A Reversible Watermarking Technique Using DCT, DWT and Adaptive Thresholding

ROHAN CHAND

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
VEER SURENDRA SAI UNIVERSITY OF TECHNOLOGY

MAY-2023

A Reversible Watermarking Technique Using DCT, DWT and Adaptive Thresholding

A major project submitted in partial fulfilment of the requirements for the

Degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

By

ROHAN CHAND

Registration No.: 1902041048

Under the Guidance of

Ms. Alina Dash

Assistant Professor

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

VEER SURENDRA SAI UNIVERSITY OF TECHNOLOGY

BURLA

VEER SURENDRA SAI UNIVERSITY OF TECHNOLOGY, BURLA, ODISHA

Declaration

I declare that this written submission represents my ideas in my own words and where other ideas or words have been included. I have adequately cited and referenced the original sources. I also declare that I adhered to all principles of academic and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will cause disciplinary action by the university and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

DATE:

Rohan Chand

Regd. No.: 1902041048

VEER SURENDRA SAI UNIVERSITY OF TECHNOLOGY, BURLA, ODISHA

Certificate

This is to certify that the major project report on "A Reversible Watermarking Technique Using DCT, DWT and Adaptive Thresholding" submitted by ROHAN CHAND, Registration No.: 1902041048, 8th Semester, Bachelor of Technology is approved for the degree of Bachelor of Technology in Computer Science and Engineering, is a record of an original research carried out by him under my supervision and guidance.

Dr. Suvasini Panigrahi
Head of the Department

Ms. Alina Dash
Supervisor

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my supervisor, Mrs. Alina Dash, for her invaluable help during the course work towards this dissertation. She was a source of constant ideas and encouragement and provided a friendly atmosphere to work in. I am really very thankful to her for everything. I am also thankful to Dr. Suvashini Panigrahi, Head of the Department and to all the faculties of Department of Computer Science and Engineering for having supported me to carry out this dissertation and for their constant advice. I would like to thank all my friends for their encouragement and understanding. I would like to express my heart-felt gratitude to them.

Rohan Chand

Regn. no.: 1902041048

<u>Approval Sheet</u>

This major project entitled "A Reversible Watermarking Technique Using DCT, DWT and Adaptive Thresholding" by **Rohan Chand** is approved for the degree of Bachelor of Technology in "Computer Science and Engineering", department of computer science and engineering.

DATE: Examiner

PLACE: Burla

Supervisor

ABSTRACT

In this report, I propose a “A Reversible Watermarking Technique Using DCT, DWT and Adaptive Thresholding” for copyright protection and authentication.

In my scheme, the technique involves the insertion of a unique watermark signal into the host image, which can later be extracted to prove ownership. Here, I have implemented a novel reversible watermarking scheme that embeds a watermark into the discrete cosine transform (DCT) coefficients of an image. The scheme first decomposes the image into non-overlapping 8x8 blocks, applies a 3-level discrete wavelet transform (DWT) on the watermark, and uses an adaptive thresholding method to select the required DC coefficient. Then the watermark is embedded in the DCT coefficients of the host image. The watermark and the host image can be extracted from the resultant image with ease by applying an inverse DWT and inverse DCT. Also, the images are subjected to various attacks to determine the robustness of the technique. Experimental results show that the proposed scheme achieves high image quality and robustness against common image processing attacks.

Keywords: **Reversible watermarking; Discrete Cosine Transform (DCT); Discrete Wavelet Transform (DWT); DC coefficient; adaptive thresholding.**

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

A watermark shows the presence of mark hidden in an anti-noise signal, for example an image, video or audio sample to protect the integrity and uniqueness of the signal. There are currently multiple types of advance watermarking techniques depending on the application. For example, in the production of various digital data such as music, video, images, and audio that contain proprietary information, the watermark should be fairly tolerant to manipulation of carrier signal.

Visible Watermarks: They are clearly visible to the naked eye.

Invisible Watermarks: These watermarks are embedded inside the image and use steganographic techniques. They are invisible to the human eyes.

Public Watermarks: These watermarks can be analyzed and changed by anyone with a particular algorithm. These are not generally not secure.

Fragile Watermarks: These can be destroyed and hampered by data manipulation. If you use fragile watermarks, you need to put in place a system that can detect data changes.

Watermarking process (lifecycle): Information has to be embedded inside the transmitted media. The embedded signal is considered as the host signal and its information content is mainly the watermark. Watermarking includes mainly three parts:

1. Embedding - This part embeds the watermark into the digital signal.
2. Attack – When the transmitted data is altered, it becomes a threat and hence called an attack.
3. Protection - Detecting watermarks from noisy signals that may have modified media due to different kinds of attacks is called protection.

1.1 MOTIVATION

Digital watermarking is considered one of the crucial methods for the protection of copyrights and authentication of ownership of digital content such as images, videos, and audio files. Watermarking allows content creators to embed a unique identifier into their content that can be used to prove ownership or detect unauthorized use of the content. Reversible watermarking is especially useful as it allows the original content to be recovered without any loss of information, which can be important in applications such as forensics and legal evidence.

The proposed scheme for reversible watermarking using DCT and DWT transforms provides a robust and secure method for embedding and extracting watermarks in digital images. The use of DCT and DWT transforms allows for the watermark to be embedded in the frequency domain, which can make it more robust against attacks. The adaptive thresholding method used for embedding the watermark also allows for the threshold value to be adjusted w.r.t the image’s characteristics and watermark used, making it more flexible and robust. Overall, the proposed scheme can be a valuable tool for protecting digital content and is utilized for multiple operations such as copyright protection, ownership identification, and detecting tamper.

1.2 OBJECTIVE

The objectives of the designed reversible watermarking scheme are:

To embed a unique identifier (watermark) in digital images for copyright protection and ownership identification.
To ensure the extraction of cover image without losing any important information, making it suitable for forensic and legal evidence.
To provide a robust and secure method for watermarking that is secure against common attacks on images like compression, adding noise, rotation and scaling.

