COPYRIGHT PROTECTION SYSTEM BASED WATERMARKING

IMAD **M**AJED **Z**EEBAREE, **H**IWA **A**LI **A**BDULLAH[*], **F**ARHAD **M**. **K**HALIFA[**]
and **O**MER **S**EDQI **K**AREEM[***]
[*]Dept. of Information Security, Technical College of Informatics-Akre University for Applied Sciences, Kurdistan Region-Iraq
[**]Dept. of Computer Networks, Bardarash Technical Institute, Akre University for Applied Sciences, Kurdistan Region-Iraq
[***]Dept. of Public Health, College of Health and Medical Techniques-Shekhan, Duhok Polytechnic University, Kurdistan Region-Iraq

(Received: August 28, 2022; Accepted for Publication: August 20, 2023)

ABSTRACT

In digital information science, there is a crisis represented in resisting tampering and protecting the copyright of digital content when storing, transmitting, and processing encrypted information in systems where digital content can easily be disseminated through communication channels. Watermarking is one of the techniques adopted in protecting digital property and information. It is the technology of infusing a watermark with property rights in other multimedia through a specific algorithm. A comparison of the two digital watermarking methods known as DWT and DWT-SVD is offered in this article. In the case of using the watermark technique with DWT wavelet transformation, the decomposition of the original image is complete for the watermark implant, and in the case of the DWT-SVD watermark technique the original image given to the DWT is first decomposed and then the watermark is transplanted into the individual values obtained by applying SVD (single value analysis). Watermarking methods in this work aim to provide protection for copywriting. Later, presentations of the presented technologies are compared based on PSNR and MSE values. The results show that the hybrid DWT-SVD technique is significantly better than the DWT technique. Finally, the proposed method has been compared with another watermarking technique. The system is also very resistant to a variety of image-processing-related attacks.

KEYWORD: watermark, DWT, SVD, Copyright Protection.

1. INTRODUCTION

Digital multimedia information has grown easier to separate in recent years because of advances in computer and network technologies [1]. The internet is a useful technique. Nowadays, people mostly get benefits from digital technology for daily issues; on another side using technology has good economic affection, high efficiency and low cost. In the near future, all digital media, such as text, audio, video, and maps, will be available for everyone [2].

Digital media is better than analogue media because it has digital data that can be reproduced easily and infinitely without any reliability [3]. There are various usable digital data systems; one of them is Watermarking, a system that processes hiding extra information within software codes, digital data (such as audio, image, video), and documents in such a way that it is nearly untraceable [4]. A digital watermark or signal covering information unique to the copyright proprietor in the item (text, audio, image, or video) must be protected [5]. This procedure involves the quantity of message data and the requirement for the invariability of embedded data when subjected to distortions such as lossy compression, removal by a third party, or modification [6,7].

Image improvement is made through meaning to modify an image so that the result is more appropriate than the original image for a specific purpose. That includes histogram processing and equalization of an image. The two approaches for improvement are the spatial and frequency domain approaches.

The spatial domain denotes the actual image plane. The approaches in this group are based on the direct operation of pixels in an image. At the

same time, the frequency domain refers to the plane of an image's 2D discrete Fourier transform.

Frequency domain filters are used to improve digital images by operating the Fourier transform of the image [8]. Singular Value Decomposition (SVD), Discrete Wavelet Transform (DWT), and the Discrete Cosine Transform (DCT) are all examples of transform (frequency) domain techniques that alter the coefficients of the transform rather than the pixel values directly to hide watermark bits [9, 10].

Using image processing technologies, it has become increasingly easier for the general public to acquire and edit photos. As a result, digital image copyright authentication has become a complex problem. In recent decades, a notion of digital watermarking has been developed to address this problem. For the most part, digital watermarking techniques may be categorized into two major groups: robust and fragile watermarking [2]. Since they can withstand frequent attacks, copyright protection relies heavily on robust watermarking systems. On the other hand, Fragile watermarking technologies are typically used to detect and restore images that have been tampered with.

A robust watermarking system for copyright protection must meet two requirements: robustness and imperceptibility. Because of their robustness, watermarks in a watermarked image can be retrieved even if attacks have distorted them. Furthermore, the quality of a watermarked image cannot be significantly affected by its imperceptibility. Therefore, no signs of watermark embedding can be seen by unaided eyes [3].

2. LITERATURE SURVEY

Chang et al. [11] developed SVD block-based approach. SVD decomposition is applied to each block of a decomposed host image. Each block's complexity is measured by computing the S component's non-zero coefficients one by one. According to their theory, the blocks with the most non-zero coefficients are more complicated. General image processing attacks can't take down this method.

Chung et al. [12] suggested two methods for enhancing SVD-based watermarking techniques' capacity and imperceptibility. According to the first proposal, tweaking the U-column vector coefficients will have less impact on the overall performance than modifying the row vectors. Likewise, the row vector of VT would be less affected by alterations to the column vectors than the column vectors, according to a second proposal. These ideas were tested and found to be effective regarding imperceptibility and capability.

They carried out various experiments on the ideas of Chung et al. [12] by Fan and his colleagues [13]. Analyses were conducted in the form of a theoretical and experimental investigation, and a watermarking system using SVD-based watermarking was established using the initial proposal. The second suggestion was to embed the watermark in U and V instead of U and V to compensate for the visual distortion that occurs when the watermark is placed in U and V. The results showed that Fan et al. [13] approach outperformed Chung et al. [12] in terms of effectiveness.

Lai [14] proposed an enhanced SVD block-based algorithm. Based on HVS features, he divided the host image into 8 x 8 non-overlapping chunks and picked the suitable chunks to extract data from. For each block, the entropy and edge entropy characteristics of the HVS were examined. After that, the entropy and edge entropy values were added and sorted in ascending order, and the blocks with the smallest magnitude values were chosen. SVDs were then applied to all blocks that DCT had changed. The proposed strategy's efficiency was proved through experimental and theoretical results.

