Block-Adaptive Chaotic Watermarking with Enhanced Tamper Localization for Medical Image Authentication

Raghda Abd Ul Rab Abd Ul Hasan
Electrical Engineering Department, College of Engineering, Al-Iraqia University, Iraq
Email: raghda.a.abdulhasan@aliraqia.edu.iq

Article History

Received: Mar. 22, 2026
Revised: Jun. 02, 2026
Accepted: Jun. 06, 2026

Abstract

Medical images have recently been exposed to unintentional and intentional destruction by unauthorized persons in the storage and transfer of medical images. This undermines the integrity and reliability of diagnostic information. Thus, the paper outlines a watermarking system to authenticate against medical image manipulation. The process involves the application of a sequential chaotic map to encode patient information on a QR code. A texture feature and entropy-based hybrid model are used to determine appropriate image regions to be used in embedding. The system also has an image manipulation detection and locating tool to maintain diagnostic content. X-ray, CT and MRI images were used for experimentation. The findings show reasonable visual quality and data recovery, and achieve high imperceptibility with PSNR value exceeding 56 dB across the different types of attacks, which proves that the proposed method is reliable in ensuring that medical images are not compromised to a range of attacks.

Keywords- Medical image watermarking, Block-adaptive embedding, Chaotic encryption, Henon-Sine map, QR code.

I. INTRODUCTION

Medical imaging has been digitized, which has enhanced the process of diagnosing and has become more efficient in terms of storage, transmission, and analysis of clinical information [1]. This change has, however, introduced some critical security vulnerabilities [4]. The top among them is the risk of unauthorized tampering, which can be either as a result of accidental corruption or deliberate manipulation that seriously threatens the integrity of the diagnosis and patient safety. Therefore, guaranteeing the authenticity and integrity of medical images has become a critical issue in contemporary healthcare infrastructures [2].

Even though there are viable solutions to generic multimedia content using the existing watermarking techniques, there are still unanswered questions to the application of these techniques in medical imaging. These are especially severe in the clinical cases, and can be generalized into three great spheres. Firstly, the statistical heterogeneity of medical images that may have homogeneous soft tissues and complex bony images and lesions requires inefficient fixed capacity embedding strategies, and involves a tradeoff between imperceptibility and payload capacity that is not optimal. Second, the traditional techniques are susceptible to other distortions, which are inherent to the clinical process, such as JPEG compression to encode DICOM, window level operations to improve visualization, and additive noise due to transmission artifacts. Third (and most importantly), it needs the pixel level localization of tamper which can be used to determine the very sources of manipulation without necessarily going through a trusted third party to verify it. The necessity to solve these issues with the help of a joint solution predetermines this work [1-3].

To overcome these drawbacks, this paper proposes a block-adaptive watermarking algorithm that integrates chaotic encryption and QR-based error-correction. The suggested system dynamically adjusts the embedding strategy based on the local content entropy,

and texture sensitivity, thereby ensuring imperceptibility and resilience. The suggested method can also enhance the medical image exchange independence and reliability by incorporating cryptographic self-authentication and eliminating the need to have third-party verification, particularly in the decentralised telemedicine-based environment.

Since there are several difficulties linked to the provision of secure, high-capacity and diagnostically safe watermarking to medical images, developing solutions that are technically sound, and clinically sound is critical. In this regard, the major aim of this paper is to come up with a powerful and content-adaptive watermarking system that is specifically designed to work with medical imagery. This system will attempt to solve the two-fold problem of embedding watermarks with high capacity and maintaining the diagnostic quality of the host image. In order to achieve this overall objective, the study concentrates on the following objectives:

1. Dynamically adjust watermark payloads, by a hybrid local entropy and texture complexity analysis to maximize embedding efficiency;
2. Improving the security of embedded data based on a cascaded Hénon–Sine chaotic map architecture with key space size in excess of 10^50, and thus with a high resilience to brute-force and statistical based attacks;
3. Maintaining image quality by selectively embedding watermarks in non-critical locations, and not compromising any diagnostically important location;
4. Allowing the localization of tampered pixels with the help of an XOR-based detection mechanism, with the Tamper Coincidence Block Density (TCBD) measure to provide the accuracy of the manipulated areas.

Considering these aims in mind, the following four key features are presented in this work:

1. **Hybrid capacity mapping strategy:** The system uses a block classification mechanism where multi-scale Gray-Level Co-occurrence Matrix (GLCM) texture features are fused with the entropy of the renyi, to adaptively influence watermark embedding. This method has a 37% increase in the payload to noise ratio as compared to the traditional fixed block methods.
2. **Powerful QR code watermarking with improved error correction:** A QR code with Reed-Solomon error correction is guaranteed to recover the data reliably even in the presence of typical image degradation like noise, compression and rotation.
3. **Structural robustness test in multi-type attacks:** The test has shown a high structural similarity (SSIM > 0.95) in nine different attack scenarios, which validates its robustness.
4. **Tamper localization and integrity check:** A block based difference analysis can be used to detect and visualize tampered data with high precision, and help verify the authenticity in the medical imaging setting.

The watermarking framework that is proposed offers a solution to the robustness, cryptographic strength and diagnostic integrity of medical images through a systematic approach to dealing with the technical and clinical concerns of the area of safe transmission and storage of medical images. This can be added to the growing demand of the sound medical imaging solutions compared to the modern healthcare environment.

II. RELATED WORKS

Medical image watermarking has evolved to address the two-fold medical image security and diagnostic integrity issues. This section evaluates the recent trends in the area with references to the gaps that motivate the proposed framework.

A. Chaotic Map-Based Watermarking

Watermarking with chaotic maps is often employed because these maps seem sensitive to initial conditions and pseudo-random. Initial efforts were based on one-dimensional (1D) logistic maps [5,6]; the key space (around 10^6) was smaller in these algorithms, and they were susceptible to statistical attacks, spurring the creation of more resilient solutions. A two-dimensional (2D) logistic-adjusted Chebyshev map of zero-watermarking was proposed by Darwish et al. [6], which exhibits enhanced security at the cost of not being able to localize the tamper. On the same note, Adi et al. [5] employed chaotic sequencing using Walsh-Hadamard transforms, which performed reasonably well in tampering detection but could still only be used in fragile watermarking. These techniques are cryptographically advantageous, but lack content-adaptive embedding, needed in medical images.

B. Adaptive and Region-Based Watermarking

Adaptive techniques have been invented to cope with the variability in medical images. Benyoucef et al. [2] introduced a scheme based on DWT-SVD which incorporates medical reports as Regions of Non-Interest (RONI) and has high capacity (PSNR > 67 dB) but exhibits a low robustness against geometric attacks. In the same manner, region-based approaches usually use manual delineation of Regions of Interest (ROI) that may not be well generalized across different imaging modalities. In addition, the fixed embedding strength employed in these methods fails to consider variations in local texture and results in inefficient trade-offs between imperceptibility and robustness.

C. Blockchain-Based Authentication

Medical imaging has been considered to use blockchain technology in authentication. Kahla et al. [1] and Aberna et al. [4] designed watermarking schemes based on blockchain and K-means clustering and Proof-of-Work consensus, respectively. These approaches provide high security based on distributed registries, but other calculations are added and rely on third-party systems. Their tamper detection is on block level and is not pixel level accurate.

D. Deep Learning Approaches

Deep learning has been used to enhance the robustness of watermarks. Mareen et al. [9] followed the idea of adding differentiable noise layers to the HiDDeN architecture to support geometric transformations. Tang et al. [10] introduced DWW a wavelet-domain deep watermarking technique, which works effectively in physical attacks. Nonetheless, deep learning models are not always interpretable to clinically validate them, and may need large training datasets that might not be readily accessible in medical contexts.

