SN Computer Science (2021) 2:82
https://doi.org/10.1007/s42979-021-00478-y

ORIGINAL RESEARCH

An Efficient Watermarking Approach Based on LL and HH Edges of DWT–SVD

Fauzia Yasmeen[1,2] · Mohammad Shorif Uddin[3]

Received: 27 November 2020 / Accepted: 19 January 2021 / Published online: 8 February 2021

Abstract

Digital watermarking is playing a vital role in the improvement of authentication, security, and copyright protection in today's digital transformation. The performance of this technique is shown to be impressive around the globe. Text, audio, video, and image data are acted as watermarks in the digital platform. In this article, a hybrid watermarking scheme is proposed to furnish the robustness and protection of digital data. This hybrid scheme is a form of discrete wavelet transform (DWT) and singular value decomposition (SVD). The embedding and extracting features are carried out through multi-level operations of DWT and SVD. Various attacks are added to the proposed method to justify the robustness of the watermark. In the end, the suggested approach is contrasted with existing methods to confirm the supremacy.

Keywords Digital watermarking · Discrete wavelet transform (DWT) · Singular value decomposition (SVD) · Imperceptibility · Robustness

Introduction

With the rapid growth of information technology, interactive media have become the most important gadgets for transmitting information [1]. The mode of communication and business has been converted into digital form due to the global pandemic situations and this scenario is increasing day by day. Thus, there are millions, and billions of data are moving worldwide in the digital platform. Recently, this has caused considerable interest within the community due to the pandemic situation of COVID-19. Considering the privilege of cyberspace, anyone can easily modify or use content without the owner's permission. So, security and authenticity become a concern to protect the information from being altered or misuse. Digital watermarking stands here to solve the issues. Digital watermarking is pursued as a marker or verification mechanism that proves an individual's identity for his/her work. This marker can be a logo for an organization or the digital signature of an author. A digital watermark can be visible or invisible and embedded into the digital carrier like text, image, audio, or video-related content. Intangibility and robustness are considered in the substantial watermarking algorithm [2]. Intangibility is calculated by PSNR value (peak signal-to-noise ratio) and robustness is computed by correlation among the original watermark and recovered watermark image [3].

Digital watermarking is classified into spatial domain and frequency domain transform. In the spatial domain, the watermark is precisely enclosed by adjusting the grayscale values of the pixels of the host image beyond any transformation [4]. On the contrary, the transformation, such as DWT, SVD, DCT, DFT, etc., is performed in the host image before embedding into the watermark image [4]. It is said that the frequency domain not only tends to be more robust in comparison with the spatial domain but also further complex than the spatial method [4]. Several research groups

This article is part of the topical collection "Cyber Security and Privacy in Communication Networks" guest edited by Rajiv Misra, R. K. Shyamsunder, Alexiei Dingli, Natalie Denk, Omer Rana, Alexander Pfeiffer, Ashok Patel and Nishtha Kesswani.

✉ Fauzia Yasmeen
fauzia328@yahoo.com

Mohammad Shorif Uddin
shorifuddin@gmail.com

[1] Department of Information and Communication Engineering, Bangladesh University of Professionals (BUP), Mirpur Cantonment, Dhaka 1216, Bangladesh

[2] Department of Computer Science and Engineering, Fareast International University, Banani, Dhaka 1213, Bangladesh

[3] Department of Computer Science and Engineering, Jahangirnagar University, Savar, Dhaka 1342, Bangladesh

have been working on the design of the watermarking technique. This has been introduced to overcome some of the inherent limitations of cryptography. The solution is to apply an appropriate hybrid method that guarantees strong authentication as well as the robustness of the owner's property.

With this aim in mind, we seek to develop a novel approach with the goal of copyright protection. We examine the three key elements of work in this area:

(1) the first part was focused on the embedding procedure

(2) the second phase was involved in the extraction process and

(3) the last stage concentrated the resistance against multiple attacks.

The remaining of the paper has been structured as follows—"Literature Review" illustrates a review of techniques used in digital watermarking, "Digital Watermarking Concept", "DWT" and "SVD" has set out the theories of digital watermarking, DWT (discrete wavelet transform), SVD (singular value decomposition) that underpin the method used in this paper, "Proposed Work" presents the embedding and extracting algorithm of our proposed work, "Performance Analysis" shows the performance analysis and discussion and "False Positive Issue" concludes the paper by examining the impact of the method.

Literature Review

The literature is reviewed to examine available methods that could be used in watermarking. A good number of research work is conducted for contemporary watermarking methods.

Zhang et al. [2] suggested a robust color image watermarking algorithm. This algorithm converts the host color image watermarking into YUV and SVD is utilized to Y component. However, the watermark is embedded into the host image followed by the modification through Arnold transform and DWT. This method claimed robustness against geometric attacks, but it is seen that the PSNR value is very low compare to other watermark-related schemes.

Singh et al. [5] proposed a block-based DWT-SVD image watermarking approach where QR (quick response code) code is considered as a watermark image. Both the original image and watermark image are decomposed by 2-level DWT on a low-frequency band and the corresponding frequency band is separated into $m \times n$ block size. As the color image is used here as a host image, SVD had to apply on each RGB component of a block to find the singular values of the watermarking. This method claims robustness against Gaussian noise and salt and pepper noise.

Similar work also has been pursued by others [6] in which a hybrid (DWT–SVD) watermarking scheme and a mathematical tool known as PSO (particle swarm optimization) are used for the efficient and secured watermarked image. RGB components of the host image are separated, and three-level DWT is performed on the R component. Then, SVD is applied on the approximate co-efficient of the R component. On the other hand, the watermark image is scrambled using Arnold transform and SVD is also used here to find the singular value of the watermark. The scaling factor is obtained from PSO to embed into the watermark image. This technique asserted good PSNR values adjacent to different attacks.

This issue was explored by Naik et al. [7], who introduced a robust watermarking technique based on DWT and SVD, which decomposed the host image by 2-level DWT and SVD is applied into the HL sub-band. The same working principle is performed on the watermark image and then the SVD of both images is embedded with a scaling factor to form a watermarked image.

Conceptually similar work has also been carried out by [8, 9] in which the cover image is divided by first-level Haar DWT and the SVD is added to the LH and HL sub-bands. Besides, the watermark is split into equal halves and LH and HL are modified before being inserted in the host image. The watermark is extracted from the reverse process. It is noted that this approach only demonstrates robustness for histogram equalization.

Harjito and Suryani [10] developed their watermarking scheme where white Gaussian is added to the scaling factor. But this technique is not resistant to some attacks like rotating, cropping, and blurring.

In the study [11], both the host and watermark are converted into the grayscale and the watermark is encrypted before the embedding procedure. Host image is decomposed by 2-D DWT and SVD is applied on lower-level frequency region. Encrypted watermark is then embedded into this LL sub-band of the host image.

A hybrid watermarking algorithm based on DWT–DCT is suggested by Akter et al. [3]. The authors applied 4th-level DWT into the original image and select HL4 and LH4 sub-bands. The properties of DCT are performed to the co-efficient of these said sub-bands. Concurrently, the watermark image is reformed and scramble it. The scrambled watermark image is then transformed into DCT. The duo of these modified host image and watermark is embedded to form the watermarked image. The reverse process is used to extract the watermark. This algorithm is tested through PSNR and MSE to evaluate the performance and compared the existing method. It can be seen the PSNR value is found 36.52 dB of the watermarked image before the attack and it is 30.21 dB after the attack. This method only used Additive White Gaussian Noise (AWGN) to prove the performance, but other significant attacks were not tested here.

This method [12] presented a unique technique that showed a comprehensive rise of PSNR value. The host image and the watermark image are split into R, G, and B channels, and the single-level 2D DWT is applied to the selected frequency sub-bands. Increased levels of host image and watermark have been associated with 2D DFT and DCT respectfully. The SVD is performed on both images before the embedding. But this method is not being tested by a variety of attacks.

