

A robust watermark algorithm for copyright protection by using 5-level DWT and two logos

Alaa Rishkek Hoshi¹, Nasharuddin Zainal², Mahamod Ismail³, Abd Al-Razak T. Rahem⁴,
Salim Muhsin Wadi⁵

^{1,2,3}Department of Electrical, Electronic and Systems Engineering, Universiti Kebangsaan Malaysia (UKM), Malaysia

⁴Department Electrical Engineering Technical College, Middle Technical University (MTU), Iraq

⁵Department Communication techniques Engineering, Al-Furat Al-Awsat Technical University (ATU), Iraq

Article Info

Article history:

Received Oct 22, 2020

Revised Mar 27, 2021

Accepted Mar 31, 2021

Keywords:

Copyright protection

Discrete wavelet transforms

Frequency domain

Information security

Watermarking

ABSTRACT

Recent growth and development of internet and multimedia technologies have made it significant to upload data; however, in this situation, the protection of intellectual property rights has become a critical issue. Digital media, including videos, audios, and images are readily distributed, reproduced, and manipulated over these networks that will be lost copyright. Also, the development of various data manipulation tools like PDF converter and photoshop editor has resulted in digital data copyright issues. So, a digital watermarking technique has emerged as an efficient technique of protecting intellectual property rights by providing digital data copyright authentication and protection. In this technique, a watermarked document was integrated into electronic data to prevent unauthorized access. In this paper, A robust watermark algorithm based on a 5-level DWT and two log was proposed to enhance the copyright protection of images in unsecured media. Our lab results validate that our algorithm scheme is robust and forceful against several sets of attacks, and high-quality watermarked image was achieved, where the algorithm was assessed by computation of many evaluation metrics such as PSNR, SNR, MAE, and RMSE.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Alaa Rishkek Hoshi

Department of Electrical, Electronic and Systems Engineering

Universiti Kebangsaan Malaysia (UKM)

43600 UKM, 43600 Bangi, Selangor, Malaysia

Email: p98735@siswa.ukm.edu.my

1. INTRODUCTION

In the current digital world, transferring large chunks of data over the internet-via multiple hierarchies-has made it significantly difficult to protect and identify the ownership of digital media. Thus, the watermark technique has been introduced as a potential solution for copyright protection, authorization, identification, and ownership [1]. With the help of digital watermarking, a user can send his/her personal information on the internet without getting worried about its manipulation or disclosure, whether unintentionally or intentionally. Subsequently, digital watermarking also helps in resisting various digital security challenges like identity theft, fraud, and counterfeiting [2]. Moreover, it can bring social and economic benefits by protecting the personal and collective information of users. In the field of medical science, digital watermarking has major significance, as it saves bandwidth requirements and storage space while ensuring high confidentiality of patient data. In this regard, digital watermarking yields several social and economic benefits like maintaining the confidentiality of patient's medical images i.e., their organs, while

eliminating any after-effects of record's tampering that could potentially risk an individual's life due to wrong diagnosis [3]. Additionally, digital watermarking also helps in ensuring a high level of national defense-security and social-economic development of vector maps. It is done by protecting geospatial information by preventing malicious tampering and unauthorized copy of digital data [4]. Thus, with the help of digital watermarking schemes, legitimate users or copyright owners can dynamically trace the circulation and transmission of digital products through concealed watermark information; hence, ensuring, the integrity of digital information.

Moreover, with the availability of various image processing tools like PDF converters and photoshop editors, ordinary people can easily modify the contents of the image which further leads to copyright dispute [5]. However, with the introduction of digital watermarking schemes, users can address copyright protection challenges. For copyright protection, digital watermarking satisfies two crucial conditions, i.e. imperceptibility, and robustness [6], [7]. Here, imperceptibility indicates that the watermarked image quality cannot be easily influenced. This means that the naked eyes cannot spot the traces of watermark embedding. Robustness, however, indicates high protection against distorted attacks; thereby, making digital watermarking excellent for copyright protection. Also, the most prominent application of digital watermarking is the protection of digital images from manipulation and illegal copying. Digital watermarking embeds information in the files while providing data that can further be used for authentication. As a result, it reduces the risk of information being copied unless instructed by the authorized personnel [8], [9]. The copy protection application is based on the threshold correlation between a pseudorandom sequence and an extracted vector. As the probability threshold decreases, the robustness increases which further leads to the prevention of unauthorized copying of the files.

This paper aims to accomplish, characterize and understand the current techniques that are utilized in watermarking, to propose a new algorithm for preventing the intellectual property rights of images on unsecured media, and to evaluate the suggestion algorithm by applying different attack techniques, the rest of this article is structured as follows. Section 2 investigates the relevant literature review related to our field of interest. Section 3 discusses the challenges and limitations of digital watermarking, while Section 4 illuminates the proposed algorithm for both embedded and extract processing. Section 5 presents result and discussion where human visual quality tested and, and many performance evaluation metrics were applied such as PSNR, SNR, MAE, and RMSE to evaluate the quality of the proposed algorithm, in addition to the test of a set of attacks and extraction after attacks were also presented. Finally, Section 6 concludes the paper.

2. LITERATURE REVIEW

In the literature, the robust watermarking schemes are characterized into two categories that include spatial and frequency domain schemes. In this research, we will concentrate on a frequency domain and will explain it in detail in the next paragraphs.

2.1. Frequency domain

Unlike the spatial domain, frequency domain schemes generally enable more robustness against multiple attacks and make it more difficult for images to be perceived. This is because, in this scheme, the watermark is embedded within the original image's transformed coefficient by trading off imperceptibility [1]. Moreover, its computational capacity and data hiding ability are more than the spatial domain; hence, making it more preferable. Some of the techniques of frequency domain are discussed below:

2.1.1. Discrete cosine transform (DCT)

Discrete cosine transform (DCT) is the most popular type of frequency domain transformation that divides a digital image into the cosine and sine frequencies, having distinct amplitudes [10], [11]. Due to this capability, DCT is highly favored in the data compression field and pattern recognition. Moreover, DCT transforms the digital image, using fourier transformation, into easy segments of frequencies [12]. The algorithm then splits the image into 8x8 non-overlapping blocks which are further used for embedding the secret information into the coefficients of the image. This allows DCT to represent data in frequency space instead of in the amplitude space. This ability makes DCT more robust against different digital image processing operations, such as contrast adjustments, brightness, and filtering. However, they are not only difficult to implement but also computationally expensive [13]. Moreover, they are vulnerable against geometric attacks, including cropping, scaling, and rotation. Regardless of its limitations, DCT expresses finite data point sequences at oscillating frequencies, which makes it highly effective in different applications like digital signal processing, reducing network bandwidth, and finding solutions of partial differential equations.

