

Quantum Watermarking: A Comprehensive Review of Principles, Challenges, and Future Prospects

Rashmi M Hullamani¹, Mahantesh Mattada² and Kavitha KJ³

¹Research Scholar, ECE Department, PESITM, Shivamogga, Visvesvaraya Technological University, Karnataka

²Associate Professor, ECE Department, PESITM, Shivamogga, Visvesvaraya Technological University, Karnataka

³Associate Professor, ECE Department, GM University, Davangere, Karnataka

Quantum Watermarking (QWM) is an emerging field that combines quantum information theory with digital watermarking techniques to enhance the security of digital content. By leveraging quantum properties such as superposition, entanglement, and the no-cloning theorem, QWM provides robust protection against unauthorised access, tampering, and duplication—offering a significant advantage over classical methods. As the volume and value of digital data grow, the need for advanced intellectual property protection becomes increasingly vital, making QWM a promising approach to next-generation data security. This paper presents a comprehensive review of the theoretical foundations of QWM, its core principles, and various classification methods based on quantum states, embedding techniques, and application domains such as authentication, copyright protection, and tamper detection. It also explores the mathematical models underlying QWM, including quantum state representations and error correction protocols, along with recent advances in experimental validations. Despite its potential, QWM faces challenges such as noise sensitivity, scalability limitations, and high computational resource requirements. Issues related to secure key management and implementation vulnerabilities also remain. Nevertheless, this review aims to serve as a foundational reference for researchers and practitioners, highlighting the promise of QWM in reshaping digital content security, particularly in sensitive domains like digital forensics and healthcare.

Keywords: QWM; entanglement; quantum states; tampering; no-cloning

I. INTRODUCTION

With the exponential growth in digital content and the parallel rise in cyber threats, traditional watermarking techniques are increasingly falling short in ensuring robust security, especially in sensitive sectors such as healthcare, digital media, and e-governance. Quantum watermarking (QWM), by harnessing the intrinsic features of quantum mechanics, promises unparalleled advantages in content

authentication, tamper detection, and copyright protection. Despite its transformative potential, the field remains fragmented with limited standardisation, experimental validation, and structured documentation. There is a pressing need for a comprehensive study that synthesises the current knowledge, outlines quantum-specific embedding and extraction algorithms, assesses practical applicability in real-world use cases like medical imaging and EHR

*Corresponding author: kavithakj219@gmail.com

protection, and identifies gaps for future exploration. This review aims to bridge that gap by offering an in-depth, structured exploration of QWM principles, methods, challenges, and opportunities for research and application.

The introduction of quantum computing and communication technology has significantly transformed the information security domain. In today's digital era, where electronic records play a vigorous role across various domains, the preservation of subtle information against tampering, unauthorised access, and duplication is of paramount importance. QWM presents a unique and robust approach to content security by harnessing the intrinsic features of quantum mechanics such as superposition, entanglement, and the no-cloning principle. These characteristics provide QWM with a distinct advantage over classical methods, as they offer intrinsic resistance to advanced forms of data replication.

In the healthcare sector, medical imaging (MI) constitutes a keystone of patient care by enabling precise diagnosis, therapeutic planning, and evidence-based clinical decisions. The confidentiality and authenticity of these medical images are critical, necessitating secure methods that can prevent unauthorised modifications or breaches. Likewise, Electronic Health Records (EHRs), comprising comprehensive patient data and longitudinal medical histories, are susceptible to cybersecurity threats. To preserve the integrity and privacy of such information, the implementation of robust and tamper-resistant security techniques is essential. This paper presents a comprehensive review of QWM with a focused examination of its application in the protection of Medical Images (MIs) and EHRs. These two components are foundational to the digital healthcare ecosystem and must be secured with mechanisms that are both effective and resilient to emerging threats.

Specifically for medical imaging, QWM offers a promising solution by embedding tamper-resistant and imperceptible watermarks directly into the quantum representation of MIs. This process ensures both the integrity and authenticity of the images throughout their transmission and storage. By integrating quantum watermarking techniques, healthcare providers can effectively protect MI data from manipulation, unauthorised redistribution, and potential breaches. The key applications of QWM in medical imaging include:

- Authentication of medical image sources and transmission pathways
- Tamper detection to identify unauthorised alterations or corruption
- Copyright and ownership protection for proprietary diagnostic data or imaging systems
- Secure sharing of sensitive diagnostic content among authorised healthcare professionals
- Ensuring integrity and traceability of image data across medical workflows and research collaborations

Several advanced techniques have been proposed for implementing QWM in Medical Imaging (MI-QWM).

These include methods such as the Quantum Fourier Transform (QFT), which reinforces the robustness of watermark embedding by spreading the watermark information across multiple quantum states. Additionally, Quantum Error Correction (QEC) techniques are employed to counteract the effects of quantum noise, thereby ensuring high fidelity of the embedded watermark. Entanglement-based methods further enhance detection accuracy and overall security by leveraging the inherent correlations between entangled quantum particles. From these observations, it is evident that QWM draws directly from the foundational principles of quantum mechanics to securely embed watermarks into digital data. The no-cloning theorem guarantees that quantum states cannot be duplicated without introducing detectable anomalies, thereby offering a natural safeguard against unauthorised copying. Superposition enables the encoding of complex, high-density watermark information by allowing quantum systems to exist in multiple states simultaneously. Entanglement contributes an added layer of security by tightly correlating the states of two or more quantum particles, such that measuring one immediately impacts the other, making unauthorised detection or tampering extremely difficult. The key features of MI-QWM include:

- High robustness against noise and compression through quantum error correction
- Tamper resistance due to the quantum no-cloning principle
- Enhanced capacity for watermarking through superposition

- Improved authentication accuracy via entanglement-based detection
- Invisibility and security due to the probabilistic nature of quantum measurements
- Resistance to eavesdropping by quantum uncertainty and collapse upon observation

In the context of Electronic Health Records (EHRs), safeguarding patient information is of paramount importance as it stores highly sensitive information, including medical histories, diagnoses, treatment plans, and other personal health details. Ensuring the security and privacy of this information is not only essential for protecting patient rights but also for adhering to regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA). QWM offers a compelling approach to enhancing the security of EHRs by embedding invisible and tamper-resistant watermarks within the data itself. These watermarks enable immediate detection of unauthorised modifications or access attempts, thereby reinforcing trust in digital healthcare systems.

Key features supported by QWM in the EHR context include:

- **Data Integrity:** Ensures that EHR content remains unaltered and authentic.
- **Access Control:** Enables enforcement of role-based permissions by verifying watermark signatures.
- **Audit Trails:** Facilitates detailed tracking of data access and modifications over time.

To implement QWM for EHR protection, several techniques can be employed:

- **Quantum Circuits:** It is designed specifically for embedding and retrieving watermark data from binary-form EHRs.
- **Quantum Cryptography Integration:** Offers secure transfer and storage of watermarked records using quantum key distribution and encryption (Solak, 2024).
- **Hybrid Classical-Quantum Models:** Combine conventional and quantum approaches to improve scalability and practical deployment across existing infrastructure.

