DIGITAL IMAGE SECURITY USING MULTIPLE WATERMARKING

A Project Report

submitted in partial fulfillment of the requirement for the award of the degree of

Master of Technology

in

COMPUTER SCIENCE & ENGINEERING

Under the Supervision of

Prof. Dr. Satya Prakash Ghrera

By

Sandeep Singh (152201)

Jaypee University of Information Technology
Waknaghat, Solan, Himachal Pradesh, India
May - 2017

CERTIFICATE

This is to certify that thesis report entitled "**Digital Image Security Using Multiple Watermarking**", submitted by **Sandeep Singh** in partial fulfillment of the requirements for the award of the degree of Master of Technology in Computer Science & Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been carried out under my supervision.

This synopsis has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

.

Date:

Signature:

Supervisor's Name:

Designation:

ACKNOWLEDGEMENT

I earnestly wish to express my heartfelt thanks and a sense of gratitude to my guide **Prof. Dr. Satya Prakash Ghrera**, Computer Science & Engineering Department, for their valuable guidance and constant inspiration in preparing this report. My frequent interactions with them in all aspects of the report writing have been a great learning experience for me. I shall always cherish his support and encouragement.

My sincere appreciation is extended to all those people who have helped me directly or indirectly in making these task a success. In this context, I would like to thank all the other staff members, both teaching and non-teaching.

I would also like to express my special gratitude and thanks to our program coordinator **Dr. Pardeep Kumar** for providing the necessary information regarding completion of this project and his kind co-operation and encouragement throughout the project.

I would also like to express my gratitude and appreciation to friends and family who were always very helpful to me. They were always there for me whenever I needed their support.

Date: Signature:

Name:

TABLE OF CONTENTS

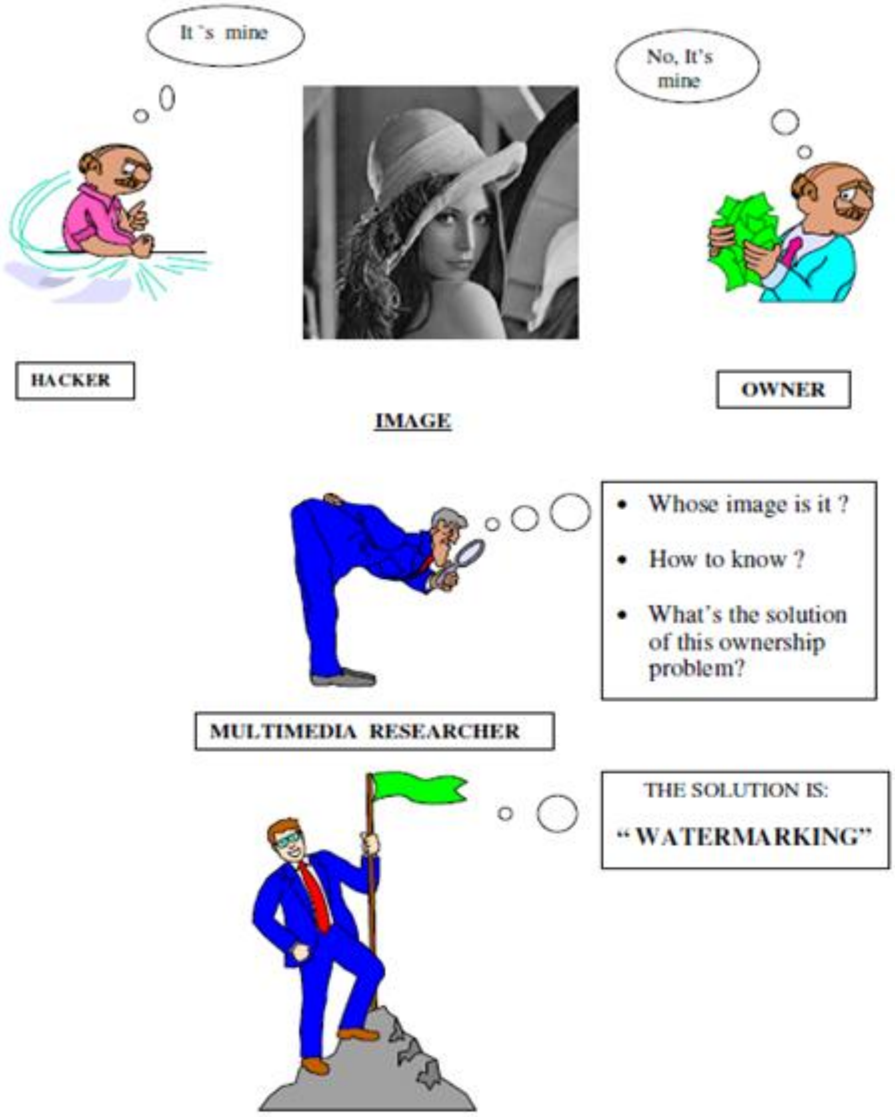
LIST OF FIGURES

LIST OF TABLES

ABSTRACT

For the confidentiality, authenticity and integration or for security of digital content data hiding techniques are used. Data hiding is a phenomenon of hiding information. Various methods have been developed for data hiding as of now but each have some limitations and some advantages too. According to the level and kind of application one or more data hiding methods is used. Data hiding can be done in audio, video, text, and image and in other form of information. In this project a data hiding technique based on multiple watermarking in frequency domain is proposed which can be used to authenticate the digital content and its author's ownership. Multi-level Discrete Wavelet Transformation (DWT) is used, to firstly transform the host image from spatial domain to frequency domain because of the beneficial properties of better spatial localization, high robustness against attacks and better perceiving of Human Visual System (HVS) of this transformation domain. After transformation multiple watermarks and their copies are embedded into the transformed coefficients of host image. These watermarks are related to each other one is text watermark which is authentication information, second is encoded QR code of this authentication information and third is CRC-16 code of this authentication information. The purpose of embedding multiple copies of these watermarks is to strengthen the robustness of watermark. Ultimate aim of this technique to extract at least one watermark in intact form either image watermark or text watermark. Extracted watermark is then compared with extracted CRC-16 code to prove the authenticity of digital content. Bit correction technique is also imposed on text watermarks to decode most accurate information. Related work for techniques used for data hiding in digital image is also described in this report.

Keywords: Digital Image, Watermark, Discrete Wavelet Transformation (DWT), Robustness, Human Visual System (HVS), CRC-16



- Whose image is it ?
- How to know ?
- What's the solution of this ownership problem?

THE SOLUTION IS:

" WATERMARKING"

CHAPTER 1

INTRODUCTION

With the proliferation of digitization of each and every thing, digital Information is ubiquitous nowadays. For the integration, confidentiality and security of Digital Information, traditional data hiding schemes have to be upgraded and need to be used in conjunction with other schemes. For this various schemes has been proposed to protect and secure the Digital Information which are Steganography, Watermarking and Cryptography and their combinations. All of these schemes have different issues to handle and different aims to achieved which is particularly depends upon the type of application domain in which digital Information is being used and manipulated. Security, robustness, imperceptibility and fragility are the main concerns which are associated with these data hiding techniques and some parameters are being used for the acceptability of scheme being used subject to the above concerns which may have different values for different applications. Watermarking is nearly related to Cryptography but watermarking is discrete from encryption [1]. Watermarking techniques based upon embedding a cover image with information which is known as watermark and then the watermarked image is disseminated and then extracted at the receiver [2]. Watermarking requirements are depended upon applications and some most desirable properties for these applications are conflicting in nature [1]. Image encryption techniques are used to provide end-to-end security of digital content during transmission over different distribution systems but watermarking techniques are used as a tool to achieve copyright protection, ownership trace and authentication [3].

1.1 What is data hiding?

Data hiding is a process of hiding information by any mean but to keep the information secret or protected. It is either achieved by hiding the very existence of information by hiding it in some other content or by changing its form so that unintentional users can not access the information meaningfully even if they know the existence of information that it exists the later thing is achieved by using cryptography and former thing is usually achieved using steganography and digital watermarking.

Table 1.1 Data hiding techniques and their goals

Data hiding technique	**Goal of data hiding technique**
Steganography	Hides the existence of secret data from third party
Digital Watermarking	Hides the existence of secret data from third party with notion of robustness
Cryptography	Makes data unreadable by third party even if they know the existence of secret data

1.2 History of data hiding

- In ancient time Chinese military and diplomatic used to wrote the secret messages on fine silk and then it was crunched into a tiny ball and after that, the ball was covered with wax. The ball was placed in the rectum or swallowed by the messenger.
- Giovanni Porta, an Italian scientist in sixteenth century, described a method to conceal a secret message within a hard-boiled egg. He used a mixture of a pint of vinegar and one ounce of alum to make an ink to write on the shell. The ink get penetrated the porous shell, left the secret message below the shell on the surface of the hardened egg albumen, which could only be read after the shell was removed.
- Special chemically affected sympathetic inks were used in world war 2 for encoding secret messages.
- In 1941 FB1 spotted first microdot, which was the technique to hide information by photographically shrinking a page of text into tiny dot having diameter less than 1

millimetre and then hide this dot into an apparently innocuous cover material such as magazines.

- In 1870-1881 during Franco-Prussian war from besieged Paris, secret messages were disseminated on microfilms using pigeon post.
- In 1905 during Russo-Japanese war, microscopic images were used which can be hide in the nostrils, ears and under fingernails.
- Johannes Trithemius printed 6 books, on cryptography and steganography in 1518 entitled ‘Polygraphiae’. Author circulated some books privately but never published, because those who read them found them rather fearsome.
- Paper watermarks appeared 700 hundred years ago in the art of handmade papermarking where they were mainly used to recognize the mill which produced the paper and about the paper format, and its quality and strength.

1.3 Steganography

‘Hiding one piece of data within another.’

Etymologically the word steganography composite of Greek words ‘steganos’ which means ‘protected or covered’ and ‘graphein’ meaning ‘writing’, So in generic sense steganography means ‘concealed writing’.

Steganography is an art and science of writing hidden messages in such a way that no one but only the sender and intended recipient can suspects the existence of the message, a form of security through obscurity.

Example:

Encoded form *“surely everyone can’t regret every time”*

Decoded form *“**s**urely **e**veryone **c**an’t **r**egret **e**very **t**ime”*

Secret message ***“secret”***

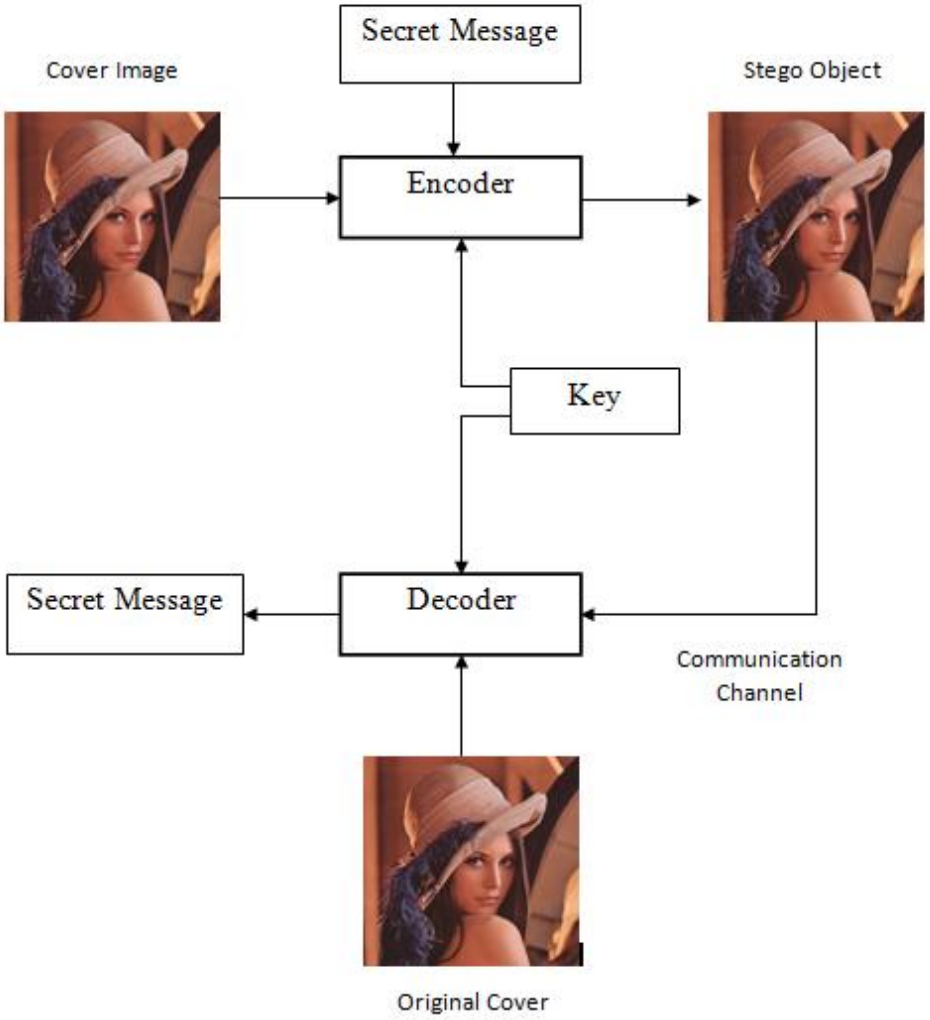


Figure 1.1 Steganographic Process

1.4 Digital Watermarking

Watermarking is also called data embedding and information hiding. Digital watermarking is the method of embedding digital data within the noise tolerant digital multimedia content. This is usually used to verify the credibility of the host content or to recognize the identity of owner of digital content but it can also employed for lot many purposes some of which are tracing copyright infringements, hidden communication, copyright protection, for banknote authentication, broadcast tracking , for source tracking and it’s also used against the piracy and many more. There may or may not be any relation between the hidden information and the host signal but in most of its application there is relation between them. The hidden information within a digital signal such as image, video, audio is known as Watermark. It have the strong integration with the content of host signal itself, there is no need of data format conversation or requirement of additional file header for it. Moreover, it is designed in a way that it can permanently reside in the host signal. Unlike encryption, access to the host data is not restricted in watermarking.

