PURBANCHAL UNIVERSITY

DEPARTMENT OF COMPUTER ENGINEERING
KHWOPA ENGINEERING COLLEGE
LIBALI-8, BHAKTAPUR

A MID-TERM REPORT
ON
"WATERMARK EMBEDDING AND EXTRACTION"

A project proposal submitted for the partial fulfillment of requirements for the degree of Bachelor of Engineering in Computer Engineering (Eight Semester)

SUBMITTED BY:

Aman Mool (740303)
Rabin Phaiju (740329)
Rodip Duwal (740334)
Roshan Dumaru (740335)

SUBMITTED TO:

DEPARTMENT OF COMPUTER ENGINEERING

Under the supervision of

Er. Bikash Chawal

10th June, 2022

ACKNOWLEDGEMENT

We are extremely grateful to Department of Computer Engineering, Khwopa Engineering College for providing us the opportunity to work on the project named **"Watermark Embedding and Extraction"** to explore our abilities and knowledge in the field of Image Processing, Artificial Intelligence and steganography that we have learned through our semester.

We grant sense of gratitude to **Er. Bikash Chawal** as well as all members of the Department of Computer Engineering for their encouragement, inspiration and guidance for accomplishing this valuable task especially to our supervisor **Er. Bikash Chawal**.

Project Team Members:

1. Aman Mool (740303)
2. Rabin Phaiju (740329)
3. Rodip Duwal (740334)
4. Roshan Dumaru (740335)

ABSTRACT

Now days due to advancement of technology it is difficult to protect creative content and intellectual property. It is very easy to copy and modify digital media resulting in great loss in business. So, the viable solution for this problem is digital watermarking. Digital watermarking is a technique by which we embed copyright mark into digital content which is used to identify the original creator and owner of digital media. It is prominently used for tracing copyright infringements.

In this project we will be studying and implementing two famous methods of Digital Watermarking. In the first phase Digital image is introduced as input and for watermarking certain text is embedded as watermark. Our main objective is to embed the text to the image both visibly for image authentication and invisibly as steganography using least significant bit of image in first part where to be compatible within the image for text, the image is converted into byte and that of text operating in bit and back to the byte data and in second phase discrete wavelet transform is used for insertion and extraction of watermark in original image by using DWT. This technique is much simpler and robust than others.

Keywords: Watermark embedding, Watermark extraction, Digital watermarking, DWT, Steganography, least significant bit

TABLE OF CONTENT

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Background

Digital media can be copied and modified easily so protecting the copyright of digital media has become an important task. The digital watermark is introduced to solve the problem of copyright. The digital watermarking is a technique of embedding any watermark image into cover image using some known algorithm depending upon the requirement in multimedia data to identify the owner of the document. There are two common methods for watermarking: spatial domain and transform domain. In spatial domain pixels of an image are modified depending upon perceptual analysis of an image. But in transform domain some frequencies are selected and modified from their original values according to certain rules. The transform domain methods are more popular because watermark embedding is more robust in this domain as compared to spatial domain. It also provides more security and imperceptibility.

In digital watermarking, the signal may be text, audio, pictures or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time. The digital watermarking could be done in two ways:

In visible digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. When a television broadcaster adds its logo to the corner of transmitted video this also is a visible watermark.

In Invisible digital watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived. The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of steganography, where a party communicated a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of convert communication between individuals.

Our aim was to study different watermarking techniques and implement them. In this project we try to implement embedding and extracting of watermarks using the least significant bit and Discrete wavelet transform method for implementing both visible and invisible embedding and to measure the accuracy of extracted watermark. In this project we try to resist our watermark from different types of attack, scalar or geometric. Therefore, the main idea was to implement embedding and extraction of watermark provided by user in concise manner.

Digital Watermarking Life-Cycle Phases

Generally Digital watermark life cycle phases with embedding, attacking, and detection and retrieval functions

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermark signal.

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called attack. While the modification may not be malicious the term attack arises from copyright application, where pirates attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data, cropping an image and so on.