In [15], the Discrete Wavelet Transform (DWT) and All Phase Discrete Cosine Biorthogonal Transform (APDCBT) presented with Singular Value Decomposition (SVD) to improve the watermark imperceptibility, the authors concluded that the proposed scheme has a little detectable effect on the original image. Furthermore, it shows better robustness against typical signal-processing attacks than other algorithms.

In [16] algorithm was proposed to ensure higher visual quality after the watermark was added to the image; blocks or pixel regions selected for the watermark are hiding such as regions in the image. Even after four bits on the least significant side of all pixels in the image were reset, the proposed result was able to withstand even the subtlest changes to the image.

The authors of [17] used a DWT-DCT hybrid technique to combine the advantages of both systems. However, DWT suffers from fraction loss during watermark insertion, increasing MSE

and lowering PSNR. Therefore, compared to previous DWT and DCT approaches, the PSNR of the retrieved secret image is higher.

The present study enhances the watermark imperceptibility. As a result, the proposed method is predicted to provide better-quality watermarked images. The system is also very resistant to a variety of image-processing-related attacks. This article provides a comparison of the two digital watermarking techniques, DWT and DWT-SVD. In the case of the DWT-SVD watermark technique, the original image provided to the DWT is first decomposed and then the watermark is transplanted into the individual values obtained by applying SVD (single value analysis). In the case of the watermark technique with DWT wavelet transformation, the decomposition of the original image is complete for the watermark implant.

3. INFORMATION HIDING

Since the advent of electronic files, various methods of hiding information have been created to protect sensitive information from prying eyes.

This paper will look at some early examples of steganography and the broad ideas that underlie its application. Our next stop will focus on the reasons for its recent emergence as a subject of international concern. Several specific tactics for concealing data in various files and assaults that can be used to get around steganography will then be covered in detail [12].

Information concealment can be divided into several categories, as Figure 1. First, information hiding can be used to hide a message meant to be retrieved by a certain individual or group in the future. In this situation, the goal is to ensure that no other party can intercept the message [18].

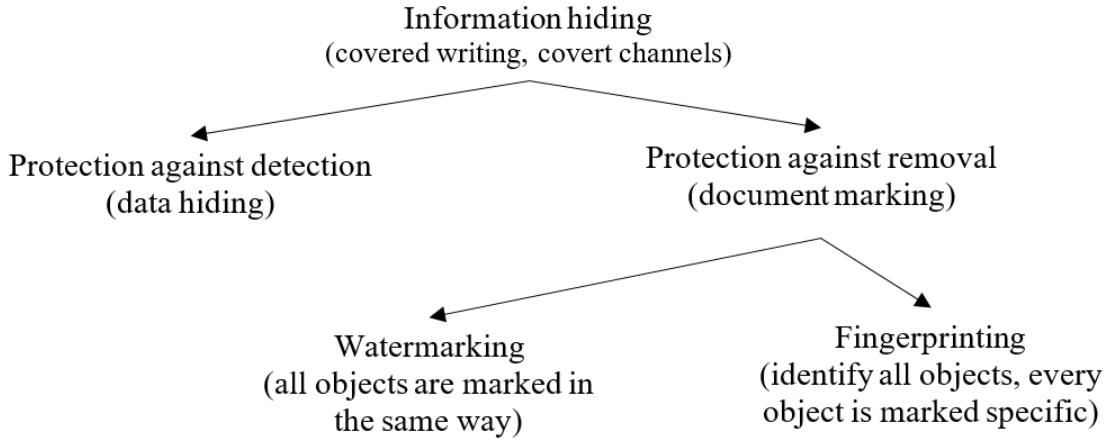

Fig. (1): Types of Information Hiding.

Copyright marking is the other major field of information hiding; in this case, the message is used to claim copyright on a work. This is the other major area of information hiding. This can be further broken down into fingerprinting and watermarking, which will be covered in further detail later.

3.1 Digital Rights and Copyright Marking

The rapid expansion of the internet has played a significant role in the increased demand for copyright marking, which has made digital versions of various types of media like images, audio, and video available. As a result, copyrighted material is easier to make and disseminate thanks to this new distribution method. Piracy of music, for example, used to necessitate a physical trade. Because the item doesn't need to be hosted on a server and may instead be distributed via a peer-to-peer network, it's more difficult for the copyright owner to track down and prosecute infringers when they use an Internet copy stored on a computer [19].

According to one estimate, Internet file sharing and MP3 piracy are predicted to cost the worldwide music industry more than £2.8 billion a year. As a result, the music industry is spending a lot of money on research on copyright watermarking, which they think will allow them to prosecute copyright violators in court since CD sales have dropped significantly since the internet took off.

These issues can be addressed in part by copyright protection. It is permissible to include the mark in any legal form, which means it will be included in any copies. This lets the copyright holder identify those who have illegally copied their work [19].

3.2 Requirements for Hiding Information Digitally

Numerous protocols and embedding strategies allow us to hide data in a particular object. However, for steganography to be used correctly, all protocols and techniques must meet several conditions. These are the most important conditions that steganography methods must meet [5]:

After the information has been encoded into the stego object, its integrity must be upheld to prevent data corruption. Information hidden from view must not be altered in any manner. This includes adding or removing data or making other alterations to the secret message. Steganography would be rendered meaningless if secret information was altered during the procedure.

The stego object must appear to the naked eye as if nothing has changed. A third party can observe that information is being disguised by the stego object and attempt to extract or destroy it, thereby making the stego object vulnerable.

