Multimedia Tools and Applications
https://doi.org/10.1007/s11042-024-19781-w

# Optimized digital watermarking: Harnessing the synergies of Schur matrix factorization, DCT, and DWT for superior image ownership proofing

Issa Al-Aiash[1] · Rabee Alquran[1] · Mahmoud AlJamal[1] · Ayoub Alsarhan[1] · Mohammad Aljaidi[2] · Dimah Al-Fraihat[3]

Received: 10 November 2023 / Revised: 24 June 2024 / Accepted: 27 June 2024

## Abstract

The contemporary context of abundant digital dissemination inherently gives rise to the need for media protection and the clear identification of ownership rights. This paper responded to this nagging issue of unauthorized media capture by developing a new digital watermarking approach uniting the Discrete Wavelet Transform DWT, Discrete Cosine Transform DCT, and Schur matrix factorization. The proposed watermark, which was a positive vector uniformly distributed, presented a high degree of robustness to several adversarial operating conditions, including histogram equalization, salt and pepper noise, ripple impact, smoothing attack, and cropping. The obtained results reveal the effectiveness of our approach. The correlation coefficient between watermarked and original images remains exceptionally high at 0.999998, ensuring minimal visual distortion. Mean Squared Error (MSE) graphs for both high-frequency (HH) and low-frequency (LL) domains demonstrate negligible changes after attacks, confirming the watermark's robustness. Notably, the watermark extraction process remains successful even after histogram equalization, as indicated by significantly lower MSE compared to random vectors. Moreover, the average processing times for different attacks are promising; Histogram Equalization and Salt and Pepper attacks each took 0.3 s, Ripple Attack required 0.28 s, Smoothing Attack completed in 0.29 s, and the Cropping Attack took 0.6 s. The robustness of our approach appears against the salt and pepper attack, which historically presented a vulnerability when employing Schur matrix factorization in image watermarking, indicating the novelty of and this contribution to improving media ownership verification. By combining disparate transformation methodologies, this technique offers a promising avenue for reinforcing the integrity and authenticity of digital media, thereby strengthening the foundations of intellectual property rights in the digital domain.

**Keywords** Digital Watermarking · Discrete Wavelet Transform (DWT) · Discrete Cosine Transform (DCT) · Schur Matrix Factorization · Media Ownership Verification

Extended author information available on the last page of the article

Published online: 17 July 2024

# 1 Introduction

The Internet is inevitably developing tremendously. Every day, data transfer rates exponentially increase, allowing the transfer of vast amounts of data through the Internet with absolute ease and convenience, such as images, videos, audio clips, and other media objects. Therefore, it is highly important to adopt certain techniques to ensure security and maintain the ownership of the data and information. One of the solutions is the image-based copy detection system. The image-based copy detection technique involves the comparison of the visual characteristics of an image to assess if it is simply a copy of another image. The visual characteristics can include color histograms, texture descriptors, and shape information [1]. The most common approach involves image hashing, creating a unique digital fingerprint for every image based on its visual features. Then, the "hash" for both images is compared. One of the disadvantages of this method is its ineffectiveness in slightly modified images, high resource consumption, dependence on the accuracy type, and likelihood of false detection [2].

Encryption techniques are common techniques used to establish security regarding images, which convert the original data into incomprehensible and unreadable data, thereby ensuring the absence of the perception of ownership [3]. However, the drawback of this method is that if the encryption is decrypted by the intruder, and the encrypted data is received, then it will be impossible to prove the ownership of the image. The most common way to prove ownership of an image is to embed a digital watermark. A digital watermark is defined as an embedded code or hidden information in the image, which is used to prove ownership and prevent copyright infringement [4]. Depending on the specific carrier, different methods can be used to embed watermarks in the image [5]. There are two fundamental types of techniques for embedding a watermark: spatial domain watermarking [6] and frequency domain watermarking [7, 8].

In watermarking, the Frequency domain is used as a technique that embeds a watermark into digital media such as images, audio, or video in the frequency domain [9]. The main goal is to transform the initial digital media's frequency domain from its time domain, insert the watermark in the transformed domain, and then convert the watermarked media back to the time domain for storage or transmission [10]. One of the most important and widely used technologies is Discrete Cosine Transform (DCT); in DCT-based watermarking, a host media is divided into non-overlapping chunks of pixels and then transformed by the DCT [11].

Reviewing the literature reveals concerns related to the vulnerability of Schur matrix factorization in the domain of watermarking. This vulnerability has been successfully addressed and resolved in the present study. The transformed coefficients undergo modification by the addition of the watermark signal, resulting in watermarked coefficients. Typically, the watermark signal is a binary sequence or a pseudo-random noise signal that remains imperceptible to the human eye or ear [12]. Additionally, the Fast Hadamard Transform (FHT) technique is utilized for the inconspicuous embedding and high accuracy ratio of watermarks within electronic images [13]. Other techniques employed include the Discrete Fourier Transform (DFT) [14], Discrete Wavelet Transform (DWT) [15], and Singular Value Decomposition (SVD) [16].

This study addresses the challenge of unauthorized media capture by introducing a novel digital watermarking method that combines DWT, DCT, and Schur matrix factorization. The proposed watermark, distributed as a positive vector uniformly, exhibits robustness against various adversarial conditions, including histogram equalization, salt and pepper noise, ripple impact, smoothing attack, and cropping. Notably, even when tested with 1000 random vectors, the watermark signal remains distinguishable. Results indicate the effectiveness of our approach, with a remarkably high correlation coefficient of 0.999998 between watermarked and original images, ensuring minimal visual distortion. Mean Squared Error (MSE) analysis in both high-frequency and low-frequency domains confirms the watermark's resilience, particularly evident in withstanding histogram equalization. Additionally, the method demonstrates promising processing times for different attacks, ranging from 0.28 to 0.6 s, under consistent hardware conditions. Importantly, our approach shows robustness against salt and pepper attacks, historically challenging for Schur matrix factorization-based watermarking, underscoring its novelty in enhancing media ownership verification. By integrating diverse transformation techniques, this method holds potential for bolstering the integrity and authenticity of digital media, thus fortifying intellectual property rights in the digital realm.

The reminder of this paper is structured as follows: Sect. 2 discusses the recent related literature in the field of watermarking, Sect. 3 introduces the concept of frequency-based watermarking and the utilized frequency transforms, Sect. 4 describes watermarking process, followed by Sect. 5 where we present the experimental results and analysis on the applied watermarking scheme. Section 6 presents the conclusion, limitations, and avenues for future research.

## 2 Literature review

Several studies have contributed significantly to the advancement of watermarking techniques. One such study introduces a novel concept of inserting a watermark into cover images, preserving robustness against attacks and imperceptibility [17]. The proposed approach integrates a hybrid watermark model combining Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). In the DWT sub-bands of the image, the watermark is inserted in the 'Singular Values'. Soualmi et al. [18] proposed a semi-blind approach for embedding the watermark based on Schur decomposition and Discrete Cosine Transform in the medical field, specifically for medical images. By using Schur decomposition, the image is resilient to cyber-attacks, and the quality of the image is retained after embedding. The image is divided into blocks and analyzed using Schur decomposition, while the watermark is embedded in the average DCT coefficient of the blocks of the image.

Emad et al. [19] suggested another technique of implementing watermarks in media utilizing DWT and segmenting the image into four subbands. Afterwards, the FHT was implemented in each subband, after which the SVD patch was carried out. This has notably enhanced the data embedding structure while also maintaining the invisibility property of the watermark. Another potential opportunity for implementing the watermark in the image is depicted in [20], for instance, to show proof of ownership. In this case, DWT and Non-negative Matrix Factorization were used, and afterwards, DWT dismembers the images into four wavelet sub-bands. The idea is to utilize NMF on each sub-band block before the eigen decomposition distortion is done.

In accordance with [21], Ahmad et al. proposed a novel approach to watermark embedding in images with Schur decomposition for media image ownership proof. This approach is attractive because it is not reversible, requires less computation than SVD, is less affected by geometric distortions, and can withstand JPEG compression attacks. In

[22], Reena et al. proposed another approach to embed watermarks in images using Schur Factorization via the Contourlet Transform (CT), Matrix Factorization, and SVD. The "cover image" and the "watermark image" are first subjected to CT. Then the watermarked image and the inverse SVD are generated by CT operations using the watermark's singular values embedding coefficients in the original image's singular values. The following section of the study's background builds on the work of prior researchers by expanding on some of the novel techniques introduced and reinitializing the expanding versatility of image watermarking as a critical tool for media security and ownership proof.

## 3 Background of study

The background of the study explores the fundamental aspects of image watermarking techniques, specifically: Frequency-based Watermarking, and Utilized Transforms. A comprehensive understanding of these crucial components serves as a foundation for exploring the intricacies and advancements in the field of digital media security and ownership verification.

### 3.1 Frequency-based watermarking

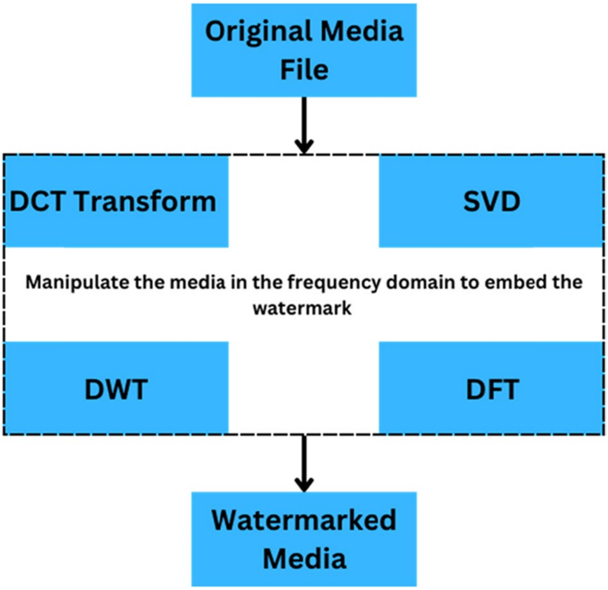
Frequency-based watermarking methods are the most widely used techniques to incorporate a digital watermark into a multimedia file, including an image, audio file, or video clip [23]. The technique aims at hiding a delicate and invisible signal that acts as a signature when unburied and is used to protect copyright, identify legitimate owners, certify authenticity, supply chain traceability, and check for counterfeits. For this reason, the signature signal is hidden in the frequency field to elude frequency signal processing proceedings such as compression, filtering, and adding noise because it is less detectable and more unlikely to be harmed or eradicated [10]. By vulnerable attacks, frequency-based watermarking is still susceptible to varieties of signal processing proceedings such as geometric distortions, cropping, or adding, thereby lowering the visibility of the embedded mark [24]. Therefore, the power and security of clear frequency-based watermarking against numerous attacks needed to be investigated to establish the finest frequency domain to conceal the sign and the greatest signal strength of the watermark between visibility and quality [25]. various Frequency-based watermarking techniques are presented in the visual domain applied to hide the watermark signal and the intensity of the signal in Fig. 1.

### 3.2 Utilized transforms

Essential transformation techniques used in digital media security and ownership verification are briefly introduced to provide insights into their operations and their role in enhancing the security of multimedia content, as follows:

1) Schur factorization watermarking is a type of digital watermarking technique utilized for embedding a watermark signal into the Schur factorization of a signal. The Schur factorization, a matrix decomposition technique, decomposes a square matrix into an upper-triangular matrix and its conjugate transpose. When applied to the image, the Schur Factorization, being a square matrix, is decomposed into two square matrices [26–28]. If we apply Schur to $n \times n$ matrix $A$, the result will be as follows:

**Fig. 1** The four most common frequency transforms in image watermarking


Original Media File
DCT Transform
SVD
Manipulate the media in the frequency domain to embed the watermark
DWT
DFT
Watermarked Media

$$Schur(A) = [J_A, K_A] \tag{1}$$

and,

$$Schure^{-1}(A) = J_A^* K_A^* J_A \tag{2}$$

where $J_A$ is a unitary orthogonal matrix, consisting of $n$ orthogonal eigenvectors of size $n \times 1$. We use the characteristic equation of $A$ to find these vectors, but if they are not orthogonal, we use the Gram-Schmidt process to convert them to orthogonal vectors. $K_A$, where the important properties of the image are stored, is found by:

$$K_A = J_A * AJ_A \tag{3}$$

and using $J_A$ obtained in the previous step. The advantage of Schur Matrix analysis of watermark images is to reduce the perturbation resulting from the embedding process in the original image, increasing imperceptibility [29].

Case study:

Given matrix:

$$A = \begin{bmatrix} 5 & 7 \\ -2 & -4 \end{bmatrix}$$

We aim to find $J_A$ which consists of two orthogonal eigenvectors of size $2 \times 1$. The characteristic equation of $A$ is the determinant of $(\beta I - A)$, where $I$ is the identity matrix and the Eigenvalues are the roots of the characteristic equation:$(\beta I - A)$

$$\det\left(\begin{bmatrix} \beta - 5 & -7 \\ 2 & \beta + 4 \end{bmatrix}\right) = \beta^2 - \beta - 6 = 0$$

Thus, $\beta_1 = -2$ and $\beta_2 = 3$ are the Eigen values of $A$.