Detection is algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking application, the extraction algorithm should be able to produce the watermark correctly. [1]

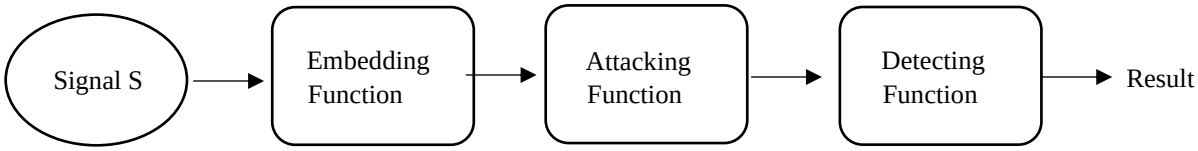

Fig 1.1: Digital Watermarking life-cycle phase

1.2 Motivation

The copyright abuse is the motivating factor in developing new encryption technologies, one such technology is digital watermarking. The focus of this project will detail digital watermarking for digital images applications.

1.3 Statement of problem

The desire for the availability of information and quick distribution has been a major factor in the development of new technology in the last decade. There is the increased use of digital images across the Internet. It is commonly applied in Internet marketing campaigns and electronic commerce web sites. Due to the growing usage of digital images on the Internet, serious issues have emerged. Counterfeiting, forgery, fraud, and pirating of this content are rising. Virtually anyone with a scanner, frame grabbers, down loader allow them to incorporate copyrighted material into presentations, web designs and Internet marketing campaigns.

1.4 Objectives

The main objective of this project is to embed and extract watermark from image visibly and invisibly.

1.5 Scope

This project is mainly appropriate for protecting intellectual property rights in all kinds of organization and institution. By using this system, owner of any contents can assert their ownership of the content and no one can use it without his/her permission. This system also more appropriate for security point of view. Like duplication of passport and currency can be avoided.

CHAPTER 2

LITERATURE REVIEW

A wavelet-based watermark casting scheme and a blind watermark retrieval technique are investigated in this research. An adaptive watermark casting method is developed to first determine significant wavelet sub bands and then select a couple of significant wavelet coefficients in these sub bands to embed watermarks. A blind watermark retrieval technique that can detect the embedded watermark without the help from the original image is proposed. Experimental results show that the embedded watermark is robust against various signal processing and compression attacks. [1]

Sumedh P. Ingale in his journal of computer science and information technology has discussed about the digital watermarking Algorithm using DWT technique. In this paper based on the requirement of the application the watermark is extracted or detected by detection algorithm to test condition of the data. [2]

Nikita Kashyap and G. R. SINHA also proposed a technique for implementing a robust image watermarking technique for the copyright protection based on 3 level DWT. In this technique a multi bit watermark is embedded into the low frequency sub-band of a cover image by using alpha blending technique. The insertion and extraction of the watermark in the grayscale cover image is found to be simpler than other transform techniques. The proposed method is compared with the 1-level and 2-level DWT based image watermarking methods by using statistical parameters such as peak-signal-to-noise-ratio (PSNR) and mean square error (MSE). The experimental results demonstrate that the watermarks generated with the proposed algorithm are invisible and the quality of watermarked image and the recovered image are improved. [3]

Now days due to advancement of technology it is difficult to protect creative content and intellectual property. It is very easy to copy and modify digital media resulting in great loss in business. So, the viable solution for this problem is digital watermarking. Digital watermarking is a technique by which we embed copyright mark into digital content which is used to identify the original creator and owner of digital media. It is prominently used for tracing copyright infringements. In this paper technique based on 1-level discrete wavelet transform is used for insertion and extraction of watermark in original image by using alpha blending. This technique is much simpler and robust than others. [4]

In this paper a wavelet-based logo watermarking scheme is presented. The logo watermark is embedded into all sub-blocks of the LLn sub-band of the transformed host image, using quantization technique. Extracted logos from all sub-blocks are merged to make the extracted watermark from distorted watermarked image. Knowing the quantization step-size, dimensions of logo and the level of wavelet transform, the watermark is extracted, without any need to have access to the original image. Robustness of the proposed algorithm was tested against the following attacks: JPEG2000 and old JPEG compression, adding salt and pepper noise, median filtering, rotating, cropping and scaling. The promising experimental results are reported and discussed.

This paper introduces a robust image watermarking technique for the copyright protection. The proposed method is based on 3-level discrete wavelet transform (DWT). Encoded secret image using spiral scanning is hidden by alpha blending technique in LL sub bands. During embedding process, secret image is dispersed within LL band depending upon alpha value. Encoded secret images are extracted and decoded to recover the original secret image. The experimental results demonstrate that the watermarks generated with the proposed algorithm are invisible and the quality of watermarked image and the recovered image are improved. The scheme is found robust to various image processing attacks such as JPEG compression, Gaussian noise, blurring, median filtering and rotation. [3]