Changes to the stego object should not affect the watermark during watermarking. An unlawful copy of the image that you'd like to change in many ways is an example of this. Resizing, clipping, and rotating the image are all examples of easy image manipulations. Because of these alterations, a watermark embedded in the image needs to be able to withstand them, or the goal of steganography will be lost.

Finally, we assume that the adversary is aware of the stego object's secret information.

3.3 Types of Watermarking

There are two forms of watermarking: fragile and robust. Both of these methods of watermarking are described in detail in the following section.

3.3.1 Fragile

Files that are watermarked with Fragile Watermarking are rendered unusable when they are altered. Using this method to record the file's copyright holder isn't a good idea because of how easy the watermark can be removed, but it can be beneficial in cases when it's vital to prove that the file hasn't been altered, like in court, where changing the file would remove the watermark. Rugged watermarking is more difficult to apply than fragile watermarking [6].

3.3.2 Robust

The goal of robust marking is to secure a file by embedding data that can't be removed easily. Although no mark is fully impenetrable, a system can be deemed robust if the number of adjustments required to remove it would leave the file unusable. Because of this, the mark should be placed in an area of the file where its removal can be readily perceived [20].

Robust marking can be divided into two categories. Fingerprinting is the process of concealing a customer's unique identifier so that they can use the file. If the material is discovered to be in the hands of a third party, the copyright owner can use the fingerprint to determine which customer breached the license agreement by sharing a copy of the file.

Instead of a fingerprint, watermarks indicate the file's copyright holder, not the buyer. Watermarks aid in the prosecution of individuals in possession of an unlawful copy, whereas fingerprints aid in the identification of those who break the license agreement. Ideally, fingerprinting should be utilized, but in the case of CDs, DVDs, and other mass-produced media, fingerprinting is not possible [6].

As a result of their ability to remain undetectable, the phrase "imperceptible watermarks" has come to describe watermarks that are difficult to spot. It's important to note, however, that this is not always the case. For example, watermarks that are visible to the naked eye can be employed. Similar to the use of watermarks in non-digital forms, the use of visible watermarks (such as the watermark on money).

4. PROPOSED ALGORITHMS

This proposal declares the logical design of the system. Also, it states the elements used in the proposed algorithm.

4.1 Discrete Wavelet Transform (DWT)

In the wavelet field, watermarks can be implanted with ease. The DWT can be used to compress audio and video files in the same way as the Discrete Cosine Transform (DCT), extract features such as fingerprints or watermarks and perform a variety of other biomedical engineering tasks [19].

A watermark image is created by transforming the cover image into the frequency domain and then applying watermark

coefficients to cover image frequency coefficients. This is a frequency domain approach that is very healthy. To deconstruct an image at a single level, DWT uses a hierarchical decomposition method that divides the original image into four bands with distinct frequencies and spatial domains [18]. An image is broken down into a lower-resolution approximation image (LL1) and horizontal (HL1), vertical (LH1), and diagonally (HH1) detail components using the one-level Discrete wavelet transform [21]. The DWT algorithm is over-applied to the LL1, which additionally decomposes the LL1 component into four subbands LL2, HL2, LH2, and HH2. Figure 2 depicts a two-level 2D-DWT procedure.

Fig. (2): Two-level 2D-DWT process.

4.1.1 DWT Watermarking Steps

Step 1: A single-level 2-D DWT is used to break up the original N*N image into subbands.

Step 2: A one-level 2-D DWT transforms the watermark into sub-bands of the size M*M image.

Step 3: The scaling factor (α) is used to embed the watermark into the lower frequency subband of the original image.

$$WI=O+\alpha W \quad (1)$$

Step 4: The watermarked image is then created using inverse 2-D DWT.

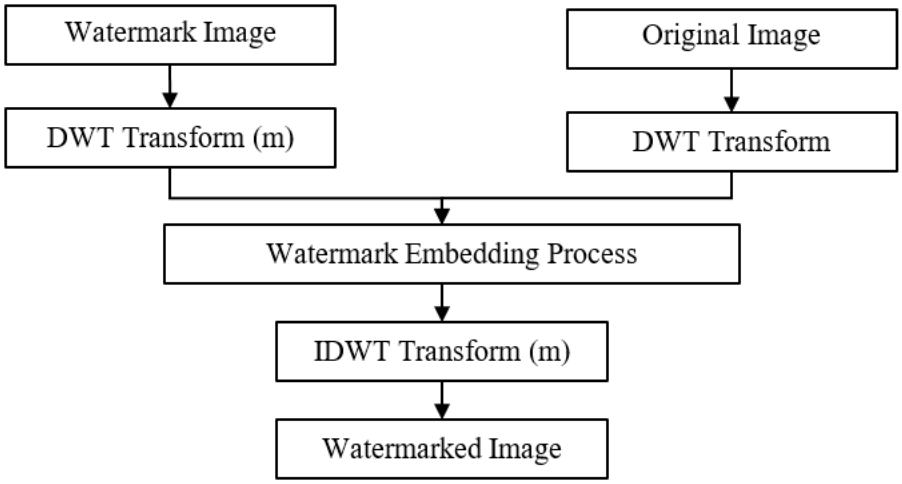

Fig. (3): DWT Embedding.

4.1.2 DWT Extract Watermarking Steps

Step 1: A single-level 2-D DWT transforms the source N*N RGB image into sub-bands.

Step 2: Single-level 2-D DWT is used to translate the watermark into sub-bands of size M*M RGB.

Step 3: A single-level 2-D DWT is used to decompose the watermarked image into its constituent subbands.

Step 4: A single 2-D DWT is used to break up the watermarked image (the embedding output) into sub-bands.

