DOI: https://doi.org/10.33103/uot.ijccce.22.4.9

A Hybrid Digital Image Watermarking By Using DWT and LSB Method

Zainab F. Makhrib[1], Abdulamir A. karim [2]

[1,2]Computer Science Department, University of Technology, Baghdad, Iraq

[1]cs.19.13@grad.uotechnology.edu.iq , [2]cs.19.13@grad.uotechnology.edu.iq

Abstract*— The Digital watermarking is a field of information hiding that entails hiding the crucial information in the original data in order to prevent illegal duplication and distribution of multimedia data such as image, video, text and ect.. In this paper, we present two techniques to embed watermarks in the cover image. The first is the Least Significant Bit (LSB) method, which is a spatial domain technique and considered fragile against attacks and other operations. The second method is the frequency domain technique, which uses Discrete Wavelet Transform (DWT) and is considered robust against attacks. The efficiency and performance of these techniques are evaluated based on Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). From the results, the value of PSNR is above 37 dB, which ensures better imperceptibility and shows better robustness. The comparison between the two techniques shows that the hybrid method was more robust than the LSB method, hence it achieves good invisibility.*

Index Terms*— Digital watermarking, Least Significant Bit (LSB), Discrete Wavelet Transform (DWT), spatial domain, frequency domain.*

I. INTRODUCTION

Due to the rapid growth of multimedia technology, data protection has become a popular topic. As a result, copyright protection for digital material has become a crucial issue as the internet has grown in popularity. With the advent of the internet and the availability of widespread and sophisticated multimedia tools, editing, distribution, and reproduction of private digital multimedia have become extremely easy and faster. The issues of unlawful duplication, counterfeit cash, business security, and intellectual property protection, among others, are becoming increasingly relevant. Due to their prevalence on the Internet, digital photographs are the most common carrier file type among the other available formats such as audio files, video files, and text files. Until now, intellectual property and value have always been associated with a physical container that could not be easily copied, ensuring that the inventor receives compensation for his effort. As a result, information concealment techniques are critical for copyright authentication. Digital watermarking has emerged as a possible method to tackle these issues[1].

Digital watermarking is a technology that secures, validates, and protects digital data's copyright. The practice of inserting secret digital data and signals into digital media such as photos, video, audio, and text is called digital watermarking. Later, the embedded data is discovered and retrieved to expose the digital media's genuine identity. Watermarking is used to establish ownership and prevent unauthorized copying. Preventative measures, data validation, data concealment, and broadcast monitoring Photographic Image Watermarking technology offers a wide range of uses, including data protection, certification, digital media distribution, and tagging of user information. Watermarking data has developed into a critical aspect of information concealment[2].

Received 08/December/2021; Accepted 28/January/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.4.9

With the growing growth of electronic commerce, Intellectual property security is crucial for content owners who make available on the Internet digital reproductions of images, books, manuscripts, and original artwork.

Additionally, as computing power becomes more readily available, there is an increasing interest in preventing video data from being manipulated. Digital watermarking has a wide range of uses, including electronic publishing, advertising, product purchase and delivery, image galleries, digital libraries, online newspapers and magazines, digital video and audio, and personal communication [3]. Additionally, it is one of the technologies being developed as appropriate tools for determining the origin, creator, owner, distributor, or authorized consumer of a document or image. Additionally, it can be used to trace photos that have been disseminated unlawfully. The digital watermarking process consists of two key steps: (1) watermark embedding, which involves embedding a watermark into cover image, and (2) watermark extraction, which involves extracting the watermark from the image [4].

This paper will embed a watermark (secret image) in the cover image (original image) to protect the watermark from the copy production process. The watermarking process is done using two proposed methods, LSB and DWT. The performance result of embedding in this method will be evaluated using metrics PSNR and MSE. Finally, a comparison will be done between the used methods to show which method has the best embedding.