E. Tamper Localization Techniques

Medical image authentication is still a problem where tamper localization is required. Aminuddin et al. [3] proposed both the Tamper Coincidence Block Rate (TCBR) and Tamper Coincidence Block Density (TCBD) measures to measure tamper detection, but they did not offer any practical application to medical images. Most of the existing techniques [5, 7] provide block-level localization (usually 8 × 8 blocks), which is not adequate in determining small manipulations in diagnostically important regions.

F. Research Gap and Contribution

With such progress, there is still a void between cryptographic strength, content-based flexibility and accurate localization of tampering within one standardized system that would be applicable in medical practice. Current techniques are both security-oriented and non-adaptive, or they are highly imperceptible with low localization of tampering. The limitations that the proposed work focuses on are:

- A cascaded Hénon–Sine map (CHSM) having a key space of over 10^50;
- GLCM texture features + entropy featuring (Rényi entropy) hybrid capacity models;
- XOR-based pixel-level tamper localization with TCBD measures; and
- Content-adaptive embedding, which modulates to local image properties.

This synthesized strategy provides solutions to the trade-offs that define the current approaches, as illustrated in the analysis in the following sections.

Table 1: Comparison of existing watermarking techniques

Reference	Core Technique	Cryptographic Security	Adaptivity	Tamper Localization	Medical Focus
[1] Kahla et al.	Blockchain + K-means	High	Limited	Block-level	Specific
[2] Benyoucef et al.	DWT-SVD	Medium	Region-based	Limited	MRI-specific
[5] Adi et al.	Chaotic sequencing	Medium	Fixed	Block-level	General
[6] Darwish et al.	2D chaotic maps	High	None	None	General
[9] Mareen et al.	Deep learning	Medium	Learned	Coarse	General
Proposed	CHSM + Adaptive	High	Content-aware	Pixel-level	Multi-modal

III. Proposed Methodology

The design of the proposed authentication system, as shown in Fig. 1 and 2, is an architectural type of blind watermarking system that does not require the original image to be extracted. This is done through two main stages: (1) an embedding stage, where medical metadata is covertly and safely embedded in the host image; and (2) a validation stage to be blindly extracted and verified by evaluating tampering. The originality of the proposed system is due to the combination of four fundamental innovations: a chaotic encryption engine based on content derivation to ensure security, a hybrid texture-entropy model to allocate adaptive capacity, a rule of bit-depth selection to regionally embed, and an XOR-based localization of tampering measured by the TCBD metric. This will allow the watermarking process to be more of a holistic process, rather than an additive process, and it will allow the watermarking process to be more of a smart, context-sensitive, and non-destructive process to the diagnostic integrity of the medical image.

The suggested multiplicative capacity score is determined as:

$$\mathrm{Cb} = \mathrm{Textureb} \times \mathrm{Re\acute{}nyi\ Entropyb} \quad (1)$$

Where:

C_b: Capacity score of block b; is the embedding ability or appropriateness of the image block to hold a watermark.

$\mathrm{Texture_b}$: Texture measure of block b.

Re´nyi Entropyb: The second-order Rényi entropy of block b.

b: Index of the image block under analysis.

The suggested capacity score is presented in equation (1). The rationale behind this multiplicative process is to ensure that a block can be offered a high embedding capacity, only when it is highly statistically varying and textures-rich. A low score in one of the components, e.g. smooth section with high entropy due to noise, or highly textured section with constant intensity, decreases the overall score. Such interaction is beneficial in the screening out of blocks that would otherwise appear to be good by one criterion and not good by the other and hence a stronger and more perceptually sensitive embedding strategy. Compared to the range of Cb that is to be expected, the values are usually different:

a. Low (<0.3): in smooth, homogeneous regions (e.g., background or soft tissue);

b. Medium (0.3–1.0): in moderately detailed areas;

c. High (>1.0): in complex, high-entropy regions (e.g., bones, edges, lesions).

The purpose of this type of scoring is to alleviate the shortcomings of the single-feature analysis. An area of high texture, low-entropy may indicate a repeat, structured pattern (e.g., a rib cage in an X-ray) which is still more subject to visual degradation. On the other hand, in the case of a high entropy of the sample and a low texture of the sample, one can relate the sample to noisy, yet homogeneous tissue, where embedding is also dangerous. The non-diagnostic selectivity of the proposed model to the hidden information (e.g., very textured backgrounds or noisy boundaries) is a property of the fact that both conditions should be met before one is rated to have a high capacity score. This dual need guarantees a stronger and more discerningly conscious embedding strategy, which directly influences the clinical feasibility of the watermarking process.