2.1.2. Discrete wavelet transforms (DWT)

Discrete wavelet transforms (DWT) is a widely used, modern technology that facilitates different operations like watermarking, image compression, and digital signal processing. However, because of its excellent multiresolution and spatial localization characteristics, DWT is widely been utilized in digital watermarking [14], [15]. Moreover, it is an efficient mathematical tool that is optimum for the hierarchical decomposing of digital images. At each level, the decomposition of images takes place into four sub-brands: three high-frequency sub-brands, namely HH, LH, and HL, and one low-frequency sub-brand (LL) see Figure 1 [1]. The high-frequency parts are used for digital watermarking while the low-frequency part plays a critical role in the extraction of the watermark. Accordingly, DWT incorporates wavelet filters that contain floating-point coefficients. These wavelets are created by translations and dilations of a fixed mother wavelet function. As a result, the wavelets provide both spatial and frequency description of an image. The importance of wavelet decomposition rests upon its capability to decompose the image matrix at a dynamic scale [16]. Due to this ability, DWT is excellent for multiresolution analysis that has compatibility with compression standards and energy compression characteristics [17]. This makes DWT great against compression and noise attacks.



Figure 1. Decomposition levels of DWT [10]

2.1.3. Discrete fourier transform (DFT)

In the watermarking scheme, discrete fourier transforms (DFT) is rotation resistant and translation invariant that makes it strong against geometric attacks, such as translation, cropping, rotation, and scaling [13]. It provides frequency components by transforming a continuous function. Due to its translation invariance attribute, spatial shifts of the digital image only impact the phase representation and not the magnitude representation of the image. Moreover, since DFT is a scaling, translation, and rotation invariant, it can be utilized to recover from geometric distortions, unlike DWT and DCT [10]. Despite its various benefits, DFT's implementation is highly complex and requires high computing cost. These features make it an unfavorable option, compared to DCT and DWT.

3. CHALLENGES AND LIMITATIONS OF DIGITAL WATERMARKING

There are multiple technical challenges and limitations in digital watermarking research. The imperceptibility and robustness trade-off makes the research very interesting. To obtain imperceptibility, the watermark should be integrated into the original signal's high-frequency components [18]. On the contrary, the watermark should be added to the low-frequency components of the original signal to obtain robustness. Thereby, the watermarking technique can be successful if the original signal's low-frequency components are utilized as the host for watermark insertion. Considering this aspect, there are multiple technical limitations and challenges related to digital watermarking, including properties of a visual signal and the human visual system (HVS).

3.1. Properties of visual signal

Since videos and images are visual signals, it is essential to comprehend the response of visual signals so that new and optimum ways could be discovered to hide information. Commonly, visual signals are recognized as space and time versus intensity of video scenes and space displays versus intensity of image information and amplitude plots. These types of waveforms can reveal critical information regarding the attributes of the signals, which could potentially endanger the robustness of the watermark [19]. Although watermarks can be embedded in irrelevant visual parts of the digital image to enhance the watermark invincibility, the robustness is negatively affected. Some of the visual signal properties are non-stationary and periodicity.

3.1.1. Non-stationary

The non-stationary property of the digital watermarking scheme is common to all signals. Video or image signals incorporate rich segments of slowly or flatly altering intensity, in addition to textured and edges regions. While it is crucial to preserve edges for sustaining the perceptual quality, the textured regions, however, need to be skillfully utilized to accumulate additional information. In addition to this, the estimation problem concerning noise framework for non-stationary noise is more challenging [20]. This is because the parameters ought to be approximated in small patches. Furthermore, due to the absence of statistically authentic and reliable information, the majority of the known digital watermarking techniques generate and overestimate values of noise variances, particularly for image regions having edges and textured regions. Non-stationary property is inherent in multiple image formation systems like maritime radars and side-look radar imaging. Thus, for practical de-noising, it is important to obtain accurate noise variance estimates.

3.1.2. Periodicity

There exist frame-to-frame and line-to-line periodicity in video and image signals. They are not entirely periodic, but there is a redundancy between the lines and frames that notably exist. These redundancies are often exploited in almost every compression scheme. Moreover, it is undeniable that digital watermarking is usually heuristic-based and periodic [21]. The limitation of such a watermarking scheme is its rigidity, concerning the data delay frequency as well as data arrival.

3.2. Properties of human visual system (HVS)

The success and foundation of any digital watermarking technique depend on the efficient utilization of the human visual system (HVS). It can be argued that imperceptibility and robustness are two conflicting digital watermarking challenges and lack of efficient use of HVS systems can significantly endanger the security of watermarking schemes [22]. One such challenge of digital watermarking is texture sensitivity. The background texture serves as the foundation for the visibility of distortion. If the background texture is strong and concentrated, the visibility distortion will be low. Also, in a strong textured image block, the energy favors even distribution within DCT coefficients. On the other hand, in a flat-featured image portion, the energy is intensive on components that have a lower frequency. This means that more watermark signals can be added to strong textured regions.

3.3. Brightness sensitivity

In the presence of backgrounds having a different level of intensity, the human eye is sensitive in discerning a low-intensity signal. As the intensity level of the surrounding region increases, the relative intensity present in the dark areas is lowered, while the sensitivity in areas, having a light background increase [23]. When the mean noise square value is identical to that of the background, the noise square inclines to be visible, a background having a mid-grey feature. This means that at low-intensity levels, the human eye has a high level of sensitivity, while at high-intensity levels the sensitivity is relatively lower.

