DIGITAL WATERMARKING USING INSTANT BIT SUBSTITUTION

by

Name	Roll No.	Registration No:
Arif Mohammed Khan	**11700314023**	**141170110205** of 2014-2015
Shivangi Shalu	**11700314092**	**141170110274** of 2014-2015
Vivek Kumar Prasad	**11700314122**	**141170110304** of 2014-2015
Zahid Fazal	**11700314124**	**141170110306** of 2014-2015

A comprehensiveproject report has been submitted in partial fulfillment of the requirements for the degree of

Bachelor of Technology

in

ELECTRONICS & COMMUNICATION ENGINEERING

Under the supervision of

Dr. ABHISHEK BASU

Assistant Professor

श्रमम् बिना न किमपि साध्यम्

Department of Electronics & Communication Engineering
RCC INSTITUTE OF INFORMATION TECHNOLOGY
Affiliated to Maulana Abul Kalam Azad University of Technology, WestBengal
CANAL SOUTH ROAD, BELIAGHATA, KOLKATA – 700015

May 2018

CERTIFICATE OF APPROVAL

This is to certify that the project titled "**DIGITAL WATERMARKING USING INSTANT BIT SUBSTITUTION**" carried out by

Name	Roll No.	Registration No:
Arif Mohammed Khan	**11700314023**	**141170110205** of 2014-2015
Shivangi Shalu	**11700314092**	**141170110274** of 2014-2015
Vivek Kumar Prasad	**11700314122**	**141170110304** of 2014-2015
Zahid Fazal	**11700314124**	**141170110306** of 2014-2015

for the partial fulfillment of the requirements for B.Tech degree in **Electronics and Communication Engineering** from **Maulana Abul Kalam Azad University of Technology, West Bengal**is absolutely based on his own work under the supervision of **Dr.ABHISHEK BASU**.The contents of this thesis,in full or in parts, have not been submitted to any other Institute or University for theaward of any degree or diploma

Supervisor:

....
Dr. ABHISHEK BASU
Assistant Professor , Dept. of ECE
RCC Institute of Information Technology

....

Dr. ABHISHEK BASU
Head of the Department (ECE)
RCC Institute of Information Technology

DECLARATION

"We Do hereby declare that this submission is our own work conformed to the norms and guidelines given in the Ethical Code of Conduct of the Instituteand that, to the best of our knowledge and belief, it contains no material previously written by another neither person nor material (data, theoretical analysis, figures, and text) which has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgement has been made in the text."

....

ARIF MOHAMMED KHAN
Registration No:141170110205 of 2014-2015
Roll No: 11700314023

....

SHIVANGI SHALU
Registration No:141170110274 of 2014-2015
Roll No: 11700314092

....

VIVEK KUMAR PRASAD
Registration No:141170110304 of 2014-2015
Roll No: 11700314122

....

ZAHID FAZAL
Registration No:141170110306 of 2014-2015
Roll No: 11700314124

Date:

Place:

CERTIFICATE of ACCEPTANCE

This is to certify that the project titled “**DIGITAL WATERMARKING USING INSTANT BIT SUBSTITUTION**” carried out by

Name	Roll No.	Registration No:
Arif Mohammed Khan	**11700314023**	**141170110205** of 2014-2015
Shivangi Shalu	**11700314092**	**141170110274** of 2014-2015
Vivek Kumar Prasad	**11700314122**	**141170110304** of 2014-2015
Zahid Fazal	**11700314124**	**141170110306** of 2014-2015

is hereby recommended to be accepted for the partial fulfillment of the requirements for B.Tech degree in **Electronics and Communication Engineering** from **Maulana Abul Kalam Azad University of Technology, West Bengal**

Name of the Examiner Signature with Date

1. ……………………………………………………………………

2.……………………………………..……………………………..

3.……………………………………………………………………

4. ……………………………………. ………………………………

ABSTRACT

Digital watermarking is a process of data hiding in a digital media(audio,video, image). Important feature of digital watermarking is copyright protection .It gives assurance to owner.

There are two types of digital watermarking on the basis of visualization: visible watermark and invisible watermark. On the basis of methodology (i.e. how to do digital watermarking) there are two basic types:Spatial Domain Watermarking Technique and Transformed Domain Technique.

We performed watermarking under spatial domain watermarking technique. We followed INSTANT BIT SUBSTITUTION method to perform watermarking.

For encoding part we changed the second last significant bit of host image whose pixel value is greater than 200, with that of the watermark image.Thus, we get our Watermarked image. For decoding part, the second last bit values with pixel valuegreater than 200 in the encoded image is multiplied with 256 and resultant value is placed in 16*16 zeros matrices.

We found that without any attack on the encoded image our watermark which we extracted was imperceptible but after few attacks on encoded image such asGausssian noise,salt &pepper noise,compression of image,cropping of image our watermark gets distorted. Hence, our code is fragile to any attack.

CONTENTS

LIST OF ABBREVIATIONS

- RGB-Red Green Blue
- PSNR - Peak Signal To Noise Ratio
- SSIM - Structural Similarity
- MSE - Mean Squared Error
- LSB - Least Significant Bit
- MSB - Most Significant Bit
- ISB - Instant Bit Substitution
- DCT - Discrete Cosine Transform
- JPEG - Joint Photographic Experts Group
- DFT - Discrete Fourier Transform
- DWT - Discrete Wavelet Transform
- IoT – Internet of Things

LIST OF FIGURES

LIST OF TABLES

Chapter 1

Introduction

1.1REQUIREMENT OF DIGITAL WATERMARKING :

Today's generation is witness of developments of digital media. A very simplest example of digital media is a photo captured by phone camera. The use of Digital media is common in present era. Other example of Digital media is text, audio, video etc.

We know an internet is the fastest medium of transferring data to any place in a world. As this technology grown up the threat of piracy and copyright very obvious thought is in owners mind. A secure data embedding procedure cannot be broken unless the unauthorized user access to a secret key that controls the insertion of the data in the host signal.

The increasing amount of research on watermarking over the past decade has been largely driven by its important applications in digital copyrights management and protection. One of the first applications for watermarking was broadcast monitoring. It is often crucially important that we are able to track when a specific video is being broadcast by a TV station. This is important to advertising agencies that want to ensure that their commercials are getting the air time they paid for. Watermarking can be used for this purpose.

Information used to identify individual images could be embedded in the images themselves using watermarking, making broadcast monitoring easier. Another very important application is owner identification. Being able to identify the owner of a specific digital work of art, such as a video or image can be quite difficult. Nevertheless, it is a very important task, especially in cases related to copyright infringement.

So, instead of including copyright notices with every image or song, we could use watermarking to embed the copyright in the image or the song itself. Transaction tracking is another interesting application of watermarking. In this case the watermark embedded in a digital work can be used to record one or more transactions taking place in the history of a copy of this work.

For example, watermarking could be used to record the recipient of every legal copy of a movie by embedding a different watermark in each copy. If the movie is then leaked to the Internet, the movie producers could identify which recipient of the movie was the source of the leak.

To enforce IP rights and to prevent illegal duplication, interpolation and distribution of multimedia data, Digital watermarking is an effective solution. Copyright protection, data authentication, covert communication and content identification can be achieved by Digital watermarking. Digital watermarking is a technique to embed copyright or other information into the underlying data.

The term "watermark" was probably originated from the German term "wassermarke". Since watermark is of no importance in the creation of the mark, the name is probably given because the marks resemble the effects of water on paper. Papers are invented in China over a thousand years ago. However, the first paper watermark did not appear until 1282, in Italy

The embedded data should maintain the quality of the host signal. In order to achieve the copyright protection, the algorithm should meet few basic requirement:

- Imperceptibility: The watermark should not affect the quality of the original signal, thus it should be invisible/ inaudible to human eyes/ ears.
- Robustness: The watermarked data should not be removed or eliminated by unauthorized distributors, thus it should be robust to resist common signal processing manipulations such as filtering, compression, filtering with compression.
- Capacity: the number of bits that can be embedded in one second of the host signal.
- Security: The watermark should only be detected by authorized person.
- Watermark detection should be done without referencing the original signals.
- The watermark should be undetectable without prior knowledge of the embedded watermark sequence.
- Universal: The same watermarking algorithm should be applicable to all multimedia under consideration.
- Textual copyright notices cannot be used to solve the copyright dispute since they can be easily forged.
- Registering every work to a central repository is too costly! – http://www.loc.gov/copyright – $30 per document.

1.2 DIGITAL WATERMARKING:

Watermarking is the process that embeds data called a watermark into an image or audio or video.The watermark can be detected and extracted later from the carrier (cover).

It can contain information such as copyright, license, authorship etc. A simple example of a digital watermark is a "seal" on the image to identify the ownership.

Any watermarking algorithm consists of three parts:

a) The watermark, which is unique to the owner.

b) The encoder for embedding the watermark into the data.

c)The decoder for extraction and verification.

The general watermarking framework is in figure:

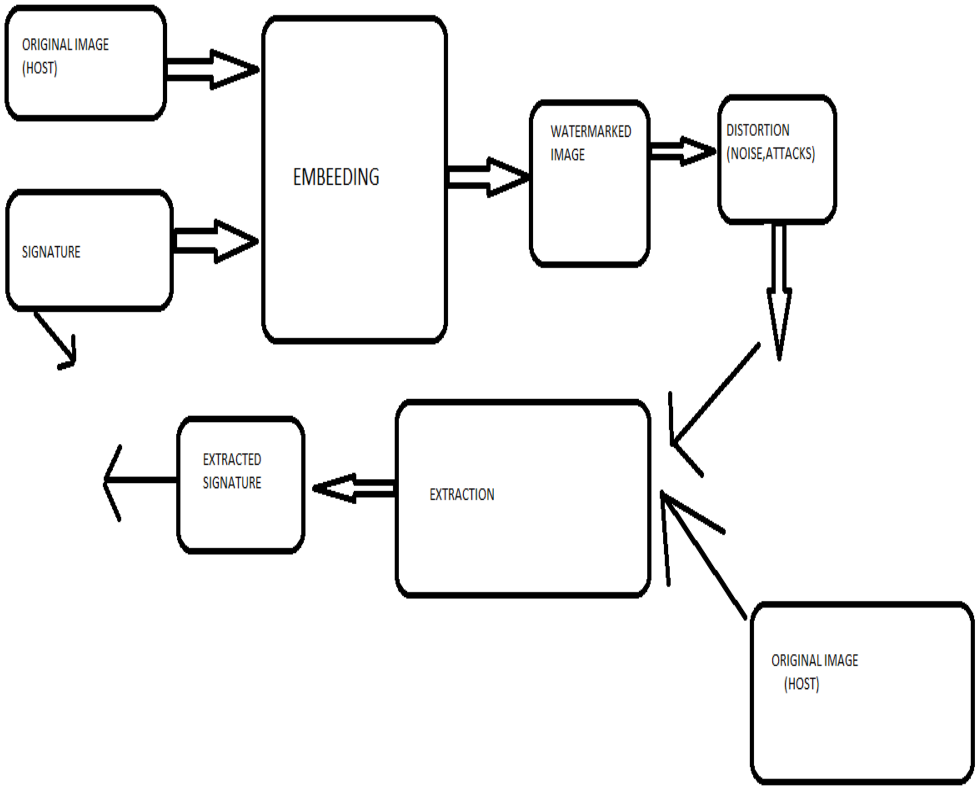


Figure 1.1: Watermarking Framework

Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence.

