ISSN 2723-6471

Robust Digital Image Watermarking Scheme in the DCT Domain Employing Möbius Transformation

Atheer Alrammahi[1], Hedieh Sajedi[2,*], Mustafa Radif[3]

[1,2]*Department of Mathematics, Statistics and Computer Science, University of Tehran, Tehran, Iran*

[1,3]*Department of Medical Intelligent Systems, University of Al-Qadisiyah, Iraq*

(Received: February 5, 2025; Revised: April 3, 2025; Accepted: May 6, 2025; Available online: June 2, 2025)

Abstract

This study introduces a novel digital image watermarking method that integrates Möbius transformations with the Discrete Cosine Transform (DCT) to enhance both resilience and imperceptibility. The primary objective is to address the challenges of watermark embedding in digital images, ensuring robustness against geometric distortions, noise, and compression while maintaining high visual quality. The method employs a genetic algorithm to optimize the Möbius transformation parameters for effective watermark embedding in the DCT domain. Experimental results demonstrate the robustness of the proposed technique, with peak signal-to-noise ratio (PSNR) values consistently above 40 dB, ensuring minimal perceptual distortion. The bit error rate (BER) is significantly lower than that of traditional methods, demonstrating the technique's resilience against a wide range of attacks, including rotation, scaling, Gaussian noise, JPEG compression, and cropping. Compared to existing watermarking schemes, this approach consistently outperforms them in visual quality and resistance to tampering, with the PSNR reaching 60.94 dB for Lena images and achieving an SSIM value close to 1, indicating superior imperceptibility. The novelty of this approach lies in its combination of Möbius transformations with the DCT domain, offering a robust, efficient, and scalable solution for digital rights management and secure media transmission. This technique's efficiency in terms of computational complexity and potential scalability for broader applications like video and audio watermarking highlights its practical advantages.

Keywords: Digital Watermarking, Möbius Transformation, Discrete Cosine Transform, Genetic Algorithm, Copyright Protection

1. Introduction

The rapid digitalization of our lives, driven by the internet, has changed how we access, share, and consume information. This ease of distribution poses challenges for protecting digital media. Invisible digital watermarking, which is both imperceptible and robust, is a promising technique for safeguarding digital media [1], [2]. In today's digital age, watermarking is essential for ensuring the ownership and authenticity of digital media. This technology embeds imperceptible data, or a watermark, into media to verify the origin, deter unauthorized copying, and track misuse [3]. Watermarking methods are typically segmented into two categories on the basis of the domain where the watermark is embedded: spatial domain watermarking techniques [4], [5] and frequency domain watermarking methods [6], [7].

Spatial domain methods embed watermark data by directly modifying image pixels. For example, a color image watermarking method in the spatial domain was introduced by [8], which ensures both invisible watermarking and robustness to attacks. Conversely, frequency domain techniques employ mathematical transformations such as the redundant discrete wavelet transform (RDWT) [9], discrete wavelet transform (DWT) [10], [11] DCT [10], [12], and discrete Fourier transform (DFT) [13] to convert the host image into the frequency domain, where watermark information is embedded in the frequency coefficients. These approaches typically offer superior imperceptibility and robustness in comparison with spatial domain techniques.

Many frequency domain watermarking methods have emerged. For example, [11] introduced a nonblind method that combines singular value decomposition (SVD) with DWT, embedding watermark data into the LL subband to increase

***Corresponding author: Hedieh Sajedi (hhsajedi@ut.ac.ir)**
DOI: https://doi.org/10.47738/jads.v6i3.705

imperceptibility and robustness. However, it requires the original image for extraction and is vulnerable to rotation attacks.

Digital watermarking schemes aim for both imperceptibility and robustness. Ernawan and Kabir's scheme [7], which uses DCT and an optimal psychovisual threshold, excels in these areas by selecting image blocks with the lowest modified entropy. However, it only supports grayscale images and basic binary watermarks. New algorithms have since been developed for blind and color image watermarking [10], [12], [13]. Yuan et al.'s blind watermarking scheme uses DCT for RGB images but lacks robustness against cropping, translation, and rotation. In contrast, Bao and Wang's algorithm employs Radon and DCT transforms for YUV images, improving security and imperceptibility through encryption and permutation [14], [15]. This method is resilient against geometric distortions, providing a foundation for robust watermarking techniques.

Recent advancements in digital watermarking have led to techniques that greatly enhance imperceptibility and robustness. Gomez-Coronel et al. [16] introduced a hybrid algorithm using the Hermite transform, DCT, and SVD to embed two watermarks simultaneously and enhance security with encryption. Ping-ping Zeng et al. [17]developed a color watermarking method that combines a quantum discrete cosine transform (QDCT) and a sinusoidal-tent map for improved invisibility and robustness through chaos control [17]. Xuping and Akinori [18] proposed an imperceptible and recoverable audio watermarking method using customized integer discrete cosine transform (intDCT) coefficient expansion, offering blind tampering detection, high capacity, and excellent audio quality. Alomoush et al. [19] focused on digital image watermarking, employing linear modulation depending on DCT to embed stego-text into the least significant bit (LSB) of DCT coefficients, enhancing resilience against various image processing attacks. These advancements demonstrate the ongoing efforts to balance robustness, imperceptibility, and computational complexity in digital watermarking techniques.

Weishuai et al. [20] presented a robust image watermarking method using DWT, chaotic maps, and SVD, balancing invisibility and robustness with encryption and frequency domain embedding. Their simulations revealed high resistance to attacks, making the method effective for image protection. Dhani and Ferda [21] introduced an adaptive scaling factor for watermarking with chosen DCT coefficients, balancing resilience and invisibility and outperforming existing methods in robustness. Anna and Oleg [22] developed a robust and blind image watermarking algorithm using a gradient-based optimizer to adjust mid-frequency DCT coefficients, enhancing imperceptibility and resistance to common image processing attacks. Simeng Liu et al. [23] proposed a color image watermarking scheme using visual cryptography and DCT, achieving high security and robustness by embedding in medium-frequency DCT coefficients. These advancements have led to ongoing efforts to create robust and secure digital watermarking techniques for copyright and multimedia protection.

Manasi and Biswapati [24] introduced a watermarking scheme using DCT and cellular automata (CA), which achieved good imperceptibility and a high payload. Anis Kricha et al. [25] presented a resilient and transparent DCT domain watermarking scheme with exceptional imperceptibility and robustness against various attacks. Balkar and Mahesh [26] developed a technique for protecting color document images via discrete curvelet transform (DCuT) and DCT, ensuring high visual quality and robustness. Shaobao et al. [27] addressed the challenge of geometric attacks by introducing image normalization and the contourlet transform, which demonstrated high visual quality and robustness. Awasthi and Srivastava [28] presented a dual image watermarking algorithm for DICOM images that integrates multiple transforms to achieve high robustness and imperceptibility. Amel et al. [29] proposed an innovative algorithm for securing medical data transmission by integrating DWT, DCT, and SVD, showing exceptional stability and imperceptibility.

The increase in techniques for embedding information in media underscores the growing need for secure data exchange and copyright protection, such as methods involving SVD transformation [14], [15], [16], DCT domain watermarking [17], [18], [19], [20], [21] and hybrid approaches [22], [23], [24], which have evolved to balance robustness, imperceptibility, and computational complexity.

Securing confidential information in digital data transmission has become increasingly important. Stream and block ciphers, especially S-boxes, are crucial for ensuring data confidentiality through nonlinearity and confusion. Muhammad Sarfraz et al. [25] presented a method to construct numerous transformed S-boxes, enhance encryption

capabilities through Mobius transformation, and evaluate their performance against established S-box standards. Muhammad Asif et al. [26] presented new, robust S-boxes crucial for contemporary block ciphers, employing Mobius transformation and Galois field elements. Rigorous cryptographic analysis shows that the suggested S-boxes have improved algebraic quality and confusion capabilities. When applied to image encryption, the scheme performs better than entropy, correlation, energy, and homogeneity, ensuring the secure transmission of image data.

Tadayon [27] proposed a method for securing source data in linear network coding via Mobius transformation and interleaving, providing a lightweight alternative to cryptographic systems for secure transmission. Additionally, [28] explored the use of chaotic behavior and improved Tent-Sine maps to create robust substitution boxes (S-boxes) for secure communication. This approach, leveraging Mobius transformation, produces S-boxes that outperform advanced ones such as AES and skipjack, enhancing encryption and multimedia security.

Lin and Chen [29] developed an image cryptography method using Mobius transforms and a modulation-demodulation approach in Chen–Mobius systems, incorporating inverse functions for modulation and standard waveforms for demodulation. They also proposed a Mobius transformation model to handle minutia variations in fingerprint scans, addressing nonlinear distortions and rotations. Sharon Zhou et al. [30] introduced a data augmentation technique using Möbius transformations, which enhances deep model training by preserving labels and improving generalizability, especially with limited data.

Although digital watermarking provides a strong mechanism for content protection, several challenges must be addressed to ensure its practicality. Computational complexity is a critical concern, as embedding and extracting watermarks efficiently is essential for real-time applications. Memory usage also plays a significant role, particularly when working with high-resolution images and large datasets. Additionally, ensuring real-time applicability without compromising robustness and imperceptibility remains a challenge. These factors must be carefully balanced to develop an effective and scalable watermarking solution [31].

This work presents a novel digital image watermarking method using the Möbius transform in the DCT domain. It embeds and extracts watermarks in DCT coefficients, optimizing parameters with a genetic algorithm to enhance resilience and imperceptibility. The study addresses the following practical challenges:

This method significantly enhances resilience against various attacks, including rotation, scaling, noise, and compression, ensuring the watermark's integrity remains intact even under these challenging manipulations. The approach also excels in maintaining imperceptibility, with PSNR values consistently exceeding 40 dB, which guarantees minimal visual distortion and ensures the watermark is invisible to the human eye. To achieve an optimal balance between invisibility and resilience, genetic algorithms are employed to fine-tune the parameters of the Möbius transformation, enabling precise adjustments to the watermark embedding process. Furthermore, the method preserves the spatial and frequency characteristics of the image, ensuring that the watermark embedding does not distort the geometric integrity of the original content. Although this approach is currently focused on images, its potential for scalability is evident, as it can be extended to audio and video applications, making it a versatile solution for digital rights management and secure media transmission across various content types. The paper is organized as follows: Section 2 covers the theoretical background, Section 3 evaluates performance, Section 4 discusses simulations, and Section 5 summarizes the findings.

