

Analysis On Digital Image Watermarking Using Dct-Dwt Techniques

Zolidah Kasiran¹; Rabi'atul Adawiyah Tarmizi²; Zarina Zainol³; Mohd Zaki Bin Ghazali⁴

^{1,2,3,4}*Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, 40450
Shah Alam, Selangor, Malaysia*

*Email: ¹zolidah@tmsk.uitm.edu.my, ²rabiattarmizi98@gmail.com,
³zarina@tmsk.uitm.edu.my ⁴mzaki559@uitm.edu.my*

Abstract

In recent years, digital images are used in various platforms by all means of purpose by people and also creators. The data also can be easily copied or altered, and anyone with a computer can create the forgeries too. The work on digital watermarking of images has introduced several strategies over the years, either using spatial or transform domain. Nevertheless, as the technologies are evolving, the digital images become more vulnerable towards illegal threats such as illegal duplication and removal attack without the creator's consent and the approach or watermarking techniques used are still aren't robust enough to secure the digital images hence, more approach can be applied to make it more secure. So to tackle the problem, the combined or hybrid of Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) watermarking techniques are developed in this project to analyses and evaluate the performance of the proposed techniques. The techniques are developed and applied to the image according to the watermarking process, which started from the embedding process until the watermark extraction. Based on the results, the purposes of the project has been achieved as the watermarking techniques showed a good performance in terms of imperceptibility and robustness, measured by the two measuring parameter which are the Peak Signal-to-Ratio (PSNR) and correlation factor values.

Key-words: cybersecurity, digital watermarking, watermarking.

I. INTRODUCTION

In recent years, digitalization has played a big role in technology, be it images, videos and audios. The technology of digitalization has also create a new way threats that attack their vulnerabilities. This issue has surged many concerns among the creators themselves. The digitized contents is vulnerable to be copied and modified with various alterations to the point it will be hard to distinguish the original and duplicated copy. Thus, this consequence affected the creators' especially to file lawsuits or other legal actions for the copyright infringements.

Throughout the years as the technologies, improved and digital images became more prone towards illegal threats such as digital attacks, it was found that the image

watermarking using transform domain is used frequently rather than spatial domain technique. Even so, there are still lacking in terms of robustness, imperceptibility and as well as achieving high performance to secure the digital images.

Digital images are vulnerable to illegal duplication and removal attacks without the creator's consent. The data can easily be copied or altered, and anyone with a computer can create the forgeries. The digital images posted or distributed on the internet are the most vulnerable to such malicious attacks, resulting in the breach of ownership or copyright from the original creators.

Based on (L. Singh et al., 2018) research, copy attack is possible on a watermarked material or media by copying or embedding it into another carrier signal. Throughout the years, numerous

techniques have been introduced to digital watermarking, be it by using either spatial or transform domain and as well as other combined hybrid of watermarking techniques in each domain. However, the approach or methods used are still are not robust enough to secure the digital images; hence more approach can be applied to make it more secure. A robust watermarking on the digital images can acquire them and prevent such illicit used of it as well as protecting the original owner of the images.

In this project, the hybrid of Discrete Cosine Transform (DCT-based) and Discrete Wavelet Transform (DWT-based) watermarking scheme of transform domain was proposed; the performance was analysed and evaluated. The DCT-based scheme was chosen as it is known to be robust against JPEG and MPEG compression attacks as well as it has less computation complexity. Meanwhile, the DWT-based scheme was chosen because of its excellence in resistance to any geometrical operations such as cropping attack and noise attack.

The significance of this project is, it preserved the authenticity of the digital images without degrading the quality of the images. This is due to the watermarking process that might degrade the images after being embedded into. For instance, the embedded watermark might degrade the image contrast and brightness to preserve the imperceptibility and robustness of the watermark itself.

Other than that, it enabled the prevention of any illegal copyright infringement and ownership of the images' creators. The watermark embedded into the images protect the ownership for the creators by the extracted watermark into them (digital images) in case any illegal copyright duplication or infringement.

II. LITERATURE

These days, images are shared and transmitted across various channels or mediums all over the world electronically. However, a lot of criminal activities are going around too, such as infringement of copyrights, production of

images, forgery of images, leakage, unauthorized dissemination and much more of the evil actions on the transmitted images.