Step 5: When the watermark has been deconstructed, the same scale factor (α) is used to apply the extraction.

$$EWI=(MW-O)/\alpha \quad (2)$$

Step 5: Finally, the retrieved watermark image is then obtained using inverse 2-D DWT.

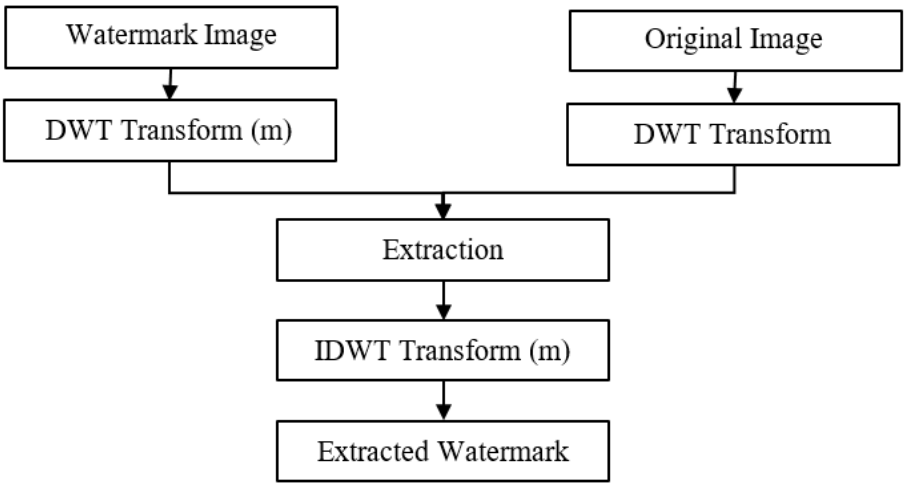

Fig. (4): DWT Extraction.

4.2 Singular Value Decomposition (SVD)

In image processing, real or complex matrix factorization can be achieved using Singular Value Decomposition (SVD). Equation 3 gives the SVD of an image M with dimensions m x m because a digital picture may be represented as a matrix with each entry representing the strength value of a pixel in the image [22]:

$$M = USV^T \quad (3)$$

A diagonal matrix with loud non-negative singular values of matrix M is known as S, and U and V are orthogonal matrices of that matrix. The columns of U and V are referred to as the left and right singular courses of M, respectively. They are just a description of the original image's geometry. The flat details of the original image are represented by the left singular matrix (U), while the vertical details are represented by the right singular matrix (V). From the first singular value in matrix S to the last one in the diagonal, the relevance of the admissions decreases in descending order. In SVD-based compression methods, this functionality is working as intended. Use SVD's digital watermarking capabilities; there are two key advantages [23]

1. The quality of the image is unaffected by minor changes in individual values.
2. The image's singular values show a high degree of consistency.

4.3 Fusion DWT-SVD

The fusion method combines two distinct approaches. Together, DWT and SVD improve the resilience and inaudibility of digital watermarking, making it more difficult to detect.

4.3.1 Watermarking Embedding process

The following outlines the steps that must be taken to successfully embed the watermark.

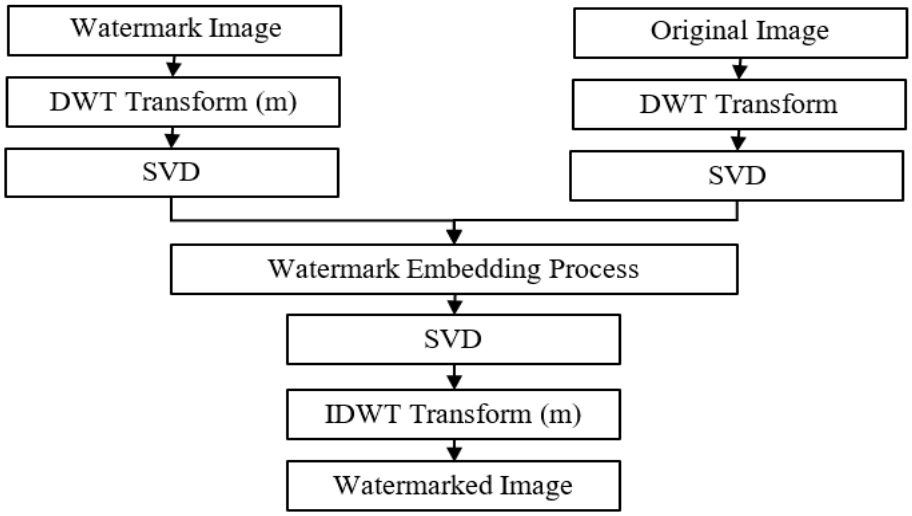

Fig. (5): DWT-SVD Embedding.

4.3.2 DWT-SVD Embedding Steps

Step 1: A single level 2-D DWT is used to convert the source image N*N RGB into sub-bands.

Step 2: SVD is carried out on the LL sub-band (RGB components) of the decomposed RGB source image, and the equation used is S = USV T.

Step 3 involves employing a single level of two-dimensional discrete wavelet transform (DWT) to transform the watermark image with size M*M RGB into sub-bands.

Step 4: SVD is performed on the LL sub-band of the decomposed RGB watermark image.

SW = WU SW WV T (4)

Step 5: Original and watermark images are combined using the scale factor (α) after SVD is applied to the watermark image.

$$SWI = S + \propto (SW) \quad (5)$$

Step 6: Embedded images are exposed to Inverse SVD transformations.

Step 7: Finally, the watermarked image is produced via inverse 2-D DWT.