Another method is approached by [13], where DCT is used in host images and a watermark is embedded by a slightly modified version of Cox's formula. This system provides robustness upon adding a watermark in the low-frequency regions compare with high-frequency regions.

It is noted that some methods provide good PSNR values in terms of watermarked images, but the robustness is low for the watermark extraction procedure. The grayscale image works well in some approaches while several techniques produce better results in color images. Fewer algorithms show robustness upon geometric attacks where some other is applicable only for lean attacks. Considering the above-mentioned difficulties discussed in the literature review, a novel hybrid watermarking procedure is approached in the presented work. This mechanism is developed to consider the grayscale and color images. Watermark embedding and extraction are evaluated in both types of images and robustness is examined in various types of attacks. This scheme is allowed an acceptable imperceptibility rate along with security issues.

Digital Watermarking Concept

Digital watermarking is a good choice for the authentication and copyright protection of images. This has proven to be a serious impediment to a widespread misuse of information in a common communication environment like the internet [14]. The basic idea of image watermarking is to embed invisible or inaudible data within multimedia content. The copyright information is contained in the watermarked substance. The hidden data for such purposes are referred to as a watermark and the content can be an image, audio, or some other type of media in any of the formats available [15]. On that account, digital watermarking has been chosen for its wide range of applications in the field of computer science, cryptography, signal processing, and communications [16].

The digital watermarking technique comprises two processes—embedding process and extraction process. In the embedding phase, the secret information (known as a watermark) is inserted into the multimedia object (known as a cover image) and is called "watermarked image" [17].

This watermarked image is then transmitted through the communication channel and the stored watermark can be retrieved at the receiver end to ensure the validity of the digital data. This retrieval process is called "watermark extraction" [17]. The embedding and extraction process is schematically shown in Fig. 1.

Imperceptibility, robustness, and security are the key features of the watermarking method. Imperceptibility is computed by the visual affinity of the host image in comparison to the watermarked image [18]. The watermarking framework ought to be robust against any deliberate or accidental assault of the watermarked substance that can be a picture, sound, video, or text [13]. A watermark system is supposed to be secure if the unauthorized person cannot extract the watermark without having complete knowledge of the embedding algorithm, the detector, and the composition of the watermark [19]. The schematic diagram of digital watermarking is shown in Fig. 1.

DWT

Discrete wavelet transform is considered the most widely used transformation technique for digital watermarking. It is indeed useful to describe DWT as any wavelet transform for which wavelets are sampled discretely [31]. The strength of DWT over Fourier transform is its ability to produce a temporal resolution in which it captures both frequency and location information. The wavelet's translations and dilations are triggered by the mother wavelet [26].

The DWT splits an image into four non-overlapping multi-resolution sub-bands—LL, LH, HL, and HH [37]. The LL (low–low) level signifies the approximate part of the cover image while the other three levels, i.e. LH (low–high), HL (high–low), and HH (high–high) provide detailed information about the host image [33]. For further decomposition, any of the sub-bands are selected and hence divide into four levels. The decomposition method is replicated until the

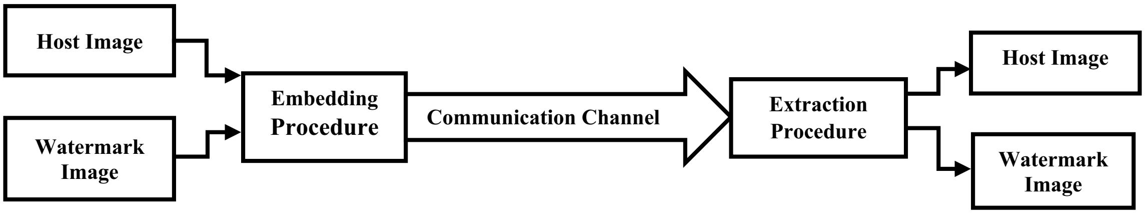


Fig. 1 Schematic diagram of digital watermarking

required levels of decomposition are reached [32]. The maximum degree of decomposition seems to be the intensity of the watermarked image [33]. At each step of decomposition, the magnitude of DWT coefficients is greater in the lower band (LL) and smaller in the other three bands (LH, HL, and HH) [33]. As HVS (human visual system) is more sensitive to low-frequency parts (LL sub-band), so watermarks are ideally put in the three other sub-bands to maintain the quality of the original image [33]. A diagram, showing the steps in the DWT decomposition process is shown in Fig. 2.

SVD

Singular value decomposition is a mathematical transformation that is used for the factorization of a real or complex matrix with diverse applications in various areas of image processing [36]. The purpose of SVD is to minimize the complexity by splitting the non-negative image matrix into $U \times S \times V^T$, where U and V denote the orthogonal matrices and S is called the diagonal matrix of singular values of the original matrix handled in decreasing order [26].

There are two key features of SVD to be used in automated watermarking techniques: [33]

(1) The changes in singular values would inevitably affect the quality of the images.
(2) The singular values of the image are therefore of high stability; they do not shift after numerous attacks.

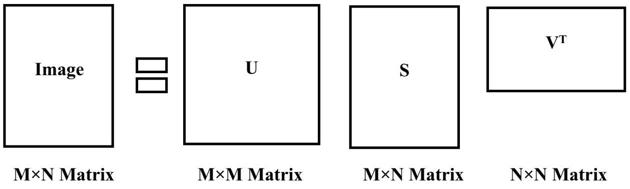


Fig. 3 The procedure of SVD decomposition

A graphical description of the procedure of SVD of an $M \times N$ image is presented in Fig. 3 [32].

Proposed Work

In our work, we explore a new hybrid approach, a fusion of DWT and SVD, for the improved quality of watermark insertion and extraction procedure. The advantage of this proposed algorithm is that it has the properties of undetectability and durability. The blend of DWT and SVD will bring to light the potential mechanisms responsible for the owner's authenticity and robustness to several kinds of attacks. The suggested algorithm belongs to two parts—the watermark embedding and extraction algorithm. Both parts along with respective flowcharts have been described in detail in "Watermark Embedding Algorithm" and "Watermark Extracting Algorithm".

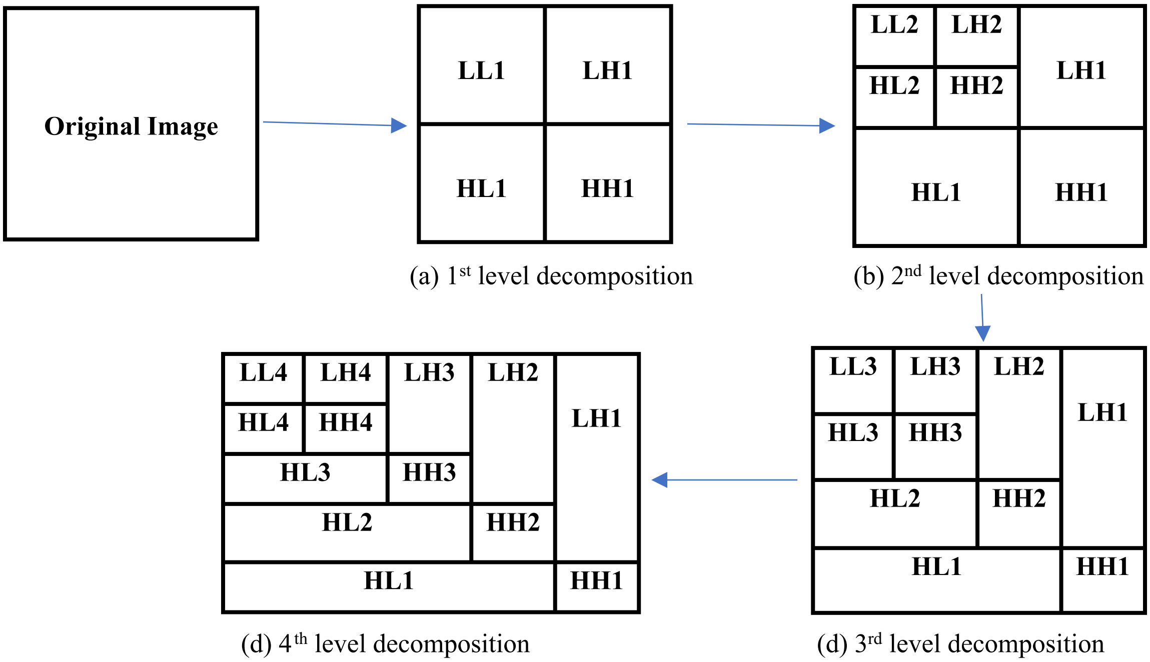


Fig. 2 Discrete wavelet transform decomposition

Watermark Embedding Algorithm

A detailed description of the steps of watermark embedding is given below:

