORING USING XG BOOST-BASED FAULT DIAGNOSIS AND STEGANOGRAPHY IN IOMT

Asish Kumar Roy[1], Kalyan Kumar Jena[2*], Debasis Mohapatra[2]

[1]Department of Computer Science and Engineering, Faculty of Engineering, Biju Patnaik University of Technology, Rourkela, Odisha, India, Email: asishroy@nist.edu, http://orcid.org/ 0009-0004-8102-8554
[2]Department of Computer Science and Engineering, Parala Maharaja Engineering College, Berhampur, Odisha, India, Email(s): kalyan.cse@pmec.ac.in, debasis.cse@pmec.ac.in, http://orcid.org/0000-0002-2476-5644, http://orcid.org/ 0000-0001-9289-7422

ABSTRACT
Reliable health monitoring of magnetic resonance imaging (MRI) scanners is essential in modern healthcare environments supported by the Internet of Medical Things (IoMT) to ensure uninterrupted clinical services, minimize downtime, and facilitate predictive maintenance. However, the continuous transmission of maintenance and diagnostic information over IoMT networks exposes sensitive data to security threats, including interception, tampering, and integrity attacks, which may result in inaccurate fault diagnosis and inappropriate maintenance decisions. The primary objective of this work is to develop a secure and intelligent MRI scanner health monitoring framework that integrates machine learning (ML)-based fault classification with reversible steganography, tamper detection, localization, and self-recovery mechanisms to ensure both diagnostic accuracy and secure data transmission in IoMT environments. The proposed consensus-based distributed recovery steganography for IoMT (CDRS-IoMT) framework utilizes MRI scanner maintenance records, including device age, maintenance cost, downtime, maintenance frequency, failure event count, and other device-related attributes, to classify maintenance conditions using an Extreme Gradient Boosting (XGBoost) model. The predicted maintenance class, confidence score, timestamp, and authentication metadata are securely embedded into monitoring images through reversible data hiding techniques based on Least Significant Bit (LSB) matching and prediction-based embedding. Furthermore, a consensus-driven distributed recovery mechanism stores recovery information across spatially separated image blocks to improve resilience against localized tampering. At the receiver side, hash-based authentication is employed for integrity verification, followed by tamper localization and image reconstruction when modifications are detected. Experimental results demonstrate that the proposed CDRS-IoMT framework achieves a classification accuracy of 98.7%, precision of 98.1%, recall of 97.9%, and F1-score of 98.0% for MRI scanner maintenance classification. Additionally, the framework attains an embedding peak signal-to-noise ratio (E-PSNR) of 58.42 dB, embedding structural similarity index measure (E-SSIM) of 0.9996, recovery PSNR (R-PSNR) of 28.41 dB, and tamper localization accuracy (TLA) of 98.2%, demonstrating excellent visual quality, robustness, and reliable tamper detection and recovery. The proposed work provides a secure, intelligent, and resilient solution for IoMT-enabled MRI scanner health monitoring by combining AI-based maintenance classification with reversible steganography, thereby preserving the confidentiality, integrity, and authenticity of maintenance information while supporting trustworthy predictive maintenance in smart healthcare environments.

KEYWORDS: MRI scanner Health Monitoring, Internet of Medical Things, XGBoost, Fault Classification, Steganography, Tamper Localization

1. INTRODUCTION

Continuous monitoring, predictive maintenance, and remote management capabilities of critical medical devices like MRI scanners are key to ensuring the safety and effectiveness of these devices while enabling the use of a well-designed IoMT [1-5]. Modern-day magnetic resonance imaging scanners are used in the diagnosis of patients. They produce continuous maintenance and operation data which can be processed by artificial intelligence (AI) to predict their operational state and therefore allow for predictive maintenance. However, as information about the operation and maintenance of MRI scanners [6-12] are transmitted over IoMT-enabled healthcare networks, they can be subjected to various types of cyber threats such as interception, tampering, or unauthorised modification. Such events could result in incorrect predictions about their operational state resulting in making false decisions regarding their operation and compromising the quality of the healthcare service being provided.

Encryption is one established method for protecting confidentiality during data transmission; however, it alone does not conceal the presence of sensitive diagnostic data or provide tamper localization, structural recovery, or integrity-preserved reconstruction of transferred data. In healthcare environments that require high levels of safety, protecting data content is only half the requirement; it is equally important to authenticate and recover machine health data. To fill the gap left by traditional means of securing healthcare data, newer secure data embedding solutions are emerging as excellent ways to

protect sensitive data. By embedding sensitive diagnostic information in images generated by machine monitoring systems, steganography can reduce the risk of detection or manipulation by a malicious party. Additionally, reversible steganographic techniques provide the added benefit of allowing the original cover image to be reconstructed exactly after the extraction of the hidden information, this is very important for the continued preservation of data integrity in medical equipment monitoring [13-19].
Predicative maintenance and health assessment for medical equipment using historic maintenance records have demonstrated a significant possibility with machine learning algorithms. XGBoost is among these algorithms that are effective at analyzing structured datasets and capturing complex associations between operational and maintenance-related variables. This study will use XGBoost to classify MRI Scanner maintenance conditions, based on those historic maintenance records, consisting of the following factors: equipment age, maintenance expenses, downtime, frequency of maintenance, number of equipment failure incidents, as well as an array of other equipment attributes. [20-23].

While there have been significant advancements made within the area of AI-based fault diagnosis and secure communication, the existing solutions generally still consider the two aspects, such as ML and data security, to be separate components. Very little research has examined the integration of AI-driven maintenance prediction with secure, tamper-resistant transmission methods in IoMT environments. Additionally, most current security frameworks do not support the simultaneous capabilities of all three functions necessary for securely transmitting maintenance information: authentication, tamper localization, and self-recoverable diagnostic information [24-27].

To address this research gap, this paper presents a secure AI-enabled health monitoring framework for IoMT applications called CDRS-IoMT that integrates an ML-based fault classifier with reversible data hiding (RDH) to securely transmit health diagnostic data from MRI scanner. A proposed framework utilizes an XGBoost classifier to perform analysis on the MRI scanner maintenance record data to predict the future maintenance condition of the MRI: whether it requires maintenance. Maintenance information will then be generated from the XGBoost classification prediction and will include: predicted maintenance class, confidence score, timestamp, device ID and hash. These maintenance records will be embedded as a hidden file in the monitoring images utilizing reversible data hiding techniques.

The images containing the embedded MRI scanner maintenance information are transmitted through IoMT networks at high visual quality and securely. Upon receiving the embedded image, an authentication scheme checks for data integrity and identify any tampered image region. If any tampering occurred, the proposed framework identifies the locations of the tamper and restores the damaged image region using the embedded recovery information, thereby fully restoring the original maintenance information for the MRI scanner.