2. BACKGROUND STUDY

2.1 Reversible Watermarking

Reversible watermarking is a technique used to embed additional information into digital images without affecting the original image. This method ensures that the hidden information can be removed and the original host image can be fully restored without any loss of data. To achieve this, reversible watermarking modifies the least significant bits of the image pixels in a way that is visually imperceptible to the human eye but can be detected by an appropriate algorithm. This method is useful for protecting the copyright of digital images or ensuring the authenticity, robust nature and perceptibility of the image. However, reversible watermarking can be more complex and computationally intensive than non-reversible techniques.

2.2 Discrete Cosine Transform

Discrete Cosine Transform, is a transformation tool used in image watermarking to convert an image from spatial domain to the distributed frequency domain. In DCT-based methods, the watermark is first converted into the frequency coefficients using DCT and then embedded into selected frequency components of the image by modifying their coefficients. High-frequency coefficients are often chosen for this purpose, as they are less visually significant to the human eye and can thus tolerate some distortion.

2.3 Discrete Wavelet Transform

DWT, is a transform tool used in the field of digital watermarking to decompose an image into multiple frequency bands. In DWT-based watermarking, the watermark is transformed into the frequency domain using DWT and placed into selected sub-bands of image by modifying the coefficients of sub-bands. The embedding process usually involves modifying the higher frequency sub-bands, as they are less visually significant and can, therefore, tolerate some level of distortion.

The inverse DWT is used to reconstruct the original image from the watermarked image. The watermark can then be extracted from the modified coefficients of the sub-bands using a similar technique as used during embedding. DWT-based watermarking is robust to various image processing operations, such as cropping, rotation, and compression, making it a popular choice for digital image watermarking applications. However, it can suffer from perceptual quality degradation and vulnerability to certain attacks, such as noise addition and filtering. Therefore, it is necessary to use additional security measures to ensure the watermark's integrity.

2.3.1 Levels of Discrete Wavelet Transform (DWT)

There are various levels at which DWT is applied. I have used a 3 level DWT on the watermark. The levels of DWT are:

Level 1 DWT:

The first level of the DWT divides the original image into four sub-bands: LL1, LH1, HL1, and HH1. LL1 represents the low-frequency content of image, while LH1, HL1, and HH1 represent the horizontal, vertical, and diagonal high-frequency details. The LL1 sub-band is further divided into four smaller sub-bands using the same DWT process. Watermark is embedded in the LH1 sub-band because it has the highest frequency content and is less sensitive to image processing operations like cropping and resizing.

Level 2 DWT:

The 2 level of the DWT decomposes the LL1 sub-band from the first level into 4 sub-bands: LL2, LH2, HL2, and HH2. The watermark is merged in the LH2 sub-band because it has the highest frequency content among all the sub-bands present in the second level.

Level 3 DWT:

The third level of DWT decomposes the LL2 sub-band from the second level into four sub-bands: LL3, LH3, HL3, and HH3. Watermark is merged in the LH3 sub-band as it contains highest frequency content among all the sub-bands in the third level.

Three-level DWT in image watermarking involves decomposing an image into 4 different sub-bands and embedding a watermark in it with the highest frequency content. The DWT is performed at three different levels, with each level representing a different frequency band. Watermark image is typically embedded through modifying coefficients of the selected sub-band, and can be extracted from watermarked image by applying the same DWT process used during the embedding process.

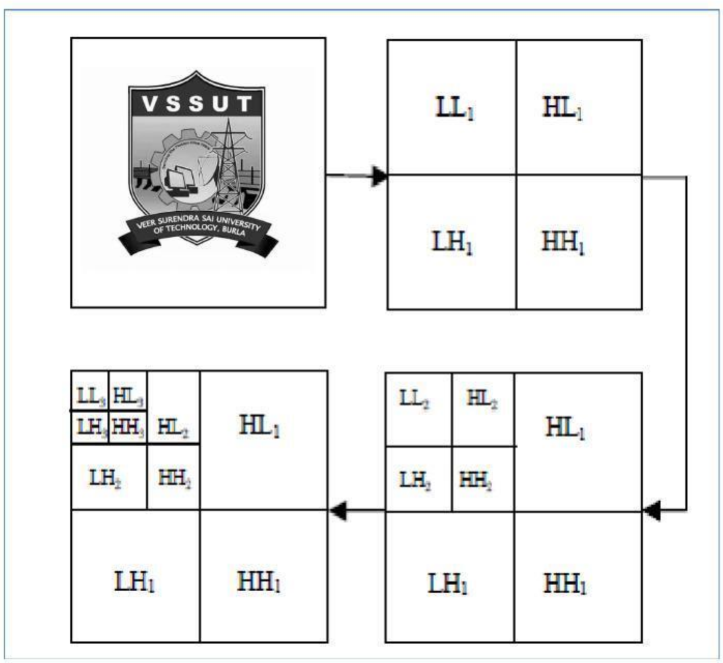

Figure 2.1 Stages of 3-Level DWT

Another example showing different sub-bands of DWT is:

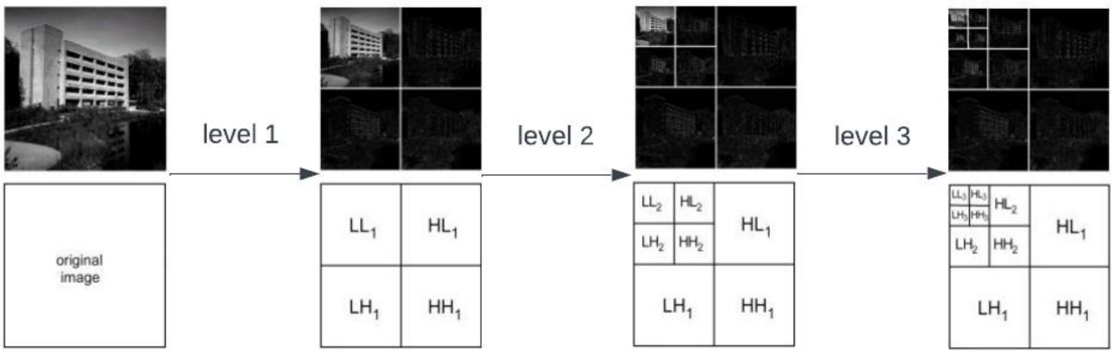

Figure 2.2 Image undergoing 3-level DWT

2.4 Adaptive Thresholding

Adaptive thresholding is a large-scale used technique in digital image watermarking to enhance the robust ability of watermark from different image processing operations. This involves setting a different threshold value for each pixel depending on its local image properties, such as neighboring pixels' intensities or variance.