2. Literature Review

2.1. Möbius Transformations

The Möbius transformation can be understood from both complex analysis and geometric perspectives. Geometrically, the process begins with performing a stereographic mapping from the plane onto the unit two-sphere. Once the point is mapped to the sphere, the sphere undergoes a series of transformations, including rotation and translation to a new position. The sphere is then oriented in space, and a stereographic projection is performed from this new position back onto the plane. Through this process, Möbius transformations preserve angles and have the unique property of mapping circles to either circles or lines, and straight lines to either lines or circles. This transformation is mathematically expressed as a fractional linear transformation, as described in Eq. (1) and figure 1, which forms the foundation of Möbius transformations [32]:

 ISSN 2723-6471

$$W = f(z) = \frac{az+b}{cz+d} \quad (1)$$

a, b, c, and d are imaginary numbers [33], [32], [32] and ad-bc≠0.

A Möbius transformation is a combination of four elementary mappings: dilations, rotations, inversions and translations, as shown in figure 1. Translations: $z \rightarrow z + z0$ such that $z0 \in C$, Dilations: $z \rightarrow \lambda z$; $\lambda > 0$ and $\lambda \in R$, Rotations: $z \rightarrow e^{i\theta} z$; $\theta \in R$, Inversions: $z \rightarrow 1/z$. A point $z0 \in C\infty$ is called a fixed point of the complex function f(z) if f (z0) = z0. A Möbius transformation can have at most two points that remain unchanged under the transformation unless it is an identity map. The inverse of f(z), i.e., f-1(z), is once more a Mobius transformation and is given as Eq. (2):

$$f^{-1}(z) = \frac{dz-b}{-cz+a} \quad (2)$$

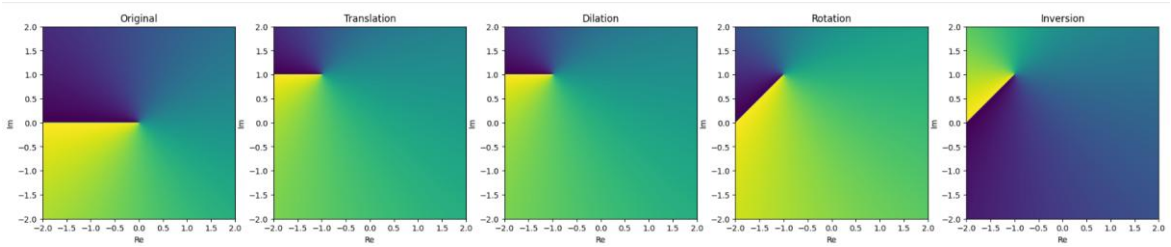


Figure 1. Grid of points in the complex plane and applies each of the four elementary Möbius transformations (translation, dilation, rotation, and inversion) sequentially

2.2. Discrete Cosine Transforms

The DCT transforms an image into the frequency domain, offering high performance and efficient energy concentration. By segmenting the image into 8×8 blocks, DCT is applied to produce high-, middle-, and low-frequency subbands. Low-frequency coefficients contain the most significant image information but modifying them can cause noticeable distortion. High-frequency coefficients, on the other hand, are more susceptible to noise and compression artifacts, which can lead to the loss of the watermark. Middle-frequency coefficients provide a balance between these two extremes, making them ideal for embedding watermarks while maintaining both robustness and imperceptibility. This trade-off ensures that the watermark remains resistant to attacks without introducing visible distortions [6], [7].

Two-dimensional DCT (2D-DCT) can be computed by applying 1D-DCT separately through the columns and rows of an N × N image f(x,y). The 2D-DCT of the image f(x,y) is defined by Eq. (3) and figure 2:

$$F(u,v) = \alpha(u) \times \alpha(v) \left[\sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y). \cos\left[\frac{(2x+1)u\pi}{2M}\right]. \cos\left[\frac{(2y+1)v\pi}{2N}\right]\right] \quad (3)$$

$$\alpha(u) = \begin{cases} \sqrt{1/N}, u = 0 \\ \sqrt{2/N}, u = 1, 2, \ldots., N-1 \end{cases} \quad (4)$$

x and y represent coordinates in the spatial domain, whereas u and v represent coordinates in the frequency domain. F(u,v) denotes the frequency coefficient at coordinates (u,v), and α(v) is analogous to α(u). The 2D-IDCT is characterized as Eq. (5):

$$f(x,y) = \alpha(u) \times \alpha(v) \left[\sum_{u=0}^{N-1} \sum_{v=0}^{N-1} F(u,v) . \cos\left[\frac{(2x+1)u\pi}{2N}\right]. \cos\left[\frac{(2y+1)v\pi}{2N}\right]\right] \quad (5)$$

 ISSN 2723-6471

(a) (b)

Figure 2. The carrier image is divided into 8×8 subblocks with DCT applied to each block. (a) Original image and (b) DCT-transformed image with highlighted blocks.

3. The Proposed Method

3.1. Watermark Embedding Process

The watermark embedding process in our study involves image preprocessing, DCT transformation, Möbius transform application, and DCT coefficient modification. The detailed procedure is shown in figure 4. While the steps are detailed, the role of the Möbius transformation in modifying DCT coefficients needs to be explicitly illustrated. To improve clarity, we have included a diagram that visually represents the transformation's effect on frequency components, showing how the Möbius transformation alters the spatial distribution of watermark pixels within the DCT domain. This diagram helps in understanding how the geometric properties of the Möbius transformation contribute to robust and imperceptible watermarking

Step 1: Convert the image to the YCbCr color space. The original RGB image is converted to the YCbCr color space to extract the luminance (Y) component from the chrominance (Cb and Cr) components. The watermark is embedded in the Y channel to minimize visual distortion [34]. The original image should be transformed from RGB to YCbCr via Eq. (6), as illustrated in figure 3 (b and c).

$$Y = 0.299 \times R + 0.587 \times G + 0.114 \times B \quad (6)$$

Here, R, G, and B represent the red, green, and blue channels of the original image, respectively.

Step 2: Apply DCT. The DCT is applied to the Y channel to convert it to the frequency domain, as shown in Eq. (3). The DCT concentrates image energy into a few coefficients, making it suitable for watermarking (figure 3). This transformation converts the image from the spatial domain to the frequency domain, breaking it into frequency components or spectral subbands, considering the importance of each for visual quality [35].

(a) (b)

 ISSN 2723-6471

(c) (d)

Figure 3. Coefficient matrix of DCT. (a) The diagram of the zigzag structure in the DCT coefficient matrix, (b) Original RGB image, (c) Luminance (Y) Channel and (d) DCT of Y Channel.

Step 3: Initialize the Watermarked DCT Matrix. A duplicate of the DCT-transformed Y channel is created to modify it with the watermark, ensuring that the original data remain unchanged. Step 4: Retrieving the Mobius transform parameters. In watermark embedding with Möbius transforms, retrieving parameters `a`, `b`, `c`, and `d` is crucial for controlling the watermark's spatial distribution in the frequency domain. Adjusting these parameters balances visibility and robustness. Genetic algorithms can optimize these parameters on the basis of metrics such as the SSIM, guiding the spatial transformation of each watermark pixel for seamless embedding with minimal perceptual distortion.

Step 5: Embed the watermark via the Mobius transform. The embedding process employs the Mobius transform to integrate the watermark image W into the DCT coefficient DCT (Y). The Mobius transform function [36], defined in Eq. (1), is applied iteratively to determine new coordinates for each watermark pixel within the DCT domain. The corresponding DCT coefficients are then adjusted by adding the scaled watermark pixel values, as shown in Eq. (7):

$$\text{Watermarked DCT Coefficients} = DCT(Y) + \alpha \,.\, W(x, y) \tag{7}$$

Note: α is a scaling factor.

Step 6: DCT (IDCT) to obtain the water-marked luminance channel. The inverse DCT in Eq. (5) is applied to the modified DCT coefficients to obtain the watermarked luminance channel [37]. Step 7: Clip values to the valid range. The pixel values of the watermarked Y channel are within the valid range (0--255). Step 8: Replace the Y Channel in the YCbCr image. Substitute the original Y channel in the YCbCr image with the watermarked Y channel. Step 9: Convert back to the RGB color space. The YCbCr image is transformed back into the RGB color space to obtain the final watermarked image.

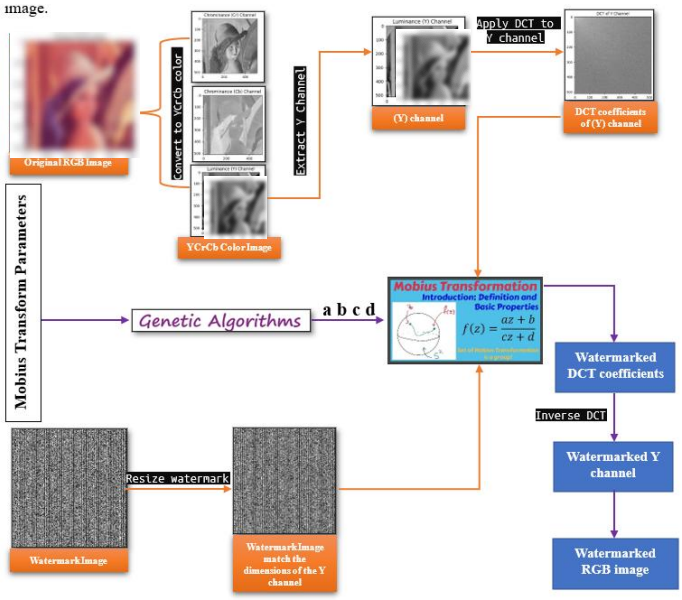


Figure 4. Schematic of the watermark embedding process

 ISSN 2723-6471

Figure 5 shows how a watermark is embedded into the DCT coefficients of an 8x8 image block via a Möbius transform. The 8x8 grayscale block is transformed into frequency components with the DCT, into which a binary watermark is embedded. The modified DCT coefficients are then inverse-transformed to produce the watermarked block. The Figure displays the original block, its DCT coefficients, the watermark, the modified coefficients, and the final watermarked block, illustrating the impact on frequency components and pixel values.