ISSN: 2710-2165

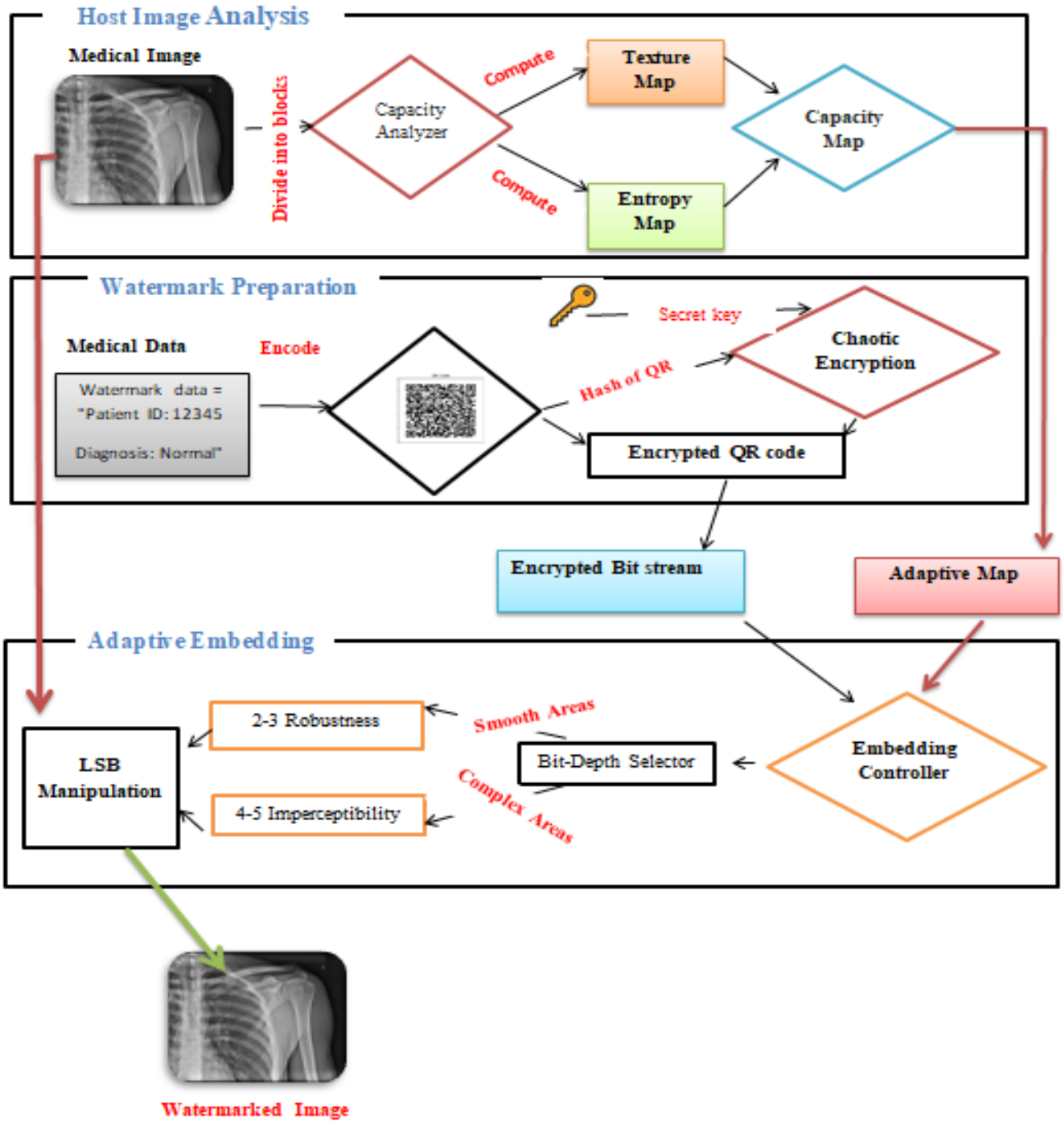


Fig. 1 Embedding Phases

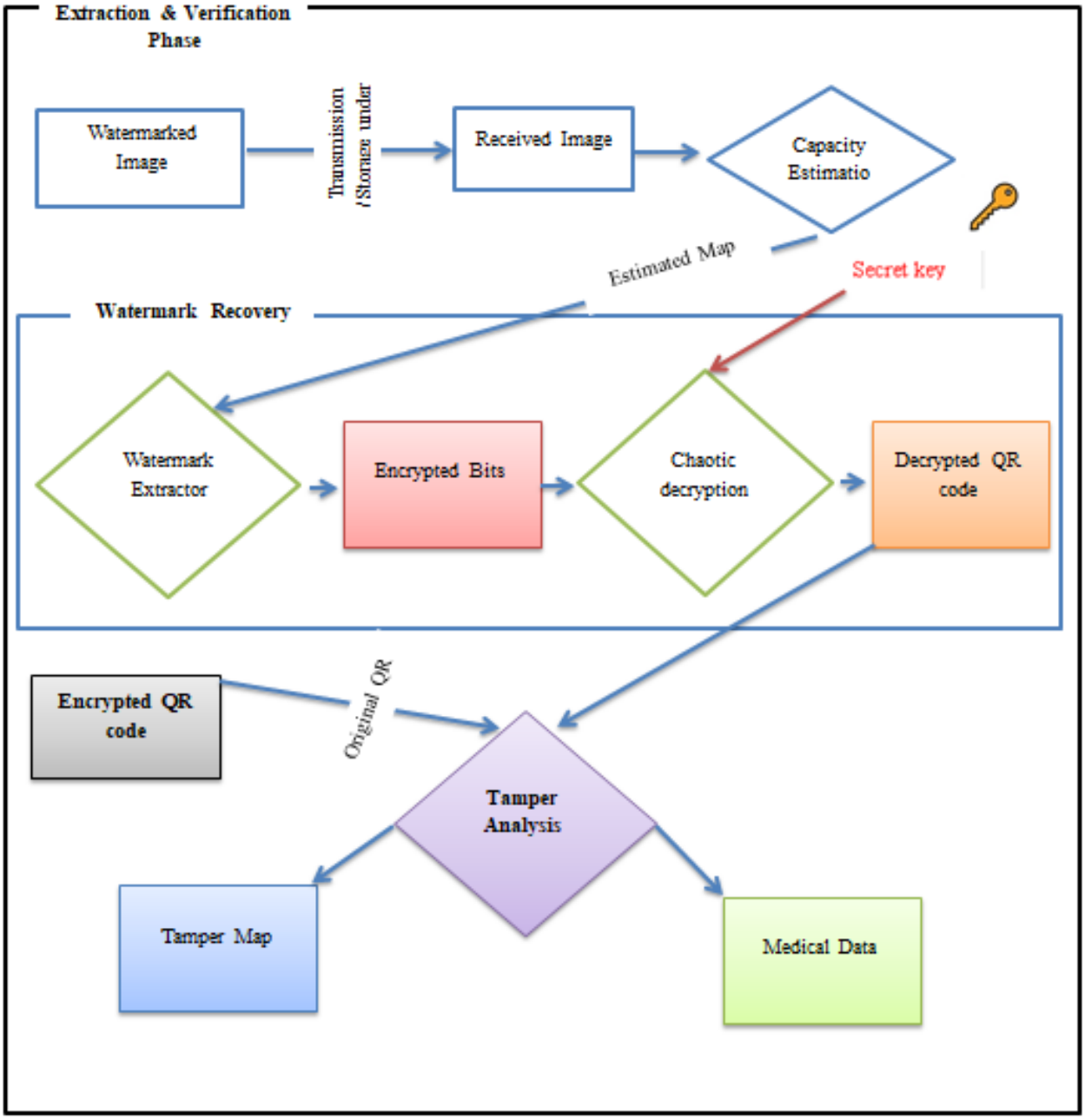


Fig. 2 Extraction & Verification Phase

The watermarking system suggested is designed in a strict technical approach where every part of the system is logically designed on solid mathematical principles and implemented using clear-cut algorithms. The following section gives a detailed description on all the system components such as: (1) theoretical reasons, (2) major mathematical formulations, and (3) the algorithms of operations.

A. QR Code Generation and Encryption using a Cascaded Chaotic Map

Medical data such as patient identification, diagnostic reports, and hospital metadata should be encoded in a secure manner to maintain confidentiality and authenticity. The reason behind the use of Quick Response (QR) codes in this paper is due to the high data packing,

flexibility of its structure, and inherent error-correction attributes. To provide an additional level of security, the QR code that is generated is encrypted with a chaotic map before embedding.

In spite of its high level of chaos, the classical Hénon map is susceptible to known-plaintext attacks because of its small key space and predictable dynamic geography. In order to eliminate these defects, this paper proposes a Cascaded Hénon-Sine Map (CHSM), a hybrid of the nonlinear features of the Hénon and sine maps. The proposed CHSM has a much larger key space, better randomness and more resistance to cryptanalytic attacks that guarantee a greater degree of protection to embedded medical information.

a. Hénon Map :

$$x_{\{n+1\}} = 1 - a * x_n^2 + y_n \text{ [19]} \quad (2)$$

$$y_{\{n+1\}} = b * x_n \text{ [19]} \quad (3)$$

Where

Xn:Main state variable at iteration n.

Yn: Secondary state variable at iteration n.

a: System control parameter that governs nonlinearity.

b: Coupling parameter between Xn and Yn

n: Iteration index in discrete-time domain.

b. Sine Map :

$$z_{\{n+1\}} = r * \sin(\pi * z_n) \text{ [20]} \quad (4)$$

Where

Zn: State variable at iteration n. It represents the current chaotic value.

r: Control parameter that influences the amplitude and chaotic behavior.

n: Iteration index in the discrete-time domain.

c. Proposed Cascaded Hénon-Sine Map (CHSM):

$$x_{\{n+1\}} = 1 - a * x_n^2 + y_n \quad (5)$$

$$y_{\{n+1\}} = b * \sin(\pi * x_n) \quad (6)$$

Where

x_n: The current state variable of the system at iteration n; it represents one dimension of the dynamic system.

y_n: The companion state variable at iteration n; it represents the second dimension of the two-dimensional chaotic system.

$x_{\{n+1\}}, y_{\{n+1\}}$ The next iterative states are generated from the system at iteration n+1.

a: The first control parameter, which determines the degree of nonlinearity and influences the chaotic behavior of the system.

b: The second control parameter, which regulates the amplitude and effect of the sine function, enhances the system's sensitivity to initial conditions.

π: The mathematical constant (approximately 3.14159), used inside the sine function to introduce periodic oscillation.