Adaptive thresholding is a method used to determine whether to embed a watermark in a particular DCT coefficient in a given scheme for reversible watermarking using DCT and DWT transforms. The method involves comparing the absolute value of each DCT coefficient with a threshold value that is determined by the standard deviation of LL sub-band coefficients of image block.

Adaptive thresholding is carried out by the following steps:

First, an input cover image is decomposed into blocks of size 8x8, and DCT is operated on each individual block.

Then, watermark is subjected to a 3-level DWT, dividing it into multiple sub-bands of frequency.

For each DC coefficient, the absolute value of the coefficient is compared with a threshold value that is determined by the standard deviation of LL3 sub-band of watermark block. If the absolute value of DC coefficient is greater than the threshold value, watermark is embedded in the DCT coefficient.

The threshold value is calculated using the standard deviation of LL sub-band, which provides an estimate of the noise level in the watermark.

If the absolute value of DC coefficient stays below the threshold value, it is left unchanged.

After embedding the required image watermark in the appropriate DC coefficients, inverse DCT is performed to obtain the resultant watermarked image.

Adaptive thresholding is beneficial because it allows for the threshold value to be adjusted according to the characteristics of host image and used watermark. This can improve the robustness of provided watermark and data against attacks and can also increase the embedding capacity. By using this method, the discussed scheme has the ability to embed the watermark in most appropriate DC coefficients, making it more effective in protecting the digital content.

2.5 DC coefficient

The zero-frequency component of the DCT transform is called as Direct current coefficient. It is the average value of pixel intensities in an 8x8 block of input image after applying DCT.

If DC coefficient's actual value is above the threshold value, then watermark embedding is done inside DC coefficient taking help of a quantization factor, which decides how many bits of watermark to embed. This process is repeated for all the 8x8 blocks of the taken image.

The DC coefficient in watermarking is effective because it is the most significant coefficient of the DCT transform and has a large impact on the image quality. By embedding the watermark in DC coefficient, the method proposed confirms that provided watermark remains hidden and can survive common image processing operations.

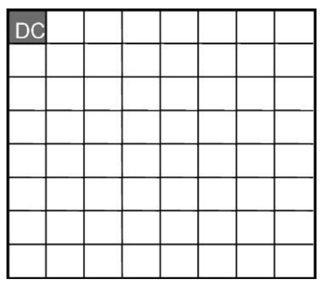

Figure 2.3 DC coefficient in a block

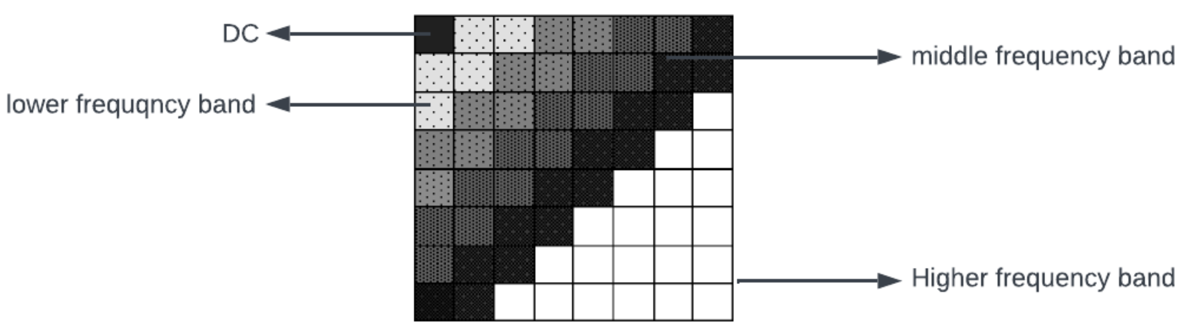

Figure 2.4 Frequency coefficient distribution in a block

3. LITERATURE SURVEY

In previous times many research works have been conducted in the field of reversible watermarking to increase the watermark's sensitivity, which makes it more exposed to minor alterations. The process of various methods used for embedding an image are done to preserve the integrity and extractability of the image. Some of such algorithms proposed recently are mentioned below.

- D. Ariatmanto et al. (2022) [1] proposed a scheme where Adaptive scaling factors based on impact of selected DCT coefficients and the use of DCT coefficients for embedding. The authors focus on the use of adaptive scaling factors related to impact of selected DCT coefficients, highlighting the importance of selecting appropriate coefficients for embedding process and proposing a method for calculating adaptive scaling factors based on the coefficients' impact. Mentioned technique is evaluated using various metrics, demonstrating its superiority compared to other existing watermarking techniques in the areas of robustness and imperceptibility. They presents an important contribution to the image watermarking platform and can be useful in various image watermarking applications.

- Ferda Ernawan et al. (2021) [2] presented an Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients, which presents an overview of existing literature on image watermarking techniques, including both spatial and transform domain approaches. They focus specifically on DWT-DCT-based watermarking techniques, highlight the need for an improved approach, and discuss the importance of selecting appropriate coefficients for watermark embedding. The authors present their proposed technique involving modifying selected DWT-DCT coefficients and evaluate it using various performance metrics, demonstrating its superiority compared to other existing watermarking techniques.

- Nayeem Hasan et al. (2021) [3] published a paper where, Encryption Based Image Watermarking Algorithm was used in 2DWT-DCT Domains. The paper presents an overview of existing literature on image watermarking techniques and encryption-based approaches, highlighting their strengths and weaknesses. The authors specifically focus on 2DWT-DCT-based watermarking techniques, discuss the importance of selecting appropriate coefficients for watermark embedding, and present the existing methods for coefficient selection and their limitations. They propose a watermarking algorithm based on encryption and evaluated its performance using various metrics, demonstrating its superiority compared to other existing watermarking techniques.