II. RELATED WORKS

- In 2009 Wang Na et.al they describe a unique resilient watermarking approach for the mixed transform domain. The original cover image is divided into four sub-bands using a Discrete Wavelet Transform (DWT). The approximation coefficients are then relocated using the Arnold transform to produce a noise-like version that is then separated into non-overlapping 8-blocks. To maximize robustness and transparency, in Each block is scanned and sorted in a zig-zag pattern. decreasing order prior to performing the DCT transform. The JND (Just Noticeable Difference) model embeds a watermarking sequence encrypted with a secret key into the DCT transform coefficients via Arnold transformation. The JND model incorporates a watermarking sequence encrypted with a secret key using Arnold transformation into the DCT transform coefficients. Without the original image, the watermark is extracted. The proposed technique offers strong robustness against common attacks including noise, filtering, and compression, according to experimental data,The Peak Signal-to-noise Ratio is 41.540 in Lena image [3].
- In 2015 Surbhi Singh et.al presented Discrete Wavelet-based data concealment is a secure and robust technique. The random coefficients and the student distribution are transformed. The watermark image is scrambled to increase security and robustness. The suggested algorithm's resilience and imperceptibility were evaluated using bit rate (BER) and peak signal - to - noise ratio (PSNR) values for various watermarks and cover images. In comparison to previous existing techniques that employ DWT coefficients, the proposed technique provides improved protection and reliability against JPEG compression as well as other attacks such as noise addition, reduced filtering, and cropping ,the Peak Signal-to-noise Ratio is 46 and the Mean Square Error (MSE) is1.3908 [4].
- In 2015 Priyanka R. Kulkarni and Altaaf O. Mulani presented a discrete wavelet transform watermarking system for digital images. The digital picture watermarking technique in this scheme is based on the DWT coefficients. The information in the original image is not changed by a specific algorithm. It mixes low-frequency DWT coefficient information with the watermark image. This combination is utilized as a key, and the watermark is extracted using it. Because the

Received 08/December/2021; Accepted 28/January/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.9

suggested approach does not change any information in the original image, watermark extraction is simple. The original image's quality is unaltered.[5]

- In 2018, Chengyou Wang and el, proposed the discrete wavelet transform (DWT) has an excellent property decomposition technique for multi-resolution images, and its low frequency component holds all of an image's critical information .A fragile watermark based on the local binary pattern (LBP) and DWT is given for the purpose of image authentication. This technique uses The LBP pattern of low frequency wavelet coefficients is used as a feature watermark and is stored in the least significant bit (LSB) of the cover image. The logistic map is used to encrypt the watermark, ensuring the proposed approach's security. Additionally, the maximum pixel values are stored in advance and used to extract the watermark on the receiving end. Due to the usage of DWT, the proposed scheme's watermarked image has high visual quality. The proposed technique not only has smaller watermark payloads than current state-of-the-art watermarking methods, but also performs well in detecting and localizing tampering for a variety of attacks ,where the average of PSNR and SSIM values of these watermarked images can reach 57.31 dB and 0.9992[6].
- In 2019 Sarita P. Ambadekarb and et.al proposed a digital image watermarking technology based on the discrete wavelet transform (DWT) and encryption. The application of DWT coefficients, distance measurement, and encryption to the embedding and extraction of a watermark technique is illustrated. Watermark embedding and extraction using watermark encryption are made considerably easier with DWT's multiresolution analysis. The approach produces a PSNR of more than 50 dB and is noise, geometric, and compression attack resistant. Copyright and content authentication applications could benefit from the proposed method [7].
- In 2020 Ashwani Kumar the author of this paper used a combination of LSB and DWT techniques to create a safe and resilient digital picture watermark. The goal of the schemes is to create genuine intellectual property rights and prohibit them from being viewed by an unauthenticated user. The cover image (the image that contains the watermark) will be divided into (HH, LH, LL, and HL) using a widely known frequency domain transformation method. This transform can be applied directly to all of the source image's subordinate bands. The extraction procedures follow earlier research on the embedding algorithm. The image's output and frequency will have an effect on its strength, ostensibly retaining a higher level of quality and resistance to numerous attacks aimed at compromising the intellectual property protection techniques, such as JPEG compression and Gaussian noise where the average of PSNR and NCC values of these watermarked images can reach 45.46dB and 0 0.9463[8].

III. DIGITAL WATERMARKING

The property of digital information is easily changed and amended, resulting in a lack of ownership information. Because anyone can edit and manipulate information in multiple forms and media, authentication of information in various forms and media is not maintained. Securing information, including multimedia documents, is critical in today's environment. The genuineness of media, such as text, images, video, or audio must be protected due to the ease with which they can be distributed on the internet. Many situations of picture authentication come as a result of digital images being seen as intellectual property that could be protected, such as art photographs, remote sensing images, and medical images[11][12].