An advanced development in this area involves embedding EHR data into medical images (MIs) using QWM techniques. This integrated approach enhances both the security and

authenticity of healthcare data by unifying medical imagery and patient information within a single, protected file. Using the unique properties of quantum mechanics, this method allows the creation of highly secure and resilient watermarks (WM), capable of withstanding common signal processing attacks like compression, noise addition, and image cropping.

By embedding EHR information directly and invisibly into medical images, this technique not only ensures confidentiality and integrity (Naima *et al.*, 2025), but also facilitates data traceability and verification across digital healthcare platforms (Chowdhury *et al.*, 2024). Such a capability is particularly beneficial in applications including telemedicine, long-term medical imaging repositories, and inter institutional collaborations where secure and efficient information sharing is essential. This advanced approach to MI-QWM provides several essential features that make it a compelling solution for securing sensitive healthcare information:

- **Security:** QWM ensures that embedded data is tampered proof, making unauthorised alterations easily detectable.
- **Confidentiality:** Only users possessing the correct quantum keys can access or interpret the embedded EHR information.
- **Non-intrusiveness:** The embedding of the WM does not degrade or interfere with the diagnostic quality of the medical images.
- **Robustness:** The watermark is resilient against common image processing attacks such as compression, cropping, and noise addition.

A. Technical Components for MI-QWM Implementation

To support the design, simulation, and validation of QWM algorithms, a combination of quantum and classical tools may be used:

- **Quantum Simulation Tools:** Platforms such as IBM Qiskit, Microsoft Quantum Development Kit (QDK), and Google Cirq are widely used for algorithm development, simulation, and verification of quantum watermarking schemes. For real-world deployment, quantum hardware available through these platforms may be leveraged.

- **Classical Tools:** Traditional programming and simulation environments like MATLAB, Python (with OpenCV), and other image processing libraries are utilised for image pre-processing, classical watermark embedding evaluation, and robustness testing.
- **Hybrid Approaches:** These approaches combine the strengths of classical and quantum computation, where watermark embedding or extraction may occur using classical methods, while encryption, authentication, or fidelity verification is handled using quantum algorithms.

The key contributions of this review study are as follows:

- Provides a comprehensive overview of quantum watermarking (QWM), detailing its foundational principles and how quantum properties such as superposition, entanglement, and the no-cloning theorem enhance watermarking security.
- Presents an in-depth classification of QWM techniques based on quantum states, embedding methods, and application areas including authentication, tamper detection, and copyright protection.
- Analyses mathematical models and quantum image representations (e.g., FRQI), as well as algorithms such as QHWT, QFT, QSD, and QPE for medical image watermarking.
- Explores the application of QWM in healthcare, particularly for securing Medical Images (MI) and Electronic Health Records (EHR), with a focus on real-world relevance like telemedicine and long-term data storage.
- Compares various quantum watermark embedding and extraction algorithms across key performance metrics like robustness, efficiency, and security.
- Identifies current challenges in QWM, including quantum noise, scalability issues, and secure key management.
- Highlights emerging quantum tools, hybrid classical–quantum models, and future prospects to guide ongoing and future research in this domain.

II. QWM ALGORITHMS FOR MEDICAL IMAGE WATERMARKING (MIW)

Quantum algorithms bring unique advantages to MIW by leveraging the principles of superposition and entanglement to improve security, robustness, and efficiency.

- **Quantum Haar Wavelet Transform (QHWT):** The QHWT adapts classical wavelet principles into the quantum domain, providing a robust mechanism to embed binary watermark data into grayscale medical images. QHWT operates on quantum image states and performs a transformation into the frequency domain, which enhances imperceptibility while enabling secure embedding. The Flexible Representation of Quantum Images (FRQI) is typically employed to represent grayscale images in the quantum format, where each pixel's position and intensity are encoded in quantum states. The effectiveness of QHWT-based watermarking is evaluated using: PSNR (Peak Signal-to-Noise Ratio) – to measure the imperceptibility and visual quality after embedding, BER (Bit Error Rate) in order to assess the accuracy of watermark extraction after processing or attack.

This method offers a balance of efficiency, high security, and low visual distortion, making it a promising candidate for secure medical image watermarking in quantum-based healthcare systems. A grayscale quantum image may be represented using the Flexible Representation of Quantum Images (FRQI) as defined by equation 1:

$$|I\rangle = \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} \cos(\theta_{xy})|0\rangle + \sin(\theta_{xy})|1\rangle|x,y\rangle \quad \text{--- (1)}$$

where:

$|x,y\rangle \rightarrow$ represents the pixel positions, which correspond to the coordinates of each pixel in an image or grid.

$\theta_{xy} \rightarrow$ is the angle encoding the intensity (grayscale value) of the pixel at (x,y) .

The QHWT decomposes the quantum image into sub-bands of approximate (AA) and detail coefficients (DH,DV,DDD_H, D_V, D_D) as defined by (2):

$$\begin{aligned}
 A &= \frac{I(x,y)+I(x+1,y)+I(x,y+1)+I(x+1,y+1)}{4} \\
 D_h &= \frac{I(x,y)-I(x+1,y)+I(x,y+1)-I(x+1,y+1)}{4} \\
 D_v &= \frac{I(x,y)+I(x+1,y)-I(x,y+1)-I(x+1,y+1)}{4} \\
 D_d &= \frac{I(x,y)-I(x+1,y)-I(x,y+1)+I(x+1,y+1)}{4}
 \end{aligned}
 \quad \text{----- (2)}$$

The binary watermark WW is embedded into the AA sub-band, ensuring imperceptibility. During extraction, the inverse Haar transform retrieves the watermark.

1. Quantum Fourier Transform (QFT)

By exploiting the frequency domain properties of QFT, watermarking schemes achieve secure and efficient embedding of information. These approaches often allow enhanced resistance to noise and common image-processing attacks and is defined as equation (3):

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \sum_{k=0}^{N-1} e^{2\pi i \frac{xk}{N}} |k\rangle \quad \text{----- (3)}$$

Where:

NN is the size of the quantum image.

$e^{2\pi i \frac{xk}{N}}$ is the Fourier kernel, enabling frequency domain transformation.

The watermark WW is embedded in selected frequencies.

For example:

$$F'(u, v) = F(u, v) + \alpha W(u, v) F'(u, v)$$

Where:

$F(u, v)F(u, v)$ is the Fourier coefficient at $(u, v)(u, v)$,

$W(u, v)W(u, v)$ is the watermark,

α is a scaling factor to balance robustness and imperceptibility.

2. Quantum Chaotic Maps

Chaotic systems in quantum computing are used for secure watermark embedding by taking advantage of their sensitivity to initial conditions and unpredictable outputs. These maps enhance the unpredictability and robustness of the watermarking process, making unauthorised extraction or tampering highly challenging.