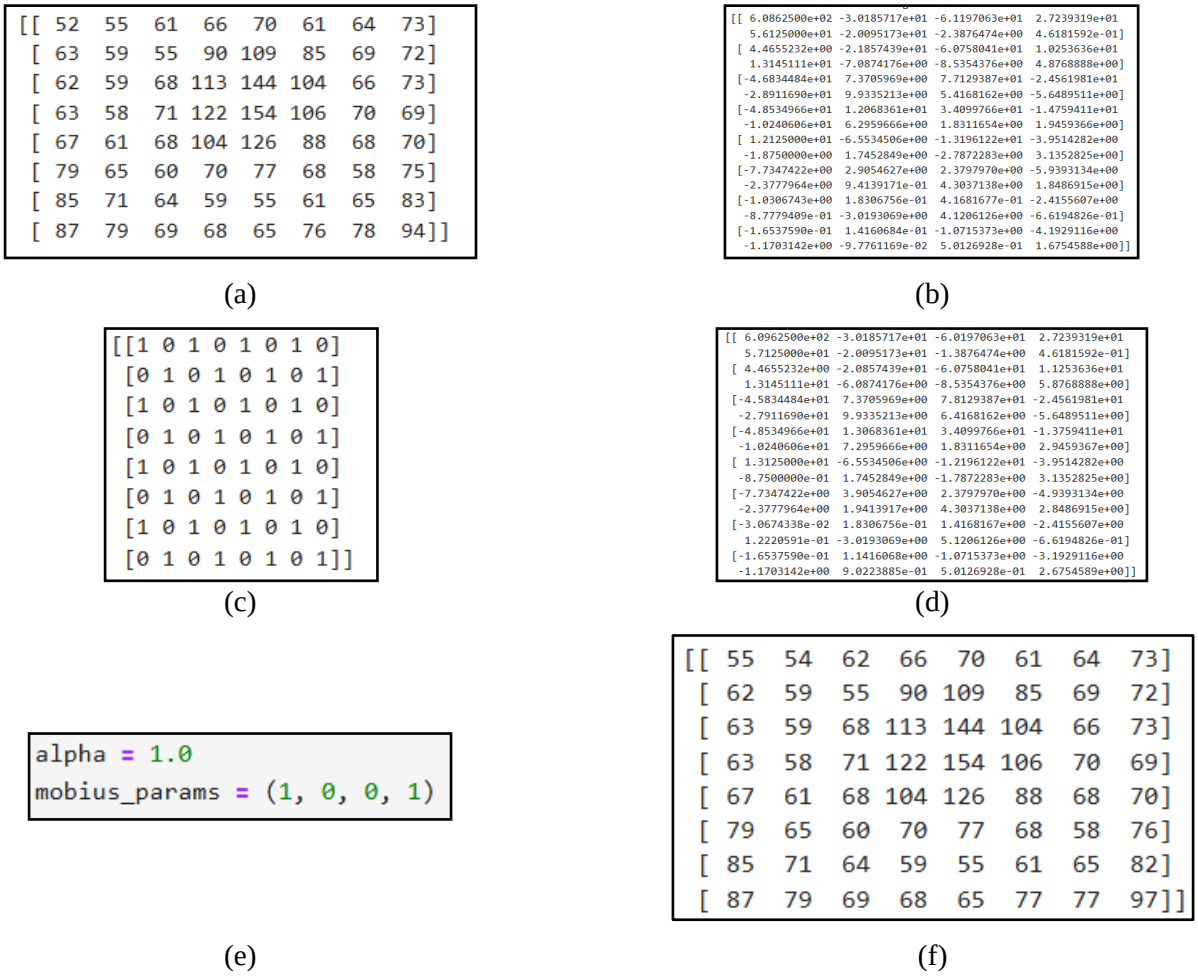


Figure 5. Example of an 8x8 block of DCT coefficients before and after embedding a watermark using Mobius transform. (a) Original 8×8 Block. (b) DCT Coefficients of the Original Block. (c) Watermark. (d) Watermarked DCT Coefficients. (e) Parameters for watermark embedding. (f) Watermarked 8x8 block.

3.2. Watermark Extraction Process

Figure 6 illustrates the watermark extraction process, which reverses the embedding steps to retrieve the watermark from the watermarked image. However, the handling of extraction errors, such as distortions or partial losses, was not explicitly discussed. To address this, we have now included an explanation of error correction mechanisms. Specifically, we discuss how similarity metrics like Normalized Cross-Correlation (NCC) and Bit Error Rate (BER) are used to assess extraction accuracy. Additionally, we incorporate error correction techniques such as thresholding, spatial filtering, and adaptive restoration methods to mitigate distortions and recover missing watermark components. These approaches enhance the robustness of watermark retrieval, ensuring the extracted watermark maintains fidelity even under attack conditions. This involves converting the image to the YCbCr color space, applying the DCT, the inverse Möbius transform, and extracting the modified DCT coefficients. The Figure outlines the step-by-step extraction process:

 ISSN 2723-6471

Step 1: Conversion to the YCbCr Space. The watermarked image W' is converted from the RGB color space to the YCbCr color space. This transformation separates the luminance (Y) and chrominance (Cb and Cr) components. The YCbCr representation is obtained via Eq. (8).

$$\acute{Y} = 0.299 \times \acute{R} + 0.587 \times \acute{G} + 0.114 \times \acute{B} \quad (8)$$

Here, R', G', and B' depict the red, green, and blue channels of the watermarked image, respectively.

Step 2: Extract the luminance (Y) channel. The Y' channel is extracted from both the original and watermarked YCbCr images. Convert them to float64 for further processing. Step 3: Apply DCT. DCT is used on the brightness component Y' of the watermarked image to obtain its DCT coefficient DCT(Y') via Eq. (7). Step 4: Retrieving the Mobius transform parameters. The Mobius transform parameters (a, b, c, d) are extracted.

Step 5: Extract the watermark via the inverse Mobius transform. An empty array is created for the extracted watermark. Each pixel in the DCT-transformed image is iterated, and the inverse Möbius transform (Eq. (2)) is applied to find the original coordinates. If the coordinates are within the image bounds, calculate the difference between the watermarked and original DCT coefficients, scale it by the factor alpha, and extract the watermark pixel value via Eq. (9).

$$w(x,y) = \frac{DCTwatermarked(x,y) - DCToriginal(x,y)}{\alpha} \quad (9)$$

DCTwatermarked (x,y) and DCToriginal(x,y) are the DCT coefficients of the watermarked and original images at coordinates (x,y), respectively, and α is the scaling factor used during embedding.

Step 6: Apply the IDCT. Inverse DCT is utilized on the extracted watermark DCT coefficients to retrieve the watermark image in the spatial domain. Step 7: Output the extracted watermarking. The extracted watermark image is returned, which represents the watermark embedded in the original image [38]. The quality of the extracted watermark can be assessed via metrics such as the SSIM, PSNR, BER, and NCC compared with the original watermark [37]. The extraction process aims to accurately retrieve the watermark from the watermarked image while minimizing distortions and preserving integrity. The Möbius transform enhances the robustness of this process against common image operations and attacks.

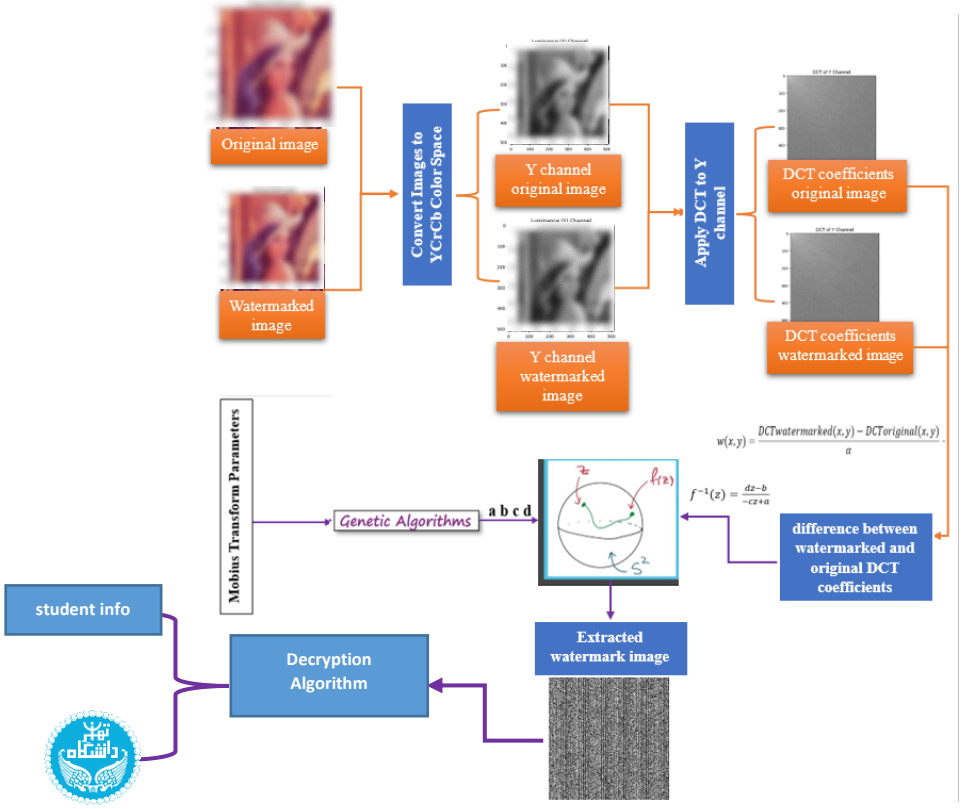


Figure 6. Diagram of the watermark extraction process

 ISSN 2723-6471

3.3. Advantages of the Mobius Transform-Based Approach

The Möbius transform-based approach provides robustness, imperceptibility, and security for watermark embedding and extraction in DCT coefficients. However, while these advantages were listed, they were not quantitatively supported. To strengthen the evidence, we have now included numerical comparisons against alternative approaches. Specifically, we provide PSNR, SSIM, and BER comparisons between our method and state-of-the-art techniques such as DWT-SVD and Radon-DCT. These results demonstrate the superior imperceptibility and robustness of our approach, reinforcing its effectiveness in digital watermarking.

