Iraqi Journal for Computer Science and Mathematics

Volume 5 | Issue 4 Article 15

2024

Secure Blind Medical Image Watermarking Using Hybrid Feature Extraction Techniques

Sawsan D. Mahmood
REsearch Groups in Intelligent Machines (REGIM Laboratory), National Engineering School of Sfax (ENIS), University of Sfax, Sfax 3038, Tunisia AND College of Education for Pure Science, University of Diyala, Iraq, pcomp.sawsan.dheyaa@uodiyala.edu.iq

Yassine Aribi
REsearch Groups in Intelligent Machines (REGIM Laboratory), National Engineering School of Sfax (ENIS), University of Sfax, Sfax 3038, Tunisia

Fadoua Drira
REsearch Groups in Intelligent Machines (REGIM Laboratory), National Engineering School of Sfax (ENIS), University of Sfax, Sfax 3038, Tunisia

Adel M. Alimi
REsearch Groups in Intelligent Machines (REGIM Laboratory), National Engineering School of Sfax (ENIS), University of Sfax, Sfax 3038, Tunisia AND Department of Electrical and Electronic Engineering Science, Faculty of Engineering and the Built Environment, University of Johannesburg, Johannesburg 2006, South Africa

Follow this and additional works at: https://ijcsm.researchcommons.org/ijcsm

Part of the Computer Engineering Commons

Recommended Citation

Mahmood, Sawsan D.; Aribi, Yassine; Drira, Fadoua; and Alimi, Adel M. (2024) "Secure Blind Medical Image Watermarking Using Hybrid Feature Extraction Techniques," *Iraqi Journal for Computer Science and Mathematics*: Vol. 5: Iss. 4, Article 15.
DOI: https://doi.org/10.52866/2788-7421.1223
Available at: https://ijcsm.researchcommons.org/ijcsm/vol5/iss4/15

This Original Study is brought to you for free and open access by Iraqi Journal for Computer Science and Mathematics. It has been accepted for inclusion in Iraqi Journal for Computer Science and Mathematics by an authorized editor of Iraqi Journal for Computer Science and Mathematics. For more information, please contact mohammad.aljanabi@aliraqia.edu.iq.

IRAQI JOURNAL FOR COMPUTER SCIENCE AND MATHEMATICS 2024;5:175–188

Scan the QR to view the full-text article on the journal website

RESEARCH ARTICLE

Secure Blind Medical Image Watermarking Using Hybrid Feature Extraction Techniques

Sawsan D. Mahmood [a,b,*], Yassine Aribi [a], Fadoua Drira [a], Adel M. Alimi [a,c]

[a] REsearch Groups in Intelligent Machines (REGIM Laboratory), National Engineering School of Sfax (ENIS), University of Sfax, Sfax 3038, Tunisia
[b] College of Education for Pure Science, University of Diyala, Iraq
[c] Department of Electrical and Electronic Engineering Science, Faculty of Engineering and the Built Environment, University of Johannesburg, Johannesburg 2006, South Africa

ABSTRACT

Watermarking offers great potential for medical images by embedding identifiable information that ensures secure and authenticated sharing of patient data while maintaining both integrity and diagnostic quality. In this paper, we present an innovative framework for blind medical image watermarking that harnesses advanced feature extraction techniques, including K-Means clustering, BRISK (Binary Robust Invariant Scalable Key-points), GFTT (Good Features to Track), and chaotic systems algorithms.

We conducted extensive experiments on the Ocular Disease Intelligent Recognition (ODIR) dataset, focusing specifically on Retinal Optical Coherence Tomography (OCT) images. The results highlight the framework's ability to preserve image quality and diagnostic utility, with minimal perceptual impact, as evidenced by strong evaluation metrics: a Mean Squared Error (MSE) of 0.0001, a Peak Signal-to-Noise Ratio (PSNR) of 85.27, a Structural Similarity Index Measure (SSIM) of 0.9999, a Normalized Correlation Coefficient (NC) of 1, and a Universal Average Change Index (UACI) of 0.

Overall, this framework represents a significant step forward in the secure sharing of medical images, ensuring that patient data remains protected and accessible without compromising diagnostic fidelity.

Keywords: Medical image watermarking, Machine learning, K-Means clustering, BRISK, GFTT, Image security, Data integrity, Entropy, PSNR, SSIM, Chaotic systems, Feature extraction, Robustness

1. Introduction

In the digital era, the secure transmission and storage of medical images have become paramount in the healthcare industry. Medical imaging plays a crucial role in diagnosis, treatment planning, and patient care, making it essential to ensure the integrity, confidentiality, and authenticity of the associated data. However, with the increasing reliance on digital technologies, medical images are vulnerable to a range of threats, including unauthorized access, tampering, and data breaches. These concerns necessitate the development of robust techniques to protect medical images while maintaining their diagnostic quality [1–3].

Watermarking has emerged as a promising solution to enhance the security of medical images. By embedding imperceptible watermarks into the images, critical information such as patient details, authentication codes, and integrity verification data can be securely transmitted along with the images. Traditional watermarking techniques have focused on spatial and frequency domain approaches, but these methods often face challenges in achieving the necessary balance between imperceptibility, robustness, and computational efficiency [4, 5].

Received 3 September 2024; accepted 10 November 2024.
Available online 26 November 2024

* Corresponding author.
E-mail address: pcomp.sawsan.dheyaa@uodiyala.edu.iq, sawsan.d.mahmood@regim.usf.tn (S. D. Mahmood).

https://doi.org/10.52866/2788-7421.1223
2788-7421/© 2024 The Author(s). This is an open-access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

Recent advancements in machine learning have opened new avenues for improving the effectiveness of watermarking techniques. Machine learning algorithms can be employed to optimize feature extraction, clustering, and classification tasks, enabling more secure and resilient watermarking methods. In this context, the combination of machine learning with traditional watermarking techniques offers a powerful approach to address the challenges of medical image protection [6, 7].

This paper introduces a novel framework for medical image watermarking that integrates K-Means clustering with Binary Robust Invariant Scalable Key-points (BRISK) and Good Features to Track (GFTT) algorithms. The proposed method leverages the strengths of spatial domain techniques to embed watermarks in a way that enhances security and robustness while preserving the image's diagnostic quality. By utilizing K-Means clustering for efficient image pixel clustering and feature extraction, then combining it with BRISK and GFTT for robust keypoint detection, this hybrid approach significantly improves the imperceptibility and resilience of watermarked images.

The framework is further enhanced by the incorporation of chaotic systems, which add an additional layer of security and ensure the reliability of watermark detection during transmission. The performance of the proposed method is evaluated using a range of image quality metrics, including Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Universal Quality Image Index (UQI), Structural Similarity Index Measure (SSIM), and Spatial Correlation Coefficient (SCC). Empirical evaluations conducted on the Ocular Disease Intelligent Recognition (ODIR) in particular, Retinal optical coherence tomography (OCT) medical images dataset demonstrate the effectiveness of the proposed framework in achieving a balance between imperceptibility, robustness, and security. The experimental results indicate that the method successfully preserves the image quality while embedding watermarks of varying lengths, ensuring high levels of security and integrity. The contributions of this paper include: (1) the integration of BRISK and GFTT for powerful feature extraction, (2) the application of K-Means clustering to enhance traditional watermarking techniques, and (3) the use of chaotic systems to strengthen the reliability and integrity of medical image sharing [8, 9].

This paper is organized as follows: Section 2 provides a background. Section 3 provides a review of related work in medical image watermarking and the integration of machine learning techniques. Section 4 details the proposed methodology, including the combination of K-Means clustering, BRISK, and GFTT algorithms. Section 5 presents experimental results and performance analysis, while Section 6 concludes with a discussion of the findings and future research directions.