Watermarking, as opposed to steganography, has the additional property of robustness against attacks. It is very tough or ideally impossible to destroy the embedded watermark by an attacker, even if the attacker knows the existence of hidden information in the cover and it is possible even if the algorithmic principle of the watermarking method is public. A practical implication for robustness requirement lies in the fact that much less information is embedded into the host data by watermarking methods as compared to steganographic methods. Steganography and watermarking are thus more complementary than competitive approaches [4]. A watermarking system is usually divided into two distinct steps, embedding process, and extraction process. The general watermarking process is shown in figure below.

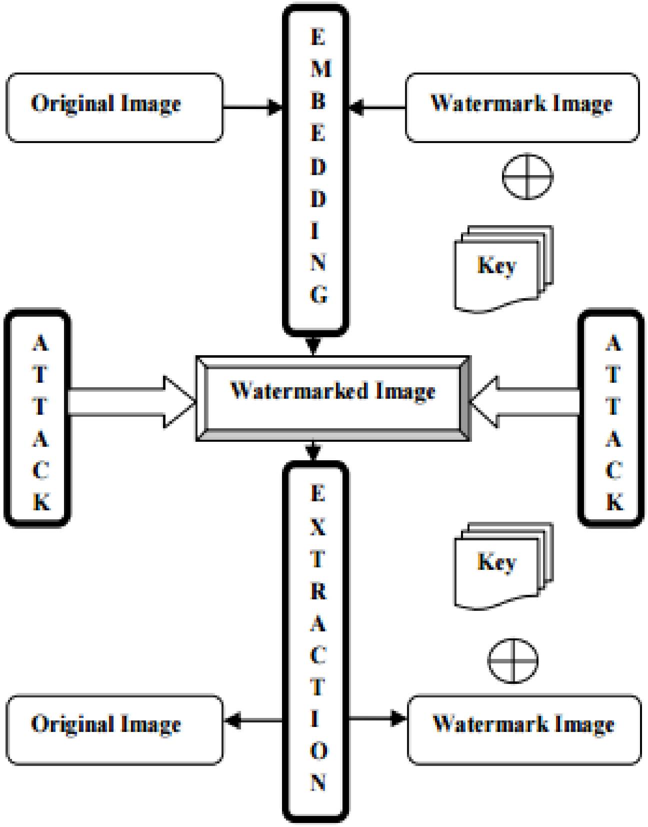


Figure 1.2 Digital Watermarking Framework [5]

Embedding Stage

In embedding process, the watermark is to be embedded into the original host image and produces a watermarked signal by an algorithm using one of the various available embedding techniques. The watermarked signal is then disseminated or stored, usually transmitted to some other person.

Distortion/Attack Stage

It is the stage, where during transmission of host signal data over the network, watermarked signal is exposed to various kinds of attacks. In this stage there is a huge possibility that watermarked data is either modified or destroyed. The capability of watermark to resist in this stage tells the robustness strength of the process.

Detection/Retrieval Stage

In watermark extraction process, embedded watermark is extracted from received watermarked signal. If the signal kept intact during transmission, then the presence of watermark is still there and it can be extracted [6].

1.4.1 Characteristics of Digital Watermarking

The major categorization of main characteristics of digital watermarking are as follows [7]:

Robustness: Capability of the watermark to resist after normal image processing operations such as image transformation, cropping, compression etc.

Imperceptibility: There should be no difference between the appearance of watermarked image and the original cover image which can be detected by the ordinary eye. The watermarked image must appear like same as the original image to the ordinary eye. The observer is unable to detect that watermark is embedded in it.

Security: The ability of not to detect, retrieve or change the embedded watermark by an unauthorized people.

Transparency: It relates to the properties of the human sensory. A transparent watermark causes no artifacts or feature loss.

Capacity: The amount of information bits that can be embedded. There is also the possibility to embed multiple watermarks in parallel. There is trade-off between Capacity and Robustness and Imperceptibility. A higher capacity is usually obtained at the cost of either robustness strength or imperceptibility, or both.

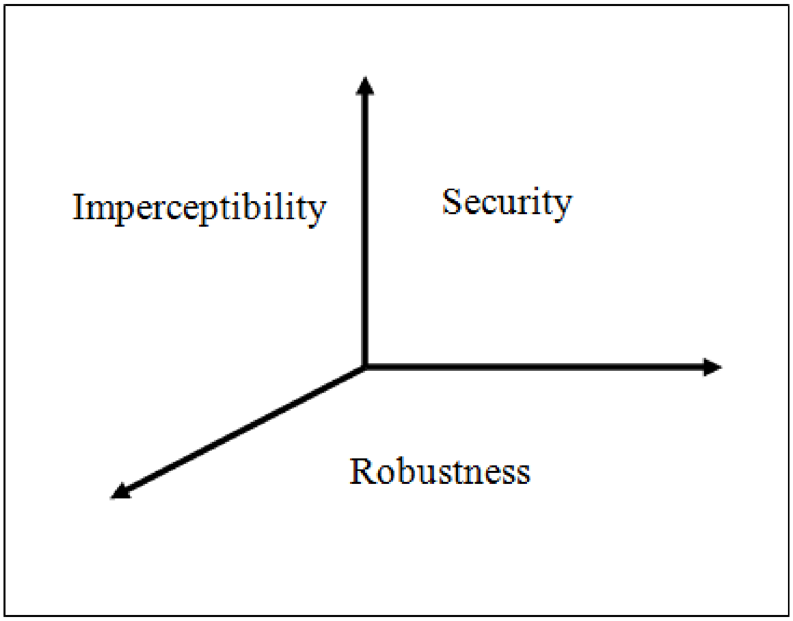


Figure 1.3 Characteristics of digital watermarking [7]

1.4.2 Classification of Digital Watermarking

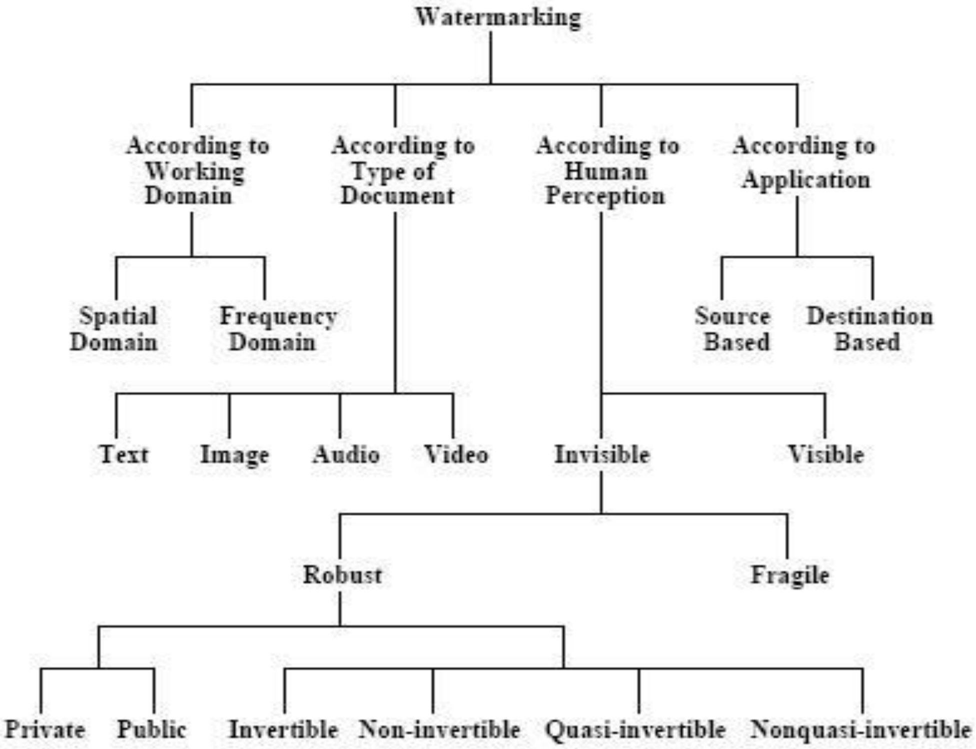


Figure 1.4 Classification of Watermarking [8]

1.4.3 Applications of Digital Watermarking

- Content Identification and management
- Broadcast monitoring
- Document and image security
- Audience measurement
- Digital fingerprinting
- Content protection for audio and video content
- Forensics and piracy deterrence
- Content filtering
- Locating content online
- Improved auditing
- Communication of ownership and copyrights
- Authentication of content and objects
- Rich media enhancement for mobile phones
- Tamper detection
- Content labeling
- Watermarking as a communication system

1.4.4 Distortion and Watermarking Attacks

- Removal Attack
- Interference Attack
- Geometric Attack
- Low pass filtering Attack
- Forgery Attack
- Security Attack
- Cryptographic Attack
- Protocol Attack
- Active Attack
- Passive Attack
- Collusion Attack
- Image Degradation
- Image Enhancement

- Image Compression
- Image Transformation

1.5 Cryptography

Cryptography also known as cryptology is an art to transmit data in the form by scrambling the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or incomprehensible during transmission. It is a process for protecting secret information from undesirable attacks by its attackers. The goal is to protect the content of the data against the attackers. It is the phenomenon of two processes.

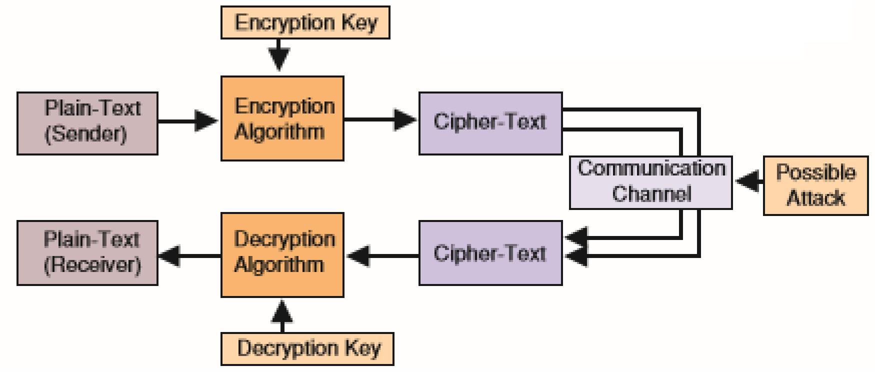


Figure 1.5 Encryption/decryption System [9]

Encryption

To change the plain text into some other unreadable form known as cipher text and then transmitted over the vulnerable medium.

Decryption

The reverse of data encryption is data decryption, which recovers the original data [9].

1.5.1 Objectives of Cryptography:

Modern cryptography concerns itself with the following 4 objectives:

1. **Confidentiality:** The inability to understand the information by unintended users.
2. **Integrity:** Alteration in the information during transmission between sender and intended receiver or storage is not possible without the alteration being detected.
3. **Non-repudiation:** If the information created or transmitted once its creator or sender cannot deny at some later stage his intentions in the creation or transmission of the information.
4. **Authentication:** Identity of the sender and receiver can be confirmed.

1.5.2 Types of Encryption Algorithms:

- **Secret Key Cryptography:** Also known as symmetric key cryptography. Only one key is used by sender and receiver.
- **Public Key Cryptography:** Also known as asymmetric encryption because two keys are used. Public key and private key. Anyone can have access to public key but the private key can only be acquired by the owner of the content. Encryption is achieved by sender using public key and the receiver will decipher the information using his private key. But for non-repudiation, Encryption is achieved by sender using private key, while the receiver uses the sender’s public key to decipher it. Thus, the receiver will get to know who sent it.
- **Hash Functions:** These are different from Secret Key Cryptography and Public Key Cryptography. Also known as one-way encryption and have no key at all. These are mainly used for ensuring that a file has remained unchanged.