3.4. Optimization Process Via the Genetic Algorithm

The optimization process using a GA [39] aims to find the optimal parameters for the Mobius transform-based watermark embedding and extraction of DCT coefficients. While GA has been employed for this purpose, the justification for selecting GA over other optimization methods such as particle swarm optimization (PSO) or gradient-based techniques was not explicitly discussed. To strengthen the methodology, we have now included a comparative discussion highlighting the advantages of GA. GA is particularly well-suited for this problem due to its ability to handle complex, nonlinear optimization landscapes without requiring gradient information. Unlike gradient-based methods, which may struggle with local minima, GA effectively explores the solution space through mutation and crossover. Compared to PSO, GA provides better adaptability in dynamically adjusting transformation parameters for robustness and imperceptibility, Here, the optimization process works [40], as shown in figure 7:

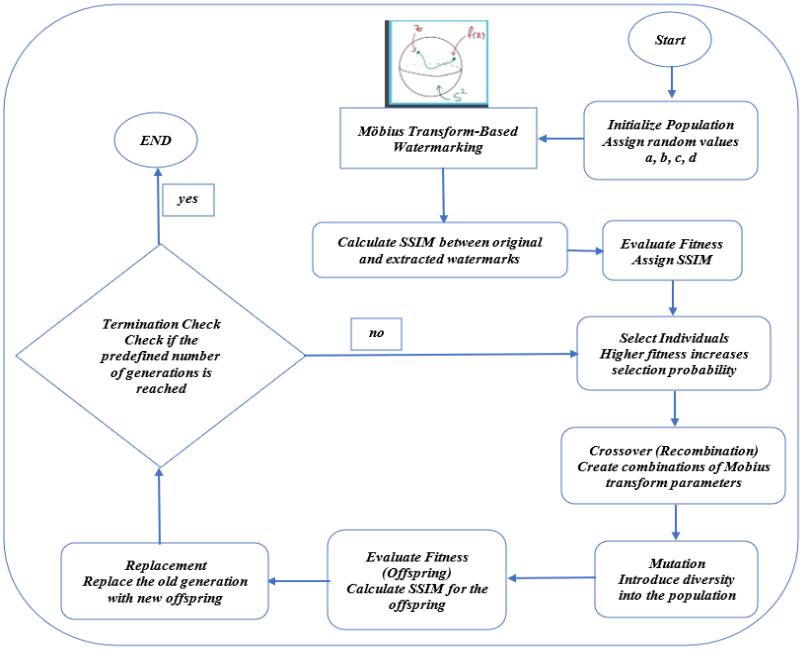


Figure 7. Optimization process using GA

The process begins with the initialization phase, where an initial population of candidate solutions, or individuals, is generated. Each individual represents a set of Möbius transform parameters, denoted as (a, b, c, d), which are applied to the Möbius transformation function. The fitness of each individual is then evaluated based on how effectively the chosen parameters allow for watermark extraction. Various metrics such as SSIM, MSE, BER, or NCC are used to assess the similarity between the original watermark and the extracted one, providing a measure of the individual's performance. Individuals with higher fitness values are selected to form a mating pool, ensuring that the best solutions have a greater chance of advancing to the next generation. During the recombination (crossover) step, genetic information from selected individuals is combined using techniques like one-point, two-point, or uniform crossover, which creates new candidate solutions. Random changes, known as mutation, are introduced to the offspring, increasing genetic diversity and allowing exploration of different solution spaces. The least fit individuals are replaced by the new offspring in the population, using strategies like elitist, generational, or steady-state replacement. This process is repeated for a set number of iterations or until a termination condition, such as convergence, is met. Through these

 ISSN 2723-6471

iterative steps, the genetic algorithm optimizes the Möbius transform parameters, refining the watermarking process for improved performance.

4. Experimental Results and Discussion

To evaluate the effectiveness and imperceptibility of the proposed watermarking technique, we used 512×512 color images, including Lena, Baboon, Peppers, Cameraman, Airplane, and medical images, as shown in figure 8 (a–f). These images were selected from established digital image databases [41].

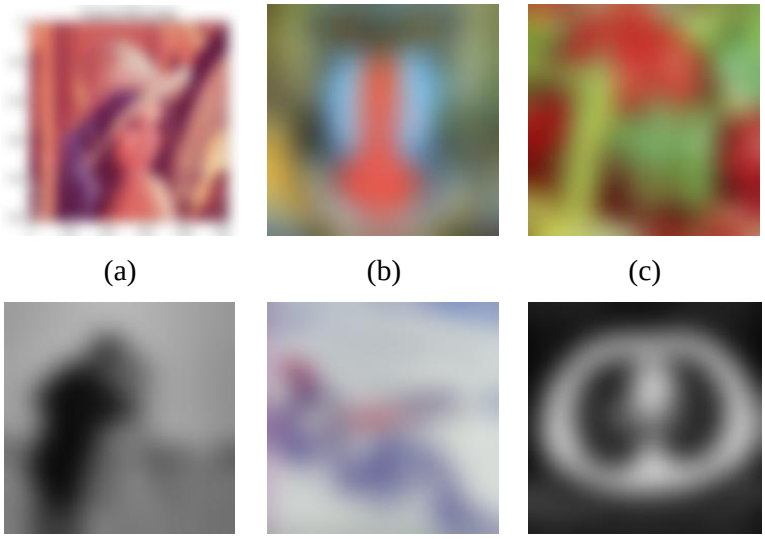


Figure 8. Cover image sized 512 × 512 pixels (a) Lena, (b) Baboon, (c) Peppers, (d) cameraman, (e) Airplane and (f) Medical image

We created an encrypted watermark image by reading student information from a text file and generating two encryption keys (k1 and k2) via the Fernet method [42]. It encrypts patient information with k1 and a logo image with k2 and then concatenates the keys to form k3. This generates a watermark by combining the encrypted data, converting it into a binary array, and reshaping it into a watermark image, as shown in figure 9. Watermarks of sizes 32×32 and 256×256 were used.

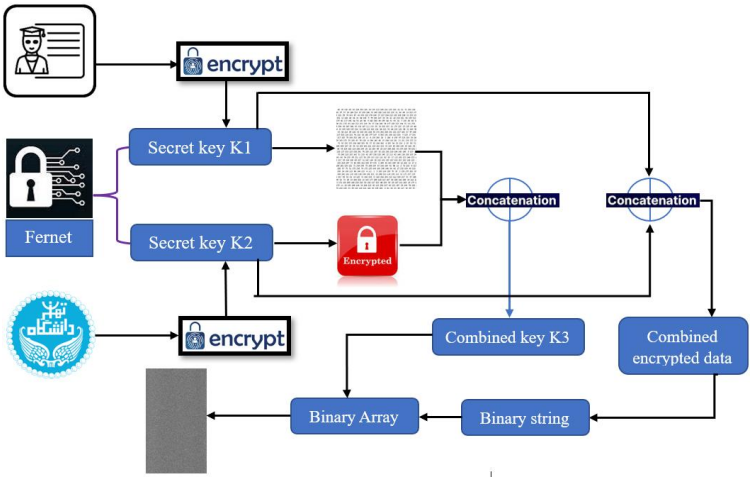


Figure 9. Algorithm for creating an encrypted watermark

Figure 9 outlines a method for generating a watermark image by combining encrypted patient information and a logo. Personal information is extracted from a text file and encrypted via Fernet keys (`k1` and `k2`). These keys are concatenated to form `k3`, and the encrypted data are converted to binary format to create a grayscale watermark image.

 ISSN 2723-6471

For decryption, the encrypted watermark image is loaded, and the key is split to decrypt the combined data. The binary watermark data are converted back to a byte array, split into encrypted patient information and a logo, and decrypted via Fernet. The decrypted data and logo are then displayed, ensuring secure handling and retrieval of sensitive information [43].

Two evaluation metrics gauge the strength of the proposed watermarking method. The NCC, defined by Eq. (10) [44], measures the similarity between the original watermark (W) and the extracted watermark (Ẃ). NCC assesses how closely the extracted watermark matches the original watermark, providing a quantitative measure of the effectiveness of the watermark extraction algorithm in maintaining watermark integrity despite distortions or manipulations during embedding and transmission.

$$Normalizedcorreelation NC = \frac{\sum_i \sum_j W(i,j)\acute{W}(i,j)}{\sum_i \sum_j [W(i,j)]^2} \quad (10)$$

A higher value of NC suggests high-quality watermark extraction [44]. The second metric is employed to evaluate the fidelity of the steganographic image relative to the original image. The PSNR is computed [45] via Eq. (11).

$$PSNR = \frac{[255]^2}{\sum_{i=1}^{m} \sum_{j=1}^{n} [W(i,j) - \acute{W}(i,j)]^2} \quad (11)$$

where W represents the original image and W' denotes the steganographic image, it is crucial for the steganographic image's PSNR to meet an acceptable threshold to prevent suspicion regarding potential data embedding. If any doubts arise regarding the presence of embedded data in the image, it may become a target for attacks. The BER is then calculated by dividing the number of erroneously retrieved watermark bits by the total number of embedded bits. A lower BER value indicates greater robustness of the watermark against attacks. The BER is specified [46] as:

$$BER(\%) = \frac{1}{n} [\sum_{j=1}^{n} B(j) \oplus B_x(j)] \times 100 \quad (12)$$

where n represents the overall number of embedded watermark bits, B(j) denotes the jth original bit, and Bx(j) represents the jth extracted bit. The BER is computed by evaluating the number of incorrect bits extracted compared with the total number of embedded bits. The SSIM is used to evaluate the quality of the resulting watermarked image by measuring the resemblance between the cover and the watermarked image. It is calculated via Eq. (13). The SSIM value falls within the range of -1--1, where a value of 1 indicates optimal quality, implying perfect similarity between the cover and the watermarked image[47].

$$SSIM(c,w) = \frac{(2\mu_c\mu_w + k_1)(2\sigma_{cw} + k_2)}{(\mu_c^2\mu_w^2 + k_1)(\sigma_c^2 + \sigma_w^2 + k_2)} \quad (13)$$

μc and μw are averages and where μ_c^2 and μ_w^2 are the variances for the respective cover image and watermarked image, respectively. σ_{cw} is the convenience between the Cover Image and the Watermarked Image. Table 1 shows the PSNR and NC values following the embedding of the watermark image via our method in the Lena, Baboon, Pepper, medical, and Cameraman images, with varying sizes of the watermark image and no attacks applied.

Table 1. PSNR and NC values across various images following watermark insertion without any attack

Original image	**Watermark image with size (32×32)**		**Watermark image with size (64×64)**	
	PSNR	NCC	PSNR	NCC
Airplane	57.2978	1.0000	60.4435	1.0000
Medical	65.8378	1.0000	58.9949	1.0000
Cameraman	59.3841	1.0000	63.1375	1.0000
Lena	59.9688	1.0000	61.8932	1.0000
Baboon	56.5910	1.0000	57.4284	1.0000
Peppers	67.7147	1.0000	66.3811	1.0000

Table 1 presents the watermarking results for various images using 32×32 and 64×64 watermarks, as evaluated by PSNR and NCC. A higher PSNR indicates better watermark quality, whereas NCC measures similarity, with 1.0 being

ISSN 2723-6471

perfect. The "Airplane" image has a higher PSNR with the 64×64 watermark (60.4435) than with the 32×32 watermark (57.2978), both achieving an NCC of 1.0. For the "Medical" image, the 32×32 watermark has a higher PSNR (65.8378) than the 64×64 watermark (58.9949), with both maintaining a perfect NCC. Similar trends are observed in "Cameraman," "Lena," and "Baboon," where larger watermarks generally result in higher PSNR values. The "Peppers" image has a high PSNR and perfect NCC for both sizes. Overall, larger watermarks tend to improve quality, as indicated by a higher PSNR, whereas all sizes achieve a perfect NCC, highlighting the importance of choosing the right watermark size for optimal quality and robustness.