Watermarking of the image has become more and more popular nowadays due to its various functional applications. Digital image watermarking is a technique used to hide digital data into a host image, be it a logo or audio or an image. Protection of copyright, the security of information, recognition of ownership and many others are among the main application of digital watermarking. The digital watermarking is one of the marker types that embedded into an audio or image data in a noise-resistant signal. Digital watermarking is also used to establish the ownership when such signals are released, and the hidden data should be digital excluding the connection to the carrier signal, as it should not be included (Vasudha B. Sankpal; R.N.Patil, 2017).

The watermarking is divided into two categories, which are the spatial domain and frequency domain techniques.

2.1. Spatial Domain

The spatial domain is a technique that deals directly with the image's pixels (G. S. Pradeep Ghantasala, 2017). The frame's pixel colour samples are changed if the spatial domain techniques are used. In total, there are three main techniques in spatial domain. The first technique under the spatial domain is the Least Significant Bit (LSB) coding, which one of the earliest watermarking methods of image. Van et al. have proposed the two LSB techniques. The image's LSB was replaced by a pseudo-noise (PN) sequence in the first technique while the LSB was given a PN sequence in the second method. Although this approach has been simple, it lacks the fundamental robustness that can be required in any application for data hiding. It was able to survive simple operations like cropping, some additive noise. Still, in activities such as brightness enhancement, resampling, quantization, image enhancement, etc., it was not possible to process the composite image. Once the formula has been discovered, it becomes an easy task for the

attacker to alter or detect the encrypted information (A. Jaikumar et al., 2017).

a) The second technique is the Patchwork technique which one of Bender et al.'s statistical methods. In this technique, patches of watermark are inserted based on statistics discovered using a Gaussian distribution. The way this strategy works is as follows: two patches are chosen randomly, say patch A and patch B. Patch A picture information is brightened and Patch B picture information is darkened. For inserting information into an image, redundant pattern encoding is used in this process (O. Y. Abdulhammed, 2021).

b) Marilou O. Espina et al. (2019) suggested a predictive coding scheme for grayscale images. In this method, the association between the adjacent pixels are exploited. A set of pixels where the watermark has to be inserted is chosen, and the gap between the adjacent pixels is replaced by other pixels.

When adding a constant to all the variations, this can be further strengthened. A cypher key is created that allows the receiver to recover the embedded watermark. Similar to LSB coding, this is much more stable (Poonam; S. M. Arora, 2018).

2.2. Transform Domain

The second technique is the transform domain. The message is embedded by adjusting the coefficient of the transform from the message's cover. Several transforms can be applied to digital images, but most commonly used are the three in particular. They are the Discrete Fourier Transform (DFT), the Discrete Cosine Transform (DCT) and also the Discrete Wavelet Transform (DWT) (P. Kumar; A. K. Sharma, 2017).

Discrete Cosine Transform (DCT) represents information rather than an amplitude space in terms of frequency space. As it applies more to how a human perceives light, the unseen components can be eliminated. The DCT technique is more robust than other techniques available in the spatial domain. This is because the spatial domain is quite difficult to implement and quite costly in computational

forms and only robust to the simple image processing (M. Begum; M. S. Uddin, 2020).

Discrete Wavelet Transform (DWT) is a technique that based on the series of small waves, called wavelets which vary in amplitudes and their short lengths. This technique is commonly used in digital image processing, such as compression or watermarking. The wavelet divides the picture into three directions; horizontal, vertical and diagonal that represents the direction variant properties of the Human Visual System. At each point of decomposition, the magnitude of the DWT coefficients is higher in the lowest bands (LL) and smaller for other bands (HH, LH, and HL) thus it is known to suit many applications.

DWT is much preferred to counter the imbalance between robustness and perceptiveness. This is because the techniques offered a simultaneous spatial location and the watermark's frequency distribution within the host image. The essential or basic concept of DWT is that it decomposes the image into sub-bands of various spatial domain and independent frequencies (Yongqiang Ma et al., 2020).

For signal analysis, the Discrete Fourier Transform (DFT) is well-known in describing the consequences of different factors on the signals. DFT is used to convert the signal from the time domain to the frequency domain or vice versa, over the years of its applications. The transformation is reversible, and the same power is retained (Kaushik H. Raviya et al., 2020).

2.3. Application of Watermark

Digital watermarking has been done or applied to various applications. The following are among the application of watermark. Copyright protection is aimed at embedding information about the source and thus usually the data's data holders to restrict other parties from claiming the data's copyright. Given a standard image manipulation such as the image processing, geometric distortions and others, the watermark should be identified (Komal M. Lande, 2019).