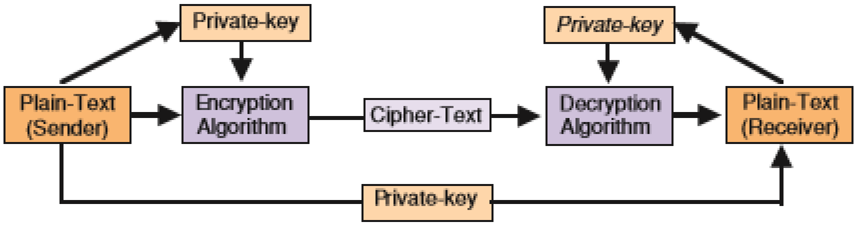


Figure 1.6 Private-key System [9]

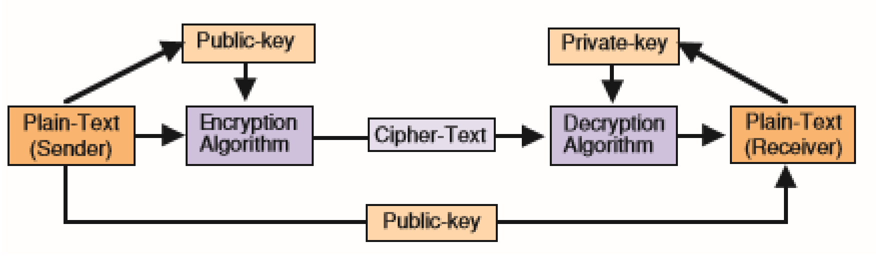


Figure 1.7 Public-key System [9]

CHAPTER 2

WATERMARKING TECHNIQUES

There are various algorithms present in the today scenario that are used to hide the information. Those algorithms come into two domains, Spatial and Frequency domain [10].

2.1 Spatial Domain Techniques

Spatial domain watermarking algorithms used to manipulate image pixels directly. Sometimes for a color image, color components are getting separated first and then information is embedded in individual color components. Some of the techniques used for digital watermarking in spatial domain are listed below [11]:

Additive Watermarking

Pseudo random noise pattern is added to the intensity of image pixels. It is the most straightforward method for embedding information. The noise signal is usually equal to or within the range of (-1, 0, 1). A key is used to generate the noise so that watermark can be detected easily and there must be very low correlation among the different keys.

Least Significant Bit

It is the simplest one technique. The least significant bit of image pixels is manipulated like if we have to embed one character which have 7 bits ascii value then we need 7 pixels to embed the information [12]:

Image bits	10111101 10111011 11011101 01110101….
Watermark	1 0 1 1…..
Watermarked Image	1011110**1** 1011101**0** 1101110**1** 0111010**1**….

This technique is quite imperceptible but it is vulnerable to most of the attacks.

SSM Modulation Based Technique

In SSM techniques energy generated at one or more than one discrete frequencies is deliberately spread or distributed in time. Modulated, small pseudo noise signal is linearly combined with host image in this technique.

Texture mapping coding Technique

This method can be used only in those images which are having some texture part where watermark can be embedded. The suitability of this technique is only for those areas having large number of arbitrary texture images and this is the disadvantage of this technique, and it cannot be automate. This technique embedd data within the continuous random texture patterns of an image.

Patchwork Algorithm

This technique is developed by Bender et alii in 1996. It is firstly published in IBM Systems Journal and based on a pseudorandom, statistical model. Watermark is inserted using Gaussian distribution with a particular statistic. A two pseudo random patches A and B are selected in which one is brighten up and another is darkened for imperceptibility [13].

Correlation-Based Technique

Watermarked_image(x, y) = cover_image(x, y) + gain_vactor * Watermark(x, y)

A pseudorandom noise pattern is added into the cover image which is generated by multiplying gain factor value with the watermark which have to be embedded. But gain factor value is the trade-off between imperceptibility and robustness. If we increase the gain factor value robustness of the process will improve but at the cost of imperceptibility of watermarked image [14].

2.2 Limitations of Spatial Domain Watermarking

Techniques concerning with spatial domain are much simpler than transformational domain but the robustness is the main drawback of these techniques. They can only survive some simple attacks like cropping and some noise addition. Another drawback of these techniques is, for improving the robustness they do not allow for the subsequent processing [11].

2.3 Frequency Domain Techniques

Apart from spatial domain there are other techniques which firstly transform the image into frequency domain and then watermark is embedded directly into the spectral coefficients. These techniques are more robust against attacks then spatial domain techniques and have high capacity of data embedding and have significantly high imperceptibility which means they produce watermarked images of high quality. The reason why frequency domain techniques are been used is that spectral coefficients are better for capturing the characteristics of human visual system (HVS) which will help deciding the intensity and position of watermark to be embedded. With the comparison of spatial-domain techniques, these are more widely used. In frequency domain techniques firstly image is transformed from spatial domain to frequency domain and then watermark is being embedded and after that inverse transformation is applied [10]. The most commonly used transforms are discussed below:

Discrete cosine transforms (DCT)

In DCT data is represented in terms of frequency space instead of an amplitude space. This method is quite useful in a sense that it corresponds more to the way humans perceive light, not perceivable part of data can be identified and thrown away. The watermarking techniques based on DCT have high robustness with comparison to spatial domain techniques. They can cope up with simple attacks such as low pass filtering of an image, brightness and contrast adjustment of an image and blurring etc. but they are more complex to implement and computational complexity is high [15][16]. They are not much robust against geometric attacks such as rotation attack, scaling of an image, cropping etc. Global DCT and Block based DCT watermarking are the classification of discrete cosine transformation based watermarking techniques.. Embedding the data into the portion which is perceptually more significant is beneficial because most of the compression schemes remove the perceptually not significant portion of the image.

DCT Block Based Watermarking Algorithm is as follow:

Step 1. Divide an image into non-overlapping blocks of 8×8

Step 2. Each block is applied with forward DCT

Step 3. Select blocks using some criterion (i.e. HVS)

Step 4. Select the coefficients by some criterion

Step 5. Embed watermark by manipulating the selected coefficients.

Step 6. Apply inverse DCT transform on each block.

In DCT, for embedding the watermark, host image is divided into different frequency bands. In Figure below, FL corresponds to lowest frequency component, FH signifies the higher frequency component and FM signifies the middle frequency component which can be selected as an embedding region. The DCT achieves good robustness against various signal processing attacks the reason is for selecting perceptually significant frequency domain coefficients [25].

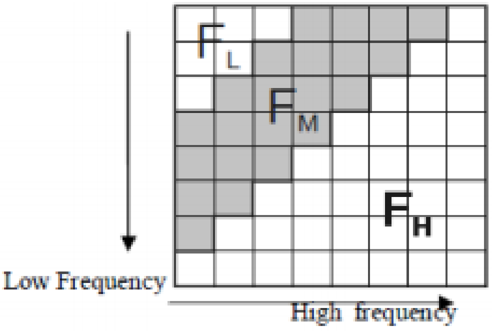
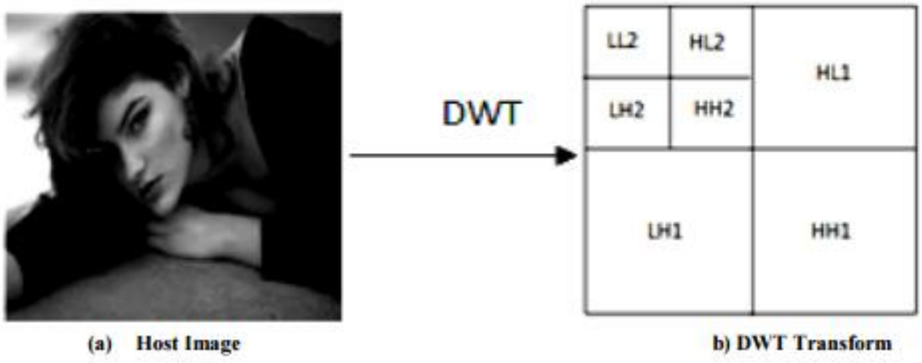


Figure 2.1 Discrete Cosine Transform Region [25]

Discrete wavelet transforms (DWT)

DWT is based on small waves, called wavelet, and these wavelets are of varying frequency and limited duration. This transformation directionally split the image into vertically, horizontally and diagonally. That’s why wavelets reflect the anisotropic properties of HVS with more precision. Magnitude of DWT coefficients is larger in top left sub-band. It is used in a wide variety of signal processing applications, which are for compressing audio and video, removal of noise in audio, and simulation of wireless antenna distribution. DWT is best suitable for watermarking problem because it is useful in achieving a better tradeoff between robustness and imperceptivity. Enhancing the strength of watermark that is to be embedded will help improve the robustness but at the cost of imperceptibility because visible distortion of image get increased as well. However, preference is given to DWT, as it best suitable for both providing simultaneous spatial localization and also watermark’s frequency spread within the cover image. DWT produces multi-resolution representation of an image by multi-differentiated decomposition of an image into sub-images having independent frequencies and different spatial domains and this phenomenon helps interpreting the image information. DWT decomposes the image into quadrants of high and low frequencies [17][18][19].

The one level DWT transformed 2-D image into four sub-bands having different frequencies. Each sub-band contains diagonal, vertical and horizontal details of decomposed image. Maximum information of an image is concentrated in low frequency components, hence they are more robust. It is scalable and original image can be obtained by applying inverse DWT. Excellent spatial localization and multi resolution features make DWT most useful in image processing as it is very convenient to recognize the portion in host image to embed watermark [36].



(a) Host Image

b) DWT Transform

Figure 2.2 2 level DWT decomposition [36]

Merits of DWT over DCT:

- Better visual image quality
- Its higher compression ratios avoid blocking artifacts.
- Better spatial localization
- The watermarking method is more robust using techniques based on DWT
- HVS perceived more clearly in DWT.
- DWT defines the multi resolution description of the image

Demerits of DWT over DCT:

The main disadvantage is the complexity of DWT which higher than DCT. The other limitation is higher computation and longer computation time.

Discrete Fourier Transform (DFT)

DFT transforms a continuous function into its frequency components. It is robust against geometric attacks. It shows translation invariance. Phase representation of the image is affected by spatial shifts but the magnitude representation is not affected. Circular shifts in the spatial domain do not affect the magnitude of the Fourier transform [20].

Some characteristics of DFT:

- Phase and magnitude representation of real image is normally in complex values.
- The central component of DFT is the main and it contains low frequency data.
- Cropping resist as effect of cropping leads to blurriness of spectrum. Synchronization is unwanted if watermark is inserted in magnitude which are normalized coordinates.
- Extracted signal get amplify with scaling of image and can be detected using correlation coefficient.

Advantages of DFT over DWT and DCT:

Rotation Scaling Translation (RST) invariant. So, It can be used to recover from geometric distortion. But DCT and DWT are RST invariant so they lack this property.

Disadvantage of DFT over DWT and DCT:

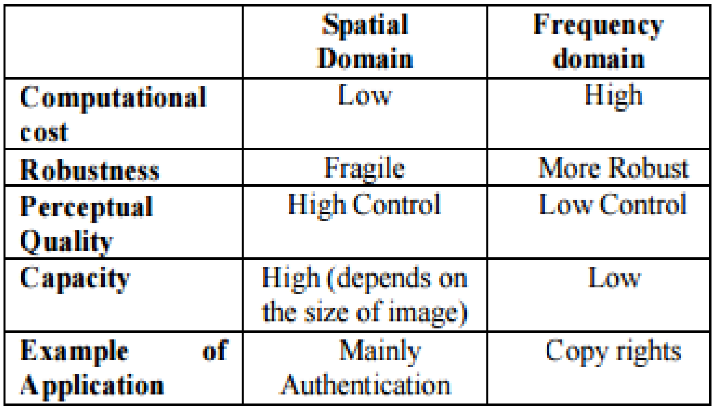
Output of DFT is always in complex value so this is the main limitation. Also it needs more frequency rate and having very poor computational efficiency. That's why DFT is not used much.