Digital watermarking is a technology that uses an algorithm to insert a watermark containing rights to intellectual property on to images, videos, audios, and other multimedia data. This type of watermark includes information about the author and the user, such as the owner's logo, serial number, or control information. In fact, it takes advantage of data's

Received 08/December/2021; Accepted 28/January/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.9

inherent redundancy and randomness and adds to it data that a is difficult to discover but distinguishable in order to safeguard copyright protection and data integrity [13][14].To design a digital watermarking systems, the following requirements are used[16]:

- Robustness (resistance): The watermark must be resistant to various attacks and manipulations.
- Capacity: an refers to the amount of digital data that can be embedded (payload).
- Security: If the carrier object or work is altered or extracted, the watermarked data should not be affected.
- Efficiency: The speed of extraction and placing of the digital watermark should be very fast
- Watermark imperceptibility (un detectability): if utilized, the watermark should have no effect on the content of the carrying object[17].

A. Stages of Digital Image Watermarking

Digital watermarking is digital signal processing technique for embedding secret data in multimedia data. This material, which is normally unseen, can only be detected and extracted using a special detector or extractor. *Fig. 1* depicts the steps involved in digital watermarking. The fundamental model of digital image watermarking is composed of two components:

1. Embedding A Watermark Process: The embedding stage is the initial phase in the procedure, and it entails embedding the watermark employing the embedding procedure and the a secret key in the original image Following that, the a watermarked image is formed. The image with the watermark is uploaded to the internet.

2. Watermark Extraction Process:Watermark Extraction is the method of identifying watermarks in watermarked photos by utilizing an extraction algorithm and a secret key. [18].

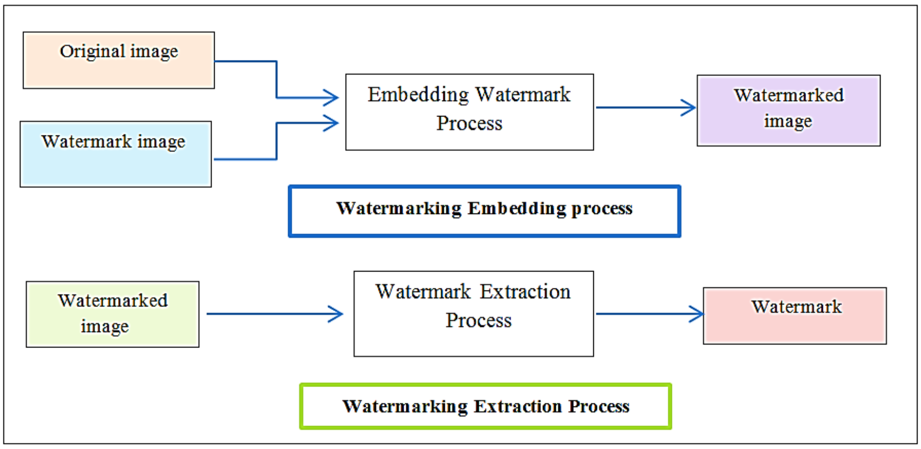
Original image
Watermark image
Embedding Watermark Process
Watermarked image
Watermarking Embedding process
Watermarked image
Watermark Extraction Process
Watermark
Watermarking Extraction Process

FIG. 1. STAGES OF DIGITAL IMAGE WATERMARKING.

B. Applications of Digital Image Watermarking

As a result of its potential application Copyright protection, annotation, security control, data verification, device administration, media forensics, and medical reporting are all examples of media applications, digital image watermarking is a highly concentrated study topic. Some of the related applications of digital image watermarking.

Received 08/December/2021; Accepted 28/January/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.9

1. Copyright Protection: A watermark is an image that is added silently and can be detected when compared to the original. Copyright watermarks are used to identify the source of an image as well as authorized users.
2. Broadcast monitoring: This program can be used by content owner to determine a when and where their content was a broadcast. Additionally, it verifies the correct timing of content broadcast via satellite television and other transmission technologies. Each sound or video clip might have a unique watermark placed before the broadcast.
3. Fingerprinting: Fingerprinting is a technique that enables a work to be uniquely identified by embedding digital information in the form of a watermark. Detecting the watermark on any unlawful copy may enable the individual who leaked the original content to be identified.
4. Medical Applications: Watermarking techniques can be used to protect patient information from unauthorized access. Among these are medical imaging, telehealth, and telemedicine. In these instances, the watermark data must not degrade the image quality.
5. Additional Uses: Watermarking digital images can be used to prove the authorship of something. Among other things, digital image watermarking can be used to avoid digital counterfeiting, fraud, identity theft, secure electronic voting, and deployable remote education. [19][20][21].