Protection of digital multimedia content has become an increasingly important issue for content owners and service providers. Watermarking is identified as a major means to achieve copyright protection. This watermarking algorithm is based on the Discrete Wavelet Transform (DWT). Watermark components are added to a high frequency sub band by considering the human visual system (HVS) characteristics. HVS characteristics are used in this scheme to develop a robust watermarking scheme with a better tradeoff between robustness and imperceptibility. A visual mask based on HVS characteristics is used for calculating the weight factor for each wavelet coefficient of the host image. The proposed scheme was tested against mostly known threats and it proves to give good robustness. Also, it still gives a high-quality watermarked image. [5]

In Previous report created as project in khwopa engineering college, “watermarking using LSB” proposed idea of applying the concept of least significant bits and transforming the grayscale image to embed the text into the image invisibly and also experimented with different attacks possible on the Watermark images. [6]

Hirose et al. proposed a method for embedding C source program with use identification number. However, watermark in the program is undecodable if only a part of the program was stolen. Moreover, if program thieves applied the same method to the already watermarked program, original watermark will be easily erased. [7]

CHAPTER 3

PROJECT MANAGEMENT

3.1 Team Members:

For this project we have a group of four members:

1. Aman Mool (740303)
2. Rabin Phaiju (740329)
3. Rodip Duwal (740334)
4. Roshan Dumaru (740335)

3.2 Work break down structure

The four group members will work on the different modules. During work, each member communicated with each other so that no problem arises in the future. After the completion of the modules, we combined all the modules to develop a single program.

Table 3.1 Gantt Chart for Completion of Program

S. N	Week Job Description	1st Week	2nd Week	3rd Week	4th Week	5th Week	6th Week	7th Week	8th Week
1.	Problem Identification	■							
2.	Analysis		■						
3.	Design			■	■				
4.	Coding				■	■	■		
5.	Implementation and testing						■	■	■
6.	Documentation	■	■	■	■	■	■	■	■

CHAPTER 4
METHODOLOGY

4.1 Background

Digital Watermarking methods have been widely explored in the past few years. This approach is based on providing the authentication and also the data hiding capabilities.

Least significant (LSB) insertion is a common. Simple approach to embedding information in a cover image. The least significant bit (in other words, the 8th bit) of some or all the bytes inside an image is changed to a bit of the text watermark. When using 21-bit image, a bit of each of the red, green, blur color components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. The utilization of text watermarking invisibly can be seen as the application of steganography. Steganography is the science that involves communication secret data in an appropriate multimedia carrier. E.g., image, audio and video files. It comes under the assumption that if the features are visible the point of attack is evident, thus the goal here is always to conceal the very existence of embedded data. [1]

LSB steganography is an image steganography technique in which messages are hidden inside an image by replacing each pixel least significant bits with the bits of the message to be hidden.

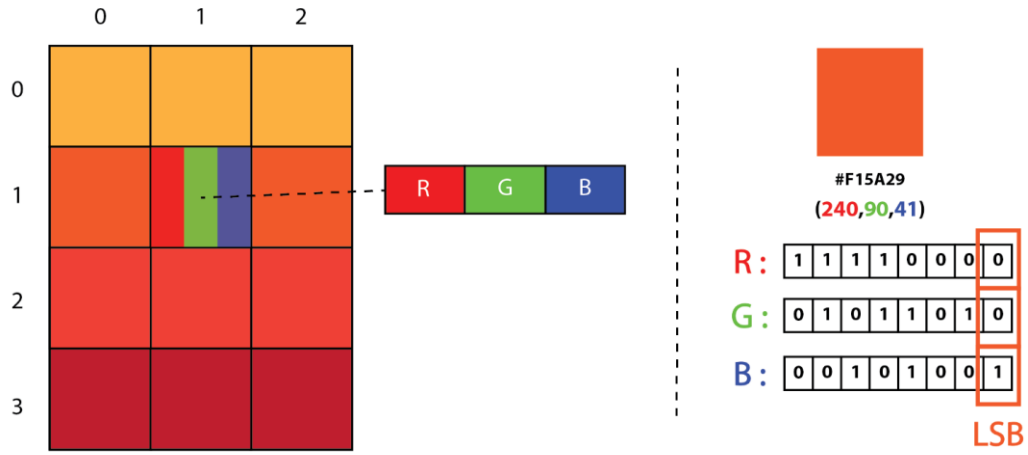

Fig 4.1: Representation of image as a 2D Array of RGB pixels [9]