Table 2.1 Comparison of different Watermarking Techniques [21]

Technique	Advantages	Disadvantages
LSB	▪ Easy implementation and understandability ▪ Low degradation ▪ High imperceptibility	▪ Low robustness ▪ Vulnerable to noise ▪ Vulnerable to geometric attacks
Correlation based	▪ Robustness can be increased by increasing gain factor value	▪ Image get distorted with increasing gain factor value
DCT	▪ Middle frequency components are used for watermark embedding to get better trade-off between robustness and imperceptibility. ▪ Pixels themselves don't affect each other	▪ Invariance properties of the system been destroyed by block wise DCT ▪ Some higher frequency components tend to be suppressed during the quantization
DWT	▪ Allows good localization in time and spatial frequency domain ▪ Compression ratio is high which is relevant to human perception	▪ High computing cost ▪ Longer time for compression ▪ Noise/blur beside edges of image or video frames

Comparison between spatial domain watermarking and frequency domain watermarking:

Table 2.2 Comparison between Spatial and Frequency Domain Watermarking [5]



	Spatial Domain	**Frequency domain**
Computational cost	Low	High
Robustness	Fragile	More Robust
Perceptual Quality	High Control	Low Control
Capacity	High (depends on the size of image)	Low
Example of Application	Mainly Authentication	Copy rights

CHAPTER 3

LITERATURE SURVEY

3.1 INTRODUCTION

Data hiding is a process of hiding information. Various methods have been developed for data hiding as of now but each have some limitations and some advantages too. According to the level and kind of application one or more data hiding methods is used. Data hiding can be done in audio, video, text, and image and in other form of information. Some data hiding techniques emphasizes on digital image security, some on robustness of digital image hiding process while other's main focus is on imperceptibility of digital image. Capacity of digital information which has to hide is also the main concern in some of the applications. The objective of some of the papers mentioned below is to achieve two or more than two parameters i.e. Security, robustness, imperceptibility and capacity but some of the parameters are trade-off which mean only one can be achieved on the cost of other. So the data hiding techniques aiming to achieve maximum requirements i.e. security, robustness, capacity, imperceptibility etc. and which can be utilized in larger domain of applications is desired. Related work for techniques used for data hiding in digital image is described below in this chapter.

With the hype of digitization of each and every thing, Digital Information is ubiquitous nowadays. For the integration, confidentiality and security of Digital Information, traditional data hiding schemes have to be upgraded and need to be used in conjunction with other schemes. For this various schemes has been proposed to protect and secure the Digital Information which are steganography, watermarking and cryptography and their combinations. All of these schemes have different issues to handle and different aims to achieved which is particularly depends upon the type of application domain in which Digital Information is being used and manipulated. Security, robustness and fragility are the main concern which are associated with these data hiding techniques and some parameters are being used for the acceptability of scheme being used subject to the above concerns which may have different values for different applications.

3.2 RELATED WORK

Various kind of existing schemes that are used for data hiding are discussed here.

R. Gayathri et al. in [22], proposed a method to provide high level of security using combined features of stegnography, cryptography and watermarking. In this scheme a binary image is divided into 8x8 blocks and zigzag hiding sequence is applied on each block so the data hided path cannot be easily predicted then the data encrypted image is created using a (2,2)VC share technique. Anyone who holds only one share cannot reveal the information about secret. Generated shares then embedded into separated cover images by Least Significant Bit (LSB) insertion technique of digital watermarking. The advantage of proposed scheme is that it provide good visual quality and additional security using stegnography but it takes more time in processing because steganographic algorithm is complex

B. Nassiri et al. in [23], proposed a scheme for medical images. In this scheme firstly original image is transformed from space domain to frequency domain using DWT to the original scale L(L=4) and then for better ensuring the invisibility of watermark psycho visual mask is added which is used to adjust the insertion force of watermark which is given by a parameter robustness alpha which is specified in the scheme. A watermark **W** is generated using pseudo-random binary sequence method then watermark **W** is encrypted using pseudo-random binary vector **P** to produce **W*** which is then embedded in the host image. Then inverse DWT is applied to obtain the marked image. This scheme is almost fragile against certain type of filters and retains the quality of image high but the robustness depended upon the force of watermark inserted or the value of alpha.

M. Rajawat et al. in [24], proposed a system which not only conceals large size of information within an image, but also limits the perceivable alteration that may happen in an image while processing it. In the proposed scheme original image **OI** and watermark image **WM** are resized to **N*N** and their RGB components are separated, then 2-level DWT is applied on both the images to divide the images into low frequency and high frequency components and then for embedding separated components of original image **OI** and watermark image **WM** are multiplied using scaling factor and new one image is obtained. After that inverse 2DWT is applied on the 2DWT transformed image to produce the watermarked original image. For tampering detection original image and watermarked image are used as reference images. Besides concealing large size of information and limits perceivable alteration it yields good PSNR value but at high level of DWT the illustration significant information is lost. Cropping and rotation attacks are not considered in this proposed work.

M. Moniruzzaman et al. in [25], suggested a scheme in which medical image is used as a host image and patient information is embedded in it as a binary watermark image without affecting the image quality. Firstly DWT is applied on host image to obtain four non-overlapping multi-resolution coefficient sets – LL, HL, LH and HH and then low frequency sub-band (LL) is divided into 3x3 non-overlapping blocks. The gray differences between centre and neighbour pixels are calculated taking centre pixel value as threshold and assigning them binary bits (**1** and **0**) accordingly. Logistic map is generated by applying XOR operation on obtained binary bits and then chaotic watermark is obtained by applying XOR operation on binary watermark image and generated logistic map. Chaotic watermark bits then embedded into the LL sub-band of host image by observing the neighbour pixels conditions. Finally inverse DWT is performed to obtained original watermarked image. The proposed method as shown by PSNR value and NC value, keeps a good quality of watermarked image and extracted watermark.

S. Bakhtiari et al. in [26], suggested an encryption technique using ECC (Elliptic Curve Cryptography) during and before JPEG compression. ECC is suitable in the environments where power consumption, storage and bandwidth are constrained. In the proposed method ECC is applied jointly with and independently of the compression algorithm. It is applied after transform encoding and quantization of image to achieve selective encryption and decryption and before compression in order to achieve perceptual encryption. In the proposed method two ECC based algorithm are presented: selective encryption of the quantised DCT coefficients and perceptual encryption based on selective bit-plane encryption. Advantage of this scheme is that it is fast and secure and it does not affect the compressed data but applied codec is required to modify if ECC is applied during compression.

P. Gupta in [27], proposed a method which used nested watermarking along with encryption for enhancing the security of the binary images. In this method a **Watermark1** is encrypted with key **E1** using XOR operation and this **Watermark1** is embedded in main **Watermak2** using key **W1**. Now **Watermark2** is encrypted with same method as of previous watermark using encryption key **E2**. Now Watermark2 is embedded in host image using key **W2**. This is blind watermarking technique and advantage of this method is high security due to encrypted watermark and more numbers of bits can be embedded but the nesting make the process complex and computation time may increased.

J. S. Bhalla et al. in [28], proposed a method of nested watermarking along with encryption using Blowfish Algorithm. Blowfish Algorithm is symmetric encryption algorithm and it is a block cipher that it divides the message into fixed length blocks during encryption and decryption and having variable-length key ranging from 32 bits to 448 bits. In this method first watermark is encrypted with Blowfish algorithm and embedded in second watermark which is main watermark. Now second watermark is again encrypted with same algorithm and embedded in host image using spatial domain technique (LSB). The advantage of this method is that it increases the embedding capacity of watermark and using Blowfish encryption algorithm increase the security and robustness of the watermark.

S. Kaur et al. in [29], proposed blind watermarking algorithm which is robust and based on both Modified Fast Haar Wavelet Transform (MFHWT) and Redundant Second Generation Wavelet Packet Transform (RSGWPT). In this proposed method MFHWT decomposes the original cover image until the size of sub-images is 4 times the watermark image then RSGWPT is applied to the last decomposition of MFHWT and for increasing the security pixels of watermark are distributed on all sub-images. Gray scale value of each pixel is calculated and divided into three parts A, B and C. The sub-images are further decomposed into 4 bands equal to the size of watermark and A, B and C are embedded into the rest of the bands leaving first one. Now watermark is embedded into the fine Scaled Frequency bands of the RSGWPT to guarantee its invisibility where minimum match occurs after comparing the coefficients of RSGWPT with parts of A,B and C. Finally inverse of MFHWT and RSGWPT is performed to obtain the original watermarked image. Proposed scheme is robust against Salt and Pepper, Poisson and Speckle noise, embedding and extraction of watermark is faster and it yields good values for PSNR and NC but the method is bit complex.

A. Al-Haj et al. in [30], proposed a scheme in which medical image is decomposed into two regions ROI (region of interest) and RONI (region of non interest). Three level DWT is applied on RONI part and three watermarks, Authentication Watermark, Integrity Watermark and Tamper Localization Watermark, later two are generated from ROI part as a hash value and CRC-16 value. In this method firstly DWT is applied on RONI part to decompose the image into 4 sub-bands LL1, HL1, LH1 and HH1, again 2-DWT is applied on HL1 sub-band to further decomposes the HL1 band into 4 sub-bands bands LL2, HL2, LH2 and HH2,, after this again, 3-DWT is applied on HL2 sub-band to decompose it further into 4 sub-bands LL3, HL3, LH3 and HH3. Now patient information is embedded as a watermark in HL3 sub-band and inverse DWT is applied then Integrity Watermark is embedded into the HL2 sub-band and again inverse DWT is applied, finally Tamper Localization watermark is embedded into the HL1 sub-band and inverse DWT is applied and ROI and RONI parts are combined and original watermarked image is obtained. Proposed method provides high imperceptibility and security.

M. Ouslim et al. in [31], proposed a biometric system based on Vector quantization watermarking based on LBG algorithm (Linde, Buzo and Gray) or generalized Lloyd algorithm (GLA) used to hide iris information of eye image in fingerprint image to ensure the security of both images. Two databases are used in this method of fingerprint images and iris images. In this method firstly XOR operation is done on 2 binary Iris images to get the permutated version of watermark and fingerprint image is decomposes into 2x2 blocks to obtained quantified vectors and then using LBG algorithm and current dictionary to get quantized fingerprint image **X'**. Then binary polarity matrix **P** is obtained by calculating the variance of indices of quantization vectors taking some threshold value. Finally XOR operation is performed of binary polarity matrix **P** with permutated watermark to obtain the Key which is transmitted to the receiver side along with quantized fingerprint image **X'.** Security is enhanced in this technique and it is robust against various attacks.

K. Anusree et al. in [32], proposed a scheme for multiple secret sharing for colour images using VC, Halftoning along with Digital watermarking. In this scheme two shares are generated. Original image is decomposed into **C, M and Y** channels then halftoning is applied on individual channel and then encoding by number of sub-pixels is done using (2,2) VCS which is known as pixel expansion. (2, 2)VCS generates two shares, each for C, M and Y channels for each image and then shares are embedded on to two separate images called sheets. Share1 of all images will be watermarked on sheet1 and share2 of all images on sheet2. Original image is only revealed if one has all the shares. XOR operation is done for decryption of VCS to combining the shares. Security is enhanced in this scheme using multiple shares but PSNR value is not upto the level of other methods and moreover there is a pixel expansion problem which arise the problem of storage.

Y. Han et al. in [33], proposed an algorithm to generate two shares based on VCS. One share is embedded into the DCT coefficients of blue components of colour image and other share is protected by copyright. In the proposed method two shares S1 and S2 are generated using (2, 2)VCS based on XOR algorithm. The blue component of colour image is separated and decomposed into non-overlapping 8x8 blocks and DCT is applied on each block. Now S1 is embedded into these blocks and inverse DCT is applied to obtain the original colour watermarked image. S2 is protected by copyright which is applicable to recovery the watermark. This scheme yield good NC value but PSNR value is not upto the level of other schemes.

S. Ghosh et al. in [34], proposed dual purpose spatial domain robust algorithm for cryptography and digital watermarking and key generation is done using Extended Hamming code and making the code self-correcting. LSB of the cover image is extracted and processed with Extended Hamming Code and then messages pixels are embedded in case of watermarking and for encryption key pixels are converted into 8-bit binary value and then LSB of second bit plane is extracted and XOR with message pixel value and then result of this and LSB of second bit plane is coded in 4-bit codes using Extended Hamming code. This method has high degree of imperceptibility and robustness but it uses spatial domain rather than frequency domain.

S. Kumar et al. in [35], proposed a method for authentication and copyright protection of digital image. In this method firstly the cover image **CI** is divided into 64 blocks and entropy of each block is calculated. The watermark image **WI** is resized to the block size of **CI** and embedded into those blocks having highest entropy by using LSB insertion method. This method yield good PSNR and MSE value which verifies the perceptibility and robustness of watermark image but its performance is not measured against attacks.