2. Background

Medical images are crucial in modern healthcare, providing essential diagnostic information and aiding in treatment planning. The sensitivity of these images, generated from modalities such as MRI, CT scans, and X-rays, necessitates robust security measures to protect patient privacy and ensure data integrity. As medical imaging increasingly relies on digital systems for storage and transmission, the risk of data breaches and unauthorized alterations becomes a significant concern [10, 11]. Therefore, securing medical images involves addressing several challenges to maintain the integrity, confidentiality, and accessibility of sensitive patient data.

Traditional watermarking techniques include spatial and frequency domain methods. Spatial domain watermark involves modifying pixel values directly to embed a watermark [12]. The watermarked image $I_{\text{watermarked}}$ is obtained by adding a watermark W to the original image I_{orig}. The watermarking process can be described as follows for each position (x, y) in the image:

$$I_{watermarked}(x, y) = I_{orig}(x, y) + W(x, y) \tag{1}$$

Frequency domain watermarking, such as Discrete Fourier Transform (DFT) or Discrete Wavelet Transform (DWT), embeds the watermark into transformed image coefficients.

Let T be a transformation domain, and $C_{i,j}$ represent the coefficient at position (i, j) in the transformed domain. The watermarked coefficient $C'_{(i,j)}$ is computed by modifying the original coefficient $C_{i,j}$ with the watermark W and a scaling factor α. The generic formula is given by:

$$C'_{i,j} = C_{i,j} + \alpha W_{i,j} \tag{2}$$

Spatial and frequency domain watermarking techniques each offer distinct trade-offs in terms of robustness and imperceptibility. Spatial domain watermarking is simple and computationally efficient but can be vulnerable to processing attacks including common image processing operations, such as compression or filtering. On the other hand, frequency domain watermarks generally provide higher robustness against alterations and attacks [13] but can compromise visual quality. The choice between these methods depends on the specific requirements of the application, balancing the need for robustness against potential perceptual impacts on the image.

The advent of machine learning has significantly advanced the field of image processing, offering sophisticated methods that address challenges faced by traditional techniques and enhance overall performance. The classical machine learning pipeline involves several fundamental stages, including feature extraction and decision-making. Feature extraction, in particular, is a critical step in many image processing applications, including medical imaging, where accurate detection and analysis of key-points are essential for tasks such as disease diagnosis and treatment planning. Binary Robust Invariant Scalable Key-points (BRISK) and Good Features to Track (GFTT) are two notable techniques that have significantly improved feature extraction capabilities in computer vision [14, 15].

The evaluation of the watermarking scheme is conducted using several metrics:

- **Peak Signal-to-Noise Ratio (PSNR):** PSNR measures the quality of the watermarked image relative to the original image. It is defined as:

$$PSNR = 10.\log_{10}\frac{R^2}{MSE} \tag{3}$$

where R is the maximum possible pixel value of the image (e.g., 255 for 8-bit images), and MSE is the Mean Squared Error between the original and watermarked images.

- **Structural Similarity Index (SSIM):** SSIM assesses the perceptual similarity between the watermarked image and the original image. It is calculated as:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{4}$$

where μ_x and μ_y are the average pixel values of the original and watermarked images, σ_x^2 and σ_y^2 are the variances, and σ_{xy} is the covariance. C_1 and C_2 are constant to stabilize the division with weak denominators.

- **Mean Squared Error (MSE):** MSE quantifies the average squared difference between pixel values of the watermarked and original images. It is given by:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}[I_{orig}(i) - I_{watermarked}(i)]^2 \tag{5}$$

Where N is the number of pixels, $I_{\text{orig}}(i)$ is the pixel value of the original image, and $I_{\text{watermarked}}(i)$ is the pixel value of the watermarked image.

- **Normalized Correlation Coefficient (NC):** NC evaluates the correlation between the original and watermarked images. It is defined as:

$$NC = \frac{\sum_{i=1}^{N} I_{orig}(i)\cdot I_{watermarked}(i)}{\sqrt{\sum_{i=1}^{N} I_{orig}^2(i)\cdot\sum_{i=1}^{N} I_{watermarked}^2(i)}} \tag{6}$$

where N is the number of pixels, and $I_{\text{orig}}(i)$ and $I_{\text{watermarked}}(i)$ are the pixel values of the original and watermarked images, respectively.

- **Unified Average Changing Intensity (UACI):** UACI measures the average change in intensity between the watermarked and original images. It is defined as:

$$UACI = \frac{1}{N}\sum_{i=1}^{N}\frac{|I_{orig}(i) - I_{watermarked}(i)|}{R} \tag{7}$$

where N is the number of pixels, $I_{\text{orig}}(i)$ and $I_{\text{watermarked}}(i)$ are the pixel values of the original and watermarked images, and R is the maximum pixel value.

In this section, we established the background and fundamental aspects that underpin our proposed framework. Moving forward, we will explore the state-of-the-art techniques in the field, which will describe our methodology. Our approach focuses on blind watermarking within the spatial domain, leveraging a sophisticated feature extraction process to enhance the security and robustness of the watermark embedding.

3. Related work

Medical image watermarking has seen significant advancements over the years, driven by the need to secure and verify the integrity of sensitive medical data [22]. Various techniques have been proposed, each addressing specific challenges related to watermark robustness, image quality preservation, and capacity. This section reviews key approaches in the field, summarizing their methodologies and performance metrics, and highlights the contributions of our proposed method [23, 24].

An analysis conducted in [25] compares the performance of color plane watermarking with conventional two-level Discrete Wavelet Transform (DWT) watermarking. The study reports that color plane watermarking achieves a Peak Signal-to-Noise Ratio (PSNR) of 73.6239 dB, significantly higher than the 56.1993 dB PSNR observed with the conventional two-level DWT approach. To assess the robustness of Arnold's Scrambling, the correlation coefficient parameter was employed. The study also suggests that watermarking should be performed on individual color planes (Red, Green, and Blue) rather than the entire image to improve PSNR. In a different approach, the work by [10] introduces an imperceptible watermarking system designed to enhance the security of optical fundus images used in teleophthalmology and automated retinal diagnosis. This system maintains perceptual transparency through adaptive quantization parameters tailored for both healthy and diseased fundus images. The watermark ensures the integrity of computer-based diagnoses, allowing for accurate patient ID recovery during integrity verification at diagnosis centers. Despite testing on a comprehensive fundus image database, the method's effectiveness for automated retinal disease diagnosis remains limited.

Recent studies have also explored the application of chaotic algorithms for medical image encryption, driven by advancements in secure image transmission and storage [11]. Researchers have investigated various chaotic algorithms, such as chaotic logistics patterns and tent maps, based on principles of diffusion and confusion. The study presents a chaotic cryptosystem for medical image encryption, utilizing an optimization algorithm to select optimal secret and public keys, aiming to address the weaknesses observed in one-dimensional chaotic systems. In [26], Hassan et al. developed a hybrid watermarking technique incorporating Fast Curvelet Transform (FCT) and Singular Value Decomposition (SVD) to embed OCT/fundus scan images as watermarks. This approach demonstrated superior robustness, imperceptibility, and security compared to existing methods. The watermarking framework effectively preserves the integrity of automated retinal disease diagnosis and can be applied to authenticate medical images in eHealth environments by retrieving electronic patient records (EPR) from watermarked images. Narima Zermi et al. (2021) [27] proposed a blind watermarking method that uses the EPR principle and data from image acquisition to ensure both security and integrity. This method is noted for its imperceptibility and robustness, enabling watermarked images to resist conventional attacks while maintaining high quality. In [12], the authors introduced a watermarking technique for digital fundus images that utilize Singular Value Decomposition (SVD) to generate and embed the watermark. The technique maintains a constant embedding number across red and blue color planes and handles up to 329,960 bits for a $565 \times 584 \times 3$ image, with 43% of pixels embedded against jittering attacks. This method achieves 54 dB imperceptibility and demonstrates a cost-effective strategy with consistent performance.