IV. DIGITAL IMAGE WATERMARKING TECHNIQUES

Techniques for digital image watermarking vary according to the working domain (i.e., spatial domain, frequency domain, or hybrid domain) and the algorithm utilized. They can be applied to text, images, audio or video files as well as source or destination-type of application.

A. Spatial Domain Watermarking Techniques

These approaches operate directly on the pixels of the original image. The watermark can be added by modifying the pixel values based on the author's logo or signature information. The image is represented by pixel intensities at known positions in space in the most often used designs, where the lowest-order bit of particular pixels in a color or gray scale image is flipped. The resulting watermark may be visible or invisible, depending on the pixel intensity. These strategies are low in complexity, have improved efficiency, and are executed more quickly. Furthermore, the quality of the watermarked image can be adjusted. This domain's most often utilized algorithms are LSB and SSM modulation[9].Least significant bit (LSB) modification is the most commonly used technique for spatial domain watermarking. Here, the least significant bit (LSB) of randomly chosen pixels can be altered to hide the most significant bit (MSB) of another. The watermark is inserted into the least significant bits of the host image and can be extracted in the same way. This type of algorithm is easy to implement and is simple. The least significant bits carry less relevant information, and, thus, the quality of the host image is not affected. It provides high perceptual transparency with a negligible impact on the host image.

B. Frequency Domain Watermarking Techniques

Spatial domain watermarking techniques are insufficiently robust and easily manipulated. In comparison to frequency-domain algorithms, these strategies are significantly more vulnerable to a variety of attacks. These disadvantages have shifted focus to the development of transform-domain watermarking techniques, which conceal data more effectively in the transform space of a signal than in its time domain. By applying a

Received 08/December/2021; Accepted 28/January/2022

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

predefined transform to the image, this technique converts it to the frequency domain. The watermark is then embedded by changing the transform domain coefficients of the original image using several transforms, including the Discrete Cosine Transform (DCT), the Discrete Fourier Transform (DFT), the Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD) [23].

Discrete wavelet transforms (DWT) approach

The discrete wavelet transform (DWT) is a mathematical procedure for dissecting an image hierarchically. It was extensively used in signal processing, image compression, and watermarking. It takes signal and decomposes it into a collection of fundamental functions known as wavelets. Wavelets are formed by translating and warping a constant function referred to as the mother wavelet. The wavelet transform describes an image's frequency as well as its spatial location. Discrete Wavelet Transformation is ideal for identifying locations in the cover image where watermark image can be efficiently placed. This trait enables the use of the human visual system's masking effect, so that modifying a DWT co-efficient alters only the region corresponding to that coefficient. Because the majority of the image energy is stored in the lower frequency sub-bands, putting a watermark in these sub-bands may impair the image. It is, however, more robust to embed the watermark in the higher frequency sub band, because the human eye is less sensitive to changes in edges, the high frequency region of the image carries information about the image's edge. Hence, these frequency sub-bands are frequently employed for watermarking [24]. DWT decomposes two-dimensional images into four sections. Because they integrate more detail from the cover image, low-frequency coefficients are more resistant to watermark embedding. The top right carries data about the horizontal image, the bottom left has information about the vertical image, and the bottom right contains data about the original's high frequency.

V. IMAGE QUALITY EVALUATION

The robustness and imperceptibility of watermark are calculated using multiple performance indicators below are the two used measures.

A. Mean Square Error (MSE)

MSE can be used to determine the image's distortion. It is defined as the average of the squares of the difference in intensities between the watermarked and original images. It is widely used due to its mathematical tractability.Show MSE formula equation (1).

$$\boldsymbol{MSE} = \frac{\mathbf{1}}{\boldsymbol{m*n}} \sum_{\boldsymbol{i=0}}^{\boldsymbol{m-1}} \sum_{\boldsymbol{j=0}}^{\boldsymbol{m-1}} [\boldsymbol{I}(\boldsymbol{i},\boldsymbol{j}) - \boldsymbol{K}(\boldsymbol{i},\boldsymbol{j})] \ldots\ldots\ldots\ldots..(1)$$

Where a I(i,j) is the cover image and K(i,j) is the watermarked image . large value for MSE means that a the watermarked image has poor quality and vice-versa. Low MSE value indicate a good watermarking method.