To find the corresponding eigenvectors, we substitute the eigenvalues into $(\beta I - A)X = 0$:

For $\beta_1 = -2$,

$$\begin{bmatrix} -7 & -7 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

resulting in:

$$V_1 = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

For $\beta_2 = 3$,

$$\begin{bmatrix} -2 & -7 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

resulting in:

$$V_2 \begin{bmatrix} 7 \\ -2 \end{bmatrix}$$

However, $V_1$ and $V_2$ are not orthogonal. Using the Gram-Schmidt process, we obtain two orthogonal vectors $u_1$ and $u_2$:

$$u_1 = v_1 \tag{4}$$

$$u_2 = v_2 - \frac{v_2 \cdot u_1}{u_1 \cdot u_1} u_1 \tag{5}$$

Resulting in:

$$u_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix}$$

and

$$u_2 = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

Thus,

$$J_A = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$$

Now, using Eq. (3), $K_A = J_A^* A J_A$, where $J_A^*$ is the transpose of $J_A$ since the entries are real numbers,

$$K_A = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 5 & 7 \\ -2 & -4 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} -2 & 9 \\ 0 & 3 \end{bmatrix}$$

Using Eq. (1), Schure $(A) = [J_A, K_A]$,

$$Schure(A) = \left[ \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}, \begin{bmatrix} -2 & 9 \\ 0 & 3 \end{bmatrix} \right]$$

Using Eq. (2), Schure$^{-1}$ *(A).*
*JA * KA * JA*,

$$Schure^{-1}(A) = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} * \begin{bmatrix} -2 & 0 \\ 9 & 3 \end{bmatrix} * \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} -4 & -7 \\ 2 & 5 \end{bmatrix}$$

2) Discrete Cosine Transform (DCT): is a technique that involves embedding the watermark in the high-frequency DCT coefficient region of the multimedia content. Applying DCT to digital media divides it into three sections, each representing a different frequency: high, middle, and low-frequency coefficients [30]. The watermark is positioned in the middle-frequency coefficient to maximize its robustness in the original image and ensure that the embedding procedure has no impact on it [31]. The functionality of the DCT transform is as follows:

$$F(u,v) = \frac{4C(u)C(v)}{n^2} \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} f(j,k) \times cos(\frac{(2j+1)u\pi}{2n}) cos(\frac{(2k+1)v\pi}{2n})$$
$$F(j,v) = \sum_{u=0}^{n-1} \sum_{v=0}^{n-1} C(u)C(v)F(u,v) \times \cos(\frac{(2j+1)u\pi}{2n}) \cos(\frac{(2k+1)v\pi}{2n})$$

where,

- $F(u,v)$: Represents the Discrete Cosine Transform (DCT) coefficient at position $(u,v)$ in the frequency domain.
- $f(j,k)$: Represents the pixel value at position $(j,k)$ in the spatial domain.
- $C(u)$ and $C(v)$: Scaling functions, typically defined as:

$$C(u) = \begin{cases} \sqrt{\frac{1}{n}} & if\ u = 0 \\ \sqrt{\frac{2}{n}} & otherwise \end{cases}$$

- $n$: Represents the size of the image (assuming a square image of size $n \times n$).
- $\pi$: Represents the mathematical constant Pi, approximately equal to 3.14159.

For example, consider matrix $A$:

$$A = \begin{bmatrix} 139 & 144 & 150 & 159 & 159 & 161 & 162 & 162 \\ 144 & 151 & 155 & 161 & 160 & 161 & 162 & 162 \\ 149 & 153 & 160 & 162 & 161 & 161 & 161 & 161 \\ 153 & 156 & 163 & 160 & 162 & 161 & 162 & 161 \\ 155 & 159 & 158 & 160 & 162 & 150 & 165 & 163 \\ 155 & 156 & 156 & 159 & 155 & 157 & 157 & 158 \\ 155 & 156 & 156 & 159 & 155 & 157 & 157 & 158 \\ 155 & 156 & 156 & 159 & 155 & 157 & 157 & 158 \end{bmatrix}$$

When DCT is applied to matrix $A$, we note that the concentration of values in the resulting matrix is in specific places, unlike the original matrix. This idea helps in applications like watermarking and data compression.

$$DCT\ of\ A = \begin{bmatrix} 1260 & -23 & -11 & -7 & -1 & 2 & -1 & -3 \\ -1 & -17 & -9 & -2 & -1 & 0 & 0 & 2 \\ -12 & -6 & -2 & 0 & 1 & 2 & 0 & -4 \\ -5 & -3 & 2 & 1 & 2 & 0 & -1 & 2 \\ 2 & -3 & 0 & 1 & 0 & -1 & 0 & 2 \\ -2 & 0 & -1 & 0 & -1 & 1 & 2 & 1 \\ -3 & 0 & -1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & -1 & -1 & 0 \end{bmatrix}$$

3) Discrete wavelet transform (DWT)

DWT is commonly used in image watermarking, offering superior energy compression and enabling multiresolution of the watermarked media. Consequently, it ensures high robustness against various image processing attacks [32]. Image processing attacks encompass a range of operations, including but not limited to averaging, blurring, JPEG compression, sharpening, and focus enhancement [33]. DWT dissects the image into four frequency channels, namely, High High (HH), High Low (HL), Low High (LH), and Low Low (LL) frequency domains. Each frequency channel maintains a consistent bandwidth on the logarithmic scale during the DWT analysis of the image. In the initial DWT level, a 2D image is split into four resolutions, as discussed earlier in this section, labeled HH, HL, LH, and LL in the DWT domain, level 1.

The LH, HL, and HH subbands represent the finest scale wavelet coefficients, whereas the LL subband captures the coarse-level coefficients. Further decomposition of each subband can increase the number of levels. As previously mentioned, the primary objective of watermarking, in this case, is to achieve an imperceptible watermark, one that does not distort the original image. Therefore, the watermark is frequently embedded in the remaining three subbands, ensuring enhanced image quality and an imperceptible watermark, particularly within the low-frequency component. (i.e., the LL subband). Watermarking is often placed in one or more of the other three subbands to maintain superior image quality, as the human visual system is more sensitive to the LL subband (lower frequency component) [34]. A visual depiction of how DWT processes an image is illustrated in Figure 2.

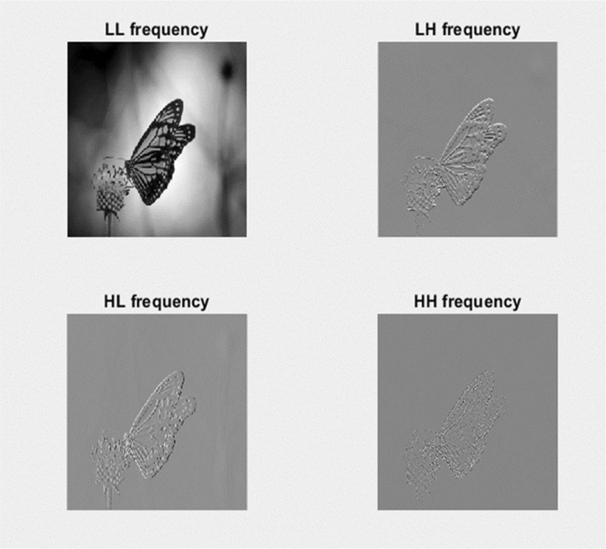


**Fig. 2** DWT sub frequencies on the cover image

## 4 Watermarking process

A set of experiments was carried out in this study to analyze the resilience of the proposed approach in watermarking against the salt and pepper attack. These experiments aimed to explore how the Schur matrix factorization performs under the influence of various salt and pepper noises, thereby determining its strength and weakness in recovering watermarks. Given the nature of the salt and pepper attack, which disrupts the integrity property of watermarked data, this research aims to understand the threat risk posed by this intrusion and propose various ways to strengthen the general resilience of the watermarking integrity.

Our proposed method introduces a robust two-stage digital watermarking model designed to integrate seamlessly within the domain of image watermarking. In the initial stage, the watermark embedding schema takes an original image through a series of transformations including Discrete Wavelet Transform and Schur Factorization, culminating in the generation of a watermarked image. This is complemented by the second stage, which meticulously outlines the watermark extraction schema, utilizing the watermarked image to retrieve the embedded watermark through inverse processing steps. Figure 3 illustrates this sophisticated approach.

### 4.1 Embedding *schema*

This part of the experimentation involved systematically investigating and implementing various embedding schemas to incorporate imperceptible watermarks within digital media. The designs and application enable different schemas of embedding to be applied to produce watermarked images or audiovisuals. The focus of every experiment was on establishing embedding techniques that do not tamper with host data but, at the same time, expose the watermark by counteractions of various levels. The strength and ability

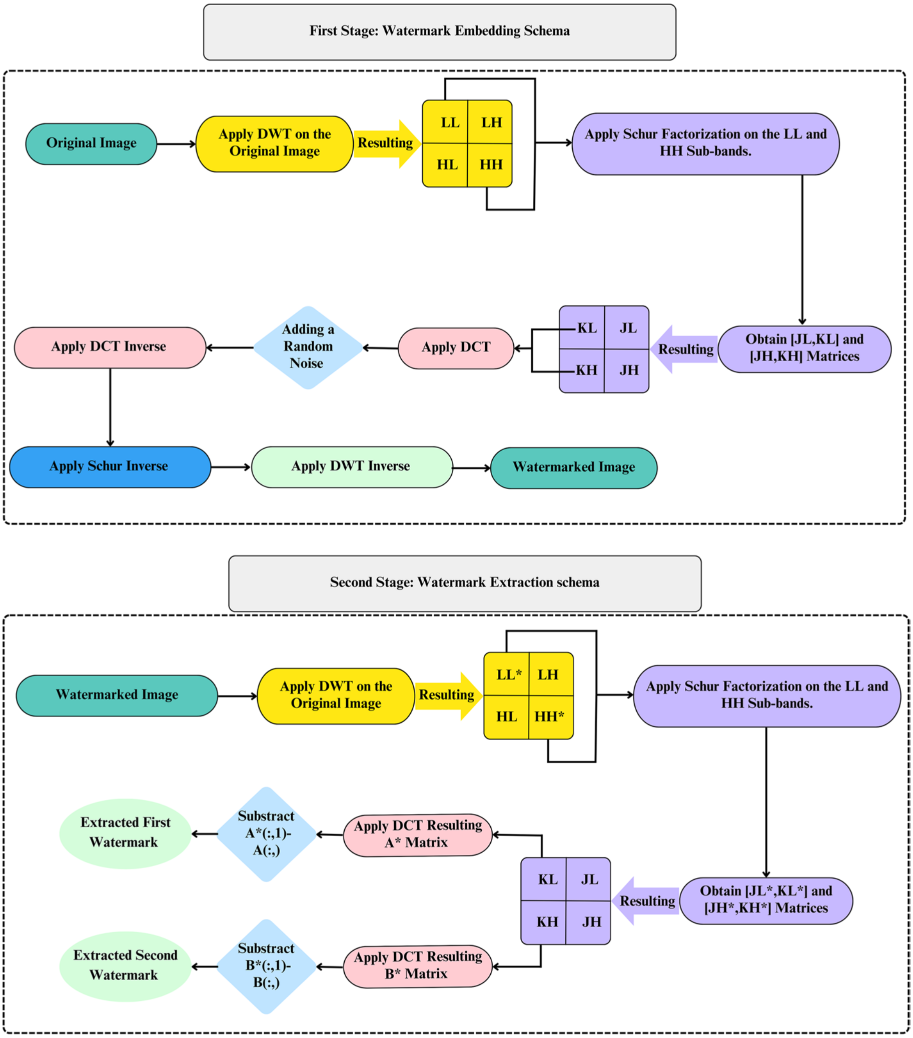

First Stage: Watermark Embedding Schema
Original Image
Apply DWT on the Original Image
Resulting
LL
LH
HL
HH
Apply Schur Factorization on the LL and HH Sub-bands.
Obtain [JL,KL] and [JH,KH] Matrices
Resulting
KL
JL
KH
JH
Apply DCT
Adding a Random Noise
Apply DCT Inverse
Apply Schur Inverse
Apply DWT Inverse
Watermarked Image
Second Stage: Watermark Extraction schema
Watermarked Image
Apply DWT on the Original Image
Resulting
LL*
LH
HL
HH*
Apply Schur Factorization on the LL and HH Sub-bands.
Obtain [JL*,KL*] and [JH*,KH*] Matrices
Resulting
KL
JL
KH
JH
Apply DCT Resulting A* Matrix
Substract A*(:,1)-A(:,)
Extracted First Watermark
Apply DCT Resulting B* Matrix
Substract B*(:,1)-B(:,)
Extracted Second Watermark

**Fig. 3** Research framework

to survive attacks were assessed for each schema, processes closely uncharged because salt and pepper threaten the watermarking process.

In digital watermarking, deciding where to embed the watermark and how strong it should be, are critical decisions. The embedding place refers to the locations within the cover image where the watermark is inserted, while the embedding strength determines the intensity or perceptibility of the watermark within those locations. These regions are typically chosen strategically to ensure robustness, imperceptibility, and resistance to attacks. The procedural activities carried out in Algorithm 1 include:

The embedding place in Algorithm 1 is determined by the matrices $A$ and $B$, which are obtained after applying the DCT to certain components of the cover image. The first column of these matrices is targeted for modification to embed the watermark. The choice of the first column for embedding is often based on its susceptibility to

**Algorithm 1** Optimized Digital Watermarking

```
Input: coverImage, x
Compute DWT on coverImage yielding (LL, LH, HL, HH);
Apply Schur factorization on LL and HH to obtain [$J_L$,$K_L$] and [$J_H$,$K_H$];
Compute DCT on $K_L$ and $K_H$ to get matrices A and B;
foreach element i in A and B do
    if i is in A then
        $\alpha = 1$;
    else
        $\alpha = 20$;
    Modify the first column of A and B as $A(i,:) = A(i,:) + x(i) \times \alpha$ and $B(i,:) = B(i,:) + x(i) \times \alpha$;
    Compute DCT inverse on A and B to get $K_L^*$ and $K_{H^*}$;
Compute Schur inverse to get
        $LL^* = J_L \times K_L^* \times J_L^T$ and
        $HH_* = J_H \times K_{H*} \times J_{HT}$;
watermarkedImage is DWT inverse of (LL*, LH, HL, HH*);
Return watermarkedImage;
Output: watermarkedImage.
```

modifications while preserving image quality. By modifying this column, the watermark can be effectively inserted without significantly altering the visual appearance of the cover image.