Compared to spatial domain techniques, frequency-domain watermarking techniques proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithms [8]. Commonly used frequency-domain transforms include the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT). However, DWT has been used in digital image watermarking more frequently due to its excellent spatial localization and multi-resolution characteristics, which are similar to the theoretical models of the human visual system. Further performance

improvements in DWT-based digital image watermarking algorithms could be obtained by increasing the level of DWT

A discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled [9]. It is useful for processing of non-stationary signals. In transform small waves which are called wavelets of varying frequency and limited duration are used as mother wavelet. Wavelets are created by translations and dilations of a fixed function called mother wavelet. Wavelet transform provides both frequency and spatial description of an image DWT is the multi resolution description of an image the decoding can be processed sequentially from a low resolution to the higher resolution. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges

In two dimensional applications, for each level of decomposition, we first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL sub band of the previous level is used as the input. To perform second level decomposition, the DWT is applied to LL1 To perform third level decomposition, the DWT is applied to LL2 band which decompose this band into the four sub-bands – LL3, LH3, HL3, HH3. This results in 10 sub-bands per component. LH1, HL1, and HH1 contain the highest frequency bands present in the image tile, while LL3 contains the lowest frequency band and the approximate image.[4]

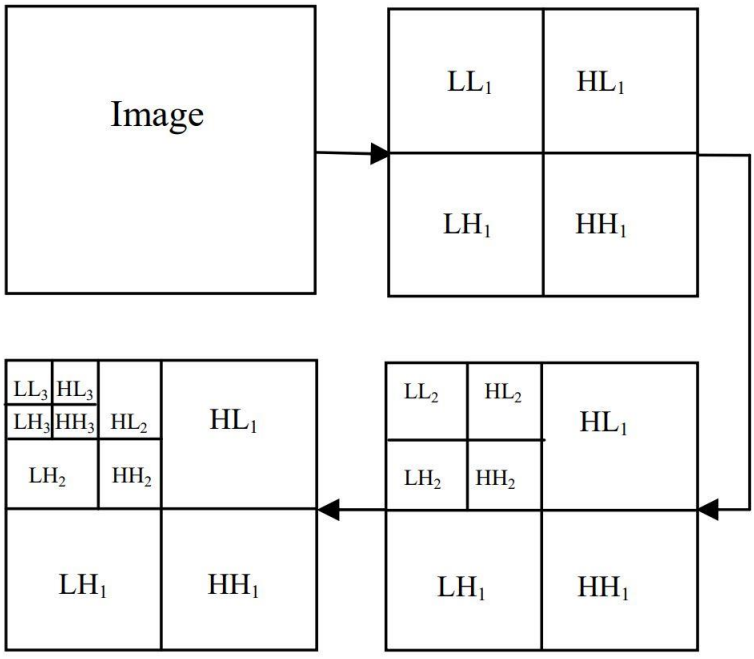

Fig 4.2: 3-Level discrete wavelet decompositions [3]

4.2 Block diagram

The block diagram represents the basic structure of Watermark system. Here the functionality of the watermarking system is categorized to two parts Visible watermarking which is especially applicable for the authentication of the image where the text is embedded in the image using the 3- DWT technique where the user is asked to place the position to place the watermark as well. whereas for the invisible embedding the watermark is embedded as a secret message which is applicable as a steganography. The LSB technique is used where the least significant bit of the image is replaced with the message. For the decoding same technique is used in reverse order.

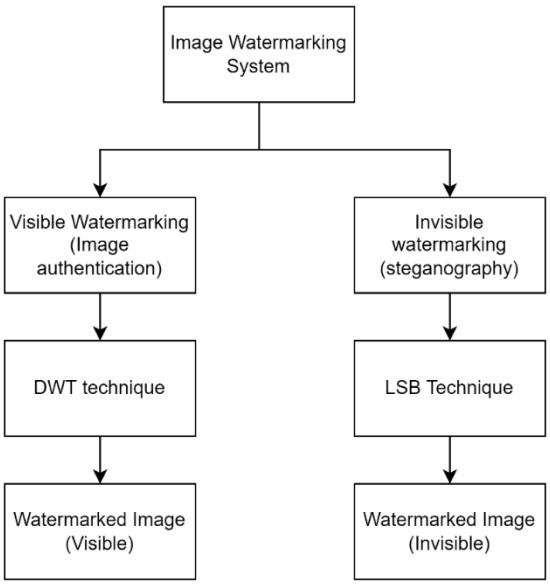

Fig 4.3: Basic Block Diagram of Watermark system.