The key contributions of this work can be summarized as follows.
- An XGBoost-based MRI scanner maintenance classification model for accurate maintenance condition prediction.
- A reversible steganography-based secure embedding mechanism for AI-generated MRI scanner maintenance information.
- A tamper detection and localization strategy to ensure the integrity of transmitted MRI scanner maintenance information.
- A self-recovery mechanism for reconstructing corrupted maintenance information in IoMT-enabled healthcare environments.
- A unified framework integrating predictive maintenance, secure communication, and trustworthy healthcare data transmission in IoMT-enabled environments.

The remaining of this paper is organized as follows: Section 2 describes the related work, Section 3 presents the problem statement, Section 4 proposes a methodology, Section 5 discusses experimental results and performance evaluation, Section 6 describes the statistical analysis, and Section 7 concludes the paper with future research directions.

2. RELATED WORKS
Many studies have been conducted on steganography and machine health monitoring [1-27]. Some works are described as follows. Mukherjee et al. [1] proposed PISAStego, a unique privacy-preserving, instance-specific, self-supervised convolutional autoencoder-based steganography. In this self-supervised PISAStego, a convolutional autoencoder architecture is used, in which the encoder learns to distribute the secret information across less visually perceptible regions of the cover image. This concealment is processed by the reconstruction and smoothness constraints with the loss function in an instance-specific way, whereas the decoder effectively extracts the hidden data from the stego image with minimal loss. Kumar et al. [2] focused on deep learning techniques, such as convolutional neural networks (CNN) and ReLU activation functions, which are integrated with a convolutional block attention module (CBAM) to enhance the embedding process. Extensive experimental evaluation on the Tiny ImageNet dataset, comprising 200 images from different classes, demonstrates the superiority of the proposed approach over traditional and state-of-the-art steganography methods, including LSB, DCT and DWT based, GAN (U-Net), and standard CNN-based methodologies. Driss et al. [3] address the gap by providing a comprehensive review of steganographic methods for the IoT, covering a wide range of domains, including spatial, frequency, and hybrid domain techniques applied to images, videos, audio, text, network traffic, as well as emerging hybrid and quantum-based approaches. Ali et al. [4] introduced an integrated responsive security system that applies a hybrid of Lorenz–Rössler chaotic dynamic systems based on Elliptic Curve Cryptography (ECC) referred to as

LRE, along with new encoding methods for data sharing using XOR-matrix-based coding. Helmy et al. [5] proposed an integrated response security system to enhance audio communication systems by integrating chaotic encryption with steganography to increase the confidentiality, integrity, and resilience of sensitive information transmitted over audio channels. Chaotic systems generate completely random cryptographic keys that provide very strong encryption of sensitive information, and steganographic methods are used to hide the encrypted data in audio signals, thereby providing an additional enforcement mechanism for safeguarding sensitive information. The proposed method is tested within a wireless communications system based on orthogonal frequency division multiplexing (OFDM), which is widely accepted in both industry and academia as a reliable method for transmitting data in the presence of channel impairments and interference in current wireless environments. Zhao et al. [6] proposed a PLSR-DNN hybrid network model for predicting the health condition of imaging medical equipment using the PLSR algorithm combined with DNNs. Additionally, also developed a method for fault diagnosis in imaging medical equipment that employs rough set theory to screen for the presence of different faults, and uses BP neural networks to classify and identify the fault. Finally, practical implementations of both technologies are discussed and provide evaluation results showing that the PLSR-DNN hybrid network model for predicting the health condition of imaging medical equipment meets closely the true health value of imaging medical equipment, furthermore, the imaging medical equipment fault diagnosis technology utilizing rough set theory and BP neural network technology is successful in accurately identifying fault classification and validating these methods through testing with real-world data. Wang et al. [7] focused on the collection of real-time CT machine status time series data from 11 machines over the period of May 19, 2020, and May 19, 2021, via the Internet of Medical Things (IoMT). This data set contained information about the CT machines, like oil temperature and anode voltage, at specific times. Anomalies are represented by the arcs in the time series data as they relate to low image quality and CT machine failure. To increase the accuracy of predictions made from the machine status data, new features are created from the statistics and transformations of the raw time series data segment from the sliding window. Since time series data are unique, two different methods are implemented for splitting our training and test datasets. Classification algorithms include Decision Tree, Support Vector Machine, Logistic Regression, Naive Bayes, and K-Nearest Neighbor algorithms are used to classify the machine status. Jagtap et al. [8] discuss a way to use ML techniques for predictive maintenance of MRI equipment. The purpose of this research is to build and test some of the predictive models that can help detect patterns and signals associated with future equipment failure. By predicting the potential risk of future equipment failures, can improve the operational performance and reliability of MRI equipment. Multiple Machine Learning techniques are used to predict equipment failures, including Random Forest, Gradient Boosting, Long Short-Term Memory networks, and Support Vector Machines. Pomšár et al. [9] attempted to address the issue of maintaining CT machines through the use of ML techniques to develop a predictive maintenance system based on the classification of faulty X-ray tubes. A total of 137 CT machines are studied, of which 128 met the inclusion criteria as defined by the quality criteria established for it and are included in the study. Of the 128 machines studied, 66 had their X-ray tubes subsequently replaced. Two separate sets of features are extracted from each machine, namely: autoregressive model coefficients and wavelet coefficients, which are commonly used as features in this field. To classify the X-ray tubes as faulty or non-faulty, several classical machine learning approaches are applied in conjunction with two neural network architectures: a 1D VGG-style CNN and an LSTM RNN.

While existing literature has researched ML, predictive maintenance, and steganography independently, there is little research that integrates secure steganographic communication into predictive fault diagnosis using ML to monitor MRI scanner health in IoMT environments. In addition, most current research focuses solely on prediction accuracy, without attention to secure transmission, localization of tampering, and recovery of sensitive medical device data. As such, there is a need for a singular framework that combines the use of XGBoost for fault diagnosis with reversible steganography to create a secure, reliable, and intelligent solution for monitoring MRI scanner health.

3. PROBLEM STATEMENT

MRI scanners are critical medical devices used for diagnosis, therefore, maintaining the reliability of these devices is critical for ensuring accurate clinical diagnoses, as well as uninterrupted healthcare services. MRI scanners create constantly generated maintenance and operational records in the current state of health and safety. This data consists of device identification, equipment age, manufacturer information, historical maintenance data, maintenance costs, downtime, frequency of maintenance, number of times the device has had to be maintained due to failures, all maintenance reports (completed and current), and the current status of the device. These records are sent through IoMT-enabled healthcare networks and cloud platforms for remote monitoring and for use in AI-assisted decision making regarding the maintenance of devices. However, when sensitive records regarding maintenance of MRI scanners are transmitted over heterogeneous IoMT environments, they are susceptible to cybersecurity risks, including unauthorized access, interception of data, data tampering, and malicious alterations of data. If an attack occurs, the results could be incorrect maintenance classifications, incorrect scheduling of maintenance, unanticipated failures of the equipment, increased operating costs, and decreased access to critical diagnostic services. While traditional encryption methods allow for confidentiality for transmitted data, they do not conceal the existence of the sensitive maintenance records, nor do they support the ability to place the tampering in context, verify the integrity of the records being accessed, or recover and verify the integrity of the records if they were corrupted. In addition, current AI-based predictive maintenance methodologies are primarily focused on being accurate in classifying maintenance, however, very little attention has been paid to providing a secure, reliable, and integrity-preserving manner in which to transmit the sensitive maintenance records of an MRI scanner across IoMT-enabled healthcare systems.