M. Malonia at el. in [36], proposed a method of watermarking using arithmetic progression which gives higher perceptibility and robustness against various attacks. In this method firstly cover RGB image is converted into grayscale image of size 512x512 then 2-DWT is applied on it to obtained four sub-bands LL1, HL1, LH1 and HH1 of size 256x256. Then QR-code image is taken and converted into grayscale image and then into binary image of 48x48 and it is taken as watermark image which is resized to 1x2304 and then into 3x768. Calculate the average of each sub-bands i.e. HL1, LH1 and HH1. Smallest average sub-band is to be embedded first then others having higher average. 1x768 elements of the watermark is taken and reshape into 256x3 elements. Now positions to insert watermark is located in sub-bands using an equation and then watermark is embedded using arithmetic progression technique. Finally inverse 2-DWT is performed to obtain the final watermarked image. This scheme has comparatively higher perceptibility and robustness against various attacks i.e. median filtering, JPEG compression, shearing, rotation, cropping and Gaussian low-pass filtering which is indicated by the PSNR value which is always above 50 db.

Table 3.1 Comparison between Related Works

Ref No.	Objective	Techniques Used	PSNR(dB)
[22]	To provide high level of security using combined features of steganography, cryptography and watermarking	Steganography, Visual Cryptography and Invisible Watermarking using LSB insertion technique	Up to 55.9110
[23]	To develop watermarking algorithm for gray scale image which emphasis on fragility rather than robustness for the authenticity of medical images using domain wavelet transform to gray level	DWT, encryption using pseudo random sequence and watermarking	Up to 38.2833
[24]	To enhance security of image using two level DWT on RGB components of original image and watermark image by combining watermarking and tamper detection method	Separation of RGB component, 2 level DWT and watermarking	Up to 61.62
[25]	For authenticity of patient's information DWT and chaotic watermark techniques are used which preserve the image quality	DWT and Chaotic Watermarking using Logistic map	Up to 49.58
[26]	To provide security to JPEG image using Elliptic Curve cryptography before and during image compression	Two ECC based encryption algorithm: selective encryption of the quantized DCT	Up to 17.70

		coefficients for during compression and perceptual encryption based on selective bit-plane encryption	
[27]	To provide image security by watermark nesting and encryption along with increasing the capacity of embedding data in the cover image	DWT, Nested Watermarking and Encryption	Not Reporte d
[28]	To provide a method of nested watermarking embedding and encryption for increasing embedding capacity and security	Watermarking and Encryption using blowfish algorithm	Not mention ed
[29]	To provide high quality watermarked image using Modified Fast Haar Wavelet Transform and Redundant Second Generation Wavelet Packet Transform and Blind watermarking	MFHWT decomposition and RSGWPT	Up to 55.18
[30]	To provide the secure transmission of medical images using hybrid techniques of encryption and watermarking	3 level DWT and 3 different Watermarks	Up to 98.1093
[31]	To enhance the security and robustness of digital images by merging the two biometric signatures using cryptography and watermarking	Vector Quantization Watermarking based on LBG algorithm and Chaotic Cryptography	Up to 10
[32]	To secure biometric data stored in	Extended Visual cryptography with half	Up to

	central databases	toning and watermarking	21.23
[33]	To increase the robustness and embedding capacity of watermarks	DCT, Visual Cryptography and Watermarking	Up to 42.008
[34]	To develop a blind watermarking algorithm in spatial domain which is self-correcting for dual purpose of watermarking and cryptography	Extended Hamming code and Watermarking	Up to 81.78
[35]	For authentication and copyright protection of the image	Block entropy and spatial domain LSB insertion watermarking technique	Up to 69.2377
[36]	To develop a watermarking technique which has higher image perceptibility and robustness against many attacks	DWT, watermarking using Arithmetic progression	Up to 79.8547

Every technique has its advantages and disadvantages in the context of some specific concerns. Some techniques have large data hiding capacity but some have more secure than others. Some techniques are more robust against various attacks but some are more fragile. Some techniques are quite complex but secure as well but some are very simple but security is not up to the level of other techniques. High degree of imperceptibility is achieved in some techniques and some have quite good PSNR values. The method in each work is different level of application. One method cannot be opted for other application in which it is not intended.

Discussion

This chapter mainly focuses on related works of various data hiding techniques and comparison among them. Each technique has its pros and cons and different technique is applicable for different domain of applications. The objective of some of the papers is to achieve two or more than two parameters i.e. Security, robustness, imperceptibility and capacity but some of the parameters are trade-off which mean only one can be achieved on the cost of other. So the data hiding techniques aiming to achieve maximum requirements i.e. security, robustness, capacity, imperceptibility etc. and which can be utilized in larger domain of applications is desired. In future there is scope to design application specific technique using combination of above mentioned techniques and further it can be accompanied by recent developed image transformation and data hiding techniques so that to make a better data hiding technique which is suitable for low bandwidth networks and low computational power machines having low battery capacity.

CHAPTER 4

METHODOLOGY

4.1 Problem Identification

With the digitization of the world most of the paper work shifted towards the digital document. Moreover the digital India campaign proliferated the digitization of documents in India as well. Digitization of media in confidential domain i.e. Banking, e-commerce, Army, e-health care etc. and in entertainment domain to educational domain or in more generic sense every field needs rigorous research to handle the issues arose in the succeeding of this campaign which are security of the digital documents in storage space and in transmission medium which aims to provide the authenticity, confidentiality and integrity of these documents. Because firstly being digitalization of everything and then its repository available on Internet made the possibility to access this media content by each and everyone connected to internet with good or bad intentions as well. Despite the best prevention efforts of the organizations and the law enforcement community, fraud and unauthorized access to media content continues to be a very popular and quite lucrative criminal activity. So in this work an effort to impose strong authentication to digital image is done. Besides providing security the techniques concerned with the digital content should be suitable in a sense that it could process the digital content within the time constraints.

4.2 Proposed Solution

With the proliferation of digital documents and the issues regarding them security of the digital content need to be upgraded time to time by embodying techniques which are suitable for current needs i.e. reducing time complexity, improving robustness, security, imperceptibility etc. In various data hiding techniques robustness, fragility, capacity, imperceptibility and security are interlinked which means that enhancing the one parameter will affect the other. This work is aimed to provide authentication security as a prime concern to the digital image along with keeping the other parameters' value in acceptable range. The solution to the above described problem is achieved by multiple watermarking by embedding three different watermarks, first is image watermark which is QR code image encoded with authentication information, second is text watermark which is original text string of same authentication information and this watermark is embedded redundantly three time in various positions of the cover image and lastly the third watermark is calculated CRC-16 code of authentication information which serve the purpose to authenticate the embedded watermark itself and to prove its integrity which will help proving the authentication of digital image or it owner's. The detail of this process is described in next section named under 'Methodology Used'.

4.3 Methodology Used

The proposed solution described above is achieved by using watermarking technique in frequency domain (i.e. multilevel Discrete Wavelet Transform) and combining it with CRC-16 code and MSB technique for proving the authentication of digital content.

4.3.1 Watermark Embedding Process

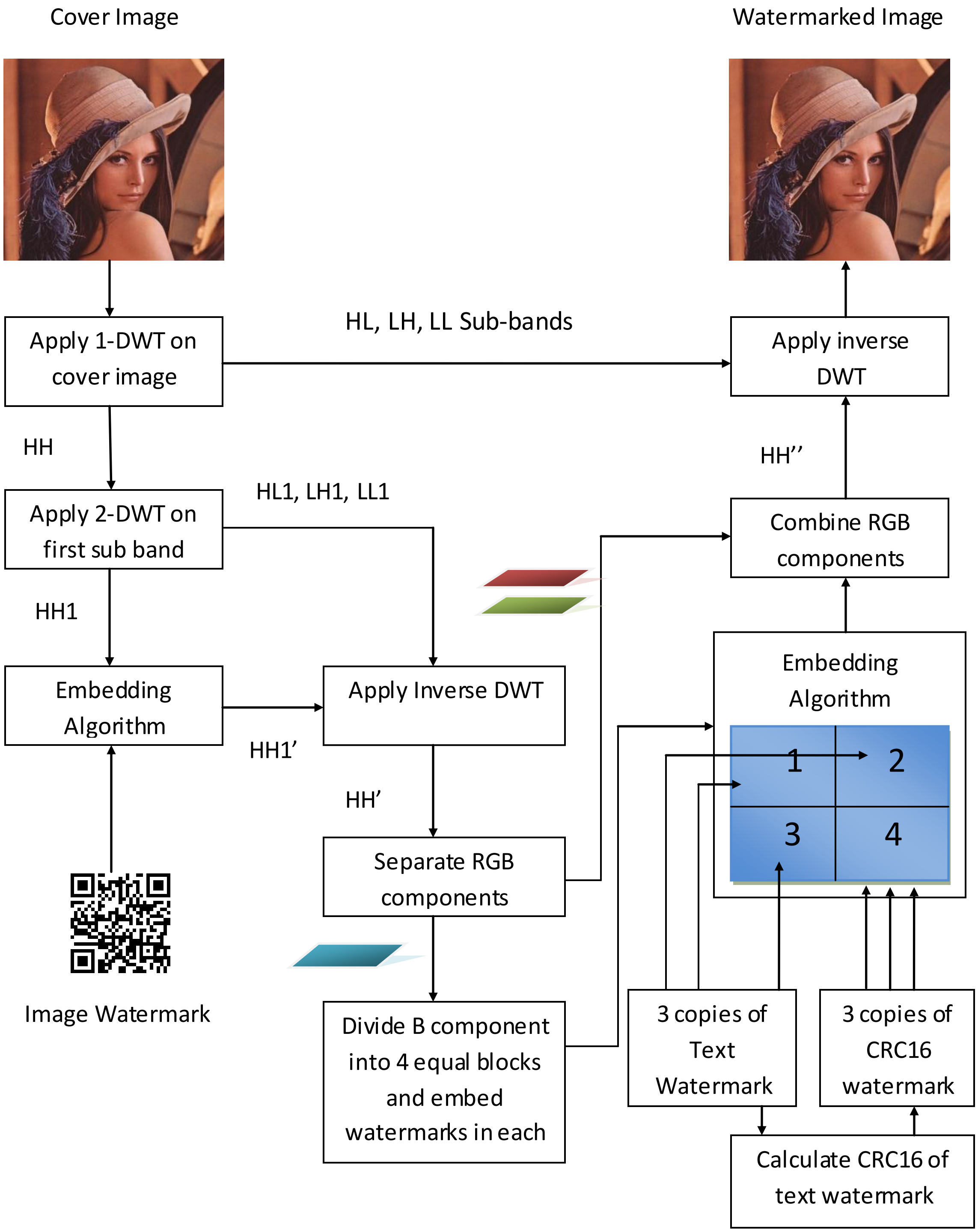


Figure 4.1 Watermark Embedding Process

4.3.2 Watermark Embedding Algorithm:

Step 1 *Separate RGB components of host cover image (X)*

Step 2 *Apply 1 level DWT on each color component of cover image*

Step 3 *Apply 2 level DWT on each color component of first sub-band(HH) which is obtained in step 2*

Step 4 *Combine the RGB components of first sub-band(HH1) obtained in step 3*

Step 5 *Embed first watermark (QR code Image of authentication Information) in HH1 sub-band obtained in step 4 using correlation-based technique*

Step 6 *Separate the RGB components of HH1 sub-band obtained in step 5 after embedding image watermark*

Step 7 *Apply inverse DWT on each color component of HH1 sub-band obtained in previous step*

Step 8 *Take the Blue (B) color component obtained in step 7 and divide it into 4 equal blocks*

Step 9 *Compute the CRC-16 of second watermark (text string of authentication information) which will be embedded (3 copies) as third watermark*

Step 10 *Take the 3 copies of second watermark (text string of authentication information) and embed them in first 3 blocks using 2-msb technique.*

Step 11 *Take third watermark (3 copies of CRC-16 of second watermark) obtained in step 9 and embed them into blocks obtained in step 8 using 1-msb technique.*

Step 12 *Combine this Blue(B) color component of HH1 sub-band obtained in step 11 with its Red(R) and Green(G) components*