Regarding the embedding strength, it refers to the degree or intensity of the modification applied to the embedding place for watermark insertion. It determines how perceptible the watermark will be in the watermarked image. In the provided algorithm (Algorithm 1), the embedding strength is controlled by the parameter $\alpha$, which is multiplied by the values of $x(i)$. The value of α$\alpha$ determines the magnitude of the modification applied to the first column of matrices $A$ and $B$. The choice of embedding strength depends on various factors, including the desired level of watermark robustness, the sensitivity of the application, and the acceptable level of distortion in the watermarked image. Higher values of α result in stronger watermark embedding but may increase the risk of perceptibility or degradation of image quality.

By carefully selecting the embedding place and adjusting the embedding strength, Algorithm 1 aims to effectively embed the watermark into the cover image while minimizing perceptual distortion and maintaining robustness against attacks. These considerations are crucial for ensuring the effectiveness and integrity of the watermarking process. The step-by-step procedure for embedding the watermark into an image is depicted in Fig. 4.

The integration of the watermark in the proposed schema remains invisible. The implementation of the DWT served to embed the watermark across multiple frequencies, thereby ensuring a robust defense against various types of attacks. Specifically, the selection of the HH frequency was intended to counter assaults such as histogram manipulations and noise addition. On the other hand, the selection of the LL frequency was aimed at mitigating attacks characterized by low-frequency traits, such as filtering. During the watermark extraction process, a comparison will be conducted between the extracted watermark and the original watermark using the mean squared error (MSE). Additionally,

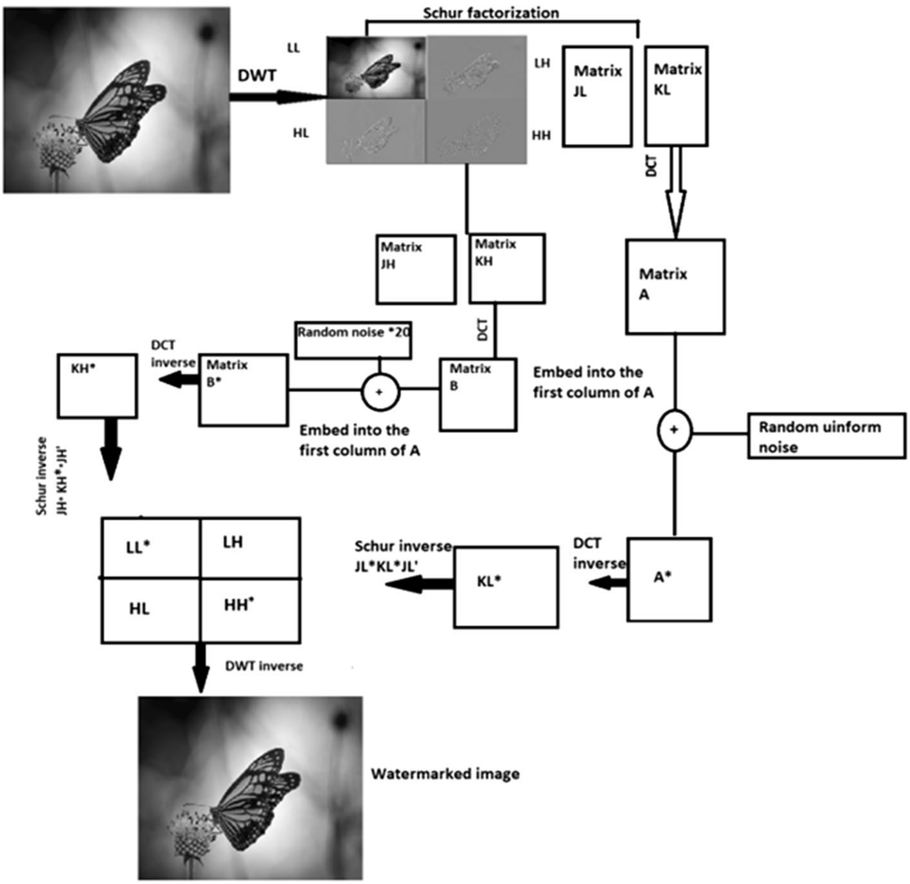


**Fig. 4** Watermark embedding schema

this extracted watermark will be compared with a collection of one thousand randomly generated vectors for further validation of the methodology's effectiveness.

### 4.2 Watermark extraction

The watermark extraction stage involved developing and using sophisticated algorithms to extract embedded watermarks from the media samples that are salt-and-pepper attacked. As aforementioned, the indicator employed applied signals out of image processing and image testing to analyze the signal; it intended to determine whether the extraction process is robust and accurate in the presence of noise and various degrees of data corruption. The fundamental question is whether the extraction algorithms are efficient in retrieving the embedded information correctly and reliably even when challenged by severe distortion caused by a salt-and-pepper attack. To extract the watermark, it is imperative to provide both the original image and the corresponding watermarked sample. The extraction process in Algorithm 2 includes:

**Algorithm 2** Watermark Extraction Process

```
Input: originalImage, watermarkedImage
Apply DWT on both originalImage and watermarkedImage;
Apply Schur matrix factorization on LL, HH of originalImage and $LL^*$ and $HH^*$ of watermarkedImage to obtain $[J_L,K_L]$, $[J_H,K_H]$, $[J^*_L, K^*_L]$, $[J^*_H, K^*_H]$;
Compute DCT on $K_L$ , $K_H$ , $K_{L^*}$, $K^*_H$ to get matrices A, B, $A^*$, $B^*$;
Calculate the watermark using:
    extracted L = $A^*(:,1) - A(:,1)$
    extracted H = $B^*(:,1) - B(:,1)$
Return extracted L, extracted H;
Output: extracted L, extracted H
```

Algorithm 2 outlines the process for extracting a watermark from a watermarked image, given the original image and the watermarked version. The algorithm begins by applying DWT to both the original image and the watermarked image. This transform decomposes the images into four components: LL (approximation), LH (horizontal detail), HL (vertical detail), and HH (diagonal detail). Next, the Schur matrix factorization is applied to the LL and HH components of both the original and watermarked images. This process yields matrices [JL, KL] for the original LL and HH, and matrices [JL*, KL*] for the watermarked LL* and HH*. DCT is then computed on the matrices KL and KL* to obtain matrices A and A*, and on matrices KH and KH* to obtain matrices B and B*. These DCT transformations are applied to extract features or characteristics of interest from the LL and HH components. The extracted watermark is calculated based on the difference between specific columns of matrices A*, A, B*, and B. The extracted watermark for the LL component is obtained by subtracting the first column of matrix A from the first column of matrix A*. Similarly, the extracted watermark for the HH component is calculated by subtracting the first column of matrix B from the first column of matrix B*. Finally, the extracted watermark components (extracted L and extracted H) are returned as the output of the algorithm.

In Fig. 5, a comprehensive schematic depiction is presented, detailing the sequential stages involved in the extraction of the watermark from the image. This process necessitates the availability of both the original image and its watermarked counterpart.

## 4.3 Dataset

We assessed our digital watermarking method using images converted to grayscale from the "Watermarked / Not Watermarked Images" dataset available on Kaggle [38]. This dataset, containing a mix of JPG and JPEG images, provides a realistic basis for testing the durability and inconspicuousness of watermarking across diverse content. After converting the images to grayscale, our proposed watermarking technique was applied, followed by subjecting them to various image processing attacks (histogram equalization, salt and pepper noise, ripple, smoothing, and cropping) to evaluate the robustness of the watermark. The use of a publicly accessible dataset ensures that our

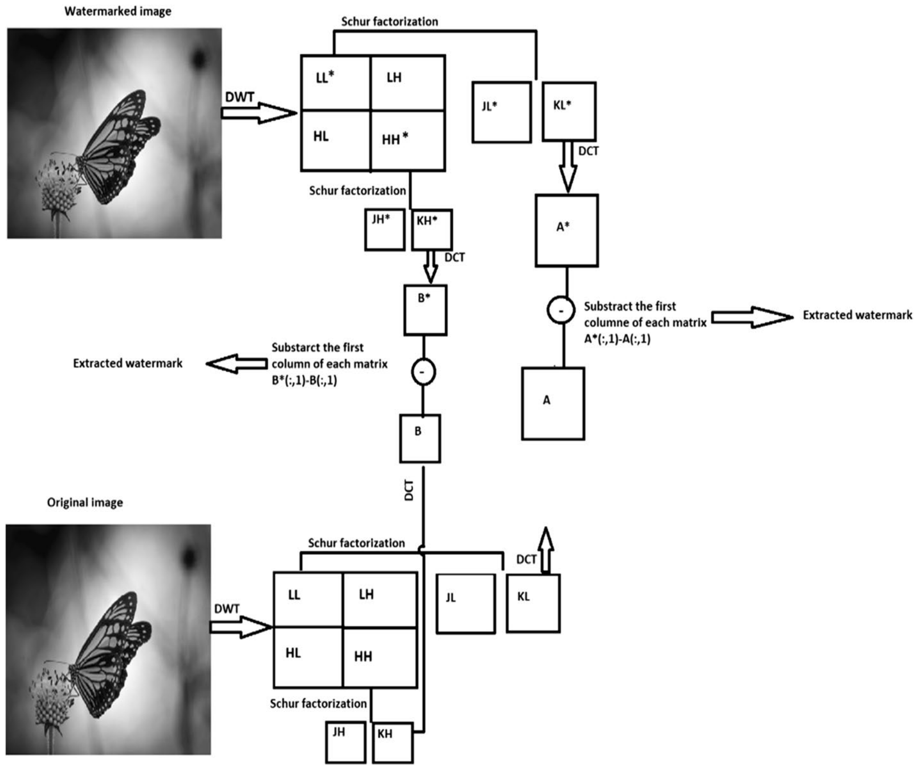


**Fig. 5** Watermark extraction schema

experimental results are transparent and can be independently verified and replicated by peers in the field of digital media security [42, 43].

## 5 Experimental results and analysis

In this section, we present the results of embedding the watermark, and apply different attacks to evaluate how robust it is. The simulations and experiments presented in this study were conducted using MATLAB 2023, a high-level language and interactive environment suitable for algorithm development, data visualization, data analysis, and numerical computation. MATLAB was chosen for its robust set of built-in functions and the ability to handle matrix operations and data visualization efficiently. This environment facilitated the implementation of the Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Schur matrix factorization, which are central to the proposed digital watermarking algorithm. As it can be clearly seen from Fig. 6, the watermark is completely invisible.

To get a better understanding of the effect of the watermark signal weight on the image, Figs. 7 and 8 represent the PSNR for various weights in both the HH and the LL frequency domain of the DWT transform, it can be seen that the PSNR value changes as the weight change.

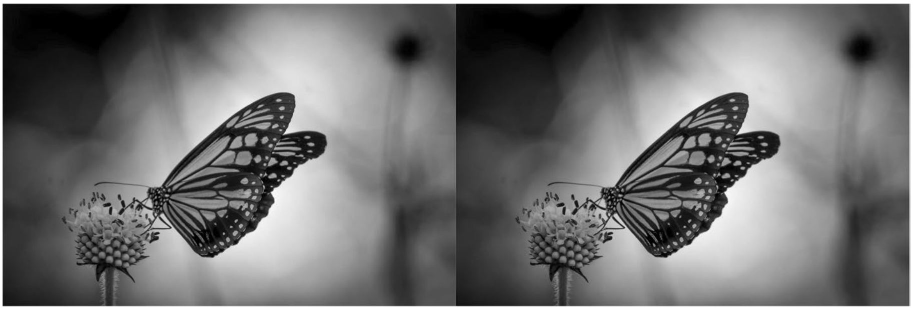


**Fig. 6** Original image and watermarked image

**Fig. 7** Peak signal to noise ratio for different noise weights in LL

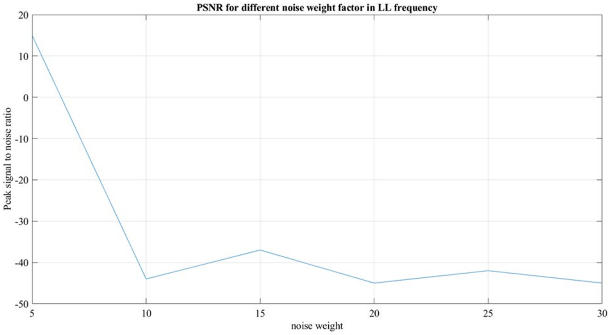


**Fig. 8** Peak signal to noise ratio for different noise weight in HH

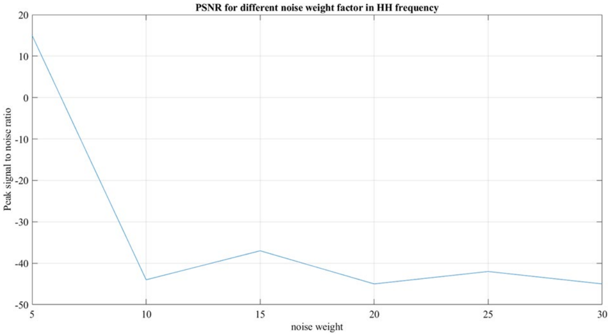


Figure 9 represent the mean squared error between 1 thousand random vectors and the two embedded ones, the mean squared error value is what we will be depending on to decide if the watermarking schema was successful or not, it can be clearly seen from Fig. 9 that the two embedded signals have a mean squared error that is far less than the other random ones, thus we can assume that it the one we embedded.