4. THE PROPOSED ALGORITHM

In this research, the proposed algorithm is based on the 5-level DWT watermarking technique which utilizes translation and wavelet features of the wavelet domain at different levels. The first logo is recommended to be embedded in three locations (LH2, HL2, and HH2). Similarly, it is suggested that secondary watermarks should be embedded in three locations (LL1, LL3, and LL5). The embedding watermarking scheme is depicted in the proposed watermarking algorithm, as shown in Figure 2. The watermark image is sized at 512x512 and the host image size is also kept at 512x512.

4.1. Proposed algorithm: embedded processes

Assume we have a host image $Hi(i,j)$ (512×512) this host image considered as a cover host image, and assume that we have a logo image $Li1(i,j)$ (512×512) as a first logo image and $Li2(i,j)$ (512×512) as a second logo image, the first process is to obtain the image $Wi1(i,j)$ (512×512) where DWT watermarking apply and first logo where embedded in certain location-based in our suggestion algorithm as shown in Figure 2, this will resulting our first watermarked image $Wi1(i,j)$, the same procedure can be followed to obtain the second watermarked image $Wi2(i,j)$ as well. Therefore, the summation of $Wi1(i,j)$ and $Wi2(i,j)$ resulting in our final watermarked image $Wi(i,j)$ following mathematical (1),(2), and (3) can represent the equations used in the embedding process.

$$Wi1(i,j) = Hi(i,j) + Li1(i,j) \quad (1)$$

$$Wi2(i,j) = Hi(i,j) + Li2(i,j) \tag{2}$$

$$Wi(i,j) = (Wi1(i,j) + Wi2(i,j)) / 2 \tag{3}$$

4.2. Proposed algorithm: extraction processes

Assume we have both host image $Hi(i,j)$ (512×512), and watermarked image $Wi(i,j)$ then we can execute a subtraction operation among host image $Hi(i,j)$ and the watermarking image $Wi(i,j)$ then apply a certain sub-bands extraction based on the location that used in our suggestion algorithm as shown in Figure 2, After this process, we can obtain the first logo image $Wi1(i,j)$ and second logo image $Wi2(i,j)$, following mathematical (4) and (5) can represent the equations used in the extraction process.

Our laboratory experiment implemented out by using MATLAB code and our suggestion algorithms shown in Figure 3, this code was accomplished utilizing using a structured one well fragment code to guarantee the quality and effectiveness of the code performances. Figure 2 shows the overall work procedure of the suggested algorithms for both the embedded and extraction process, while Figure 3 shows the entire process along with a set of attacks that were applied, in addition to the evaluation process.