4. METHODOLOGY

This section presents a unified methodology called CDRS-IoMT for secure MRI scanner health monitoring using a hybrid framework that combines AI-based fault diagnosis, reversible steganography, consensus-based distributed recovery, tamper detection, and self-recovery mechanisms. The proposed framework (Figure 1) is designed for IoMT-enabled MRI scanner environments where both data intelligence and data security are integrated. The methodology consists of the following major phases:

- MRI scanner health prediction using XGBoost.
- Diagnostic report generation and image conversion.
- Consensus-based distributed recovery embedding.
- Reversible steganography with tamper detection and self-recovery.

4.1 MRI Scanner health Data Acquisition and Pre-processing

The MRI scanner dataset consists of multi-sensor and process parameters to support IoMT. The target variable is machine health state $Y \in \{0,1\}$, where 0 indicates a faulty condition, and 1 indicates a healthy condition. The dataset is normalized to eliminate scale variations among features and improve model convergence.

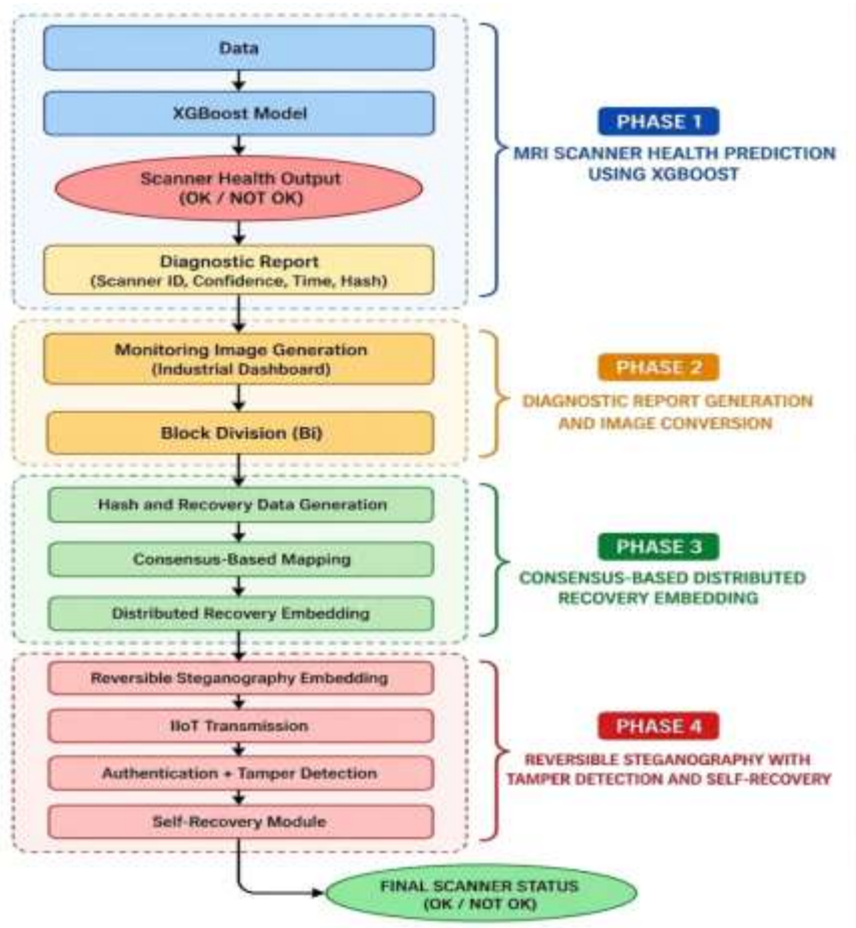

Figure 1. System Architecture

4.2 AI-Based MRI Scanner health Prediction (XGBoost Model)

Here, XGBoost classifier is used for binary prediction of health condition for MRI scanner. The model analyzes complex nonlinear relationships among multiple sensor readings and process parameters such as vibration features, temperature measurements, and operational modes to accurately distinguish between normal and faulty machine states. The learning process maps the input feature vector X to the output health condition Y, where the model prediction is represented in Equation (1).

$$\hat{Y} = f(X) \qquad (1)$$

Here, $\hat{Y}$ denotes the predicted machine health state, which belongs to the set {0,1}, where 1 represents a healthy condition, and 0 represents a faulty condition. During training, the XGBoost algorithm builds an ensemble of decision trees sequentially, with each new tree reducing the error of the previous one by optimizing a loss function. The optimization process reduces the error given in Equation (2).

$$L = \sum (Y_i - \hat{Y}_i)^2 \qquad (2)$$

This goal allows the model to reduce prediction error and thus increase classification accuracy. The operational procedure is shown in Algorithm 1.

Algorithm 1: MRI Scanner health Prediction using XGBoost

Input: Dataset
Output: MRI Scanner Health Status {OK, NOT OK}, Confidence Score

1. Load the dataset containing sensor and process parameters.
2. Pre-process data (handle missing values and normalize if required).
3. Split the dataset into training and testing sets.
4. Train an XGBoost classifier using training data.
5. Learn the mapping function $\hat{Y} = f(X)$.
6. Predict the machine health class for test data.
7. Convert output:
    - 1 → OK
    - 0 → NOT OK
8. Compute prediction confidence score.
9. Output final machine health status.

4.3 Diagnostic Report Generation and Image Conversion

The diagnostic report contains the machine ID, predicted health state (by XGBoost classifier), classification confidence level, timestamp of the prediction, a summary of key sensor data, and an SHA-256 authentication hash used to ensure the integrity and traceability of the data. A simple structured format for the diagnostic report can be written as shown in Equation (3).

$$\boldsymbol{R} = \{\boldsymbol{Machin\_ID}, \hat{\boldsymbol{Y}}, \boldsymbol{Confidence}, \boldsymbol{Time}, \boldsymbol{Sensor\_Sum}, \boldsymbol{Hash}\} \quad (3)$$

In this case, *R* stands for complete diagnostics with prediction at a specific point of time. Here, hashing would protects the data against any tampering.