Quantum chaotic maps generate pseudorandom sequences for embedding the WM, enhancing security. One such map is the Logistic Map as defined by 4:

$$x_{n+1} = rx_n(1 - x_n), \quad 0 < x_n < 1, r \in [3.57, 4] \quad \text{---(4)}$$

In the quantum version, a quantum superposition state encodes the chaotic sequence defined by equation 5:

$$|\psi\rangle = \sum_n \sqrt{P(x_n)} |n\rangle \quad \text{----- (5)}$$

where,

$P(x_n)$ is the probability distribution of the chaotic sequence

The chaotic sequence is used to randomise WM embedding locations as represented by the equation 6:

$$I'(x, y) = I(x, y) \oplus W(x, y, k) \quad \text{----- (6)}$$

where k is derived from the chaotic sequence.

3. QKD

QKD is applied for secure key exchange in watermarking and ensures that encryption keys used for embedding WMs are protected from interception, leveraging quantum entanglement for ultimate security. QKD ensures secure watermark embedding by generating a shared secret key using quantum states, such as in the BB84 protocol:

- Prepare quantum states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$.
- Send states over a quantum channel.
- Measure using random bases, ensuring a secure key.

The shared key KK governs the embedding process and is defined by equation 7:

$$I'(x, y) = I(x, y) \oplus K \quad \text{----- (7)}$$

This guarantees that only authorised parties with KK can extract the watermark.

4. Flexible Representation of Quantum Images (FRQI)

This representation encodes grayscale images into quantum states, facilitating efficient embedding of watermark data. FRQI-based techniques ensure high imperceptibility and adaptability in quantum watermarking schemes. FRQI encodes the entire image into a quantum state, facilitating watermark embedding. The image is represented as defined by 8:

$$|I\rangle = \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} (\cos(\theta_i)|0\rangle + \sin(\theta_i)|1\rangle)|i\rangle \quad \text{----- (8)}$$

where:

θ_i encodes the grayscale intensity of pixel i .

The watermark $|$

$W\rangle$ is encoded similarly and embedded by modifying θ_i .

For example:

$$\theta_i' = \theta_i + \alpha W_i$$

Where α controls the embedding strength.

Quantum algorithms such as the Quantum Haar Wavelet Transform (QHWT), Quantum Fourier Transform (QFT), chaotic maps, Quantum Key Distribution (QKD), and the Flexible Representation of Quantum Images (FRQI) contribute significantly to enhancing the imperceptibility, robustness, and security of watermarking techniques in medical imaging. These algorithms apply core quantum mechanical principles to overcome limitations commonly observed in classical systems, particularly with respect to computational efficiency and data protection (Dhar & Sahu, 2024). Their relevance is especially pronounced in critical applications such as telemedicine, where maintaining data confidentiality and integrity is essential. In addition to the above methods, several other quantum-based strategies are being explored for their potential to further improve watermarking approaches in medical image security. Some of these include:

i. Quantum Image Processing (QIP):

QIP harnesses the capabilities of quantum computing to perform image-related operations with greater speed and efficiency compared to classical techniques. By utilising phenomena like superposition and entanglement, QIP supports tasks such as image compression, enhancement, and feature extraction. These functions can be effectively applied to embed watermarks in a way that minimises visual distortion and preserves the diagnostic quality of the medical images.

ii. Quantum Cryptographic Techniques:

In this, again 2 types of cryptographic techniques may be employed as:

- a. Quantum Key Distribution (QKD): This method ensures the secure transmission of watermark-related data by utilising cryptographic keys that cannot be intercepted or duplicated. When integrated with systems such as the Quantum Public Key Infrastructure (QPKI), QKD supports a robust framework for the secure embedding and retrieval of

watermark information, ensuring confidentiality and integrity throughout the communication and storage processes (Rupa *et al.*, 2024).

- b. Quantum Secret Sharing (QSS): In this approach, the watermark is split into multiple quantum shares and distributed among authorised stakeholders. Only when all shares are combined can the watermark be reconstructed, ensuring strong access control and collaborative security.

iii. Quantum Machine Learning (QML):

In this type, the following ML are used for MI processing:

iv. Quantum Neural Networks (QNNs):

These networks can be trained on medical image features to generate adaptive watermark patterns that are more resilient to attacks.

v. Quantum Support Vector Machines (QSVMs):

QSVMs can be used to classify medical images and detect optimal regions for watermark insertion, ensuring that embedded data remains hidden and secure without degrading the image.

5. Quantum Error Correction (QEC)

Quantum watermarking techniques are particularly vulnerable to environmental disturbances such as noise and decoherence. To address these issues, quantum error correction methods like Shor's Code and Surface Codes are employed. These schemes are specifically designed to preserve the integrity of embedded watermark information during quantum operations or transmission. By counteracting the effects of quantum noise and operational faults, they help maintain the reliability of the watermark even in compressed or altered media.

6. Quantum Entanglement for Image Authentication

Quantum entanglement serves as a distinctive mechanism to securely bind a watermark with the host image. Any unauthorised modification to the image directly disrupts the entangled quantum state, making tampering readily detectable. This technique is especially useful in scenarios where passive, non-invasive image verification is required, such as in clinical image authentication.

7. Quantum Turing Machines (QTM)

It provides a theoretical model for simulating watermarking processes in quantum systems. These abstract machines allow researchers to analyse and understand the computational behaviour of watermark embedding and extraction at a fundamental level. Through QTM, complex interactions between image data and watermark information can be explored in ways not feasible using classical computational models.

8. Quantum State Transfer (QST)

This method facilitates the secure and lossless transmission of WM data across quantum communication networks. Utilising the principles of quantum teleportation, this technique ensures that the embedded WM may be relocated without physically moving the underlying data, and without the risk of interception offering a highly secure communication pathway.

9. Quantum Denoising Techniques

These techniques are essential for sustaining the clarity and fidelity of watermark-embedded images, particularly under conditions involving image compression or transmission noise. These techniques enable effective recovery and preservation of both the diagnostic image and the embedded watermark, which is critical in medical imaging applications.

The integration of these advanced quantum mechanisms significantly enhances the overall performance, security, and adaptability of watermarking systems in medical imaging. When properly implemented, these technologies offer solutions that are secure, resilient, and computationally efficient. Hybrid frameworks that combine quantum and classical methods are also emerging as practical approaches, capable of functioning within today's technological constraints while remaining adaptable to future developments in healthcare data security.

III. QUANTUM EMBEDDING AND EXTRACTION ALGORITHMS: AN OVERVIEW

Quantum embedding and extraction offer significant advantages, including enabling exponential speedup in certain quantum algorithms, facilitating the parallel processing of complex data, and serving as a natural fit for quantum machine learning applications. These benefits make them powerful tools for leveraging quantum systems to solve problems beyond the reach of classical computing. However, their implementation comes with limitations. High fidelity is required during the embedding process to prevent errors, and embedding high-dimensional data can demand substantial qubit resources, which may exceed the capacity of current quantum hardware. Additionally, quantum noise and decoherence pose challenges by potentially degrading embedding's, impacting the reliability of computations. Overcoming these limitations is essential to fully realise the potential of quantum embedding and extraction techniques.