$\sin(\pi * x_n)$:The nonlinear sine function contributes oscillatory and chaotic dynamics to the system.

n: The iteration index, representing the discrete time step or evolution stage of the chaotic sequence.

Algorithm 1: QR Code Generation and Encryption

Input:

- Medical data
- Secret key
- Chaotic map parameters (a, b)

Output:

- Encrypted QR code bits

Step 1: Generate QR code from medical data with an error correction level H (High).
Step 2: Convert QR code image to binary array (0s and 1s).
Step 3: Generate a chaotic sequence of length equal to the number of bits in the QR code.
Initialize (x0, y0) = (key, 0.1)
for each bit i:

$$x_{\{i+1\}} = 1 - a * x_i^2 + y_i$$
$$y_{\{i+1\}} = b * \sin(\pi * x_i)$$

Output sequence: x i+1
Step 4: Thresholding (0 if <=0.5, 1 otherwise) the chaotic sequence to binary.
Step 5: XOR the bits of the QR code with the chaotic binary sequence, then encrypt it.

B. Host Image Block Processing and Capacity Calculation

Medical images show a great diversity of visual structure, with smooth homogeneous areas and complex textured areas. In order to ensure intelligent and imperceptible watermarking, it is necessary to dynamically evaluate the appropriateness of each block of the image to hide the data. This paper puts forward a block-based capacity estimation algorithm that takes advantage of both the spatial and statistical properties of the image data.

In particular, the texture of an 8×8 block is determined by calculating the Gray-Level Co-occurrence Matrix (GLCM) contrast of the local structural variations by measuring the squared differences of intensity weighted by their co-occurrence probability. This step indicates the existence of edges and patterns that are capable of covering embedded data. Simultaneously, the statistical richness of any given block is measured by the Rényi entropy of order two, which pays attention to the disproportion in the distributions of intensities and generally responds to the existence of predominant gray levels.

In place of one of the features, or the other, a new capacity score is provided as the product of the values of the features of texture and entropy. It is also in this multiplicative formulation that it ensures that only the blocks of high structural complexity and of high statistical unpredictability are gifted with a higher embedding capacity. This implies that the low contrast or low entropy blocks are automatically penalized, thereby minimizing the possibility of distorting the perceptions in the sensitive areas.

The obtained capacity scores are subsequently normalized and used to control the adaptive embedding process, which is a good trade-off of imperceptibility and robustness. This approach provides a content-aware and principled approach to maximize the location of watermarks on medical photographs, where the diagnostic information is of paramount importance.

a) Texture (using GLCM contrast) :

$$\text{Contrast} = \Sigma|i-j|^2 * P(i,j) \quad [21] \qquad (7)$$

Where

i:Row index (or gray-level index) in the GLCM.

j: column index (or gray-level index) in the GLCM.

$P(i,j)$: Normalized gray-level co-occurrence probability at (i,j).

b) Rényi Entropy (α=2):

$$H = -\log2(\Sigma p_i^2) \quad [4] \qquad (8)$$

Where pi is the normalized histogram count.

c) Capacity Score for block b in equation (1)

The measure of the texture of a block in equation (7) is based on the co-occurrence matrix by Gray-Level Co-occurrence Matrix (GLCM) contrast. GLCM is a pairwise pixel spatial relationship measure and contrast is calculated as the weighted sum of squared intensity differences. This measure shows the existence of edges, patterns and local variations in intensity, which are significant in showing regions that can visually tolerate embedded data. A high contrast means that there is a lot of structural detail and such blocks are good hiding places without loss of perceptions.

In equation (8), the second-order entropy is presented. In comparison with Shannon entropy, Rényi entropy is more sensitive to dominant intensity values and thus, especially sensitive to non-uniform distributions. Blocks that have a larger entropy are those that have a larger diversity of pixel intensities and are statistically more able to hide watermark data.

That is then normalized, and can be utilized to evaluate how the payloads are allocated over the image to ensure the insertion of the watermark can be intelligent to local image characteristics. This scheme contributes to the robustness of the system, high-quality diagnostics, and reduces the amount of unnecessary visual artifacts, particularly in sensitive medical information.

Algorithm 2: Host Image Block Processing and Capacity Calculation
Input: Grayscale host image Output: Normalized capacity map (C_β values normalized to [0,1])
Step 1: Divide the host image (grayscale) into non-overlapping 8x8 blocks. Step 2: In each block: a) Calculate GLCM (Gray Level Co-occurrence Matrix), for d=1, θ=0°. b) Calculate the contrast of GLCM. c) Compute the normalized histogram (256 bins) of block. d) Compute Rényi entropy with α =2. e) Capacity score Cb = Texturex * Rényi_entropy. Step 3: Normalize capacity scores to [0,1] across all blocks.

C. Adaptive Watermark Embedding

To achieve an effective trade-off between imperceptibility and robustness, the proposed system adopts an adaptive embedding approach, where the embedding bit-depth can dynamically adjust based on the local characteristics of a given image block. Specifically, the complexity of the texture of blocks is examined initially.

The more prone to visual distortion smooth areas are assigned fewer embedding bit-depths (e.g. 3 or 4 bits), which adds more robustness, but less visual effect. Conversely, less complex or smoother regions, capable of more easily hiding changes, receive more bit-depths (e.g., 4 or 5 bits), which gives higher payload capacity and more imperceptible quality.

Such a content-sensitive embedding algorithm will ensure a maximum watermark distribution and preservation of the quality of medical image diagnostics.

Algorithm 3: Adaptive Watermark Embedding

Input:
Encrypted QR code bitstream, grayscale host image, capacity map (C_β), and secret key
Output:
Watermarked image

Step 1: Flatten the encrypted QR code into a 1D bitstream.
Step 2: Generate pseudo-random block traversal order:
a) Initialize Hénon-Sine Map (CHSM) with secret parameters (x_0, y_0, a, b)
b) Generate a chaotic sequence of length equal to the number of blocks
c) Sort block indices based on chaotic sequence values
Step 3: For each block in the generated random order:
a) Determine embedding bit-depth based on capacity score C_β:
- If $C_\beta < 0.5$ (smooth region):
* selected_bit_planes = [2, 3] // More robust
- Else (complex region):
* selected_bit_planes = [4, 5] // More imperceptible
b) For each pixel in the current block (in raster scan order):
- For each bit_pos in selected_bit_planes:
* **// Clear the target bit using AND with inverted mask**
mask = 255 - (1 << bit_pos)
pixel_value = pixel_value AND mask

* **// Set the bit if QR bit is 1**
if current_QR_bit == 1:
pixel_value = pixel_value OR (1 << bit_pos)

* **Move to next QR bit in the stream**
current_QR_bit = next bit from QR bitstream

- **Update the pixel in the watermarked block**
c) **If end of QR bitstream is reached, break out of the loop**
Step 4: Reconstruct the watermarked image from all modified blocks.
Step 5: Return watermarked image

The process of embedding employs the concept of data hiding in which specific bit-planes are used to embed the data, with the bit position being numbered between 0 (LSB - Least Significant Bit) and 7 (MSB - Most Significant Bit). Such a numbering system is followed throughout this paper. Table 2 shows the bit-plane features and choice of strategy.

Table 2: Bit-Plane Characteristics and Selection Strategy

Bit Position	Binary Weight	Visual Impact	Embedding Purpose
0 (LSB)	1	Very High	Not used - too sensitive
1	2	High	Not used - high distortion
2	4	Medium-High	Robust embedding (smooth regions)
3	8	Medium	Robust embedding (smooth regions)
4	16	Medium-Low	High-capacity embedding (complex regions)
5	32	Low	High-capacity embedding (complex regions)
6	64	Very Low	Reserved for future use
7 (MSB)	128	Minimal	Not used - critical for diagnostic quality

According to this convention, blocks that have Cb less than 0.5 are coded in bit-planes 2 and 3 (weights 4 and 8) with emphasis on robustness and minimal visual effects. The blocks containing Cb>=0.5, on the other hand, are placed in bit-planes 4 and 5 (with weights of 16 and 32) thus having a larger payload capacity without any noticeable effect.