The watermark is inserted to detect if the image has been changed or not. Through the use of fragile or semi-fragile watermark, the changes or manipulation within the content can be validated and detected. This is due to the low robustness of modification in the image. Other than that, the watermark is also used as encryption to any media within. For instance, any users can view or download any media on the internet. However, the authenticity of the downloaded files is unknown. No one knows because most of the contents (whether authentic or not) will remain intact after transmitted over the internet (Aaqib Rashid, 2016).

2.4. Properties of Watermarking

There are several properties of watermarking that deemed as essential. Below are the properties of watermarking that are most practical in terms of its applications.

Imperceptibility is a vital requirement for electronic watermarking; that is, the insertion of the watermark should imperceptibly convert the visual resemblance between the watermarked version and the original media item and the perceptual value of the original signal. The first two important reasons in maintaining the host media imperceptibility are due to the presence and absence of the watermark after it has been deeply skewed until the data embedded is lost. The absence of the watermark from the original press resonated from the malicious attack, as stated previously, should be forbidden. Alternatively, suspicious perceptible objects can introduce an established watermark, and maybe host media detect its precise location. This information may provide access to maliciously manipulate, delete, or remove data from the watermark. Consequently, the information contained in it may no longer be available (Shuming Jiao et al., 2019).

For all watermarking systems, robustness is a critical property. There are so many causes for watermark being damaged, altered during transmission, and targeted in pay media applications by hackers. Therefore, the watermark is should be robust, that it can withstand all attacks and threats. The security of watermarking is characterized by the ability of

the watermark to withstand attacks. An attack is any processing in watermarking terminology that may hinder the identification of the watermark or the transmission of the information conveyed by the watermark. An active attack changes the watermarked image directly, where there are no passive attacks. Many successful attacks specifically bypass the watermarking process and are often marked as an attack on the systems (A.S.Kapse et al., 2018).

The false-is when the watermark identification or detection does not contain any watermark on it, expected in detector's precondition runs. Similarly, the probability of any precondition detector powered by a false positive event can be debated. Two particular ways are available in describing the mentioned probability. The two differ in whether the host image or the watermark is the subjective parameter considered. The false-positive instance from the first example is the odds that might be settled or autocratically selected in the watermarks is preconditioned. Where the detector must say, that watermark is present in that image (Anuja D., Rahul D., 2017).

Payload means the quantity of data involving watermarking. High watermark payload refers to the method of hiding large amounts of data. The main factors that affect payload are image or data length, embedding frequency, the roughness of the image, visual sensitivity, etc. High payload and improved watermark lead to the invisibility of perception (Suhad A. Ali et al., 2017).

2.5. Advantage and Disadvantage of DCT and DWT Techniques

The advantage in using DWT is DWT's time or frequency decomposition features, which imitate the abstract representations of the human visual system. So that is why they have been frequently used. Moreover, to increase the performance of DWT, it is better too, to combine the transform with other techniques (Benoraira A. et al., 2015).

Meanwhile, the good side of using the DCT is, it works by splitting the image into sections of different frequencies ranging from low to high

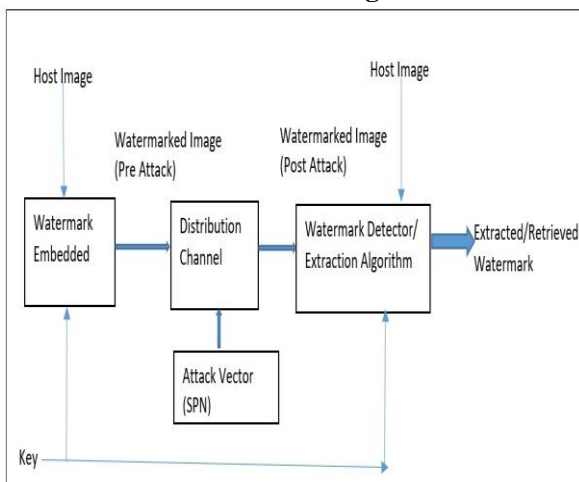
frequency coefficients. So, making it much easier to incorporate the watermark information into the medium frequency band thus, giving additional resistance to the loss compression techniques while preventing major changes in the cover image. The DCT has the property of very strong energy compaction (M. Pooja Prakash et al., 2018). However compared to DWT, DCT lacked in the speed of simulation time, based on Ankita Agrawal and Anubha Prajapati (2017) finding, which is the simulation time is 1.48 seconds for the DCT, and 0.9 seconds for the same image size for DWT that tested on ten pictures. So, DWT can be determined to be much quicker than DCT.