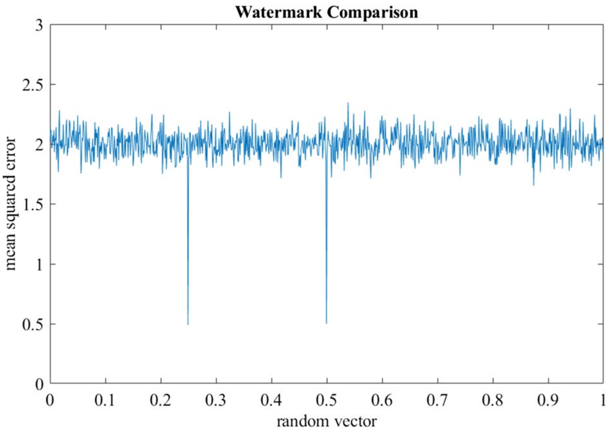


**Fig. 9** Histogram equalization attack and the extracted watermark

## 5.1 Histogram equalization attack

Histogram equalization sets the intensity values of pixels in the input image so that the intensity distribution in the output picture is uniform, in other words, the picture's lighting is modified to be more uniform by redistributing across the whole available range that is usually around 256 Gy scale levels [35, 39]. Figure 10 shows how histogram equalization affects the image. It increases contrast and produces a more consistent histogram. This approach may be used to a whole image or only a portion of an image.

We can clearly see that the histogram attack was implemented to a high degree. Still, the watermark extracted has a much smaller error than all the other randomly generated ones, meaning the extraction was successful.

The attack parameters were as follows:

1. Image size = 512,512 pixels.
2. Image format is jpg.
3. Number of energy buns for attack: 64.
4. Average CPU runtime per image of the dataset: 0.3 s.

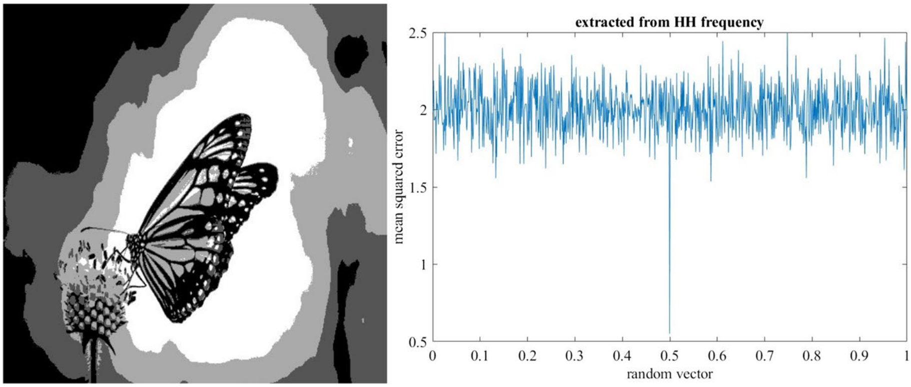


**Fig. 10** Histogram equalization attack and the extracted watermark

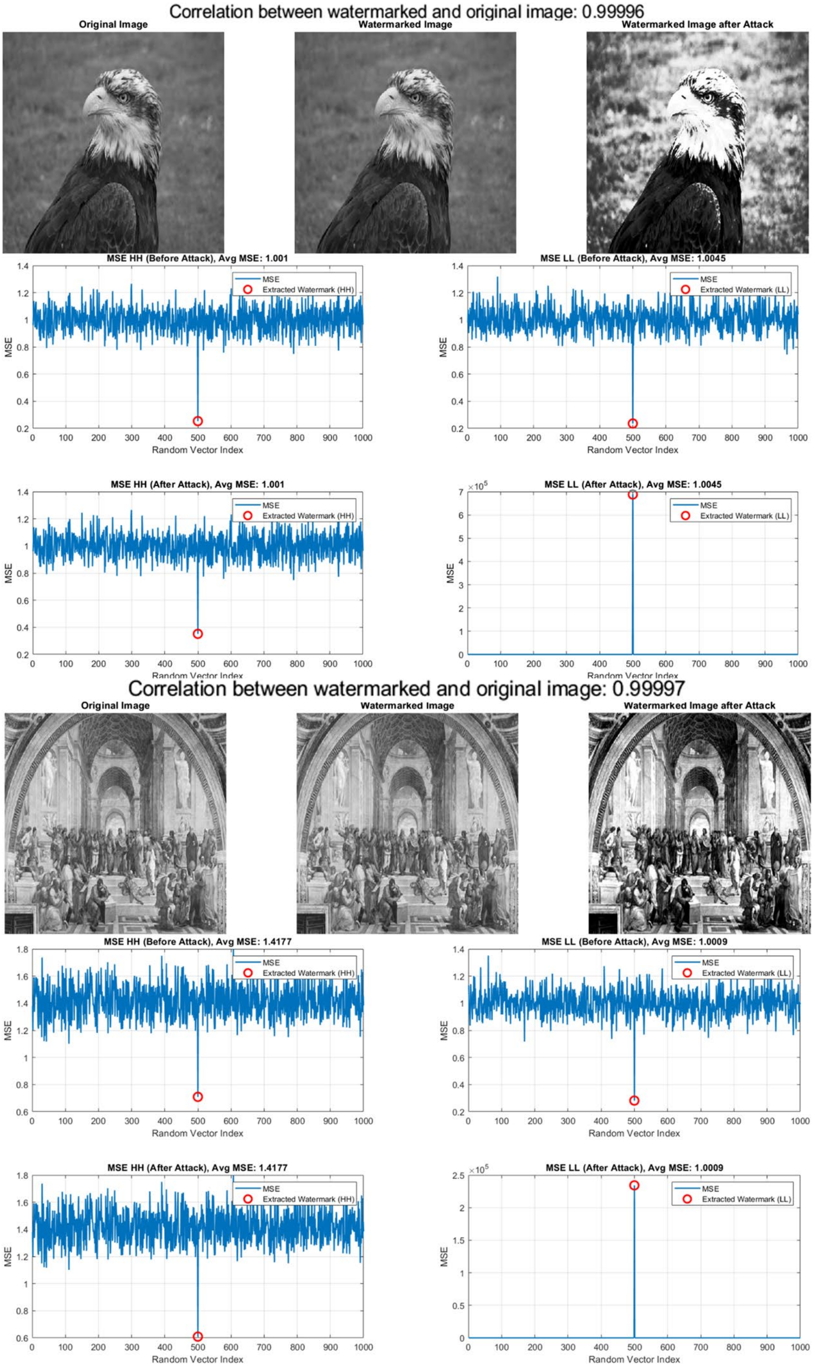


**Fig. 11** Comparative MSE Analysis of Embedded Watermarks in Different Image Domains Subject under Histogram Equalization Attack

Figure 11 proposed digital watermarking method exhibits high imperceptibility and resilience to histogram equalization attacks. The correlation between the watermarked and the original images remains exceptionally high, with a coefficient of 0.999998, indicating the watermark's invisibility in the visual spectrum. This is essential for ensuring that the quality of the image for viewers is not compromised. The Mean Squared Error (MSE) graphs for the high-frequency (HH) and low-frequency (LL) domains, both before and after the attack, show a negligible change in values, underscoring the robustness of the watermark. The red circles pinpoint the extracted watermark, which stands out distinctly with a considerably lower MSE compared to the sea of random vectors, confirming the effectiveness of the watermark extraction even after the histogram equalization attack.

Figure 12 shows that the results are consistent with the previous findings, demonstrating the watermarking method's effectiveness across different content types. The correlation coefficients for both the HH and LL domains remain above 0.999996 after the attack, signifying the watermark's stability.

## 5.2 Salt and pepper attack

Salt and pepper is a sparsely occurring white and black pixels spread out through the image [36, 40, 41]. Hence the name white pixels will have the value of 255 and 0 for the black ones. Figure 13 displays the salt and pepper attack and the extracted watermark. The watermark is extracted successfully after the salt and pepper attack; as expected, embedding in the high-frequency component survived the salt and pepper attack with a mean squared error that is significantly lower than the error associated with randomly generated noises.

The attack parameters were as follows:

1. Image size = 512,512 pixels.
2. Image format is jpg.
3. Attack intensity: 0.01 noise level.
4. Average CPU runtime per image of the dataset: 0.3 s.

The results depicted in Figs. 14 and 15 demonstrate the watermarking algorithm's robust defense against the salt and pepper attack. High correlation coefficients (0.999998 and 0.999999) between the original and watermarked images indicate the watermark's invisibility, a critical aspect of the watermark's imperceptibility and an unaltered visual quality. The MSE plots for the HH and LL domains show the watermark's endurance, with the extracted watermark's MSE values remaining notably lower than the average MSE, both before and after the salt and pepper attack. This consistent low MSE of the watermark across different images and the watermark's detectability even after the attack illustrate the method's effective resilience and the watermark's capacity to serve as a reliable tool for asserting ownership rights in digital media.

## 5.3 Ripple attack

As can be seen in Fig. 16, the ripple effect is like the waves we get when interacting with a surface of water; it looks like the waves spreading through it.

When applying the ripple attack the watermark also was extracted with a significantly low error compared to all other randomly generated watermarks, yielding in a successful extraction.

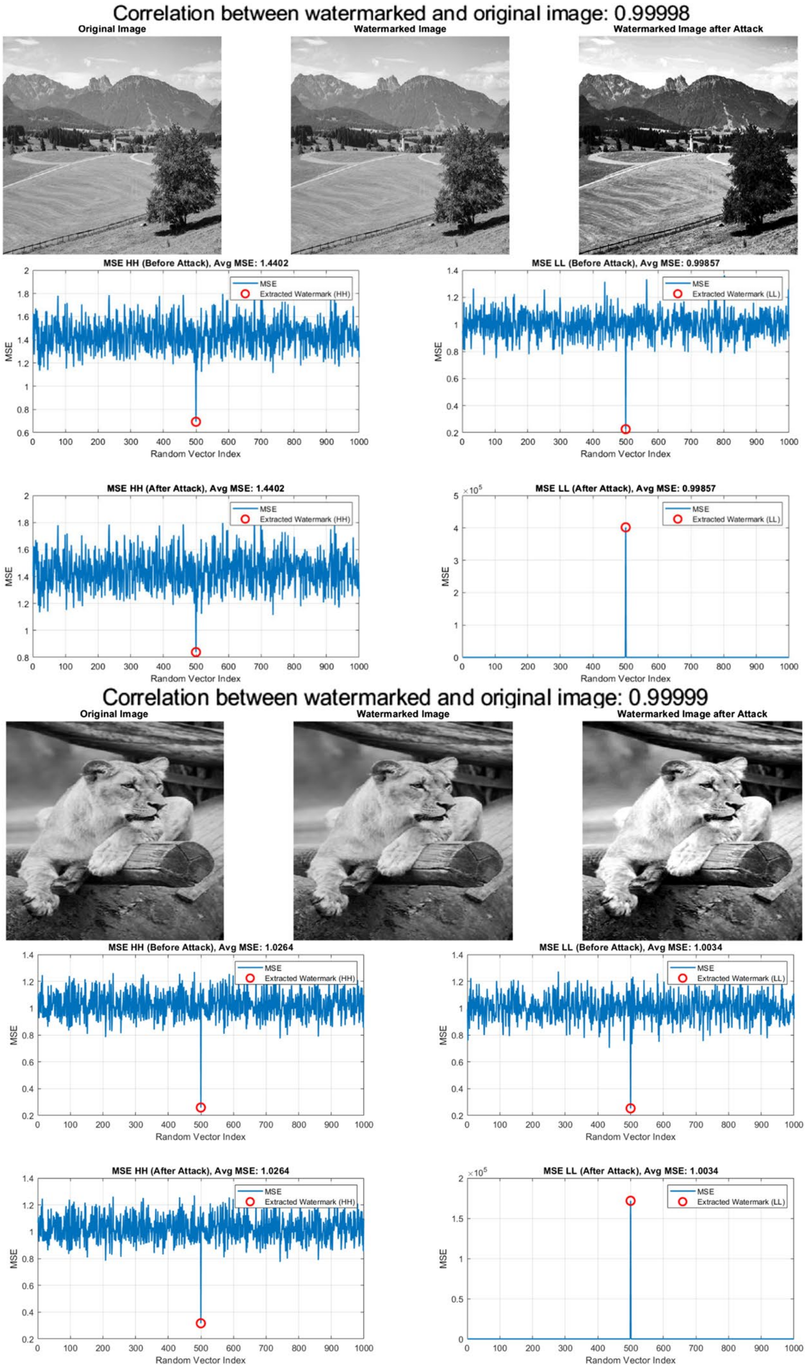


**Fig. 12** Continue Comparative MSE Analysis of Embedded Watermarks in Different Image Domains Subject under Histogram Equalization Attack

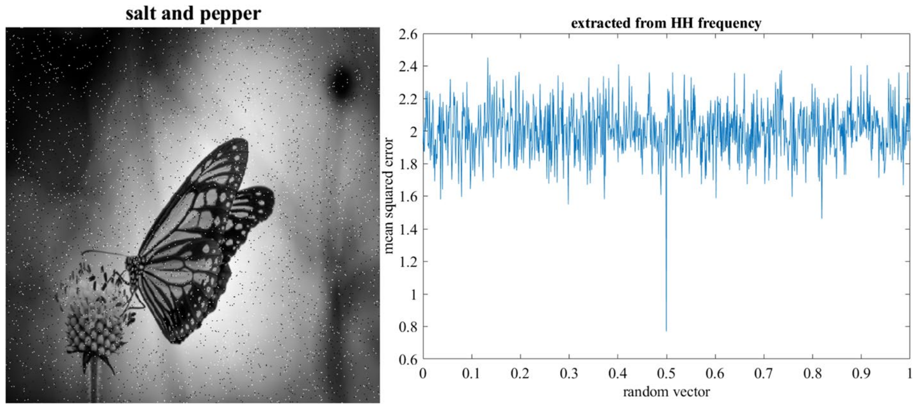


**Fig. 13** Salt and pepper attack and the extracted watermark

The attack parameters were as follows:

1. Image size = 512,512 pixels.
2. Image format is jpg.
3. Attack frequency: 0.5.
4. Attack amplitude: 10.
5. Average CPU runtime per image of the dataset: 0.3 s.