Quantum Embedding involves mapping classical data into the quantum domain by encoding it into quantum states. This process leverages quantum phenomena such as superposition and entanglement to represent data in exponentially large Hilbert spaces. Various embedding methods exist; each tailored to specific applications. For instance, angle encoding uses rotation angles of quantum gates to encode numerical data into qubits, offering a straightforward approach compatible with noisy intermediate-scale quantum (NISQ) devices. Quantum kernel embedding maps classical data into high-dimensional quantum feature spaces, enhancing the performance of machine learning models like quantum support vector machines (QSVM). Similarly, tensor network encoding and quantum graph embedding efficiently represent complex datasets like high-dimensional data or graph structures, which are common in fields such as bioinformatics and material science. The general quantum embedding mathematical modelling is defined as below:

- i. **Encoding Classical Data:** Classical data $x = (x_1, x_2, \dots, x_n)$ is mapped to a quantum state indicated by the equation 9:

$$x \rightarrow |\psi(x)\rangle = \sum_{i=1}^{2^n} \alpha_i |i\rangle, \text{ Where } \sum |\alpha_i|^2 = 1 \text{ -----(9)}$$

- ii. **Amplitude Encoding:** The angle encoding is defined by the equation 10:

$$|\psi(x)\rangle = \frac{1}{\|x\|} \sum_{i=1}^n x_i |i\rangle \text{ -----(10)}$$

This is efficient in terms of qubits but may require complex circuits.

- iii. **Basis Encoding:** Each x_i is represented by n qubits where $x_i \rightarrow |x_i\rangle$

- iv. **Hybrid Encoding:** Combines amplitude and basis encoding for specific applications.

The following section discusses various quantum-based watermark embedding algorithms:

QWM using angle encoding is a technique that integrates classical data into quantum systems by encoding it into the angles of quantum gate operations, such as rotations Rx, Ry, and Rz. In this approach, classical information, like a watermark, is embedded into the quantum state by applying these rotation gates with angles determined by the data. The encoded data may be used to track or protect quantum information in a similar way classical watermarking protects digital content, but with the additional benefits of quantum superposition and entanglement. For example, a classical watermark might be embedded by using specific rotation angles that correspond to certain values in the data. This encoding process embeds the watermark into the quantum state, which can later be extracted or verified through quantum measurements. Angle encoding in quantum watermarking is particularly beneficial because it is efficient in terms of qubit usage, requiring fewer qubits than other methods like amplitude encoding. However, the technique's precision is constrained by the limited resolution of quantum gates, which could impact the robustness of the watermark, especially in the presence of quantum noise or gate imperfections.

Mathematical Model: Each feature x_i of classical data is embedded as defined by 11 and 12 respectively:

$$|\psi(x_i)\rangle = \cos(x_i) |0\rangle + \sin(x_i) |1\rangle, \text{ ----- (11)}$$

or using multi-qubit states:

$$|\psi(x_1, x_2, \dots, x_n)\rangle = Rx(x_1)Ry(x_2) \dots |0\rangle \otimes n \text{ ----- (12)}$$

Angle encoding finds significant applications in quantum machine learning models, particularly in variational quantum classifiers and quantum neural networks. By encoding classical data as rotation angles of quantum gates, it enables efficient data representation and processing within

quantum circuits. One key advantage of angle encoding is its lower qubit requirement compared to amplitude encoding, making it more suitable for near-term quantum devices with limited qubit availability. However, its resolution is constrained by the precision of quantum gates, as finite gate accuracy can introduce errors and limit the fidelity of the encoded data. This makes it essential to address hardware imperfections to ensure accurate computations and effective deployment of angle encoding in real-world applications.

Quantum graph embedding involves mapping classical graph structures into quantum states to leverage the power of quantum computing for solving graph-related problems, such as maximum cut or graph colouring. In this method, a graph is represented by a set of quantum states, where the vertices and edges are encoded into the quantum system, and quantum algorithms are used to explore the graph's properties. For example, in solving the maximum cut problem, the goal is to partition the graph into two sets such that the number of edges between the sets is maximised. Quantum graph embedding encodes this problem into quantum states, allowing quantum algorithms like the Quantum Approximate Optimization Algorithm (QAOA) to find the optimal partition more efficiently than classical approaches in certain cases. Similarly, for graph colouring, the quantum system can be used to explore different colour assignments for the vertices, optimising the colouring in a way that minimises conflicts. The advantage of quantum graph embedding is its ability to leverage quantum parallelism and entanglement, potentially offering exponential speedups for solving graph problems. However, the approach faces scalability issues, especially for dense graphs, where the number of quantum resources required increases significantly as the graph size grows. Despite these challenges, quantum graph embedding offers a promising avenue for solving complex graph-related problems in optimisation, combinatorics, and machine learning. The nodes i and j in a graph are encoded as defined by equation 13:

$$|\psi(G)\rangle = \frac{1}{\sqrt{Z}} \sum_{(i,j) \in E} w_{ij} |i,j\rangle \text{ ----- (13)}$$

where w_{ij} is the weight of the edge and Z is a normalisation factor.

Tensor network encoding in QWM involves encoding classical data into quantum states using tensor networks, such as Matrix Product States (MPS) or Tree Tensor Networks (TTN). These networks represent complex data structures efficiently by decomposing them into smaller, interconnected tensors that encapsulate the relationships between different parts of the data. In the context of quantum watermarking, the classical information—such as a watermark—can be embedded into the quantum system by manipulating the tensors that make up the quantum state. MPS and TTN are particularly powerful for this task because they allow for efficient representation and manipulation of high-dimensional data in quantum systems, making them ideal for storing and embedding information in a quantum state while minimising the number of qubits required. Tensor network encoding leverages the quantum entanglement properties of the network, enabling the watermark to be robust against certain types of noise or interference. The main advantage of this method is its efficiency in representing large data with relatively few resources, as tensor networks reduce the computational overhead of encoding complex data. However, for very high-dimensional or highly intricate data, implementing tensor network encoding can become computationally complex and challenging, especially when trying to maintain the fidelity of the embedded watermark across quantum operations. The mathematical Model is defined by the equation 14 as:

$$|\psi(x)\rangle = \sum_{i_1, i_2, \dots} T_{i_1, i_2, \dots} |i_1, i_2, \dots\rangle \quad (14)$$

where TT represents the tensor network.