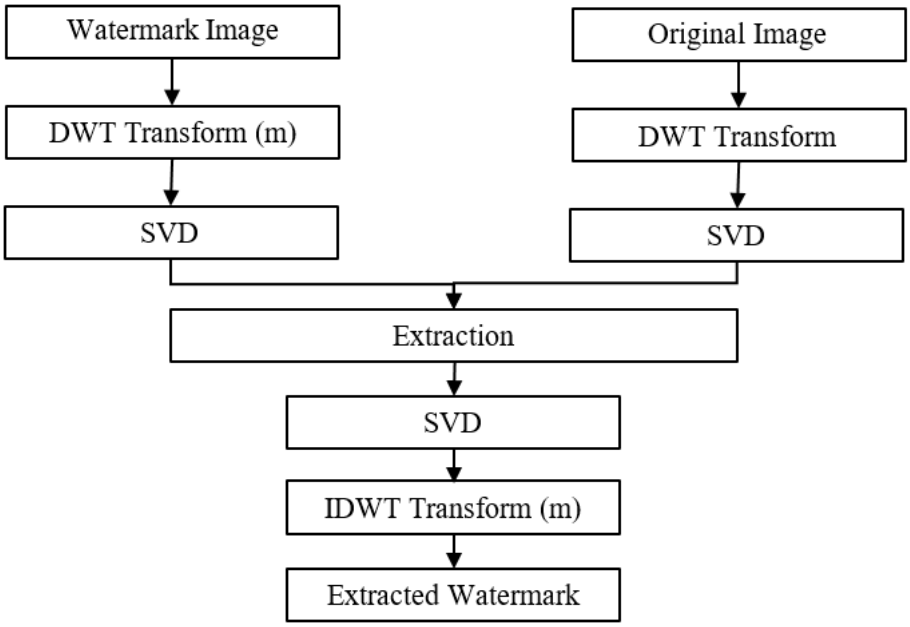

Fig. (6): DWT-SVD Extraction.

4.3.3. DWT-SVD Based Extraction Steps

Step 1: A single level 2-D DWT is used to convert the original N*N RGB image into sub-bands.

Step 2: On the decomposed RGB image, SVD is applied to the LL subband.

S = USVT (6)

Step 3: The watermark, which is an M*M RGB image, is then converted into sub-bands by employing a single level of the 2-D discrete wavelet transform.

Step 4: SVD calculation is made on the LL sub-band of the decomposed RGB watermark image.

SW = WU SW WV T (7)

Step 5: With the use of a single level 2-D discrete wavelet transform, the watermarked image that results from embedding is converted into subbands.

Step 6: When an RGB image is dissected, the LL sub-band is subjected to SVD.

SWI= WU SW WV T (8)

Step 7: After that, the extraction is used on the final resultant SVD image while maintaining the same value of the scale factor (α).

EWI=(SWI-S)/α (9)

Step 8: After extraction, the resulting image is subjected to Inverse SVD.

Step 9: an inverse two-dimensional discrete wavelet transform is carried out to retrieve the extracted watermark image.

5. RESULTS AND DISCUSSION

This section shows the results of the proposed system when it runs on eight grayscale images. Also, it will clarify and discuss that.

5.1 Image Quality

For all things and functions, quality is an extremely important element to consider. Image quality is a crucial factor in the process of recognizing objects based on images. The use of ground truth is necessary to reliably evaluate image quality. But in actuality, determining what the ground truth is can be a very difficult challenge. Full orientation measurements, such as Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR), are being utilized to evaluate image quality. Irrelevance concerning PSNR, and MSE, recently, two more full direction metrics called SSIM (Structured Similarity Indexing Method) and FSIM (Feature Similarity Indexing Method) have been established to compare the structural and feature comparison measures between restored and original objects based on perception. Technically, the quality of an image can be described, in addition to objectively identifying the deviation from the ideal or reference model. Images of human looks, for example, can be used to convey the subjective perception or forecast of a picture [24, 25].

5.2 Quality Measurement Technique

It is possible to evaluate and measure images' quality using a wide variety of techniques, including MSE (Mean Square Error), UIQI (Universal Image Quality Index), PSNR (Peak Signal to Noise Ratio), SSIM (Structured Similarity Index Method), FSIM (Feature Similarity Method), HVS (Human Vision System), etc. MSE and PSNR approaches were the focus of our efforts in this study [26].

5.2.1 Mean Square Error

MSE is the greatest shared estimator of the image quality measurement metric. It is a full reference metric, and the values nearer to zero become better. MSE looks like a signal fidelity measure. Measures that quantify the degree of similarity between two signals or the degree of error/distortion that exists between them are the primary purpose of signal fidelity measures. It is assumed that one of the signals will be a perfect copy of the original while the other is marred by noise or faults [19, 27]. It's also possible to refer to the MSE as an estimator's Mean Squared Deviation (MSD). As a method for estimating an image quantity that has not been directly observed, the estimator is described. The MSE or MSD is a metric for calculating the mean square error. The error is the difference between the estimated outcome and the estimator. Because it's a function of the expected squared or quadratic loss, it's a risk factor [28]. Between two pictures like I (i, j) and I' (i, j), the MSE is defined as follows:

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}} \sum_{\mathrm{i}=1}^{\mathrm{M}} \cdot \sum_{\mathrm{j}=1}^{\mathrm{N}} [\mathrm{I}(\mathrm{i},\mathrm{j}) - \mathrm{I}'(\mathrm{i},\mathrm{j})]^2 \quad (10)$$

5.2.2 Peak Signal-to-Noise Ratio

This indicates that a greater PSNR value results in better image quality because the PSNR value approaches infinity while the MSE value approaches 0 percent. On the other end of the spectrum, a low PSNR indicates a large discrepancy in the numerical values of the images [29]. And during compression, PSNR has been considered one of the most significant indicators to assess compression quality. The most commonly used quality assessment method for determining how well lossy image compression codecs rebuild images is the Peak signal-to-noise ratio. Compression or distortion introduces errors into a signal, which are referred to as "noise". [30]. The PSNR is expressed as [30]:

$$\mathrm{PSNR} = 10 \log_{10} \left(\frac{(\mathrm{MAX})^2}{\mathrm{MSE}} \right) \mathrm{db} \quad (11)$$

5.3 Experimental Results

The suggested technique was evaluated on eight grayscale images, including Boats, Barbara, Fingerprint, Couple, Bridge, Lake, Lena, and Hill, to see how well it worked. A watermark in the form of a 32x32 binary picture. Figure 7 depicts all of the images and the watermark that was utilized.