Figures 17 and 18 present the resilience of the digital watermarking scheme under ripple attacks, maintaining high correlation coefficients (0.999998 and 0.999996 respectively) that signify the watermark's imperceptibility post-attack. The MSE plots demonstrate the watermark's robustness; despite the undulating distortions characteristic of the ripple effect, the extracted watermark's MSE values remain distinctively lower than those of random vectors, confirming successful retrieval. This consistent performance across different image types be it natural landscapes, wildlife, or intricate artworks highlights the method's versatility and robust capacity to withstand ripple distortions while preserving the integrity of the watermark for reliable ownership verification.

### 5.4 Smoothing attack

Smoothing attack takes a block of pixels and averages them out; some of its uses include the beauty filters in some applications, as can be seen in Fig. 19; the watermark was successfully extracted, comparing its mean squared error to the randomly generated watermarks, the watermark was extracted from the LL frequency.

The attack parameters were as follows:

1. Image size 512,512
2. Image format: JPG
3. Standard deviation of Gaussian filter = 3
4. Average CPU runtime = 0.29 s

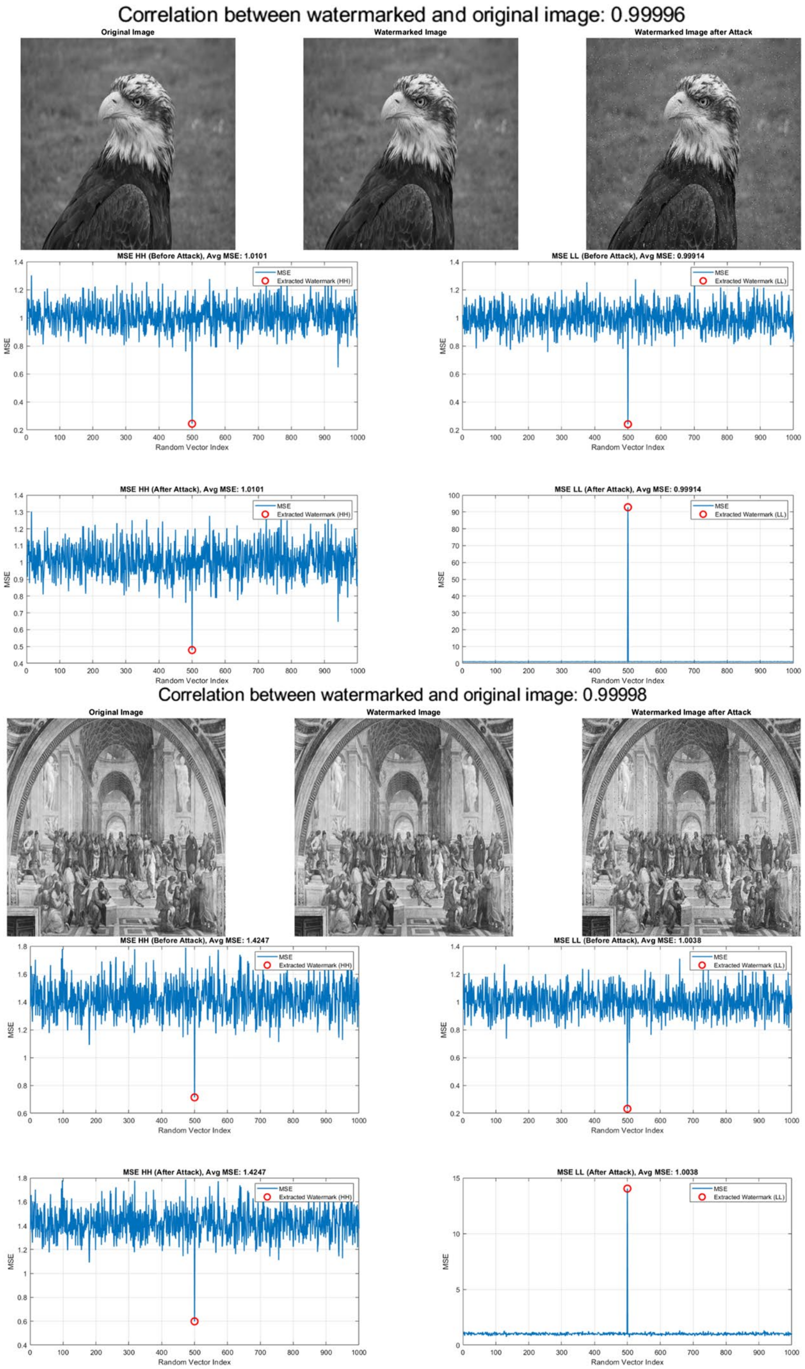


**Fig. 14** Comparative MSE Analysis of Embedded Watermarks in Different Image Domains Subject under Salt and Pepper Attack

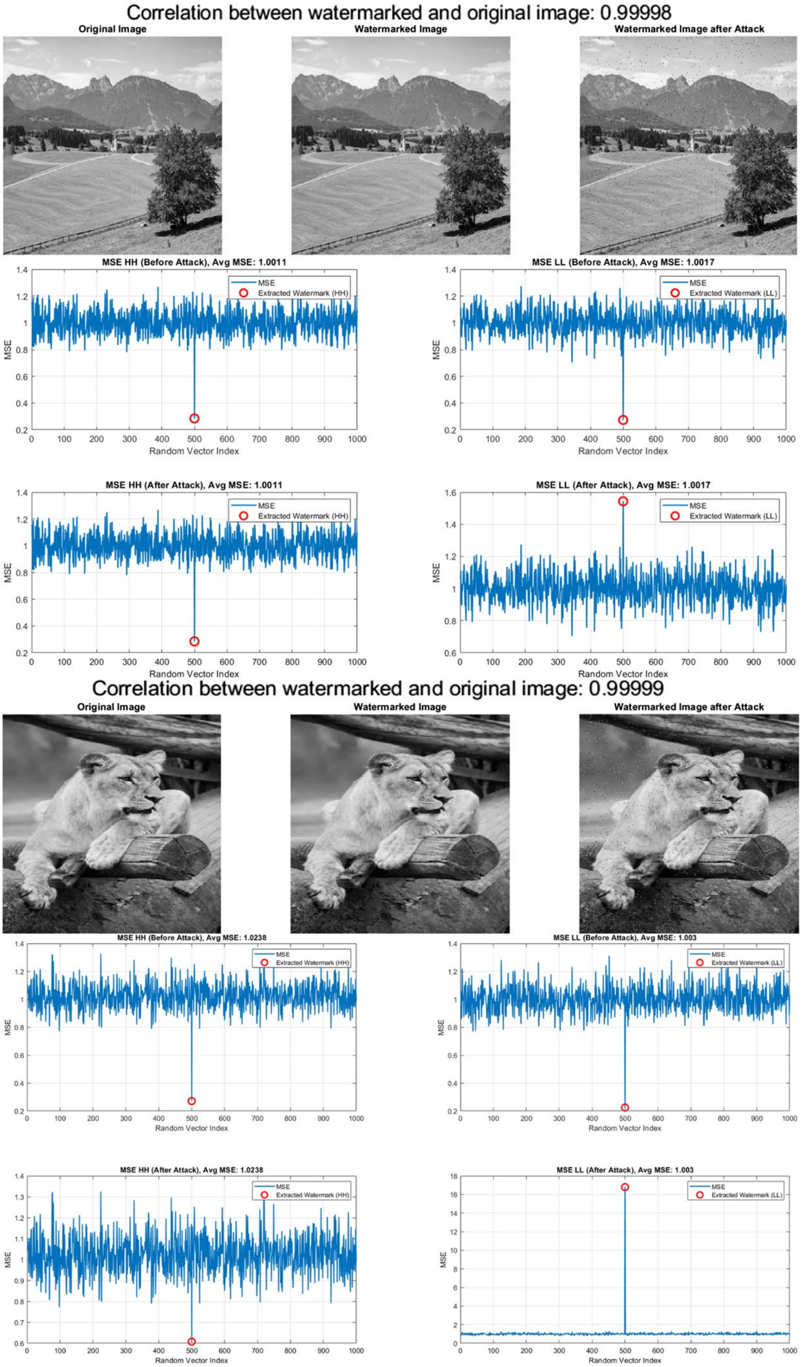


**Fig. 15** Continue Comparative MSE Analysis of Embedded Watermarks in Different Image Domains Subject under Salt and Pepper Attack

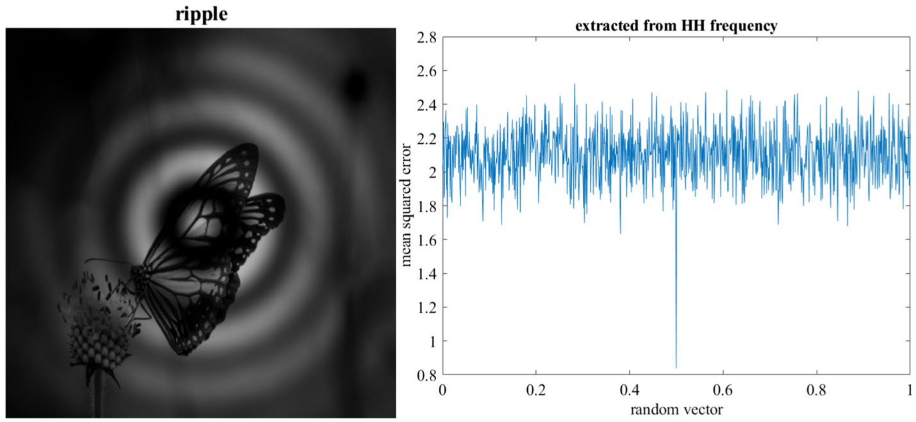


**Fig. 16** Ripple attack and the extracted watermark

Figures 20 and 21 illustrate the digital watermark's integrity in the face of smoothing attacks. Despite the smoothing process designed to blur and reduce image detail, the correlation between the original and watermarked images remains exceedingly high, at 0.999998 and 0.999995, respectively, signifying the watermark's stealthiness and the negligible impact on the image's visual fidelity. The Mean Squared Error (MSE) values for the high-frequency (HH) and low-frequency (LL) components before and after the attack exhibit only slight fluctuations, indicating the watermark's tenacity. Particularly noteworthy is the watermark's detectability post-attack, with its MSE staying distinctively below the surrounding random vectors' average MSE, reinforcing the technique's capability to withstand smoothing a common image processing operation while ensuring reliable extraction and verification of digital ownership.

## 5.5 Cropping attack

When cropping 50% of the picture we were successfully able to extract the watermark having mean square error significantly lower than the randomly generated vectors, cropping is done by replacing 50% of the watermarked image pixels with zeros, in this case we replaced the bottom 50% of the pixels with the value zero, resulting in a black bottom half of the image. Comparing the value of the mean squared error correlated to the extracted watermark against the 1000 randomly generated vectors, we notice a significantly lower error, meaning the watermark was successfully extracted, Fig. 22 depicts the cropping attack and the mean squared error of the extracted watermark.