Quantum Kernel Embedding is a technique that maps classical data into a quantum feature space using quantum kernels, a core concept for integrating quantum computing with machine learning. In this process, classical data is encoded into quantum states, and the relationships between data points are captured in a quantum feature space, which is represented by a quantum kernel. Quantum kernels allow quantum algorithms to calculate the similarity between data points more efficiently than classical methods, as they exploit quantum properties like superposition and entanglement. This method is particularly useful in machine learning tasks such as classification, clustering, and regression, as it enables the creation of complex decision boundaries that are computationally difficult for classical algorithms to identify. The quantum feature space, being high-dimensional, offers an exponentially larger capacity to represent intricate data patterns. Quantum kernel embedding, therefore, enhances the expressiveness and capability of machine learning models, particularly in cases where classical algorithms struggle to capture non-linearity's or high-dimensional relationships. However, one of its challenges is the requirement for efficient evaluation of the quantum kernel, as noise and sampling limitations in quantum hardware can affect the accuracy and reliability of kernel computations. The mathematical Model is defined by the equation 15:

$$K(x, y) = |\langle \psi(x) | \psi(y) \rangle|^2 \quad (15)$$

where, $|\psi(x)\rangle$ and $|\psi(y)\rangle$

→ Quantum states representing the embeddings

of classical data points x and y , respectively.

Quantum tomography is the process of reconstructing the density matrix of a quantum state by performing a series of measurements on a quantum system. This technique is particularly useful in quantum watermarking extraction, where the goal is to retrieve or verify embedded information (such as a watermark) in a quantum system. Quantum tomography involves taking measurements of various quantum observables in different bases, which provides statistical data on the quantum state's properties. By analysing the outcomes of these measurements, a complete description of the quantum state can be reconstructed. The

density matrix generated through this process encodes all the information about the quantum state, including both pure and mixed states, and allows for the determination of key characteristics such as purity, coherence, and entanglement. In the context of quantum watermarking, quantum tomography can be used to extract or verify the presence of the watermark by comparing the reconstructed state to the expected form of the watermarked quantum state. While it provides a complete and accurate picture of the quantum system, quantum tomography is computationally demanding, especially as the size of the quantum system grows, due to the exponential increase in the number of parameters required to describe the system. The mathematical model is given by the equation 16:

$$\rho = \sum_{i,j} \langle i | \rho | j \rangle | i \rangle \langle j | \quad (16)$$

where, $| i \rangle$ and $| j \rangle \rightarrow$
Represent basis states in the quantum system.

$\langle i | \rho | j \rangle$
 $\rightarrow$ elements of the density matrix, corresponding to the probability amplitudes or correlations between the states

Quantum watermarking based on Quantum State Discrimination (QSD) involves determining which quantum state, from a known set of states $\{|\psi_i\rangle\}$, has been prepared in a quantum system. This concept leverages the principles of quantum mechanics, such as superposition and entanglement, to encode unique watermark information into quantum states. Quantum state discrimination is crucial because quantum states cannot be perfectly distinguished if they are non-orthogonal, due to the no-cloning theorem and the probabilistic nature of quantum measurements. Instead, strategies like minimum-error discrimination or unambiguous state discrimination are employed, balancing accuracy and certainty. In watermarking, this enables the secure embedding and retrieval of information while preserving the quantum system's integrity, making it a potential tool for intellectual property protection, quantum communication, and secure authentication in quantum technologies. The mathematical model is defined by 17:

For nn known states, the optimal measurement minimises the error:

$$P_{error} = \min_{\{\pi_i\}} \sum_i p_i T_r(\pi_i \rho_i) \quad (17)$$

Where,

$\{\rho_i\} \rightarrow$ A set of quantum states that need to be distinguished.

$p_i \rightarrow$ The probability of each state ρ_i .

$\{\pi_i\}$
 $\rightarrow$ A set of positive operator
- valued measurement (POVM) elements satisfying

$$\sum_i \pi_i = I,$$

where I is the identity operator.

$T_r(\pi_i \rho_i)$
 $\rightarrow$ The probability of measuring outcome i when the system is in state ρ_i .

Quantum watermarking based on Quantum Phase Estimation (QPE) utilises the ability of quantum algorithms to extract eigenvalues (phases) of a unitary operator UU. In this process, the watermark information is encoded into the quantum state as a phase shift. QPE works by preparing a quantum system in a superposition state, applying the unitary operator UU, and performing quantum measurements to extract the eigenvalues associated with the encoded watermark. The robustness of this approach lies in the fundamental properties of quantum mechanics, ensuring high security and resistance to tampering. This method can embed the watermark in a way that is detectable only by authorised users, leveraging quantum superposition and entanglement to secure intellectual property in applications such as quantum cryptography and digital rights management. The mathematical model is defined by equation 18:

Mathematical Model: For an eigenstate

$$U | u \rangle = e^{i\phi} | u \rangle, \text{----- (18)}$$

where ϕ is the phase to be estimated.

Quantum watermarking extraction with quantum error mitigation is a process designed to ensure the integrity and accuracy of quantum computations by reducing the impact of noise, which is inherent in quantum systems. Noise in quantum computations can lead to errors that compromise the fidelity of results, particularly in noisy intermediate-scale quantum (NISQ) devices. By embedding a "quantum watermark"—a unique and distinguishable quantum state or pattern—into the computation, this technique allows for the identification and isolation of errors. Quantum error mitigation methods, such as zero-noise extrapolation, probabilistic error cancellation, or symmetry verification, are then applied to extract the desired noise-free results. This approach combines the robustness of quantum watermarking with advanced error correction strategies, enabling reliable quantum information processing even in the presence of hardware imperfections. It is particularly useful for applications in secure quantum communication, quantum cryptography, and error-resilient quantum computing. The mathematical model that uses error models $E(\rho)$ to infer the ideal result as defined by equation 19:

$$\rho_{ideal} \approx M(\rho_{noisy}), \text{----- (19)}$$

where M is the mitigation map.

QWM with entanglement extraction involves leveraging the unique properties of quantum entanglement to encode, secure, and verify information. The concept of entanglement extraction focuses on isolating and quantifying the degree of entanglement present in a given quantum state. This process is crucial for verifying the authenticity and integrity of quantum watermarked data, as entanglement serves as a non-cloneable resource that can uniquely represent

ownership or authorisation. By analysing the entanglement characteristics of a quantum state, such as its fidelity or concurrence, the embedded watermark can be extracted and authenticated. This approach offers robust security, as any tampering (Xia *et al.*, 2023; Sahu, 2022) with the quantum state would disturb the entanglement, making it detectable and ensuring the reliability of the watermarking process. The mathematical model defined by the equation 20 that uses measures like the concurrence or entanglement entropy:

$$S(\rho_A) = -Tr(\rho_A \log \rho_A), \text{----- (20)}$$

where ρ_A is the reduced density matrix.