1.2.1 VISIBLE WATERMARK:

Visible watermark is a translucent overlaid into an image andis visible to the viewer. Visible watermarking is used to indicate ownership and for copyright protection.

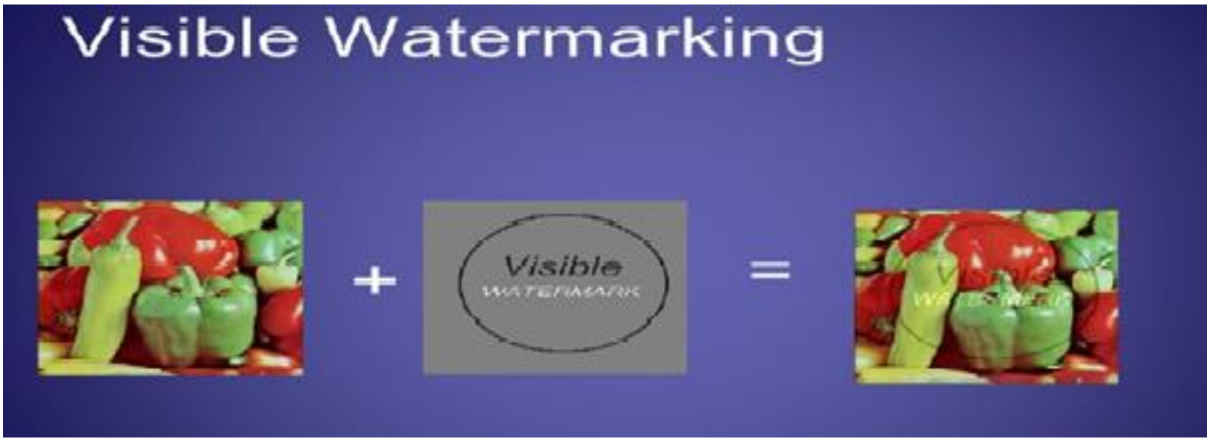


Figure 1.2: Visible Watermark

1.2.2 INVISIBLE WATERMARK:

An invisible watermark is embedded into the data in such a way that the changes made to the pixel values are perceptually not noticed. Invisible watermark is used as evidence of ownership and to detect misappropriated images.

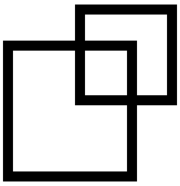


Figure 1.3: Watermark

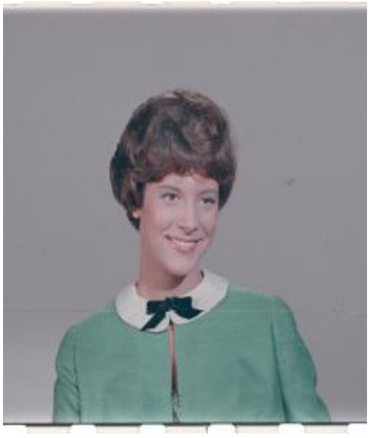


Figure 1.4: Original Image

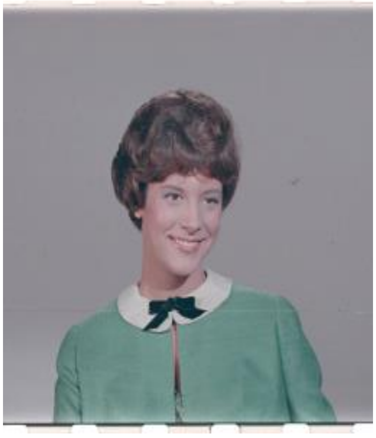


Figure 1.5: Watermarked Image

1.2.3 CLASSIFICATION OF WATERMARK:

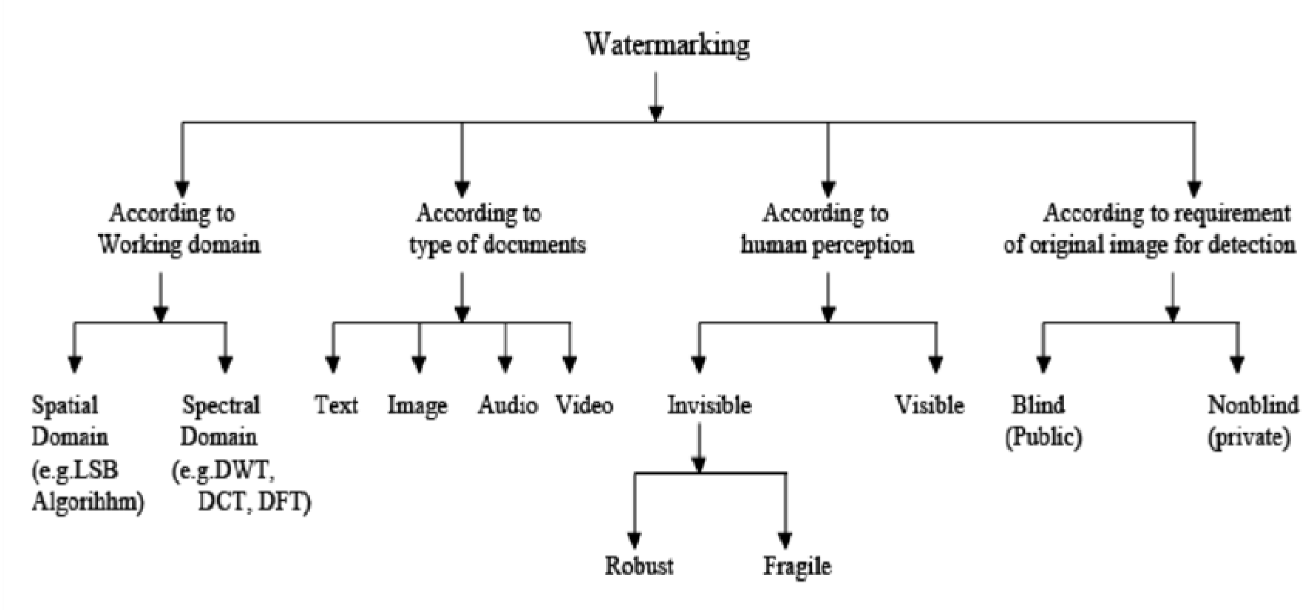

Watermarking
According to Working domain
According to type of documents
According to human perception
According to requirement of original image for detection
Spatial Domain (e.g.LSB Algorihhm)
Spectral Domain (e.g.DWT, DCT, DFT)
Text
Image
Audio
Video
Invisible
Visible
Blind (Public)
Nonblind (private)
Robust
Fragile

Figure 1.6: Watermark Classification

Every watermarking system has some very important desirable properties. Some of these properties are often conflicting and we are often forced to accept some tradeoffs between these properties depending on the application of the watermarking system.

For a strong watermark embedding, a good watermarking technique is needed to be applied. Watermark can be embedded either in spatial or frequency domain. For a strong watermark embedding, a good watermarking technique is needed to be applied. Watermark can be embedded either in spatial or frequency domain.

Robust:Robustness watermarking is mainly used to sign copyright information of the digital works, the embedded watermark can resist the common edit processing, image processing and lossycompression, and the watermark is not destroyed after some attack and can still be detected to provide certification. It resists various attacks, geometrical or non-geometrical without affecting embedded watermark.

Fragile: Fragile watermarking is mainly used for integrity protection, which must be very sensitive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking.

Semi fragile: Semi fragile watermarking is capable of tolerating some degree of the change to a watermarked image, such as the addition of quantization noise from lossy compression.

Image watermarking: This is used to hide the special information into the image and to later detect and extract that special information for the author‘s ownership.

Video watermarking: This adds watermark in the video stream to control video applications. It is the extension of image watermarking. This method requires real time extraction and robustness for compression.

Audio watermarking: This application area is one of the most popular and hot issue due to internet music, MP3.

Text watermarking: This adds watermark to the PDF, DOC and other text file to prevent the changes made to text. The watermark is inserted in the font shape and the space between characters and line spaces.

1.2.4 WATERMARKING TECHNIQUES:

- Spatial Domain Watermarking Technique.
- Transformed Domain Technique.

Spatial Domain Watermarking Technique:

The simplest example of a spatial domain watermarking techniques to insert data into digital signals in noise-free environments is least significant bit (LSB) coding. There are many variants of this technique. It essentially involves embedding the watermark by replacing the least significant bit of the image data with a bit of the watermark data.

The most straightforward way to embed a watermark into an image in the spatial is to add a pseudo random noise pattern to the luminance values of its pixels. Schyndel[2] proposed a method based on bit plane manipulation of the least significant bit (LSB) which offers easy and rapid decoding. He inserts the watermark into LSB only around image contours. Caronmi hides small geometric patterns called tags in regions where the tags would be least visible, such as the very bright, very dark or texture regions.

Techniques in spatial domain class generally share the following characteristics:

- The watermark is applied in the pixel domain
- No transforms are applied to the host signal during watermark embedding.
- Combination with the host signal is based on simple operations, in the pixel domain.
- The watermark can be detected by correlating the expected pattern with the received signal.

Transformed Domain Technique:

Generally Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) are used as the methods of data transformation. In these methods, a watermark that one wishes to embed distributively in overall domain of an original data, and the watermark, is hardly to be deleted once embedded.

The main strength offered by transform domain techniques is that they can take advantage of special properties of alternate domains to address the limitations of pixel-based methods.

While there are many robust watermarks in the DCT domain, there are relatively fewer existing data hiding watermarking techniques in DCT domain. Kim, [3] embed watermark bits as pseudo-random sequences in the frequency domain. Langelaar, [4] hide watermarks by removing or retaining selected DCT coefficients. Borg, [5] hide watermark in JPEG images by forcing selected DCT blocks to satisfy certain linear or circular constraint. Some embeds watermark patterns in the quantization module after DCT or in selected blocks based on human visual models. Choi, utilize inter-block correlation by forcing DCT coefficients of a block to be greater or smaller than the average of the neighboring blocks.

1.3 INSTANT BIT SUBSTITUTION:

In a digital image, information can be inserted directly into every bit of image information or the more busy areas of an image can be calculated so as to hide such messages in less perceptible parts of an image.
Tirkelet.al were one of the first used techniques for image watermarking. Two techniques were presented tohide data in the spatial domain of images by them. These methods were based on the pixel value's Least Significant Bit (LSB) modifications.

An example of the less predictable or less perceptible is Least Significant Bit insertion. This section explains how this works for an 8-bit grayscale image and the possible effects of altering such an image. The principle of embedding is fairly simple and effective.

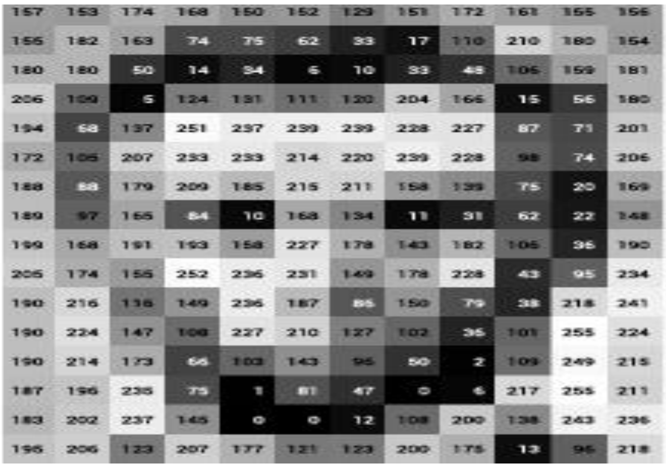
If we use a grayscale bitmap image, which is 8- bit, we would need to read in the file and then add data to the least significant bits of each pixel, in every 8-bit pixel.
In a grayscale image each pixel is represented by 1 byte consist of 8 bits. It can represent 256 gray colors between the black which is 0 to the white which is 255.