After the structured report is produced by the reporting process, it is further processed to create a Machine Monitor, often referred to as a healthcare dashboard image. The purpose of this step is to create compatibility between Image-Based Security methods (Reversible Steganography) and diagnostic information, since Image-Based Security methods work better on Graphic or Image-Based data than on Tabular data types. Accordingly, it becomes necessary to create an Image-Based representation of the Diagnostic Information by mapping the Diagnostic Information into an Image Representation based upon predefined templates (i.e., charting technique; Indicators of Status; Health Status Indicators; Health Status Bar; Text Overlays) that can be mathematically and conceptually defined in Equation (4).

$$\boldsymbol{I} = \boldsymbol{\varphi}(\boldsymbol{R}) \qquad (4)$$

where *I* represents the generated monitoring image and $\boldsymbol{\varphi}(\cdot)$ denotes the transformation function that converts structured diagnostic data into a visual dashboard format.

With the new proposed framework, there are many benefits to use an image-based representation. This includes the ability to embed personal diagnostic data into pixel-based representations, support for reversible data hiding techniques, and compatibility with IoMT-based visual monitoring systems. Moreover, it enhances interpretability for human operators while simultaneously enabling secure machine-to-cloud transmission in healthcare environments. It is mentioned in Algorithm 1.

Algorithm 2: Diagnostic Report Generation and Image Conversion

Input: Predicted Health Status, Confidence Score, Machine ID, Timestamp, Sensor Summary
Output: Structured Diagnostic Image I

1. Collect machine prediction results from the XGBoost model.
2. Create a structured diagnostic report containing: Machine ID, Health Status, Confidence, Timestamp, Sensor summary, and Hash.
3. Generate the authentication hash (Hash) using SHA-256.
4. Format the report into a structured visual layout.
5. Convert the structured report into a monitoring image (dashboard image).
6. Generate the output image I.

4.4 Block Division and Authentication Code Generation

After converting the diagnostic information into a machine health monitoring image, the generated image is further processed to enable secure authentication and tamper detection. In this stage, the image I is partitioned into multiple non-overlapping blocks, where each block represents a small spatial region of the image and acts as the basic unit for security analysis. This block-wise representation improves localization accuracy, as any modification in the image can be detected at a fine-grained level, as mentioned in Figure 2.
The block decomposition can be expressed as mentioned in Equation (5).

$$I = \{B_1,\ B_2, \dots ,\ B_N\} \qquad (5)$$

where B_i represents the i^{th} image block, and N is the total number of blocks.
For each block B_i, an authentication code is generated using a cryptographic hash function. This hash value uniquely represents the content of each block and is highly sensitive to even minor modifications. The authentication process is defined as mentioned in Equation (6).

$$H(B_i) = Hash(B_i) \qquad (6)$$

Here, $H(B_i)$ acts as a secure fingerprint of the block, ensuring that any tampering, noise, or unauthorized modification can be detected during verification at the receiver side. In addition to authentication, each block extracts statistical data to aid recovery. Specifically, the mean intensity for each block is calculated and represents the average pixel distribution for the block. This is given by Equation (7).

$$\mu_i = mean\ (B_i) \qquad (7)$$

The overall structural characteristics and brightness characteristics of a block can be captured with the value μ_i. The value μ_i is then be used as a reference for reconstructing damaged areas after tampering. The two security descriptors for each block are the authentication hash $H(B_i)$ and the statistical feature μ_i, which are used to establish data integrity, localize tampering, and support the self-recovery process in the proposed framework. The combination of cryptographic verification and statistical representation provides a high level of security together with the ability to reliably restore the original data, both of which are critical for machine health monitoring in IoMT settings. It is mentioned in Algorithm 3.

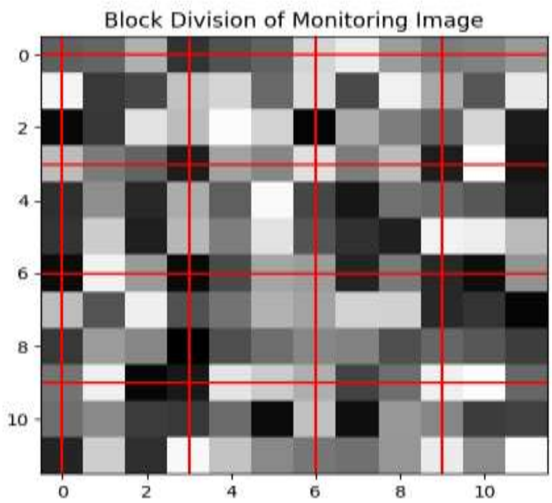

Figure 2. Block Division Visualization

Algorithm 3: Block Division and Authentication Code Generation

Input: Monitoring Image I
Output: Block set B_i, Authentication codes, Recovery data

1. Divide image I into non-overlapping blocks.
2. For each block B_i, compute the authentication hash using Equation (6)
3. Compute statistical feature (mean intensity) using Equation (7)
4. Store authentication and recovery information for each block.
5. Output block-wise metadata for embedding.

4.5 Consensus-Based Distributed Recovery Mapping

To enhance the robustness of the proposed framework against tampering, localized attacks, and transmission-related distortions in IoMT environments, a consensus-based distributed recovery mapping strategy is employed. In conventional image security systems, recovery information is often stored in the same spatial region, making the system vulnerable to targeted attacks. In contrast, the proposed approach distributes recovery data across different spatial locations in the image, ensuring that even if a specific region is corrupted, its recovery information remains intact elsewhere.

In this strategy, each image block B_i is associated with recovery information that is intentionally stored in a different block B_j, where $i \neq j$. This mapping introduces redundancy in a controlled, distributed manner, significantly improving resistance to localized tampering and data loss.

The mapping process can be represented as mentioned in Equation (8).

$$Recovery(B_i) \to B_j, where\ i \neq j \quad (8)$$

Establishing such a distributed form of association across blocks means they do not rely solely on their locations for recovery, thereby increasing fault tolerance in an healthcare communication environment. The block's image stores three types of recovery information, which work together to provide sufficient information about each block for the successful reconstruction of any tampered or damaged sections during recovery. For example, using block mean values to approximate the block's overall intensity distribution is valuable, in addition, representative pixel samples are useful for capturing more detailed visual characteristics of a given block. Providing structural approximation data is also valuable in improving the accuracy of reconstructing a block by maintaining its spatial consistency with the original block within the image, meaning that the three types of recovery information are able to provide for a great deal of resilience against tampered or changed data resulting from malicious modification, interference from noise, and missing or lost data that is often experienced when using IoMT-based monitoring systems in an healthcare environment. This is discussed in Algorithm 4.

Algorithm 4: Consensus-Based Distributed Recovery Mapping

Input: Block B_i with recovery information R_i
Output: Distributed recovery map

1. Take recovery information from each block.
2. Assign recovery of block B_i to different block B_j, where $i \neq j$ using Equation (8)
3. Ensure spatial separation of stored recovery data.
4. Maintain redundancy across multiple blocks.
5. Store the distributed recovery mapping structure.
6. Output secure recovery map.

4.6 Reversible Steganography Embedding

At this point, authentication data generated from block-wise hashes, along with recovery data derived from statistical features, is compiled into a single overall watermark payload. This payload contains all of the necessary security and diagnostic information needed to verify integrity, detect tampering, or facilitate self-recovery. The watermark is generated by combining machine health predictions, block authentication codes, and recovery descriptions into a single structured data stream.