- S. V. Malik et al. (2017) [5] implemented Digital Watermarking using DWT-SVD Algorithm. It presents a literature study of digital watermarking techniques with their applications. The authors discussed the use of discrete wavelet transform and singular value decomposition algorithms for watermarking and their advantages over other techniques. They present a DWT-SVD algorithm for embedding the watermark into the host image, and a watermark extraction technique based on inverse transform. The proposed technique is evaluated using various metrics, demonstrating its effectiveness. The paper provides an important contribution to the field of digital watermarking and can be useful in various digital image protection applications.

- Leng X. X. et al. (2013) [10] published a paper on Digital Image Zero-watermarking Technology. It provides a review of zero-watermarking techniques. The authors discuss the limitations of traditional watermarking techniques and how zero-watermarking overcomes these limitations by embedding the watermark information in the image itself rather than altering the pixel values. They present various zero-watermarking techniques, including the use of DCT, DWT, and (SVD). The paper also discusses the challenges associated with zero-watermarking, such as attacks and false detection, and presents some potential solutions. Overall, the paper provides a valuable contribution to the field of digital image watermarking and can serve as a reference for researchers interested in developing zero-watermarking techniques.

Table 3.1: Summary of Related work:

SL No.	Author details	Techniques Used	Results
1	D. Ariatmanto et al. (2022) [1]	DCT-based watermark embedding and Adaptive scaling factors.	Proposed method achieved higher PSNR and NC compared to other methods. Adaptive scaling factors improved robustness against common attacks
2	Ferda Ernawan et al. (2021) [2]	Modified selected DWT-DCT coefficients for watermark embedding	Proposed method showed better robustness against common attacks and higher SSIM compared to other methods
3	Nayeem Hasan et al. (2021) [3]	2DWT-DCT-based watermark embedding. Encryption using Advanced Encryption Standard (AES)	Proposed method showed better robustness against common attacks and higher PSNR compared to other methods
4	S. V. Malik et al. (2017) [5]	DWT-SVD-based watermark embedding	Proposed method showed good performance on robustness against common attacks and achieved higher PSNR compared to other methods
5	Leng X. X. et al. (2013) [10]	Zero-watermarking method based on the mean value of image blocks	Proposed method achieved higher NC compared to other methods in zero-watermarking scenarios

4. WORK DONE

I have proposed a reversible watermarking scheme which means that the host image and provided watermark can be extracted without any distortions after the embedding process. The proposed method decomposes image into 8x8 non-overlapping blocks and applies the discrete cosine transform (DCT) on each decomposed block. The DCT is a transform technique that converts an image from spatial domain to a range of frequency domain.

The adaptive thresholding method compares the absolute value of the DCT coefficient with a threshold value that is determined by the standard deviation of LL sub-band of DWT coefficients of the watermark block. If the absolute value of the DCT coefficient is greater than threshold value, watermark is embedded in the DC coefficient.

To embed the watermark, a 3-level discrete wavelet transform is applied on the watermark image. The DWT is a transform that decomposes a signal or image into different frequency sub-bands. The watermark is then embedded in the DCT coefficients of host image using an adaptive thresholding method.

After embedding, the resultant image is obtained by applying inverse DC Transform to the modified DCT blocks. An inverse DWT is applied to the watermarked image to obtain LL sub-band coefficients. The watermark is then extracted from the LL sub-band coefficients using an adaptive thresholding method.

The embedding scheme is reversible, which means that both the original host image and watermark can be extracted without any loss of information.

Overall, the proposed scheme provides a robust and secure method for embedding and extracting watermarks in digital images while maintaining the data of the original image

The phases of the proposed watermarking framework are:

EMBEDDING ALGORITHM:

1. The original host image and required watermark are taken as input.
2. The original image is decomposed into non-overlapping blocks of size 8x8.
3. DCT method is applied to each block of the image.
4. The watermark is subjected to 3-level DWT
5. Using adaptive thresholding watermark is embedded in the modified coefficients
6. Watermarked image is obtained through inverse DCT.

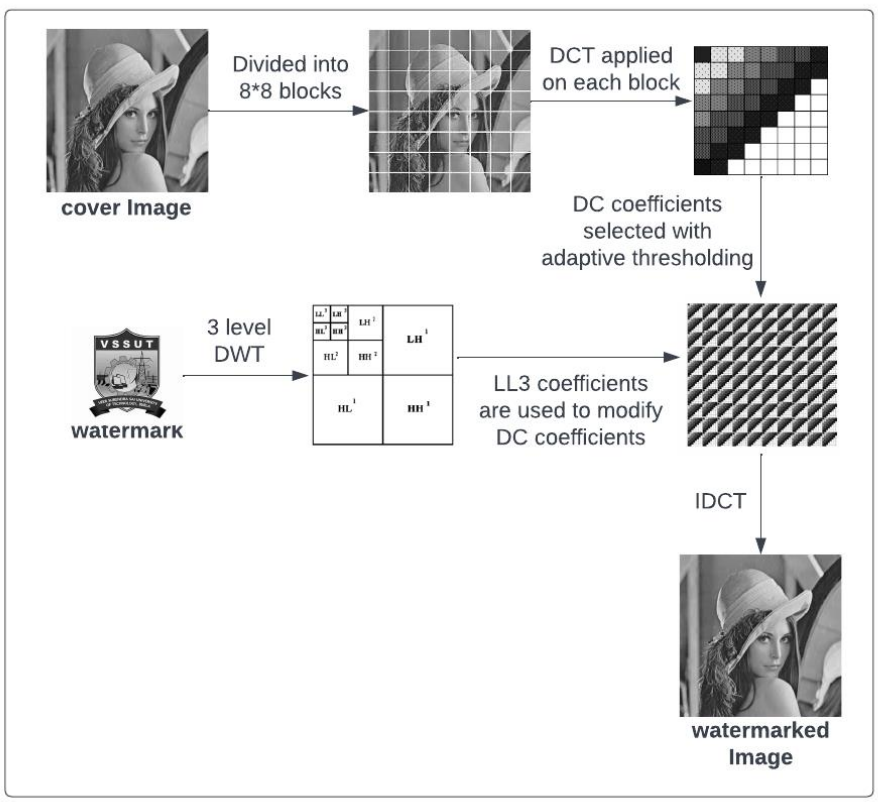

Figure 4.1 Watermark embedding

EXTRACTION ALGORITHM:

1. The watermarked image and required watermark are taken as input.
2. It is divided into 8x8 blocks.
3. DCT is applied on each divided block.
4. Inverse DCT is applied along with thresholding technique to extract cover.
5. Inverse DWT is applied to get the watermark back.