In each of the aforementioned attack scenarios, the successful extraction of the watermark remains feasible. Nonetheless, the utilization of random noises inevitably introduces some degree of disparity between the extracted watermark and its original form. In the study of [37] about seminal work on watermarking techniques, the researchers emphasized this imperfection in the extraction process, especially in the context of utilizing random noise for watermarking images. The pivotal criterion for assessment lies in the comparison of the mean squared error between the original watermark and the error in the extracted watermark. When the error in the extracted watermark falls significantly below that of

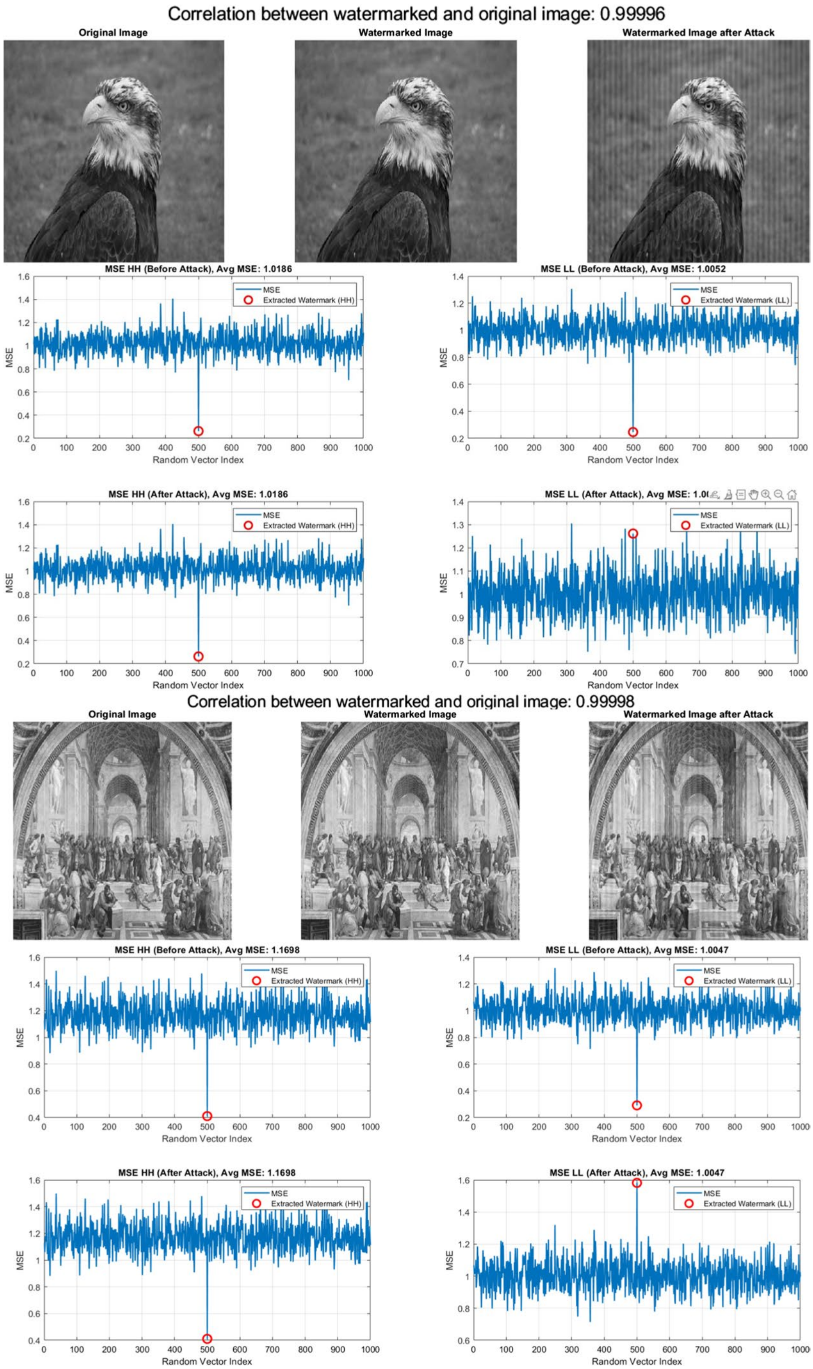


**Fig. 17** Comparative MSE Analysis of Embedded Watermarks in Different Image Domains Subject under Ripple Attack

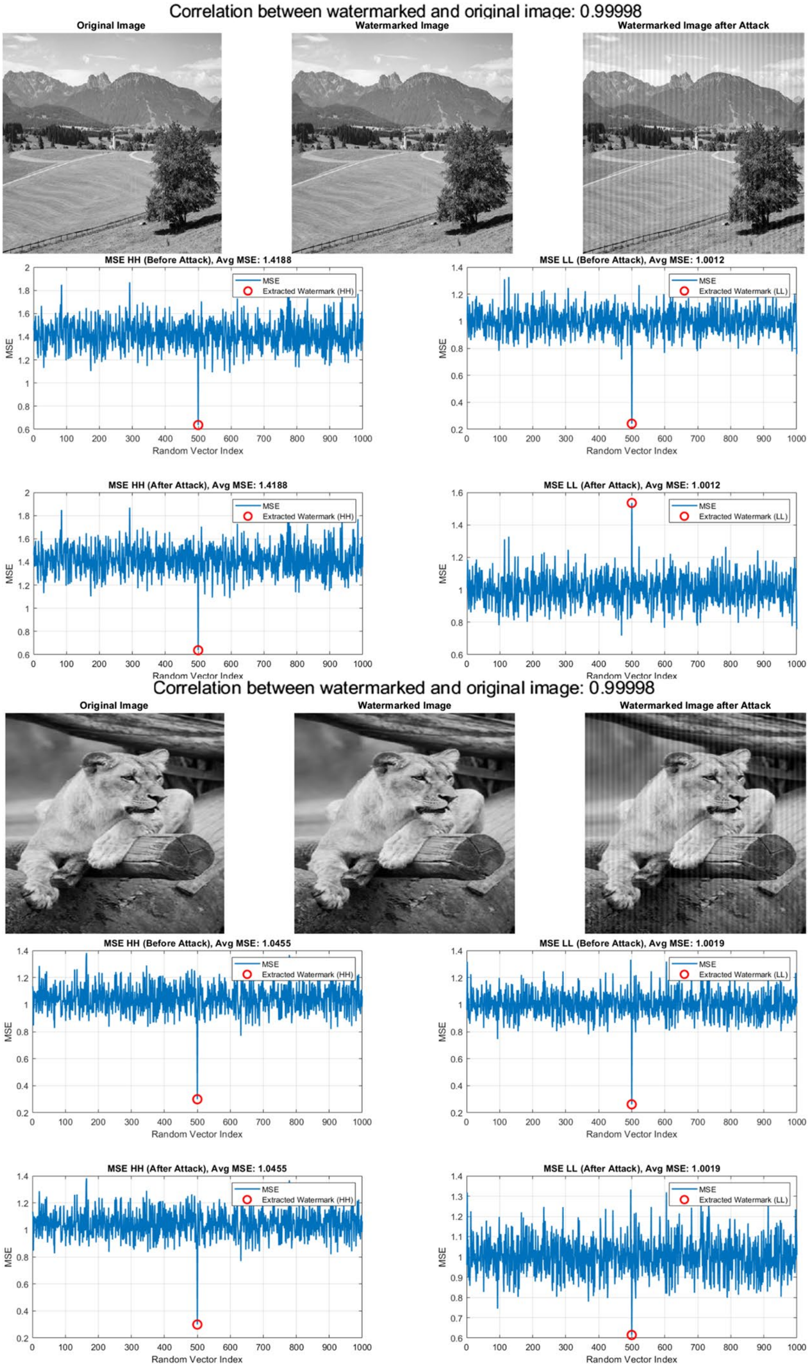


**Fig. 18** Continue Comparative MSE Analysis of Embedded Watermarks in Different Image Domains Subject under Salt and Ripple Attack

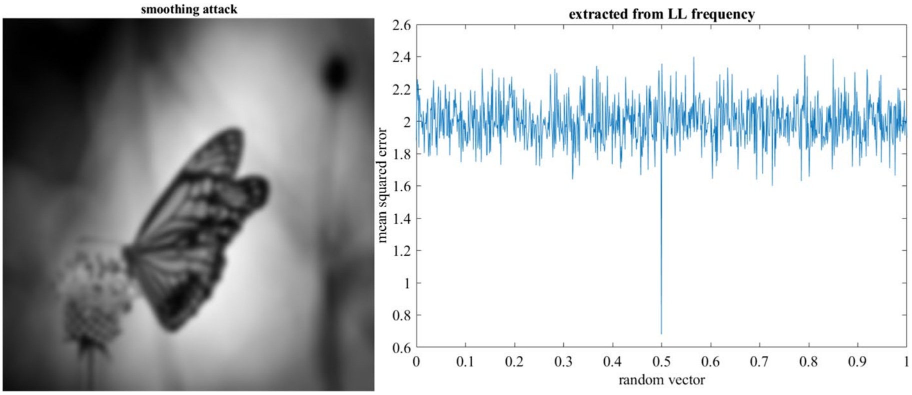


**Fig. 19** Smoothing attack and the extracted watermark

1000 randomly generated vectors, it is deemed as a successful match, affirming the accomplishment of the extraction process.

The attack parameters were as follows:

1. Image size = 512,512 pixels.
2. Image format is jpg.
3. Cropping the bottom half of the image.
4. Average CPU runtime per image of the dataset: 0.2 s.

The outcomes displayed in Figs. 23 and 24 exhibit the efficacy of the watermarking method when subjected to cropping attacks, with correlation values of 0.999998 and 0.999999, signifying the watermark's imperceptibility in both intact and cropped images. Despite the severe modification that cropping represents, the watermark endures with its detectability barely impacted, as evidenced by the low MSE of the extracted watermark, distinguishably lesser than the average MSE in both the high-frequency (HH) and low-frequency (LL) areas. The stability of these values before and after the attack demonstrates the watermark's resilience and the robustness of the watermarking technique, ensuring the digital watermark remains a viable and reliable tool for ownership verification even when substantial portions of the media are removed.

Table 1 presents average run times for different types of attacks applied to images as part of testing the robustness of a watermarking system. The histogram equalization and salt and pepper attacks both have an average processing time of 0.3 s per image, which indicates these attacks are not only common but also can be executed quickly, potentially allowing for rapid testing of watermark resilience. The ripple and smoothing attacks have slightly lower average run times, at 0.28 and 0.29 s respectively, suggesting that these attacks, while slightly less computationally intensive, are also executed efficiently. The cropping attack stands out with a higher average run time of 0.6 s per image, which is double the time of the other attacks. This could be due to the additional computational steps required to modify the image size and content.

The efficiency of our proposed digital watermarking algorithm was rigorously evaluated by measuring the execution time for each type of digital attack simulation on a dataset of 100 images. The average processing times are as follows: Histogram Equalization and