$$Wi1(i,j) = Hi(i,j) - Wi(i,j) \tag{4}$$

$$Wi2(i,j) = Hi(i,j) - Wi(i,j) \tag{5}$$

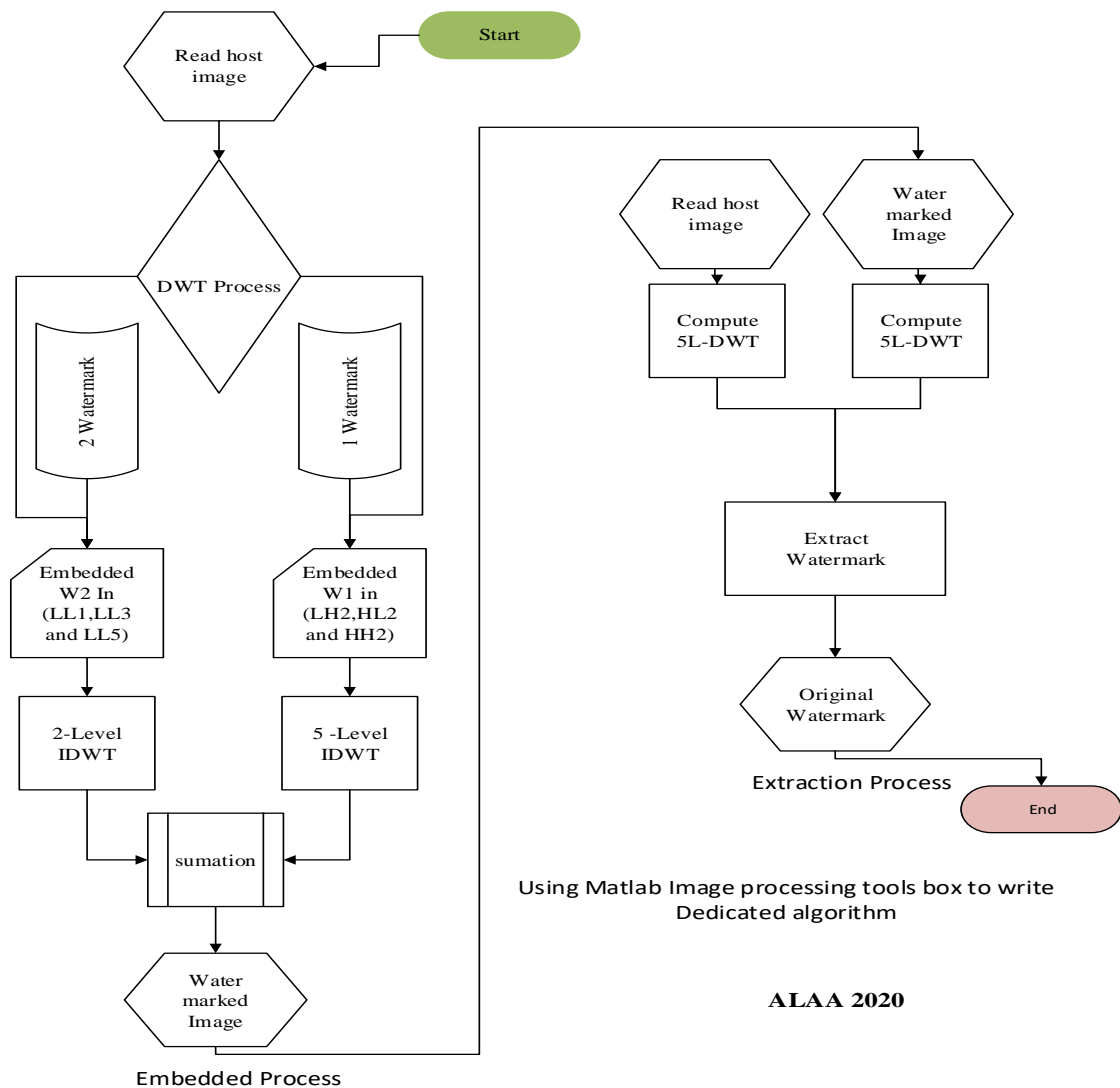


Figure 2. Embedded and extraction process in proposed algorithm

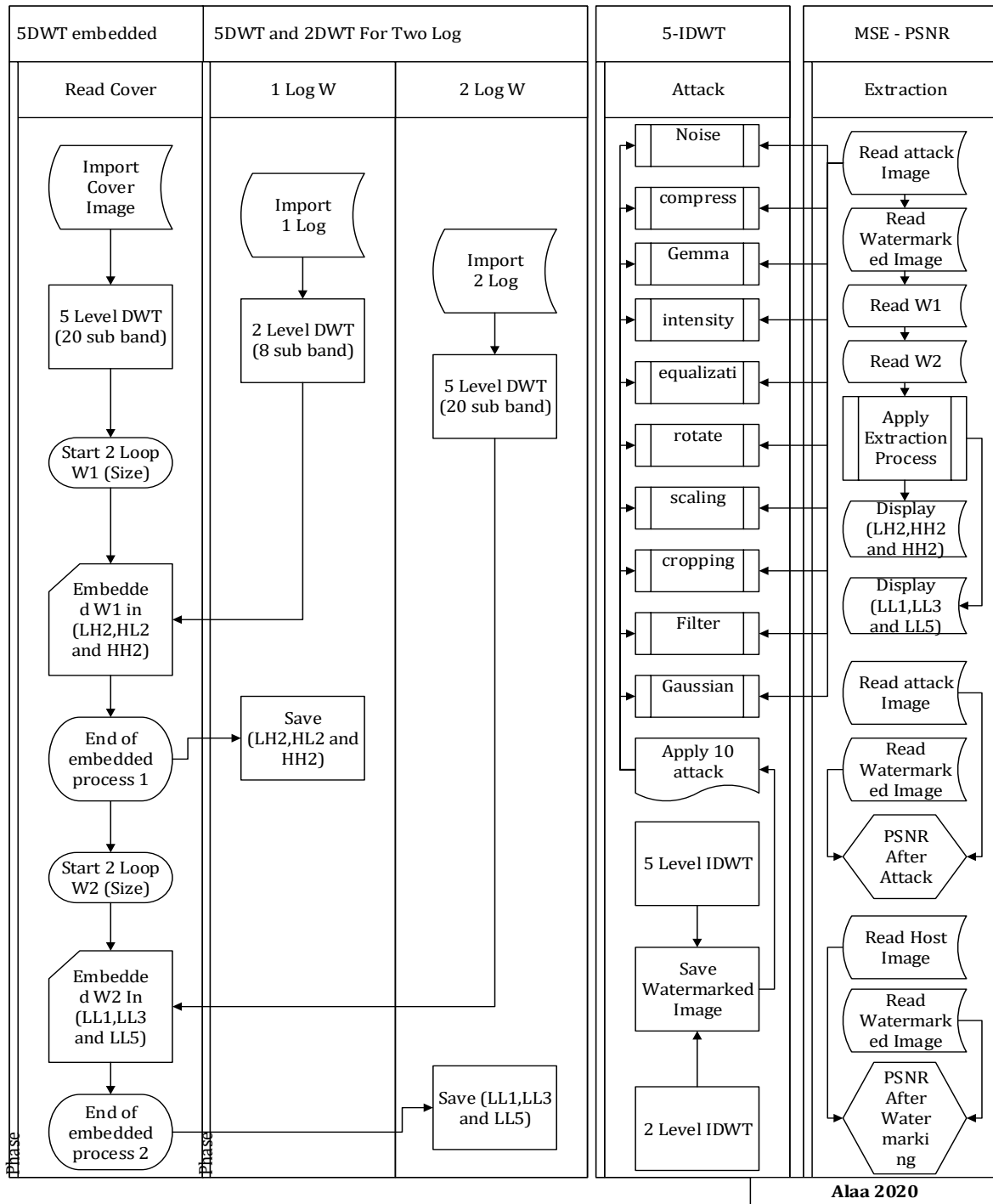


Figure 3. Proposed algorithm scheme

5. RESULTS AND DISCUSSION

5.1. Experimental results: human visual quality

The performance of the proposed watermarking scheme is examined by performing multiple experiments on different grayscale images, each having a size of 512x512. These greyscale test images include girlface, Lena, Muhammad Ali, perm, and thumbnail, Table 1 demonstrates eight test images together with watermarked images. Besides, Table 1 also demonstrates the logos used, while Figure 4 presents the decomposition and position of two watermarks in girlface cover image.