B. Peak Signal to Noise Ratio (PSNR)

PSNR used to measure the quality of the watermarked image by comparing the cover image with the watermarked image, i.e.,a It compares the cover image to the watermarked image statistically. The PSNR value represents the degree to which the altered image can be reconstructed. This measure is used to distinguish the cover image from the watermarked image. In any technique if the PSNR value is above 30dB it is considered to be a good technique while higher PSNR indicate a good watermarking method. Equation (2) show the PSNR formal.

$$PSNR = \mathbf{10}\log_{10}\frac{255^2}{MSE} \ldots\ldots\ldots\ldots(2)$$

VI. THE PROPOSED METHOD AND RESULT DISCUSSION

In this paper, we present two techniques for embedding watermarks in the cover image. The first is the Least Significant Bit (LSB) technique, and the second is hybrid technique, Discrete Wavelet Transform (DWT) and (LSB) to achieve robustness in digital image watermarking.

A. Least Significant Bit method

The LSB technique is used in two phases. The first phase is to embed a watermark with a size of 128*128 in a cover image with a size of 512*512 pixels. The watermark image and the cover image specifications are relatively large, whether gray or RGB, in order to bear the watermark image, which is embedded in the cover image.The embeding phase is depend on secret key composed of 8 digits with the range (1-8), where the numbers 1-8 are selected randomly . Every digit in the key determines the bit position (sequence) of the watermark pixels which will be embeded in the LSB of the cover image. The extracting phase is the reverse of the embedding phase, which depends on the sectet key to extract the watermark pixel.

Example: assume that the key is:

53861247

Then the bit number 5 of the watermark pixel will be embedded in the LSB of the first pixel of the cover image ,bit number 3 will be embedded in the LSB of the second pixel and bit number 7 will be embeded in the LSB of the eight pixel. Algorithms1 is used to embed the watermark into the cover image using LSB technique.

```
    algorithms1: Watermark Embedding Method By using the LSB technique
    Input: cover image, watermark and secret key
    Output: watermarked image.
--------------------------------------------------------------------------
    Begin
    Step1: Select a cover image of the size M*M and watermark of size N*N as an input
    Step2: a secret key of size 8 digits with the range (1-8).
    Step 3: use the key to determine the bit position of the watermark pixel which
embedded in the LSB of the cover image.
    Output 4: obtain Watermarked .
```

In order to obtain the watermark the watermarked image, the inverse of the watermark embedding method is performed.

DOI: https://doi.org/10.33103/uot.ijccce.22.4.9

TABLE I. PERFORMANCE EVALUATION THE PSNR AND MSE

Cover image	Watermark	Watermarked	PSNR	MSE
			37.978	10.358
			38.434	9.325
			38.836	8.501

It can be notice from Table I that the watermarked image a similar to the cover image since PSNR value is greater than 30 dB.[10] This means a good embedding.

B. Hybrid method

This approach uses Discrete Wavelet Transforms and the LSB Technique to incorporate 128*128 image watermarks within a cover image. The cover image is decomposed into four sub-bands, namely, LL, LH, HL, and HH using the DWT technique. A watermark is then embedded into the HH part of the cover image using the LSB technique. The LL part contains the significant information of the image and it cannot used for embedding watermark images. Finally, IDWT is applied to all four parts to get a watermarked image. To retrieve the watermark images from the watermarked image, the watermarked image is decomposed into four sub –bands using DWT. the LSB technique is used to extract the watermark from the HH band, and the watermarked images are retrieved. Two metrics, PSNR and MSE, are used to validate the quality of the images before and after the embedding process They are used to verify the image's quality both before and after embedding. *Fig. 2* shows the watermark embedding process in the method.