In this project, the two techniques are combined so that their disadvantage can complement each other, just as how DWT has to be combined with other techniques to enhance its performance, and so do DCT.

III. RESEARCH METHODS

The Every digital watermarking method includes two algorithms: one for the embedding algorithm and other as the detecting algorithm. These two processes are similar for all the type of watermarking methods.

Figure 1 – Research Design of Digital Watermarking



The context diagram in Figure 1, shows the overall view of the watermarking process. The watermark embedded into the host image and exposed to the insecure phase that exposed to noise attack. After the watermarked images tested the attack, an extraction algorithm has

been used to retrieve the watermark back. Then, the watermarked image was analyzed according to the properties of watermarking to observe if there are some alterations or damage to the watermark from the attacks. Thus, evaluating and analyzing process were done to determine whether the watermark can be considered as robust enough, for instance.

Below is the overall process of the digital watermarking using DCT-DWT technique on the image, divided into two according to the embedded process and extraction.

Figure 2 – Embedding process flow chart of watermarking

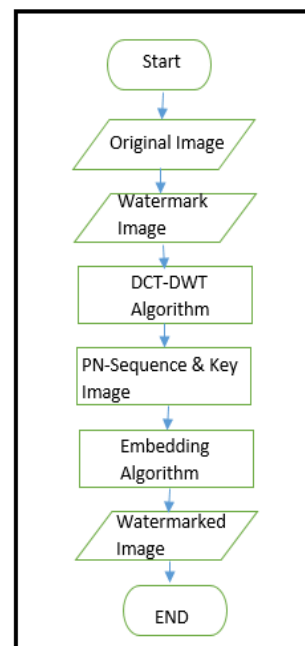
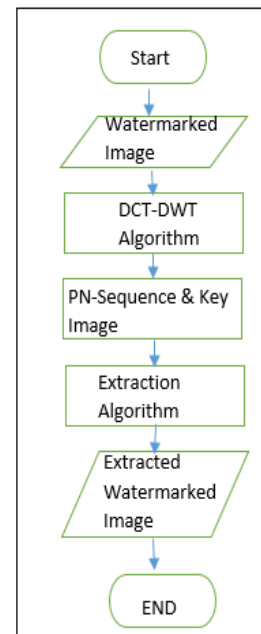


Figure 3: Extraction process flowchart of the retrieved watermark



The process flowchart in Figure 2, shows the process of embedding watermark into the host image. DCT-DWT watermarking scheme is embedded into the original image with a DCT-DWT and calculation of PSNR values before the watermarked algorithm is embedded to the image.

Figure 3 shows the process flowchart of the watermark after being retrieved from the distribution stage, which tested by noise attack using an extraction algorithm.

3.1. Selecting the Cover Image and Watermark Image Process

To watermark the original/cover image with another secrete image, selecting process has

been done to load the image after the button of 'Select Image' and 'Select Watermark' being executed. The selecting process has been done by using the test image, which is the 512 x 512 grayscale cover image and 8-bits length of watermark image. The file type of the test image is .bmp format.

3.1.1. Embedding Process

The embedding process starts with defining the DWT phase where the cover image has been decomposed into four frequency bands, which is the first pass level of DWT (LL, LH, HL and HH) frequency coefficients along with the Haar Wavelet Transform. The DWT was applied to the sub-bands to get another four smaller sub-bands (LL1, LH1, HL1, and HH1). All sub-bands were tested to determine which sub-bands should be chosen to have a more imperceptible and robust watermark in using this combined or hybrid techniques.

As for DCT, the image is being broken into four 8x8 blocks so that the function and the image blocks can be computed separately. Then, all the cover and watermark images' details were converted into the frequency components based on the domain. After both images have been converted, the middle-band frequency is chosen because the human eye is sensitive to existing noise that might appear on low frequency that may cause the watermark become perceptible. In contrast, if the high-frequency band is used, the watermark will be affected by means discarded.

Next process is reading through the cover or original image by determining the size of the cover image such that in height and width M_c and N_c respectively and to determine the maximum message of the watermark image concerning the cover image and the block size and converting the message into a vector.