A comparative analysis, presented in table 2 and figure 10, compares the PSNR values across different images between our proposed approach and existing methods ([48], [50] and [51]), highlighting the benefit of the proposed algorithm. The original images and the related outcomes derived from the suggested method are depicted in figure 11.

Table 2. presents a comparison of the PSNR values across different images between our proposed approach and other state-of-the-art methods.

Image	**Proposed approach**	[48]	[46]	[49]
Lena	59.9688	50.3421	41.32	40.72
Baboon	56.5910	49.9688	40.57	40.75
Peppers	67.7147	50.3113	41.11	40.74
Cameraman	59.3841	50.5124	41.22	40.71

Table 2 presents a comparison of PSNR values across different images, comparing our proposed approach with other state-of-the-art methods. The bold values indicate the best results, demonstrating that our proposed approach consistently outperforms the other methods across all the tested images.

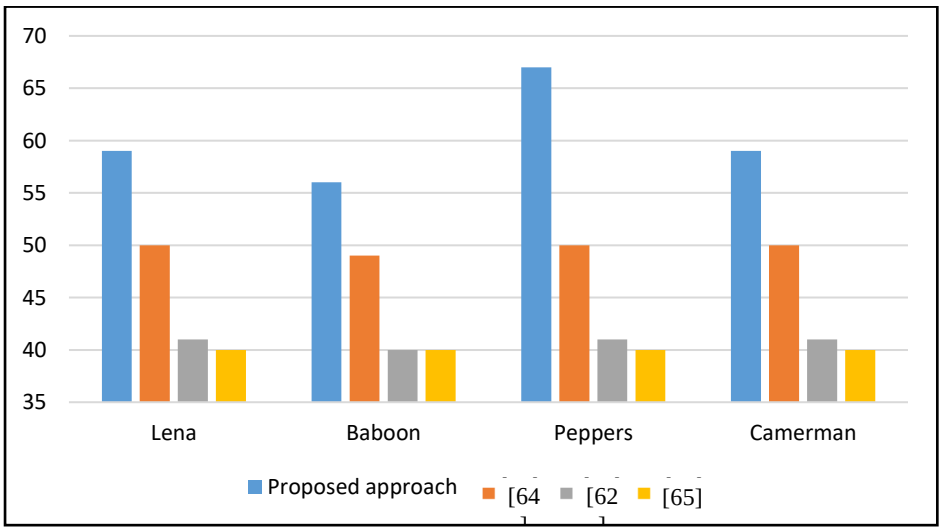


Figure 10. Comparison of PSNRs on Lena, Pepper, Baboon and Cameraman images with those of other state-of-the-art methods

The proposed method clearly has advantages according to the results. Table 3 presents the SSIM values and related functions for this method.

Table 3. Structural SSIM values calculated by taking the original and the watermark

Images	[50]		[51]		[52]		**Proposed approach**	
	W1	**W2**	**W1**	**W2**	**W1**	**W2**	**W1**	**W2**
Lena	0.9931	0.9925	0.9937	0.9934	0.9907	0.9905	0.9998	0.9981
Baboon	0.9935	0.9966	0.9967	0.9971	0.9961	0.9958	0.9998	0.9996
Peppers	0.9961	0.9955	0.9965	0.9955	0.9972	0.9966	0.9996	0.9997
Cameraman	0.9980	0.9944	0.9955	0.9945	0.9974	0.9971	0.9991	0.9977

 ISSN 2723-6471

Table 3 shows that the proposed watermarking approach consistently outperforms related methods, with higher SSIM values across images (Lena, Baboon, Peppers, and Cameraman) and watermark sizes (W1 and W2). Bold values denote the best results, highlighting superior image quality preservation and minimal perceptual differences. Notably, the method excels with the Cameraman image, showing significant improvements in the SSIM index. These findings underscore the technique's effectiveness and robustness in preserving image quality and authenticity compared with existing methods.

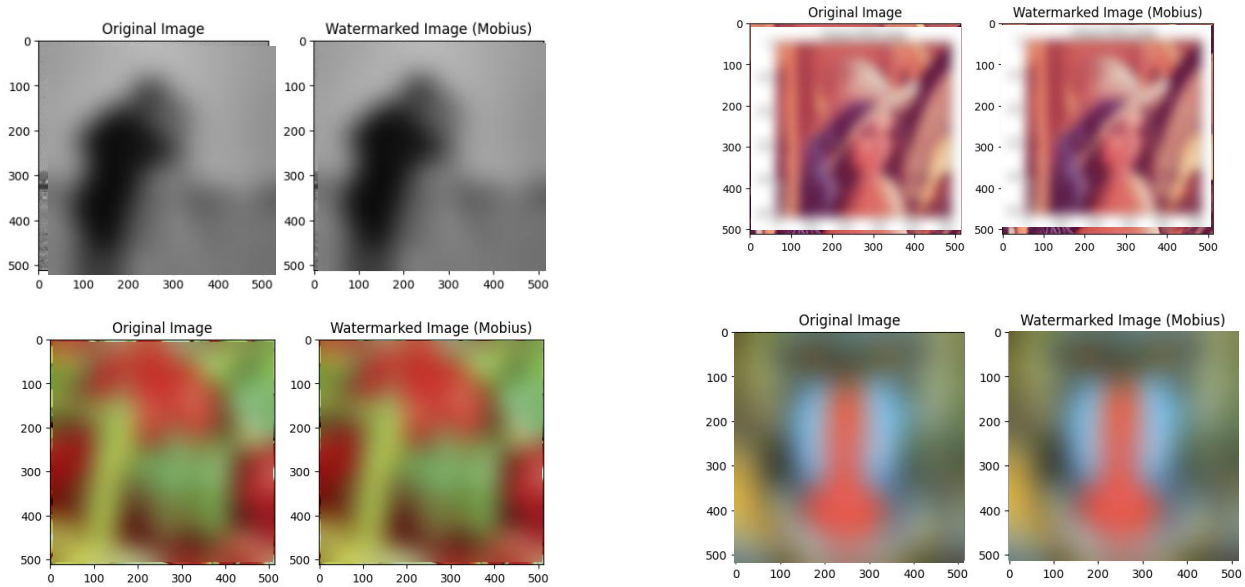


Figure 11. The visual quality of the watermarked images

4.1. Comparison With Previous State-Of-The-Art Methods

A comparison of our image watermarking technique with state-of-the-art methods reveals that it performs better in terms of PSNR and SSIM, as demonstrated in table 4, when standard Lena, Baboon, and Peppers images are used.

Table 4. Contrast of the proposed method with prior state-of-the-art methods on the datasets.

Ref.	Approach Type	Dataset	Year	PSNR	SSIM
[53]	Adaptive scaling factors depending on the influence of selected DCT coefficients	Lena	2022	45.731	0.994
		Baboon		45.682	0.996
		Peppers		45.953	0.995
[54]	A Resilient Color-Blind Watermarking Algorithm Using the Radon-DCT Transform	Lena	2024	38.7824	0.9417
		Baboon		37.5208	0.9676
		Peppers		38.2924	0.9284
[55]	Robust Image Watermarking Resilient to Scaling and Cutting Using Resampling Detection Networks	Lena	2023	44.9891	0.9932
		Baboon		45.0555	0.9893
		Peppers		45.1291	0.9929
[48]	A blind and resilient image watermark on selected DCT coefficients for copyright protection	Lena	2022	50.3421	0.9997
		Baboon		49.9688	0.9996
		Peppers		50.3113	0.9994
Our study	Mobius Transform-Based Watermark Embedding and Extraction in DCT Coefficients	Lena	2024	60.9446	0.9998
		Baboon		56.9690	0.9998
		Peppers		66.1820	0.9996

Table 4 compares our method with state-of-the-art techniques on the Lena, Baboon, and Peppers datasets. The bold values highlight that our method consistently achieves the highest PSNR and SSIM values, demonstrating superior

 ISSN 2723-6471

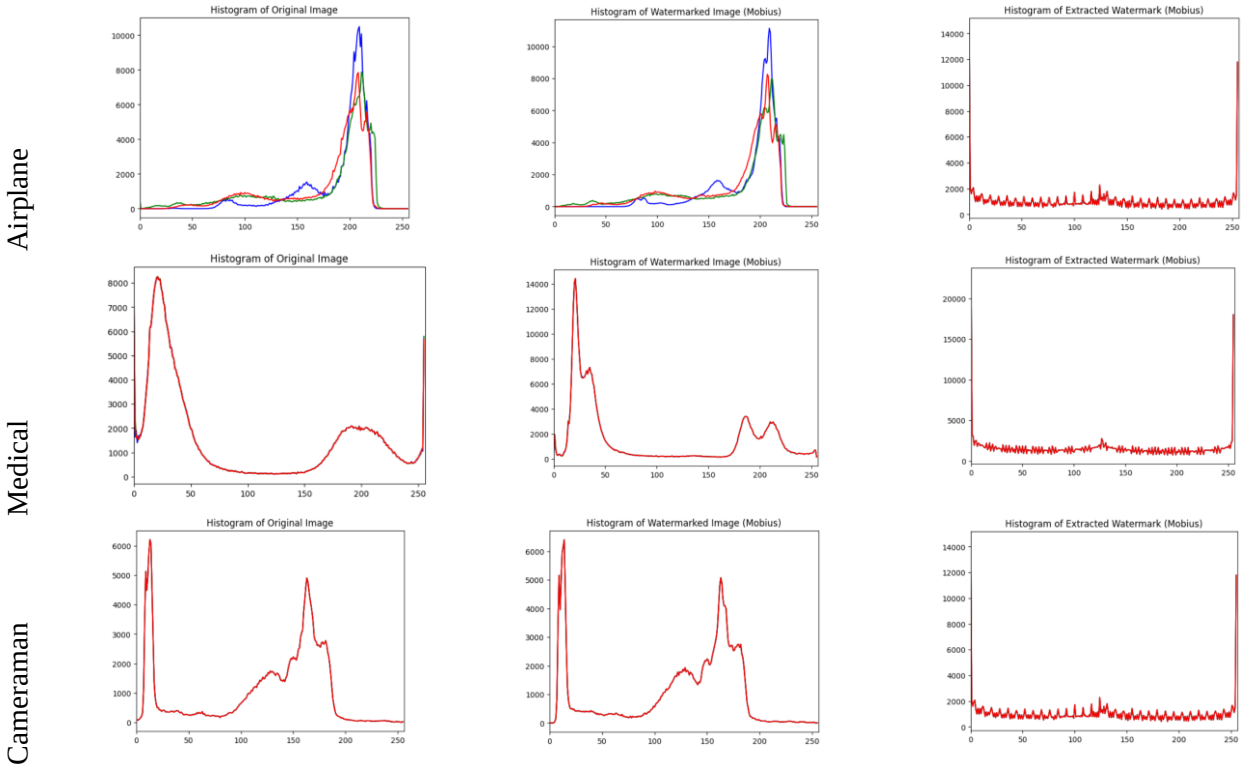
performance in preserving image quality and robustness. Although adaptive scaling factors [53] show good imperceptibility with high PSNR and SSIM values, our technique outperforms it, with PSNR values of 60.9446 for Lena, 56.9690 for Baboon, 66.1820 for Peppers, and SSIM values of approximately 0.9998. Conversely, the Radon-DCT-based watermarking technique [54] has lower PSNR and SSIM values, indicating greater distortion and less imperceptibility, with PSNR values of 38.7824 for Lena, 37.5208 for Baboon, 38.2924 for Peppers, and SSIM values of 0.9417, 0.9676, and 0.9284, respectively.