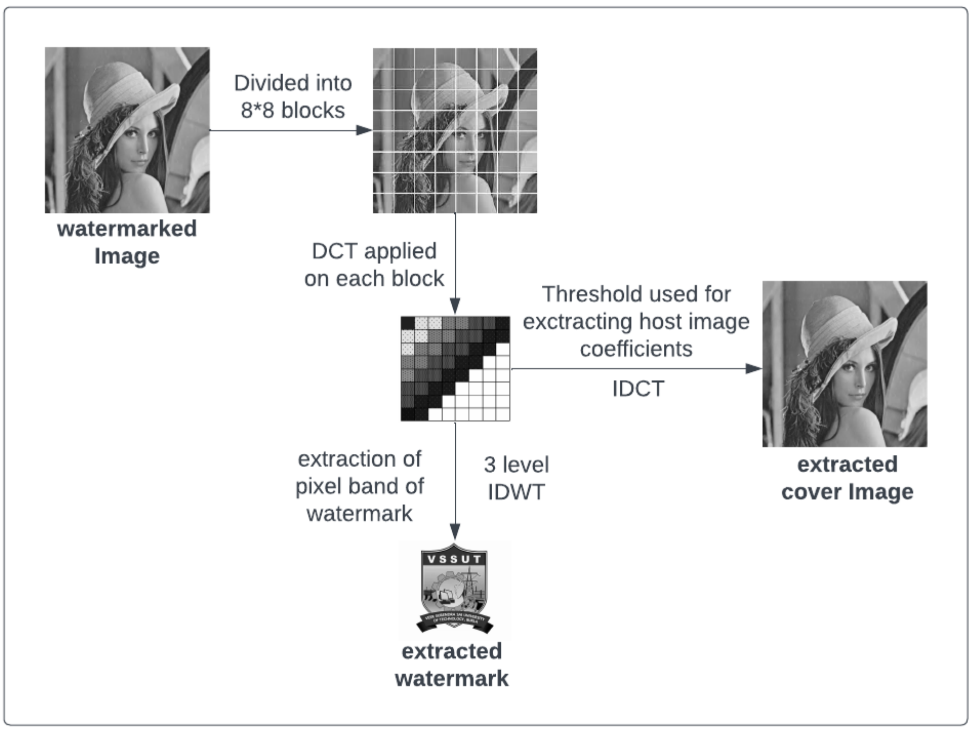

Figure 4.2 Watermark Extraction

5. EXPERIMENT RESULTS

Sample of five 512x512 resolution grayscale images (Lenna, Pepper, Sailboat, Baboon, House) from SIPI image database [14] are taken and used as input images to the watermark embedding process. A small 150x 150 grayscale logo is used as a watermark.

The scheme was trained with the following system specifications:

Processor: Intel Core i7-9750H CPU with 2.60GHz

Memory: 8GB

Programming Language: Python

IDE: Visual Studio Code

Packages Used: OpenCV, NumPy, Matplotlib

Following outputs were derived:

Figure 5.1 Watermarked Images of Test Images

The extraction was performed to obtain the original host image and watermark image:

Figure 5.2 Extraction of Host and Watermark

5.1 Image Quality Metrics

The image quality metrics listed below are used to compare the processed watermarked image to that of the original cover image.

PSNR

The Peak Signal-to-Noise Ratio is the ratio of the maximum possible strength of a given signal to that of the strength of its corresponding noise. It measures the difference, taking into account the amount of noise that was added during the transmission or processing of the signal. Higher PSNR values obtained represents that reconstructed image is closer to the original image. From the different test images used the average value of PSNR obtained is 61.7.

MSE

MSE stands for Mean Squared Error, which is a common measure of the difference between two signals or images. It calculates the average squared difference between the pixel values of two images, with a lower MSE indicating better similarity between the images. From the various test images taken the average value of MSE was calculated to be 0.105.

SSIM

SSIM stands for Structural Similarity Index. It is a widely used image quality metric that measures the similarity between two images based on their structural information, luminance, and contrast. SSIM provides a value between 0 and 1, where 1 indicates perfect similarity between the two images. From the different test images used the average SSIM obtained is 0.99.

NCC

NCC (Normalized Cross-Correlation) is a measure presenting the similarity of two signals or images. NCC is calculated by taking the cross-correlation between the two signals and normalizing it by the standard deviation of each signal. The resulting value ranges from -1 to

1 (1 represents a perfect match, 0 represents no correlation, and -1 shows a perfect anti-correlation. From the sample input images processed the average NCC obtained is 0.99.

BER

BER (Bit Error Rate) is a measure of the error rate in a digital communication system that transmits binary data. It represents the ratio of the total number of bits received that contains errors to the total number of bits which are transferred. If the BER value is lower, the performance of the communication system is considered to be better. Amongst the various sample images taken the average BER % is calculated to be 1.31.

5.2 Performance of the model

The following table 5.1 and table 5.2 depicts various image quality metrics which are calculated by considering the provided input image and the produced watermarked image.