Table 1. Host images together with watermarked images and watermark logo used

Covered image	Watermarked image	Logo 1	Logo 2
 girlface	 Watermarkedimage	 Logo1	 Logo2
 thumbnailG	 Watermarkedimage	 Logo1	 Logo2
 permG	 Watermarkedimage	 Logo1	 Logo2
 lena	 Watermarkedimage	 Logo1	 Logo2
 MuhammadAliG	 Watermarkedimage	 Logo1	 Logo2

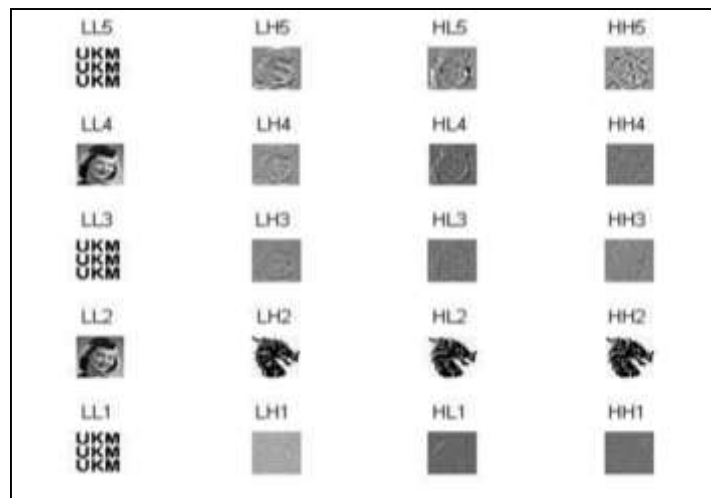













Figure 4. Decomposition and position of two watermark in girlface cover image for human visual observation

5.2. Experimental results: after apply set of attacks

For testing the performance and robustness of the proposed design, our watermarked images were tested through the application of different types of attacks, using MATLAB. These attacks include Gaussian, filtering, cropping, rotating, equalization, resizing, gamma, intensity, Hostr75, and noise attack. The attack parameters and attacked images for girlface, Lena, and permG are shown in Tables 2 and 3, respectively.

From the values obtained above, we can conclude that the algorithm used was good in repelling various types of attacks, although the distortion results obtained in the rotate test, and the image quality obtained remains good for visual observation












Table 2. Watermarked-after attacked images and parameters

No:	Name	Girlface Parameters	Result Image	No:	Name	Girlface Parameters	Result Image
1.	Watermarked image	2 Logo	 Watermarkedimage	7.	ResizeAFT	Automatic	 ResizeAFT
2.	Gaussian	Mean = 0 Variance = 0.001	 Gaussian	8.	Gamma	[l=0 h=0.8] [b=0 t=1]	 Gamma
3.	Filter	Window Size = 3x3	 Filter	9.	Intensity	1.5	 Intensity
4.	Crop	On both sides	 crop	10.	Hostr75	Q = 75	 hostr75
5.	Rotate	512x256	 Rotate	11.	Noise	0.02	 Noise
6.	Equal	20°	 Equal				

5.3. Experimental results: image quality evaluation

To examine the performance of the watermarked images, the present study considered some quality measures, including SNR, PSNR, RMSE, and MAE. Additionally, J's plugin was used to analyze the quality of the images. This plugin used the test image $T_i(a,b)$ to compare it with the reference image $R_i(a,b)$. The two selected images should be identical having the size of $[na, nb]$. The calculation of SNR, PSNR, RMSE, and MAE is given as:

Table 3. Parameters and attacked images for lena

No:	Name	Lena Parameters	Result Image	No:	Name	Lena Parameters	Result Image
1.	Watermarked image	2 Logo	 Watermarkedimage	7.	ResizeAFT	Automatic	 ResizeAFT
2.	Gaussian	Mean = 0	 Gaussian	8.	Gamma	[l=0 h=0.8]	 Gamma
3.	Filter	Variance = 0.001	 filter	9.	Intensity	[b=0 t=1]	 Intensity
4.	Crop	Window Size	 crop	10.	Hostr75	1.5	 hostr75
5.	Rotate	= 3×3	 rotate	11.	Noise	Q = 75	 Noise
6.	Equal	On both sides	 equal				

5.3.1. Signal to noise ratio (SNR)

Signal to noise ratio (SNR) is responsible for calculating the imaging sensitivity [24]. This indicates that the strength of the signal is relative to the noise in the background. Mathematically, it can be expressed as the following mathematical (6):

$$SNR = 10. \log 10 \left[\frac{\sum_0^{N_a-1} \sum_0^{N_b-1} [Ri(a,b)]^2}{\sum_0^{N_a-1} \sum_0^{N_b-1} [Ri(a,b) - Ti(a,b)]^2} \right] \tag{6}$$

5.3.2. Peak signal to noise ratio (PSNR)

PSNR measures the level of degradation of the embedded image in accordance with the host image [14]. This is achieved by taking the ratio of maximum signal power and corruption noise power. Mathematically, PSNR can be calculated as the following mathematical (7):

$$PSNR = 10. \log 10 \left[\frac{Max (Ri(a,b))^2}{\frac{1}{N_a N_b} \sum_0^{N_a-1} \sum_0^{N_b-1} [Ri(a,b) - Ti(a,b)]^2} \right] \tag{7}$$

5.3.3. Root mean square error (RMSE)

Root mean square error (RMSE) compares two meshes [25]. Mathematically, it can be expressed as the following mathematical (8):

$$RMSE = \sqrt{\frac{1}{N_a N_b} \cdot \sum_0^{N_a-1} \sum_0^{N_b-1} [Ri(a, b) - Ti(a, b)]^2} \tag{8}$$

5.3.4. Mean absolute error (MAE)

Mean absolute error (MAE) calculates the average error magnitude. Mathematically, it can be represented as the following mathematical (9):

$$MAE = \frac{1}{N_a N_b} \cdot \sum_0^{N_a-1} \sum_0^{N_b-1} [Ri(a, b) - Ti(a, b)] \tag{9}$$

In the experiment, various standard host images, such as girlface, Lena, Muhammad Ali, permG, and thumbnailG were taken to test the proposed watermarked technique. Additionally, 11 types of different attacks were also applied to examine the performance of the scheme. Once the watermarking process was completed, SNR, PSNR, RMSE, and MAE were calculated as shown in Table 4(a) and (b), Table 5(a) and (b), Table 6(a) and (b). SNR and PSNR test result show very good and high value which mean that our suggestion algorithm used is robust to preserve image quality where our host image (girlface) was used as a reference for test mechanism.