Early work in medical image watermarking by Swaraja et al. [7] utilized a hybrid approach combining Discrete Wavelet Transform (DWT), Schur decomposition, and Particle Swarm Optimization (PSO). This technique achieved a Peak Signal-to-Noise Ratio (PSNR) of 36.99, suggesting good image quality preservation. However, the study lacked detailed metrics such as Mean Squared Error (MSE) and Structural Similarity Index (SSIM), which are essential for a comprehensive performance evaluation.

In a subsequent study, Su et al. [28] proposed a self-embedding fragile watermarking scheme utilizing binary message embedding. This method demonstrated a high PSNR of 45.05 and an SSIM of 0.9759, indicating effective tamper detection and high image quality preservation. Despite these promising results, the absence of additional metrics like MSE and Universal Image Quality Index (UIQI) limits the scope of performance assessment.

Jabbar et al. [29] combined hash signatures with watermarking techniques in the frequency domain. Their approach achieved an impressive PSNR of 72.62, showcasing its ability to maintain high image quality. However, the method did not include SSIM and MSE metrics, which are crucial for evaluating the impact on image structure and quality. Amiri et al. [30] explored a wavelet-based method combined with equilibrium optimization, achieving a PSNR of 41.11 and an SSIM of 0.9999. While this approach effectively preserved image quality and structural similarity, the evaluation would benefit from including MSE metrics to understand the degree of image distortion better. Taj et al. [31] introduced a reversible-zero watermarking scheme that employed a combination of DWT, Integer Wavelet Transform (IWT), and Difference Expansion. Their method achieved a PSNR of 20.8825, but detailed performance metrics such as MSE and capacity were not thoroughly addressed.

Arevalo-Ancona et al presented a combined approach to image verification and authentication, combining reversible watermark and zero-watermarking, to enhance the security of medical images. In zero-watermarking, a convolutional neural network extracts unique features from the image and combines them with the patient's image to generate a master share. For added robustness, a QR code is integrated with this master share. The QR code is embedded in the image by reverse watermarking method within regions of no interest determined by K-means algorithm. This approach determines the optimal region for QR code embedding in the intermediate frequency coefficients of the discrete Fourier transform [32].

The reviewed literature indicates substantial progress in medical image watermarking, with various techniques achieving notable results in PSNR and SSIM. However, comprehensive performance evaluation and capacity utilization remain as for improvement [33]. As previous studies, dealing with blind watermarks, especially with medical images containing complex details, is a major challenge due to the high resolution required to preserve the unique properties of medical imaging. While using the spatial domain to watermark medical images have both advantages and challenges. Although spatial domain watermarking is generally vulnerable to various attacks, making it less robust than frequency domain methods, it is often preferred for medical images due to its simplicity and effectiveness in preserving image quality. This approach ensures minimal alteration of critical image details, which is essential in medical imaging where diagnostic accuracy is of utmost importance. Thus, while frequency domain techniques offer greater robustness, spatial domain watermarking remains a practical option for medical applications where image fidelity preservation is of paramount importance. There is a clear need for effective techniques to enhance the robustness of spatially based medical image watermarking, while balancing security and computational efficiency. A promising solution involves leveraging key-points; however, careful selection of these key-points is essential to develop a flexible watermarking method. Given the sensitivity of medical images, ensuring a high level of security is of paramount importance. Therefore, adopting techniques that enhance security without significantly increasing computational time would be of great value in this context.

White-box and black-box algorithms in machine learning differ primarily in terms of transparency and interpretability. White-box models, such as linear regression and decision trees, are fully interpretable, allowing users to see and understand each step in the decision-making process. This transparency makes them ideal for applications where understanding and justifying decisions is critical, such as healthcare or finance. Conversely, black-box models, such as neural networks and ensemble methods, operate with complex, nonlinear computations that are difficult to interpret. While they often achieve higher accuracy on complex tasks, the lack of transparency can make these models difficult to trust or troubleshoot in sensitive applications. The choice between white-box and black-box models depends on the need for interpretability versus predictive power.

Deep learning models are considered black box algorithms because their decision-making processes are not transparent; we do not fully understand how the network arrives at specific decisions. In contrast, white box models provide a controlled decision-making process, with clearly defined and interpretable features. This makes white box approaches preferable in the medical domain, where control over specific features is essential for trust and accountability. While there are solutions, such as explainable artificial intelligence (XAI), that aim to provide insights into black box models, these approaches still do not provide the same level of transparency as white box models that are inherently interpretable. To address this challenge, we propose utilizing advanced feature extraction techniques to enhance the robustness of spatial-domain-based medical image watermarking frameworks, while ensuring high levels of security. Each features extraction technique comes with its own strengths and limitations. Through experimental analysis, both BRISK and GFTT have shown promising results. Our contribution further explores these feature extraction techniques, aiming to leverage their synergy to identify the most robust key-points. To enhance key-point selection, we apply the k-means algorithm for efficient detection of primary key-points, with an additional layer of security provided by chaotic systems. Details of this contribution will be thoroughly discussed in the following section.

4. Methodology

This section outlines the methodology for embedding a text message into an image using a series of well-defined algorithms. The process is supported by visual aids and tables that illustrate the workflow, parameters, and results of the proposed techniques.

4.1. Study of Feature extraction techniques

Based on a comparative study [20, 41] examining different feature extraction techniques, including BRISK, SIFT, ORB, and GFTT, highlighted promising results, especially for BRISK, which showed exceptional potential in general object detection [41, 44]. BRISK's ability to handle fine structures and complex details makes it particularly suitable for applications that require high accuracy, such as document processing, and especially medical imaging, where preservation of detailed features is of paramount importance. These results motivated us to choose BRISK and GFTT as the core feature extraction techniques in our approach, with the aim of leveraging their complementary strengths to capture robust and detailed features.

For example, **BRISK** is designed to detect and describe key points robustly, handling variations such as scale changes and rotations. This makes it particularly useful for identifying and tracking important features in medical images. In fact, it detects key-points$\{k_i\}$ that are invariant to transformations and computes descriptors $\{d_i\}$ associated with each key-point indexed by i where N is the total number of detected key-points. To formalize this, let $BRISK(I)$ denote the set of key-points and descriptors detected in image I, as shown in the following equation:

$$BRISK(I) = \{(k_i, d_i) | i \in \{1, 2, \ldots, N\}\} \tag{8}$$

In addition, **GFTT** focuses on detecting stable and distinctive points in images, typically corners or edges, that are ideal for tracking and matching. It identifies points in an image that are robust and distinctive, typically corners or edges. It evaluates the quality of these points using the eigenvalues of the image's structure tensor, which is derived from the gradients of the image [16]. Points with high eigenvalues are preferred as they represent strong features that are stable under transformations. GFTT has been explored in several renowned applications and is instrumental in preserving image details during restoration, thanks to its capability to identify and maintain key features [17, 18].

The structure tensor M at a point (x, y) is defined as:

$$M = \begin{bmatrix} I_x^2 & I_x I_y \\ I_x I_y & I_y^2 \end{bmatrix} \tag{9}$$

where I_x and I_y are the image gradients in the x and y directions, respectively.