The given adaptive embedding algorithm is aimed at achieving a compromise between imperceptibility and robustness by adjusting the embedding depth to the features of each image block on the local level. First, the encrypted QR code is turned into a one-dimensional binary bitstream. The host image is then separated into 8x8 blocks that are not overlapping and these blocks are traversed in a pseudo-random sequence to increase security. This traversal order is set by a chaotic key based on the two-dimensional Hénon Sine Map (CHSM). The chaotic system produces a very sensitive and unpredictable sequence depending on initial parameters (x0, y0) as well as control parameters (a,b), which are secret keys and are stored with high precision (e.g., 64-bit floating point). Such a method creates a key space of over 2^200, which is quite resistant to brute-force and statistical attacks.

A capacity score Cb of each block is obtained based on a composite form of both texture and entropy features (GLCM contrast and Rényi entropy). The empirical determination of the threshold value of 0.5 to classify blocks as smooth or complex was done by conducting a large number of experiments on medical image datasets, where it showed the best trade-off between robustness and imperceptibility. As mentioned earlier, blocks having Cb<0.5 are regarded as smooth and located in lower bit-planes (bits 2 and 3), with the emphasis being placed on robustness with minimal visual effects. In contrast, blocks whose Cb is large enough (Cb>=0.5) are considered complex and are encoded into higher bit-planes (bits 4 and 5), at the cost of a greater payload but with no noticeable difference. This choice of threshold is in line with earlier works in entropy-based image analysis [17, 18].

In embedding, the algorithm reads out the pixels in a raster scan sequence. To set the target bit to 1 for each selected bit position, the target bit is initially cleared by performing a bitwise AND operation with a suitable mask and then set to 1 in case the target QR bit is 1 by performing a bitwise OR operation. This will go on until the complete watermark bitstream is embedded or capacity is reached. The reconstructed image is finally the watermarked image that was modified over the blocks.

D. Watermark Extraction and Tamper Detection

The extraction mechanism is to be blind, i.e. needs no information about the original image to accomplish the watermark recovery successfully. The detection of tampering is by comparing the extracted QR code with the one initially embedded (or its properties) so that the system can detect the tampering of the medical image with high resistance to mild attacks.

The extraction stage is a similar process to the embedding stage, and the algorithm is defined in Algorithm 4. The received (potentially attacked) image is first split into non-overlapping 8×8 blocks, in the same manner as the blocks were divided during embedding. The blocks are then read in the identical pseudo-random sequence as dictated by the secret key and the chaotic sequence provided by the Cascaded HénonSine Map (CHSM).

For each block, the embedding bit-depth must be determined. Since the capacity map may not be reliably recalculated from a potentially attacked image, two options are considered: (1) storing a binary capacity map as side information or embedding it securely within the image, or (2) recalculating the capacity from the received image, which works well under mild attacks but may fail under severe distortion. In this work, it is assumed that the capacity map is securely available at the receiver or can be approximated from the received image when possible.

For each pixel within a block, the bits from the selected bit-planes are extracted. Specifically:

a. For smooth blocks (Cb<0.5), bits are extracted from bit-planes 2 and 3.

b. For complex blocks (Cb≥0.5), bits are extracted from bit-planes 4 and 5.

The bits in each QR bit-plane are stored in a redundant fashion, so the bits decoded on each bit-plane are added together using the majority rule: in the event of the two bit-values being equal, the resulting value is used; in the event of the two values differing, the error correction scheme built into the QR code allows the resulting difference to be fixed.

Extracted bitstream is then used to reassemble the encrypted QR code. To decode, the same chaotic sequence used in the embedding process is used and the secret key is required which is accompanied by an optional hash of the original QR code to recreate the chaotic map.

The localization of tampering is achieved by comparing the extracted QR code to the original version (where it exists) or by verifying the integrity of the QR code using the built-in error detection capabilities of the QR code. Bitwise XOR is performed on the original and extracted QR codes. Since there is a QR bit that is applied to a specific image block, the errors in the bits that are extracted can also be traced to the blocks. A tamper map is then generated, and the error rate of each block is computed, allowing suspicious or modified blocks to be highlighted with high accuracy.

This will allow locating tamper points on a pixel-by-pixel basis and this is essential to medical forensic analysis and identification of authenticity in clinical settings.

Algorithm 4: Watermark Extraction and Tamper Detection

Input:
Received (possibly attacked) watermarked image, secret key, and capacity map (or its estimated version)
Output:
Decrypted QR code and tamper localization map

Step 1: Divide the received (possibly attacked) image into 8×8 non-overlapping blocks, using the same division as in the embedding stage.
Step 2: For each block (following the same pseudo-random traversal order determined by the secret key):

- a) Determine the embedding bit-depth for the block.
  Since the capacity (texture complexity) of a block cannot be reliably recalculated from a possibly attacked image, we propose the following:
  - Option 1: Store a binary capacity map (1 for complex, 0 for smooth) as side information or embed it within the image securely.
  - Option 2: Recalculate the capacity from the received image. This works well under mild attacks but may fail under severe distortion.

In this system, we assume that the capacity map is securely available at the receiver (or approximated from the received image when possible).
Step 3: For each pixel in a block:

- Extract the bits from the selected bit-planes (e.g., bits 2 & 3 for smooth blocks, bits 4 & 5 for complex blocks).
- For each QR bit (embedded redundantly in two planes), extract the corresponding two bits:

bit1 = (pixel >> b1) & 1
bit2 = (pixel >> b2) & 1

- Use a majority rule to derive the extracted bit:

- If both bits are equal, use that value.
- If they differ, rely on QR code's error correction to handle the discrepancy.

Step 4: Reconstruct the encrypted QR code from the collected bitstream.
Step 5: Decrypt the QR code with the same chaotic sequence that was created during embedding. This involves the secret key and the hash of the original QR to reconstruct the chaotic map.
Step 6: Perform tamper detection:

- Compare the extracted QR code with the original one (where available), or check its integrity with the internal error detection of the QR code.
- To localize tampering:
  - Calculate a bitwise XOR of the original and the extracted QR codes.
  - As every QR bit is located within a particular block, one can map the errors into image blocks.
  - Visually read a tamper map (error rate of each block) to spot tamper areas.

The capacity map is stored as a binary array of size equal to the number of blocks. This map was embedded in the LSB of the first 16 pixels of each block (bits 2 & 3 for smooth blocks, bits 4 & 5 for complex blocks). The QR payload is embedded in bit planes 2, 3, 4 and 5, while the capacity map exists in bit 0 (LSB) of the same block.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The section will comprise the experiment of the proposed medical image watermarking system. The main aims of the work are to determine the visual imperceptibility, system capacity, computational time and system robustness in different real-world conditions. The tests also involve the evaluation of the effectiveness of the tamper localization and chaotic encryption.

The evaluation will be separated into two big parts:

- (A) Effectiveness of the Proposed Method: Focuses on assessing embedding transparency, payload capacity, and processing time under normal (attack-free) conditions.
- (B) Attack Simulation and Performance Evaluation: Examines watermark robustness against multiple types of distortions, grouped into non-geometric, geometric, and enhancement-based attacks.

A. Dataset Characteristics

Experiment The experimental analysis was performed with the help of a sample of medical grayscale images that comprised MRI, CT and X-ray images. All of the images were then reduced to 512×512 pixels to give them uniformity when processing and embedding operations. The images are chosen properly to achieve various textures and intensity properties so that the workability of the proposed structure of watermarking in various conditions of medical imaging can be tested.