Step 13 *Apply inverse DWT and ,* ***Watermarked Image obtained***

4.3.3 Watermark Extraction Process

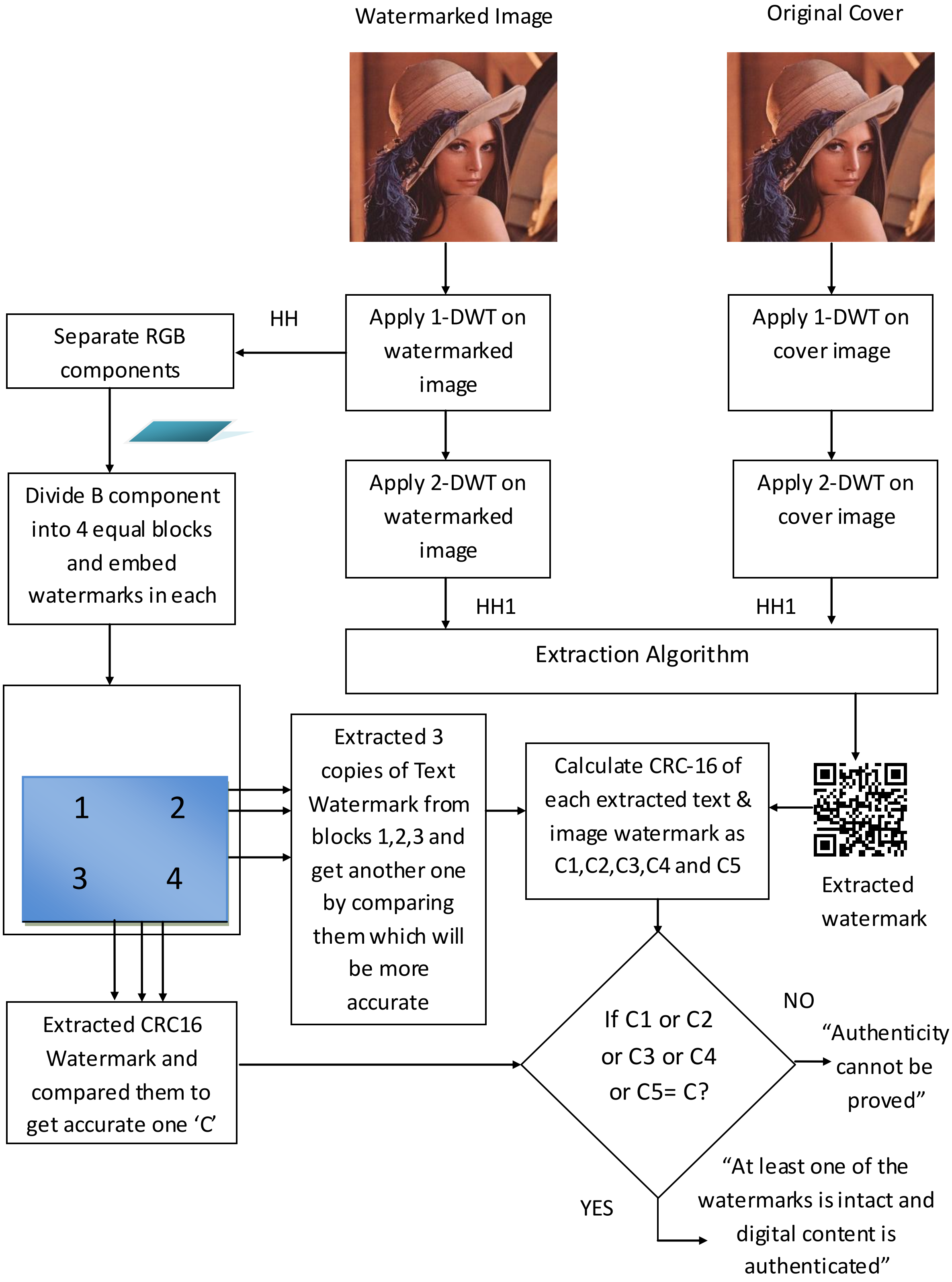

Watermarked Image
Original Cover
Apply 1-DWT on watermarked image
Apply 1-DWT on cover image
HH
Separate RGB components
Apply 2-DWT on watermarked image
Apply 2-DWT on cover image
Divide B component into 4 equal blocks and embed watermarks in each
HH1
HH1
Extraction Algorithm
1
2
3
4
Extracted 3 copies of Text Watermark from blocks 1,2,3 and get another one by comparing them which will be more accurate
Calculate CRC-16 of each extracted text & image watermark as C1,C2,C3,C4 and C5
Extracted watermark
Extracted CRC16 Watermark and compared them to get accurate one 'C'
If C1 or C2 or C3 or C4 or C5= C?
NO
"Authenticity cannot be proved"
YES
"At least one of the watermarks is intact and digital content is authenticated"

Figure 4.2 Watermark Extraction Process

4.3.4 Watermark Extraction Algorithm:

Step 1 *Separate RGB components of original cover image (X) and watermarked image (W)*

Step 2 *Apply 1 level DWT on each color component of cover image (X) and watermarked image (W)*

Step 3 *Take the Blue (B) component of first sub-band (HH) of watermarked image (W) for extraction of second and third watermark*

Step 4 *Apply 2 level DWT on each color component of the first sub-band of cover image (X) and watermarked image (W) each*

Step 5 *Combine the RGB components of first sub-band(HH1) of cover image (X) and watermarked image (W) each, obtained in step 4*

Step 6 *Extract the first watermark (QR encoded image) using the reverse technique used for embedding purpose and decode the embedded information in QR code*

Step 7 *Divide the Blue (B) component of first sub-band (HH) of watermarked image (W) obtained in step 3 into 4 equal blocks.*

Step 8 *Extract the copies of second watermark from 1,2 and 3 blocks and also get another copy of watermark by comparing individual bits of extracted watermarks to get more accurate one*

Step 9 *Extract the copies of third watermark from blocks which is embedded CRC-16 of second watermark and compare their bits to get more accurate CRC-16 code(C)*

Step 10 *Calculate the CRC-16 of all copies of second watermark obtained in step 8 as C1, C2, C3 and C4 respectively and also for the decoded QR code information obtained in step 6 as C5*

Step 11 *Compare all calculated CRC-16 values (C1,C2,C3,C4 and C5) obtained in step 10 with the third watermark (extracted CRC-16 value- C)*

Step 12 *If 'C1 equals to C' or 'C2 equals to C' or 'C3 equals to C' or 'C4 equals to C' or 'C5 equals to C' is true then at least one of the embedded watermarks is true and **authenticity of owner can be verified**, otherwise*

Authenticity cannot be proved

4.4 Performance Analysis Parameters

PSNR (Peak to Signal Ratio)

The imperceptibility of a watermarked image is measured using this factor. It tells similarity between the original image and watermarked image. It can also be used for the comparison of original watermark with the extracted watermark. It's expressed as quality measure. Higher imperceptibility and security concern with the higher PSNR value. Mean Square Error (MSE) value is first computed for its computation. PSNR can be represented as [5]:

$$\text{PSNR} = 10 \log_{10} \left[\frac{255^2}{\text{MSE}} \right]$$

It is the ratio between maximum possible power of a signal and the power of corrupt noise. Here 255 is maximum possible pixel value of the cover image. MSE is computed as:

$$\text{MSE} = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} (X(i,j) - X_w(i,j))^2}{N^2}$$

Where, N represents number of rows and columns (here considered same value), X(i,j) is the original image pixel value and Xw (i,j) is the watermarked image pixel value.

Normalized Cross Correlation

Normalized Cross Correlation is used to measure what is the similarity between the cover image and the watermarked image as well as original watermark and the watermark which is recovered. Higher value of NCC shows result in better technique. It is calculated by the formula [5]:

$$\text{NCC} = \frac{\sum i \sum j \,[\, I(i,j) - I_w(i,j) \,]}{\sum i \sum j \,[\, I(i,j) + I_w(i,j) \,]}$$

Where, I(i,j) is the original image pixel value and Iw (i,j) is the watermarked image pixel value.

Peak Signal to noise Ratio and Normalized Cross Correlation are trade-offs over the term gain factor. If gain factor is to kept high PSNR value will be lower down but NCC value yield good strength and vice-versa in case if we kept gain factor value high.

Table 4.1 PSNR Vs NCC over gain factor

Parameter	**Gain factor value if 'Low'**	**Gain factor value if 'High'**
PSNR	High	Low
NCC	Low	High

CHAPTER 5

IMPLEMENTATION AND RESULTS

5.1 Tool Used – MATLAB R2013a

MATLAB (**mat**rix **lab**oratory) licensed under proprietary commercial software developed by Mathworks and it is multi-paradigm environment like functional, procedural, object-oriented, array etc. It is a fourth generation programming language. It provides interactive environment for numerical computation, visualization and programming. It is widely used for image processing as it concerns with matrix manipulation, but it have also wide range of usages in different domain for different purposes.

Features of MATLAB

Matrix manipulation
Function plotting
Algorithm implementation
User interfaces creation
Creating models and application
Interfacing with other languages' programs including C++, C, Fortan etc

Syntax and basic MATLAB operations and functions

Assignments

```
A=B
A=B+C
A=B+C*D
```

Important commands

```
clear all;
close all;
workspace;
clc;
```

Vectors

```
%Row vector
A=[2  4  5  6  8]
%Column vector
A=[2;  3;  5;  6;  8]
```

Matrix

```
zeros(n,m) – create an nxm matrix of zeros
ones(n,m) – create an nxm matrix of ones
eye(n,m) – create an nxm identity matrix
rand(n,m) – create an nxm matrix having elements between 0 and 1
% adding two matrices
X=[7, 5; 1, 2]
Y=[1, 2; 2, 3]
Z=X+Y
%For displaying result
disp(Z);
%For diagnol element of matrix
diag(Z)
```

Images

Supported Image Formats

BMP, GIF, JPEG, HDF, PCX, PNG, TIFF, XWD

Bit Depth

Unit8, unit16 or double

Basic functions related to images

```
A=imread('path')
imshow(A);
B=rgb2gray(A)
imwrite(B, 'location path')
Red_component= A( : : 1)
Green_component= A( : : 2)
Blue_component= A( : : 3)
```

Colon notation

```
%for loop using colon
%init : incremental : terminator
I=1 : 2 :10
%for accessing elements corresponding to 1 and 2 row and 2 and 3
%coloum of matrix Z
Z(1 : 2,2 : 3)
```

Plotting

```
%Plotting on x and y coordinates
plot(x, y), xlabel('time'), ylabel('velocity'), title('acceleration')
```

```
%Plotting subplots with title
figure();
subplot(1,2,1);
imshow(A);
title('Image A','FontSize', 22);
subplot(1,2,2);
imshow(B);
title('Image B','FontSize', 22);
```

5.2 Dataset Used

For the above methodology described in chapter 4 below is the dataset which I have used for the purpose of implementation. In the below Table 5.2.1 under the section of 'Cover Images used in the project' there are three images along with their sources from where these obtained, which are utilized in this project as a host images and watermarks are embedded in these images. Various watermarks used in this project are mentioned below in Table 5.2.2. The three watermarks used in this project are, one is text watermark which is 50 characters long text string having authentication information shown as 'Second watermark' in below Table 5.2.2. Another is image watermark which is encoded QR code of same authentication information which is embedded as text watermark. The third watermark is computed CRC-16 code of authentication information embedded as a 'Third watermark' shown in table below and it serve the purpose to authenticate the intactness of extracted watermarks. The possibility of false positive rate is extremely low.

Table 5.1 Cover images used in the project

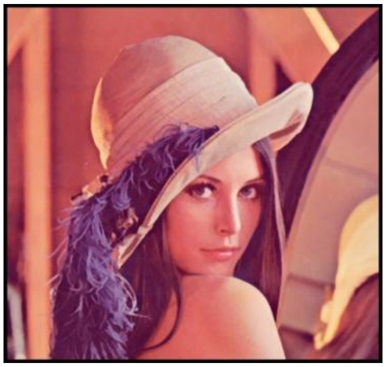
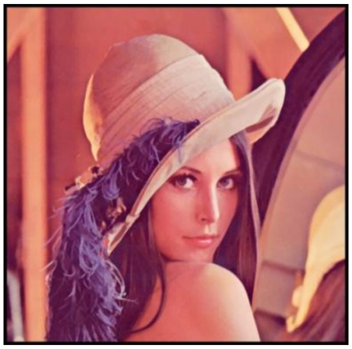
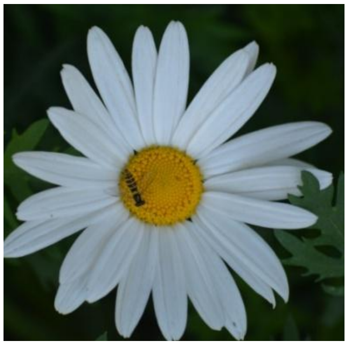
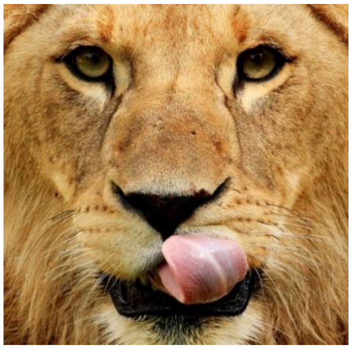
Cover Image	Source
	"standard test image widely used in the field of image processing since 1973"
	Click by DSLR (own work)
	"Portrait of a young lion (Panthera leo), taken at Tierpark Hellabrunn, Munich. By Martin Falbisoner" **(Labeled for non commercial reuse)**

Table 5.2 Watermarks used in the project

Data Set	**Cover Image (1024x1024)**	**First Watermark (128x128 QR code image of Second watermark)**	**Second Water-mark**	**Third Watermark**
Data Set 1			"Text String"	"CRC-16 of Text String"
Data Set 2			"Text String"	"CRC-16 of Text String"
Data Set 3			"Text String"	"CRC-16 of Text String"

5.3 Implementation and Results for Dataset 1

5.3.1 Implementation

In the below Figure 5.3.1, cover image and watermark image, also called payload image of dataset 1 is shown. Apart from payload image, 3 copies of 50 characters long text watermark and 3 copies of their corresponding CRC-16 code is also embedded. Redundancy is imparted to improve the robustness for text watermark.