The eigenvalues λ_1 and λ_2 of this tensor are computed as:

$$\lambda_{1,2} = \frac{1}{2}\left[(I_x^2 + I_y^2) \pm \sqrt{(I_x^2 - I_y^2)^2 + 4(I_x I_y)^2}\right] \tag{10}$$

4.2. K-means based Feature postprocessing

Following the extraction of features, the main idea is to obtain strength or core key-point the K-Means clustering could offer a powerful approach in optimizing and simplifying the analysis process. It groups similar features into distinct clusters, which helps in organizing the feature vectors effectively. This clustering approach reduces the dimensionality of the feature space, thereby decreasing the complexity of the solution. This process helps with more effective watermark embedding. In general, the K-Means algorithm minimizes the within-cluster sum of squares computed as follows:

$$J = \sum_{i=1}^{k} \sum_{x \in C_i} \|x - \mu_i\|^2 \tag{11}$$

where C_i represents the set of points in cluster i, and μ_i is the centroid of cluster i.

4.3. Chaotic System integration

Furthermore, chaotic systems, known for their complex and sensitive dynamics, have been integrated into watermarking to improve security and reliability [19]. Chaotic maps, such as the logistic map, generate pseudorandom sequences for watermark embedding:

$$x_{n+1} = r \cdot x_n(1 - x_n) \tag{12}$$

where r is a control parameter, x_n is the sequence value at iteration n and x_{n+1} is the next value. By combining chaotic systems with machine learning-based water- marking methods, the watermarking process gains additional complexity, making unauthorized decoding more challenging and maintaining watermark detectability amidst distortions [20, 21].

4.4. Proposed framework overview

The embedding process begins with converting the text message into a binary format, referred to as Binary (M). The image is then decomposed into its Red, Green, and Blue (RGB) color bands. The algorithm utilizes these bands to embed the binary message. Specifically, the Green and Blue bands are modified based on the binary data, To get a good and more complex embedding to keep hidden the message hidden, as consideration that method as more sophisticated and complex by using one band, and the modified bands are then recombined with the unchanged Red band to produce the final watermarked image as shown in Fig. 1.

To ensure precise embedding and effective message retrieval, key control points within the image are selected using the approach. This technique is used to select important control locations within the image, ensuring accurate embedding and efficient message retrieval. This approach entails the utilization of BRISK (Binary Robust Invariant Scalable Key-points) to identify key-points in the red band. These key points are then tracked to determine significant control points. Subsequently, the Good Feature to Track technique (GFTT) is employed to enhance the identification of these control points. To optimize their arrangement, then K-Means clustering is applied to these points pixel result to combining BRISK and GFTT. Initially, during the training phase to achieve optimal feature extraction technique, we employed the Orientated FAST and Rotated BRIEF (ORB) as well as the Scale Invariant Feature Transform (SIFT) tech-

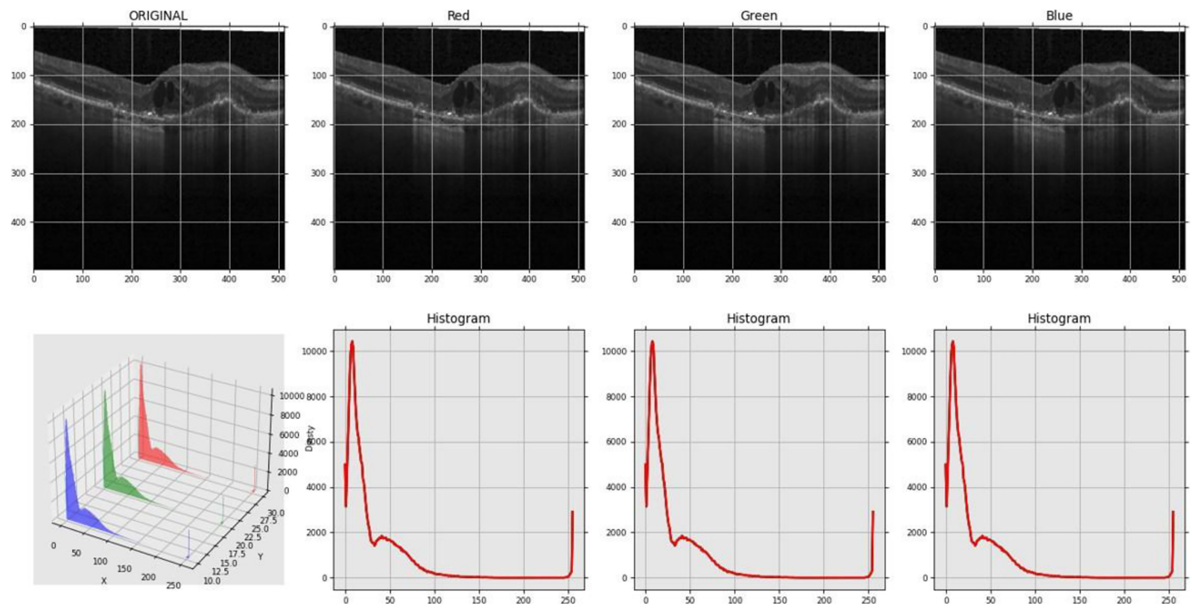

Fig. 1. Distribution of Histograms.

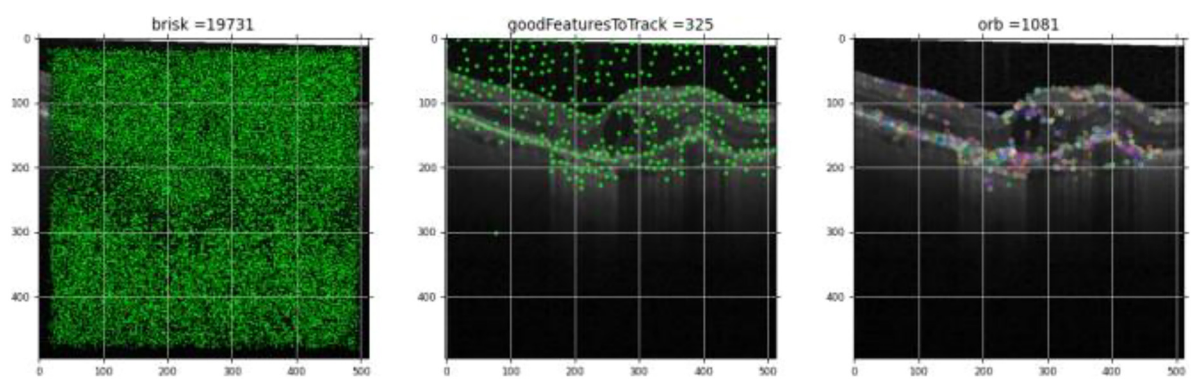

Fig. 2. Hybrid Feature Extraction Techniques.

niques. We then compared the results obtained from these techniques and identified the most favorable outcome. By merging the BRISK and GFTT algorithms as shown in Fig. 2. The clustering process is depicted in Fig. 4, which illustrates how centroids are iteratively updated to group key points effectively.

The Logistic map is employed to distribute hiding points within the image. The Logistic map outlines the process of generating hiding points using the Logistic map function. The map generates pseudo-random positions that are used to determine where the binary data will be embedded within the image. during converting the pixels from the image matrix to vector, a matrix was created from *width* = 5 and *height* = 5 called the G matrix, convert X and Y Coordinates from two dimensions (2D) to index in one dimensions (1D) in band green image, the size of matrix which is applied [5 × 5], [7 × 7], [9 × 9], noticed that there is no difference between the sizes of matrixes used for the last result of metrics. This produces pixel distribution using a very intelligent method. The generated hiding points are visualized in Fig. 5, showing the distribution of these points across the image matrix.

Fig. 3 provides a comprehensive overview of the entire watermarking process as described above. It visually represents each step, including message conversion, image band modification, and the recombination of bands to produce the watermarked image.

Table 1 summarizes the key parameters used in the Logistic map algorithm. The initial value X_0 and control parameter R are crucial for determining the hiding points' distribution within the image. The matrix size indicates the dimensions used for indexing in the Logistic map distribution process.