The PN sequence is embedded into the middle-bands components of the DCT blocks. If the watermark bit contains 0, then the PN sequence zero is used and if the watermark bit contains 1, then PN sequence one is used instead.

3.1.2. Watermark Retrieval Process

The retrieval process had combined both DCT and DWT retrieval techniques to retrieve back

the watermark image. Firstly, both DCT and DWT function is needed to be applied to the watermark image and watermarked image. The DCT function is applied as the watermarked image needed to be transformed into the frequency domain. While for DWT, the image has been decomposed once more into four frequency bands, through the 1st and 2nd pass level as described previous section.

For DCT, the retrieval process is started by identifying the middle-bands of the images to generate the reduced image and applying them to the watermark blocks to start detecting the bits where the watermark is embedded. Meanwhile, DWT will then compare the difference of the decomposed image in LL1/LH1/HL1/HH1 sub-bands. As the cross-relation has detected a peak in the watermarked image, therefore the watermark image is retrieved from the combined retrieval techniques.

In this process, the correlation factor is also calculated concerning the PN sequence. Correlation factor is the measuring degree of similarity between two images. In this project, the correlation factor is measured after the watermark image is retrieved from the retrieval process until the filtering process after the attack is launched for the image that acted as the watermark.

3.1.3. Salt and Pepper Noise Attack Process

The attack used on the watermark image is salt and pepper noise. After the watermarked image is loaded, the pushbutton "Add Noise" would make the attack launched on the watermarked image. This is to test the robustness of the techniques used. As the input space is enabled, the edit space needed to be defined with 'amunt' instead of defining any range or numbers for its to function accordingly. The noisy image, which is the image that has been attacked, is defined with the variable (h) and imnoise function is declared with the chosen noise type, which is the salt & pepper noise.

3.1.4. Noise Filtering Process

For the salt and pepper noise filtering, a median filter is used to filter the noise from the watermarked image. The median filter is chosen

due to its properties because the filter is less sensitive compared to the linear technique since it can filter the salt and pepper noise without significantly reducing the picture sharpness.

3.2. Watermark Extraction Process

The same techniques do the extraction of the watermark image after the filtering process as the retrieval process but the techniques used are applied to the filtered image and watermark image. For the extraction process, both DCT and DWT techniques are combined to extract back the filtered image and watermark image. Firstly, both DCT and DWT function is needed to be applied to the filtered image and watermark image. The DCT function is applied to the filtered image as it needed to be transformed into the frequency domain. While for DWT, the image is decomposed once more into four frequency bands.

For DCT, the extraction process is started by identifying the middle-bands of the images to generate the reduced image and applying them to the watermark blocks to start detecting the bits where the noise is attacked into. Meanwhile, DWT will then compare the difference of the decomposed image in the chosen bands. As the cross-relation has detected a peak in the filtered image, therefore the watermark image is extracted from the filtered image after the attack and the correlation factor is also being measured in this process.

3.3. Peak Signal-to-Noise (PSNR)






For the PSNR value, it is measured in decibel (dB). It is the parameter used to measure the imperceptibility of the watermark embedded into the original image. The higher the PSNR value also, the better the re-constructed image in comparison with the original. In this project, the PSNR is only measured for the watermarked image.

IV. RESULT AND ANALYSIS

For the result and analysis, a table is constructed to compare the measuring parameter, which is the PSNR value and correlation factor based on the test image top-sec.bmp on different sub-bands of DWT, HL1 and HH1.

Based on Table 4.1, there is a significant difference between the PSNR values of the images as DWT is applied to the different sub-bands. By the value, the imperceptibility of the techniques used can be shown by the higher PSNR between the images. For LL1, the PSNR value has the lowest, which is 0.074, indicates that if that sub-band is chosen, the imperceptibility of the watermark will not be achieved. Meanwhile, for the sub-bands LH1, the value is higher than LL1 with 61.6011 but still lower compared to sub-bands HH1.

Table 1: Comparison value of PSNR in LL1, LH1, HL1 and HH1

Original Image top-sec.bmp	LL1	LH1	HL1	HH1
				
	PSNR value: 0.0743	PSNR value: 61.6011	PSNR value: 96.6103	PSNR value: 65.0094

The highest PSNR value achieved is through sub-bands HL1 with a value of 96.6103. This indicates that to achieve a higher value of imperceptibility, sub-band HL1 needs to be chosen to apply DCT transform on the DWT sub-bands. However, the correlation factor value has to be taken into account too to determine whether the sub-bands HL1 should be chosen to have both imperceptibility and robustness of the techniques used.