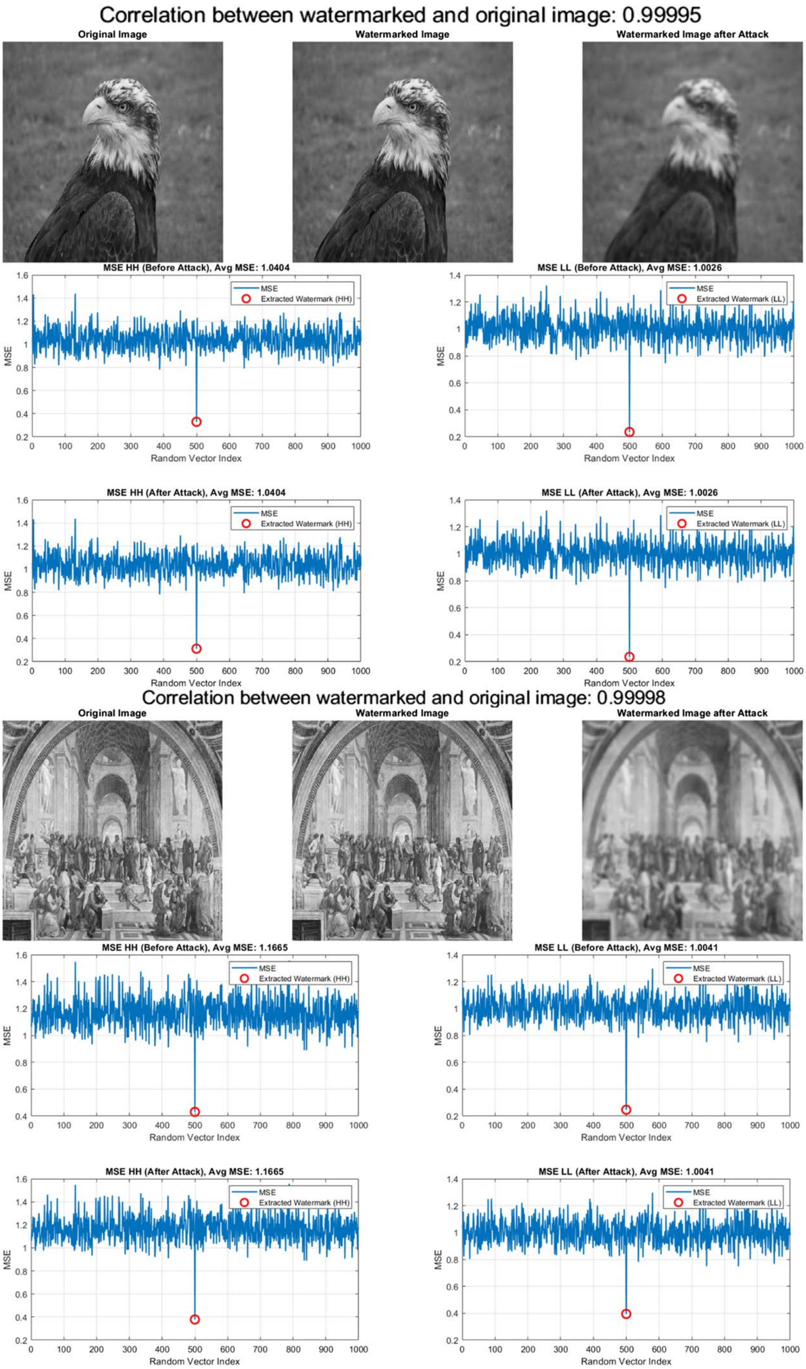


**Fig. 20** Comparative MSE Analysis of Embedded Watermarks in Different Image Domains Subject Smoothing Attack

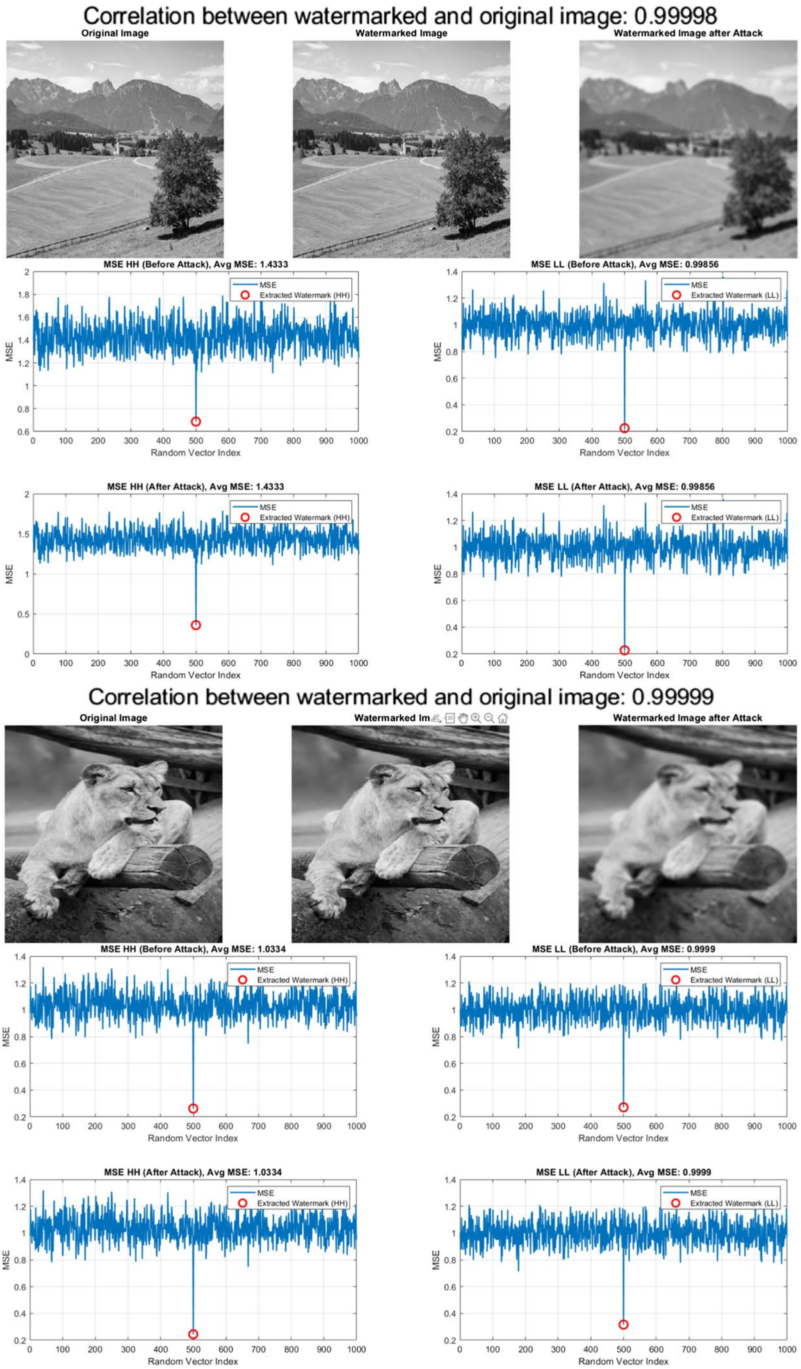


**Fig. 21** Continue Comparative MSE Analysis of Embedded Watermarks in Different Image Domains Subject under Smoothing Attack

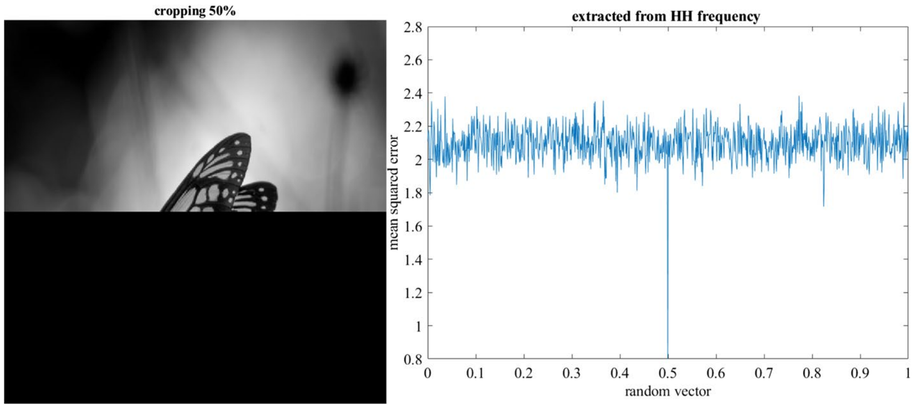


**Fig. 22** Cropping 50% attack and the extracted watermark

Salt and Pepper attacks each took 0.3 s, Ripple Attack required 0.28 s, Smoothing Attack was completed in 0.29 s, and the Cropping Attack took 0.6 s. These metrics were obtained under consistent hardware conditions, indicative of the algorithm's performance relative to typical operational standards. The implications of these results underscore the algorithm's suitability for real-time applications and scenarios demanding rapid image processing, such as media streaming, content management, and automated digital archiving. Considering the favorable performance, especially under computationally intensive conditions like the Cropping Attack, our algorithm shows promise for widespread adoption and scalability.

### 5.6 Comparison with previous work

Salt and pepper noise, characterized by random extreme pixel values in images, poses challenges for Schur decomposition, a powerful technique sensitive to such extremes. This noise disrupts the original image structure, impacting the accuracy of the decomposition process and resulting in significant deviations from the noise-free version. Consequently, watermark extraction methods relying on Schur decomposition may encounter reduced robustness, as the altered matrix affects the reliability of watermark extraction, especially in the presence of noise. Balancing robustness and invisibility becomes challenging, requiring careful consideration of trade-offs in designing watermarking schemes that perform well under various attacks, including salt and pepper noise. Recent studies in the domain of digital watermarking, such as those by [44] and [45], have made significant strides in improving imperceptibility and computational efficiency. However, they present limitations such as low robustness to salt and pepper noise and the requirement for square matrices, which complicate their application in diverse scenarios. In [46], LWT-Schur Decomposition demonstrates strong robustness against various attacks but falls short when faced with histogram equalization and cropping attacks. The technique presented in [47] has also contributed to the field of Schur Decomposition Watermarking, offering blind extraction and fewer computations than SVD, though their method shows reduced robustness to significant cropping attacks. Table 2 presents the comparison of our work with related works.

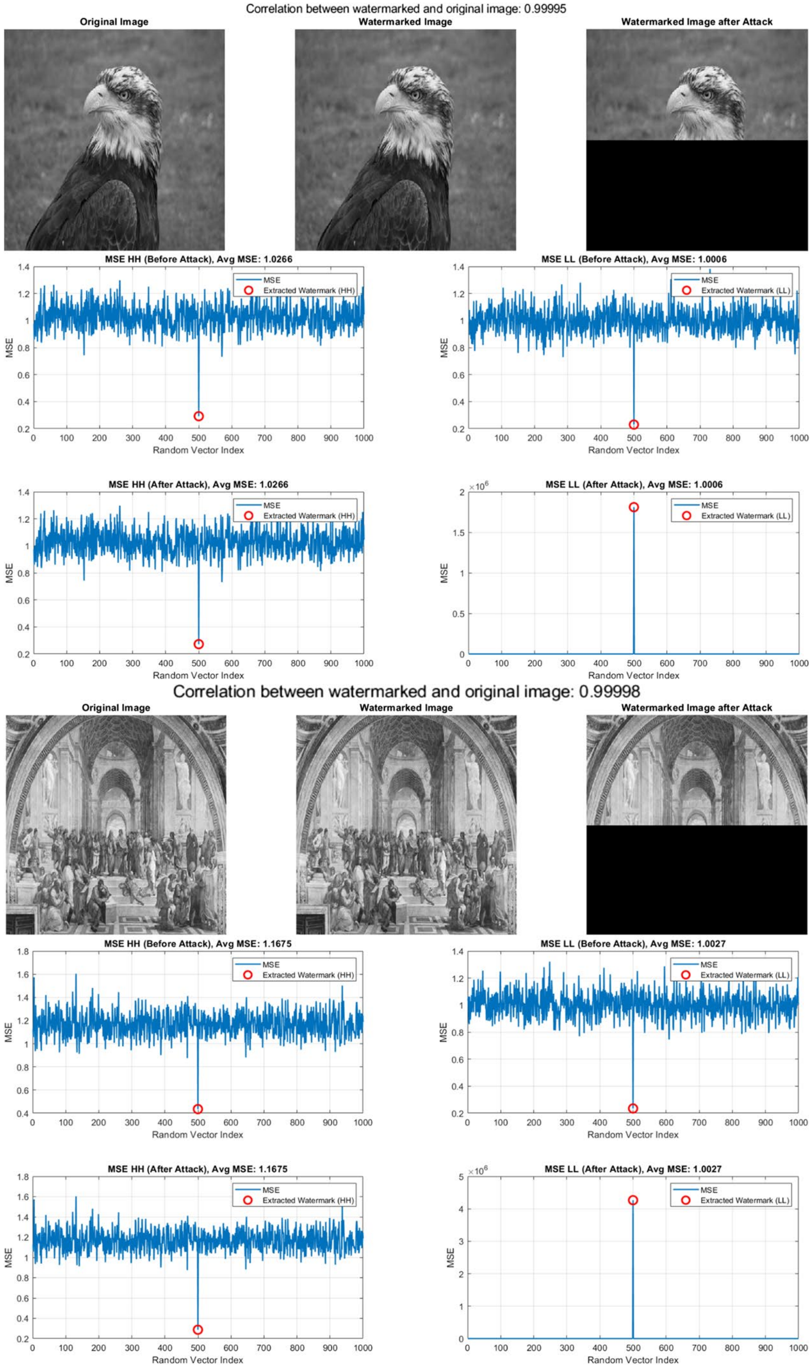


**Fig. 23** Comparative MSE Analysis of Embedded Watermarks in Different Image Domains Subject under Cropping Attack

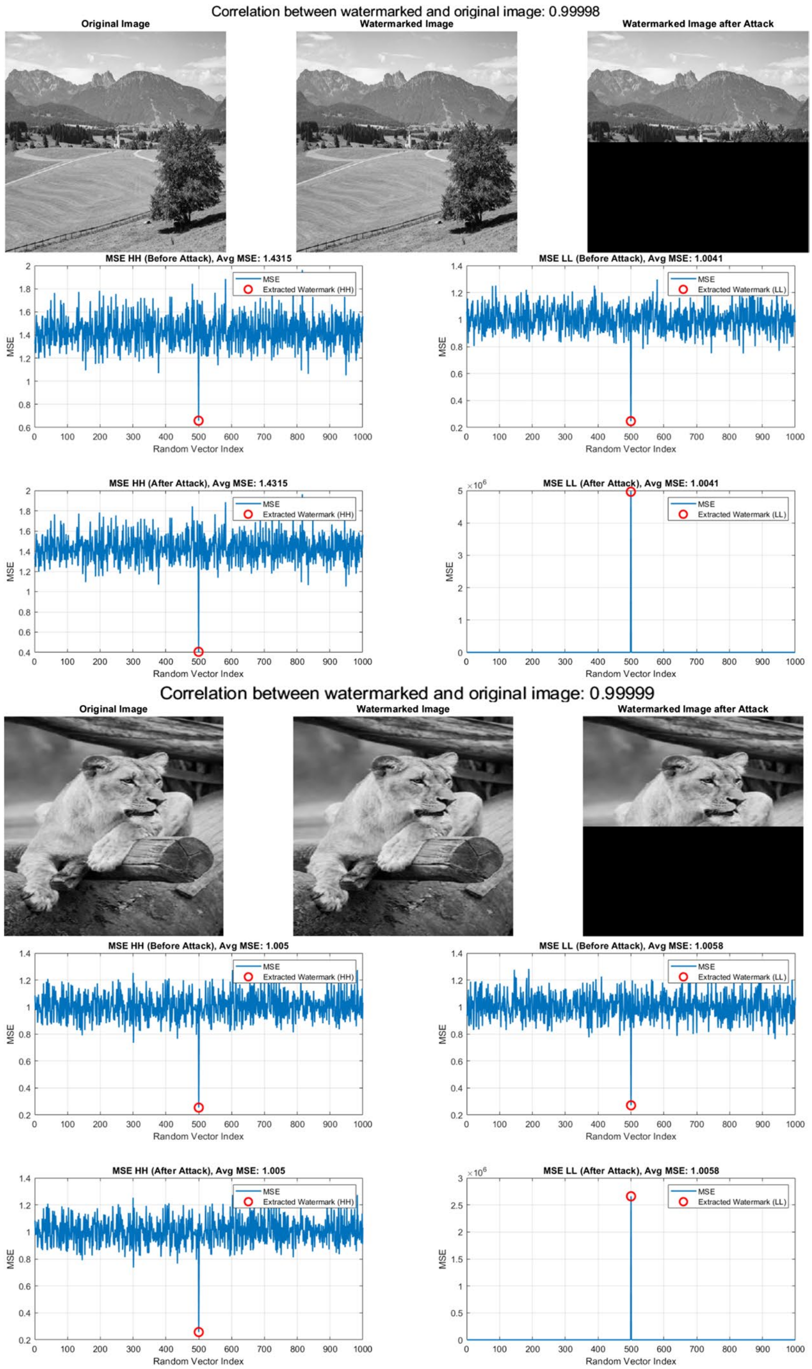


**Fig. 24** Continue Comparative MSE Analysis of Embedded Watermarks in Different Image Domains Subject under Cropping Attack

**Table 1** Average run times for different types of attacks applied to images

| Attack | Run Time (AVG per image) |
|---|---|
| Histogram equalization attack | 0.3 s |
| Salt and pepper attack | 0.3 s |
| Ripple attack | 0.28 s |
| Smoothing attack | 0.29 s |
| Cropping attack | 0.6 s |

Building upon these recent advancements, our work introduces a hybrid approach that integrates DWT, Schur decomposition, and DCT, specifically designed to address these identified vulnerabilities. By synergistically combining these methods, we not only enhance the watermark's imperceptibility and reduce computational load but also significantly improve robustness against noising and cropping attacks. Our approach seeks to fill the research gaps by offering a solution that maintains image quality while ensuring watermark security, a critical metric that has not been fully realized in the methods presented within 2023 and 2024 literature. Furthermore, we acknowledge and aim to explore the payload capacity limitations further, signaling a new direction for future research and potential advancements in the watermarking field.