Table 5.1: Image quality metrics (psnr, ssim, ncc, mse, and ber)

IMAGE	PSNR	SSIM	NCC	MSE	BER(%)
Lenna	60.771	0.999	0.999	0.054	0.68
Peppers	64.042	0.999	0.999	0.025	0.32
Sailboat	56.428	0.998	0.999	0.147	1.77
Baboon	74.25	0.999	0.999	0.002	0.03
House	53.334	0.999	0.999	0.301	1.75
Average	61.765	0.998	0.999	0.105	0.91

Table 5.2: comparison of PSNR values with other proposed schemes

IMAGE	Image Size	Chih-Chin Lai [11]	Nasrin M. Makbol et al. [6]	Ferda Ernawan et al. [2]	Dhani Ariatmanto et al. [1]	Proposed scheme
		PSNR (db)	PSNR (db)	PSNR (db)	PSNR (db)	PSNR (db)
Lenna	512 x 512	48.708	44.824	47.176	45.731	**60.771**
Peppers	512 x 512	46.763	43.889	47.158	45.953	**64.042**
Sailboat	512 x 512	45.613	42.479	46.918	43.796	**56.428**
Baboon	512 x 512	35.596	43.301	46.116	45.682	**74.254**
House	512 x 512	40.185	41.944	47.300	43.830	**53.334**
Average		43.373	43.287	46.934	44.998	**61.765**

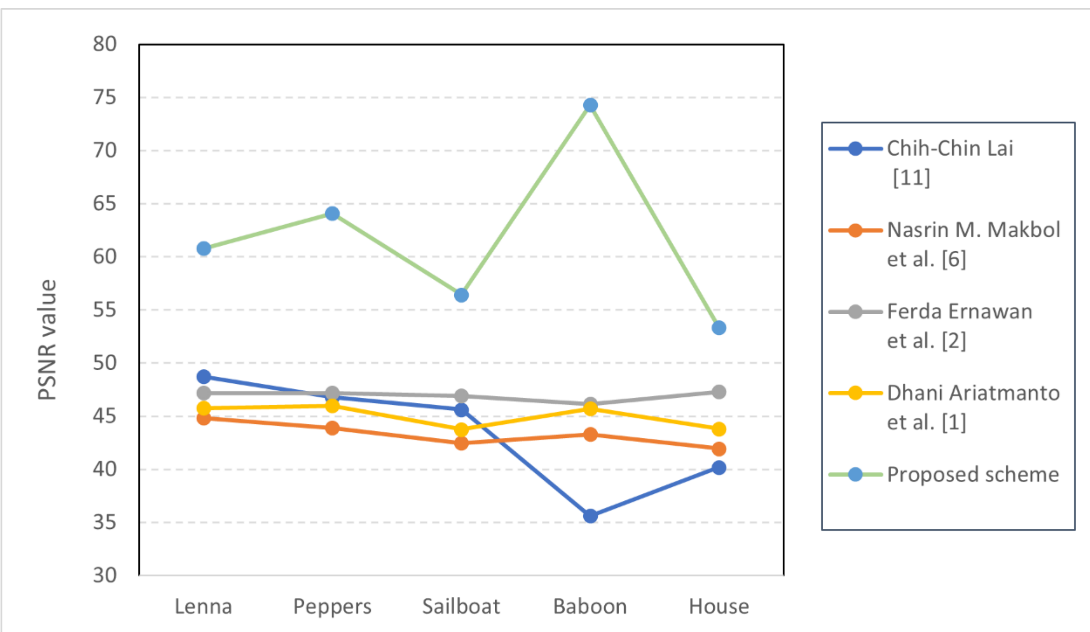

Fig 5.3 Performance Analysis of PSNR values

Table 5.3: Comparison of average psnr values with other existing methods

Feng et al. [12]	Lang et al. [9]	Lin et al. [13]	Guo et al. [8]	Anand et al. [4]	Hu et al. [7]	proposed
37.72	40.021	36.425	40.321	44.19	40.48	61.765

Table 5.4: comparison of SSIM values with other proposed schemes

IMAGE	Image Size	Chih-Chin Lai [11]	Nasrin M. Makbol et al. [6]	Ferda Ernawan et al. [2]	Dhani Ariatmanto et al. [1]	Proposed scheme
		SSIM	SSIM	SSIM	SSIM	SSIM
Lenna	512 x 512	0.992	0.980	0.987	0.994	**0.999**
Peppers	512 x 512	0.992	0.981	0.987	0.995	**0.999**
Sailboat	512 x 512	0.986	0.965	0.985	0.990	**0.998**
Baboon	512 x 512	0.988	0.986	0.990	0.996	**0.999**
House	512 x 512	0.985	0.957	0.985	0.987	**0.999**
Average		0.988	0.973	0.986	0.992	**0.998**

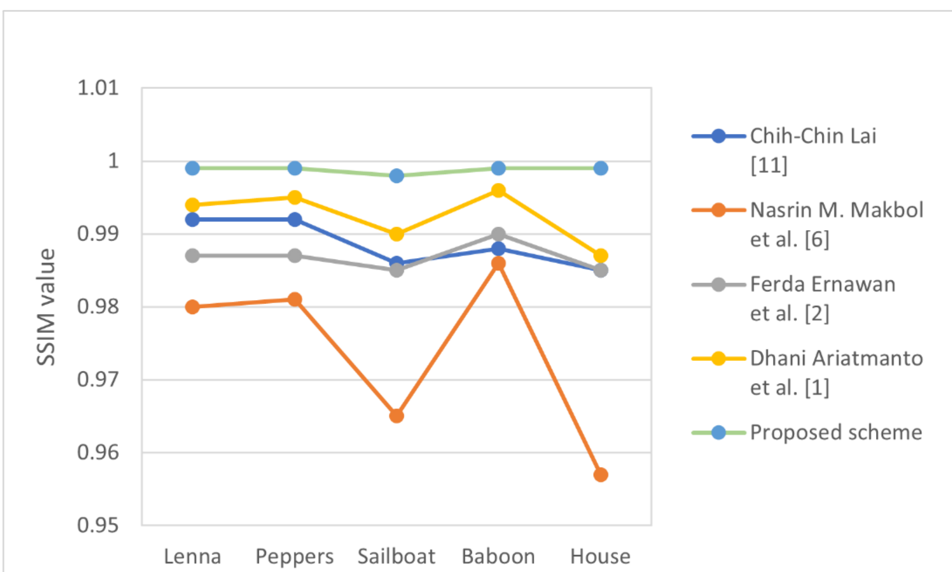

Fig 5.4 Performance Analysis of SSIM values

5.3 Attack on Images

Watermark attacks refer to any processing or manipulation of digital watermarked content that can disrupt the information being sent or the detection of the watermark itself. These attacks can be carried out through various means, ranging from simple modifications to advanced cryptographic techniques. Malicious attackers may use these attacks to retrieve, alter or remove watermarked data, or to insert incorrect data into the content.