Shadow tomography is a concept in quantum information science that enables the efficient extraction of key properties of quantum states using a minimal number of measurements. In the context of quantum watermarking extraction, shadow tomography is particularly valuable as it allows for the verification or retrieval of watermark information embedded in quantum states without fully reconstructing the state itself. By leveraging advanced mathematical techniques, such as randomised measurements and classical post-processing, shadow tomography significantly reduces the complexity and resources required compared to traditional methods. This makes it ideal for applications where preserving the quantum state's integrity is critical, as it avoids excessive disturbance to the system while ensuring accurate and reliable extraction of the embedded watermark. The mathematical model as defined by equation 21 that uses random measurements to estimate observables:

$$\langle O \rangle \approx \frac{1}{M} \sum_{i=1}^M Tr(O \rho^{(i)}) \text{----- (21)}$$

where M is the number of measurements. The Table 1 provides the comparison of different quantum watermark embedding algorithms used for medical images and Electronic Health Records (EHR):

Table 1. Comparison of different Quantum Watermark Embedding algorithms used for medical images and Electronic Health Records (EHR) (Moad *et al.*, 2022; Wu *et al.*, 2020; Hu *et al.*, 2019; Bose, 2022)

Algorithm	Description	Watermarking Approach	Security Level	Efficiency	Robustness	Medical Image/EHR Application
Quantum Diffusion Encoding	Embeds watermark in the quantum state using diffusion channels.	Quantum state manipulation	High (due to quantum encryption)	Moderate (requires quantum operations)	High (resilient to attacks)	Used for medical image privacy and secure transmission of EHRs.
Quantum Fourier Transform (QFT)	Applies quantum Fourier transform to embed watermarks in frequency space.	Frequency domain manipulation	High (quantum interference)	Moderate (complex computations)	Moderate (vulnerable to noise)	Suitable for medical images requiring frequency-based processing.
Quantum Neural Network (QNN)-based Watermarking	Embeds watermark using a neural network approach in quantum systems.	Neural network-based quantum embedding	Very high (neural network security)	High (adaptable to image data)	High (robust to noise and distortions)	Used for embedding watermarks in medical images with neural network adaptability for dynamic EHR data.

Quantum Secrecy Watermarking	Leverages quantum entanglement and secrecy to embed watermark data.	Entanglement-based embedding	Very high (quantum encryption)	Low (requires entangled states)	Very high (extremely robust)	Effective for confidential EHRs where data privacy is paramount.
Quantum Superdense Coding	Utilizes quantum entanglement to encode multiple bits of watermark in fewer quantum bits.	Superdense coding with quantum bits	High (secure due to entanglement)	High (efficient encoding)	Moderate (susceptible to decoherence)	Potential use for encoding watermarks in medical images to reduce data size.
Quantum Phase Encoding	Watermark embedding through phase modulation in quantum systems.	Phase encoding of quantum states	High (phase information is hard to detect)	Moderate (requires phase shifts)	High (resilient to noise)	Suitable for embedding watermarks in both images and EHRs requiring phase robustness.
Quantum Singular Value Decomposition (SVD)	Uses SVD for watermark embedding in quantum images.	Singular value decomposition	Moderate (requires optimal decomposition)	High (fast and efficient)	Moderate (vulnerable to attack if not properly protected)	Used for medical images requiring effective SVD-based processing.

Quantum Watermarking using	Embeds watermark by using quantum random walks on quantum graphs.	Random walk-based quantum encoding	walk-quantum	High (complex quantum walk structure)	(complex walk complexity)	Low (quantum walk complexity)	High (difficult to reverse)	to	Could be applied to EHRs and complex medical image datasets for extra protection.
----------------------------	---	------------------------------------	--------------	---------------------------------------	---------------------------	-------------------------------	-----------------------------	----	---

This table summarises various quantum watermarking techniques, with their potential applications in the medical domain, particularly in safeguarding medical images and EHR data.

The Table 2 provides a comparison for various quantum watermark extraction algorithms used in the context of medical images and Electronic Health Records (EHRs). The table highlights key aspects such as algorithm type, advantages, and potential limitations:

Table 2. Comparison for various quantum watermark extraction algorithms used in the context of medical images and Electronic Health Records (EHRs) (Li *et al.*, 2024; Lakhani *et al.*, 2024; Tang *et al.*, 2023; Artiles *et al.*, 2022)

Algorithm	Type	Advantages	Limitations	Applications
Quantum-based LSB (Least Significant Bit)	Classical and Quantum Hybrid	Simple implementation, low computational complexity, robust to noise.	Limited capacity, vulnerability to certain attacks.	Embedding watermarks in medical images.
Quantum Fourier Transform (QFT) Watermarking	Quantum Transform-based	High security due to quantum encoding, good for high-capacity watermarks.	High computational cost, complexity in extraction.	EHR data integrity verification.
Quantum Entanglement-based Watermarking	Quantum Entanglement	High robustness to attacks, secure due to quantum entanglement.	Requires entangled quantum states, harder to implement.	Medical image authentication.
Quantum Error-correcting Code Watermarking	Quantum Error Correction (QECC)	High error resilience, ensures data integrity during extraction.	Complex and resource-intensive, might affect data fidelity.	Medical image data protection, EHRs.
Quantum Superdense Coding	Quantum Communication-based	High capacity for watermark embedding, efficient data transfer.	Sensitive to noise, requires precise measurement and entanglement.	Embedding large watermarks in EHRs.
Quantum Hybrid Transform Watermarking	Hybrid Classical-Quantum Transform	Combines classical and quantum approaches, enhanced security and efficiency.	May require advanced quantum hardware, not fully scalable for large datasets.	Medical imaging data and patient records.
Quantum Steganography-based Watermarking	Steganography (Quantum)	Excellent for hiding watermarks without detection, high-level security [22].	Vulnerable to detection with sophisticated quantum attacks.	Hiding sensitive information in medical images.

Quantum Cryptography-based Watermarking	Quantum Cryptography	Strong security, leveraging encryption for watermark embedding.	Complex, high resource requirement for embedding and extraction.	Secure transmission of EHRs and images.
---	----------------------	---	--	---

This table presents a general comparison of different quantum watermarking techniques, focusing on their use for securing medical images and EHRs. Each algorithm has strengths and weaknesses depending on the specific requirements of security, capacity, and computational complexity.

The Table 3 provides a comparison for quantum watermark embedding and extraction algorithms used for medical images and Electronic Health Records (EHR) with respect to various aspects:

Table 3. A comparison for quantum watermark embedding and extraction algorithms (Fang *et al.*, 2019; Li *et al.*, 2021; Chopparapu *et al.*, 2023, 2024; Fang *et al.*, 2020 & Rijati *et al.*, 2025)