Algorithm 1: Watermark Embedding

Input: Host Image (512×512 pixels) and Logo Watermark Image (256×256 pixels).

Output:

1) Perform 4th level and 3rd level DWT transformation on the host image and watermark image.

Host Image:

$$DWT\ (LL3) = [LL4, LH4, HL4, HH4]$$

Watermark Image:

$$DWT\ (LL2) = [LL3, LH3, HL3, HH3]$$

2) Apply 1st level and 2nd level SVD on LH4 and HL4 sub-bands.

$$\text{Host image:}\begin{cases} SVD\ (LL4) = [U_{h1}, S_{h1}, V_{h1}^{T}] \\ SVD(S_{h1}) = [U_{h2}, S_{h2}, V_{h2}^{T}] \end{cases}$$

$$\text{Host image:}\begin{cases} SVD\ (HH4) = [U_{h3}, S_{h3}, V_{h3}^{T}] \\ SVD\ (S_{h3}) = [U_{h4}, S_{h4}, V_{h4}^{T}] \end{cases}$$

$$\text{Watermark:}\begin{cases} SVD\ (LL3) = [U_{w1}, S_{w1}, V_{w1}^{T}] \\ SVD(S_{w1}) = [U_{w2}, S_{w2}, V_{w2}^{T}] \end{cases}$$

$$\text{Watermark:}\begin{cases} SVD\ (HH3) = [U_{w3}, S_{w3}, V_{w3}^{T}] \\ SVD\ (S_{w3}) = [U_{w4}, S_{w4}, V_{w4}^{T}] \end{cases}$$

3) Add 1st level and 2nd level singular values of their corresponding sub-bands.

$$\text{Host image:}\begin{cases} New\_S\_h\_LL4 = S_{h1} + S_{h2} \\ New\_S\_h\_HH4 = S_{h3} + S_{h4} \end{cases}$$

$$\text{Watermark:}\begin{cases} New\_S\_W\_LL3 = S_{w1} + S_{w2} \\ New\_S\_W\_HH3 = S_{w3} + S_{w4} \end{cases}$$

4) Fit the watermark into the host image to generate the watermarked image

$$W\_I\_S\_LL4 = New\_S\_h\_LL4 + alpha \times New\_S\_W\_LL3$$

$$W\_I\_S\_HH4 = New\_S\_h\_HH4 + alpha \times New\_S\_W\_HH3$$

5) Apply Inverse Singular Value Decomposition.

$$W\_I\_LL4 = U_{h1} \times W\_I\_S\_LL4 \times V_{h1}^{T}$$

$$W\_I\_HH4 = U_{h3} \times W\_I\_S\_HH4 \times V_{h3}^{T}$$

6) Employ 4th, 3rd, 2nd, and 1st level IDWT to compute the final watermarked image.

The flowchart of watermark embedding is presented in Fig. 4.

Watermark Extracting Algorithm

The procedure of watermark extraction is explained in the following Algorithm 2.

Algorithm 2: Watermark Extraction

Input: Host Image (512×512 pixels), Watermarked Image (512×512 pixels).

Output:

1) Both the watermarked image and host image are split by 4th level DWT.

   Watermarked Image:

$$DWT\ (LL3) = [LL4, LH4, HL4, HH4]$$

   Host Image:

$$DWT\ (LL3) = [LL4, LH4, HL4, HH4]$$

2) Utilize 1st level and 2nd level SVD on LH4 and HL4 sub-bands of watermarked image and host image.

$$\text{Watermarked image :}\ \begin{cases} SVD\ (LL4) = [U_{W\_I\_1}, S_{W\_I\_1}, V_{W\_I\_1}^T] \\ SVD(S_{W\_I\_1}) = [U_{W\_I\_2}, S_{W\_I\_2}, V_{W\_I\_2}^T] \end{cases}$$

$$\text{Watermarked image: :}\ \begin{cases} SVD\ (HH4) = [U_{W\_I\_3}, S_{W\_I\_3}, V_{W\_I\_3}^T] \\ SVD(S_{W\_I\_3}) = [U_{W\_I\_4}, S_{W\_I\_4}, V_{W\_I\_4}^T] \end{cases}$$

$$\text{Host Image}\ \begin{cases} SVD\ (LL4) = [U_{h1}, S_{h1}, V_{h1}^T] \\ SVD(S_{h1}) = [U_{h2}, S_{h2}, V_{h2}^T] \end{cases}$$

$$\text{Host Image:}\ \begin{cases} SVD\ (HH4) = [U_{h3}, S_{h3}, V_{h3}^T] \\ SVD\ (S_{h3}) = [U_{h4}, S_{h4}, V_{h4}^T] \end{cases}$$

3) Append 1st level and 2nd level SVD of corresponding sub-bands.

   Watermarked image:

$$\begin{cases} New\_S\_W\_I\_LL4 = S_{w\_I\_1} + S_{w\_I\_2} \\ New\_S\_W\_I\_HH4 = S_{w\_I\_3} + S_{w\_I\_4} \end{cases}$$

   Host image:

$$\begin{cases} New\_S\_h\_LL4 = S_{h1} + S_{h2} \\ New\_S\_h\_HH4 = S_{h3} + S_{h4} \end{cases}$$

4) Extract singular value of watermark from watermarked image to host image.

$$New\_S\_W\_LL3 = (New\_S\_W\_I\_LL4 - New\_S\_h\_LL4)/alpha$$

$$New\_S\_W\_HH3 = (New\_S\_W\_I\_HH4 - New\_S\_h\_HH4)/alpha$$

5) Recover 1st level singular value of watermark using the following equation:

$$S_{w1} = New\_S\_W\_LL3 - S_{w2}$$

$$S_{w3} = New\_S\_W\_HH3 - S_{w4}$$

6) Restore 1st level singular value of watermark using the following equation:

$$SVD(LL3) = U_{w1} \times S_{w1} \times V_{w1}^T$$

$$SVD(HH3) = U_{w3} \times S_{w3} \times V_{w3}^T$$

7) Apply 3rd, 2nd and 1st level of IDWT to extract the watermark image.

The flowchart of watermark extraction is shown in Fig. 5.