Fig. 4 visualizes the K-Means clustering process used to determine key control points in the image. It

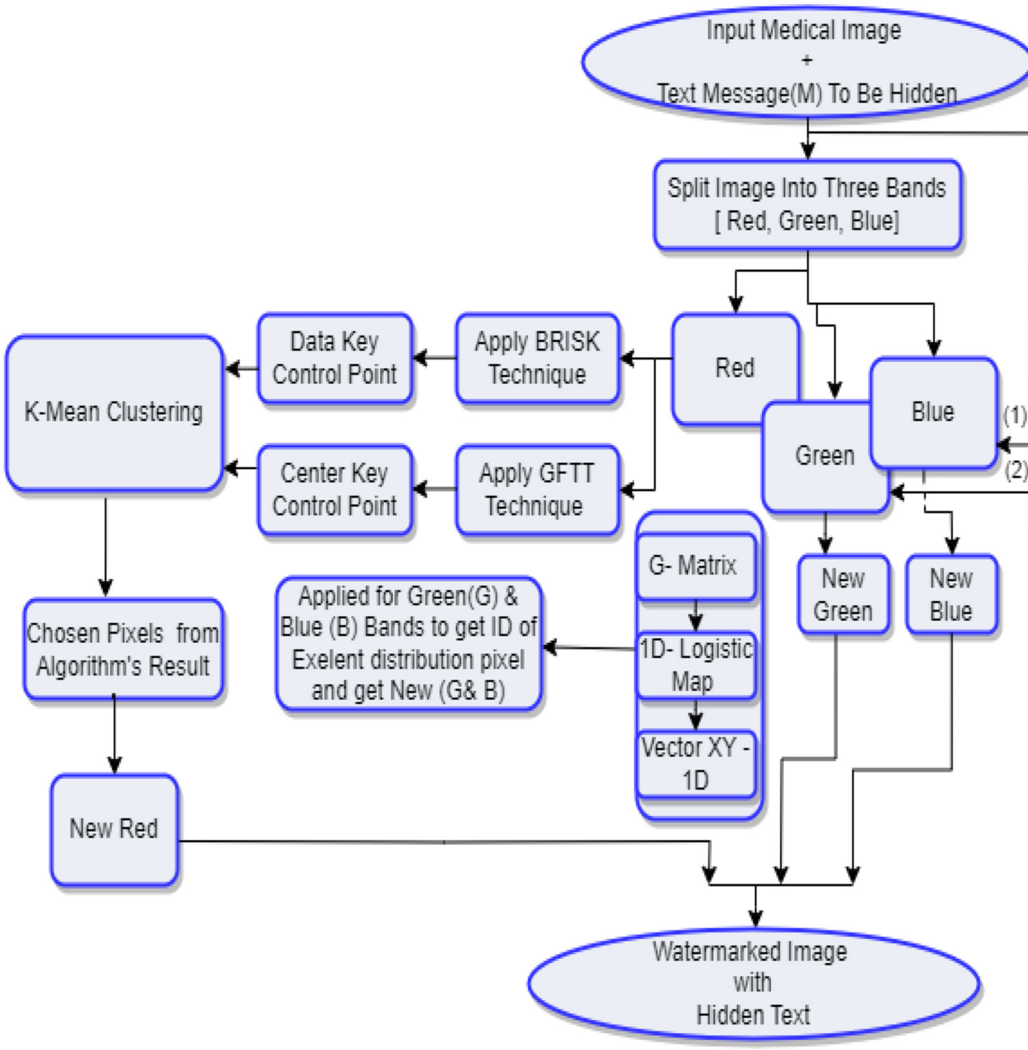

Fig. 3. Workflow diagram illustrating the message embedding process in an image. The diagram shows the sequence from converting the message into binary format to modifying the color bands and generating the final watermarked image.

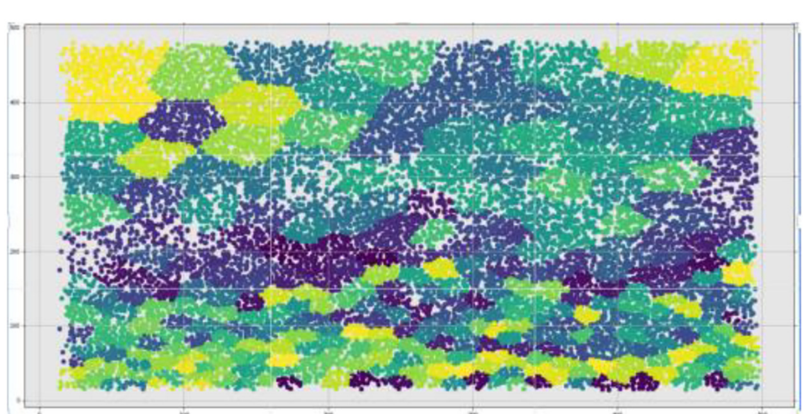

Fig. 4. Illustration of K-Means clustering applied to key control points in the Red band of the image. The figure shows how points are grouped around centroids and the iterative refinement of these clusters Logistic map generates pseudo-random hiding locations within the image based on the iterative function

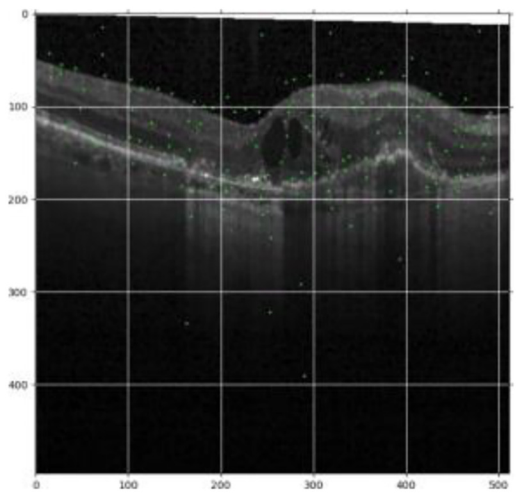

Fig. 5. Distribution of hiding points using the Logistic map. The figure demonstrates how the Logistic map generates pseudo-random hiding locations within the image based on the iterative function

Table 1. Parameters for Logistic Map Distribution.

Parameter	Value
Initial Value (X_0)	0.4
Control Parameter (R)	3.0
Matrix size	5×5

highlights the initial random assignment of centroids and the iterative updates that refine the clustering process based on the image's feature points. Fig. 5 illustrates the distribution of hiding points across the image matrix as determined by the Logistic map. It shows how the pseudo-random values generated by the map are used to select specific image locations for embedding message data.

5. Experimental results and analysis

5.1. Dataset Description

To evaluate the effectiveness of the proposed watermarking scheme, we utilized Ocular Disease Intelligent Recognition (ODIR) in particular, Retinal optical coherence tomography (Retinal- OCT) medical images sourced from IEEE data Port [34]. The dataset comprises three types of image files: Test, Training and Val images. Each file contains four types of image class CNV, DMI, DRUSEN, NORMAL. The Val file image, used for our experiments, are in JPG format with dimensions of 512×496, 768×496 pixels, adhering to the Joint Photographic Experts Group (JPEG) standard. Each image is represented in RGB color space, which includes the red, green, and blue channels. The experiments were conducted using Google Colab for online execution. Retinal optical coherence tomography (Retinal - OCT) of the retina is a high-resolution imaging technique that captures detailed cross-sectional views of patients' retinas. Each year, around 30 million OCT scans are conducted, with the analysis and interpretation of these images requiring substantial time and effort. To assess the proposed technique, each image was processed ten times with varying lengths of the embedded secret message. This testing allowed us to evaluate the imperceptibility and robustness of the watermarking scheme under different conditions. Additionally, we compared the performance of our method against several recent alternatives to gauge its effectiveness.