Aspect	Quantum Watermark Embedding Algorithm	Quantum Watermark Extraction Algorithm
Purpose	Embeds secret medical information (e.g., patient data, diagnosis) into quantum states of medical images or EHR for protection.	Extracts the watermark to verify the integrity of the medical image or EHR data.
Quantum State Representation	Utilises quantum bits (qubits) to encode watermark data within the quantum state of an image or EHR.	Reads the quantum state, recovering the embedded watermark without fully measuring the quantum state.
Measurement Approach	Uses a limited number of quantum operations (e.g., quantum gates) to embed watermark information, preserving the quantum properties.	Extracts the watermark by performing shadow tomography or other quantum measurement techniques, avoiding full state collapse.
Data Embedding Technique	Embeds the watermark as perturbations in quantum features (e.g., phase, amplitude) of the image or data using unitary operations.	Measures the extracted quantum state and applies classical decoding to reveal the watermark.
Robustness	Watermarking maintains the quantum nature of the data, resistant to quantum noise and manipulations.	Extraction is resistant to noise, errors, and attacks, with the watermark still detectable even with limited measurements.
Security	Quantum cryptography enhances the security, ensuring the watermark is imperceptible and secure against unauthorised tampering.	The watermark can be verified securely using quantum measurements, and any discrepancies indicate tampering or unauthorised access.
Complexity	Quantum circuits used for embedding the watermark are computationally efficient but	Extraction is complex, involving quantum measurement techniques like shadow

	require understanding of quantum mechanics.	tomography or quantum state tomography for precise retrieval.
Resource Requirements	Requires a quantum computer or quantum simulator to embed the watermark into quantum medical data.	Extraction also needs quantum resources but may require fewer qubits or operations compared to full state tomography.
Applications	Used for securing medical images (MRI, CT scans) or EHR by embedding sensitive data such as patient identifiers, treatment plans, or diagnostic information.	Applied to verify that medical images or EHR data have not been tampered with during transmission or storage, ensuring authenticity.
Advantage	Provides a secure and efficient method for watermarking medical images and EHR, leveraging quantum properties.	Enables extraction with minimal resource usage, allowing for verification of watermarked data without full state reconstruction.
Limitations	Requires access to a quantum system or simulator, and performance can be impacted by quantum noise.	May still require classical methods for final decoding, and potential quantum noise could affect the accuracy of watermark extraction.

This comparison highlights the strengths and limitations of both the embedding and extraction phases in quantum watermarking, with a specific focus on applications in the medical domain. These embedding and extraction processes are indispensable for bridging classical data with quantum systems, enabling breakthroughs in optimization, machine learning, cryptography, and beyond. As quantum hardware advances, these methods will play an increasingly critical role in harnessing the full potential of quantum computing. The general block diagram representing the process of Quantum watermarking embedding and extraction is shown in the Figure 1.

Quantum watermark embedding involves converting a classical image into a quantum representation (like NEQR or FRQI) and securely embedding a watermark using quantum operations, often protected by a key from Quantum Key Distribution (QKD). This ensures high security due to quantum properties like superposition and entanglement. During extraction, the watermarked quantum image is measured to retrieve classical bits, and the watermark is recovered using the same QKD key and reverse quantum logic. This process enables tamper detection and ownership verification with improved robustness and security over classical methods.

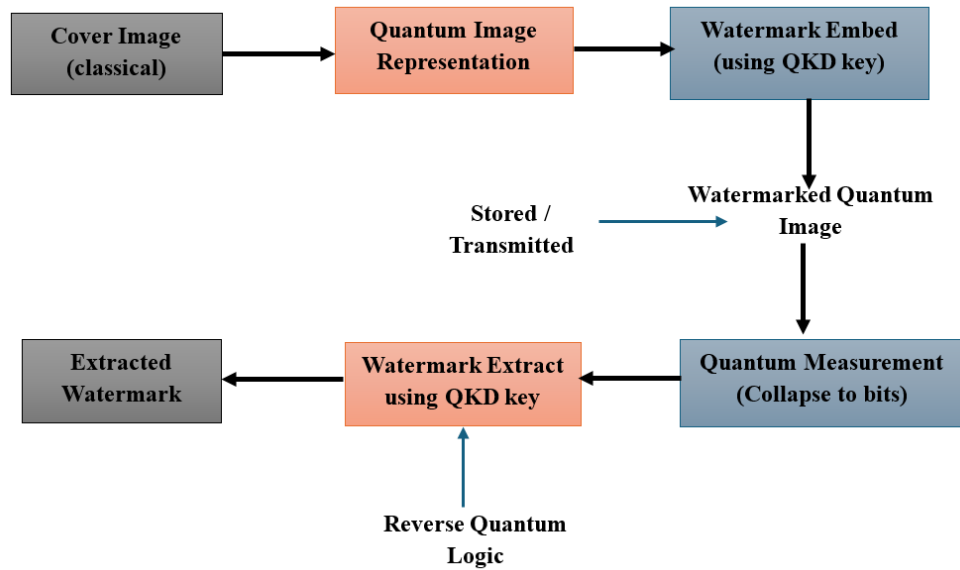


Figure 1. General Block Diagram of Quantum Watermark Embedding and Extraction Process

To assess the effectiveness and reliability of quantum watermarking techniques, several performance measurement parameters are utilised. Peak Signal-to-Noise Ratio (PSNR) is a critical metric that evaluates the imperceptibility of the watermark by comparing the original and watermarked images. A higher PSNR value indicates minimal distortion, which is essential in medical imaging where diagnostic accuracy must be preserved. Typically, a PSNR value above 40 dB is considered excellent for maintaining image quality. Bit Error Rate (BER) is another important parameter used to measure the accuracy of watermark extraction. It quantifies the proportion of incorrectly extracted bits relative to the total number of watermark bits, with a lower BER signifying higher reliability of the watermarking scheme. Additionally, Structural Similarity Index Measure (SSIM) can be employed to evaluate the perceptual similarity between the original and watermarked images, offering insights into visual fidelity. Normalised Correlation (NC) is often used to assess the similarity between the original and extracted watermark, providing a quantitative measure of extraction accuracy. Robustness is also evaluated by subjecting the watermarked content to common attacks such as compression, noise addition, and cropping, to determine the resilience of the embedded watermark.

These performance metrics collectively help validate the strength, imperceptibility, and applicability of quantum watermarking methods, particularly in sensitive domains like healthcare.

Despite its advanced capabilities, the proposed quantum watermarking (QWM) techniques are not without limitations. One major shortcoming is the high sensitivity to quantum noise and decoherence, which can degrade the fidelity of the embedded watermark during transmission or computation. Furthermore, the current limitations of quantum hardware, including restricted qubit availability, gate errors, and limited coherence times, pose significant challenges to real-world implementation. Another limitation is the complexity of quantum circuit design and simulation, which demands specialised expertise and tools, potentially limiting widespread adoption. Scalability is also a concern, especially when dealing with high-resolution medical images or large EHR datasets, as embedding and extraction operations may become computationally expensive. Moreover, secure key management in quantum environments remains a complex issue, particularly when integrating with classical systems. Addressing these shortcomings will be essential for transitioning QWM from theoretical

research to practical deployment in critical domains such as healthcare.

IV. CONCLUSION

Quantum watermarking represents a paradigm shift in digital security by leveraging the principles of quantum mechanics to achieve unprecedented levels of robustness, authenticity, and resistance to tampering. This technology has significant implications for securing sensitive data, particularly in fields like healthcare, where protecting medical images and Electronic Health Records (EHR) is critical. Despite its potential, quantum watermarking is still in its infancy and faces several challenges, including noise sensitivity, scalability issues, and high resource requirements. Security concerns such as vulnerabilities at the classical-quantum interface and key management complexities also need to be addressed. Additionally, the limited availability of reliable quantum hardware remains a significant barrier to its widespread adoption. Future research directions, including advanced error correction, hybrid classical-quantum models, real-world experimental validation, and hardware advancements, promise to overcome these limitations. The integration of AI and application-specific optimization can further enhance the applicability and effectiveness of quantum watermarking. As quantum

computing and communication technologies continue to evolve, quantum watermarking is poised to become a cornerstone of digital security, offering robust solutions for protecting sensitive data in various domains. Continued investment in research and development will be essential for unlocking the full potential of this transformative technology, ensuring its readiness for real-world applications.