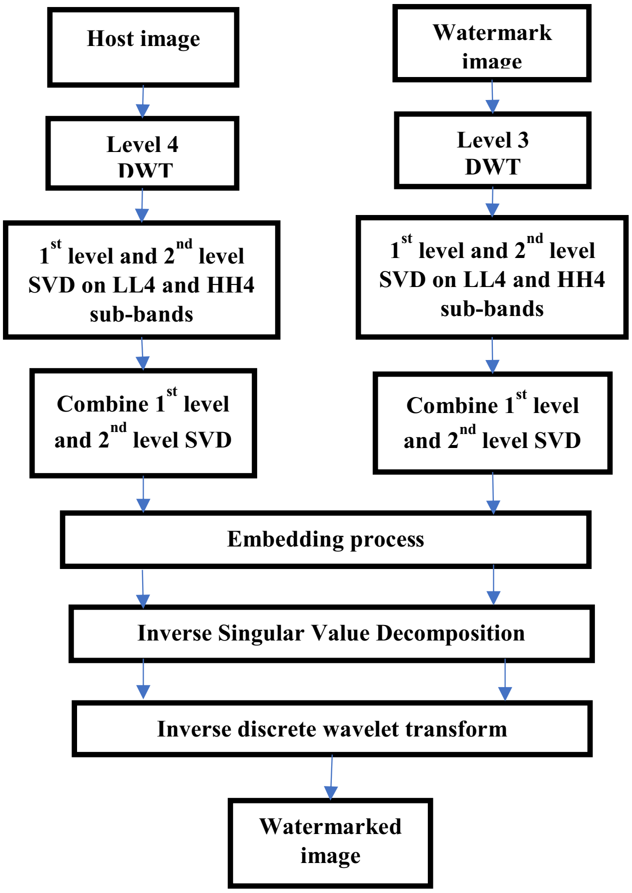

Host image
Watermark image
Level 4 DWT
Level 3 DWT
1st level and 2nd level SVD on LL4 and HH4 sub-bands
1st level and 2nd level SVD on LL4 and HH4 sub-bands
Combine 1st level and 2nd level SVD
Combine 1st level and 2nd level SVD
Embedding process
Inverse Singular Value Decomposition
Inverse discrete wavelet transform
Watermarked image

Fig. 4 Flowchart of watermark embedding

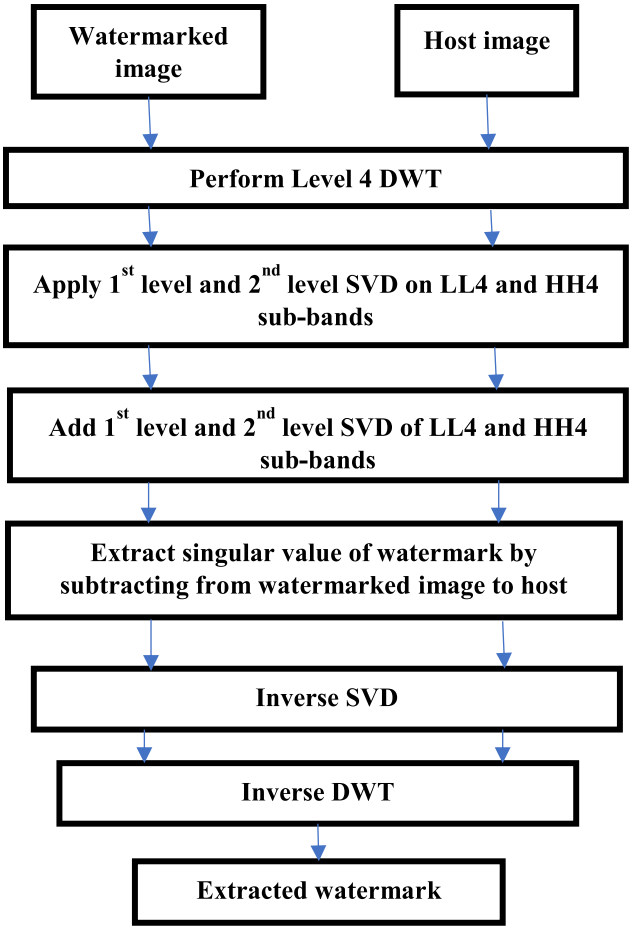

Watermarked image
Host image
Perform Level 4 DWT
Apply 1st level and 2nd level SVD on LL4 and HH4 sub-bands
Add 1st level and 2nd level SVD of LL4 and HH4 sub-bands
Extract singular value of watermark by subtracting from watermarked image to host
Inverse SVD
Inverse DWT
Extracted watermark

Fig. 5 Flowchart of watermark extraction

Performance Analysis

The proposed algorithm has been accomplished using MATLAB R2016a software. This technique is carried out under several conditions with different types of host images and logo watermark image. The sizes of the host image are taken as 512 × 512 pixels and the watermark image as 256 × 256 pixels.

Proof of Imperceptibility

Imperceptibility implies that the visual quality of the host image should not be skewed by the presence of the watermark [3]. Peak signal-to-noise ratio (PSNR) is used as a primary tool to show the visual effect between the host image and the watermarked image whereas MSE is calculated as the square of error amidst those images [34]. Besides, the Structural Similarity Index Measure (SSIM) and Normalized Correlation (NC) act as essential parameters for the evidence of invisibility. The range of SSIM varies from 0 to 1. Although 1 indicates the perfect match of the reconstructed image compares to the original one, the values range from 0.9 to 1 are designated as appropriate regenerated

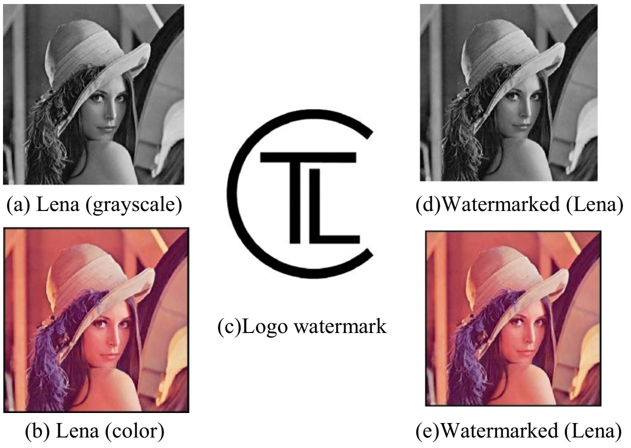
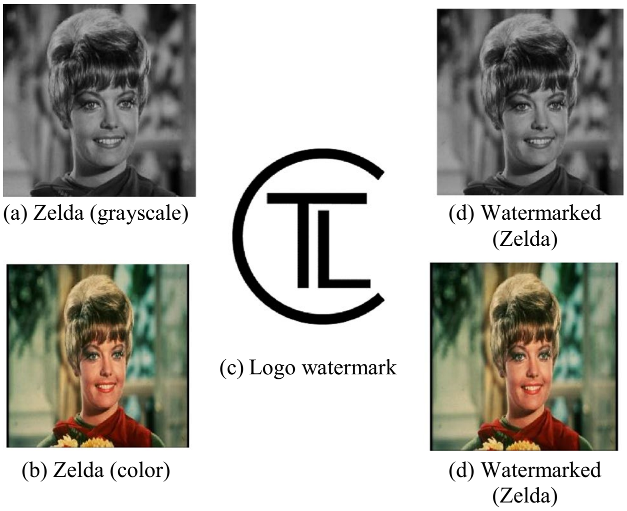

(a) Lena (grayscale)
(d)Watermarked (Lena)
(c)Logo watermark
(b) Lena (color)
(e)Watermarked (Lena)

Fig. 6 Host image of **a** Lena (grayscale) and **b** Lena (color), **c** Logo watermark and watermarked image of **d** Lena (grayscale) and **e** Lena (color)

Table 1 PSNR, MSE, SSIM, and normalized coefficient (NC) of watermarked. image of Lena (grayscale) and Lena (color)

Image name	Scaling factor (alpha)	PSNR	MSE	SSIM	NC	FSIM	GMSD
Lena (grayscale)	0.03	43.8362	2.6882	0.9909	0.9995	0.9984	0.0025
	0.0405						
	0.05						
	0.06						
Lena (color)	0.03	34.7266	21.8990	0.9885	0.9975	0.9961	0.0053
	0.0405						
	0.05						
	0.06						