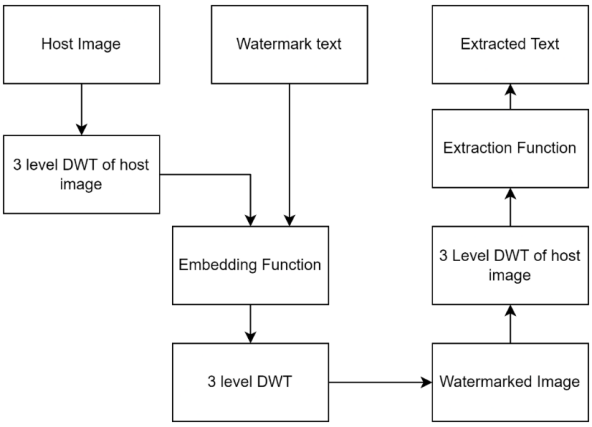

Fig 4.4: Basic Block Diagram representing embedding and extraction using DWT.

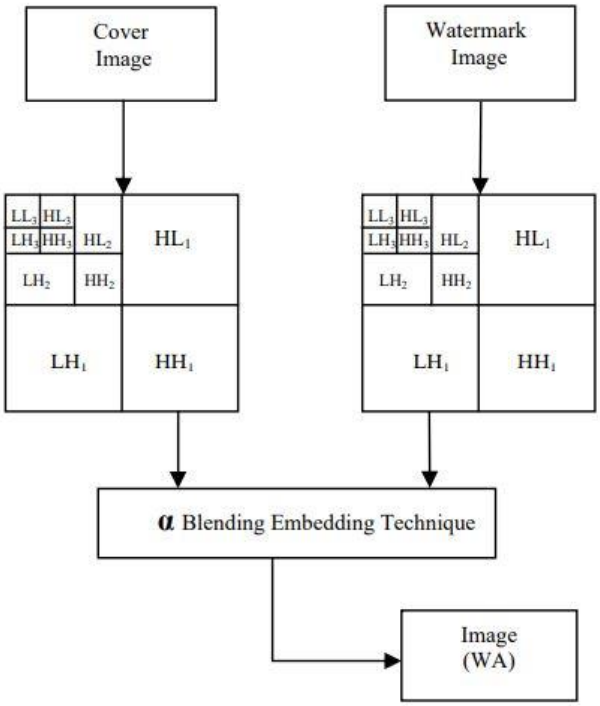

Fig 4.5: watermark embedding technique with alpha blending.

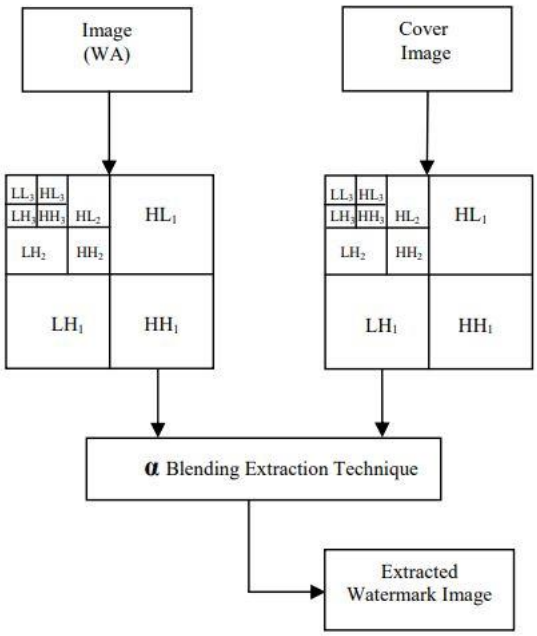

Fig 4.6: watermark extraction technique with alpha blending.