5.2. Results and Analysis

Table 2 provides a comparative analysis of the proposed method with several recent alternatives. The proposed method consistently outperforms others in terms of PSNR, SSIM, and other key metrics, demonstrating its superior performance in preserving image quality and robustness. Overall, these results validate the effectiveness of the proposed watermarking technique in secure medical image watermarking, showcasing its potential for practical applications in medical imaging and data security. This comparison highlights the relative strengths and limitations of each approach with compare frequency/spatial based domain watermarking and illustrates the advancements achieved by our proposed method [35–37]. This table clearly shows that while earlier methods have made significant contributions, our approach provides superior results in terms of PSNR, SSIM, and minimal MSE, establishing a new benchmark in medical image watermarking [38].

The integration of machine learning and chaotic systems into our method not only improves robustness but also ensures the preservation of image quality, addressing the limitations of existing techniques, this is an obvious reason that our result is best of the other techniques.

Figs. 6 to 8 illustrate the performance of the proposed method using various metrics, where Fig. 6 show the PSNR and SSIM metrics for the proposed watermarking method across various lengths of the embedded message. While the Fig. 7 represent MSE and NC (x10) metrics for the proposed watermarking method, showing performance in preserving image quality and correlation.

The experimental results demonstrate that the proposed watermarking technique excels in maintaining image quality and robustness. Fig. 6 shows that the PSNR and SSIM values for the proposed method are consistently high, indicating that the watermarked images retain excellent visual quality and perceptual

Table 2. Comparative analysis of medical image watermarking techniques and metrics for watermarking methods.

			Evaluation Metrics					
Ref.	Domain	Watermark type	PSNR	SSIM	MSE	NC	UACI	Method/Technique
Swaraja et al. [7]	Frequency	Blind	36.99	-	-	1	398,654	Human Visual System (HVS) with the integration of Discrete Wavelet Transform (DWT) and Schur transform along with the Particle Swarm Bacterial For Aging Optimization algorithm (PSBFO).
Su et al. [28]	Spatial	Fragile	45.05	0.9759	-	0.9944	-	Self-embedding fragile watermarking
Jabbar et al. [29]	Frequency	Robust	72.62	-	-	1	-	SLT (Sine Logistic Transform), DCT (Discrete Cosine Transform), and DWT (Discrete Wavelet Transform)
Amiri et al. [30]	Frequency	-	41.11	-	13.92	-	-	Wavelet-based Fusion with Equilibrium Optimization
Taj et al. [31]	Frequency	Reversible-Zero Watermark	38.71	-	-	1	BER = 0	Reversible-zero watermarking with DWT (IWT), and different expansion techniques
Proposed method	Spatial	Blind	85.26	0.9999	0.0001	1	0.0	Blind watermarking, BRISK, GFTT Feature Extraction techniques

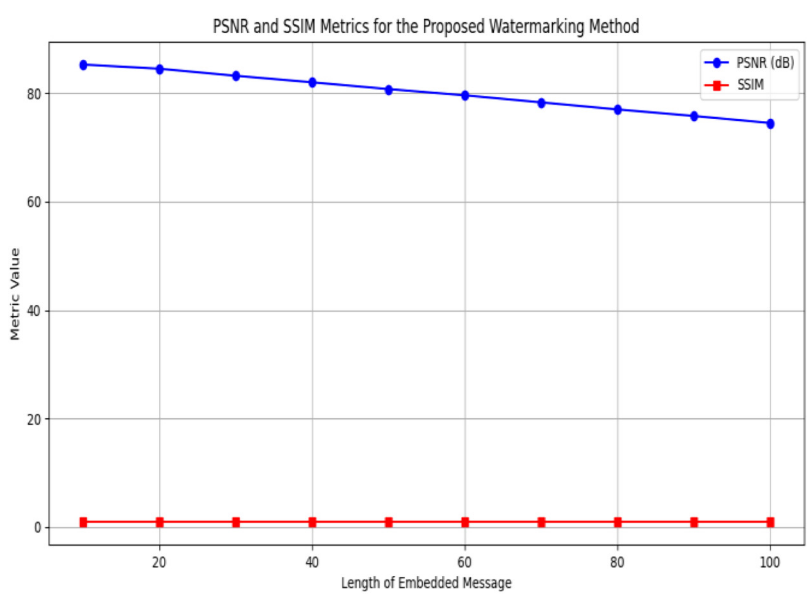

Fig. 6. PSNR and SSIM metrics for the proposed watermarking method across various lengths of the embedded message.

similarity compared to the originals. Fig. 7 highlights that the Mean Squared Error (MSE) is very low, and the Normalized Correlation (NC) is very high, signifying that the proposed method effectively preserves the integrity of the original images while embedding the watermark. Fig. 8 demonstrates that the Unified Average Changing Intensity (UACI) values for the proposed method are very low, indicating that the watermarking technique is robust against various forms of image under various conditions.

6. Conclusion and future work

In this study, we proposed an advanced watermarking technique for medical images that utilizes a combination of blind watermarking, feature extraction techniques in particular BRISK and GFTT, least significant bit (LSB) techniques, and chaotic systems (specifically, the Logistic map distribution) to embed and retrieve secret information securely. Our method was rigorously evaluated using a dataset

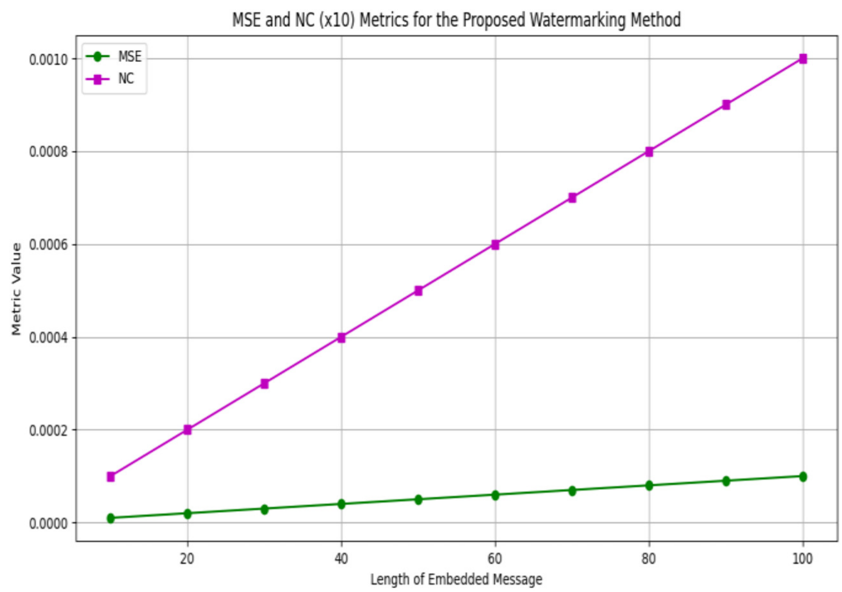

Fig. 7. MSE and NC (x10) metrics for the proposed watermarking method, showing performance in preserving image quality and correlation.