Table 2: Correlation Factor(CF) on Salt & Pepper Noise Attack between sub-bands

Sub-bands \ Noise Ratio	0.2	0.4	0.6	0.8	1.0
LL1	0.62106	0.665-63	0.636594	0.672328	0.646637
LH1	0.972251	0.814781	0.725875	0.687115	0.659415
HL1	0.876412	0.722741	0.692543	0.692578	0.679093
HH1	0.594076	0.589738	0.623107	0.643123	0.677067

Based on Table 2, which is the correlation factor value, the sub-band HH1 showed the lowest correlation factor value at the lowest value of noise attack compared to other sub-bands. Even with the lowest attack value, sub-band HH1 did not show excellent performance in terms of robustness against the attack, thus, eliminate the sub-band from being the chosen one. Meanwhile, between LL1 and LH1, LH1 showed better performance by having a higher correlation factor value compared to LL1 even though LL1 has higher PSNR value earlier. However, the correlation values of HL1's result clearly stated that if the hybrid techniques are applied on the sub-bands, it gives better robustness against noise attack started from the value 0.972251 compared to all other sub-bands. Other than that, the sub-band HL1 also has an excellent performance in terms of imperceptibility as it also has the highest PSNR value too.

Comparison table of PSNR and correlation factor between LL1, LH1, HL1 and HH1 sub-bands

Table 3: Comparison of PSNR and Correlation Factor value of all four bands

Parameter	LL1	LH1	HL1	HH1
PSNR Value	Low	Moderate	Highest	Moderate
Correlation Factor Value	Low	Highest	High	Lowest

Based on the comparison on Table 3 of PSNR and correlation factor values, LL1 showed low overall performances in both parameters. That eliminates it right away from being chosen as the sub-bands to apply DCT transform on the DWT sub-bands in both embedding and retrieving/extracting process. Even though LH1 has the highest value for correlation factor it still has moderate value for PSNR value in comparison with the other two remaining sub-bands HL1 and HH1. For sub-bands HH1, even though it has moderate PSNR value, it still isn't enough to choose it as it showed the lowest value in correlation factor which is crucial for the robustness properties of the watermark.

For the sub-bands HL1 based on its high performance on both PSNR and correlation factor, obviously it has an overall good performance in order to be chosen. This is because by its high value in PSNR, it surely can achieve the imperceptibility properties of watermarking. And for its high value of correlation factor, it also able to achieve the robustness properties of watermarking too as it has a high or the highest value even after attack. To achieve the excellent overall performance of the combined techniques used, the sub-bands chosen to embed and to extract the watermark are also crucial because there are significant changes between the sub-bands used too. Aside from that, the hybrid watermarking techniques also can resist salt and pepper noise attack up to the highest value 1.0 as the extraction of the watermark is successfully recovered after regardless of their correlation factor values.

V. CONCLUSION

The DCT-DWT based algorithms were successfully developed and fulfilled the objectives of the project by producing watermarking techniques that achieved an excellent performance in securing the images from the digital attack in terms of imperceptibility and robustness of the watermarking techniques used. The main objective of this project is to develop hybrid watermarking algorithms from DCT and DWT watermarking schemes. Meanwhile, the project aims to analyze and evaluate the performance of the proposed algorithm.

Throughout the project development phase, all the objectives have been fulfilled. This can be seen through the previous chapter, where the algorithms and combined techniques are used along the watermarking until the extraction process of the image. Based on the testing process, all the sub-bands of DWT are tested to find which sub-bands have to be chosen to produce a final algorithm when it is being combined with the DCT transform. As stated in the result, the sub-bands HL1 is chosen due to its high PSNR and correlation factor values that

resulted in high imperceptibility and robustness of the watermarking techniques used..