4.3 Flowchart

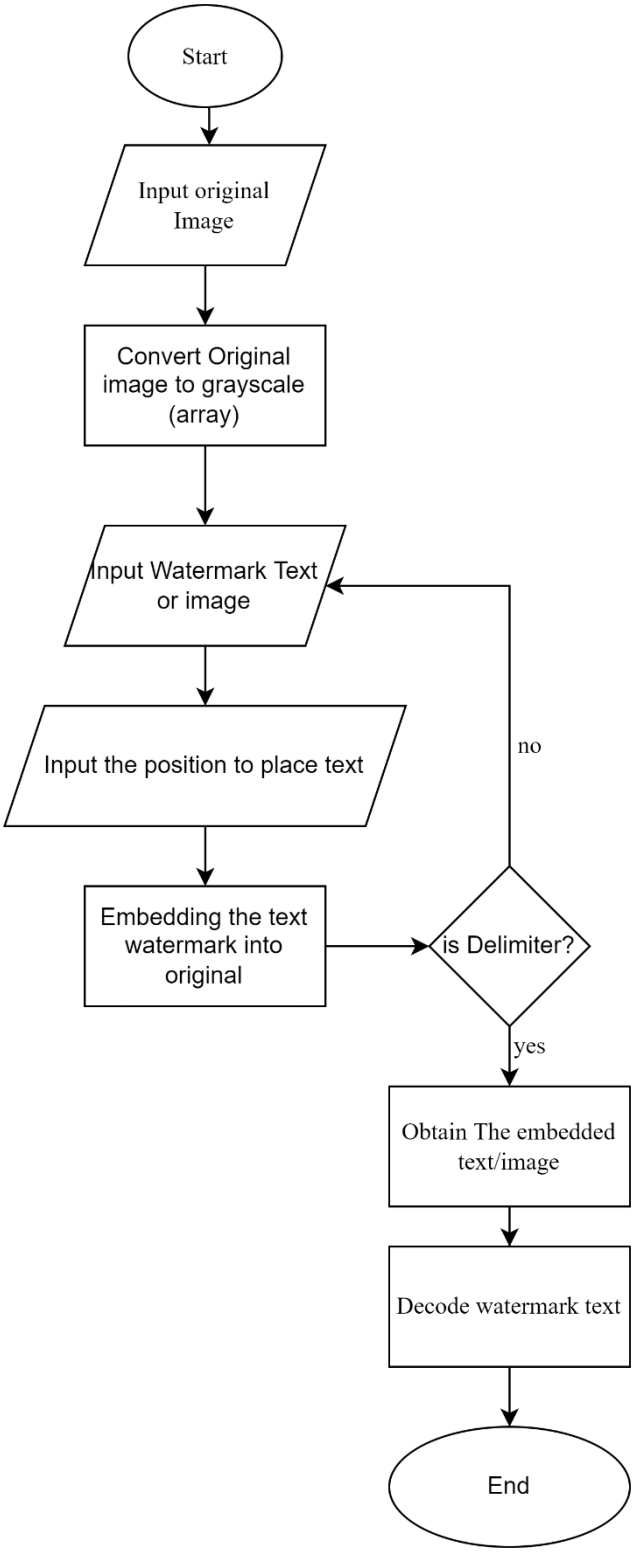

Fig 4.7: Flowchart for Digital Watermarking System

4.4 Algorithm

To accomplish our project, we have performed following series of task in step-by-step format. To accomplish the LSB steganography we implemented following algorithm:

1. Take the original Image
2. Convert the original Image into gray scale
3. Byte conversion of gray scale image
4. Write the certain text to be embedded as watermark in grayscale image.
5. Add the delimiter in the end of the text so that when program decodes it knows when to stop.
6. Check if the total pixel available is sufficient for message. If yes proceed to iterating the pixel one by one and modify least significant bits to bits of text
7. Embedding watermark into grayscale image by using encoding technique
8. Extracting the watermarked text from image using the reverse decoding technique.

Where as for the visible embedding and extraction we did following

For embedding we need a host image and a watermarked image

Step 1: First level DWT is performed on the host image to decompose it into four sub bands LL1, HL1, LH1 and HH1.

Step 2: The second level DWT is performed on the LL1 sub band to get four smaller sub bands LL2, HL2, LH2 and HH2.

Step 3: The third level DWT is performed on the LL2 sub band to get four smaller sub bands LL3, HL3, LH3 and HH3.

Step 4: First level DWT is performed on the watermark image to decompose it into four sub bands wLL1, wHL1, wLH1 and wHH1.

Step 5: The second level DWT is performed on the LL1 sub band to get four smaller sub bands wLL2, wHL2, wLH2 and wHH2.

Step 6: The third level DWT is performed on the LL2 sub band to get four smaller sub bands w LL3, wHL3, wLH3 and wHH3

Step7: A embedding function is used to add the two sub bands are added with an embedding formula with value 'a' as in is as follows: new LL3=LL3+ a*wLL3

Step8: Now Inverse DWT is performed using the sub bands new LL3, LH3, HL3, HH3 to get image new LL2.

Step 9: Inverse DWT is performed using the sub bands newLL2, LH2, HL2, HH2 to get image new LL1.