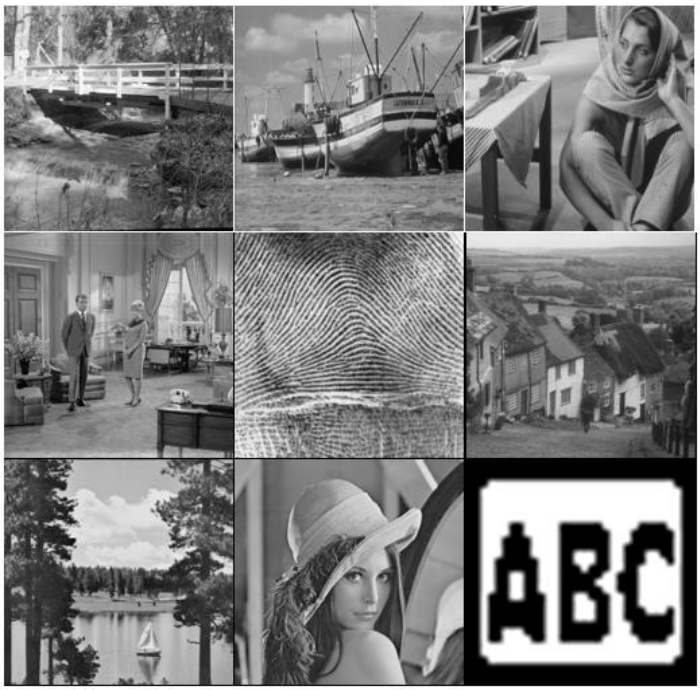

Fig. (7): Original cover images and watermark. (a) Barbara, (b) Boats, (c) Bridge, (d) Couple, (e) Fingerprint, (f) Hill, (g) Lake, (h) Lena, (i) ABC watermark.

5.4 Experimental Results Analysis

Smearing the Peak Signal-to-Noise Ratio (PSNR) as an image quality metric is done in all of the trials to evaluate the quality of the watermarked image. The PSNR (Peak Signal to Noise Ratio) and MSE values are used to evaluate the quality of the image that has been watermarked (Mean Square Error). An ideal PSNR and MSE should be infinite and zero, respectively. However, as this is not possible with the watermarked image, it is desirable to have a high PSNR while maintaining a low MSE.

The MSE, Eq. 10, and PSNR, Eq. 11, analyses are presented in Table 1. Low PSNR levels are rumoured to be necessary for effective watermarking. On the other hand, low MSE values mean that there is no watermark that can be seen.

Table (1): Comparison between DWT and DWT-SVD according to MSE and PSNR Values

Name of Image	Value of Scaling factor(α)	Value of PSNR		Value of MSE	
		DWT	DWT-SVD	DWT	DWT-SVD
Hill	0.03	36.3791	36.4505	14.9682	14.7242
Loch	0.03	36.3791	36.4493	14.9682	14.7283
Couple	0.03	36.3794	36.4571	14.9673	14.7017
Lena	0.03	36.3791	36.4538	14.9681	14.7131
Barbara	0.03	36.3791	36.4453	14.9681	14.7417
Boat	0.03	36.3792	36.4591	14.9678	14.7417
Fingerprint	0.03	36.3799	36.4638	14.9655	14.6792
Bridge	0.03	36.4016	36.5121	14.8909	14.5168

The PSNR and MSE findings for the Bridge image are the best, while the ones for the Barbara image are the poorest. But all values are very close, indicating that the watermark algorithm is stable since the variation of the covering image does not affect the quality of the watermark. See figure 8 Comparison between DWT and DWT-SVD according to PSNR

Values. And figure 9 Comparison between DWT and DWT-SVD according to MSE Values.

All figures indicate that the DWT-SVD algorithm has an advantage over the DWT algorithm in terms of the quality of results.

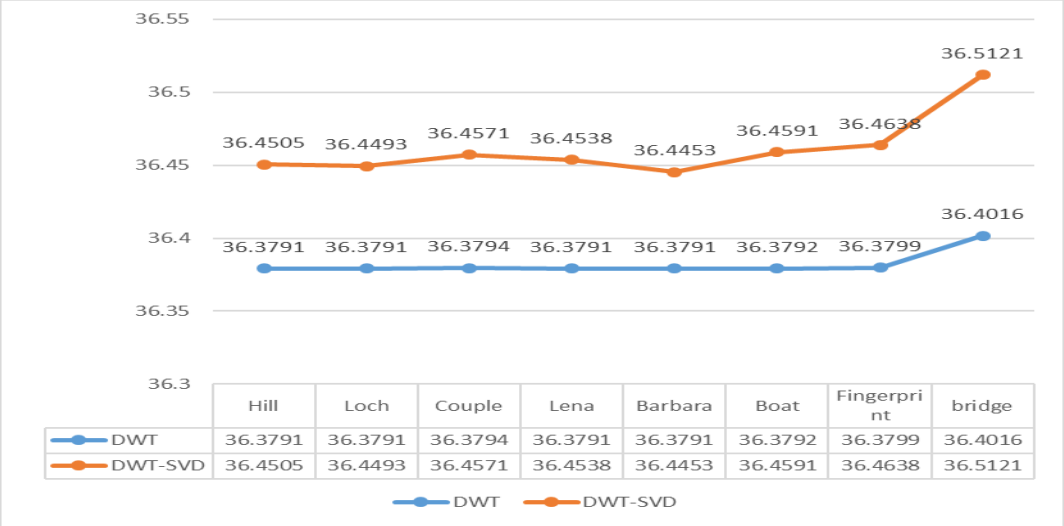

Fig. 8: Comparison between DWT and DWT-SVD according to PSNR Values.