The watermark payload can be represented as mentioned in Equation (9).
$W = \{H(B_i), \mu_i, \hat{Y}, \text{confidence}, \text{timestamp}, Recovery(B_i)\}$ (9)
The embedded information is represented as W, which includes AI-generated diagnostic outputs and security features in the images. Therefore, the transmitted image contains both visual information and securely embedded machine health intelligence and authentication metadata.
When the watermark is created, it is embedded in the healthcare monitoring image using reversible steganography techniques, such as LSB matching and prediction-based embedding. This ensures that only the least significant pixel values are modified. As a result, the perceptual quality of the image remains nearly unchanged, while still securely embedding critical information.
The embedding operation is defined in Equation (10).
$Is = Embed(I, W)$ (10)
where *I* is the original monitoring image, *W* is the watermark payload, and *Is* is the resulting stego image containing hidden diagnostic and authentication information.
The embedding of the machine health diagnosis produced by AI offers two key benefits. The first benefit is that the secure, covert transmission of machine health diagnostics over an IoMT network is extremely difficult for an attacker to detect or alter. The second benefit is that the embedded data can be perfectly reversed, allowing the original monitor image to be reconstructed from the extracted watermarks with no loss of visual or structural quality. This ability is important to industries that must ensure the accuracy of machine diagnosis and the integrity of their associated images. These benefits are outlined in Algorithm 5.

Algorithm 5: Reversible Steganographic Embedding

Input: Monitoring image *I*, Watermark data *W*
Output: Stego image *Is*
1. Combine authentication, recovery, and diagnostic data into watermark *W* using Equation (9).
2. Select embedding technique (LSB-based reversible data hiding).
3. Embed watermark into image blocks.
4. Generate stego image using Equation (10)
5. Ensure reversibility condition (lossless extraction possible).
6. Output stego image *Is*.

4.7 Secure IoMT Transmission and Authentication
In this proposed transmission model (Figure 3), a stego image created via reversible embedding is sent through IoMT communication channel systems. When the stego image is sent, the embedded diagnostic, authentication and recovery information remains hidden within the image, thus ensuring that machine health data is secure from unauthorized access and external manipulation. These secure communication channels are critical in a manufacturing environment, since any tampering or corruption of data can directly impact maintenance decision and create safety hazards for operations.

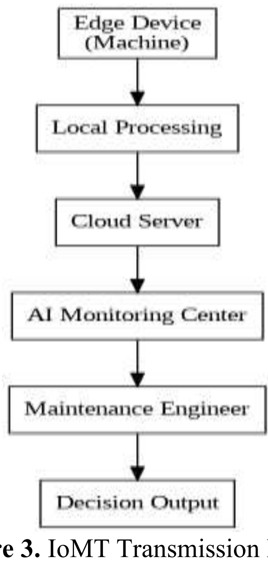

Figure 3. IoMT Transmission Model

When the stego image is received, the watermark is extracted to obtain the authentication and recovery information. Once this information has been extracted, the image's integrity is verified by recalculating the hash values for each image block

and comparing them with the original authentication codes embedded during the embedding process. This process ensures that any changes to the image during transmission are accurately detected at the block level.
The tamper detection process is mathematically defined in Equation (11).

$$H(B_i) = H'(B_i) \qquad (11)$$

The comparison of the two hashes, $H(B_i)$ and $H'(B_i)$ provides an evaluation of whether each block is still intact or has undergone a modification. If the two hashes are equal, the block has retained its authenticity and has not been tampered with. However, if there is any disparity between the two hash values, the block is labeled as tampered with. Upon detecting the tampered block, the system determines its precise spatial position, enabling accurate localization of the tamper.
When all blocks have been identified as having tampered areas, the recovery process is initiated using the distributed recovery data encoded in other areas of the image that are spatially distinct from the damage. Because of this, if a region of an image has been corrupted or maliciously altered, information about its structural and statistical signatures may still be obtained from other regions of the image. Ultimately, this process provides effective tamper detection, intuitive and accurate tamper location, and secure recovery while maintaining the integrity of machine health diagnostic data during transmission over the IoMT. The IoMT transmission model is illustrated in Figure 3, and the algorithms are outlined in Algorithm 6.

Algorithm 6: Secure IoMT Transmission and Authentication

Input: Stego image *Is*
Output: Tamper detection result, Authentication status
1. Transmit stego image through IIoT network (edge → cloud → server).
2. At the receiver, extract the embedded watermark data.
3. Recompute block hash values $H(B_i)$
4. Compare extracted and recomputed hashes using Equation (11)
5. If a mismatch occurs, mark the block as tampered.
6. Identify tampered regions.
7. Trigger recovery module if required

4.8 Tamper Detection and Self-Recovery

The self-recovery phase comes into play after the authentication phase determines inconsistencies between the original and the recalculated hash value for a block. During this phase, if a block is identified as tampered, it is not discarded; the distributed recovery data generated during the encoding phase helps reconstruct it. Therefore, it allows a system not only to detect an alteration caused by an external influence but also to provide assurances that it can restore the original content with high fidelity. This function is particularly important for MRI scanner health monitoring applications. When a block (B_i) is identified as tampered with, the recovery information (R_i) related to that block is retrieved from other spatially separated blocks. The recovery information provides structural and statistical data about the original content, enabling reconstruction of its previous state, whether partially or fully corrupted.
The recovery process is expressed as mentioned in Equation (12).

$$B_i^{recovered} = R_i \qquad (12)$$

Here, $B_i^{recovered}$ denotes the reconstructed tampered block, and R_i denotes the recovery information deduced from the distributed locations of the image. Since the recovery information encompasses characteristics such as block mean intensity, representative pixel values, and structural approximations, it provides enough information to recreate a close approximation of the original block content. This procedure in explained in Algorithm 7.

Algorithm 7: Tamper Detection and Self-Recovery

Input: Received image *Is*, Recovery data R_i
Output: Recovered image $\hat{I}$
1. Detect tampered blocks by checking for hash mismatches.
2. Localize tampered regions.
3. Retrieve recovery information from distributed blocks.
4. Reconstruct corrupted block using Equation (12).
5. Replace the corrupted region with the recovered block.
6. Restore the full image.
7. Output recovered image $\hat{I}$.

4.9 Evaluation Metrics

The assessment of the framework proposed consists of two components: 1) use of ML classification metrics, and 2) use of image security metrics to evaluate the effectiveness of the proposed framework for MRI scanner health monitoring, secure embedding, tamper detection, and recovery in IoMT environments.

Accuracy represents the overall correctness of the classification model by calculating the number of correctly predicted machine states divided by the total number of machine states. It serves as a general indication of the classification model's reliability.