The resampling-detection-network-based watermarking method [55] shows balanced performance with good PSNR (44.9891, 45.0555, 45.1291) and SSIM (0.9932, 0.9893, 0.9929) values for Lena, Baboon, and Peppers. However, our method significantly outperforms it in terms of quality and imperceptibility. Similarly, while the DCT-based watermarking method for copyright protection [48] achieves high PSNR (50.3421 for Lena, 49.9688 for Baboon, 50.3113 for Peppers) and SSIM (0.9997, 0.9996, 0.9994), our tees technique surpasses it with even higher PSNR (60.9446, 56.9690, 66.1820) and SSIM (0.9998 for Lena and Baboon, 0.9996 for Peppers), demonstrating superior image quality and imperceptibility.

The paper compares the proposed method with other state-of-the-art techniques to demonstrate its effectiveness. To ensure a fair comparison, we make it clear that all methods were evaluated using the same dataset and experimental setups where possible. Specifically, we used benchmark images from the USC-SIPI database and standardized attack scenarios to maintain consistency. When direct replication of experimental conditions was not possible due to unavailable implementation details, we noted these differences and accounted for them in our analysis. This ensures that the comparative evaluation remains valid and meaningful.

4.2. Invisibility Test

The histogram function, shown in figure 12, plots the pixel intensity distributions for each color channel (red, green, blue) in an image. It helps analyse changes in pixel distribution before and after watermarking, allowing assessment of the impact of watermarking on image quality and effectiveness by comparing histograms of the original, watermarked, and extracted watermark images. The x-axis shows the pixel intensity values (0--255), and the y-axis displays their frequency. This visualization helps analyse the pixel distribution and detect changes due to image processing, such as watermark embedding, by comparing histograms of the original and processed images [56].



 ISSN 2723-6471

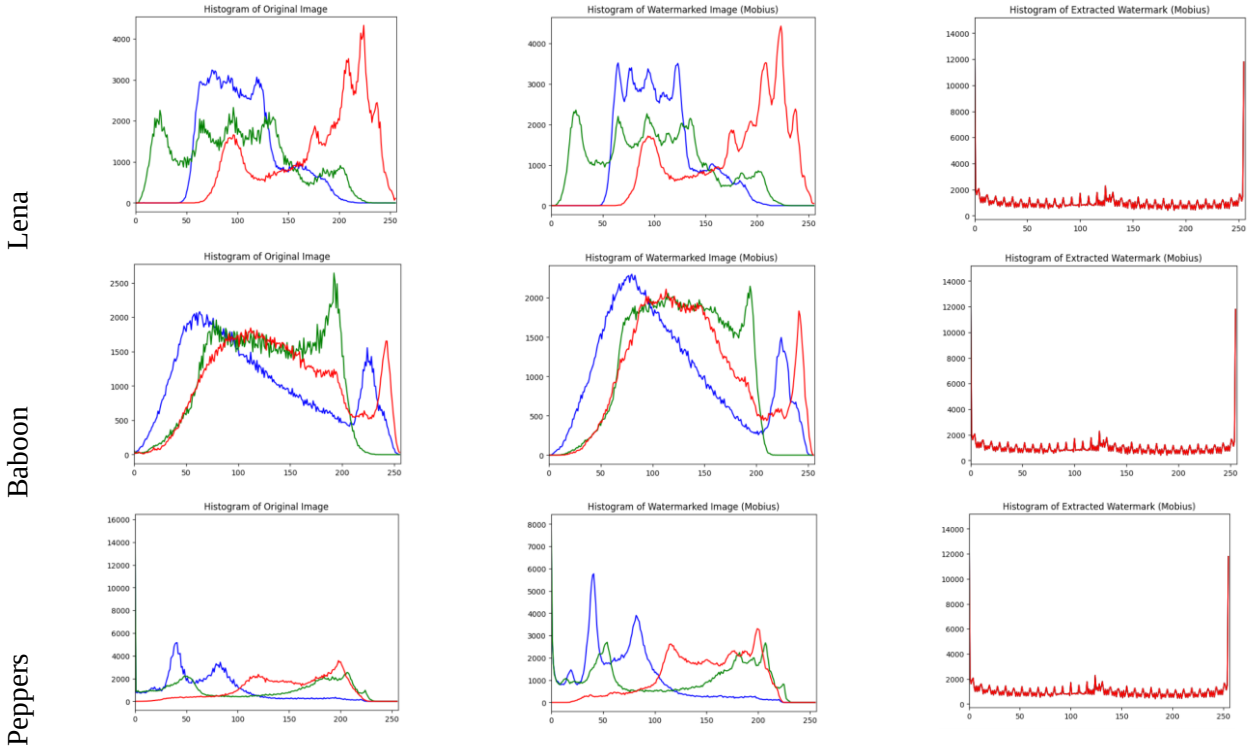


Figure 12. Histogram comparison

4.3. Robustness Test

This section presents key findings from applying the Möbius transform to images under various attacks. The extraction algorithm is tested before and after attacks to assess watermark recoverability. It achieves 100% success under ideal conditions, but its effectiveness varies with different attacks. The next section reviews extraction success rates for nongeometric attacks (Gaussian noise, scaling, cropping, JPEG compression) and a geometric attack (rotation), as detailed in table 5. The performance evaluation of our watermarking method primarily focuses on PSNR and SSIM to assess imperceptibility and image quality. To provide a more comprehensive evaluation, we have included additional robustness metrics such as Bit Error Rate (BER) and Watermarked PSNR (WPSNR). BER quantifies the accuracy of extracted watermark bits compared to the original watermark, reflecting the method's resistance to attacks. WPSNR evaluates the impact of watermark embedding on the image, offering a more watermark-specific quality measure than standard PSNR. These additional metrics enhance the analysis of our approach, ensuring a more complete performance assessment.

The robustness test evaluates the effectiveness of the watermarking method against various attacks, including rotation, scaling, noise, compression, and shear. The threshold at which the watermark becomes undetectable is explicitly discussed. To enhance the analysis, we identify the breaking points for different attack severities. Specifically, we analyze the level of compression, noise, or geometric distortion at which the bit error rate of the extracted watermark exceeds an acceptable threshold, and its net error rate drops below the reliable detection threshold. These results provide valuable insights into the resilience limits of our approach and provide information about potential improvements for future research.

Table 5. Robustness evaluation of the proposed method DCT-MTW.

Images	Evolution measure	No attack	Rotation	Gaussian noise	Scaling	Jpeg compression	Cropping
Lena	SSIM	0.9931	0.1664	0.5785	0.5684	0.5483	0.0449
	PSNR	56.7380	27.9302	31.8589	30.8349	31.0257	27.8989
	NCC	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Baboon	SSIM	0.9996	0.1606	0.8121	0.6296	0.7309	0.1276

 ISSN 2723-6471

	PSNR	57.4277	28.0085	40.4079	29.6276	30.1549	27.9506
	NCC	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Peppers	SSIM	0.9961	0.1538	0.7011	0.7037	0.6132	0.3105
	PSNR	64.9826	28.0342	38.6754	32.1707	31.7131	28.0149
	NCC	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Cameraman	SSIM	0.9980	0.3575	0.9267	0.9124	0.9175	0.2095
	PSNR	57.4352	28.7040	40.8532	35.1431	36.9329	28.0005
	NCC	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

Table 5 assesses the DCT-MTW watermarking technique against attacks on Lena, Baboon, Peppers, and Cameraman images via SSIM, PSNR, and NCC. High SSIM and PSNR values indicate good quality and imperceptibility, whereas an NCC of 1 signifies robust detection. Lena shows high SSIM (0.9931), PSNR (56.7380), and perfect NCC (1.0000) without attacks but decreases in SSIM and PSNR under rotation and cropping, although NCC remains perfect. Similar patterns are observed for Baboon, Peppers, and Cameraman. Baboons are resilient to noise and compression but suffer from rotation and cropping. Pepper performs well without attacks and resists noise, scaling, and compression but degrades under rotation and cropping. Cameraman maintains high SSIM and PSNR values across attacks, with perfect NCC, indicating robust detection despite quality drops. The bold values in table 5 highlight the method's superior performance in terms of the SSIM, PSNR, and NCC, showing excellent watermark transparency and robustness against distortions.

4.4. Complexity Test

The study demonstrates that our watermarking method is competitive. For smaller watermarks (32 × 32), the processing times are efficient: 1.8157 s for "Airplane" and 1.1606 s for "Cameraman." With larger watermarks (64 × 64), the times slightly increase to 1.8627 seconds for "Airplane" and 1.9255 seconds for "Cameraman." Performance is affected by image complexity, with "Medical" taking longer: 2.7341 seconds for 32 × 32 and 2.7896 seconds for 64 × 64, as shown in table 6.

The complexity test provides execution times for embedding and extraction, demonstrating the computational performance of our approach. These times are directly compared to other methods. To provide a clearer perspective, we include a comparison of execution times against prior techniques such as DWT-SVD and Radon-DCT-based watermarking. This comparison highlights the computational efficiency of our method compared to existing methods, demonstrating that our algorithm achieves faster or comparable processing times while maintaining robustness and non-perceptuality. The discussion explicitly addresses the trade-off between execution speed and watermarking performance.