Despite the promising features, the study also highlights certain challenges, including scalability issues, noise sensitivity, and the need for quantum-compatible infrastructure. Nevertheless, QWM represents a transformative approach to digital content protection, with profound implications for the digital forensics' community. It introduces new paradigms for secure evidence authentication, tamper detection, and data provenance in forensic investigations. As quantum computing matures, QWM is poised to become a cornerstone in the next generation of secure information systems, offering unmatched resilience and security assurance in high-stakes digital environments.

V. ACKNOWLEDGEMENT

We the authors hereby acknowledge the support provided by our respective institutions and colleagues during the preparation of this review.

VI. REFERENCES

- Artiles, JAP, Chaves, DPB and Pimentel, C 2022, 'Robust image watermarking algorithm using chaotic sequences', *J. Inf. Secur. Appl.*, vol. 68, p. 103219. <https://doi.org/10.1016/j.jisa.2022.103219>
- Bose, A and Maity, SP 2022, 'Secure sparse watermarking on DWT-SVD for digital images', *J. Inf. Secur. Appl.*, vol. 68, p. 103255. <https://doi.org/10.1016/j.jisa.2022.103255>
- Chopparapu, S and Seventline, JB 2023, 'An efficient multi-modal facial gesture-based ensemble classification and reaction to sound framework for large video sequences', *Eng., Technol. Appl. Sci. Res.*, vol. 13, no. 4, pp. 11263–11270. <https://doi.org/10.48084/etasr.6087>
- Chopparapu, S and Seventline, JB 2024, 'A hybrid facial features extraction-based classification framework for typhlotic people', *Bull. Electr.*

- Eng. Inf., vol. 13, no. 1, pp. 338–349. <https://doi.org/10.11591/eei.v13i1.5628>
- Chowdhury, K, Deb, S, Roy, KS, Podder, D and Sahu, AK 2024, 'A systematic survey on TPE schemes for the cloud: Classification, challenges, and future scopes', *IEEE Access* 12, pp. 160669–160689. <https://doi.org/10.1109/ACCESS.2024.3479228>
- Dhar, S and Sahu, AK 2024, 'Digital to quantum watermarking: A journey from past to present and into the future', *Comput. Sci. Rev.*, vol. 54, p. 100679. <https://doi.org/10.1016/j.cosrev.2024.100679>
- Fang, H, Chen, D, Huang, Q, Zhang, J, Ma, Z, Zhang, W and Yu, N 2020, 'Deep template-based watermarking', *IEEE Trans. Circuits Syst. Video Technol.*, vol. 31, no. 4, pp. 1436–1451. <https://doi.org/10.1109/TCSVT.2020.3009349>
- Fang, H, Zhang, W, Ma, Z, Zhou, H, Sun, S, Cui, H and Yu, N 2019, 'A camera shooting resilient watermarking scheme for underpainting documents', *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 11, pp. 4075–4089. <https://doi.org/10.1109/TCSVT.2019.2953720>
- Hu, WW, Zhou, RG, El-Rafei, A and Jiang, SX 2019, 'Quantum image watermarking algorithm based on Haar wavelet transform', *IEEE Access* 7, pp. 121303–121320. <https://doi.org/10.1109/ACCESS.2019.2937390>
- Lakhani, A, Gupta, N and Anand, A 2024, 'Enhancing robustness and security of medical images through composite watermarking method', *Soft Comput.*, pp. 1–14. <https://doi.org/10.1007/s00500-023-09557-z>
- Li, D, Dai, X, Gui, J, Liu, J and Jin, X 2024, 'A reversible watermarking for image content authentication based on wavelet transform', *Signal, Image Video Process.*, vol. 18, pp. 2799–2809. <https://doi.org/10.1007/s11760-023-02950-z>
- Li, J, Li, Y, Li, J, Zhang, Q, Yang, G, Chen, S and Li, J 2021, 'Single exposure optical image watermarking using a cGAN network', *IEEE Photonics J.*, vol. 13, no. 2, p. 6900111. <https://doi.org/10.1109/JPHOT.2021.3068299>
- Moad, MS, Kafi, MR and Khaldi, A 2022, 'Medical image watermarking for secure e-healthcare applications', *Multimedia Tools Appl.*, vol. 81, no. 30, pp. 44087–44107. <https://doi.org/10.1007/s11042-022-12004-0>
- Naima, S, Boukhamla, AZE, Narima, Z *et al.* 2025, 'Secure and imperceptible frequency-based watermarking for medical images', *Circuits, System and Signal Processing*, vol. 44, pp. 196–217. <https://doi.org/10.1007/s00034-024-02814-y>
- Rijati, N, Ghosal, SK, Sahu, AK, Sambas, A and Setiadi, DRIM 2025, 'DWT-DCT image watermarking with quantum-inspired optimization', *Int. J. Intell. Eng. Syst.*, vol. 18, pp. 1034–1044. <https://doi.org/10.22266/ijies2025.0229.74>
- Rupa, C, Malleswari, RP, Sultana, SA, Abbas, M and Sahu, AK 2024, 'Data privacy protection using Lucas series based hybrid reversible watermarking approach', *IEEE Access* 12, pp. 134578–134593. <https://doi.org/10.1109/ACCESS.2024.3459041>
- Sahu, AK 2022, 'A logistic map based blind and fragile watermarking for tamper detection and localization in images', *J. Ambient Intell. Hum. Comput.*, vol. 13, pp. 3869–3881. <https://doi.org/10.1007/s12652-021-03365-9>
- Solak, S, Abdirashid, AM, Adjevi, A and Sahu, AK 2024, 'Robust data hiding method based on frequency coefficient variance in repetitive compression', *Engineering Science and*

Technology, an International Journal, vol. 56, p. 101756.

Tang, Z, Chai, X, Lu, Y, Wang, B and Tan, Y 2023, 'An end-to-end screen shooting resilient blind watermarking scheme for medical images', J. Inf. Secur. Appl., vol. 76, p. 103547. <https://doi.org/10.1016/j.jisa.2023.103547>

Wu, H, Liu, G, Yao, Y and Zhang, X 2020, 'Watermarking neural networks with watermarked images', IEEE Trans. Circuits Syst. Video Technol., vol. 31, no. 7, pp. 2591–2601. <https://doi.org/10.1109/TCSVT.2020.3030671>

Xia, X, Zhang, S, Wang, K and Gao, T 2023, 'A novel color image tampering detection and self-recovery based on fragile watermarking', J. Inf. Secur. Appl., vol. 78, p. 103619. <https://doi.org/10.1016/j.jisa.2023.103619>