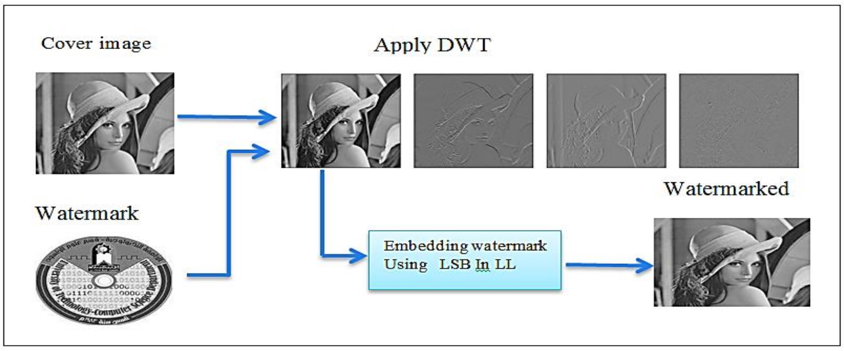

FIG. 2. WATERMARK EMBEDDING IN WAVELET DOMAIN.

```
Algorithm 2: Hybrid Watermark Embedding Method Using DWT and LSB
Input: cover image and Watermark.
Output: watermarked image.
Begin
```

Received 08/December/2021; Accepted 28/January/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.9

```
  Step1 : for i=1 to number of pixel
   Step2: for j=1 to number of pixel
   Step3: Apply the transform DWT to cover image with size ( 512* 512)obtain four subbands (LL, LH, HL and HH).
  Step4: Select the watermark image to  the size (128*128).
  Step5: Apply the Watermark Embedding Method By using the LSB technique (algorithm 1):  to embed watermark in the LL part of the cover image.
  Step 6: to embed the watermark to produce (LL new) while keeping the reset coefficient the same as (LL new, LH, HL, and HH).
  Step 7: Apply the inverse transform IDWT for the modified image to reconstruct the watermarked image.
Step 8: Output: watermarked image
Step9:End
```

After embedding the watermark in the cover picture, the extraction method is used to extract the watermark from the cover image and validate the cover image's ownership or copyright. This process is achieved by using Algorithm 3.

```
Algorithms 3: Watermark Extracting Using DWT and LSB Hybrid Method
Input: watermarked image.
Output:  watermark.
Begin
   Step 1: Apply DWT on watermarked image to produced a four coefficients (LL new, LH, HL, and HH).
  Step2: Use ILSB technique watermark from (Llnew ) part in the cover image coefficient
  Step3: Convert binary representation watermark form to decimal to obtain the extracted watermarked image.
   Step 4:Repeat step2  the result is the watermark image with size (128*128).
  Step5: Apply the inverse transform IDWT for the modified image to obtain the extracted watermark image.
  Step6:Output:  watermark with size (128*128)
  Step7: End.
```

TABLE II. PERFORMANCE EVALUATION THE PSNR AND MSE

Image	Cover image	Watermark	Watermarked	PSNR	MSE
Giral image				48.135	0.999
Airplane image				48.938	0.8303
house image				49.485	0.7321

Received 08/December/2021; Accepted 28/January/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.9

Performance evaluation of the second watermark embedding technique, which has been presented above, is carried out by determining two performance evaluation metrics. Where The PSNR and MES values of these watermarked images are (48.135 dB and 0.999) for the giral image, (48.938 dB and 0.8303) for the airplane image, and (49.485 dB and 0.7321) for the house image. It can be noticed that all PSNR values are higher than 40 dB, which is quite acceptable for the human eye, with almost no sign of watermark existence. Additionally, this demonstrates that the watermark has little influence on cover images. Hence, DWT techniques must be used with LSB techniques in order to obtain a high payload. The quality of the watermarked image is good in terms of perceptibility.

VII. COMPARISON BETWEEN THE TWO WATERMARKING TECHNIQUES

In this section, a comparison was made between the two watermarking techniques (LSB and hybrid DWT), including (Image Quality Evaluation, Size, working domain, Robustness, Limitations, Applications). It could be noticed that the hybrid method was better than LSB in the process of embedding the watermark. Table III lists the comparison between the two watermarking techniques.