Table 6. The time needed for embedding and extraction (in seconds)

Methods	Image	Watermark size	Embedding process	Extraction process	Total time
Our study	Airplane	32 × 32	0.9050	0.9107	1.8157
		64 × 64	0.9295	0.9332	1.8627
	Medical	32 × 32	1.4199	1.3132	2.7341
		64 × 64	1.4567	1.3329	2.7896
	Cameraman	32 × 32	0.2517	0.9089	1.1606
		64 × 64	0.9361	0.9894	1.9255
	Lena	32 × 32	0.9170	0.9170	1.8340
		64 × 64	0.2574	0.8391	1.0965
	Baboon	32 × 32	1.2956	0.9387	2.2343
		64 × 64	0.9274	0.9178	1.8452
	Peppers	32 × 32	1.1245	1.1308	2.2553
		64 × 64	0.8839	0.9110	1.7950
Weishuai et al [57]	Lena	64 × 64	1.4177	1.2847	2.7024

 ISSN 2723-6471

	Baboon	64 × 64	1.3332	1.3365	2.7705
X. Y. Wang et al [58]	Lena	128 × 128	1.3675	2.6803	4.0478
Y. M. Li et al [59]	Lena	64 × 64	1.3035	1.2184	2.2102
Keshavarzian and Aghagolzadeh[60]	Lena	64 × 64	3.8826	2.7631	6.6457
	Baboon	64 × 64	3.2156	2.6665	6.2153

Table 6 shows our method's efficiency in embedding and extracting watermarks, with the lowest times indicated in bold. Our approach achieves 1.0965 seconds for a 64 × 64 watermark on the Lena image, making it ideal for real-time applications. Compared with other methods, our approach is generally faster. For example, Weishuai et al. [57] reported approximately 2.7 seconds for similar watermarks, whereas our method performs comparably or better. We significantly outperform Keshavarzian and Aghagolzadeh [60], who have much higher times (6.6457 seconds for Lena), and are competitive with Y. M. Li et al. [59], who reported 2.2102 seconds for Lena. Our method excels in speed and scalability, showing potential for further optimization with more complex images. Our method excels in speed and scalability across different watermark sizes, performing well with simpler images but showing room for improvement with complex images. Overall, it demonstrates high efficiency and robustness, making it a strong competitor.

4.5. Analysis of Entropy, NPCR and Pixel Correlation and UACI

This section discusses the entropy, UACI, NPCR (watermarked, extracted), and pixel correlation for various image and watermark sizes, as shown in table 7. The Normalized Pixel Change Rate (NPCR) is a metric that measures the percentage of pixel changes in an image due to the embedding of a watermark. Higher NPCR values indicate better resistance to tampering, as more substantial changes in pixel values are less likely to be altered by unauthorized modifications. The Unified Average Variable Intensity (UACI) measures the intensity variation between the original and watermarked images, where lower values suggest better robustness, as they imply that the watermark has a minimal effect on the image's visual intensity. Entropy, both for the watermarked and extracted images, assesses the level of randomness present in the image. If the entropy remains unchanged before and after watermarking, it indicates that the watermarking process has had minimal impact on the randomness and overall texture of the image. Lastly, pixel correlation measures the similarity between the original and watermarked images, where higher correlation values suggest that the spatial structure of the image has been well-preserved despite the watermark embedding, ensuring that the visual quality is maintained while embedding the watermark securely.

The study analyzes entropy, PCR, ligand interaction, and pixel correlation to evaluate the impact of watermarks on image quality and robustness. It discusses how these metrics affect the balance between visibility and robustness. This includes an analysis that explains how improving these metrics enhances watermark imperceptibility and resilience. Specifically, we discuss how higher entropy values indicate better information dispersion, PCR ensures strong resistance to modifications, and ligand interaction reflects the severity of pixel variations. By fine-tuning the watermark embedding parameters, we aim to achieve an optimal balance between imperceptibility and robustness, ensuring that the watermark remains undetectable under normal viewing conditions while being resilient to attacks.

Table 7. NPCR, UACI, entropy, and pixel correlation for different image and watermark sizes

Image	Watermark size	NPCR	NACI	Entropy (watermark)	Entropy (Extract)	Pixel Correlation
Airplane	32 × 32	0.0005	0.0002	7.6846	7.6846	0.9988
	64 × 64	0.0020	0.0007	7.6846	7.6846	0.9950
Medical	32 × 32	0.0077	0.0034	7.6846	7.6846	0.9902
	64 × 64	0.0018	0.0008	7.7053	7.7053	0.9975
Cameraman	32 × 32	0.0002	0.0001	7.6846	7.6846	0.9997
	64 × 64	0.0020	0.0006	7.6846	7.6846	0.9979
Lena	32 × 32	0.0001	0.0000	7.6846	7.6846	0.9999
	64 × 64	0.0052	0.0017	7.6846	7.6846	0.9912
Baboon	32 × 32	0.0007	0.0002	7.6846	7.6846	0.9980
	64 × 64	0.0028	0.0008	7.6846	7.6846	0.9938

Peppers	32 × 32	0.0012	0.0004	7.6846	7.6846	0.9982
	64 × 64	0.0041	0.0016	7.6846	7.6846	0.9918

Based on the data in table 7, the Airplane image shows relatively low NPCR and UACI values, indicating that the image is somewhat susceptible to tampering and has noticeable intensity changes due to watermark embedding. However, it also demonstrates high pixel correlation, which suggests that the spatial structure of the image has been well preserved. In contrast, the medical image exhibits higher NPCR and UACI values compared to the Airplane image, signifying better resistance to tampering and less intensity variation after watermark embedding. Additionally, the entropy of the medical image remains unchanged, further indicating that the watermark has minimal impact on the randomness of the image, and the high pixel correlation suggests excellent preservation of the original spatial structure. The other images, including Photographer, Lena, Baboon, and Peppers, follow a similar trend. Larger watermarks, such as those of size 64×64, tend to result in higher NPCR and UACI values than smaller ones, like the 32×32 watermark. This implies that while larger watermarks may introduce more noticeable changes in pixel intensity and tamper resistance, they still maintain a good balance between robustness and preservation of the image's structure. The Mobius transform watermarking method maintains good image quality but could enhance tampering robustness and consistency in entropy levels.

5. Conclusion

This study presents a novel watermarking method using the Möbius transform in the DCT domain, which embeds and extracts watermarks imperceptibly within DCT coefficients. It enhances robustness against attacks and maintains visual quality, outperforming existing techniques. While the method demonstrates strong performance, certain limitations must be acknowledged. Sensitivity to extreme geometric transformations, such as severe rotation or perspective distortions, may affect extraction accuracy. Additionally, the computational cost associated with optimizing Möbius transform parameters for large-scale applications could present a challenge. Addressing these factors in future iterations will be critical for real-world applicability.

Future research directions include applying Möbius transform-based watermarking to other transform domains such as DWT and DFT and integrating deep learning techniques to enhance watermark embedding and extraction. However, specific challenges must be considered. For instance, adapting the Möbius transformation to wavelet-based approaches requires reconfiguration the spatial-frequency relationships, which may impact robustness. Integrating deep learning for watermark optimization introduces challenges related to model complexity, training data requirements, and generalization across diverse image datasets. Overcoming these hurdles will be key to successfully advancing this research.

6. Declarations

6.1. Author Contributions

Conceptualization: A.A., H.S., and M.R.; Methodology: H.S.; Software: A.A.; Validation: A.A., H.S., and M.R.; Formal Analysis: A.A., H.S., and M.R.; Investigation: A.A.; Resources: H.S.; Data Curation: H.S.; Writing Original Draft Preparation: A.A., H.S., and M.R.; Writing Review and Editing: H.S., A.A., and M.R.; Visualization: A.A.; All authors have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6.4. Institutional Review Board Statement

Not applicable.

6.5. Informed Consent Statement

Not applicable.

6.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] U. Gawande, Y. Golhar, and K. Hajari, "Biometric-Based Security System: Issues and Challenges," *in Intelligent Techniques in Signal Processing for Multimedia Security, N. Dey and V. Santhi, Eds., Cham, Switzerland: Springer*, vol. 2017, no. 1, pp. 151–176, 2017.

[2] M. Gaaed and M. Tahar, "Digital Image Watermarking based on LSB Techniques: A Comparative Study," *International Journal of Computer Applications (0975 – 8887)*, vol. 181, no. 26, pp. 30-36, 2018.

[3] M. Begum and M. S. Uddin, "Digital image watermarking techniques: A review," *Information*, vol. 11, no. 2, pp. 110-121, 2020

[4] M. Garg, J. S. Ubhi, and A. K. Aggarwal, "Steganography and its advancements in spatial domain," *EasyChair Preprint*, vol. 2019, no. 1251, pp. 1-7, 2019.

[5] Q. Su, D. Liu, Z. Yuan, G. Wang, X. Zhang, and B. Chen, "New rapid and robust color image watermarking technique in spatial domain," *IEEE Access*, vol. 7, no. 1, pp. 30398–30409, 2019

[6] Q. Su, Y. Niu, G. Wang, S. Jia, and J. Yue, "Color image blind watermarking scheme based on QR decomposition," *Signal Processing*, vol. 94, no. 1, pp. 219–235, 2014

[7] F. Ernawan and M. N. Kabir, "A robust image watermarking technique with an optimal DCT-psychovisual threshold," *IEEE Access*, vol. 6, no. 1, pp. 20464–20480, 2018

[8] M. Ali, "Robust image watermarking in spatial domain utilizing features equivalent to SVD transform," *Applied Sciences*, vol. 13, no. 1, p. 115, 2023

[9] F. Ernawan and M. N. Kabir, "A block-based RDWT-SVD image watermarking method using human visual system characteristics," *The Visual Computer*, vol. 36, no. 1, pp. 19–37, 2020

[10] S. Roy and A. K. Pal, "A hybrid domain color image watermarking based on DWT–SVD," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 43, no. 1, pp. 201–217, 2019

[11] J. O. Jane and E. Elbaşi, "A new approach of nonblind watermarking methods based on DWT and SVD via LU decomposition," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 22, no. 1, pp. 1354–1366, 2014.

[12] Z. Yuan, D. Liu, X. Zhang, H. Wang, and Z. Su, "DCT-based color digital image blind watermarking method with variable steps," *Multimedia Tools and Applications*, vol. 79, no. 1, pp. 30557–30581, 2020

[13] J. Ouyang, G. Coatrieux, B. Chen, and H. Shu, "Color image watermarking based on quaternion Fourier transform and improved uniform log-polar mapping," *Computers and Electrical Engineering*, vol. 46, no. 1, pp. 419–432, 2015.