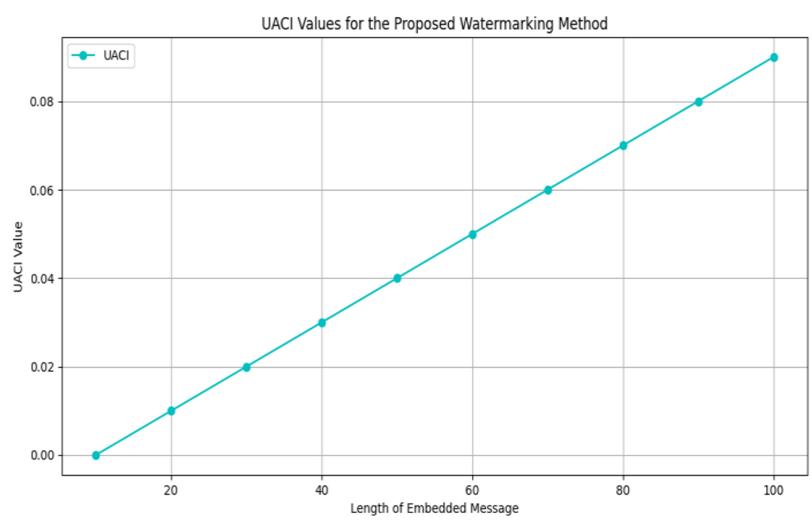

Fig. 8. UACI values for the proposed watermarking method, indicating robustness.

of RGB retinal medical images, consisting of images from both healthy and retinopathic patients. The experimental results demonstrate that the proposed watermarking technique excels in terms of imperceptibility, robustness, and security. MSE and PSNR values illustrate a trade-off between watermark length and image quality, with minimal distortion for longer watermarks. High UQI and SSIM values affirm the preservation of image quality and structural integrity post-watermarking, while SCC values close to 1 underscore the retention of spatial correlations. The proposed method achieved impressive performance metrics, including high Peak Signal-to-Noise Ratio (PSNR) values, excellent Structural Similarity Index (SSIM) scores, and minimal Mean Squared Error (MSE) values. The robustness of the method was further confirmed by its low Unified Average Changing Intensity (UACI) and high Normalized Correlation (NC) values, indicating its effectiveness in preserving image quality while embedding the watermark. Comparative analysis with recent methods highlighted the superiority of our approach, particularly in its ability to maintain high quality and robustness under various conditions.

Despite the promising results, there are several areas for improvement and further investigation. Future work could focus on enhancing the scalability of the watermarking technique to accommodate larger

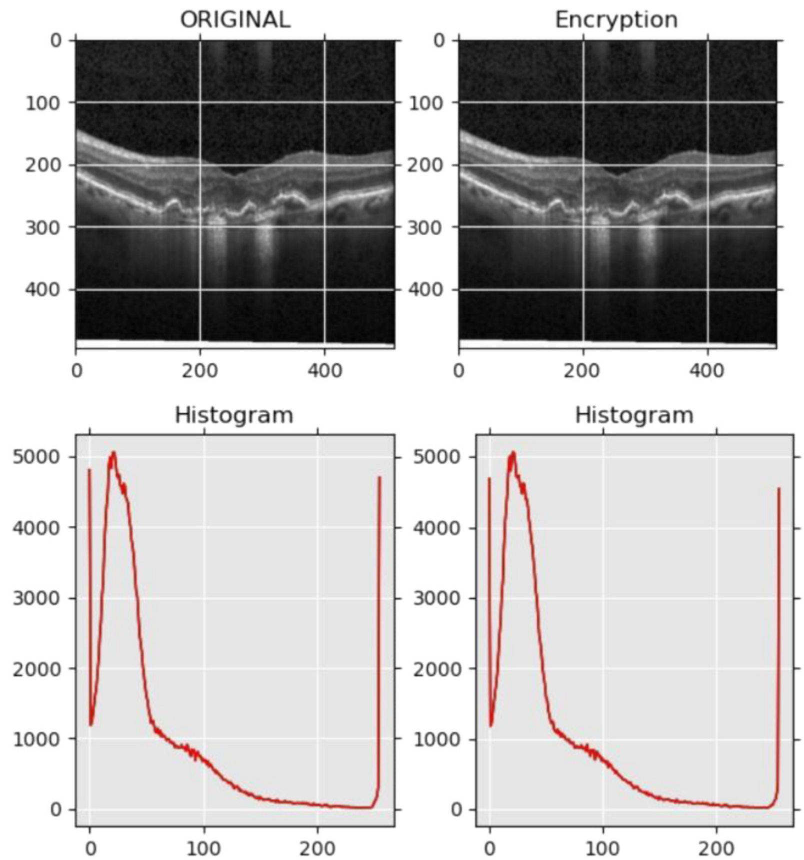

Fig. 9. Original and Encryption.

datasets and higher resolution images. Exploring additional chaotic systems and advanced cryptographic techniques could further bolster the security of the watermarking process, making it even more resilient against sophisticated attacks.

Another potential area of research is the integration of machine learning algorithms to adaptively optimize watermark embedding parameters based on image content and characteristics. This could lead to more intelligent and context-aware watermarking solutions. Additionally, expanding the methodology to handle multimodal medical images, such as combining images with other imaging modalities (e.g., Ultrasound, X Ray, CT or MRI), could provide a more comprehensive approach to medical image security.

Funding

None.

Acknowledgement

None.

Conflicts of interest

None.

References

1. G. Bhatnagar, Q. M. J. Wu, and Z. Liu. “A robust dct based watermarking technique for color images.” *Multimedia Tools and Applications*, vol. 55 no. 2, pp. 315–332, 2012.
2. A. Krizhevsky, I. Sutskever, and G. E. Hinton. “Imagenet classification with deep con- volutional neural networks.” *Advances in Neural Information Processing Systems*, vol. 25, pp. 1097–1105, 2012.
3. J. Zhang, X. Liu, L. Wei, and G. Hua. “Hidden: Hiding data with deep networks.” Proceedings of the European Conference on Computer Vision (ECCV), pp. 682–697, 2018.
4. Z. Zhang, Y. Wu, Z. Yang, and C. Chen. “Robust invisible watermarking of 3d point clouds with geodesic-aware embedding.” Proceedings of the IEEE/CVF International Conference on Computer Vision, pp. 8623–8632, 2019.
5. A. R. Hassan, S. Shirmohammadi, and L. Zhang. “A medical image watermarking technique based on dwt and lsb.” Proceedings of the 2016 ACM on International Conference on Multimedia Retrieval, pp. 439–442, 2016.
6. A. Al-Haj, F. Mohammad, and I. Barhumi. “Hybrid watermarking of medical images for secure transfer.” Proceedings of the 2009 International Conference on Signal Acquisition and Processing, pp. 217–220, 2009.