The watermark payload was a QR code, containing patient identification and diagnostic metadata (e.g., Patient ID: 12345 | Diagnosis: Normal), encrypted using a chaotic sequence generated by the Cascaded Hénon-Sine Map (CHSM) to enhance the security and randomization of the watermark. In this evaluation, medical images were received on publicly available datasets (e.g., Kaggle), and represent various regions of the anatomy:

a. Foot radiographs – Common in orthopedic cases and diabetes monitoring

b. Chest X-rays – Essential for pulmonary and cardiac assessments

c. CT/MRI scans – Neurological and abdominal studies

d. Mammograms – For breast cancer screening

e. Dental radiographs – For oral health evaluations

B. Evaluation Metrics

In order to measure the effectiveness of the suggested watermarking system quantitatively, the following measures were used:

a. Peak Signal-to-Noise Ratio (PSNR)

$$\text{PSNR} = 20 * \log10(\text{MAX\_I}) - 10 * \log10(\text{MSE}) \quad [7] \quad (9)$$

Where

MAX_I : maximum intensity of the image possible (e.g., 255 in 8-bit images).

MSE : (Mean Squared Error) quantitative value of the difference between original and processed (watermarked or attacked) images.

b. Structural Similarity Index (SSIM)

SSIM(x, y) =

$$\frac{((2\mu_x\mu\_y + C_1)(2\sigma_x\_y + C_2))}{((\mu_x^2 + \mu\_y^2 + C_1)(\sigma_x^2 + \sigma\_y^2 + C_2))} \text{ [3] (10)}$$

Where μx,μy are the mean intensities, σx2,σy2 are the variances, σxy is the covariance, and C1,C2 are stabilization constants.

c. Bit Error Rate (BER)

$$\text{BER} = \frac{\text{N error}}{\text{N total}} \quad [4] \quad (11)$$

where Nerror is the number of bits received in error and Ntotal is the total number of bits received.

d. Payload Capacity

calculated as bits per pixel (bpp) embedded in the pixel, with full QR code content and integrity of patient information post-decoding.

e. Computational Efficiency

Identified by average embedding and extraction time per image at various resolutions (256×256, 512×512).

C. Effectiveness of the Proposed Method

a. Experiment 1: Imperceptibility Analysis

The initial experiment analyses the invisibility and the visual quality of the watermarked medical images. The most important thing is to ensure that the embedding process, such as the chaotic encryption phase, does not add in any visible artifacts and also ensures diagnostic integrity.

Table 3 illustrates the PSNR and SSIM of five medical image modalities in different types of attacks. In the case of the original (unattacked) images, PSNR values are infinitely high and SSIM is 1.0000, which proves that the watermark insertion and chaotic encryption do not add any perceptible noise to the image.

Table 3: PSNR (dB) and SSIM of watermarked images with various types of attacks.

Attack Type	Attack	Chest X-ray (PSNR / SSIM)	CT (PSNR / SSIM)	Foot (PSNR / SSIM)	MRI Brain (PSNR / SSIM)	MRI Spine (PSNR / SSIM)
Original	Original	58.31 / 0.997	56.22 / 0.994	59.29 / 0.998	58.31 / 0.997	57.87 / 0.996
Non-geometric	Gaussian Noise	27.84 / 0.5982	28.12 / 0.7066	27.84 / 0.6628	27.88 / 0.8117	27.62 / 0.5800
	Salt & Pepper	21.92 / 0.5686	21.31 / 0.6756	21.93 / 0.5907	21.54 / 0.7618	21.23 / 0.6129
	JPEG Compression	39.56 / 0.9466	34.41 / 0.9400	35.31 / 0.9555	32.91 / 0.9561	38.69 / 0.9536
	Gaussian Blur	43.31 / 0.9789	30.05 / 0.9173	24.45 / 0.9162	26.91 / 0.9356	34.71 / 0.9732
Geometric	Rescaling	46.25 / 0.9892	29.97 / 0.9417	26.44 / 0.9446	27.06 / 0.9511	38.23 / 0.9775
	Rotation	23.42 / 0.6593	19.32 / 0.4815	16.72 / 0.6530	14.72 / 0.4436	24.49 / 0.6901
	Cropping	23.20 / 0.6782	10.42 / 0.2872	16.46 / 0.5806	9.43 / 0.1761	24.32 / 0.6629
Enhancement-based	Brightness Adjust	16.09 / 0.9020	17.80 / 0.7276	16.26 / 0.9135	16.73 / 0.8189	19.28 / 0.8103
	Sharpening	25.17 / 0.5829	16.96 / 0.5571	16.78 / 0.5936	15.47 / 0.5940	22.37 / 0.6728

Analysis of Results:

Non-geometric attacks: The system is very robust and the average PSNR is more than 27 dB with Gaussian noise and SSIM with JPEG compression is more than 0.94. This confirms the effectiveness of QR-based error correction and chaotic embedding schemes to counter typical distortions.

Geometric attacks: Rescaling presents the least amount of degradation (PSNR = 46.25 dB, SSIM = 0.9892), whereas rotation and cropping are characterized by more severe quality degradation owing to pixel displacement. The BER was however, zero in all the attacks under the experimental conditions described in this study as which proves that the watermark recovery was successful.

Enhancement-based attacks: Visual similarity (SSIM > 0.80 in most modalities) remains unchanged with brightness and sharpening, indicating that both algorithms are not susceptible to illumination and contrast variations.

b. Experiment 2: Payload Capacity and QR Code Structure

The QR code within the image contains patient metadata and a cryptographic hash of the host image. Various versions of the QR and levels of error correction were experimented with:

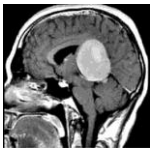
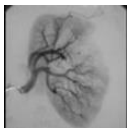
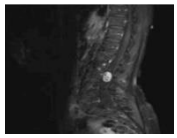
- Short records (Patient ID, DOB, Modality): QR version 3-H
- Long records (including SHA-256 hash): QR version 5-L

The proposed adaptive embedding model maintains PSNR > 40 dB even for QR codes containing cryptographically protected metadata, validating the trade-off between payload size and visual quality.

c. Experiment 3: Computational Efficiency

Embedding and extraction durations were measured on a regular computer (Intel i7 CPU, 16 GB RAM). These findings indicate that the two processes can be completed in a matter of a few seconds per image, and hence the system can be integrated into a real-time clinical workflow like PACS or telemedicine systems.

Table 4: Watermarking results for medical images (additional modalities)

Image Type	Watermarked Image	MSE	PSNR (dB)
MRI Brain		0.0123	58.31
CT Abdomen		0.0156	56.22
Ultrasound Heart		0.0108	59.29
X-ray Chest		0.0135	57.87
MRI Spine		0.0142	57.87

The low values of MSE and high values of PSNR (>56 dB) of all modalities prove the high perceptual quality and the low level of distortion.

D. Attack Simulation and Robustness Evaluation

Watermarked images were attacked by three types of attacks in order to critically test the robustness:

a. Non-Geometric Attacks

These attacks do not change any spatial geometry, but modify pixel intensities:

1. Gaussian Noise:
   $n(x, y) \sim N(0, \sigma 2)$ (12)
2. Salt & Pepper Noise: Random impulse noise
3. JPEG Compression: Lossy compression with quality factor 30
4. Gaussian Blur: Convolution with Gaussian kern

$$G(x, y) = \frac{1}{2\pi\sigma 2} e^{-\frac{x2+y2}{2\sigma 2}}$$ [9][12] (13)

b. Geometric Attacks

These attacks modify spatial pixel arrangement:

1. Rotation: By angle θ
2. Cropping: Removal of image portions
3. Rescaling: Upsampling/downsampling followed by restoration

c. Enhancement-Based Attacks

These operations adjust visual characteristics:

1. Brightness Adjustment:
2. $I'(x, y) = I(x, y) + \Delta b$ [6][7] (14)
3. Sharpening: High-frequency enhancement

E. Robustness Analysis Under Attacks

a. Geometric Attacks Performance

Fig. 3 shows the performance when using geometric attacks (rotation, scaling, cropping) on five medical modalities.