The principle of encoding uses the Least Significant Bit of each of these bytes, the bit on the far right side. If data is encoded to only the last two significant bits (which are the first and second LSB) of each color component it is most likely not going to be detectable; the human retina becomes the limiting factor in viewing pictures.

For the sake of this example only the least significant bit of each pixel will be used for embedding information. If the pixel value is 138 which is the value 10000110 in binary and the watermark bit is 1, the value of the pixel will be 10000111 in binary which is 139 in decimal. In this example we change the underline pixel.

GREY SCALE IMAGE:

Grayscale images are distinct from one-bit bi-tonal black-and-white images, which in the context of computer imaging are images with only two colors, black and white (also called *binary images*). Grayscale images have many shades of gray in between. Grayscale images can be the result of measuring the intensity of light at each pixel according to a particular weighted combination of frequencies (or wavelengths), and in such cases they are monochromatic proper when only a single frequency.



157	153	174	168	150	152	129	151	172	161	155	156
155	182	163	74	75	62	33	17	110	210	180	154
180	180	50	14	34	6	10	33	48	106	159	181
206	109	5	124	131	111	120	204	166	15	56	180
194	68	137	251	237	239	239	228	227	87	71	201
172	105	207	233	233	214	220	239	228	98	74	206
188	88	179	209	185	215	211	158	139	75	20	169
189	97	165	84	10	168	134	11	31	62	22	148
199	168	191	193	158	227	178	143	182	106	36	190
205	174	155	252	236	231	149	178	228	43	95	234
190	216	116	149	236	187	86	150	79	38	218	241
190	224	147	108	227	210	127	102	36	101	255	224
190	214	173	66	103	143	96	50	2	109	249	215
187	196	235	75	1	81	47	0	6	217	255	211
183	202	237	145	0	0	12	108	200	138	243	236
195	206	123	207	177	121	123	200	175	13	96	218

Figure 1.7: Grey Scale Pixel Value for an image

RGB IMAGE:

RGB (red, green, and blue) refers to a system for representing the colors to be used on a computer display. Red, green, and blue can be combined in various proportions to obtain any color in the visible spectrum. Levels of R, G, and B can each range from 0 to 100 percent of full intensity.

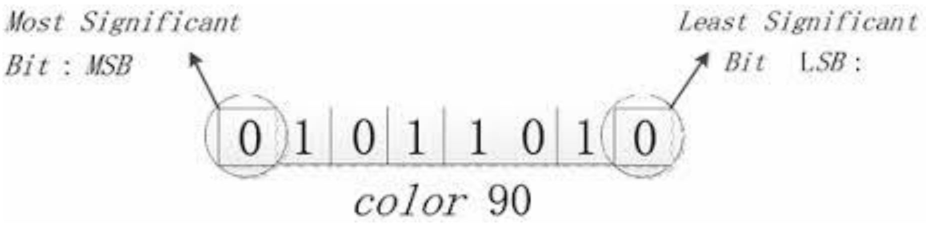


Figure 1.8: Bit Conversion of Pixel Value

In instant bit substitution method we changed the second least significant bit of certain pixel values, which cannot affect the quality of image as well as pixel values.

But it changes certain values of pixels due to watermark image when embedded to it.

The robustness depends on the number of bits that are being replaced in the host signal.

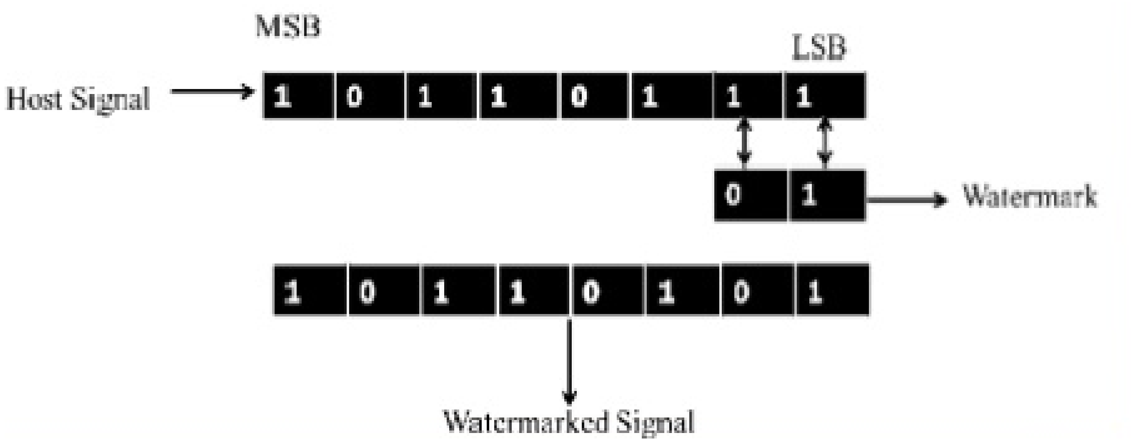


Figure 1.9: Instant Bit Substitution

ADVANTAGE OF IBS:

- IBS substitution is the simplest and most common stego-technique and it can also be used for different color models.
- This method can reach a very high capacity with very little, if any, visible impact to the cover digital media.
- It is relatively easy to apply on images and radio data.
- Many tools for LSB data substitution are available on internet.

DISADVANTAGE OF IBS:

- It is relatively simple to detect hidden data.
- It does not offer robustness against small modification(including compression) at stego images.

Chapter 2

Literature Survey

Secure and Robust Fragile Watermarking Scheme for Medical Images [2.1]:

It proposes a new fragile watermarking-based scheme for image authentication and self-recovery for medical applications. The proposed scheme locates image tampering as well as recovers the original image. A host image is broken into 4 × 4 blocks and singular value decomposition (SVD) is applied by inserting the traces of block wise SVD into the least significant bit of the image pixels to figure out the transformation in the original image. Two authentication bits namely block authentication and self-recovery bits are used to survive the vector quantization attack. The insertion of self-recovery bits is determined with Arnold transformation, which recovers the original image even after a high tampering rate. SVD-based watermarking information improves the image authentication and provides a way to detect different attacked area of the watermarked image. The proposed scheme is tested against different types of attacks such as text removal attack, text insertion attack, and copy and paste attack. Compared with the state-of-the art methods, the proposed scheme greatly improves both tamper localization accuracy and the peak signal to noise ratio of self-recovered image.

Visual Attention-Based Image Watermarking [2.2]:

This paper exploit the concept that if distortion due to high strength watermarking can avoid visually attentive regions, such distortions are unlikely to be noticeable to any viewer and proposes a novel visual attention-based highly robust image watermarking methodology by embedding lower and higher strength watermarks in visually salient and non-salient regions, respectively. A new low complexity wavelet domain visual attention model is proposed that allows to design new robust watermarking algorithms. The proposed new saliency model outperforms the state-of-the-art method in joint saliency detection and low computational complexity performances. In evaluating watermarking performances, the proposed blind and non-blind algorithms exhibit increased robustness to various natural image processing and filtering attacks with minimal or no effect on image quality, as verified by both subjective and objective visual quality evaluation.

SBPG: Secure Better Portable Graphics for Trustworthy Media Communications in the IoT [2.3]:

This paper addresses some of the challenges faced in the IoT infrastructure, specifically secure communication and user authentication in the context of automated analysis of biomedical images and communication of the analysis results and related metadata in a smart healthcare framework. A hardware architecture for a secure digital camera integrated with the secure better portable graphics (SBPG) compression algorithm, suitable for applications in the IoT, is proposed in this paper. The proposed SBPG architecture offers two layers of protection, concurrent encryption and watermarking, which address all issues related to security, privacy, and digital rights management. The experimental results demonstrate that the new compression technique BPG outperforms JPEG in terms of compression quality and compressed file size while providing increased image quality. High performance requirements of BPG have been met by employing two techniques: 1) insertion of an encrypted signature in the center portion of the image and 2) frequency-domain watermarking using block-wise DCT of size 8 × 8 pixels. These approaches optimize the proposed architecture by decreasing computational complexity while maintaining strong protection, with concomitant increase of the speed of the watermarking and compression processes.

A Review of Text Watermarking: Theory,Methods, and Applications [2.4]:

This paper studies the theory, methods, and applications of text watermarking, which includes the discussion on the definition, embedding and extracting processes, requirements, approaches, and language applications of the established text watermarking methods. This paper reviews in detail the new classification of text watermarking, which is through embedding process and its related issues of attacks and language applicability. Open research challenges and future directions are also investigated, with a focus on its information integrity, information availability, originality preservation, information-confidentiality, protection of sensitive information, document transformation, cryptography application, and language flexibility.

A Survey on Big Data Market: Pricing, Trading and Protection [2.5]:

For this paper, they conducted a comprehensive survey on the lifecycle of data and data trading. To be specific, they first studied a variety of data pricing models, categorizing them into different groups, and conducting a comprehensive comparison of the pros and cons of these models. Then, they focused on the design of data trading platforms and schemes, supporting efficient, secure, and privacy-preserving data trading. Finally, they reviewed digital copyright protection mechanisms, including digital copyright identifier, digital rights management, digital encryption, watermarking, and others, and outline challenges in data protection in the data trading lifecycle.

A Robust Image Watermarking Technique with an Optimal DCT-psycho-visual Threshold [2.6]:

It presents a reliable digital watermarking technique that provides high imperceptibility and robustness for copyright protection using an optimal discrete cosine transform (DCT) psycho-visual threshold. An embedding process in this watermarking technique utilizes certain frequency regions of DCT, such that insertion of watermark bits causes the least image distortion. Thus, the optimal psycho-visual threshold is determined to embed the watermark in the host image for the best image quality. During the insertion of watermark bits into the certain frequencies of the image, watermark bits are not directly inserted into the frequency coefficient; rather, the certain coefficients are modified based on some rules to construct the watermarked image. The embedding frequencies are determined by using modified entropy finding large redundant areas. Furthermore, the watermark is scrambled before embedding to provide an additional security.

Hybrid Predictor Based Four-Phase Adaptive Reversible Watermarking [2.7]:

It propose a prediction error expansion based watermarking scheme that allows embedding reversible watermark in the image with low distortion. Research work proposes four-phase representation of image which allows exploitation of larger prediction context. It also proposes a hybrid predictor that helps enhance the prediction accuracy. To reduce image distortion at lower capacity payloads, it uses sorting of estimated prediction errors through sorting of prediction context variances. For improvement at higher capacity payloads, adaptive embedding is used to determine whether to embed single or two bits in a given prediction error. The results are compared against some state-of-the-art techniques in the field and show promising results.

Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption [2.8]:

This paper presents a chaotic encryption-based blind digital image watermarking technique applicable to both grayscale and color images. Discrete cosine transform (DCT) is used before embedding the watermark in the host image. The host image is divided into 8 × 8 non-overlapping blocks prior to DCT application, and the watermark bit is embedded by modifying difference between DCT coefficients of adjacent blocks. Arnold transform is used in addition to chaotic encryption to add double-layer security to the watermark. Three different variants of the proposed algorithm have been tested and analyzed. The simulation results show that the proposed scheme is robust to most of the image processing operations like joint picture expert group compression, sharpening, cropping, and median filtering. To validate the efficiency of the proposed technique, the simulation results are compared with certain state-of-art techniques.

On the Properties of Non-Media Digital Watermarking: A Review of State of the Art Techniques [2.9]:

This paper reviews recent developments in the non-media applications of data watermarking, which have emerged over the last decade as an exciting new sub-domain. Since the intended receiver should be able to detect the watermark, it redefine invisibility in an acceptable way that is often application-specific and thus cannot be easily generalized. This paper classify the data in terms of data mining rules on complex types of data such as time-series, symbolic sequences, data streams, and so forth. We emphasize the challenges involved in non-media watermarking in terms of common watermarking properties, including invisibility, capacity, robustness, and security.

Secure and robust digital image watermarking scheme using logistic and RSA encryption [2.10]:

This paper proposed a new digital image watermarking model based on scrambling algorithm Logistic and RSA asymmetric encryption algorithm to guarantee the security of the hidden data at the foundation of large embedding capacity, good robustness and high computational efficiency. The experiments involved applying the encryption algorithms of Logistic and RSA to the watermark image and performing the hybrid decomposition of discrete wavelet transform (DWT) and Singular Value Decomposition (SVD) on the host image, and the watermark was embedded into the low-frequency sub-band of the host. The values of PSNR and NCC were measured to estimate the imperceptibility and robustness of the proposed watermarking scheme, and the CPU running time was recorded to measure the complexity of the proposed main algorithm in execution time. Experimental results showed the superiority of the proposed watermarking scheme.

Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review [2.11]:

This paper presents a survey of medical images watermarking and offers an evident scene for concerned researchers by analysing the robustness and limitations of various existing approaches. This includes studying the security levels of medical images within PACS system, clarifying the requirements of medical images watermarking and defining the purposes of watermarking approaches when applied to medical images.

Digital image watermarking based on angle quantization in discrete contourlet transform [2.12]:

A robust and transparent watermarking scheme based on contourlet transform and quantization index modulation is proposed in this paper. In proposal algorithm, after taking contourlet, the coefficients are divided into three quadrants by using the symmetric property of the contourlet coefficients, then the angle coefficients are modulated for each of three points. The experimental results revealed that if the information of the image is utilized to determine the watermark and by using quantization index modulation properties, a higher robustness and more effective imperceptibility in proposed algorithm are achieved.

Transparent Digital Watermark on Drug's Images [2.13]:

The pharmaceutical system research and development foundation has an intention to identify the ownership of the pictures of drugs which are going to be shown on YaAndYou.net website by inserting digital watermark which does not affect the quality of pictures. If the picture is modified, the research team can verify its originality. To add a digital watermark on pictures of drugs is to create the transparent digital watermark by using Alpha Channels and Alpha Blending techniques. The permanent watermark on the pictures of drugs will support users who need to consider the drug pictures which are not garbled and able to verify the ownership of the pictures from the website, Yaandyou.net. The research team has developed the program for creating digital watermark from an open source tool and tested with 265 pictures of drugs. The experimental results show digital watermark in the form which is embedded in the drug photos, taken by staffs of

Yaandyou.net. The presence of digital watermark does not reduce the quality of the photos, and the pictures can be proven that they are originated from Yaandyou.net with 100% accuracy of correctness via image editing program and 80.50% via template matching method of Open CV program.

Watermarking through image geometry change tracking [2.14]:

This paper contributes to the state of the art by proposing an image watermarking technique that attempts to model the attacks like cropping, scaling and rotation in terms of the image geometry. The proposed scheme is acceptably resistant to common geometric attacks and common image processing attacks. The watermark embedding is also done efficiently to offer resistance to image processing attacks. The watermark detection procedure is blind and key based, also not requiring the original cover work for watermark extraction. Efforts have been given to ensure that the proposed scheme conforms to robustness against attacks and exhibits high visual fidelity of the watermarked cover.

Adaptive Digital Watermarking for Copyright Protection of Digital Images in Wavelet Domain [2.15]:

In this paper, an adaptive invisible watermarking scheme is proposed in wavelet domain. The proposed method is adaptive in the sense that the scaling and embedding factors are calculated using Bhattacharyya distance and the fourth cumulant moment - kurtosis. The proposed method can be easily employed to preserve the ownership rights and in addition for piracy of digital data prevention. The proposed method is robust to all image and signal processing attacks and highly secured for the protection of copyright information as the process is executed in wavelet domain. Experimental results and statistical evaluation of the results shows the efficacy of the proposed method.

Robust Method for Protecting Electronic Document on Waterway Transport with Steganographic Means by Embedding Digital Watermarks into Images [2.16]:

The scope of this paper is the development and analysis of algorithms for implementation of the digital watermark (DWM) on the basis of the brightness modulation in blocks of graphic documents, allowing at the same time providing covert insertion of any sequence of a given amount of information and authentication of the image, in which Digital Watermark was incorporated. To enhance the robustness of embedded digital watermark attachments, it is required to apply the same transformations in compression of graphic documents in stegno-algorithm like in the compression algorithms for these files.

A new robust watermarking system in integer DCT domain [2.17]:

In this paper, a robust watermarking technique is proposed using integer discrete cosine transform, non-linear chaotic map and dynamic stochastic resonance (DSR). Firstly, the host image is transformed into integer DCT domain where the coefficients are partitioned into non-over-lapping blocks. A circulant matrix is then constructed from the selected blocks. Block selection is done using a non-linear chaotic map. This circulant matrix is used for embedding the watermark by computing the singular values. The extraction of the watermark is done by producing the dynamic stochastic resonance (DSR) phenomena and casting a verification step. This verification step essentially solves the false positive detection problem that arises in SVD based watermarking.

On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching [2.18]:

In this paper, a novel technique based on the matching of bit pairs and symmetric key cryptography is proposed. Pixel bits of original image and encrypted watermark image are arranged in pairs. The pixel bits are represented in pairs following the proposed algorithm, then the encrypted watermark pixel bit pairs are compared with all bit pairs of original image and accordingly the replacement of bit pairs takes place with the respective matched pair assigned number binary equivalent. If no match is found then go for replacing the 0th pair with watermark bits and replace the two LSB with the value of pair number 0. The proposed mechanism shows good quality of watermarked image along with good PSNR values with a good payload.

A study on image digital watermarking based on wavelet transform [2.19]:

This paper studies the methods of image digital watermarking based on wavelet transform. Firstly, the characteristics of image digital watermarking as well as its processing procedure are introduced. On this basis, the discrete wavelet transform (DWT) is selected to achieve the embedding and distilling of image digital watermarking. Simulation test proves that this algorithm can embed or distill digital watermark effectively. Meanwhile it also proves that this watermark has better abilities of hiding and anti-interference. This method results in significant amount of computational savings as well.

A new robust digital watermarking using local polar harmonic transform [2.20]:

This paper proposes a robust digital image watermarking scheme based on local polar harmonic transform. The proposed scheme has the following advantages:

(1) The stable and uniform image feature points are extracted by the improved speeded-up robust feature (SURF) detector, in which the probability density gradient is utilized

(2) The affine invariant local feature regions are constructed adaptively according to the variation of local probability density

(3) A new and effective 2D transform, named polar harmonic transform (PHT), is introduced to embed watermark in the digital image.

Experiments are carried out on a digital image set of 100 images collected from Internet, and the preliminary results show that the proposed image watermarking is not only invisible and robust against common image processing operations such as filtering, noise adding, and JPEG compression, but also robust against the geometric distortions.

Digital watermarking algorithm based on space-time coding [2.21]:

In this paper, the digital image watermarking system is extended from SISO to MIMO systems based on space-time coding and MIMO communication theory. The new watermarking algorithm is designed in the new framework of space-time coding and MIMO-based communication theory. The watermark capacity and the detection error rate also are further studied under the conditions of different space-time coding. These studies will provide a new idea for the design of new digital watermarking algorithm.

Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network [2.22]:

Digital watermarking, which has been proven effective for protecting digital data, has recently gained considerable research interest. This study aims to develop an enhanced technique for producing watermarked images with high invisibility. During extraction, watermarks can be successfully extracted without the need for the original image. It has developed discrete wavelet transform with a Haar filter to embed a binary watermark image in selected coefficient blocks. A probabilistic neural network is used to extract the watermark image. To evaluate the efficiency of the algorithm and the quality of the extracted watermark images, we used widely known image quality function measurements, such as peak signal-to-noise ratio (PSNR) and normalized cross correlation (NCC). Results indicate the excellent invisibility of the extracted watermark image (PSNR = 68.27 dB), as well as exceptional watermark extraction (NCC = 0.9779). Experimental results reveal that the proposed watermarking algorithm yields watermarked images with superior imperceptibility and robustness to common attacks, such as JPEG compression, rotation, Gaussian noise, cropping, and median filter.

A new multiplicative watermark detector in the contourlet domain using t Location-Scale distribution [2.23]:

In this study, a multiplicative watermarking scheme is proposed in the contourlet domain. Overall, selection of proper models is of great importance, as watermark detection processes can be replicated as decision rules. Accordingly, in this study, contourlet coefficients were modeled based on t-location scale distribution. Based on the Kolmogorov–Smirnov test, t Location-Scale distribution showed high efficiency in modeling the coefficients. We used the likelihood ratio decision rule and t-location scale distribution to design an optimal multiplicative watermark detector. Then, we derive the receiver operating characteristics (ROC) analytically. The detector showed higher efficiency than other watermarking schemes in the literature, based on the experimental results, and its robustness against different attacks was verified.

Digital images authentication scheme based on bimodal biometric watermarking in an independent domain [2.24]:

With the growing accessibility and usability of internet there is a growing concern over content protection of digital images. Recently, to eliminate the traditional use of passwords and to ensure that the access to the image is restricted only to legitimate users, security solutions are increasingly combined with biometrics. Consequently, biometric-based watermarking algorithms, that involve embedding the identity of the owner, are proposed to solve ownership disputes. This paper presents a new scheme for protecting and authenticating invisibly watermarked digital images. It applies Independent Component Analysis to the cover image and enables the insertion of two independent watermarks based on fingerprint and iris biometrics. In this approach biometric techniques are used for watermarks generation and for owners authentication. The main advantage of proposed algorithm is construction of ICA based watermarking domain to enable insertion of two independent watermarks, that improve authentication accuracy and makes scheme more robust.

An Adaptive Digital Image Watermarking Algorithm Based on Morphological Haar Wavelet Transform [2.25]:

At present, much more of the wavelet-based digital watermarking algorithms are based on linear wavelet transform and fewer on non-linear wavelet transform. This paper proposes an adaptive digital image watermarking algorithm based on non-linear wavelet transform--Morphological Haar Wavelet Transform. In the algorithm, the original image and the watermark image are decomposed with multi-scale morphological wavelet transform respectively. Then the watermark information is adaptively embedded into the original image in different resolutions, combining the features of Human Visual System (HVS). The experimental results show that our method is more robust and effective than the ordinary wavelet transform algorithms.