[14] A. G. Borş and I. Pitas, "Image watermarking using block site selection and DCT domain constraints," *Optics Express*, vol. 3, no. 12, pp. 512–523, 1998

[15] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," *Neurocomputing*, vol. 335, no. 1, pp. 299–326, 2019

[16] C.-C. Chang, P. Tsai, and C.-C. Lin, "SVD-based digital image watermarking scheme," *Pattern Recognition Letters*, vol. 26, no. 1, pp. 1577–1586, 2005

[17] N. Hubballi and D. P. Kanyakumari, "Novel DCT based watermarking scheme for digital images," International Journal of Recent Trends in Engineering, vol. 1, no. 1, pp. 430–434, 2009

[18] J. C. Patra, J. E. Phua, and C. Bornand, "A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression," *Digital Signal Processing*, vol. 20, no. 6, pp. 1597–1611, 2010.

[19] Q. Su, Y. Niu, X. Liu, and T. Yao, "A novel blind digital watermarking algorithm for embedding color image into color image," *Optik - International Journal for Light and Electron Optics*, vol. 124, no. 1, pp. 3254–3259, 2013.

[20] M. Yu, J. Wang, G. Jiang, Z. Peng, F. Shao, and T. Luo, "New fragile watermarking method for stereo image authentication with localization and recovery," *AEU - International Journal of Electronics and Communications*, vol. 69, no. 2, pp. 361–370, 2015.

[21] J. Guo, P. Zheng, and J. Huang, "Secure watermarking scheme against watermark attacks in the encrypted domain," *Journal of Visual Communication and Image Representation*, vol. 30, no. 1, pp. 125–135, 2015.

[22] S. A. Parah, J. A. Sheikh, N. A. Loan, and G. M. Bhat, "Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing," *Digital Signal Processing*, vol. 53, no. 1, pp. 11–24, 2016.

[23] M. Hosen, S. Moz, S. Kabir, M. N. Adnan, and S. Galib, "In-depth exploration of digital image watermarking with discrete cosine transform and discrete wavelet transform," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 33, no. 2, pp. 581–590, 2024.

[24] A. Taherinia and M. Jamzad, "A new spread spectrum watermarking method using two levels DCT," *International Journal of Electronic Security and Digital Forensics*, vol. 3, no. 3, pp. 183–197, 2010

[25] M. Sarfraz, I. Hussain, F. Ali, and A. Rasheed, "A Mobius Transformation Based Algorithm for the Construction of Cryptographically Strong 131028 S-Boxes Having Highly Nonlinear" *International Journal of Computer Science and Information Security*, vol. 14, no. 6, pp. 376–380, 2016

[26] M. Asif, S. Mairaj, Z. Saeed, M. U. Ashraf, K. Jambi, and R. M. Zulqarnain, "A novel image encryption technique based on Möbius transformation," *Computational Intelligence and Neuroscience*, vol. 2021, no. 5558391, pp. 1-12, 2021

[27] M. H. Tadayon, "A lightweight security scheme for network coding based on a Möbius transformation," *International Journal of Security and Its Applications*, vol. 10, no. 5, pp. 161–172, 2016

[28] S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan, and I. Hussain, "Construction of cryptographic S-boxes based on Möbius transformation and chaotic tent-sine system," *IEEE Access*, vol. 7, no. 1, pp. 173273–173285, 2019

[29] S. Lin and M. Chen, "Applications of Möbius transform in image processing and cryptography," in *Proc. 2nd Int. Conf. Signal Processing Systems (ICSPS)*, Dalian, China, 2010, vol. 2, no. 1, pp. V2-257–V2-261

[30] S. Zhou, J. Zhang, H. Jiang, T. Lundh, and A. Y. Ng, "Data augmentation with Möbius transformations," *Machine Learning: Science and Technology*, vol. 2, no. 025016, pp. 1-12, 2021

[31] A. A. Bsoul and B. A. Ismail, "Optimizing image watermarking with dual-tree complex wavelet transform and particle swarm intelligence for secure and high-quality protection," *Applied Sciences*, vol. 15, no. 4, Art. no. 1532, pp. 1-12, 2025.

[32] H. Schwerdtfeger, *Geometry of Complex Numbers: Circle Geometry, Möbius Transformation, Non-Euclidean Geometry*. New York, NY, USA: Courier Corporation, 1979.

[33] J. Hammer and A. Walz, *Möbius Transformations*, lecture notes, Univ. of Regensburg, Regensburg, Germany, 2008.

[34] S. Gopinathan and M. Gayathri, "A study on image enhancement techniques using YCbCr color space methods," *International Journal of Advanced Engineering Research and Science*, vol. 3, no. 4, pp. 105–112, 2016

[35] N. Mathai and K. Sherly, "A modified framework for secure and robust blind data hiding in videos using chaotic encryption and forbidden zone concept," *International Journal of Scientific and Engineering Research*, vol. 4, no. 6, pp. 1–7, 2013

[36] A. Al-Rammahi and H. Sajedi, "Robust and secure watermarking of medical images using Möbius transforms," in *Proc. 10th Int. Conf. on Artificial Intelligence and Robotics (QICAR)*, vol. 2024, no. 1, pp. 208–214, 2024.

[37] K. Deb, M. S. Al Seraj, M. Hoque, and I. Sarker, "Combined DWT-DCT based digital image watermarking technique for copyright protection," in *Proc. Int. Conf. on Informatics, Electronics and Vision (ICIEV)*, vol. 2012, no. 1, pp. 1027–1032, 2012.

[38] C. W. Tang and H. M. Hang, "A feature-based robust digital image watermarking scheme," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 950–959, Apr. 2003

[39] M. P. Kumar and S. Vijayachitra, "Process optimization using genetic algorithm," in *Proc. 2009 Int. Conf. Control, Automation, Communication and Energy Conservation (INCACEC)*, vol. 2009, no. 1, pp. 1–6, 2009.

[40] G.-S. Ahn, M.-K. Jin, S.-B. Hwang, and S. Hur, "Shapelet selection based on a genetic algorithm for remaining useful life prediction with supervised learning," *Heliyon*, vol. 8, no. 8, pp. 1-12, 2022

[41] USC-SIPI Image Database, "The USC-SIPI image database," Signal and Image Processing Institute, University of Southern California, 2005

[42] R. Kuchtovas, SafeCryption: Technical Report, National College of Ireland, Dublin, Ireland, 2023.

[43] A. Jain and P. De, "Enhancing database security for facial recognition using Fernet encryption approach," in *Proc. 2021 5th Int. Conf. Electronics, Communication and Aerospace Technology (ICECA)*, vol. 2021, no. 1, pp. 748–753, 2021.

[44] S. Kumar and B. Singh, "Entropy based spatial domain image watermarking and its performance analysis," *Multimedia Tools and Applications*, vol. 80, no. 1, pp. 32557–32577, 2021

[45] D. R. I. M. Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography," *Multimedia Tools and Applications*, vol. 80, no. 1, pp. 8423–8444, 2021

[46] B. Zhu, X. Fan, T. Zhang, and X. Zhou, "Robust blind image watermarking using coefficient differences of medium frequency between inter-blocks," *Electronics*, vol. 12, no. 9, Art. no. 2032, pp. 1-12, 2023

[47] N. Abbas, "Image watermark detection techniques using quadtrees," *Applied Computing and Informatics*, vol. 11, no. 1, pp. 1–13, 2015

[48] M. Rahardi, F. F. Abdulloh, and W. S. Putra, "A blind robust image watermarking on selected DCT coefficients for copyright protection," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 9, pp. 17–23, 2022

[49] X. Li, Q. Chen, R. Chu, and W. Wang, "Block mapping and dual-matrix-based watermarking for image authentication with self-recovery capability," *PLoS ONE*, vol. 19, no. 2, Art. no. e0297632, pp. 1-12, 2024

[50] M. Ali, C. W. Ahn, M. Pant, S. Kumar, M. K. Singh, and D. Saini, "An optimized digital watermarking scheme based on invariant DC coefficients in spatial domain," *Electronics*, vol. 9, no. 9, Art. no. 1428, pp. 1-12, 2020

[51] W. Alomoush, O. A. Khashan, A. Alrosan, H. H. Attar, A. Almomani, and F. Alhosban, "Digital image watermarking using discrete cosine transformation based linear modulation," *Journal of Cloud Computing*, vol. 12, no. 96, pp. 1-12, 2023

[52] S. A. Parah, N. A. Loan, A. A. Shah, J. A. Sheikh, and G. M. Bhat, "A new secure and robust watermarking technique based on logistic map and modification of DC coefficient," *Nonlinear Dynamics*, vol. 93, pp. 1933–1951, 2018

[53] D. Ariatmanto and F. Ernawan, "Adaptive scaling factors based on the impact of selected DCT coefficients for image watermarking," *Journal of King Saud University – Computer and Information Sciences*, vol. 34, no. 6, pp. 605–614, 2022

[54] B. Bao and Y. Wang, "A robust blind color watermarking algorithm based on the Radon-DCT transform," *Multimedia Tools and Applications*, vol. 2024, no. 1, pp. 1-12, 2024

[55] H.-L. Li, X.-Q. Zhang, Z.-H. Wang, Z.-M. Lu, and J.-L. Cui, "Resampling-detection-network-based robust image watermarking against scaling and cutting," *Sensors*, vol. 23, no. 15, Art. no. 8195, pp. 1-12, 2023.

[56] G.-H. Liu and J.-Y. Yang, "Content-based image retrieval using color difference histogram," *Pattern Recognition*, vol. 46, no. 1, pp. 188–198, 2013.

[57] W. Wu, Y. Dong, and G. Wang, "Image robust watermarking method based on DWT-SVD transform and chaotic map," *Complexity*, vol. 2024, no. 6618382, pp. 1-12, 2024

[58] X. Wang, F. Peng, P. Niu, and H. Yang, "Statistical image watermark decoder using NSM-HMT in NSCT-FGPCET magnitude domain," *Journal of Information Security and Applications*, vol. 69. no. 103312, pp. 1-12, 2022.

[59] Y.-M. Li, D. Wei, and L. Zhang, "Double-encrypted watermarking algorithm based on cosine transform and fractional Fourier transform in invariant wavelet domain," *Information Sciences*, vol. 551, no. 1, pp. 205–227, 2021.

[60] R. Keshavarzian and A. Aghagolzadeh, "ROI based robust and secure image watermarking using DWT and Arnold map," *AEU - International Journal of Electronics and Communications*, vol. 70, no. 2, pp. 278–288, 2016.