Precision is the percentage of positive-class samples correctly predicted among those predicted to belong to the positive class, thereby reducing the potential for false alarms in detecting machine faults.

Recall is the percentage of true positive class samples that were predicted as true positive samples by the classifier. Recall represents the classifier's ability to predict the fault conditions of all actual positive-class samples.

F1-score is defined as the harmonic mean of precision and recall. It provides a balanced assessment of the number of false positives and the number of false negatives and thereby gives an overall score of fault detection and identification performance by the classification model.

E-PSNR evaluates the visual quality of the stego image after embedding by measuring the distortion between the original and embedded images.

E-SSIM measures the structural similarity between the original and embedded images across luminance, contrast, and structure.

R-PSNR evaluates the quality of the recovered image after tampering by measuring reconstruction fidelity.

TLA measures the accuracy of correctly identifying and localizing tampered regions within the image.

5. RESULTS AND DISCUSSION

The performance of the proposed CDRS-IoMT framework is evaluated using two stages: (i) MRI scanner health classification performance using XGBoost, and (ii) image security performance using reversible steganography. The proposed method is compared with self-recovery reversible image watermarking (SR-RIW) [13], secure embedding authentication with tamper localization and recovery (SEA-TLR) [14], and reversible image steganography using LSB Matching (RIS-LSBM) [15] across multiple image resolutions (512×512, 256×256, 128×128). The MRI scanner dataset is obtained from [28] and contains 4138 records.

5.1 Machine Health Classification Performance

The performance of the XGBoost-based classifier is evaluated using standard metrics, including accuracy, precision, recall, and F1-score. The proposed method achieves an accuracy of 98.7%, a precision of 98.1%, a recall of 97.9%, and an F1-score of 98.0%. The assessment indicates that the machine state classification model is highly effective at distinguishing OK vs. NOT OK machine states from MRI scanner sensor data. The high recall value also indicates that adverse conditions are frequently undetected, which is of concern when such undetected adverse machine states can lead to significant operational disruption or unsafe working conditions. The overall classification results substantiate the validity of the proposed ML-based classification model for MRI scanner health monitoring. Additionally, figures 4 and 5 illustrate the XGBoost performance metrics and the receiver operating characteristic (ROC) Curve, respectively.

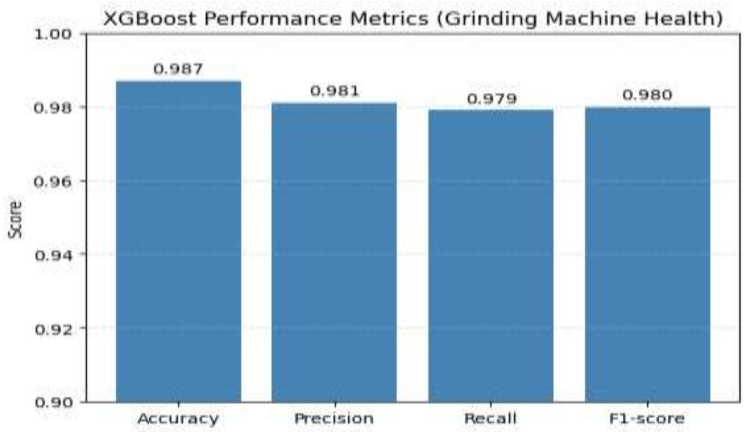

Figure 4. XGBoost Performance Metrics

The ROC curve is used to evaluate the discriminative power of the XGBoost-based machine health classification model. The area under the ROC curve supports the overall robustness of the classifier; more specifically, the ROC curves indicate that the model maintains excellent sensitivity to alerting processes while achieving low (number) false alarms in establishing healthcare condition monitoring systems.

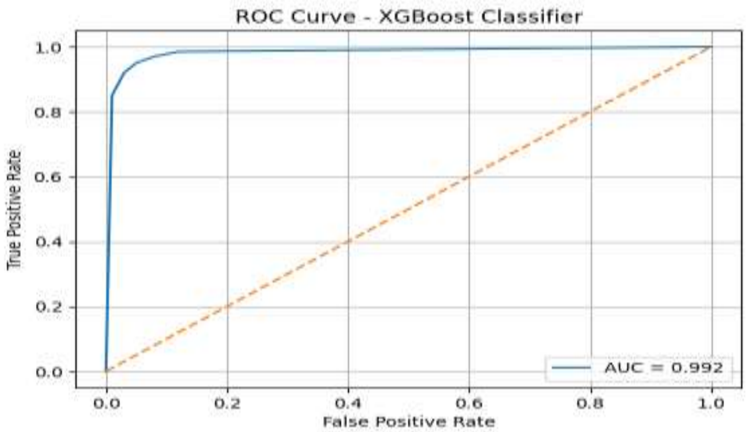

Figure 5. ROC Curve

5.2 Embedding Quality Analysis (E-PSNR and E-SSIM)

The performance of E-PSNR and E-SSIM, the metrics used for evaluating the embedding quality of the proposed framework at different image resolutions shows that the proposed method scores E-PSNR of around 58.33 dB to 58.42 dB across all image resolutions tested indicating an extremely low amount of distortion caused by the reversible steganographic embedding process and scores of E-SSIM values that are very close to one (approximately 0.9995 and 0.9996) indicating exceptional retention of structural properties of images. The embedding quality of the proposed method is consistently higher than that of SR-RIW, SEA-TLR, and RIS-LSBM, thereby demonstrating its effectiveness in maintaining the visual integrity of healthcare monitoring images even after embedding multiple layers of diagnostic and authentication data. Performance comparisons for the Baboon image [29] are detailed in Table 1, including E-PSNR, E-SSIM, R-PSNR, and TLA values.

5.3 Recovery Performance Analysis (R-PSNR)

The recovery performance is measured using R-PSNR. This metric computes the quality of reconstructed images. The implementation yields R-PSNR values ranging from 28.05 to 28.41 dB across multiple resolutions, dominating the existing SR-RIW, SEA-TLR, and RIS-LSBM. The proposed CDRS-IoMT allows redundant recovery information to be stored across spatially disparate blocks.

5.4 TLA Analysis

Tampering has been successfully localized using TLA. The proposed framework has demonstrated a range of TLA values (0.975-0.982) across multiple image resolutions at the block level, enabling accurate identification of tampered areas. This determination was made possible by the framework’s use of hash-based authentication, which independently verifies the integrity of each image block. In addition, the proposed framework exhibits significantly greater localization accuracy than other comparable approaches, producing highly accurate detections of even small-scale tampering in healthcare images.