Step10: Inverse DWT is performed using the sub bands new LL2, LH1, HL1, HH1 to get the watermarked image now we get the watermarked image that can be used for various purposes.

For extraction host image and watermarked text are used:

Step 1: First level DWT is performed on the host image to decompose it into four sub bands LL1, HL1, LH1 and HH1.

Step 2: The second level DWT is performed on the LL1 sub band to get four smaller sub bands LL2, HL2, LH2 and HH2.

Step 3: The third level DWT is performed on the LL2 sub band to get four smaller sub bands LL3, HL3, LH3 and HH3.

Step 4: First level DWT is performed on the watermarked image to decompose it into four sub bands nLL1, nHL1, nLH1 and nHH1.

Step 5: The second level DWT is performed on the LL1 sub band to get four smaller sub bands nLL2, nHL2, nLH2 and nHH2.

Step 6: The third level DWT is performed on the LL2 sub band to get four smaller sub bands n LL3, n HL3, n LH3 and nHH3.

Step7: Then following extracting is performed to get wLL3 with the extraction formulae with same value of 'a' as in embedding wLL3= new LL3-LL3/ a

Step 8: Apply inverse DWT on wLL3 with all other sub bands (LH, HL, HH) equal to zero to get wLL2

Step 9: Repeat step 8 two times each level to get the extracted watermarks.

4.5 Tools and Platform

1. Programming language - Python

2. Visual Studio Code

3. Documentation Tools- Microsoft Word and Microsoft PowerPoint

4. Platform- Window

CHAPTER 5
RESULT AND DISCUSSION

5.1 Overview

To find out whether the watermark image is embedded into the original image or not, it is point of testing to show in what ways watermark can be embedded and extracted from the original image. It is important to extract for authentication.

For the assurance of completion of the project. We go through different experiments. Here in this project, we embedded the text as well as the image using 1-DWT using HAAR method and the histogram of resulting and original image is as below:

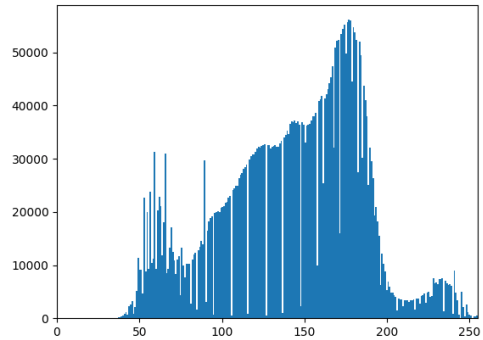

Fig 5.1: histogram of original image

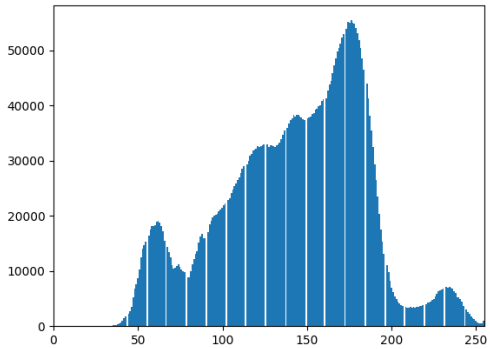

Fig 5.2: histogram of watermarked image

The histogram of original image and the watermarked image is somehow very much similar to each other. Therefore, after the encoding of the text or image into the original image it doesn't distort the original image.

5.2 Output Results

The resulting output after embedding and extraction of the watermark in the images are shown below:

Fig 5.3: Original Image and text to be embedded

Here after the user has added the original image, user is asked to enter the text or the image to be embed as watermark in above example we included the text which is converted to gray scale image to be embedded.