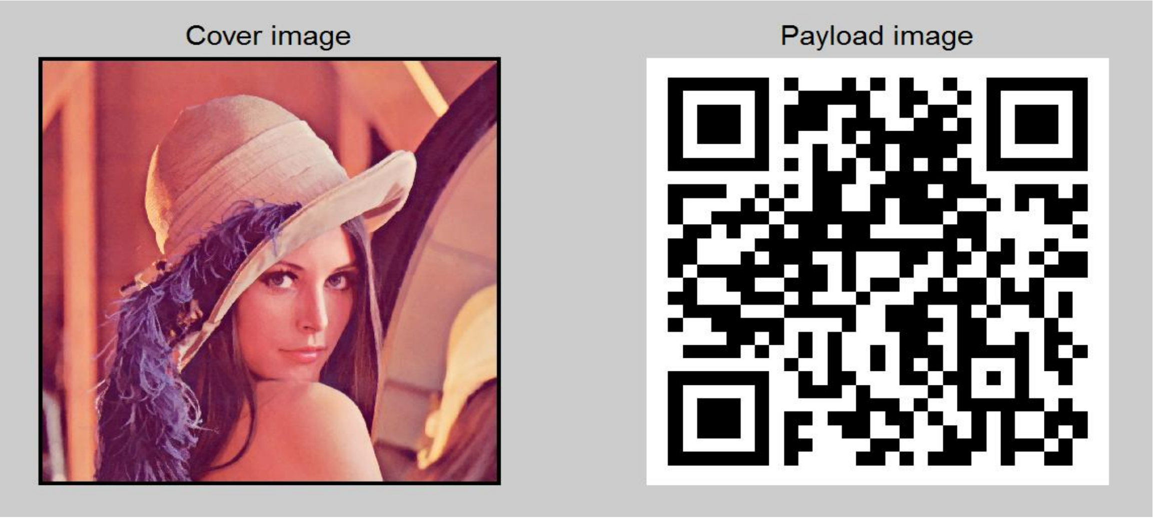


Figure 5.3.1 Dataset 1

For watermark embedding process, in Figure 5.3.2, 1 level DWT is applied to transform the image into frequency domain and separate its component into 4 sub-bands HH, HL, LH and LL respectively. HH being the first sub-band and contains maximum information. On HH sub-band again 2 level DWT is applied to divide it further into 4 sub-bands HH1, HL1, LH1 and LL1 which are shown in below Figure 5.3.3. HH1 again contains the maximum information of HH sub-band. In this HH1 sub-band 'image watermark' which QR code are embedded.

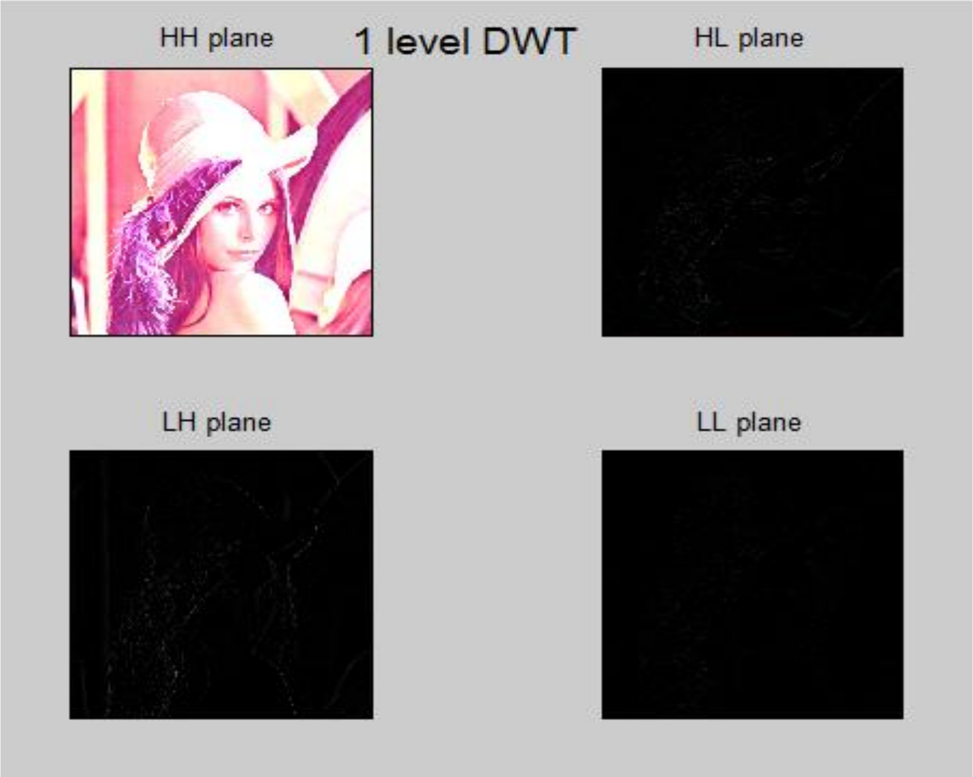


Figure 5.3.2 1 level DWT of cover image

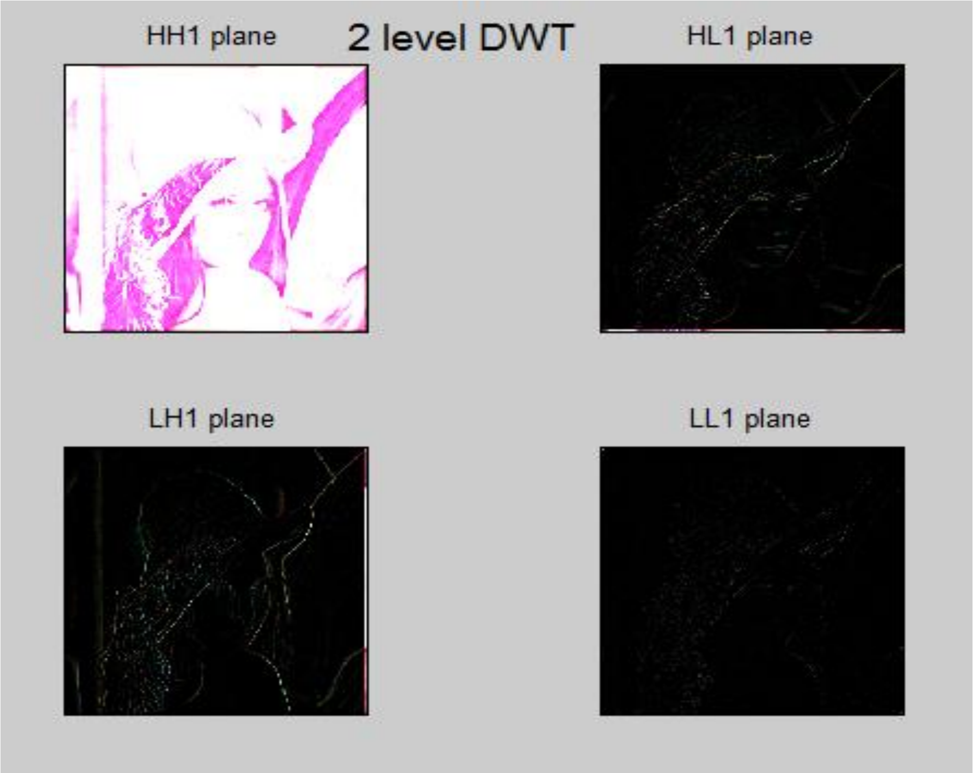


Figure 5.3.3 2 level DWT of cover image

In Figure 5.3.4, HH1 sub-band is shown before embedding image watermark and after embedding watermark and the perceptibility of watermark in even in HH1 sub-band is very low.

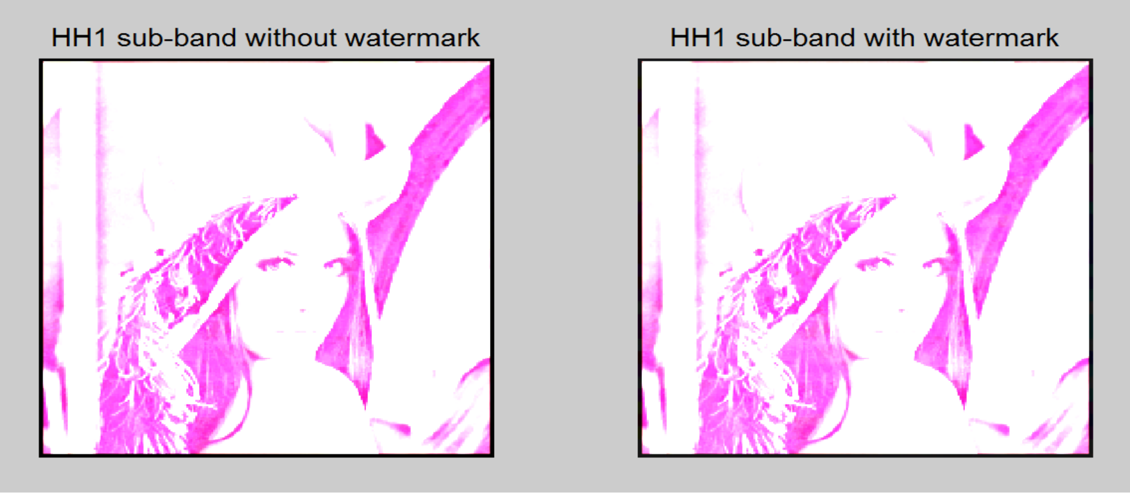


Figure 5.3.4 HH1 sub-band with or without image watermark

After embedding image watermark in HH1 sub-band inverse DWT is applied on HH sub-bands to obtained HH sub-band back again. After that blue colour component of HH sub-band is get separated and divided into four blocks and in first three blocks, 3 identical copies of text watermark which is shown as ‘Second Watermark’ in above table are embedded. And 3 identical copies of computed CRC-16 code of second watermark is also embedded in blue component of HH sub-band but in random locations. After embedding all three watermarks inverse DWT is performed to obtain the watermarked image which is shown below in the Figure 5.3.5.

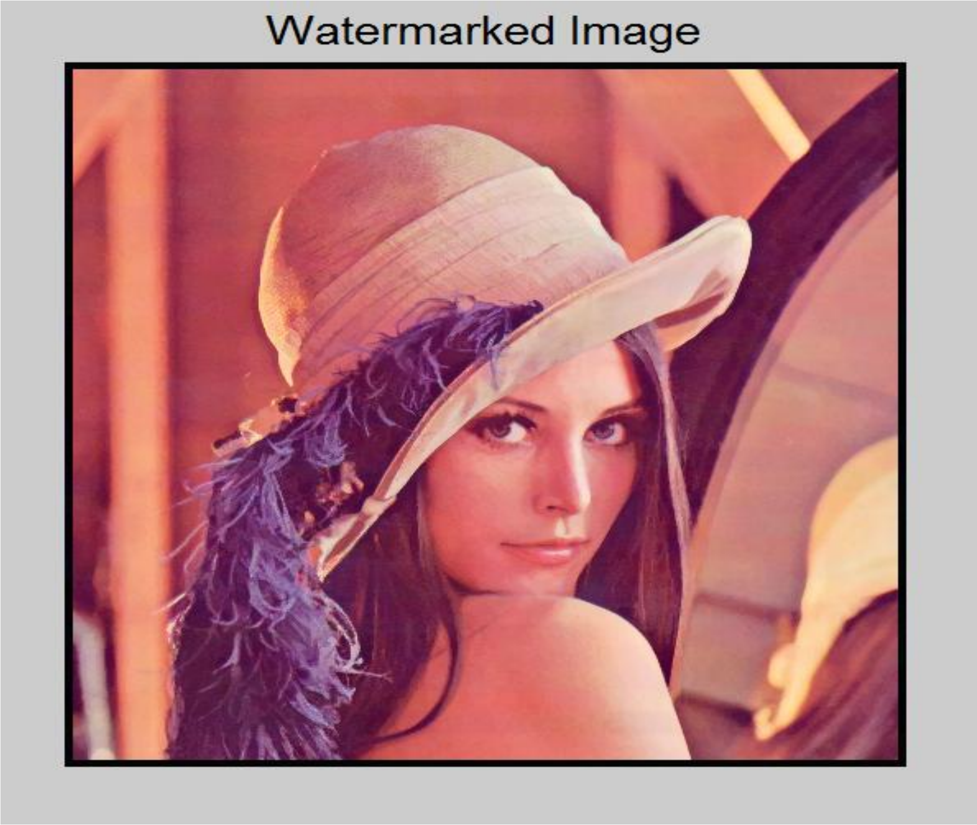


Figure 5.3.5 Watermarked Image

In watermark extraction process, the original cover image is used along with watermarked image to extract ‘image watermark’, but for text watermark there is no need of original cover image. Image watermark is extracted by transforming both images to 2 level DWT and to HH1 sub-bands of both the images are obtained which are being compared to extract ‘image watermark’. Text watermarks which are 3 identical copies of authentication information and 3 identical copies of its CRC-16 code are extracted from blue component of HH sub-band of watermarked image after applying 1 level DWT on watermarked image. Extracted CRC-16 code is compared with computed CRC-16 codes of all other watermarks after extraction and intactness of authentication information is proved accordingly. In below Figure 5.3.6 extracted image watermark and cover image left behind after watermark extraction is shown.