Table 4 (a). Girlface cover image

girlface Cover Image used as a reference image					
Ref. Image	Test Image	SNR (dB)	PSNR (dB)	RMSE	MAE
girlface.png	Watermarkedimage.png	61.960	68.431	0.078	0.006
girlface.png	Gaussian.png	21.996	28.467	7.808	6.144
girlface.png	Filter.png	24.862	31.333	5.614	2.858
girlface.png	crop.png	4.856	11.327	56.182	26.775
girlface.png	ResizeAFT.png	25.468	31.939	5.236	2.861
girlface.png	Rotate.png	3.401	9.872	66.426	47.142
girlface.png	Equal.png	5.765	12.236	50.597	44.066
girlface.png	Intensity.png	12.016	18.487	24.637	20.980
girlface.png	Gamma.png	10.042	16.513	30.925	28.273
girlface.png	hostr75.png	30.297	36.768	3.002	2.063
girlface.png	Noise.png	13.723	20.194	20.242	2.526

Table 4 (b). Girlface watermarked image

girlface watermarked image used as a reference image					
Ref. Image	Test Image	SNR (dB)	PSNR (dB)	RMSE	MAE
Watermarkedimage.png	Gaussian.png	21.997	28.468	7.808	6.144
Watermarkedimage.png	Filter.png	24.862	31.332	5.614	2.858
Watermarkedimage.png	crop.png	4.856	11.327	56.184	26.771
Watermarkedimage.png	ResizeAFT.png	25.468	31.939	5.236	2.861
Watermarkedimage.png	Rotate.png	3.402	9.872	66.426	47.142
Watermarkedimage.png	Equal.png	5.767	12.237	50.591	44.060
Watermarkedimage.png	Intensity.png	12.018	18.489	24.631	20.974
Watermarkedimage.png	Gamma.png	10.041	16.511	30.930	28.279
Watermarkedimage.png	hostr75.png	30.299	36.770	3.002	2.062
Watermarkedimage.png	Noise.png	13.723	20.194	20.242	2.520

SNR and PSNR test result show very good and high value which mean that our suggestion algorithm used is robust to preserve image quality against a different type of attacks where our watermarked image (girlface) was used as a reference for test mechanism. SNR and especially PSNR test result show the excellent and high value which mean that our suggestion algorithm used is robust to preserve image quality where our host image (Lena) was used as a reference for test mechanism. We may see some low values here, but they are still good for fending off attacks.

SNR and PSNR test result show very good and high value which mean that our suggestion algorithm used is robust to preserve image quality against a different type of attacks where our watermarked image

(Lena was used as a reference for test mechanism. We see a noticeable improvement in the results which reflects the image quality improvement embedding algorithm.

Again, SNR and especially PSNR test result show the excellent and high value which mean a that our suggestion algorithm used is robust to preserve image quality where our host image (Muhammad Ali) was used as a reference for test mechanism. SNR and PSNR test result show the very good and high value which mean that our suggestion algorithm used is robust to preserve image quality against a different type of attacks where our watermarked image (Lena) was used as a reference for test mechanism, we see a noticeable improvement in the results which reflects the image quality improvement embedding algorithm.

Table 5 (a). Lena cover image

Lena Cover image used as a reference image					
Ref.Image	Test Image	SNR (dB)	PSNR (dB)	RMSE	MAE
lena.png	Watermarkedimage.png	65.295	70.242	0.078	0.006
lena.png	Gaussian.png	25.247	30.194	7.885	6.251
lena.png	Filter.png	24.066	29.013	9.033	5.476
lena.png	crop.png	5.139	10.086	79.840	35.262
lena.png	ResizeAFT.png	24.110	29.058	8.987	5.616
lena.png	Rotate.png	3.353	8.300	98.061	76.198
lena.png	Equal.png	30.397	35.344	4.358	3.938
lena.png	Intensity.png	13.917	18.864	29.060	24.996
lena.png	Gamma.png	14.321	19.268	27.740	25.170
lena.png	hostr75.png	29.736	34.683	4.702	3.528
lena.png	Noise.png	16.804	21.751	20.843	2.537

Table 5 (b). Lena watermarked image

Lena watermarked image used as a reference image					
Ref.Image	Test Image	SNR (dB)	PSNR (dB)	RMSE	MAE
Watermarkedimage.png	Gaussian.png	25.247	30.194	7.885	6.251
Watermarkedimage.png	Filter.png	24.066	29.013	9.034	5.476
Watermarkedimage.png	crop.png	5.139	10.086	79.842	35.258
Watermarkedimage.png	ResizeAFT.png	24.111	29.058	8.987	5.616
Watermarkedimage.png	Rotate.png	3.353	8.300	98.061	76.197
Watermarkedimage.png	Equal.png	30.417	35.364	4.348	3.932
Watermarkedimage.png	Intensity.png	13.919	18.866	29.054	24.990
Watermarkedimage.png	Gamma.png	14.319	19.266	27.746	25.176
Watermarkedimage.png	hostr75.png	29.737	34.684	4.702	3.528
Watermarkedimage.png	Noise.png	16.804	21.751	20.843	2.531

Table 6 (a). Muhammad Ali cover image

Muhammad Ali Cover image used as a reference image					
Ref.Image	Test Image	SNR (dB)	PSNR (dB)	RMSE	MAE
MuhammadAliG.png	Watermarkedimage.png	66.864	70.242	0.078	0.006
MuhammadAliG.png	Gaussian.png	26.635	30.012	8.051	6.415
MuhammadAliG.png	Filter.png	25.196	28.574	9.502	3.940
MuhammadAliG.png	crop.png	5.572	8.950	90.997	43.206
MuhammadAliG.png	ResizeAFT.png	25.834	29.211	8.829	4.073
MuhammadAliG.png	Rotate.png	5.559	8.937	91.130	62.277
MuhammadAliG.png	Equal.png	11.714	15.092	44.865	39.308
MuhammadAliG.png	Intensity.png	13.099	16.477	38.254	35.914
MuhammadAliG.png	Gamma.png	16.295	19.673	26.476	25.339
MuhammadAliG.png	hostr75.png	50.553	53.931	0.512	0.230
MuhammadAliG.png	Noise.png	18.560	21.938	20.399	2.519