(a) Zelda (grayscale)

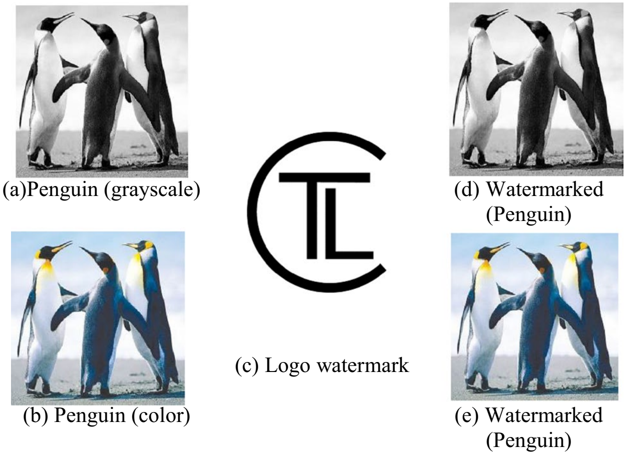
(d) Watermarked (Zelda)

(c) Logo watermark

(b) Zelda (color)

(d) Watermarked (Zelda)

Fig. 7 Host image of **a** Zelda (grayscale) and **b** Zelda (color), **c** Logo watermark and watermarked image of **d** Zelda (grayscale) and **e** Zelda (color)


(a)Penguin (grayscale)

(d) Watermarked (Penguin)

(c) Logo watermark

(b) Penguin (color)

(e) Watermarked (Penguin)

Fig. 8 Host image of **a** Penguin (grayscale) and **b** Penguin (color), **c** Logo watermark and watermarked image of **d** Penguin (grayscale) and **e** Penguin (color)

images. NC is also used to measure the similarity between two images.

Mathematically, PSNR and MSE can be expressed as follows:

$$\mathrm{PSNR(dB)} = 10\log_{10}\frac{\mathrm{MAX}^2}{\mathrm{MSE}} \tag{1}$$

$$\mathrm{MSE} = \frac{1}{H \times W}\sum_{i=1}^{H}\sum_{j=1}^{W}\left[X(i,j) - Y(i,j)\right]^2. \tag{2}$$

Apart from PSNR, MSE, SSIM, and NC, a new metric known as feature similarity index (FSIM) has been applied to correlate the feature similarity measure among the host image and the watermarked image [35] for image quality assessment (IQA). The phase congruency (PC) and the gradient magnitude (GM) are the two main parameters in FSIM to measure the image quality [36]. At first, the feature similarity of phase congruency (PC) of host and watermarked images can be defined as

$$S_{\mathrm{PC}}(x) = \frac{2\mathrm{PC}_h(x)\cdot\mathrm{PC}_{\mathrm{WI}(x)} + T_1}{\mathrm{PC}_h^2(x) + \mathrm{PC}_{\mathrm{WI}}^2(x) + T_1}, \tag{3}$$

where, S_{PC} is the feature similarity of phase congruency (PC) between host image and watermarked image, PC_h and $\mathrm{PC}_{\mathrm{WI}}$ are the phase congruency of host image and watermarked image, respectively, and T_1 is a positive constant for boosting the stability of S_{PC}.

Likewise, the similarity measure of GM value can be calculated as follows:

$$S_{\mathrm{GM}}(x) = \frac{2G_h(x)\cdot G_{\mathrm{WI}}(x) + T_2}{G_h^2(x) + G_{\mathrm{WI}}^2(x) + T_2}, \tag{4}$$

where S_{GM} is the similarity computation of gradient magnitude of both images (host and watermarked), G_h and G_{WI} are the gradient values of host and watermarked image and T_2 is the positive constant factor relying on the changing values of gradient magnitude.

Table 2 PSNR, MSE, SSIM, and normalized coefficient (NC) of watermarked

Image name	Scaling factor (alpha)	PSNR	MSE	SSIM	NC	FSIM	GMSD
Zelda (grayscale)	0.03	39.5227	7.257	0.9456	0.9978	0.9966	0.0042
	0.0405						
	0.05						
	0.06						
Zelda (color)	0.03	37.8992	10.5478	0.9848	0.9988	0.9971	0.0038
	0.0405						
	0.05						
	0.06						

Image of Zelda (grayscale) and Zelda (color)

Table 3 PSNR, MSE, SSIM, and normalized coefficient (NC) of watermarked image of Penguin (grayscale) and Penguin (color)

Image name	Scaling factor (alpha)	PSNR	MSE	SSIM	NC	FSIM	GMSD
Penguin (grayscale)	0.03	37.7820	10.8362	0.9669	0.9992	0.9970	0.0044
	0.0405						
	0.05						
	0.06						
Penguin (color)	0.03	36.2125	15.5535	0.9745	0.9992	0.9969	0.0043
	0.0405						
	0.05						
	0.06						

The similarity S_L (x) of f_h (x) and f_{WI} (x) can be found by combining the S_{PC} (x) and S_{GM} (x):

$$S_L(x) = \left[S_{PC}(x)\right]^{\alpha} \cdot \left[S_{GM}(x)\right]^{\beta}, \tag{5}$$

where α and β regulate the corresponding importance of PC and GM features. The values of α and β have been set to 1 for convenience.

The expression of FSIM can be computed in the following way

$$\text{FSIM} = \frac{\sum_{x\epsilon\Omega} S_L(x) \cdot \text{PC}_m(x)}{\sum_{x\epsilon\Omega} \text{PC}_m(x)}, \tag{6}$$

where Ω is the whole image spatial domain.

An additional mathematical tool, called gradient magnitude similarity deviation (GMSD) has been used to evaluate the performance of image quality assessment. To predict the overall image quality, GMSD analyses the exploit of global variation of the gradient-based local-quality map [36]. The gradient is normally computed by transforming an image with a linear filter. The GMS map is represented pixel-wise and serves as the local-quality map of the distorted image. The gradient magnitude similarity deviation (GMSD) can be calculated as follows:

$$\text{GMSD} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(\text{GMS}(i) - \text{GMSM})^2}, \tag{7}$$

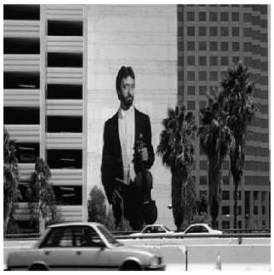
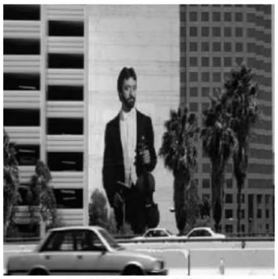
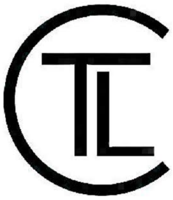
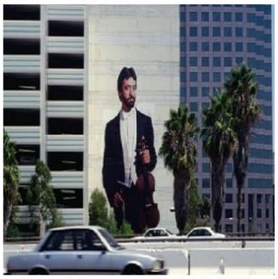
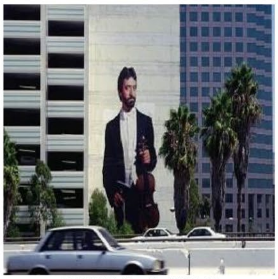
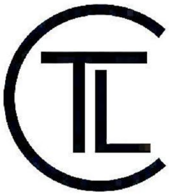
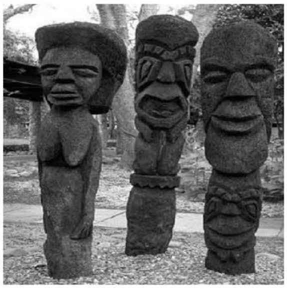
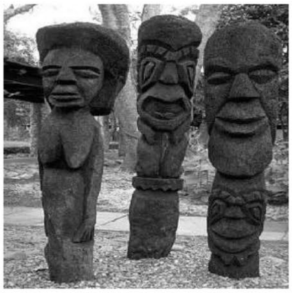
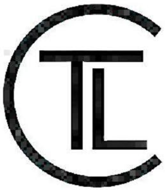
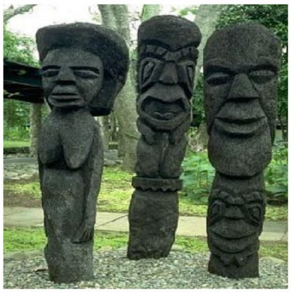
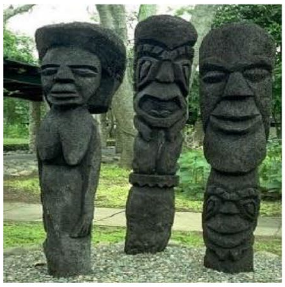
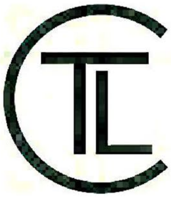
where, N is the total number of pixels in the image, GMS is the gradient magnitude similarity at location i, and GMSM is the gradient magnitude similarity map at location i.