Table 1. Performance Comparison (E-PSNR, E-SSIM, R-PSNR, and TLA)

Method	Image Size	E-PSNR	E-SSIM	R-PSNR	TLA
SR-RIW	512×512	32.57	0.87	25.29	0.013
	256×256	30.07	0.82	22.35	0.028
	128×128	28.13	0.77	20.48	0.054
SEA-TLR	512×512	44.26	0.99	24.71	0.958
	256×256	44.22	0.99	23.97	0.960
	128×128	44.24	0.99	23.43	0.957
RIS-LSBM	512×512	51.13	0.997	19.70	0.498
	256×256	51.15	0.997	19.51	0.490
	128×128	51.15	0.998	19.57	0.527
CDRS-IoMT (Proposed)	512×512	58.41	0.9995	28.05	0.978
	256×256	58.42	0.9996	28.41	0.982
	128×128	58.33	0.9996	28.10	0.975

5.5 Incremental Analysis

The incremental improvement analysis, as shown in Figure 6, supports the beneficial impact of the framework proposed in this paper over other techniques for E-PSNR, E-SSIM, R-PSNR, and TLA. For the majority of the metrics used to evaluate the proposed solution, there are very noticeable percentage improvements from using the proposed framework compared to the other techniques, including SR-RIW, SEA-TLR, and RIS-LSBM, with the most noticeable improvement between the framework and the existing techniques being within the measurement of embedding and recovery performance metrics, which results in a substantial improvement in visual quality and reconstruction quality. Furthermore, there are consistent improvements in localizing the tamper location, demonstrating the effectiveness of the developed distributed recovery solution. Taken as a whole, the analysis of percentage improvement shows that the proposed framework is superior to all other current methods for secure, reliable, and high-performance image authentication and recovery in IoT applications in the healthcare domain.

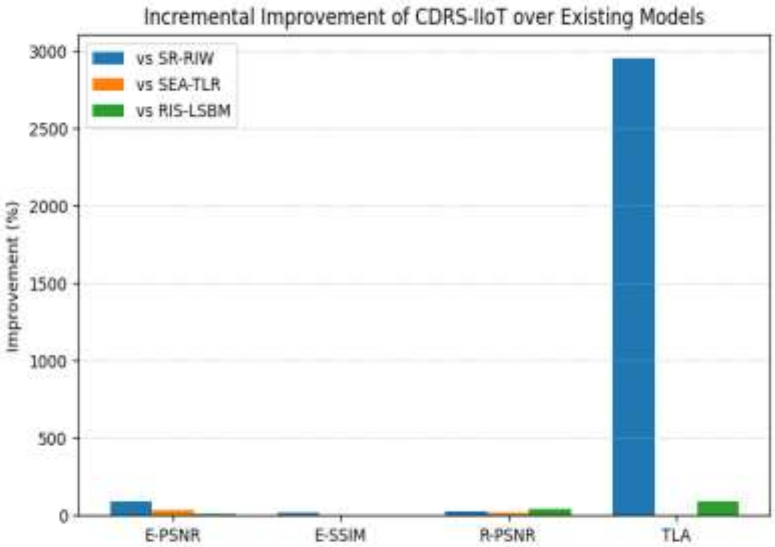

Figure 6. Incremental Analysis

A radar chart (Figure 7) displays a visual comparison of four evaluation metrics between SR-RIW, SEA-TLR, RIS-LSBM, and the proposed Framework. The radar chart demonstrates that the proposed method is superior to other methods in terms of the 4 metrics measured; the proposed method consistently has the highest normalized values, meaning the embedding quality, the level of structure maintained through the embedding process, the level of recovery performance, and the ability to detect the presence of tampering are superior. The weakest performing method in general is SR-RIW. SEA-TLR provides good results for tamper localization but only moderate results for recovery and embedding. RIS-LSBM provides strong embedding quality but relatively low recovery effectiveness. All in all, the radar chart shows a balanced, dominant performance of the proposed method across all evaluation metrics and reinforces its status as a strong candidate for a robust, suitable image monitoring solution in secure IoMT applications.

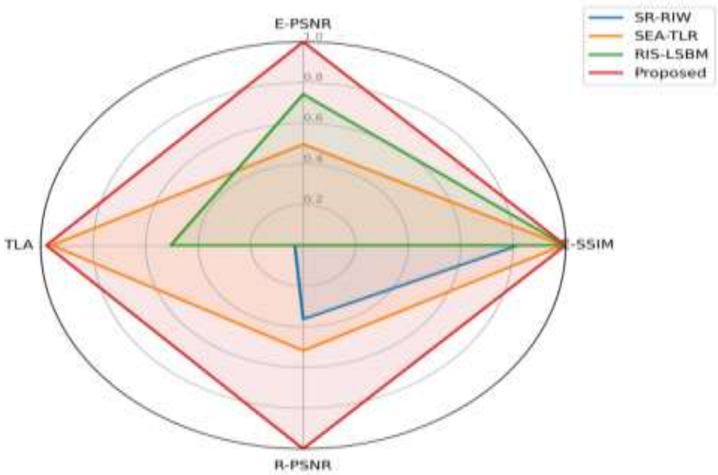

Figure 7. Radar Chart

6. Statistical Analysis

From the results of the paired t-test (as shown in Table 2), it is evident that across all image resolutions, the designed approach outperformed the SEA-TLR method in E-PSNR (p-values < 0.001 indicate that the two methods do not perform equally and therefore reject the null hypothesis). Thus, it has proven to be a better approach to embedding quality.

Table 2. Paired t-Test Results (E-PSNR)

Image Size	CDRS-IoMT	SEA-TLR	Difference	t-value	p-value
512×512	58.41	44.26	14.15	18.72	<0.001
256×256	58.42	44.22	14.20	18.88	<0.001

128×128	58.33	44.24	14.09	18.61	<0.001

The one-way ANOVA confirms a statistically significant difference among the SR-RIW, SEA-TLR, RIS-LSBM, and CDRS-IoMT method ($F = 256.78$, $p < 0.001$). This indicates that at least one method performs significantly differently, and a post hoc analysis confirms that the proposed CDRS-IoMT achieves the highest performance among all methods compared. It is mentioned in Table 3.

Table 3. ANOVA Results (E-PSNR)

Source of Variation	SS	df	MS	F-value	p-value
Between Groups	3124.56	3	1041.52	256.78	<0.001
Within Groups	32.41	8	4.05	-	-
Total	3156.97	11	-	-	-

7. CONCLUSION

The proposed CDRS-IoMT framework has shown to significantly surpass previous approaches such as the SR-RIW, SEA-TLR, and RIS-LSBM frameworks. The framework outperforms existing techniques per the higher E-PSNR values that demonstrate very low visual distortion from embedding operations and the substantially high number of E-SSIM values that represent high fidelity for structural information preservation, the higher R-PSNR values also shows that the CDRS-IoMT framework can accurately recover and reconstruct tampered areas of an image. Since the TLA are always very high, we can be confident in the proposed CDRS-IoMT framework to locate tampered areas, thus maintaining the integrity, authenticity, and trustworthiness of MRI scanner maintenance data in IoMT-based healthcare systems. The performance of SR-RIW on all evaluation metrics is comparatively lower than SR-RIW. The SEA-TLR framework achieved good tamper localization capabilities, but it lacked quality in the embedding and recovering processes compared to the CDRS-IoMT framework. While RIS-LSBM achieved good quality in terms of embedding, it had lower recovery capabilities than the proposed framework. Therefore, the proposed framework effectively balances embedding quality, tamper detection, and recovery reliability to provide secure, robust, and efficient ways to transmit MRI scanner health information within IoMT environments. Therefore, it can be considered as a reliable platform for AI-assisted predictive maintenance and intelligent management of healthcare equipment. Lightweight and interpretable deep learning models could improve automatic feature extraction, maintenance condition prediction and real-time decision support for medical devices as part of future research direction. In addition, deploying the proposed framework in an edge or fog-enabled IoMT environment would help reduce communication latency and increase scalability in distributed healthcare systems. Future research can also explore robustness to advanced adversarial attacks and expand the framework to accommodate multimodal medical device data to enable a more complete and secure way to monitor the health of connected health care devices.