Digital watermarking for camera-captured images based on just noticeable distortion and Wiener filtering [2.26]:

This paper proposes a digital image watermarking method for camera-captured images. In this proposed method, an image component of all image pixels is used for embedding an individual watermark bit in order to provide large amount of the embedded watermark. The watermark strength is adjusted in accordance with the modified just noticeable distortion. After the watermarked image is printed and then captured by a digital camera, the reliable watermark extraction is accomplished based on the techniques of reducing distortions introduced from the printing and camera-capturing processes, and predicting original image component from the watermarked image component. In the experiments, various types of pixel value distortions and geometric distortions are considered and explored. With the proposed method, the results show that the watermark can be invisibly embedded, and reliably extracted. We also demonstrate its robustness against various types of distortions from the printing and camera-capturing processes.

Imperceptible reversible watermarking of radiographic images based on quantum noise masking [2.27]:

It proposes a new fragile reversible watermarking scheme for digital radiographic images, the main originality of which stands in masking a reversible watermark into the image quantum noise (the dominant noise in radiographic images). More clearly, in order to ensure the watermark imperceptibility, our scheme differentiates the image black background, where message embedding is conducted into pixel gray values with the well-known histogram shifting (HS) modulation, from the anatomical object, where HS is applied to wavelet detail coefficients, masking the watermark with the image quantum noise. In order to maintain the watermark embedder and reader synchronized in terms of image partitioning and insertion domain, our scheme makes use of different classification processes that are invariant to message embedding.

Ownership protection of plenoptic images by robust and reversible watermarking [2.28]:

Plenoptic images are highly demanded for 3D representation of broad scenes. Contrary to the images captured by conventional cameras, plenoptic images carry a considerable amount of angular information, which is very appealing for 3D reconstruction and display of the scene. Plenoptic images are gaining increasing importance in areas like medical imaging, manufacturing control, metrology, or even entertainment business. Thus, the adaptation and refinement of watermarking techniques to plenoptic images is a matter of raising interest. In this paper a new method for plenoptic image watermarking is proposed. A secret key is used to specify the location of logo insertion. Employing discrete cosine transform (DCT) and singular value decomposition (SVD), a robust feature is extracted to carry the watermark. The Peak Signal to Noise Ratio (PSNR) of the watermarked image is always higher than 54.75 dB which is by far more than enough for Human Visual System (HVS) to discriminate the watermarked image. The proposed method is fully reversible and, if no attack occurs, the embedded logo can be extracted perfectly even with the lowest figures of watermark strength. Even if enormous attacks occur, such as Gaussian noise, JPEG compression and median filtering, our method exhibits significant robustness, demonstrated by promising bit error rate (BER) performance.

Chapter 3

System Design

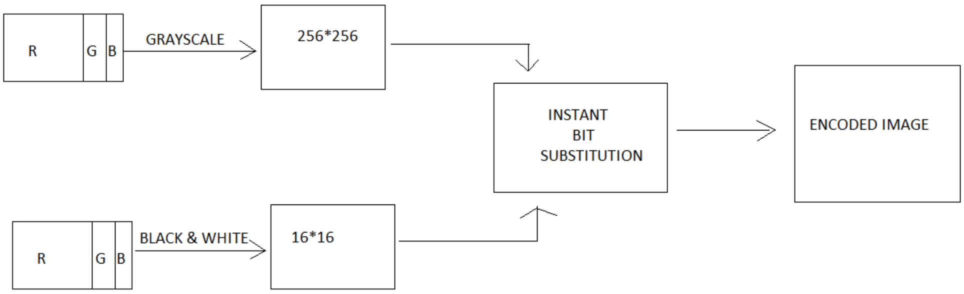


Figure 3.1: Block Diagram of Encoder

3.1 DESIGN OF AN ENCODER:

- First, we are taking a Cover Image and resize it into 256*256 pixels and then convert the RGB Cover Image into a Grayscale Image.
- Then we take the Watermark Image and resize it into 16*16 pixels and convert it into Black and White Image.
- Take a zeros matrix of size 256*256.
- Now we take two loops and a counter to visit each pixel of the Cover Image once.
- As we visit the first pixel whose value is greater than the threshold value (here it's 200) we convert the decimal pixel number into its binary form and substitute the second last bit of the pixel with the value of first pixel of the Watermark Image, for second pixel greater than threshold with the value of second pixel of Cover Image.

Let P (a pixel of the Cover Image) =205

P is greater than 200, so it is converted into Binary form:

205--------->1 1 0 0 1 1 0 1

Let the corresponding pixel of Cover Image be 1

Therefore the 2nd last bit of the Cover Image get substituted with the value of Cover Image

1 1 0 0 1 1 0 1-------->1 1 0 0 1 1 1 1

- Now the substituted binary form is converted back into decimal form

1 1 0 0 1 1 1 1-------->207

- Now the substituted pixel value is placed in the zero matrix in the same position as it is in the Cover Image.
- If the pixel value of the Cover Image is less than the threshold value it is placed in the zero matrix in the same position as it is in the Cover Image
- The matrix which we obtain after substituting the zeros from the zero matrix is the Encoded Image.

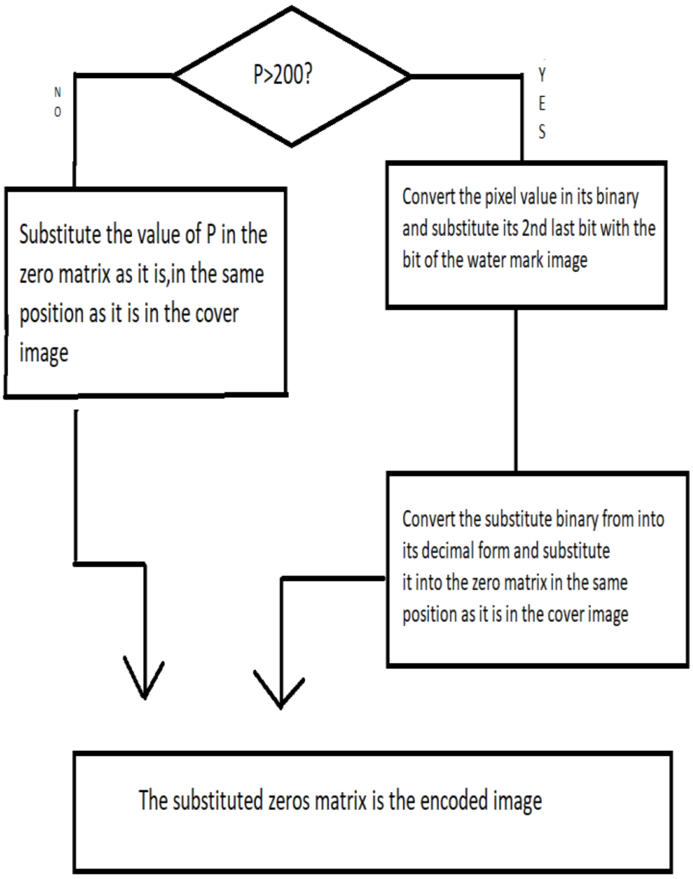

P>200?
NO
YES
Substitute the value of P in the zero matrix as it is,in the same position as it is in the cover image
Convert the pixel value in its binary and substitute its 2nd last bit with the bit of the water mark image
Convert the substitute binary from into its decimal form and substitute it into the zero matrix in the same position as it is in the cover image
The substituted zeros matrix is the encoded image

Figure 3.2: Flowchart of Encoder

3.2 DESIGN OF A DECODER:

- First take the encoded image as the input.
- Take a zeros matrix of size 16*16.
- Now we take two loops and a counter to visit each pixel of the Encoded Image once.
- As we visit the first pixel whose value is greater than the threshold value (here it's 200) we convert the decimal pixel number into its binary form and take the 2nd last bit and multiply it with 256, the result thus obtained is placed in the 1st pixel of the zeros matrix, the other pixels greater than threshold value are substituted in the consecutive positions of the zero matrix.

Let P (a pixel of the Encoded Image) =207

P is greater than 200, so it is converted into Binary form:

207 -------->1 1 0 0 1 1 1 1

The 2nd last bit here is 1 which is then multiplied with 256:

1*256=256

- The Substituted value can either be or 256.
- The resultant substituted zero 16*16 matrix obtained is the Watermark.

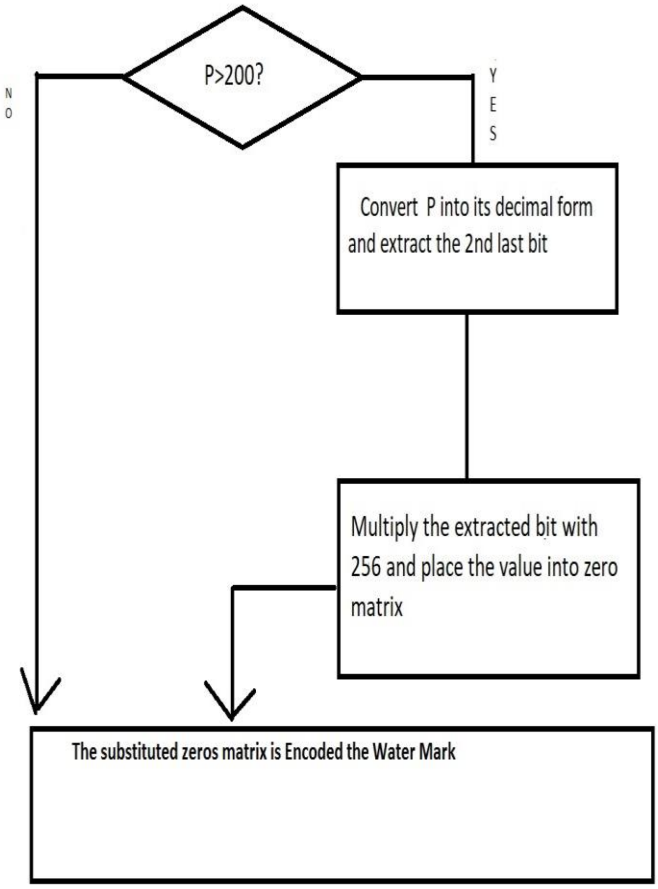

P>200?
NO
YES
Convert P into its decimal form and extract the 2nd last bit
Multiply the extracted bit with 256 and place the value into zero matrix
The substituted zeros matrix is Encoded the Water Mark

Figure 3.3: Flowchart of Decoder

Chapter 4:

Result

4.1 GUI of ENCODING:

After running the encoding code, image 4.1 is obtained where after clicking on “input image to be watermarked” we upload the image to be watermarked. Then clicking on “convert to grey scale” the image to be watermarked is obtained. In a similar way on clicking “input watermark” we upload the watermark image. On clicking “click to watermark” we obtain the watermarked image. Similarly to obtain PSNR, SSM and MSE we need to click on “Peak signal to noise ratio”, “SSIM” and “MSE” we get their values.