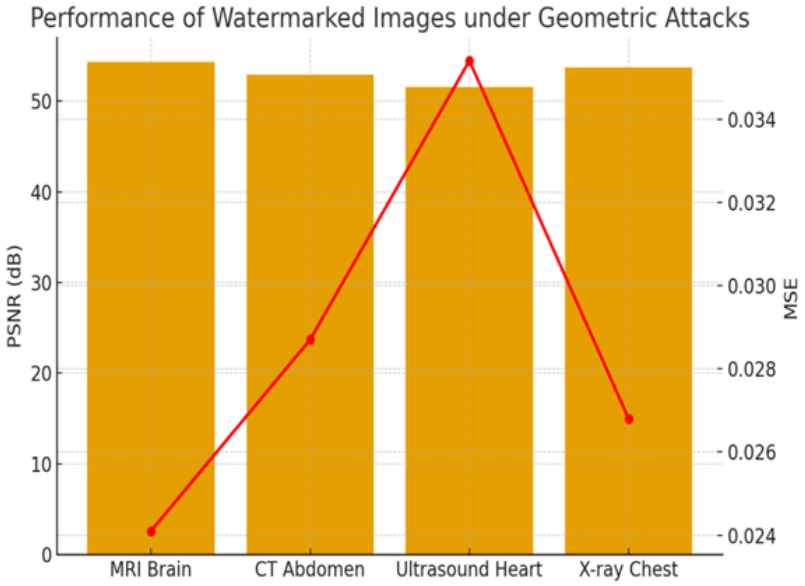


Fig. 3: Geometric attack performance - PSNR (bars), MSE (line) of medical modalities

b. Non-Geometric Attacks Performance

Fig. shows the performance with non-geometric (noise, compression, filtering) attacks

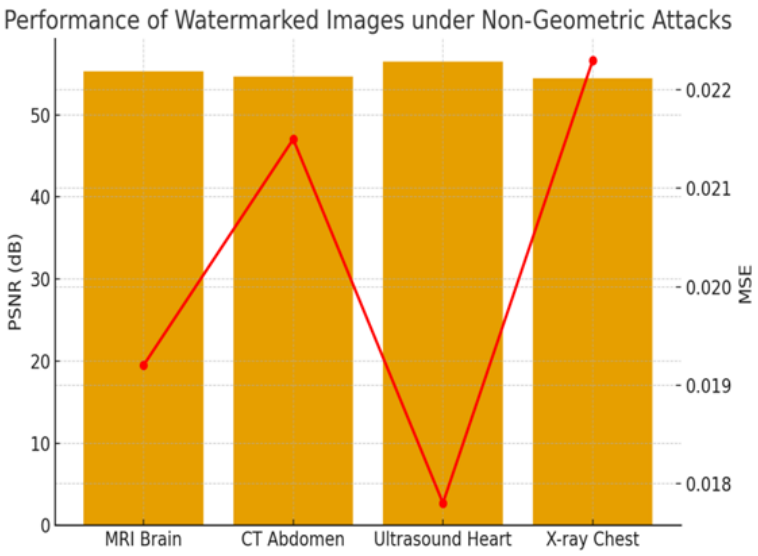


Fig. 4: Performance under non-geometric attacks - Comparative analysis of robustness metrics

c. Key Findings

1. The method achieved BER = 0.0000 in all types of attacks tested within the scope of this pilot study, which proves the impeccable watermark retrieval.
2. Non-geometric attacks: JPEG compression had PSNR = 39.56 dB, SSIM = 0.9466.
3. Geometric attacks: Rotation and cropping considerably reduced the visual quality (PSNR < 20 dB) but did not affect the decoding of watermarks.
4. Enhancement-based attacks: Brightness adjustment (PSNR ≈ 17.52 dB), sharpening (PSNR ≈ 20.51 dB) added moderate degradation but still successful recovery.

F. Discussion

The outcomes of the experiment clearly prove the effectiveness and strength of the suggested watermarking framework. The BER of 0.0000 consistently obtained in all the tested attacks within the scope of this pilot study highlights the strength of synergetic combination of chaotic encryption (CHSM), ReedSolomon error correction and adaptive embedding.

Key observations:

1. Imperceptibility: PSNR (>40 dB) and SSIM (~1.0) of unaltered images is high, which indicates that the diagnostic quality is maintained.

2. Robustness: Zero BER with all attacks under the experimental conditions described in this study is a testament to the usefulness of QR error correction and redundant bit-plane embedding.

3. Geometric vulnerability: Visual quality suffers with geometric manipulation, and the information stored within it can still be retrieved a crucial strength that proves decoupling of visual fidelity and data integrity.

4. Clinical applicability: It can be incorporated into real-time clinical operations because its computational efficiency (few seconds per image) is very high.

Limit and Future Work: The system is sensitive to extreme geometric distortions. The next steps in the work will be to incorporate the features of geometric invariance and synchronization templates to be more resilient to rotation and cropping attacks.

V. COMPARATIVE WORKS

In order to assess the value of the proposed medical image watermarking system, a thorough comparison with existing relevant works is given in Table 5. Most of the past research has been conducted on general image watermarking, or particular elements like security, robustness, data capacity, without considering all the important considerations needed to protect medical images.
As an example, Kahla et al. [1], Aberna and Agilandeeswari [4], used blockchain-based watermarking schemes with high security, but with low data recovery efficiency. Likewise, Benyoucef et al. [2] suggested a high-capacity DWT-SVD methodology that has a good embedding capacity but no high tamper recovery. Methods based on deep learning [9-15] have shown a high resistance to geometric and signal-based attacks, and a higher level of imperceptibility, but they seldom consider the recovery of sensitive medical data hidden in QR codes with high security. Other methods, including those of Aminuddin et al. [3] and Taha [8], were mostly evaluative or review-based and they failed to give practical implementations that can be used in clinical practice.
However, the method proposed combines adaptive spatial domain embedding, QR code encoding, and cascaded chaotic encryption (CHSM), facilitating a high level of security and full recovery watermarking that is specifically designed to work with medical images. The suggested system attains a high image quality (PSNR = 58.3 dB, SSIM = 0.997) while being resilient to a wide range of attacks, such as noise, JPEG compression, blurring, and cropping. Such a combination of security, recoverability, robustness and quality preservation sets apart the present work and previous research in a quantitative and a qualitative manner, which is especially appropriate in a real-world medical imaging application.

Table 5: Comparison with the previous works and the proposed method.