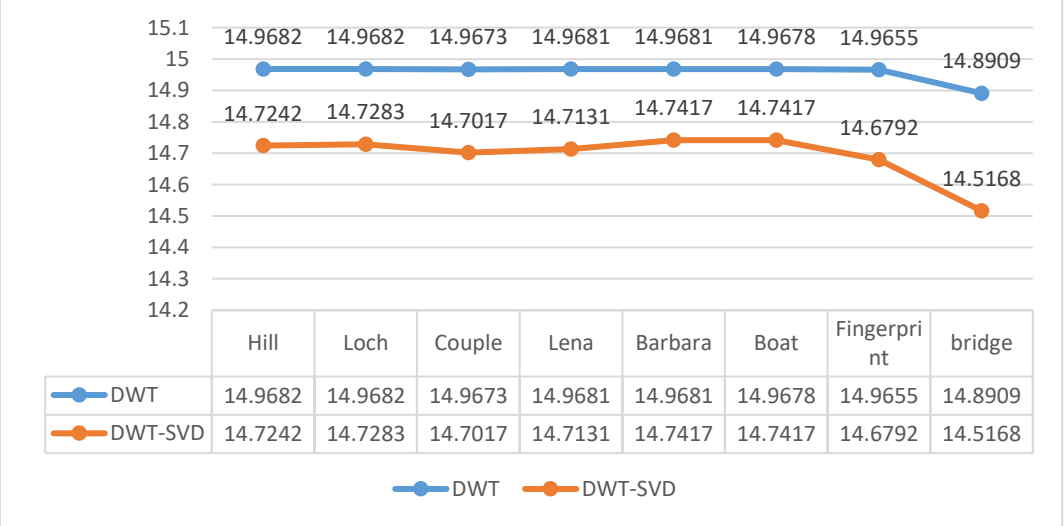

Fig. (9): Comparison between DWT and DWT-SVD according to MSE Values.

A range of widely used signal processing attacks, including JPEG compression, Gaussian noise, and salt and pepper noise, are applied to the watermarked photos in order to evaluate the robustness of the suggested technique. The outcomes reveal that the retrieved watermarks produced by the suggested technique exhibit strong resilience against different types of attacks. Table 2 presents the normalized correlation coefficient (NCC) values of the extracted watermarks under various attacks in order to assess the robustness of the suggested approach objectively. In order to assess the quality of an extracted watermark, the normalized correlation coefficient (NCC) is computed to look at how comparable the original and extracted watermarks are. Moreover, a watermarking method based on DWT, APDCBT, and SVD has been compared with the suggested approach [15]. Considering the randomness of the noise, the NCC values of the extracted watermarks after noise attacks are the average values from multiple experiments.

Table (2): The normalized correlation coefficient NCC values of the extracted watermarks under different attacks.

Attack	Zhou, Zhang & Wang. [15]	Proposed
Embedding intensity	0.05	0.05
Salt and pepper noise (0.005)	0.9988	1
Salt and pepper noise (0.01)	0.9985	0.9993
Gaussian noise (0, 0.005)	0.9986	0.9789
Gaussian noise (0, 0.01)	0.9993	0.9894
Scaling (2, 0.5)	0.9638	0.9837
Scaling (0.5, 2)	0.9672	0.9902
Median filtering (3 × 3)	0.9793	0.9855
Median filtering (5 × 5)	0.9724	0.9809
Average filtering (3 × 3)	0.9741	0.9811
Average filtering (5 × 5)	0.9690	0.9766
Rotation (5◦)	0.9897	0.9864
Rotation (15◦)	1	0.9988
Contrast enhancement (1.2)	1	0.9994
Contrast enhancement (1.5)	1	0.9996
Brightness adjustment (+50)	0.9741	0.9935
Brightness adjustment (+100)	0.9707	0.9893

Table 2 demonstrates that the NCC values attained under the same attacks by the suggested method are about equal to, if not larger than, those produced by other methods. Moreover, the NCC outcomes exhibit remarkable stability across a range of attack intensities. These results suggest that the proposed method is highly robust compared with the scheme proposed in reference [15].

6. CONCLUSIONS

DWT and DWT-SVD watermarking techniques can be used to determine the copyright protection and security of streams or photos and to increase the image's robustness. According to the findings of this study, the hybrid DWT-SVD technique is significantly better than the DWT technique when compared based on MSE and PSNR. This means that the quality of the original image is reduced more when the DWT technique is used to implant the watermark in comparison to the DWT-SVD technique implanting since the DWT technique requires more energy. The algorithm that has been suggested is reliable since changes to the cover picture do not have an impact on the watermark's overall quality.

REFERENCES

C. I. Podilchuk and E. J. Delp, "Digital Watermarking: Algorithms and Applications", IEEE Signal Processing Magazine, (2001) July.

Verma, V.; Singh, M.J. Digital image watermarking techniques: A comparative study. Int. J. Adv. Electr. Electron. Eng. 2013, 2, 173–184.

Hai, T.; Li, C.M.; Zain, J.M.; Abdalla, A.N. Robust image watermarking theories and techniques: A review. J. Appl. Res. Technol. 2014, 12, 122–138.