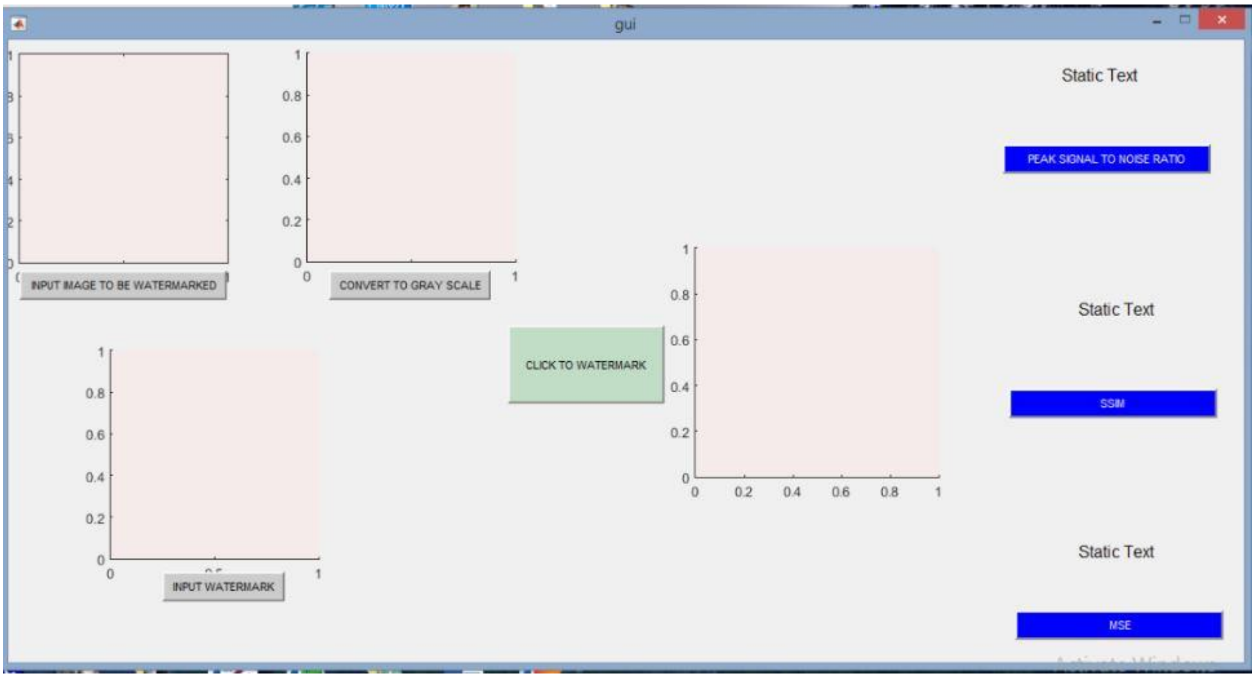
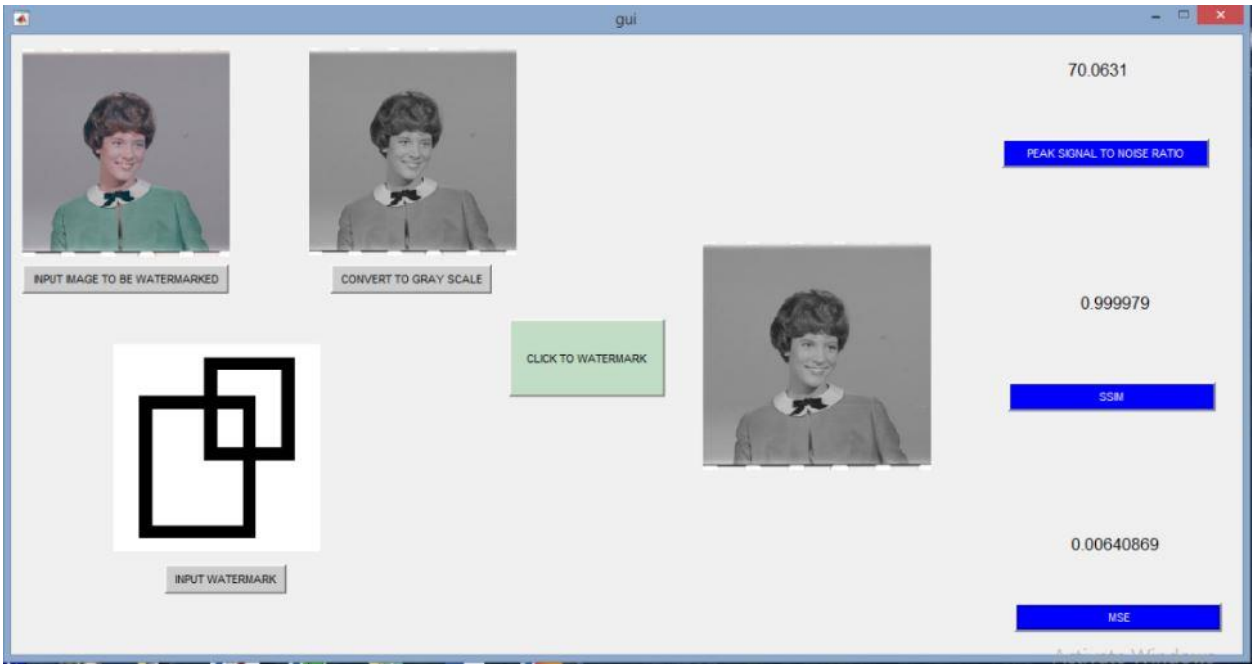


Image 4.1: Result after running the encoding code



70.0631

0.999979

0.00640869

Image 4.2: Result after encoding of images

Image 4.2 is obtained as a result after uploading the image to be watermarked, watermark image and final image with watermark along with values of PSNR, SSIM and MSE.

PSNR, SSIM and MSE of Encoded Image:

PSNR	SSIM	MSE
70.0631	0.999979	0.00640869

Table 4.1: PSNR, SSIM, MSE of Encoded Image

Similarly, we repeat the same process for six different images and obtain the resultant watermarked image along with PSNR, MSE and SSM value for all the images. Image 4.3 shows the result after running the code for six images and image 4.4 shows the output after uploading six images to be watermarked, watermark image and the resultant image after watermarking along with PSNR, MSE and SSM values for individual images.

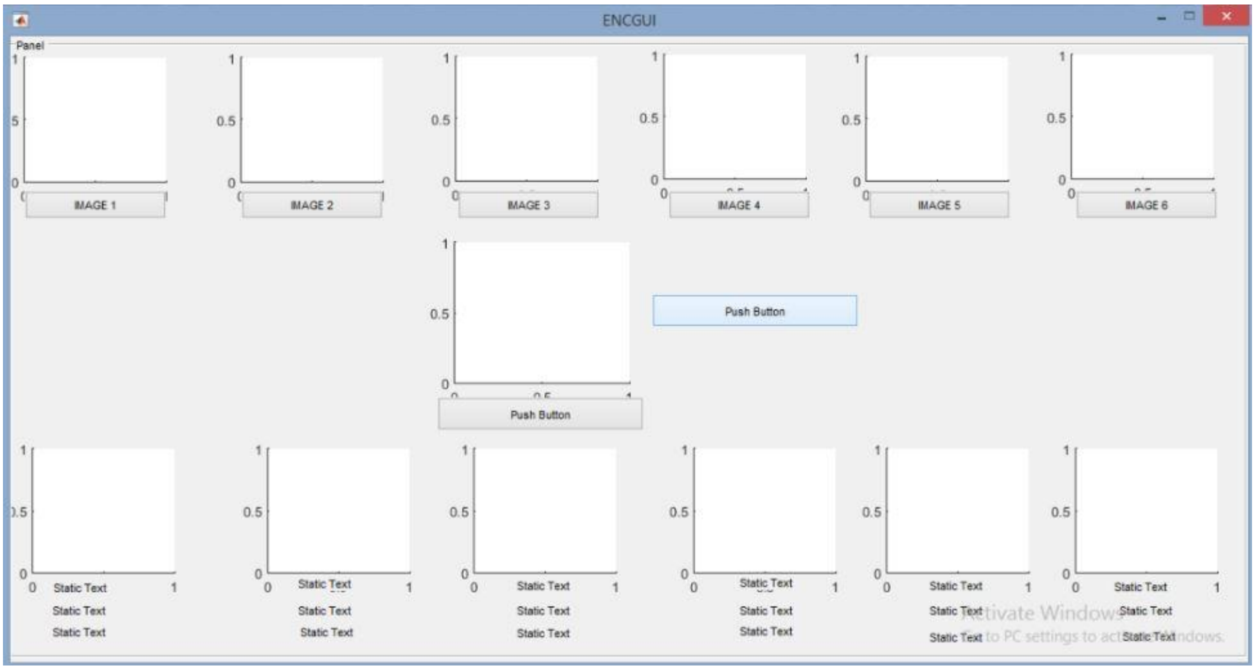
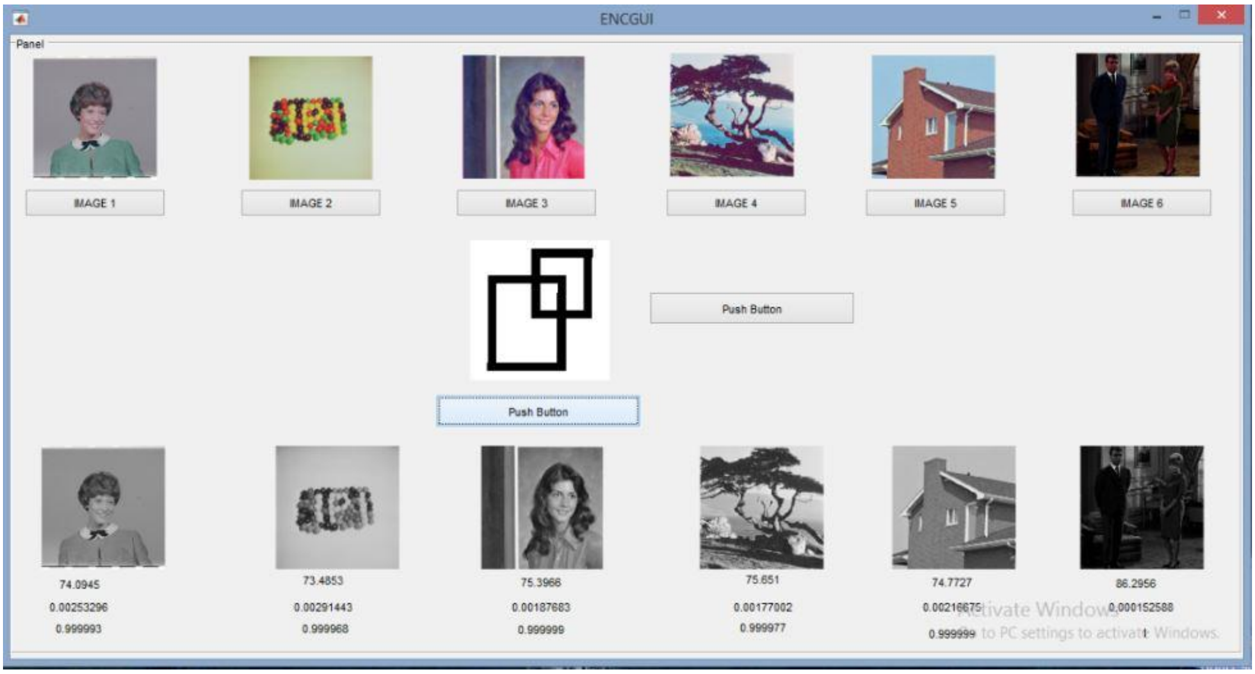