The value of GMSD represents the range of magnitude of distortion in an image. The higher the GMSD score, the greater the distortion range, and hence, the lower the perceptual quality of the image.

Initially, the test is performed for the grayscale and colored version of the same host image. The scaling factor-alpha of the watermark image is chosen manually through a trial-and-error basis. The range beyond the values from 0.03 to 0.06 gives a drastic change of extracted watermark images. Thus, the scaling factor-alpha has been set within this range. Figure 6 shows the watermarked images of Lena (grayscale) and Lena (color) and the subsequent Table 1 displays the testimony of these images. The PSNR values of Lena (grayscale) and Lena (color) are found here as 43.8362 and 34.7266 dB. MSE, SSIM, NC, and FSIM values also validate the output. GMSD is a distortion index where a lower value indicates higher quality.

Furthermore, Figs. 7 and 8 indicate the watermarked images of grayscale and color formats of Zelda and penguin

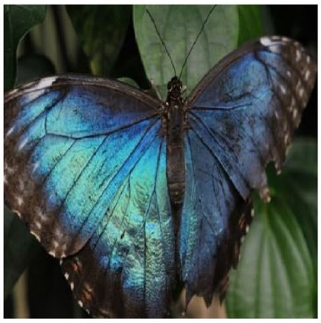
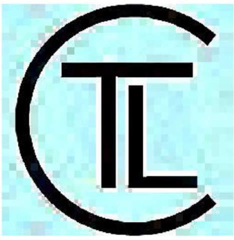
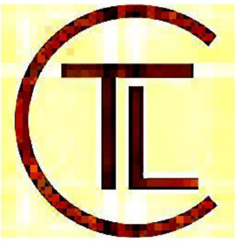
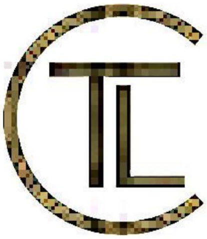
Fig. 9 Implementation of test images of Berkeley Segmentation Dataset

Image Name	Watermarked Image	Extracted Watermark
 Test image # 119082 [grayscale]	 FSIM: 0.9977 GMSD: 0.0041	 FSIM: 0.9415 GMSD: 0.1044
 Test image # 119082 [color]	 FSIM: 0.9976 GMSD: 0.0040	 FSIM: 0.9417 GMSD: 0.1044
 Test image # 101085 [grayscale]	 FSIM: 0.9975 GMSD: 0.0044	 FSIM: 0.8464 GMSD: 0.2142
 Test image # 101085 [color]	 FSIM: 0.9975 GMSD: 0.0044	 FSIM: 0.8490 GMSD: 0.2100

and the consecutive Tables 2 and 3 convey the values of those images. It can be seen that the PSNR values inclusive of MSE, SSIM, and NC of Zelda and penguin provide well-founded results for watermarked images and extraction of the watermark process. The value of FSIM is also on a normalized scale. GMSD identically shows a very good appraisal which indicates the minimal distortion between the host and the watermarked images.

The proposed method is also executed through some test images, taken from open-source databases, such as Berkeley

Fig. 10 Implementation of test images taken from THUR15000 dataset

Image Name	Watermarked Image	Extracted Watermark
 Butterfly	 FSIM: 0.9977 GMSD: 0.0036	 FSIM: 0.8842 GMSD: 0.2277
 CoffeeMug	 FSIM: 0.9979 GMSD: 0.0035	 FSIM: 0.8535 GMSD: 0.1995
 Giraffe	 FSIM: 0.9975 GMSD: 0.0044	 FSIM: 0.7917 GMSD: 0.2702

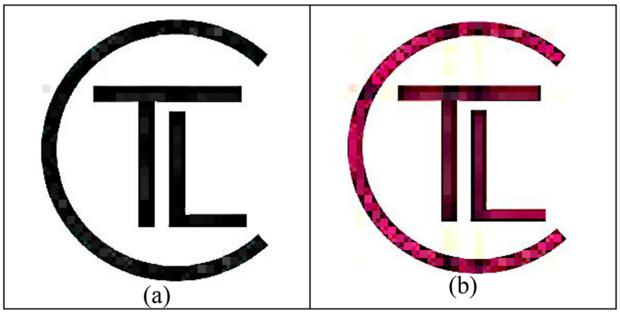


Fig. 11 Extracted watermark from **a** Lena (grayscale) and **b** Lena (color)

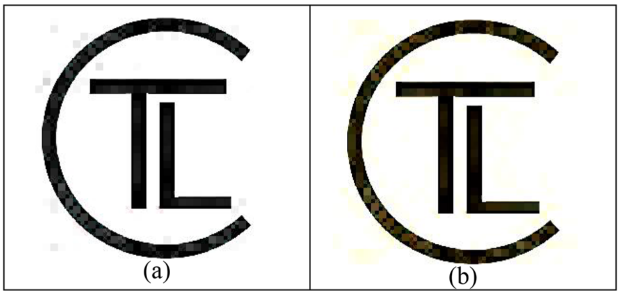


Fig. 12 Extracted watermark from **a** Zelda (grayscale) and **b** Zelda (color)

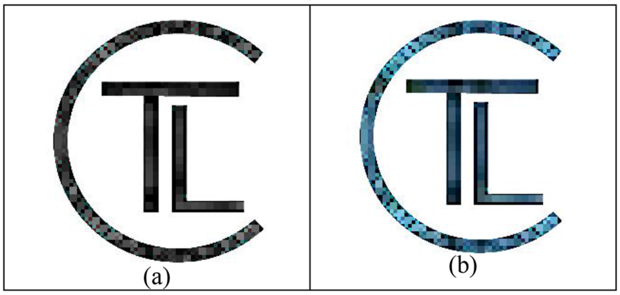


Fig. 13 Extracted watermark from **a** Penguin (grayscale) and **b** Penguin (color)

Table 4 PSNR, MSE, SSIM, and normalized coefficient (NC) of extracted watermark of Lena (grayscale) and Lena (color)

Image name	Scaling factor (alpha)	PSNR	MSE	SSIM	NC
Lena (grayscale)	0.03	24.5273	229.2717	0.8730	0.9915
	0.0405	26.1248	158.7102	0.8854	0.9934
	0.05	24.5168	229.88253	0.7865	0.9905
	0.06	16.4422	1.47e+03	0.6809	0.9751
Lena (color)	0.03	13.1160	3.1731e+03	0.7708	0.9780
	0.0405	15.8829	1.6780e+03	0.7772	0.9822
	0.05	17.1975	1.2397e−03	0.5651	0.9822
	0.06	15.1247	1.9981e+03	0.2654	0.9744