TABLE III. THE COMPARISON BETWEEN WATERMARKING TECHNIQUES

	Least Significant Bit(LSB)		hybrid method (DWT) and LSB	
Image Quality Evaluation	**PSNR**	**MSE**	**PSNR**	**MSE**
	37.978	10.358	48.135	0.999
	38.434	9.325	48.938	0.8303
	38.836	8.501	49.485	0.7321
Size of watermark	128*128		128*128	
Size of cover	512*512		512*512	
Type of image	Color and Gray scale		Color and Gray scale	
working domain	spatial domain watermarking		Frequency (Transform) Domain Watermarking	
robustness	Watermarked image of high quality - High resilience to attacks -Fast speed		Resistant to compression, cropping, filtering, and noise adding, -Better imperceptibility	
Limitations	Less Robust against geometric attacks, like scaling and rotation		Weaker resistance to change operations[11]	
Applications	Image authentication		Copyright protection and information about the owner	

Table IV indicates the comparison of the proposed method with other research. It was noticed that the proposed method have a larger PSNR (48.135) at the same image size, which means an excellent watermarking than the other.

TABLE IV. COMPARTION WITH THE OTHER METHOD

Method	Image size	PSNR
Shubh Lakshmi Agrwal and el at [12]	512x512	39.2
Ashwani Kumar[8]	512x512	45.4
T Sindhu[13]	512x512	43.59
Proposed method	512x512	48.135

Received 08/December/2021; Accepted 28/January/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.9

VIII. CONCLUSIONS

Digital watermarking is a field of information hiding that hides the crucial information in the original data for protection against illegal duplication and distribution of multimedia data. This paper presents a comparison between two techniques for embedding watermarks in the cover image. The first is the Least Significant Bit (LSB) method, and the second is the hybrid Discrete Wavelet Transform (DWT) and the Least Significant Bit (LSB). Robustness and imperceptibility are calculated using performance indicators, which are Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The result shows that the average PSNR and MSE have 38.416db and 9.369, respectively, in the first method, as shown in Table I, and 48.852db and 0.8538 in the second method, as shown in Table II. The comparison between the two techniques showed that the hybrid DWT method was more robust than the LSB method, in which the test result shows it achieves good invisibility. When compared to the frequency domain, the spatial domain technique provides greater security and successful recovery of watermarked images. The paper recommends hybrid DWT-LSB-based techniques for achieving robustness in digital image watermarking. One of the many advantages of the wavelet transform is that it is believed to more accurately model aspects of the HVS (Human Visual System) as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands (LH, HL, HH). Embedding watermarks in these regions allows us to increase the robustness of our watermarks with little to no additional impact on image quality.

REFERENCES

[1] N. Singh, M. Jain, and S. Sharma, “A Survey of Digital Watermarking Techniques,” Int. J. Mod. Commun. Technol. Res., vol. 1, no. 2321, p. issue-6, 2013, doi: 10.14445/22315381/ijett-v46p220.

[2] P. Pal, H. V. Singh, and S. K. Verma, “Study on Watermarking Techniques in Digital Images,” in Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018, 2018, vol. 1, no. Icoei, pp. 372–376, doi: 10.1109/ICOEI.2018.8553743.

[3] S. Godhar1 and Vyom Kulshreshtha, “A Fundamental Study of Digital Image Watermarking,” Ijreas, vol. 2, no. 2, pp. 126–136, 2012.

[4] A. D. Salman, “Dynamic , Secure , and Invariant Watermarking System for Multiview Plus Depth Video,” no. 1, pp. 9–14.

[5] N. Wang, Y. Wang, and X. Li, “A novel robust watermarking algorithm based on DWT and DCT,” CIS 2009 - 2009 Int. Conf. Comput. Intell. Secur., vol. 1, pp. 437–441, 2009, doi: 10.1109/CIS.2009.135.

[6] S. Singh, H. V. Singh, and A. Mohan, “Secure and Robust Watermarking Using Wavelet Transform and Student t-distribution,” Procedia Comput. Sci., vol. 70, pp. 442–447, 2015, doi: 10.1016/j.procs.2015.10.071.

[7] A. O. M. Priyanka R. Kulkarni, “Robust Invisible Digital Image Watermarking using Discrete Wavelet Transform,” Int. J. Eng. Res. Technol., vol. 4, no. 1, pp. 139–141, 2015, [Online]. Available: www.ijert.org.

[8] C. Wang, H. Zhang, and X. Zhou, “LBP and DWT based fragile watermarking for image authentication,” J. Inf. Process. Syst., vol. 14, no. 3, pp. 666–679, 2018, doi: 10.3745/JIPS.03.0096.