Image 4.3: Result after running the encoding code



```
74.0945       73.4853       75.3966       75.651        74.7727       86.2956
0.00253296    0.00291443    0.00187683    0.00177002    0.00216675    0.000152588
0.999993      0.999968      0.999999      0.999977      0.999999      1
```

Image 4.4: Result after encoding of images

PSNR, MSE, SSIM for different Encoded Images:

Image	PSNR	MSE	SSIM
Image 1	74.0945	0.00253296	0.999993
Image 2	73.4853	0.00291443	0.999968
Image 3	75.3966	0.00187683	0.999999
Image 4	75.651	0.00177002	0.999977
Image 5	74.7727	0.00216675	0.999999
Image 6	86.2956	0.000152588	1

Table 4.2: PSNR, MSE, SSIM of different encoded images

4.2 GUI of Decoding:

After running the decoding code, image 4.5 is obtained where we get the watermark from the watermarked image. After decoding process, the watermark is extracted from the watermarked image

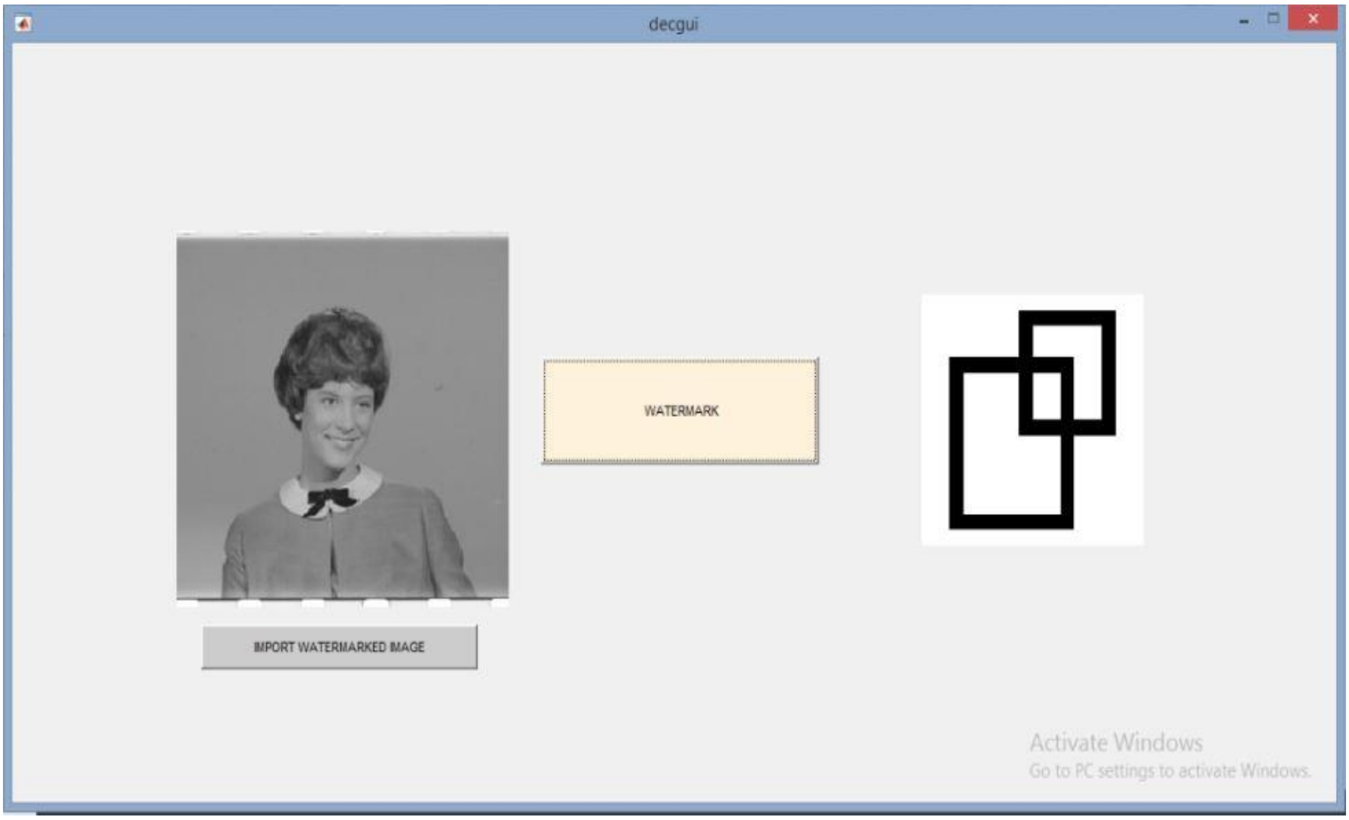


Image 4.5: Result after decoding of image

4.3 Robustness Test:

To test the robustness of the watermark we did certain changes while encoding like we cropped the image, compressed the image, added Gaussian noise and added Salt and Pepper image and then we decoded the changed image and obtained the PSNR, MSE and SSIM of individual images. After decoding of changed watermarked images, watermark is extracted.

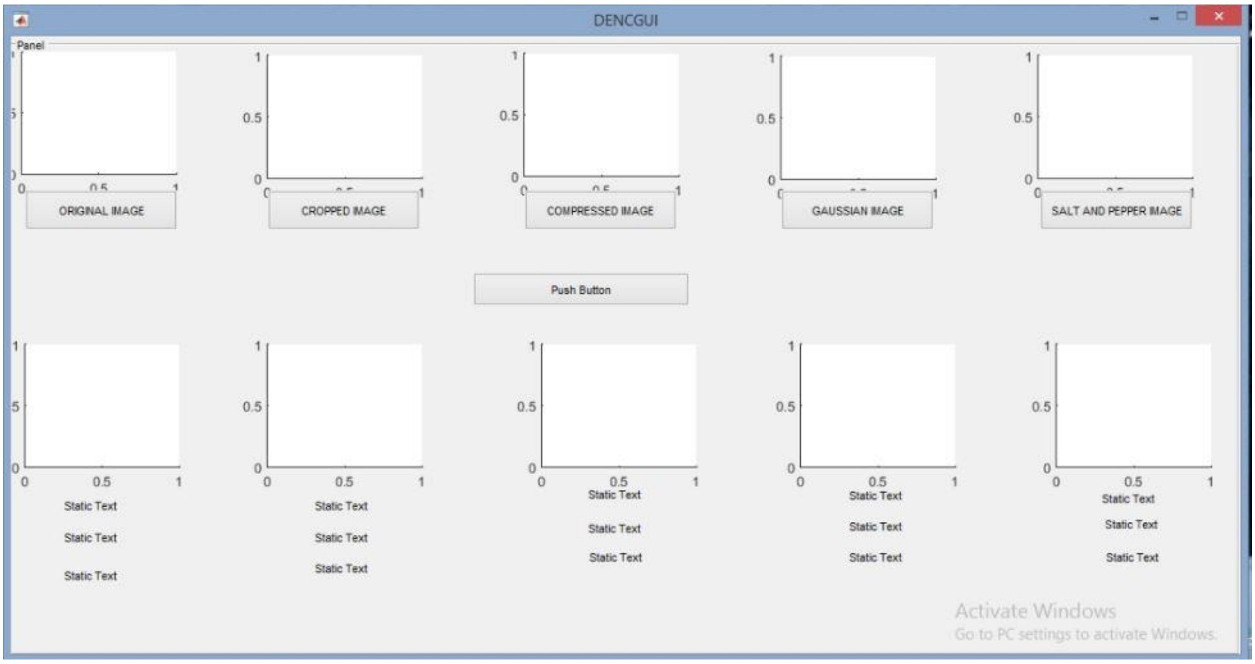
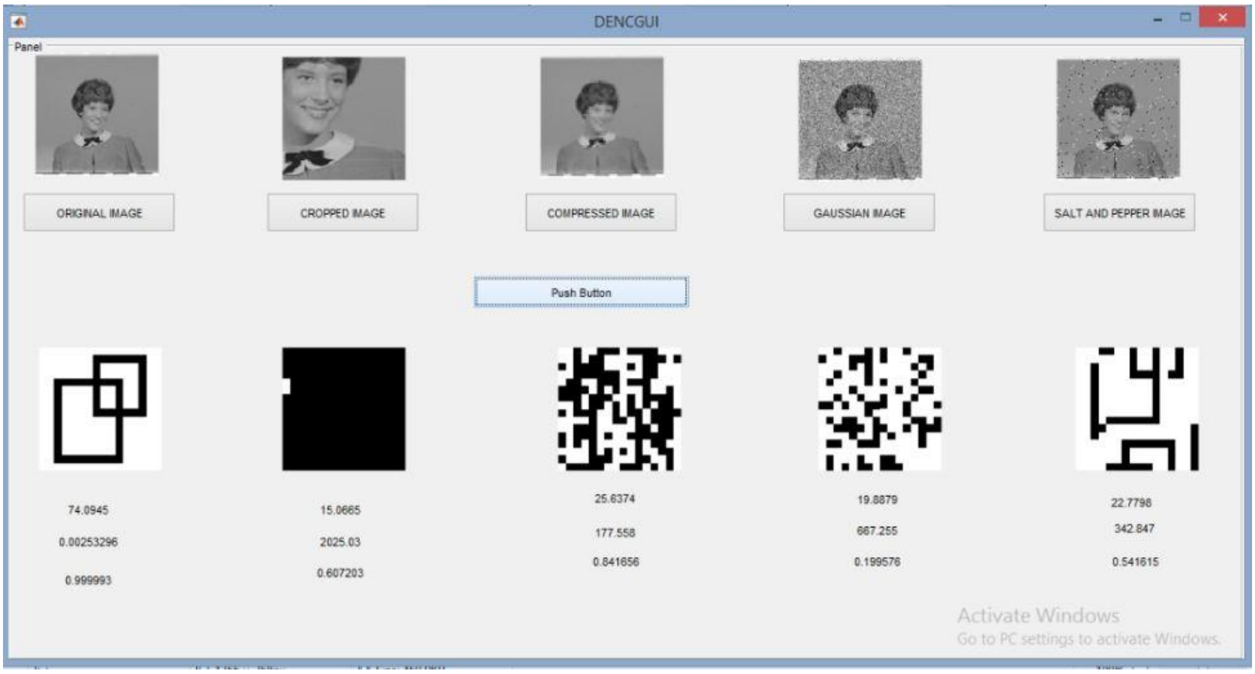


Image 4.6: Result obtained after running the decoding code



```
74.0945          15.0665     25.6374     19.8879     22.7798
0.00253296       2025.03     177.558     667.255     342.847
0.999993         0.607203    0.841656    0.199576    0.541615
```

Image 4.7: Result after decoding of images

PSNR, MSE, SSIM for different Decoded Images after Robustness Test:

Image	PSNR	MSE	SSIM
Original Image	74.0945	0.00253296	0.999993
Cropped Image	15.0665	2025.03	0.607203
Compressed Image	25.6374	177.558	0.841656
Gaussian Image	19.8879	667.255	0.199576
Salt and Pepper Image	22.7796	342.847	0.541615

Table 4.3: PSNR, MSE, SSIM for Decoded Image after robustness test

Extracted Watermark:

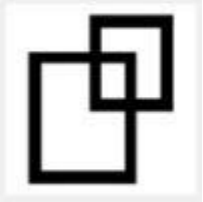
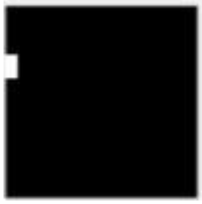
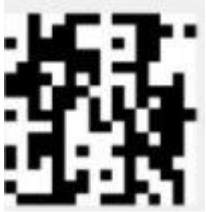
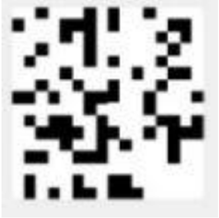
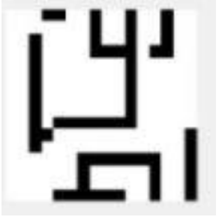
Original Image	Cropped Image	Compressed Image	Gaussian Image	Salt and Pepper Image
				

Table 4.4: Extracted watermarks from different images

Chapter 5

Discussion

The main aim of the present work is the development of image watermarking algorithms, with the state-of-the-art performance. The algorithms performance is validated in the presence of the standard watermarking attacks.