Table 6 (b). Muhammad Ali watermarked image

Muhammad Ali watermarked image used as a reference image					
Ref.Image	Test Image	SNR (dB)	PSNR (dB)	RMSE	MAE
Watermarkedimage.png	Gaussian.png	26.635	30.013	8.051	6.415
Watermarkedimage.png	Filter.png	25.195	28.573	9.503	3.940
Watermarkedimage.png	crop.png	5.572	8.949	90.999	43.202
Watermarkedimage.png	ResizeAFT.png	25.834	29.211	8.829	4.072
Watermarkedimage.png	Rotate.png	5.559	8.937	91.131	62.277
Watermarkedimage.png	Equal.png	11.714	15.091	44.869	39.311
Watermarkedimage.png	Intensity.png	13.100	16.478	38.249	35.908
Watermarkedimage.png	Gamma.png	16.294	19.671	26.481	25.345
Watermarkedimage.png	hostr75.png	50.447	53.825	0.519	0.235
Watermarkedimage.png	Noise.png	18.560	21.938	20.399	2.5130

5.4. Experimental results: extraction after attacks

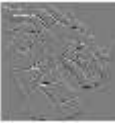


















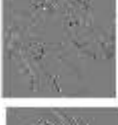




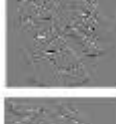
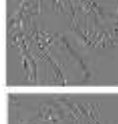





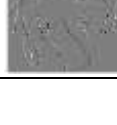




During the experiment, embedded sub bands such as LH2, HL2, HH2, LL1, LL3, and LL5 were also extracted from the watermarked images before and after applying different types of attacks. For this purpose, the MATLAB platform was used for presenting visual results for the watermarked image, Gaussian, filter, gamma, cropping, and Hostr100 as shown in Tables 7 and 8.

Table 7. Visual results after attacks for girlface

Test image	girlface					
	1 st watermark logo			2 nd watermark logo		
	LH2	HL2	HH2	LL1	LL3	LL5
Extraction from the watermarked image						
Gaussian						
Filter						
Gamma						
Cropped both sides						
Hostr100						

The embedded process included six different locations in the host image, which varied between low and high-frequency location, this explains the variation in the results obtained, as the low-frequency filtration has a high ability to maintain logo images quality, while we observe a little difficulty to remarkable the logo image at higher frequencies location used. Despite this, the viewer remains to distinguish the logo image used clearly and with high explicitly for human visual observation test.

Table 8. Visual results after attacks for lena

Test image	Lena			2 nd watermark logo		
	LH2	1 st watermark logo HL2	HH2	LL1	LL3	LL5
Extraction from the watermarked image						
Gaussian						
Filter						
Gamma						
Cropped both sides						
Hostr100						

6. CONCLUSION

In this research, the importance and significance of digital watermarking, watermarking techniques, and its important areas of application have been highlighted. Additionally, the research has also shed light on the various types of attacks as well as on the classification of watermarking schemes. Considering the potential applications, the present study has also provided in-depth insight into the challenges faced by watermarking techniques. Furthermore, the research has also discussed previous studies and related work made by multiple researchers in a similar domain. In this research, a robust watermarking algorithm for copyright protection in unsecured media by using 5-level DWT and two logos have been proposed. The present study examined and evaluated the offered schema by exposing the algorithm to ten different types of attacks. Experimental results with optimal SNR values evaluate the reconstructed image's quality against the original image while PSNR values depict image quality. The results obtained from the experiment show that the proposed scheme is robust and effective against different types of attacks and the extracted watermark logo improves the image quality and visual features. From these achievements, it can be stated that the offered schema is capable of providing copyright protection to digital images in social media. In Conclusion, it can be deduced that the proposed scheme can significantly contribute to safeguarding rights of intellectual property and enhancing digital object ownership when hovering through social media. Future studies may focus on enhancements of the algorithm performance or suggestion a new embedded and extraction process using a different location or different watermark techniques.

REFERENCES

- [1] R. K. Singh, D. K. Shaw, and J. Sahoo, "A secure and robust block based DWT-SVD image watermarking approach," *J. Inf. Optim. Sci.*, vol. 38, no. 6, pp. 911-925, 2017, doi: 10.1080/02522667.2017.1372137.
- [2] A. Zear, A. K. Singh, and P. Kumar, "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine," *Multimed. Tools Appl.*, vol. 77, no. 4, pp. 4863-4882, 2018, doi: 10.1007/s11042-016-3862-8.
- [3] P. Bhinder, N. Jindal, and K. Singh, "An improved robust image-adaptive watermarking with two watermarks using statistical decoder," *Multimed. Tools Appl.*, vol. 79, no. 1, pp. 183-217, 2019, doi: 10.1007/s11042-019-07941-2.