Table 5 PSNR, MSE, SSIM, and normalized coefficient (NC) of extracted watermark of Zelda (grayscale) and Zelda (color)

Image name	Scaling factor (alpha)	PSNR	MSE	SSIM	NC
Zelda (grayscale)	0.03	22.1221	398.9067	0.8489	0.9864
	0.0405	23.8825	265.9714	0.8466	0.9897
	0.05	19.2370	775.1358	0.6865	0.9800
	0.06	13.3743	2.98993+03	0.6528	0.9568
Zelda (color)	0.03	21.2145	491.6205	0.8409	0.9830
	0.0405	23.3645	299.6593	0.8000	0.9889
	0.05	19.6075	711.7574	0.3286	0.9897
	0.06	15.4228	1.8655e+03	0.2723	0.9813

Table 6 PSNR, MSE, SSIM, and normalized coefficient (NC) of the extracted watermark of Penguin (grayscale) and Penguin (color)

Image name	Scaling factor (alpha)	PSNR	MSE	SSIM	NC
Penguin (grayscale)	0.03	15.2000	1.9637e+03	0.7775	0.9572
	0.0405	19.1488	791.0350	0.8224	0.9776
	0.05	21.2233	490.6251	0.8388	0.9845
	0.06	22.6236	355.4041	0.8458	0.9879
Penguin (color)	0.03	11.3263	4.7912e+03	0.7369	0.9070
	0.0405	14.7251	2.1906e+03	0.7928	0.9495
	0.05	16.9044	1.3263e+03	0.8128	0.9665
	0.06	18.5946	898.7107	0.8236	0.9757

Segmentation Dataset (BSD) [37] and THUR15K dataset [38]. The values of FSIM and GMSD show the validation of the proposed method. Figures 9 and 10 illustrate the watermarked and extracted watermark images from different test images of the specified datasets.

Proof of Robustness

Robustness implies that how efficiently the watermark can be extracted from various types of attacks employed in the watermarked image. Both geometric and non-geometric attacks are considered for stability assessment. Geometric attacks include cropping, rotation, and scaling. JPEG compression, median filtering, average filtering, noise, and histogram equalization are dealt with non-geometric attacks [20]. The Figs. 9, 10, 11, 12 and 13 illustrate the retrieved watermark (without noise) from the watermarked image and Tables 4, 5, and 6 summarize the range of parameters used in interpretation purpose.

The following Table 7 shows the PSNR values that are retrieved from the several watermarked images under numerous attacks.

Table 8 summarizes the NC (normalized coefficient) values of the extracted watermark, recovered from multiple attacked watermarked images.

Table 9 indicates the comparison of the watermarked image and extracted watermark between the proposed method and existing methods for the grayscale image.

The NC (normalized correlation) values of the extracted watermark (grayscale image) from different attacks are shown in Table 10.

Table 7 PSNR values of different watermarked images under several attacks

AttackTypes Image	Gaussian Noise	Salt & Pepper Noise	Speckle Noise	Rotation (45)	Cropping (Centre)	Stretching	Histogram Equalization
Lena (grayscale)	22.7486	28.2034	31.0079	8.6259	12.5245	19.6259	43.8362
Lena (color)	22.6379	27.1944	28.7169	7.4978	12.9091	17.8495	34.7266
Zelda (grayscale)	22.6329	28.4315	31.9341	10.0036	15.3277	12.9917	39.5227
Zelda (color)	22.6340	28.1504	29.7252	8.9065	12.9289	14.6426	37.8992
Penguin (grayscale)	23.4751	26.9394	26.7432	4.2390	9.7350	29.0525	37.7796
Penguin (color)	23.2242	27.0539	26.2734	4.3304	10.7407	19.2806	36.1177

Table 8 NC (normalized coefficient) values of watermark extracted from attacked watermarked images

Attack Image	Noisy Gaussian	Salt and pepper noise	Speckle noise	Rotation (45)	Cropping	Stretching	Histogram equalization
Lena (grayscale)	0.9923	0.9932	0.9934	0.9762	0.9936	0.9962	0.9934
Lena (color)	0.9788	0.9813	0.9820	0.9865	0.9844	0.9943	0.9821
Zelda (grayscale)	0.9879	0.9892	0.9898	0.9559	0.9862	0.9952	0.9897
Zelda (color)	0.9865	0.9883	0.9889	0.9853	0.9859	0.9913	0.9889
Penguin (grayscale)	0.9737	0.9768	0.9775	0.9962	0.9911	0.9863	0.9776
Penguin (color)	0.9423	0.9480	0.9483	0.9968	0.9720	0.9904	0.9495

Table 9 Comparison chart of the proposed method with existing methods of Lena (grayscale)

Method	Watermarked image	Extracted watermark	
	PSNR	PSNR	NC
Tao [21]	42.38	–	1
Salama and Mokhtar [22]	41.28	30	–
Khanna et al. [23]	40.6926	–	–
Kusumaningrum et al. [24]	53.9215	–	1
Kang and Yang [25]	41.63	–	–
Wang and Zhao [8]	40.74	–	1
Proposed method	43.8362	26.1248	0.9934

Here is the chart in Table 11, which shows the comparison of the proposed method with existing methods for colored images.

The watermark extraction from the colored image under several attacks is compared in Table 12.

False-Positive Issue

In SVD-based watermarking system, different types of errors, such as message error, false-negative, and false-positive errors, can occur. The most significant problem in the SVD-based image watermarking scheme is a false-positive error. This error happens during the extraction of the watermark process. A transformation technique along with SVD can resolve the issue. In this paper, we have applied multi-level DWT transform accompanying SVD to mitigate this error. Owing to DWT transform and to find out the singular values of LL and HH edges of host and watermark image and embed those singular values into the host part could inhibit the false-positive fallacy.

Table 11 Comparison chart of the proposed method with existing methods of Lena (color)

Method	Watermarked image	Extracted watermark
	PSNR	NC
Sharma and Jain [26]	52.92	–
Xie et al. [27]	43.2552	–
Mohammed et al. [28]	45.833	–
Harjito and Suryano [10]	48.9727	0.919262
Naik et al. [7]	32.47	0.9929
Proposed method	34.7266	0.9822

Conclusion

This paper proposed an improved DWT–SVD-based hybrid approach which is proved to be a good mechanism for both grayscale and color images. The blending of the 1st level and the 2nd level of singular values are inserted into the lower-level and higher-level frequency regions of the cover image. It is said that adding singular values in the host image cause false-positive results, but our proposed approach has overcome this issue. We have applied our method in three types of duo images (grayscale and color) to exhibit the outcome. The authenticity and robustness are found at an acceptable rate for both types of images using the proposed method. More efforts will be taken in near future for further improvement of the imperceptibility and robustness, such as the incorporation of the modified Fibonacci sequence for watermark encryption and particle swarm optimization (PSO) for embedding purposes. We will also work on infusing multiple watermarks with the host image for more flexibility.

Table 10 Comparison of NC value of watermark extraction under several attacks of Lena (grayscale)

Attack	[8]	[24]	[25]	[17]	Proposed method
Gaussian noise	0.9959	0.9541	0.9157	0.9588	0.9923
Salt and pepper noise	0.9868	0.8840	0.9391	0.9850	0.9932
Speckle noise	0.9955	–	–	–	0.9934
Histogram equalization	0.8176	–	1	–	0.9934

Table 12 Comparison of NC value of watermark extraction under several attacks of Lena (Color)

Attack	[27]	[28]	[10]	[29]	[30]	Proposed method
Gaussian noise	0.9734	0.9543	0.5748	0.5946	0.9368	0.9923
Salt and pepper noise	0.9625	0.7639	0.0080	0.6006	0.9715	0.9932
Speckle noise	–	–	–	–	0.9774	0.9934
Histogram equalization	–	–	–	0.5137	0.9223	0.9934
Cropping	0.9142	–	0.0154619	0.8224	–	0.9844

Acknowledgements The authors are thankful to the ICT Division under the Ministry of Posts, Telecommunication and Information Technology, Government of the Peoples Republic of Bangladesh for Ph.D. Fellowship to Fauzia Yasmeen to conduct this research.