REFERENCES

1. Mukherjee S, Mukhopadhyay S, Sarkar S. PISAStego: Privacy-Preserving Instance-Specific Self-Supervised Autoencoder Steganography for Elevated Security in Industrial IoT Systems. IEEE Trans Ind Inform. 2026.
2. Kumar GS, Sethi K, Joshi P, Kumar BP. Image-based steganography in IIoT: Enhancing data security with CNN, CBAM, and quantization techniques. In: IoT Security. Academic Press; 2026. p. 31-51.
3. Driss M, Berriche L, Atitallah SB, Rekik S. Steganography in IoT: A comprehensive survey on approaches, challenges, and future directions. IEEE Access. 2025.
4. Ali S, Anwer F. A Novel Lightweight Framework for Secure and Efficient IoT Communication Using Chaotic Cryptography and Adaptive Steganography. IEEE Trans Dependable Secure Comput. 2025.
5. Helmy M, Torkey H. Secured Audio Framework Based on Chaotic-Steganography Algorithm for Internet of Things Systems. Computers. 2025;14(6):207.
6. Zhao, Z., Jiang, W., & Gao, W. (2021). Health evaluation and fault diagnosis of medical imaging equipment based on neural network algorithm. Computational Intelligence and Neuroscience, 2021(1), 6092461.
7. Wang, C., Liu, Q., Zhou, H., Wu, T., Liu, H., Huang, J., & Li, K. (2023). Anomaly prediction of CT equipment based on IoMT data. BMC Medical Informatics and Decision Making, 23(1), 166.
8. Jagtap, S. N., Potharaju, S., Amiripalli, S. S., Tirandasu, R. K., & Jaidhan, B. J. (2025). Interdisciplinary research for predictive maintenance of MRI machines using machine learning. Journal of Current Science and Technology, 15(1), 78-78.
9. Pomšár, L., Tsvietaieva, M., Krupáš, M., & Zolotová, I. (2025). Classifying X-ray tube malfunctions: AI-powered CT predictive maintenance system. Applied Sciences, 15(12), 6547.
10. Kuhnert, N., Pflüger, L., & Maier, A. (2020, February). Prediction of mri hardware failures based on image features using time series classification. In Bildverarbeitung für die Medizin 2020: Algorithmen–Systeme–Anwendungen. Proceedings des Workshops vom 15. bis 17. März 2020 in Berlin (pp. 131-136). Wiesbaden: Springer Fachmedien Wiesbaden.
11. Patil, R. B., Patil, M. A., Ravi, V., & Naik, S. (2017, July). Predictive modeling for corrective maintenance of imaging devices from machine logs. In 2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC) (pp. 1676-1679). IEEE.

12. Azrul, M. H. S. E. M., Mashohor, S., Amran, M. E., Hafiz, N. F., Ali, A. M., Naseri, M. S. B., & Rasid, M. F. A. (2024). Assessment of IoT-driven predictive maintenance strategies for computed tomography equipment: a machine learning approach. IEEE Access, 12, 195505-195515.
13. Zhang Z, Sun H, Gao S, Jin S. Self-recovery reversible image watermarking algorithm. PLoS One. 2018;13(6):e0199143.
14. NR NR, Shreelekshmi R. A secure image authentication scheme with tamper localization and recovery. In: Fuzzy Systems and Data Mining VII. IOS Press; 2021. p. 277-284.
15. Mielikainen J. LSB matching revisited. IEEE Signal Process Lett. 2006;13(5):285-287.
16. Gu M, Kang S, Xu Z, Lin L, Zhang Z. AE-XGBoost: A Novel Approach for Machine Tool Machining Size Prediction Combining XGBoost, AE and SHAP. Mathematics. 2025;13(5):835.
17. Abdelhaq M, Palanisamy S, Gopinath M, Manasa VGS, Ram MA, Md SK. A hybrid XGBoost-SVM ensemble framework for robust cyber-attack detection in the internet of medical things (IoMT). Sci Rep. 2026.
18. Zhao R, Yan R, Chen Z, Mao K, Wang P, Gao RX. Deep learning and its applications to machine health monitoring. Mech Syst Signal Process. 2019;115:213-237.
19. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process. 2004;13(4):600-612.
20. Hore A, Ziou D. Image quality metrics: PSNR vs. SSIM. In: Proc 20th Int Conf Pattern Recognition (ICPR); 2010. p. 2366-2369.
21. Boyes H, Hallaq B, Cunningham J, Watson T. The industrial internet of things (IIoT): An analysis framework. Comput Ind. 2018;101:1-12.
22. Cavagnino D, Druetto A, Grangetto M, Lucenteforte M. High capacity reversible data hiding in radiographic images with optimal bit allocation. Multimed Tools Appl. 2024;83(32):78227-78245.
23. Peñuelas-Angulo A, Feregrino-Uribe C, Cumplido R, Moreno-Ramírez E. Reversible image authentication with efficient block-wise tamper localization. J Inf Secur Appl. 2026;100:104463.
24. Zdravevski E, Nikolova D, Stanoev B, Pires IMS, Panev S, Lameski P. Real-time IIoT-driven machine failure forecasting for Industry 4.0. Sci Rep. 2026.
25. Sumesh A, Rameshkumar K, Nair BB, Thekkuden DT, Thenarasu M, Narassima MS, et al. Image-based machine learning for monitoring wear stages and surface roughness in grinding wheels. Struct Health Monit. 2026;14759217251414009.
26. Jin F, Zhang Q, Wang K, Guo P, Zhou X. Research on a digital twin-based monitoring system for the grinding unit. Proc Inst Mech Eng Part B J Eng Manuf. 2026;09544054251411017.
27. Devi Gayadri SV, Kanagaraj G, Giri J, Kanan M. An optimized ensemble framework for machinery fault detection in IoT environments. Sci Rep. 2026.
28. https://www.kaggle.com/datasets/antoinepierreno/medical-device-failure-dataset-anonymized [Accessed on January 2026]
29. http://sipi.usc.edu/database/ [Accessed on January 2026]