There are several types of watermark attacks, including basic attacks (such as filtering or noise addition), cryptographic attacks (such as brute-force or key-based attacks), legal attacks (such as removing or altering watermarks to evade copyright infringement detection), geometric attacks (such as cropping or rotation), removal attacks (such as masking or cloning), and protocol attacks (such as exploiting vulnerabilities in communication protocols). These attacks hold the ability to prove many existing digital watermarking techniques ineffective and highlight the need for robust watermarking techniques that can withstand such attacks.

Below is the base image we are using for the experiment purpose.

Fig 5.5 Lenna

Fig 5.6 watermark

The image after watermarking

Fig 5.7 Watermarked Lenna

5.3.1 Types of attacks

There are various types of attacks on the images. Some are listed below:

Noise Insertion Attack: This attack involves adding unwanted noise to an image for reducing its quality and make the watermark difficult or impossible to detect. The attacker may add various kinds of noise like as Poisson noise, Gaussian noise, salt-and-pepper noise, or random value noise, to the watermarked image.

Filter Attack: This attack involves applying a filter to the watermarked image to modify or extract the watermark. Filters such as median filters, low-pass filters, or high-pass filters can be used to smooth, blur or sharpen the image, which can affect the watermark's detectability. This type of attack can be particularly effective when the filter parameters are similar to those used in the watermarking process.

Compression Attack: This attack involves compressing the watermarked image using a lossy compression algorithm, such as JPEG, which may remove or alter the watermark. Lossy compression algorithms discard some of the image's information to achieve high compression rates, and this can result in a loss of fidelity, including the watermark. This type of attack can be challenging to defend against since many lossy compression algorithms are widely used and may be difficult to avoid.

In general, these attacks are intended to disrupt the watermarking process and make it difficult or impossible to detect the watermark. Robust watermarking techniques should be designed to withstand these types of attacks by incorporating techniques such as error correction, spread spectrum, or frequency domain watermarking.

The following figure shows the image subjected to various attacks:

Fig 5.8 Lenna-Gaussian low pass filter

Fig 5.9 Lenna-Salt and pepper

Fig 5.10 Lenna-Median Filter

Fig 5.11 Lenna-Jpeg compression

5.4 Results after Attack on Images

Table 5.5: Abbreviations used in this report

Abbreviation	Description
GF-3	Gaussian low-pass filter (kernel: 3×3)
GF-5	Gaussian low-pass (kernel: 5×5)
JPEGQ-4	JPEG compression (quality: 40)
JPEGQ-5	JPEG compression (quality: 50)
JPEGQ-9	JPEG compression (quality: 90)
SN-1	Speckle noise (variance:0.001)
SPN-02	Salt & pepper noise (density: 0.002)
MF-3	Median filter (kernel size: 3×3)

The NCC values obtained after subjecting 'Lenna' image to various attacks are:

Table 5.6: PSNR and NCC values of Lenna under various attacks

Attacks	NCC	PSNR
GF-3	0.9956	36.51
GF-5	0.9935	35.54
JPEGQ-4	0.9956	35.69
JPEGQ-5	0.9962	40.77
JPEGQ-9	0.9988	40.77
SN-1	0.9460	36.21
SPN-02	0.9913	35.67
MF-3	0.9960	37.34

The attacks were performed on multiple watermarked images and their NC values are listed:

Table 5.7: NCC values of different images under various attacks

IMAGES	GF-3	GF-5	JPEGQ-4	JPEGQ-9	SN-1	SPN-02	MF -3
Lenna	0.995	0.993	0.995	0.998	0.946	0.991	0.996
Pepper	0.995	0.994	0.994	0.998	0.963	0.992	0.994
Sailboat	0.992	0.989	0.996	0.999	0.919	0.992	0.992
Baboon	0.985	0.974	0.990	0.998	0.917	0.988	0.979
House	0.999	0.999	0.999	0.999	0.946	0.994	0.999

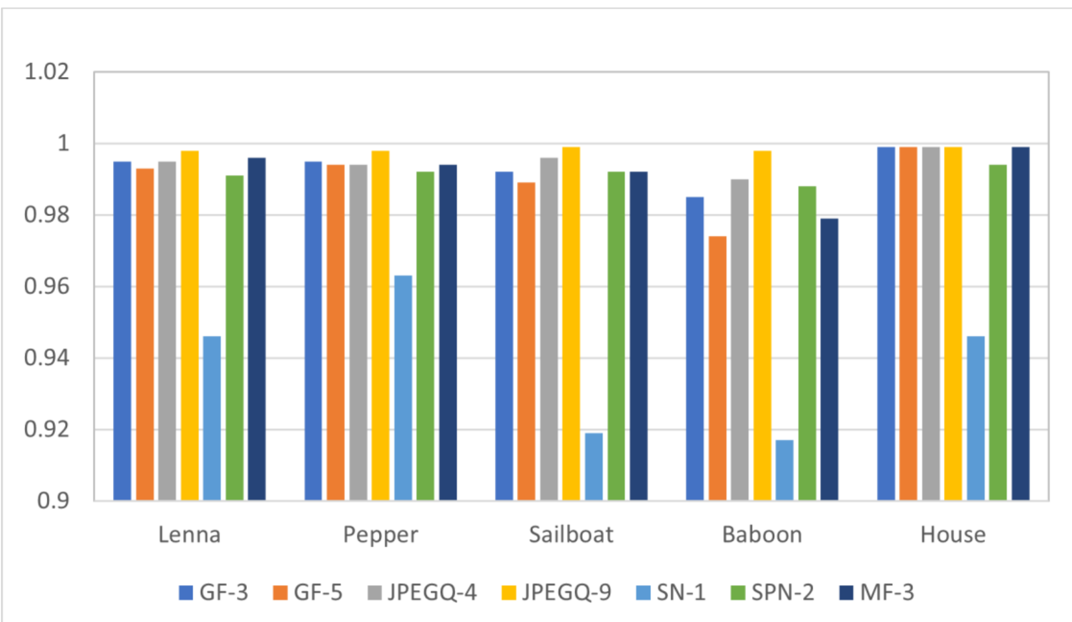

Fig 5.11 NCC value comparison of different images

The scheme produces desirable NCC value when the image is observed under various attacks.

5. CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

The watermarking technique proposed in this study, which utilizes DWT, DCT, and adaptive thresholding, has demonstrated superior performance with desirable values of PSNR, SSIM and NCC values as compared to other watermarking methods. The greater PSNR and SSIM values indicate that proposed scheme produces a greater degree of visual and numerical fidelity between the cover images and watermarked images. Also, the proposed technique obtained better NCC values when put under various attacks and compressions.

The discussed digital watermarking technique was evaluated with PSNR, SSIM, MSE, SSIM, NCC, BER % metrics on a set of grayscale test images. The results showed that the technique achieved desirable values compared to existing watermarking techniques. This suggests that the discussed method is more robust and imperceptible in embedding watermarks. Therefore, the scheme can be used effectively to ensure the ownership and integrity of digital content.

5.2 Future Scope

The proposed scheme has several potential areas for future research and improvement. Firstly, it can be extended to handle color images and video data. Secondly, efforts can be made to optimize the scheme's computational efficiency, particularly for large-scale applications. Different error correction codes can be added to make it more robust which can recover watermark even if some parts are lost. Addressing these areas can enhance the scheme's robustness and effectiveness, making it a more reliable method for digital watermarking in various applications.

REFERENCES

[1] Ariatmanto, D., & Ernawan, F. (2022). Adaptive scaling factors based on the impact of selected DCT coefficients for image watermarking. Journal of King Saud University-Computer and Information Sciences, 34(3), 605-614.

[2] Ernawan, F., Ariatmanto, D., & Firdaus, A. (2021). An improved image watermarking by modifying selected DWT-DCT coefficients. IEEE Access, 9, 45474-45485.

[3] Hasan, N., Islam, M. S., Chen, W., Kabir, M. A., & Al-Ahmadi, S. (2021). Encryption based image watermarking algorithm in 2DWT-DCT domains. Sensors, 21(16), 5540.

[4] Anand, A., & Singh, A. K. (2020). An improved DWT-SVD domain watermarking for medical information security. Computer Communications, 152, 72-80.

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

[6] Makbol, N. M., Khoo, B. E., & Rassem, T. H. (2016). Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. IET Image processing, 10(1), 34-52.

[7] Hu, H. T., Chang, J. R., & Hsu, L. Y. (2016). Robust blind image watermarking by modulating the mean of partly sign-altered DCT coefficients guided by human visual perception. AEU-International Journal of Electronics and Communications, 70(10), 1374-1381.

[8] Guo, J., Zheng, P., & Huang, J. (2015). Secure watermarking scheme against watermark attacks in the encrypted domain. Journal of Visual Communication and Image Representation, 30, 125-135.

[9] Lang, J., & Zhang, Z. G. (2014). Blind digital watermarking method in the fractional Fourier transform domain. Optics and Lasers in Engineering, 53, 112-121.

[10] Leng, X. X., Xiao, J., Li, D. Y., & Shen, Z. Y. (2013). Study on the digital image zero-watermarking technology. In Advanced Materials Research (Vol. 765, pp. 1113-1117). Trans Tech Publications Ltd.

[11] Lai, C. C. (2011). An improved SVD-based watermarking scheme using human visual characteristics. Optics Communications, 284(4), 938-944.
[12] Feng, L. P., Zheng, L. B., & Cao, P. (2010, July). A DWT-DCT based blind watermarking algorithm for copyright protection. In 2010 3rd international conference on computer science and information technology (Vol. 7, pp. 455-458). IEEE.
[13] Lin, S. D., Shie, S. C., & Guo, J. Y. (2010). Improving the robustness of DCT-based image watermarking against JPEG compression. Computer Standards & Interfaces, 32(1-2), 54-60.
[14] SIPI Image Database. Available: http://sipi.usc.edu/database/database.php

rohan final

By ALINA DASH

WORD COUNT 5035

TIME SUBMITTED 05-MAY-2023 10:47AM

PAPER ID 99389788

rohan final

ORIGINALITY REPORT

12%
SIMILARITY INDEX

PRIMARY SOURCES

1	www.mdpi.com Internet	47 words — 1%
2	dokumen.pub Internet	28 words — 1%
3	dspace.univ-eloued.dz Internet	25 words — 1%
4	Om Prakash Singh, A. K. Singh, Gautam Srivastava, Neeraj Kumar. "Image watermarking using soft computing techniques: A comprehensive survey", Multimedia Tools and Applications, 2020 Crossref	24 words — < 1%
5	mdpi-res.com Internet	22 words — < 1%
6	Yuxin Shen, Chen Tang, Min Xu, Mingming Chen, Zhenkun Lei. "A DWT-SVD based adaptive color multi-watermarking scheme for copyright protection using AMEF and PSO-GWO", Expert Systems with Applications, 2021 Crossref	19 words — < 1%
7	link.springer.com Internet	19 words — < 1%

8 Elham Moeinaddini, Fatemeh Afsari. "Robust watermarking in DWT domain using SVD and opposition and dimensional based modified firefly algorithm", Multimedia Tools and Applications, 2018
Crossref
18 words — < 1%

9 coek.info
Internet
17 words — < 1%

10 tel.archives-ouvertes.fr
Internet
16 words — < 1%

11 Tamirat Tagesse Takore, P. Rajesh Kumar, G. Lavanya Devi. "A New Robust and Imperceptible Image Watermarking Scheme Based on Hybrid Transform and PSO", International Journal of Intelligent Systems and Applications, 2018
Crossref
15 words — < 1%

12 Tao Chen, Hongtao Lu. "Robust spatial LSB watermarking of color images against JPEG compression", 2012 IEEE Fifth International Conference on Advanced Computational Intelligence (ICACI), 2012
Crossref
14 words — < 1%

13 Ferda Ernawan, Dhani Ariatmanto, Ahmad Firdaus. "An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients", IEEE Access, 2021
Crossref
13 words — < 1%

14 Majid Rahardi, Ferian Fauzi Abdulloh, Wahyu Sukestyastama Putra. "A Blind Robust Image Watermarking on Selected DCT Coefficients for Copyright Protection", International Journal of Advanced Computer Science and Applications, 2022
Crossref
13 words — < 1%