Robustness testing is any quality assurance methodology focused on testing the robustness of software. Robustness testing has also been used to describe the process of verifying the robustness (i.e. correctness) of test cases in the test process.

Robustness:

A digital watermark is called "fragile" if it fails to be detectable after the slightest modification. Fragile watermarks are commonly used for tamper detection (integrity proof). Modifications to an original work that clearly are noticeable, commonly are not referred to as watermarks.

A digital watermark is called *semi-fragile* if it resists benign transformations, but fails detection after malignant transformations. Semi-fragile watermarks commonly are used to detect malignant transformation.

Perceptibility:

A digital watermark is called *imperceptible* if the original cover signal and the marked signal are perceptually indistinguishable.

A digital watermark is called *perceptible* if its presence in the marked signal is noticeable (e.g. Digital On-screen Graphics like a Network Logo, Content Bug, Codes, Opaque images). On videos and images, some are made transparent/translucent for convenience for consumers due to the fact that they block portion of the view; therefore degrading it.

This should not be confused with *perceptual*, that is, watermarking which uses the limitations of human perception to be imperceptible.

PSNR	SSIM	MSE
70.0631	0.999979	0.00640869

Table 5.1: PSNR, SSIM, MSE of Encoded Image

From the table given, we can say that our code is performing well, when it is not subjected to any robustness attack. Also various test performed on the encoded image gives result which is within the desirable range so we can say that our code is imperceptible.

We have performed following attack on our original image:

- Cropping the image
- Compressing the image
- Salt & pepper noise attack on the image
- Gaussian noise attack on the image.

We see that our code is very fragile to these robustness attack.

Chapter 6

Concluding Remark

6.1 CONCLUSION:

We successfully encoded a watermark into a cover image and we have also successfully extracted the watermark from the encoded image. We have used the instant bit substitution method for encryption and also decryption.

Digital watermarking is a rapidly evolving area of research and development. We only discussed the key problems in this area and presented some known solutions.

One key research problem that we still face today is the development of truly robust, transparent and secure watermarking technique for different digital media including images, video and audio.

Another key problem is the development of semi-fragile authentication techniques. The solution to these problem will require application of known results and development of new results in the fields of information and coding theory.

When multimedia content is used for legal purposes, medical applications, news reporting, and commercial transactions, it is important to ensure that the content was originated from a specific source and that it had not been changed, manipulated or falsified. This can be achieved by embedding a watermark in the data.

Subsequently, when the photo is checked, the watermark is extracted using a unique key associated with the source, and the integrity of the data is verified through the integrity of the extracted watermark.

The watermark can also include information from the original image that can aid in undoing any modification and recovering the original. Clearly a watermark used for authentication purposes should not affect the quality of an image and should be resistant to forgeries. Robustness is not critical as removal of the watermark renders the content inauthentic and hence of no value.

6.2 FUTURE WORK:

As we were not getting required result (desired watermark) in our code, when external attacks applied on our encoded image. Our future work will be on robustness. Also after image processing we will go for audio, video watermarking.

Multiple Embedding: Normally, the watermarking technique does not allow multiple watermarking, because by doing it, the previous watermark is not preserved and it getsdamaged. It is observed that the design is successful in implementing a multiple watermarking in each plane. The design allows the owner to perform multiple watermarking on multiple image planes like Red, Green and Blue separately by making use of different DC thresholds.

Different type of noise is added in the watermarked image to damage the watermarked image almost up to 60 to 70 %, however, the recovery of the watermark is observed to be of acceptable quality. The design of algorithm withstands most of the attacks like histogram equalization, intensity change like gamma correction, addition of noise like salt and pepper, Gaussian noise, Poisson noise and speckle noise. Various signal processing operations are applied to check against the robustness of the watermark.

Chapter 7

Reference

[1.1] IJEIT vol 2,issue 9 march 2013 by prabhisheksingh.

[1.2] Schyndelv.r.g ,image processing 1994 IEEE international conference.

[1.3] Kim ,w.g image watermarking schemes IEEE international conference 1999.

[1.4] Langelaar, G.cLagendijk watermarking by DCT coefficient removal.

[1.5] Brog,image watermarking using DCT domain constraint IEEE 1996.

[2.1] Secure and Robust Fragile Watermarking Scheme for Medical Images
Authors: AbdulazizShehab; Mohamed Elhoseny; Khan Muhammad; Arun Kumar Sangaiah; Po Yang; Haojun Huang; GuolinHou
IEEE AccessYear: 2018

[2.2]Visual Attention-Based Image Watermarking
Authors: DeepayanBhowmik; Matthew Oakes; CharithAbhayaratne
IEEE AccessYear: 2016

[2.3] SBPG: Secure Better Portable Graphics for Trustworthy Media Communications in the IoT
Authors: Saraju P. Mohanty; Elias Kougianos; ParthasarathyGuturu
IEEE AccessYear: 2018

[2.4]A Review of Text Watermarking: Theory, Methods, and Applications
Authors: NurulShamimiKamaruddin; AmirrudinKamsin; Lip Yee Por; Hameedur Rahman
IEEE AccessYear: 2018

[2.5]A Survey on Big Data Market: Pricing, Trading and Protection
Authors: Fan Liang; Wei Yu; Dou An; Qingyu Yang; Xinwen Fu; Wei Zhao
IEEE AccessYear: 2018

[2.6] A Robust Image Watermarking Technique With an Optimal DCT-Psychovisual Threshold
Authors: FerdaErnawan; Muhammad NomaniKabir
IEEE AccessYear: 2018

[2.7] Hybrid Predictor Based Four-Phase Adaptive Reversible Watermarking
Authors: Muhammad Ishtiaq; Waqar Ali; Waseem Shahzad; Muhammad ArfanJaffar; Yunyoung Nam
IEEE AccessYear: 2018

[2.8] Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption
Authors: Nazir A. Loan; Nasir N. Hurrah; Shabir A. Parah; Jong Weon Lee; Javaid A. Sheikh; G. Mohiuddin Bhat
IEEE AccessYear: 2018

[2.9] On the Properties of Non-Media Digital Watermarking: A Review of State of the Art Techniques
Authors: ArezouSoltaniPanah; Ron Van Schyndel; TimosSellis; Elisa Bertino
IEEE AccessYear: 2016

[2.10]Secure and robust digital image watermarking scheme using logistic and RSA encryption.

Authors: Liu Yang[a],TangShanyu[b],LiuRan[a],ZhangLiping[a],MaZhao[a]

Science Direct Year: 2017

[2.11] Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art research.

Authors: AsaadF.Qasim[ab]; FaridMeziane[a]; RobAspin[a]
Science Direct Year: 2017

[2.12] Digital image watermarking based on angle quantization in discrete contourlet transformAuthors: AbdulmawlaNajih; S.A.R.Al-Haddad; Abd Rahman Ramli; S.J.Hashim; Mohammad Ali Nematollahi

Science Direct Year: 2016

[2.13]Transparent Digital Watermark on Drug's Images

Authors: Chaiwoot Seetha; SuthidaGoollawattanaporn; ChularatTanprasert
Science Direct Year: 2013

[2.14] Watermarking through image geometry change tracking

Authors: Ratnakirti Roy[a]; TauheedAhmed[b]; SuvamoyChangder[a]
Science Direct Year: 2018

[2.15] Adaptive Digital Watermarking for Copyright Protection of Digital Images in Wavelet Domain

Authors: S.Prasanth Vaidya, P.V.S.S.R. Chandra Mouli
Science Direct Year: 2015

[2.16] Robust Method for Protecting Electronic Document on Waterway Transport with Steganographic Means by Embedding Digital Watermarks into Images

Authors: Maksim Bukharmetov, AnatoliyNyrkov, Sergei Sokolov, Sergei Chernyi, Vladimir Kuznetsov, David Mamunts
Science Direct Year: 2017

[2.17] A new robust watermarking system in integer DCT domain

Author: Satendra Pal Singh; Gaurav Bhatnagar
Science Direct Year: 2018

[2.18] On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching

Authors: Sanjeev Narayan; BalManas; RanjanNayak; Subir Kumar Sarkar
Science Direct Year: 2018

[2.19] A study on image digital watermarking based on wavelet transform

Authors: Hui-fang LI[a]; Ning CHANG[b]; Xiao-mingCHEN[c]
Science Direct Year: 2010

[2.20] A new robust digital watermarking using local polar harmonic transformAuthors: Wang Xiang-yang[ab]; LiuYu-nan[a]; LiShuo[a]; Yang Hong-ying[a]; Niu Pan-pan[a]; Zhang Yan[a]
Science Direct Year: 2015

[2.21] Digital watermarking algorithm based on space-time coding

Authors: Fan Zhang[ab]; XinhongZhang[b]Rui Li[a]
Science Direct Year: 2010

[2.22] Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network

Authors: Yahya AL-Nabhani; Hamid A.Jalab; Ainuddin Wahid; Rafidah Md Noor
Science Direct Year: 2015

[2.23] A new multiplicative watermark detector in the contourlet domain using t Location-Scale distribution

Authors: SadeghEtemad; Maryam Amirmazlaghani
Science Direct Year: 2017

[2.24] Digital images authentication scheme based on bimodal biometric watermarking in an independent domain

Authors: WiolettaWójtowicz; Marek R. Ogiela
Science Direct Year: 2016

[2.25] An Adaptive Digital Image Watermarking Algorithm Based on Morphological Haar Wavelet Transform

Authors: Xiaosheng Huang; Sujuan Zhao
Science Direct Year: 2012

[2.26] Digital watermarking for camera-captured images based on just noticeable distortion and Wiener filtering

Authors: KharitthaThongkor[a]; ThumrongratAmornraksa[a]; Edward J.Delp[b]
Science Direct Year: 2018

[2.27] Imperceptible reversible watermarking of radiographic images based on quantum noise masking

Authors: Wei Pan[a]; DalelBouslimi[a]; Mohamed Karasad[a]; Michel Cozic[b]; GouenouCoatrieux[ac]
Science Direct Year: 2018

[2.28] Ownership protection of plenoptic images by robust and reversible watermarkingAuthors: A.Ansari[a]; S.Hong[a]; G.Saavedra[a]; B.Javidi[b]; M.Martinez-Corral[a]
Science Direct Year: 2018