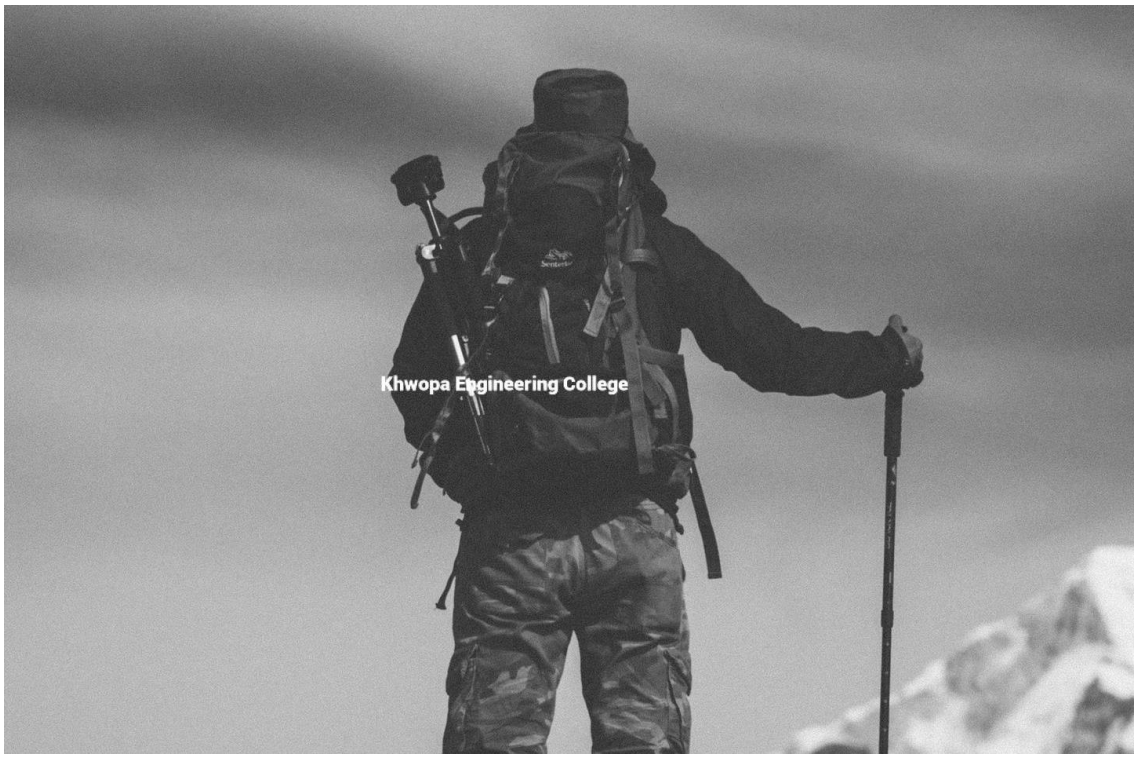

Fig 5.4: Watermarked Image with text

Fig 5.5: Extracted Text from the watermarked Image

In the second example we embedded the image instead of text it basically works the same.

Fig 5.6: Original Image and logo to be embedded.

Fig 5.7: Watermarked Image with Logo embedded

Fig 5.8: Extracted Watermarked logo from image

Chapter 6

Work to be done

We have completed our almost 80% of our project. And remaining Work to be done in our project are:

- Complete the UI of the application.
- Improve the decoding time of LSB steganography (Invisible watermarking)
- Add different attacks and noise to the image to check the efficiency of the watermark image.
- Increase the level of DWT to level 3.
- Do different comparison testing of different techniques.

CONCLUSION

Digital watermarking technology is an emerging field in computer science, Cryptography, Signal processing and communications. The watermarking research is more exciting as it needs collective concepts from the entire field along with Human psycho-visual analysis, Multimedia and computer graphics. The watermark may be of visible or invisible type and each has got its own application. Visible can be used in the field of authentication of the product whereas the invisible watermark can be used as the steganography in cryptography. We have implemented both visible and invisible text watermark into the image using the DWT as well as LSB in this project work.

So, our project has been towards the better performance for preventing the owners from the copyright and identifies the image of owner's license information and to track illegal copies.

REFERENCES

[1] M. a. S. V. Narang, "Digital watermarking using discrete wavelet transform.," International Journal of Computer Applications, 2013.

[2] S. P. Ingale, "Digital Watermarking Algorithm using DWT Technique," *International Journal of Computer Science and Mobile Computing,* vol. V, no. 5, pp. 01-09, 2017.

[3] G. R. S. Nikita Kashyap, "Image Watermarking Using 3-Level Discrete Image Watermarking Using 3-Level Discrete," I.J.Modern Education and Computer Science, Bhilai, 2012.

[4] J. K. Satendra Kumar, "Enhanced digital image watermarking scheme based on DWT and SVD," *International Journal of Computer Applications,* 2012.

[5] S. S. A. N. M. Basheer, "Digital image watermarking algorithm in discrete wavelet transform domain using hvs characteristics,," *Wireless Communications and Mobile,* 2015.

[6] N. Shrestha, "watermarking using LSB," 2012.

[7] N. O. E. Hirose, "Symposium on cryptography and information security," 1998.

[8] "Digital image watermarking algorithm in discrete wavelet transform domain using hvs characteristics,".

[9] D. Jain, "LSB Image Steganography," 23 7 2020.