[9] S. P. Ambadekar, J. Jain, and J. Khanapuri, Digital image watermarking through encryption and DWT for copyright protection, vol. 727. Springer Singapore, 2019.

[10] A. Kumar, A Review on Implementation of Digital Image Watermarking Techniques Using LSB and DWT, vol. 933. Springer Singapore, 2020.

[11] E. H. Rachmawanto, C. A. Sari, Y. P. Astuti, and L. Umaroh, “A robust image watermarking using hybrid DCT and SLT,” Proc. - 2016 Int. Semin. Appl. Technol. Inf. Commun. ISEMANTIC 2016, pp. 312–316, 2017, doi: 10.1109/ISEMANTIC.2016.7873857.

[12] J. Zhang and A. T. S. Ho, “An efficient digital image-in-image watermarking algorithm using the integer discrete cosine transform (IntDCT),” ICICS-PCM 2003 - Proc. 2003 Jt. Conf. 4th Int. Conf. Information, Commun. Signal Process. 4th Pacific-Rim Conf. Multimed., vol. 2, pp. 1163–1167, 2003, doi: 10.1109/ICICS.2003.1292643.

[13] T. Liu and Z. D. Qiu, “The survey of digital watermarking-based image authentication techniques,” Int. Conf. Signal Process. Proceedings, ICSP, vol. 2, pp. 1556–1559, 2002, doi: 10.1109/ICOSP.2002.1180093.

[14] Y. Zhang, “Digital watermarking technology: A review,” 2009 Int. Conf. Futur. Comput. Commun. FCC 2009, pp. 250–252, 2009, doi: 10.1109/FCC.2009.76.

[15] L. K. Saini and V. Shrivastava, “A Survey of Digital Watermarking Techniques and its Applications,” no. February 2013, 2014, [Online]. Available: http://arxiv.org/abs/1407.4735.

Received 08/December/2021; Accepted 28/January/2022

DOI: https://doi.org/10.33103/uot.ijccce.22.4.9

[16] U. H. Panchal and R. Srivastava, “A comprehensive survey on digital image watermarking techniques,” Proc. - 2015 5th Int. Conf. Commun. Syst. Netw. Technol. CSNT 2015, pp. 591–595, 2015, doi: 10.1109/CSNT.2015.165.

[17] H. H. O. Nasereddin, “Digital watermarking a technology overview,” vol. 6, no. January, pp. 89–93, 2011.

[18] R. Patel and P. Bhatt, “A Review Paper on Digital Watermarking and its Techniques,” Int. J. Comput. Appl., vol. 110, no. 1, pp. 10–13, 2015, doi: 10.5120/19279-0692.

[19] M. Begum and M. S. Uddin, “Digital image watermarking techniques: A review,” Inf., vol. 11, no. 2, 2020, doi: 10.3390/info11020110.

[20] N. Agarwal, A. K. Singh, and P. K. Singh, “Survey of robust and imperceptible watermarking,” Multimed. Tools Appl., vol. 78, no. 7, pp. 8603–8633, 2019, doi: 10.1007/s11042-018-7128-5.

[21] Z. Wenyin and F. Y. Shih, “Semi-fragile spatial watermarking based on local binary pattern operators,” Opt. Commun., vol. 284, no. 16–17, pp. 3904–3912, 2011, doi: 10.1016/j.optcom.2011.04.004.

[22] G. Bhargava and A. Jhapate, “A Study on Digital Watermarking Techniques,” Int. J. Recent Trends Eng., vol. 1, no. 3, p. 5, 2009, doi: 10.24113/ijoscience.v4i3.130.

[23] Z. F. Yaseen and A. A. Kareem, “Image Steganography Based on Hybrid Edge Detector to Hide Encrypted Image using Vernam Algorithm,” in 2019 2nd Scientific Conference of Computer Sciences (SCCS), 2019, pp. 75–80.

[24] Z. F. Makhrib and A. A. Karim, “Digital Watermark Technique : A Review Digital Watermark Technique : A Review,” in 2nd International Virtual Conference on Pure Science (2IVCPS 2021), 2021, vol. 1999, p. 012118, doi: 10.1088/1742-6596/1999/1/012118.

Received 08/December/2021; Accepted 28/January/2022