Funding No funding is received for this research.

Compliance with Ethical Standards

Conflict of interest The authors declare that they have no conflict of interest.

Ethical Approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Tarhouni N, Charfeddine M, Amar CB. Novel and robust image watermarking for copyright protection and integrity control. Circuits Syst Signal Process. 2020;39(10):5059–103.
2. Zhang L, Xiao JW, Luo JY. A robust color image watermarking based on SVD and DWT. Int J Commun (IJC). 2014;3:62.
3. Akter A, Nur-E-Tajnina, Ullah MA. Digital image watermarking based on DWT-DCT: evaluate for a new embedding algorithm. In: 3rd International conference on informatics, electronics and vision (ICIEV), Dhaka, p. 1–6, 2014.
4. Kumar S, Dutta A. Performance analysis of spatial domain digital watermarking techniques. In: International conference on information communication and embedded system (ICICES). Chennai, p. 1–4, 2016.
5. Singh RK, Shaw DK, Sahoo J. A secure and robust block-based DWT–SVD image watermarking approach. J Inf Optim Sci. 2017;38:11–925.
6. Sanku D, Kiran S, Takore TT, Kumar PR. Digital image watermarking in RGB host using DWT, SVD, and PSO techniques. In: Proceedings of 2nd international conference on micro-electronics, electromagnetics and telecommunications (Springer Nature), p. 333–342, 2018.
7. Naik NS, Naveena N, Manikantan K. Robust digital image watermarking using DWT+SVD approach. In: IEEE International conference on computational intelligence and computing research, Madurai, p. 1–6, 2015.
8. Wang B, Zhao P. An adaptive image watermarking method combining SVD and Wang-Landau sampling in DWT domain. Mathematics. 2020;8:691.
9. Shahrezaee M, Razmjooy N. Image watermarking based on DWT–SVD. In: Proceedings of the 2nd international conference on combinatorics, cryptography and computation, p. 62–67, 2017.
10. Harjito B, Suryani E. Robust image watermarking using DWT and SVD for copyright protection. In: AIP Conference proceedings, 2017.
11. Gonge SS, Ghatol A. A robust and secure DWT–SVD digital image watermarking using encrypted watermark for copyright protection of cheque image. In: International symposium on security in computing and communications, p. 290–303, 2015.
12. Kallianpur AK, Bharath MV, Manikantan K. Digital image watermarking using optimized transform-domain approach. In: IEEE UP section conference on electrical computer and electronics (UPCON), Allahabad, p. 1–6, 2015.
13. Parah SA, Ashraf S, Asharf A. Robustness analysis of a digital image watermarking technique for various frequency bands in DCT domain. In: IEEE International symposium on nanoelectronic and information systems, Indore, 2015. p. 57–62.
14. Fazli S, Moeini M. A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks. Optik (Elsevier). 2016;127(2):964–72.
15. Emek S, Pazarci M. A cascade DWT–DCT based digital watermarking scheme. In: 13th European signal processing conference, Antalya, p. 1–4, 2005.
16. Aparna JR, Sonal A. Comparison of digital watermarking techniques. In: International conference on computation of power, energy, information and communication (ICCPEIC), Chennai, p. 87–92, 2014.
17. Khan M, Kushwaha A, Verma T. A new digital image watermarking algorithm based on image interlacing, DWT, DCT. In: International conference on industrial instrumentation and control (ICIC) College of Engineering Pune, India, p. 885–890, 2015.
18. Bansal N, Bansal A, Deolia V, Pathak P. Comparative analysis of LSB, DCT, and DWT for digital watermarking. In: 2nd International conference on computing for sustainable global development (INDIACom), New Delhi, p. 40–45, 2015.
19. Patel R, Bhatt P. A review paper on digital watermarking and its techniques. Int J Comput Appl. 2015;110(1):10–3.
20. Zope-Chaudhari S, Venkatachalam P. Robust copyright protection of raster images using wavelet-based digital watermarking. In: IEEE Geoscience and remote sensing symposium, Quebec City, QC, p. 3129–3132, 2014.
21. Wang T. Digital image watermarking using dual-scrambling and singular value decomposition. In: IEEE International conference on computational science and engineering (CSE) and IEEE international conference on embedded and ubiquitous computing (EUC), Guangzhou, p. 724–727, 2017.
22. Salama AS, Mokhtar MA. Combined technique for improving digital image watermarking. In: 2nd IEEE international conference on computer and communications (ICCC), Chengdu, 2016, p. 557–562, 2016.
23. Khanna AK, Roy NR, Verma B. Digital image watermarking and its optimization using genetic algorithm. In: International conference on computing, communication, and automation (ICCCA), Noida, p. 1140–1144, 2016.
24. Kusumaningrum DP, Rachmawanto EH, Sari CA, Pradana RP. DWT–SVD combination method for copyrights protection. Sci J Inform. 2020;7(1):311.
25. Kang Q, Li K, Yang J. A digital watermarking approach based on DCT domain combining QR code and chaotic theory. In: IEEE

10th International conference on intelligent computer communication and processing (ICCP), Cluj Napoca, p. 331–337, 2014.

26. Sharma P, Jain T. Robust digital watermarking for coloured images using SVD and DWT technique. In: IEEE International advance computing conference (IACC), Gurgaon, p. 1024–1027, 2014.
27. Xie Y, Wang Y, Ma M. Design of a hybrid digital watermarking algorithm with high robustness. J Web Eng. 2020;19(5–6):716.
28. Mohammed AA, Salih DA, Saeed AM, Kheder MQ. An imperceptible semi-blind image watermarking scheme in DWT–SVD domain using a zigzag embedding technique. Multimedia tools and applications. New York: Springer; 2020.
29. Singh N, Joshi S, Birla S. Color image watermarking with watermark authentication against false positive detection using SVD. Int Conf Sustain Comput Sci Technol Manag. 2019;195:725–46.
30. Roy S, Pal AK. A hybrid domain color image watermarking based on DWT–SVD. Iran J Sci Technol Trans Electr Eng. 2019;2:201–17.
31. Arora SM. A DWT–SVD based robust digital watermarking for digital images. Proced Comput Sci. 2018;132:1441–8.
32. Kadian P, Arora N, Arora SM. Performance evaluation of robust watermarking using DWT–SVD and RDWT–SVD. In: 6th International conference on signal processing and integrated networks (SPIN), Noida, India, p. 987–991, 2019.
33. Pathak Y, Dehariya S. A more secure transmission of medical images by two label DWT and SVD based watermarking technique. In: International conference on advances in engineering and technology research (ICAETR—2014), Unnao, p. 1–5, 2014.
34. Furqan A, Kumar M. Study and analysis of robust DWT–SVD domain based digital image watermarking technique using MATLAB. In: IEEE international conference on computational intelligence and communication technology, Ghaziabad, p. 638–644, 2015.
35. Sara U, Akter M, Uddin MS. Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study. J Comput Commun. 2019;7:8–18. https://doi.org/10.4236/jcc.2019.73002.
36. Zhang L, Zhang L, Mou X, Zhang D. FSIM: a feature similarity index for image quality assessment. IEEE Trans Image Process. 2011;20(8):2378–86. https://doi.org/10.1109/TIP.2011.2109730.
37. The Berkeley Segmentation Dataset (BSD). https://www2.eecs.berkeley.edu/Research/Projects/CS/vision/bsds.
38. THUR15K Dataset. http://mmcheng.net/gsal/.

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