BIBLIOGRAPHY

1. A. JAIKUMAR; K. SATHISHKUMAR; W. MESIYASTALIN. An Analysis on Digital Watermarking Techniques for Several Applications. *International Research Journal in Global Engineering and Sciences*, vol 2(1), p. 71-76, 2017
2. A. S. KAPSE; SHARAYU BELOKAR; YOGITA GORDE; RADHA RANE, SHRUTIKA YEWTKAR. Digital Image Security Using Digital Watermarking. *International Research Journal of Engineering and Technology (IRJET)*, vol5(3), p. 163-166, 2018
3. AAQIB RASHID. Digital Watermarking Applications and Techniques: A Brief Review. *International Journal of Computer Applications Technology and Research*, Volume 5–Issue 3, p. 147-150, 2016
4. ANKITA AGRAWAL; ANUBHA PRAJAPATI. A Review of Digital Watermarking Technique for The Copyright Protection of Digital Data using Transform Function. *International Research Journal of Engineering and Technology*, vol 4(10), 2017
5. ANUJA DIXIT; RAHUL DIXIT. A Review on Digital Image Watermarking Techniques. *International Journal of Image, Graphics and Signal Processing*, vol 4, p. 56-66, 2017
6. BENORAIRA A.; BENMAHAMMED K.; BOUCENNA N;. Blind image watermarking technique based on differential embedding in DWT and DCT domains. *EURASIP J. Adv. Signal Process.*, p. 55, 2015
7. G. S. PRADEEP GHANTASALA. A Study on Features, Types, Applications and Techniques of Digital Image Watermarking, *International Journal of Computer Science & Engineering Technology*, vol8(8), p. 331-334, 2017
8. KAUSHIK H. RAVIYA; DWIVEDIVED VYAS; ASHISH M. KOTHARI. Image Watermarking – Hybrid Approach for Embedding Binary Watermark into the Digital Image. *International Journal of Recent Technology and Engineering*, vol 9(4), p. 397-401, 2020
9. KOMAL M. LANDE. Survey Of Digital Watermarking Techniques And Its Application. *International Research Journal of Engineering and Technology*, vol 6(6) p. 437-441, 2019
10. L. SINGH; AK SINGH; PK SINGH. Secure data hiding techniques: a survey. *Multimedia Tools Application* 79, 15901–15921, 2018
11. M. POOJA PRAKASH; R. SREERAJ; FEPSLIN ATHISHMON; K. SUTHENDRAN. Combined Cryptography And Digital watermarking For Secure Transmission of Medical Images in EHR Systems. *International Journal of Pure and Applied Mathematics*, vol 118(8), p. 265-269, 2018
12. MAHBUBA BEGUM; MOHAMMAD SHORIF UDDIN. Digital Image Watermarking Techniques: A Review. *Journal of Information*, vol 11, 2020
- 13.
14. MARILOU O. ESPINA; ARNEL C. FAJARDO; BOBBY D. GERARDO; RUJI P. MEDINA. Multiple Level Information Security Using Image Steganography and Authentication. *International Journal of Advanced Trends in Computer Science and*

- Engineering, vol 8(6), p. 3297-3303, 2019
15. OMAR YOUNIS ABDULHAMMED. Improving Encryption Digital Watermark by Using Blue Monkey Algorithm. *Journal of Computers*, vol 20(1), p. 129-135, 2021
 16. PARMALIK KUMAR; A. K. SHARMA. Analysis of Digital Watermarking Techniques Using Transform-Based Function. *International Journal on Future Revolution in Computer Science & Communication Engineering*, vol 3(6), 2017
 17. POONAM; SHAIKALI M. ARORA. A DWT-SVD based Robust Digital Watermarking for Digital. *Procedia Computer Science* 132 (2018), p. 1441–1448, 2018
 18. SHUMING JIAO; CHANGYUAN ZHOU; YISHI SHI; WENBIN ZOU; XIA LI. Review on optical image hiding and watermarking techniques. *Journal of Optics and Laser Technology*, vol 109, p. 370-380, 2019
 19. SUHAD A ALI; MAJID JABBAR JAWAD; MOHAMMED ABDULLAH NASER. Copyright protection for digital image by watermarking technique. *Journal of Information Processing Systems* 13(3), p. 599-617, 2017
 20. VASUDHA B. SANKPAL; R.N.PATIL. A Review on Different Digital Watermarking Techniques. *International Journal of Innovative Science and Research Technology*, vol 2 (10), p. 453-458
 21. YONGQIANG MA; SHUNLI WANG; JINPING SONG; YANDONG YU; WEI SUN, JING BIAN. Comparison of the Schemes in Digital Image Watermarking Techniques. 2nd International Conference on Electronic Engineering and Informatics, Indonesia, p 1-4, 2020