- [4] Y. Liu, F. Yang, K. Gao, W. Dong, and J. Song, "A zero-watermarking scheme with embedding timestamp in vector maps for Big Data computing," *Cluster Comput.*, vol. 20, no. 4, pp. 3667-3675, 2017, doi: 10.1007/s10586-017-1251-3.
- [5] P. Kadian, N. Arora, and S. M. Arora, "A Highly Secure and Robust Copyright Protection Method for Grayscale Images using DWT-SVD," 2019.
- [6] X. Zhou, H. Zhang, and C. Wang, "A robust image watermarking technique based on DWT, APDCBT, and SVD," *Symmetry (Basel)*, vol. 10, no. 3, p. 77, 2018, doi: 10.3390/sym10030077.
- [7] N. H. Abbas, S. M. S. Ahmad, S. Parveen, W. A. Wan, and A. R. Bin Ramli, "Design of high performance copyright protection watermarking based on lifting wavelet transform and bi empirical mode decomposition," *Multimed. Tools Appl.*, vol. 77, no. 19, pp. 24593-24614, 2018, doi: 10.1007/s11042-017-5488-x.
- [8] A. Sheshaayee and D. Sujatha, "Analysis of techniques involving data hiding and watermarking," in *2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, 2017, pp. 593-596, doi: 10.1109/ICIMIA.2017.7975529.
- [9] O. Hosam, "Attacking image watermarking and steganography-a survey," *Int. J. Inf. Technol. Comput. Sci.*, vol. 11, no. 3, pp. 23-37, 2019, doi: 10.5815/ijitcs.2019.03.03.
- [10] P. Pal, H. V. Singh, and S. K. Verma, "Study on watermarking techniques in digital images," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2018, pp. 372-376, doi: 10.1109/ICOEI.2018.8553743.
- [11] M. Singh and A. Saxena, "Image watermarking using discrete cosine transform [DCT] and genetic algorithm [GA]," *Int. J. Innov. Eng. Res. Manag.*, vol. 4, no. 3, pp. 1-13, 2017.
- [12] K. Madhavi, G. Rajesh, and K. S. Priya, "A secure and robust digital image watermarking techniques," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 12, pp. 2758-2761, 2019.
- [13] U. Yadav, J. P. Sharma, D. Sharma, and P. K. Sharma, "Different watermarking techniques & its applications: a review," *Int. J. Sci. Eng. Res.*, vol. 5, no. 4, 2014.
- [14] nbsplyoti sahu and nbspDolley shukla, "Digital Image Watermarking Method 4 Level DWT-DCT on the Basis of PSNR," *Int. J. Eng. Dev. Res.*, vol. 3, pp. 1008-1012, 2015.
- [15] R. R. Coifman, Y. Meyer, S. Quake, and M. V. Wickerhauser, "Signal processing and compression with wavelet packets," in *Wavelets and their applications*, Springer, 1994, pp. 363-379.
- [16] L. Zhang and D. Wei, "Dual DCT-DWT-SVD digital watermarking algorithm based on particle swarm optimization," *Multimed. Tools Appl.*, vol. 78, no. 19, pp. 28003-28023, 2019, doi: 10.1007/s11042-019-07902-9.
- [17] A. J. Hussein, S. Yuksel, and E. Elbasi, "Dynamic Binary Location based Multi-watermark Embedding Algorithm in DWT," *J. Theor. Appl. Inf. Technol.*, vol. 78, no. 2, p. 253, 2015.
- [18] A. Dixit and R. Dixit, "A Review on Digital Image Watermarking Techniques," *Int. J. Image, Graph. Signal Process.*, vol. 9, no. 4, 2017, doi: 10.5815/ijigsp.2017.04.07.
- [19] M. A. Nematollahi, C. Vorakulpipat, and H. G. Rosales, *Digital watermarking*. Springer, 2017.
- [20] S. G. Bahncmiri, M. Ponomarenko, and K. Egiazarian, "Deep Convolutional Autoencoder for Estimation of Nonstationary Noise in Images," in *2019 8th European Workshop on Visual Information Processing (EUVIP)*, 2019, pp. 238-243, doi: 10.1109/EUVIP47703.2019.8946273.
- [21] A. Awad, J. Traub, and S. Sakr, "Adaptive Watermarks: A Concept Drift-based Approach for Predicting Event-Time Progress in Data Streams," in *EDBT*, 2019, pp. 622-625.
- [22] S. B. B. Ahmadi, G. Zhang, S. Wei, and L. Boukela, "An intelligent and blind image watermarking scheme based on hybrid SVD transforms using human visual system characteristics," *Vis. Comput.*, pp. 1-25, 2020, doi: 10.1007/s00371-020-01808-6.
- [23] A. R. Yuliani and D. Rosiyadi, "Copyright protection for color images based on transform domain and luminance component," in *2016 International Conference on Information Technology Systems and Innovation (ICITSI)*, 2016, pp. 1-4, doi: 10.1109/ICITSI.2016.7858199.
- [24] P. A. van Walree, F.-X. Socheleau, R. Otnes, and T. Jenserud, "The watermark benchmark for underwater acoustic modulation schemes," *IEEE J. Ocean. Eng.*, vol. 42, no. 4, pp. 1007-1018, 2017, doi: 10.1109/JOE.2017.2699078.
- [25] O. M. El Zein, L. M. El Bakrawy, and N. I. Ghali, "A robust 3D mesh watermarking algorithm utilizing fuzzy C-Means clustering," *Futur. Comput. Informatics J.*, vol. 2, no. 2, pp. 148-156, 2017, doi: 10.1016/j.fcij.2017.10.007.

BIOGRAPHIES OF AUTHORS



Alaa Rishkek Hoshi, 2001 Rafidain university college, Iraq/Baghdad B.Sc. Software Engineering, 2010 Informatic Institution for Postgraduate Studies, Iraq/Baghdad Higher Diploma-WebSite Technology, 2016 Cankaya university, Turkey/Ankara Master Information Technology, 2019 Phd. student in UKM, Malaysia.



Assoc. Prof. IR. DR. Nasharuddin Bin Zainal (UKM), Dr.Eng. of International Development (Computer Engineering), Tokyo Institute of Technology, M.Eng. of Communication and Computer, Universiti Kebangsaan Malaysia, B.Eng. of Information Engineering (Computer Engineering), Tokyo Institute of Technology, Image and Video Processing, Pattern Recognition, Robotics, Universiti Kebangsaan Malaysia.



Prof. DR. Mahamod Ismail, Retired Professor (Wireless Communication and Networking), Department of Electrical, Electronics & System Engineering, Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia.



ABD Al-Razak T. Rahem, 2013-2016 PhD Department of Electrical, Electronics and Systems Engineering, Faculty of Engineering and Built Environment, UKM, Malaysia, 2010-2012 Msc. Tech (Information Technology), College of Engineering, Bharati Vidyapeeth Deemed University, India/Pune, 1998-2002 B. Sc Computer Engineering and information technology, University Of TechnoloGY, Iraq/Baghdad. Instructor/Middle Technical University (government) Faculty of Engineering Department of computers.



Salim Muhsin Wadi, B.Sc. in Communication Techniques Engineering, AL-Najaf Technical College 2002. M.Sc. in Communication Engineering, Electric and Electronic Dept. University of Technology 2005. Ph.D. in Communication Engineering, Electrical, Electronic and System Engineering Dept. The National University of Malaysia (UKM) 2015. Senior lecturer/Technical College-Najaf, Communications Techniques Engineering Department-Najaf, Iraq