Isamadeen A. Khalifa, Farhad M. Khalifa, Subhi RM Zeebaree, Musa Ataş, "Comparison between BPNN and RBNN in Frequency Domain Image Steganalysis using Co-Occurrence Matrix", International Engineering and Science Symposium (IESS 2019), Proceedings Book, pp.239-243.

Saraju P. Mohanty, "Digital Watermarking: A Tutorial Review", Indian Institute of Science, Bangalore, 1999.

Zamani, M., Manaf, A.B.A., Ahmad, R.B., Jaryani, F., Chaeikar, S.S. and Zeidanloo, H.R., 2010, March. "Genetic audio watermarking". In *International Conference on Business Administration and Information Processing* (pp. 514-517). Springer, Berlin, Heidelberg.

Saman Shojae Chaeikar, Azizah Bt Abdul Manaf, and Mazdak Zamani. Comparative analysis between Master key and Interpretative Key Management (IKM) Framework to provide utilization guidelines for researchers and developers. Cryptography and Security in Computing, Publisher online InTech. 2012.

Babawuro Usman, Shehu Ayuba, "Practical Digital Image Enhancements using Spatial and Frequency Domains Techniques",

International Research Journal of Computer Science, Vol. 2, Iss. 5, pp. 27-32, 2015.

C.-C. Lai, Member, and C.-C. Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE Transactions on Instrumentation and Measurement, vol. 59, no. 11, **(2010)** November.

P.-Y. Lin, J.-S. Lee and C.-C. Chang, "Dual Digital Watermarking for Internet Media Based on Hybrid Strategies", IEEE Transactions on Circuits and System for Video Technology, vol. 19, no. 8, **(2009)** August.

Chang, C.C., Tsai, P., Lin, C.C.: 'SVD-based digital image watermarking scheme', Pattern Recognit. Lett, 2005, 26, (10), pp. 1577–1586

Chung, K.L., Yang, W.N., Huang, Y.H., et al.: 'On SVD-based watermarking algorithm', Appl. Math. Comput., 2007, 188, (1), pp. 54–57

Fan, M.Q., Wang, H.X., Li, S.K.: 'Restudy on SVD-based watermarking scheme', Appl. Math. Comput., 2008, 203, (2), pp. 926–930

Lai, C.C.: 'An improved SVD-based watermarking scheme using human visual characteristics', Opt. Commun., 2011, 284, (4), pp. 938–944

Zhou, Xiao & Zhang, Heng & Wang, Chengyou. (2018). A Robust Image Watermarking Technique Based on DWT, APDCBT, and SVD. Symmetry. 10. 77. 10.3390/sym10030077.

J. Abraham and V. Paul, "Image watermarking using DCT in selected pixel regions," 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kanyakumari, 2014, pp. 398-402. doi: 10.1109/ICCICCT.2014.6992994.

Khalifa, Isamadeen A., Subhi RM Zeebaree, Musa Ataş, and Farhad M. Khalifa. "Image Steganalysis in Frequency Domain Using Co-Occurrence Matrix and Bpnn." *Science Journal of University of Zakho* 7, no. 1 (201349): 27-32.

Malik, V., Sangwan, N. and Sangwan, S., 2017. Digital Watermarking using DWT-SVD Algorithm. Advances in Computational Sciences and Technology, 10(7), pp.2161-2171.

M. V. Malakooti, Z. F. Panah and S. M. Hashemi, "Image Recognition Method based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD)", SDIWC, (2013).

F. M. Khalifa and M. G. Saeed, "Image Watermarking Using All Phase Discrete Cosine Biorthogonal Transform in Selected Pixel Blocks," Polytech. J., vol. 10, no. 1, pp. 68–73, 2020, doi: 10.25156/ptj.v10n1y2020.pp68-73.

M. V. Malakooti, Z. F. Panah and S. M. Hashemi, "Image Recognition Method based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD)", SDIWC, (2013).

Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 10, Number 7 (2017) pp. 2161-2171 © Research India Publications

Jabade, V.S. and Gengaje, D.S.R., 2011. Literature review of wavelet based digital image watermarking techniques. *International Journal of Computer Applications*, *31*(1), pp.28-35.

Thung, K.-H. and Raveendran, P. (2009) A Survey of Image Quality Measures. IEEE Technical Postgraduates (TECHPOS) International Conference, Kuala Lumpur, 14-15 December 2009, 1-4.

Sogaard, J., Krasula, L., Shahid, M., Temel, D., Brunnstrom, K., and Razaak, M. (2016) Applicability of Existing Objective Metrics of Perceptual Quality for Adaptive Video Streaming. Society for Imaging Science and Technology IS&T International Symposium on Electronic Imaging.

Prateek Gupta, Priyanka Sarivastava, Satyam Bhardwaj, Vikrant Bhateja, "A HVS Based Perceptual Quality Estimation Measure for Color Images," ACEEE International Journal on Signal & Image Processing, Vol. 03, pp. 63-69, 2012.

Hasoon, S. O. and F. M. Khalifa. 2012. Steganalysis using KL transform and radial basis neural network. AL-Rafidain J. Comput. Sci. Math. 9(1): 47-58.

M. D. Swanson, B. Zhu, and A. H. Tewfik, "Robust Data Hiding for Images", IEEE Digital Signal Processing Workshop, pp. 37-40, Department of Electrical Engineering, University of Minnesota.

Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity", IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, 2004.

Deshpande, R.G., Ragha, L.L. and Sharma, S.K. (2018) Video Quality Assessment through PSNR Estimation for Different Compression Standards. Indonesian Journal of Electrical Engineering and Computer Science, 11, 918-924.