Our study stands out from previous ones because it examines how well our method withstands the salt and pepper attack, which has been a longstanding issue with Schur matrix factorization in image watermarking. This aspect highlights the originality of our contribution in enhancing media ownership verification. By utilizing different transformation techniques, our approach shows potential in bolstering the trustworthiness and authenticity of digital media, thus fortifying the basis of intellectual property rights online. In Table 2, we present a comparison between the outcomes derived from our study and those attained from prior related research.

## 6 Conclusion, limitations, and future work

The proposed watermarking framework demonstrates the capacity to seamlessly embed watermarks, ensuring imperceptibility, thereby adhering to the fundamental principle of watermarking. Even after subjecting the cover image to a multitude of attacks that modify the pixel values and significantly alter its visual appearance, the embedded watermark remains resilient and retrievable, thereby safeguarding its ownership. Moreover, the presented solution addresses the vulnerability to the salt and pepper attack previously associated with Schur-based methodologies.

The study's findings suggest a promising approach to digital watermarking, addressing concerns surrounding media protection and ownership rights in the era of extensive digital dissemination. However, several limitations warrant consideration. Firstly, the testing scenarios may not fully encompass all potential adversarial conditions, including the absence of explicit validation for the randomness of our system. Furthermore, the assumption of consistent hardware conditions for testing may not fully reflect the variability of hardware capabilities and environments encountered in practical applications. While the emphasis on processing speed is noted, it's essential to balance speed considerations with other

**Table 2** Comparison with previous studies

| Author | Method used | Domain | Advantage | Disadvantage | Performance metrics |
|---|---|---|---|---|---|
| [45] | DWT | Copyright protection/ Transform domain | - High imperceptibility<br>- Improved computational time | - Low robustness to salt and pepper noise | Compression Ratio (CR): 0.698417<br>(moderate level of compression) |
| | DCT | | - Preserves image quality | - Highly susceptible to salt and pepper noise | CR: 0.016736<br>(very high level of compression) |
| [46] | LWT-Schur Decomposition | | - Resilience to various attacks<br>- No False Positive Problem (FPP) | - Susceptible to histogram equalization and cropping attack | Normalized<br>Correlation Coefficient (NCC) between the original image and the processed image is close to 0.53, NCC for cropping attack is close to 0.77 |
| [47] | Schur Decomposition Watermarking | | - Blind extraction<br>- Fewer computations than SVD | - Reduced robustness to 50% cropping attack | (NCC: 0.64674, 0.56319) |
| Proposed Method | Hybrid<br>(DWT, Schur, DCT) | | - Enhances watermark's imperceptibility<br>- Effective against various attacks (geometric and noise-based attacks)<br>- Effective against salt and pepper attack<br>- Significantly reduced computational load<br>- Significantly improves robustness against noising and cropping attacks<br>- Maintains image quality while ensuring watermark security | - Requires further exploration of payload capacity limitations for potential advancements | - NCC between watermarked and original image values is close to 1.0 under most of the attacks<br>- Average run times for different types of attacks applied to images were close to 0.3 s for most attacks and 0.6 for the Cropping attack |

performance metrics such as robustness and security. Finally, while the study highlights the potential for real-time applications like media streaming and content management, the scalability and implementation challenges in such contexts remain unclear. Addressing these limitations through further research and experimentation would enhance the credibility and applicability of the proposed watermarking approach.

In future research, the authors intend to explore the application of watermarking techniques within the healthcare sector, specifically focusing on the implementation of invisible signatures in X-ray images and MRI scans. This initiative aims to establish a robust framework for securing and authenticating critical medical data and reports.

**Author contributions** Issa AL-Aiash, Rabee Alquran, and Mahmoud AlJamal: Conceptualization, Methodology, Results, Writing- original draft preparation.

Ayoub Alsarhan: Methodology, Supervision, Writing original draft preparation.

Mohammad Aljaidi: Formal Analysis, Writing- Reviewing and Editing, Investigation.

Dimah Al-Fraihat: Formal Analysis, Writing original draft preparation, Writing- Reviewing and Editing, Administration**.**

**Funding** Not applicable.

**Data availability** The data repository used for experimentation is publicly available at: https://www.kaggle.com/datasets/felicepollano/watermarked-not-watermarked-images

## Declarations

**Ethical approval** Not applicable.

**Competing interests** The authors declare no competing interests.

## References

1. Zhou Zhili, Yunlong Wang QM, Jonathan Wu, Yang Ching-Nung, Sun Xingming (2016) Effective and efficient global context verification for image copy detection. IEEE Trans Inf Forensics Secur 12(1):48–63
2. Liu Z, Liu T, Gibbon D, Shahraray B (2010) Effective and scalable video copy detection. In: Proceedings of the International Conference on Multimedia Information Retrieval, pp 119–128
3. Qiu Y, Ying Q, Lin X, Zhang Y, Qian Z (2020) Reversible data hiding in encrypted images with dual data embedding. IEEE Access 8:23209–23220
4. Sinhal R, Ansari IA (2022) Multipurpose image watermarking: ownership check, tamper detection and self-recovery. Circuits Syst Signal Process 41(6):3199–3221
5. Su Q (2016) Color image watermarking: algorithms and technologies. Walter de Gruyter GmbH & Co KG vol. 1
6. Qingtang Su, Wang G, Zhang X, Lv G, Chen B (2018) A new algorithm of blind color image watermarking based on lu decomposition. Multidimens Syst Signal Process 29:1055–1074
7. Abraham J, Paul V (2019) An imperceptible spatial domain color image watermarking scheme. J King Saud Univ - Comput Inf Sci 31(1):125–133
8. Roy S, Pal AK (2017) A blind dct based color watermarking algorithm for embedding multiple watermarks. AEU Int J Electronic Comm 72:149–161
9. Boujerfaoui S, Riad R, Douzi H, Ros F, Harba R (2022) Image watermarking between conventional and learningbased techniques: A literature review. Electronics 12(1):74
10. Singh R, Ashok A (2021) An optimized robust watermarking technique using ckgsa in frequency domain. J Inf Secur Appl 58:102734
11. Parah SA, Sheikh JA, Loan NA, Bhat GM (2016) Robust and blind watermarking technique in dct domain using inter-block coefficient differencing. Digit Signal Process 53:11–24
12. Moosazadeh M, Ekbatanifard G (2019) A new dct-based robust image watermarking method using teaching-learningbased optimization. J Inf Secur Appl 47:28–38

13. Abdallah EE, Hamza AB, Bhattacharya P (2006) A robust block-based image watermarking scheme using fast Hadamard transform and singular value decomposition. In: 18th International Conference on Pattern Recognition (ICPR'06), vol. 3. IEEE, pp 673–676
14. Zhang X, Qingtang Su, Yuan Z, Liu D (2020) An efficient blind color image watermarking algorithm in spatial domain combining discrete fourier transform. Optik 219:165272
15. Begum M, Ferdush J, Uddin MS (2022) A hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition. J King Saud Univ - Comput Inf Sci 34(8):5856–5867
16. Singh S, Singh B (2022) A robust data hiding scheme using singular value decomposition and wavelet transform. In: International Conference on Advanced Communication and Intelligent Systems. Cham: Springer Nature, pp 81–88
17. Lai C-C, Tsai C-C (2010) Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans Instrum Meas 59(11):3060–3063
18. Soualmi A, Alti A, Laouamer L (2018) Schur and DCT decomposition based medical images watermarking. In: 2018 Sixth International Conference on Enterprise Systems (ES), IEEE, pp 204–210
19. Abdallah EE, Ben Hamza A, Bhattacharya P (2007) Improved image watermarking scheme using fast hadamard and discrete wavelet transforms. J Electronic Imaging 16(3):033020–033020
20. Ouhsain M, Hamza AB (2009) Image watermarking scheme using nonnegative matrix factorization and wavelet transform. Expert Syst Appl 36(2):2123–2129
21. Mohammad AA (2012) A new digital image watermarking scheme based on schur decomposition. Multimed Tools Appl 59:851–883
22. Gunjan R, Mitra P, Gaur MS (2012) Contourlet based image watermarking scheme using Schur factorization and SVD. In: Advances in Communication, Network, and Computing: Third International Conference, CNC 2012, Chennai, India, February 24-25, 2012, Revised Selected Papers, vol. 3. Springer Berlin Heidelberg, pp 337–340
23. Ali BB, Masmoudi Y, Dhouib S (2016) DTW-global constraint learning using tabu search algorithm. Procedia Comp Sci 82:12–19
24. Hosam O (2019) Attacking image watermarking and steganography-a survey. Int J Info Technol Comp Sci 11(3):23–37
25. Ahmed R, Riaz MM, Ghafoor A (2018) Attack resistant watermarking technique based on fast curvelet transform and robust principal component analysis. Multimed Tools Appl 77:9443–9453
26. Petra CG, Schenk O, Lubin M, Gärtner K (2014) An augmented incomplete¨ factorization approach for computing the schur complement in stochastic optimization. SIAM J Sci Comput 36(2):C139–C162
27. Golpar Raboky E (2022) On generalized schur complement of matrices and its applications to real and integer matrix factorizations. J Math Model 10(1):39–51
28. Meenakshi K, Swaraja K, Kora P (2020) A hybrid matrix factorization technique to free the watermarking scheme from false positive and negative problems. Multimedia Tools Appl 79(39–40):29865–29900
29. Maurer D, Wieners C (2016) A scalable parallel factorization of finite element matrices with distributed schur complements. Numer Linear Algebr Appl 23(5):848–864
30. Alotaibi RA, Elrefaei LA (2019) Textimage watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT). Appl Comput Inform 15(2):191–202
31. Gunjal M, Jha J (2014) Image steganography using discrete cosine transform (dct) and blowfish algorithm. Int J Comp Trends Technol (IJCTT) 11(4):144–150
32. Guo Y, Li B-Z, Goel N (2017) Optimised blind image watermarking method based on firefly algorithm in dwt-qr transform domain. IET Image Processing 11(6):406–415
33. Huang CP, Liao CJ, Hsieh CH (2009) A blind image watermarking based on dual detector. J Info Sci Eng 25(6)
34. Chow YW, Susilo W, Tonien J, Zong W (2017) A QR code watermarking approach based on the DWT-DCT technique. In: Information Security and Privacy: 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3–5, 2017, Proceedings, Part II 22. Springer International Publishing, pp 314–331
35. Bagade SS, Shandilya VK (2011) Use of histogram equalization in image processing for image enhancement. Int J Software Eng Res Practices 1(2):6–10
36. Azzeh J, Zahran B, Alqadi Z (2018) Salt and pepper noise: Effects and removal. JOIV: Int J Info Visualization 2(4):252–256
37. Raam RS, Sathyam K, Srivatsan A, Devakumar T (2021) DCT based image watermarking. Turkish Journal of Computer and Mathematics Education 12(10):1281–1288
38. Pollano F (n.d.) Watermarked and not watermarked images dataset. Available at: https://www.kaggle.com/datasets/felicepollano/watermarked-not-watermarked-images. Accessed 9 June 2023
39. Al-Fraihat D, Sharrab Y, Al-Ghuwairi AR, Alshishani H, Algarni A (2024). Hyperparameter optimization for software bug prediction using ensemble learning. IEEE Access 12:51869–51878

40. Al-Fraihat, D, Sharrab Y, Alzyoud F, Qahmash A, Tarawneh M, Maaita A (2024) Speech recognition utilizing deep learning: a systematic review of the latest developments. Hum-centric Comput Inf Sci 14
41. Al-Ghuwairi AR, Al-Fraihat D, Sharrab Y, Alrashidi H, Almujally N, Kittaneh A, Ali A (2023) Visualizing software refactoring using radar charts. Scientific Reports 13(1):19530
42. Maini DS, Aggarwal AK (2018) Camera position estimation using 2D image dataset. Int J Innov Eng Technol 10(2):199–203
43. Aggarwal AK (2023) Thermal imaging for cancer detection. Imaging Radiation Research 6(1):2638
44. Tiwari A, Srivastava VK (2024) Image watermarking techniques based on Schur decomposition and various image invariant moments: a review. Multimed Tools Appl 83(6):16447–16483
45. Abd-Elsalam RO, Saleh SQ (n.d.) Digital image watermarking methods based on transformation techniques: A comparative study
46. Tiwari A, Srivastava VK (2023) Novel schemes for the improvement of lifting wavelet transform-based image watermarking using Schur decomposition. The Journal of Supercomputing 79(12):13142–13179
47. Su Q, Niu Y, Liu X, Zhu Y (2012) Embedding color watermarks in color images based on Schur decomposition. Opti Commun 285(7):1792–1802

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

## Authors and Affiliations

**Issa Al-Aiash[1] · Rabee Alquran[1] · Mahmoud AlJamal[1] · Ayoub Alsarhan[1] · Mohammad Aljaidi[2] · Dimah Al-Fraihat[3]**

✉ Dimah Al-Fraihat
d.fraihat@iu.edu.jo

Issa Al-Aiash
issaalayyash76@gmail.com

Rabee Alquran
alquran.rabee@gmail.com

Mahmoud AlJamal
mahmood.yj.98@gmail.com

Ayoub Alsarhan
ayoubm@hu.edu.jo

Mohammad Aljaidi
mjaidi@zu.edu.jo

[1] Department of Information Technology, Faculty of Prince Al-Hussein Bin Abdallah II for Information Technology, The Hashemite University, Zarqa 13133, Jordan

[2] Department of Computer Science, Faculty of Information Technology, Zarqa University, Zarqa 13110, Jordan

[3] Department of Software Engineering, Faculty of Information Technology, Isra University, Amman 11622, Jordan