7. K. Swaraja, K. Meenakshi, and P. Kora. “An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine.” *Biomedical Signal Processing and Control*, vol. 55, p. 101665, 2020.
8. P. Khare and V. K. Srivastava. “A secured and robust medical image watermarking approach for protecting integrity of medical images.” *Transactions in Emerging Telecommunications Technologies*, vol. 32 no. 2, p. 3918, 2021.
9. M. Nazari and M. Mehrabian. “A novel chaotic iwt-lsb blind watermarking approach with flexible capacity for secure transmission of authenticated medical images.” *Multimedia Tools and Applications*, vol. 80 no. 7, pp. 10615–10655, 2021.
10. A. Singh and M. K. Dutta. “Imperceptible watermarking for security of fundus images in tele-ophthalmology applications and computer-aided diagnosis of retina dis- eases.” *International Journal of Medical Informatics*, vol. 108, no. October, pp. 110–124, 2017. doi: 10.1016/j.ijmedinf.2017.10.010.
11. K. Shankar, M. Elhoseny, E. D. Chelvi, S. K. Lakshmanaprabu, and W. Wu. “An efficient optimal key based chaos function for medical image security.” *IEEE Access*, vol. 6, pp. 77145–77154, 2018. doi: 10.1109/ACCESS.2018.2874026.
12. A. G. Klington and K. Ramesh. “Cost-effective watermarking scheme for authentication of digital fundus images in healthcare data management,” 2021. doi: 10.5755/j01.itc.50.4.28957.
13. M. Sayah, M. Redouane, and A. Khaldi. “A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications.” *Microprocessors and Microsystems*, vol. 90, no. September, p. 104490, 2022. doi: 10.1016/j.micpro.2022.104490.
14. J. Shi, *et al.*. “Good features to track.” In: 1994 Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, pp. 593–600, 1994, IEEE.
15. K. Gourrame, *et al.* . “A zero-bit fourier image watermarking for print-cam process.” *Multimedia Tools and Applications*, vol. 78, pp. 2621–2638, 2019. doi: 10.1007/s11042-018-6781-7.
16. Y. Lin, Y. Jiang, X. Jiao, and B. Han. “Learned good features to track.” *IEEE Transactions on Circuits and Systems for Video Technology*, 2024.
17. F. Drira, F. Lebourgeois, and H. Emptoz. “A new pde-based approach for singularity- preserving regularization: application to degraded characters restoration.” *Int. J. Document Anal. Recognit.*, vol. 15, no. 3, pp. 183–212, 2012. doi: 10.1007/S10032-011-0165-5.
18. F. Drira, F. Lebourgeois, and H. Emptoz. “Document images restoration by a new tensor based diffusion process: Application to the recognition of old printed documents.” In: 10th International Conference on Document Analysis and Recognition, ICDAR 2009, Barcelona, Spain, 26–29 July 2009, pp. 321–325, 2009. doi: 10.1109/ICDAR.2009.109.
19. A. Roček, M. Javorník, K. Slavíček, and O. Dostál. “Zero watermarking: Critical analysis of its role in current medical imaging.” *Journal of Digital Imaging*, vol. 34, pp. 204–211, 2021. doi: 10.1007/s10278-020-00403-5.
20. S. D. Mahmood, F. Drira, H. F. Mahdi, Y. Aribi, and A. M. Alimi. “Chaotic model-based blind watermarking with lsb technique for digital fundus image authentication.” In: 2023 International Conference on Cyberworlds (CW), pp. 395–402, 2023. doi: 10.1109/CW58918.2023.00068.
21. Y. Wang, *et al.* . “A hybrid deep learning approach to predict malignancy of breast lesions using mammograms.” In: Proceedings of the SPIE 10579, Medical Imaging 2018: Imaging Informatics for Healthcare, Research, and Applications, Huston, TX, USA, p. 105790, 2018. doi: 10.1117/12.2292922.
22. S. A. Nawaz, J. Li, U. A. Bhatti, A. Mehmood, M. U. Shoukat, and M. A. Bhatti. “Advance hybrid medical watermarking algorithm using speeded up robust fea tures and discrete cosine transform.” *PLoS ONE*, vol. 15, no. 10, p. 0232902, 2020. doi: 10.1371/journal.pone.0232902.
23. K. M. Hosny and M. M. Darwish. “Robust color image watermarking using invariant quaternion legendre-fourier moments.” *Multimedia Tools and Applications*, vol. 77, pp. 24727–24750, 2018. doi: 10.1007/s11042-017-5116-3.
24. K. M. Hosny and M. M. Darwish. “Resilient color image watermarking using accurate quaternion radial substituted chebyshev moments.” *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 15, pp. 1–25, 2019. doi: 10.1145/3317693.
25. S. A. Mostafa, A. Mustapha, A. A. Hazeem, S. H. Khaleefah, and M. A. Mohammed. “An agent-based inference engine for efficient and reliable automated car failure diagnosis assistance.” *IEEE Access*, vol. 6, pp. 8322–8331, 2018. doi: 10.1109/ACCESS.2018.2819030.
26. A. K. Sahu, S. Sharma, and D. Puthal. “Lightweight multi-party authentication and key agreement protocol in iot-based e-healthcare service.” *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 17, no. 2s, pp. 1–20, 2021. doi: 10.1145/3398039.
27. N. Zermi, A. Khaldi, R. Ka, F. Kahlessenane, and S. Euschi. “A dwt-svd based robust digital watermarking for medical image security.” *Forensic Science International*, vol. 320, 2021. doi: 10.1016/j.forsciint.2021.110691.
28. G. D. Su, C. C. Chang, and C. C. Lin. “Effective self-recovery and tampering localization fragile watermarking for medical images.” *IEEE Access*, vol. 8, pp. 160840–160857, 2020.
29. A. K. Jabbar, A. T. Hashim, and Q. F. Hassan. “Medical image authentication by combining hash signature and watermarking based on frequency domains.” *Journal of Physics: Conference Series*, vol. 1963, no. 1, p. 012039, 2021.
30. S. Amiri, A. Mosallanejad, and A. Sheikhahmadi. “Medical images fusion based on equilibrium optimization and discrete wavelet.” *International Journal of Nonlinear Analysis and Applications*, vol. 12, no. Special Issue, pp. 1337–1354, 2021.
31. R. Taj, F. Tao, S. Kanwal, A. Almogren, A. Altameem, and A. U. Rehman. “A reversible-zero watermarking scheme for medical images.” *Scientific Reports*, vol. 14, no. 1, p. 17320, 2024.
32. R. E. Arevalo-Ancona and M. Cedillo-Hernandez, “Improving the security of medical imaging via DFT-based reversible watermarking and deep learning-based zero-watermarking.” In *2024 47th International Conference on Telecommunications and Signal Processing (TSP)*, pp. 10–15, IEEE.
33. Priyanka, S. Maheshkar. “Region-based hybrid medical image watermarking for secure telemedicine applications.” *Multimedia Tools and Applications*, vol. 76, pp. 3617–3647, 2016. doi: 10.1007/s11042-016-3457-0.
34. F. V. Leuciuc, M. D. Craciun, I. S. Holubiac, M. A. Mohammed, K. H. Abdulkareem, and G. Pricop. “Statistical medical pattern recognition for body composition data using bioelectrical impedance analyzer. CMC: Computers,” *Materials & Continua*, vol. 67, pp. 2601–2617, 2021.
35. Y. jianing: ODIR. doi: 10.21227/a01s-a634.
36. C. Kwan, J. Larkin, and B. Chou. “Perceptually lossless compression of mastcam images with error recovery.” *Signal Processing, Sensor Fusion, and Security*, vol. 1101815, 2019.
37. M. Cedillo-Hernandez, A. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano- Miyatake, and H. Perez-Meana. “Digital color images ownership authentication via efficient and robust watermarking in a hybrid domain.” *Radioengineering*, pp. 536–551, 2017.

38. C. Kwan. “Strange behaviors and root cause in the compression of previously compressed videos.” *Signal and Image Processing*, vol. 1, 2015.
39. Q. Mastoi, *et al.*, *Machine learning-data mining integrated approach for premature ventricular contraction prediction*. Neural Computing and Applications, 2021.
40. A. Zenati, W. Ouarda, and A. M. Alimi, “A new digital steganography system based on hiding online signature within document image data in YUV color space.” *Multimed Tools Appl*, vol. 80, pp. 18653–18676, 2021. doi: 10.1007/s11042-020-10376-9.
41. A. Zenati, W. Ouarda, and A. M. Alimi, “SSDIS-BEM: A new signature steganography document image system based on beta elliptic modeling.” *Engineering Science and Technology, an International Journal*, vol. 23, no. 3, pp. 470–482, 2020.
42. F. H. Al-Rubbiay, A. Y. Youssef, and S. D. Mahmood, “Medical image authentication and restoration based on mCloud computing: Towards reliant medical digitization era.” In *Doctoral Symposium on Computational Intelligence*, Singapore: Springer Nature Singapore, pp. 487–500, 2023.
43. S. D. M. Mahmood, Automatic detection of epidural hematoma on the brain by using image processing techniques (Master’s thesis, Fen Bilimleri Enstitüsü).
44. M. G. Forero, *et al.* “Comparative analysis of detectors and feature descriptors for multispectral image matching in rice crops.” *Plants*, vol. 10, no. 9, p. 1791, 2021.