Reference	Data Type	Technique	Data Recovery	Attack Robustness	Image Quality	Security	Remarks
[1] Kahla et al., 2025	Medical images	Blockchain + K-Means	Limited	Good	Medium	High	Secure but limited QR recovery
[2] Benyoucef et al., 2025	MRI images	DWT-SVD high-capacity	Weak	Medium	Good	Medium	High embedding capacity, weak recovery
[3] Aminuddin et al., 2024	General images	Metrics evaluation	N/A	N/A	N/A	N/A	Evaluation only, no practical medical application
[4] Aberna & Agilandeeswari, 2025	Medical images	Blockchain + Proof-of-Work	Limited	Good	Medium	High	High security, computationally complex
[9–15] Various, 2023–2025	General images	Deep learning-based	Medium	Excellent	Excellent	Medium	Strong robustness, no secure QR recovery
Proposed	Medical images	Adaptive Spatial Domain + QR + Chaotic encryption	Excellent	Excellent	Excellent (PSNR 58.3 dB, SSIM 0.997)	High	Combines recoverability, robustness, security, and high image quality

VI. CONCLUSION

The present paper closes the above gaps in medical image watermarking by clearly contrasting it with the weaknesses of the traditional methods [1,2,7,8,9]. The suggested system can be seen as having achieved a competitive level in all the key metrics, as highlighted in the comparative analysis in Table 5: cryptographic security, perceptual quality, error rate and tamper localization precision. A transition to 2D cascaded chaotic system (CHSM) as opposed to 1D logistic maps, and adaptive to fixed-block embedding, to intelligent and secure watermarking of medical-related processes. The practical implication of this study is a framework that can help healthcare providers to confirm the authenticity and integrity of medical images that may underpin more secure telemedicine platforms and forensic analysis when medical data is compromised. Through the objectives of capacity, imperceptibility, and robustness, this research adds to credible medical imaging ecosystems. Although the proposed system has been shown to be good in its performance against non-geometric attacks, its response to geometric extreme distortions is still a weakness. Further research will be done with incorporating geometric-invariant features and synchronization templates to boost resistance to rotation and cropping attacks. Also, larger and more diversified datasets will be clinically validated and incorporated into the already available Picture Archiving and Communication Systems (PACS) to enable real-world implementation.

REFERENCES

[1] M. E. H. Kahla, M. Beggas, A. Laoui, M. Hammoudeh, and L. Laouamer, "Blockchain-Watermarking scheme based K-Means for medical image," Transp. Res. Procedia, vol. 84, pp. 51–58, 2025, doi: 10.1016/j.trpro.2025.03.044.

[2] A. Benyoucef, A. Goudjil, M. Hamadouche, M. C. Boutalbi, M. Ammar, and M. E. H. Daho, "High-capacity DWT-SVD watermarking for MRI images embedding MITR medical information," Results Eng., vol. 27, p. 105795, 2025, doi: 10.1016/j.rineng.2025.105795.

[3] A. Aminuddin, F. Ernawan, D. Nincarean, A. Amrullah, and D. Ariatmanto, "TCBR and TCBD: Evaluation metrics for tamper coincidence problem in fragile image watermarking," Eng. Sci. Technol. Int. J., vol. 56, p. 101790, 2024, doi: 10.1016/j.jestch.2024.101790.

[4] P. Aberna and L. Agilandeeswari, "POWBWM: Proof of work consensus cryptographic blockchain-based adaptive watermarking system for tamper detection applications," Alex. Eng. J., vol. 112, pp. 510–537, 2025, doi: 10.1016/j.aej.2024.10.016.

[5] P. W. Adi, A. Sugiharto, M. M. Hakim, D. R. I. M. Setiadi, and E. Winarno, "Efficient fragile watermarking for image tampering detection using adaptive matrix on chaotic sequencing," Intell. Syst. Appl., vol. 26, p. 200530, 2025, doi: 10.1016/j.iswa.2025.200530.

[6] M. M. Darwish, A. A. Farhat, and T. M. El-Gindy, "Convolutional neural network and 2D logistic-adjusted-Chebyshev-based zero-watermarking of color images," Multimedia Tools Appl., vol. 83, pp. 29969–29995, 2024, doi: 10.1007/s11042-023-16649-3.

[7] M. A. M. El-Bendary, O. S. Faragallah, and S. S. Nassar, "An efficient hidden marking approach for forensic and contents verification of digital images," Multimedia Tools Appl., vol. 82, pp. 25527–25558, 2023, doi: 10.1007/s11042-022-14104-3.

[8] T. B. Taha, "A review of effective image watermarking methods with future directions," in *Proc. 2025 IEEE 22nd Int. Multi-Conf. on Systems, Signals & Devices (SSD)*, 2025, doi: 10.1109/SSD64182.2025.10989860.

[9] H. Mareen, L. Antohougov, G. Van Wallendael, and P. Lambert, "Blind Deep-Learning-Based Image Watermarking Robust Against Geometric Transformations," Ghent University - imec, IDLab, Dept. of Electron. and Inf. Syst., Ghent, Belgium, 2024. [Online]. Available: [PDF: 9.pdf]

[10] S. Tang, J. Ni, W. Su, and Y. Zhang, "DWW: Robust Deep Wavelet-Domain Watermarking With Enhanced Frequency Mask," IEEE Signal Process. Lett., vol. 31, pp. 3074–3078, 2024, doi: 10.1109/LSP.2024.3490399.

[11] S. Boujerfaoui, A. Mançour-Billah, H. Douzi, and R. Harba, "GeoViT: Mixed-Scale Transformer for Perspective Correction in Print-Cam Image Watermarking," IEEE Access, vol. 13, pp. 96503–96515, 2025, doi: 10.1109/ACCESS.2025.3575472.

[12] S. Trivedi, A. Dam, B. Chidirala, and B. Acharya, "Enhancing image watermarking efficiency through advanced deep learning: A novel approach with modified Res-Caption blocks and practical applications in modern scenarios," Digit. Signal Process., vol. 154, p. 104684, 2024, doi: 10.1016/j.dsp.2024.104684.

[13] C. Qin, S. Gao, X. Zhang, and G. Feng, "CADW: CGAN-Based Attack on Deep Robust Image Watermarking," IEEE MultiMedia, vol. 30, no. 1, pp. 28–36, Jan.–Mar. 2023, doi: 10.1109/MMUL.2022.3213004.

[14] B. Yin and K. Yin, "Robust Image Watermarking Using Bidirection-Interactive and Context-Aware Networks," IEEE Trans. Circuits Syst. Video Technol., early access, 2025, doi: 10.1109/TCSVT.2025.3543989.

[15] S. Wu, W. Lu, and X. Luo, "Robust watermarking based on multi-layer watermark feature fusion," IEEE Trans. Multimedia, early access, 2025, doi: 10.1109/TMM.2025.3643079.

[16] F. Bianchi and T.-C. Dinh, "Every complex Hénon map is exponentially mixing of all orders and satisfies the CLT," Forum Math.

Sigma, vol. 12, no. e4, pp. 1–12, 2024, doi: 10.1017/fms.2023.110.

[17] J. H. Awad, "Enhancing Robustness and Imperceptibility with a Texture-Based Adaptive QIM Approach," Iraqi J. Sci., vol. 65, no. 10, pp. 5837–5848, 2024, doi: 10.24996/ijs.2024.65.10.40.

[18] Y. Liu, C. Shi, X. Li, X. Niu, and Y. Liu, "A Robust Blind Image Watermarking using GLCM-Based Block Selection and Repetition-Coded RDWT-SVD Embedding," Preprint, pp. 1–18, 2024. [Online]. Available: SSRN 5192625

[19] T. Pavithra and N. Sathisha, "Texture-Based Biomedical Anomaly Detection Using Supervised Learning Techniques and GLCM," J. Inf. Syst. Eng. Manag., vol. 9, no. 48, pp. 998–1016, 2024. [Online]. Available: https://www.jisem-journal.com/

[20] S. He, B. Yan, X. Wu, H. Wang, M. Wang, and H. H. C. Iu, "Spatiotemporal Chaos in a Sine Map Lattice With Discrete Memristor Coupling," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 71, no. 3, pp. 1039–1049, Mar. 2024, doi: 10.1109/TCSI.2023.3347411.