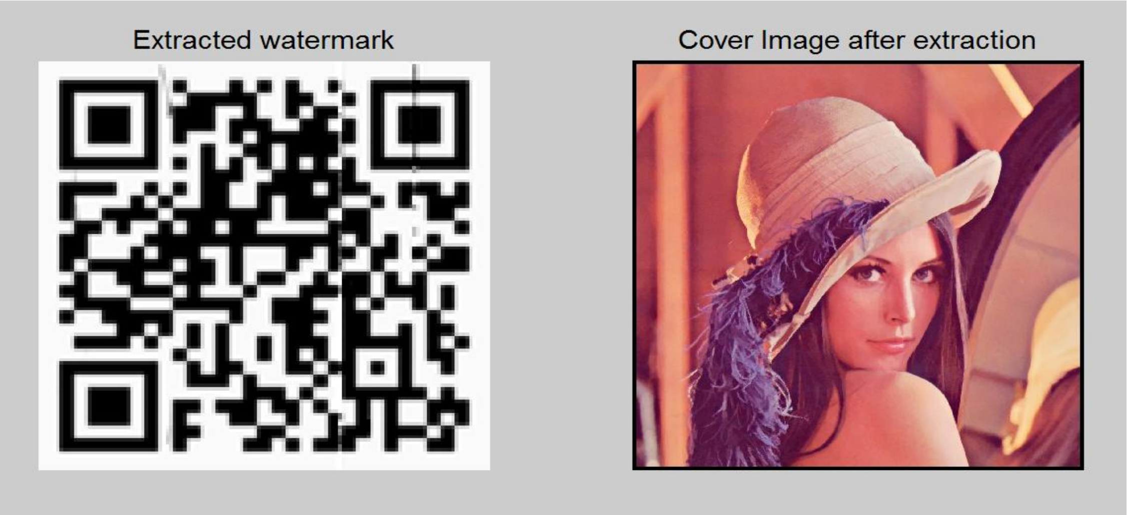


Figure 5.3.6 Extracted Image watermark

In the below Figure 5.3.7, watermarked image is shown exposed to various noise attacks such as ‘salt & pepper noise’, ‘speckle noise’, ‘Gaussian noise’ and ‘poisson noise’.

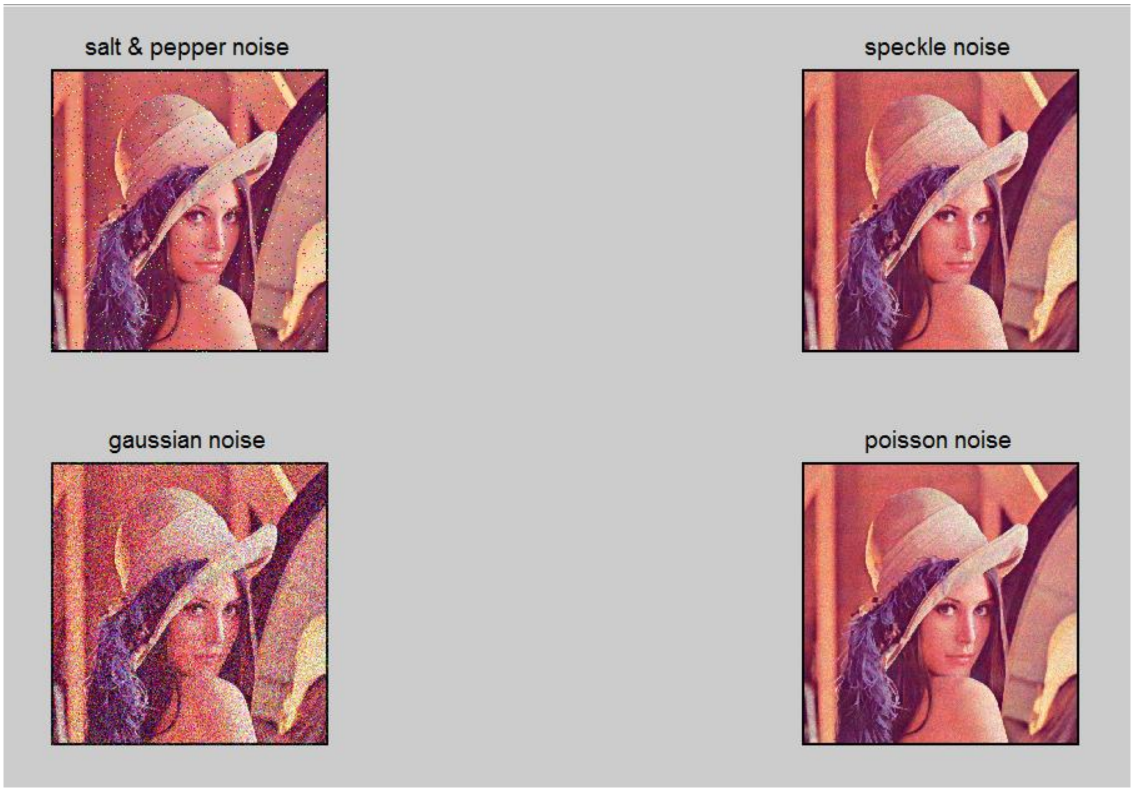


Figure 5.3.7 Watermarked Image exposed to various noise attacks

In the below Figure 5.3.8, watermarked image is shown exposed to cropping attacks labelled as Instance 1, Instance 2 and Instance 3 corresponding to these results are shown in next section.

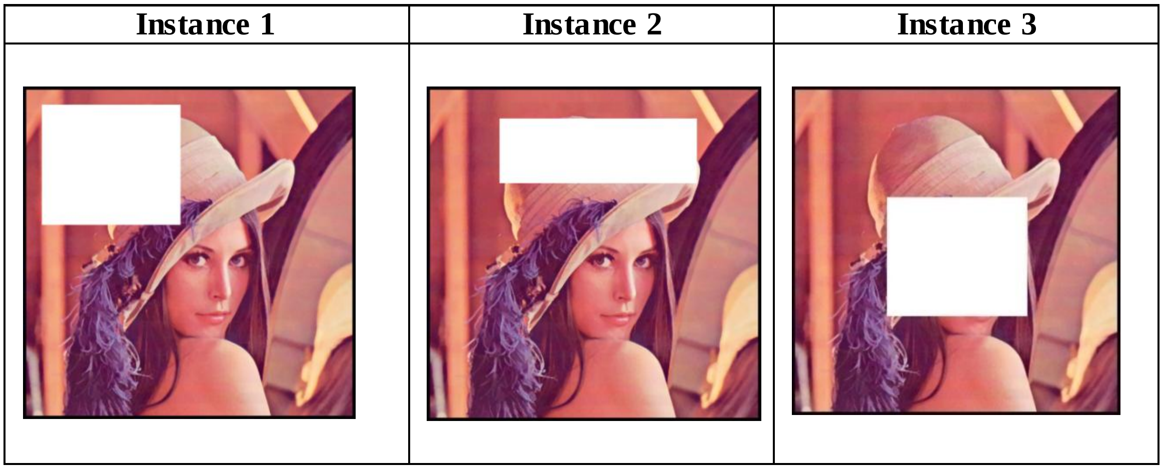


Figure 5.3.8 Watermarked Image exposed to cropping attacks

5.3.2 Results and discussion

Watermarked image is exposed to various attacks listed in below tables and then watermarks have been extracted. The status of watermarks like NC value of 'image watermark' , status of 'text watermark' if at least one watermark is intact then the value to corresponding cell is 'intact' otherwise 'corrupt' and finally information status is mentioned in the below tables weather information is decoded or not after being exposed the watermarked image to listed attacks. If information status is decoded that mean authentication information is decoded successfully and it will authenticate the digital content.

Table 5.3.1 shows the results corresponding to gain factor value = 0.1 for dataset 1.

Table 5.3.1 Results for dataset 1 corresponding to gain factor= 0.1

Attacks		NC value, text watermark and information extraction status corresponding to various attacks			
		Gain factor=0.1			
		PSNR	NC (for image watermark)	Text Watermark Status	Information Status
Without attack		34.5842	0.982	intact	decoded
salt and pepper	d=0.001	34.5842	0.9775	intact	decoded
	d=0.002	34.5842	0.9719	intact	decoded

noise	**d=0.003**	34.5842	0.9658	intact	decoded
speckle noise	**v=.001**	34.5842	0.9746	corrupt	decoded
	v=.002	34.5842	0.967	corrupt	decoded
	v=.003	34.5842	0.9573	corrupt	decoded
gaussian noise	**v=.001**	34.5842	0.96	corrupt	decoded
	v=.002	34.5842	0.9362	corrupt	decoded
	v=.003	34.5842	0.9135	corrupt	decoded
poisson		34.5842	0.9401	corrupt	decoded
croppin g	**Instance1**	34.5842	0.0298	intact	decoded
	Instance2	34.5842	-0.0118	intact	decoded
	Instance3	34.5842	0.0323	intact	decoded
Resizing	**90%**	34.5842	0.981	corrupt	decoded
	75%	34.5842	0.9813	corrupt	decoded

Table 5.3.2 shows the results corresponding to gain factor value = 0.09 for dataset 1.

Table 5.3.2 Results for dataset 1 corresponding to gain factor= 0.09

Attacks		**NC value, text watermark and information extraction status corresponding to various attacks**			
		Gain factor=0.09			
		PSNR	**NC (for image watermark)**	**Text Watermark Status**	**Information Status**
Without attack		35.5222	0.9837	intact	decoded
salt and pepper noise	**d=0.001**	35.5222	0.9788	intact	decoded
	d=0.002	35.5222	0.973	intact	decoded
	d=0.003	35.5222	0.9673	intact	decoded
speckle noise	**v=.001**	35.5222	0.9763	corrupt	decoded
	v=.002	35.5222	0.968	corrupt	decoded
	v=.003	35.5222	0.9593	corrupt	decoded
gaussian noise	**v=.001**	35.5222	0.9603	corrupt	decoded
	v=.002	35.5222	0.9364	corrupt	decoded
	v=.003	35.5222	0.912	corrupt	decoded
poisson		35.5222	0.9414	corrupt	decoded
cropping	**Instance1**	35.5222	0.0119	intact	decoded
	Instance2	35.5222	0.0024	intact	decoded
	Instance3	35.5222	0.0608	intact	decoded
resizing	**90%**	35.5222	0.9827	corrupt	decoded
	75%	35.5222	0.9832	corrupt	decoded

Table 5.3.3 shows the results corresponding to gain factor value = 0.08 for dataset 1.

Table 5.3.3 Results for dataset 1 corresponding to gain factor= 0.08

Attacks		**NC value, text watermark and information extraction status corresponding to various attacks**			
		Gain factor=0.08			
		PSNR	**NC (for image watermark)**	**Text Watermark Status**	**Information Status**
Without attack		36.4239	0.9825	intact	decoded
salt and pepper noise	**d=0.001**	36.4239	0.975	intact	decoded
	d=0.002	36.4239	0.9675	intact	decoded
	d=0.003	36.4239	0.9589	intact	decoded
speckle noise	**v=.001**	36.4239	0.9729	corrupt	decoded
	v=.002	36.4239	0.9627	corrupt	decoded
	v=.003	36.4239	0.9519	corrupt	decoded
gaussian noise	**v=.001**	36.4239	0.9496	corrupt	decoded
	v=.002	36.4239	0.9158	corrupt	decoded
	v=.003	36.4239	0.8833	corrupt	Not
poisson		36.4239	0.926	corrupt	Not
cropping	**Instance1**	36.4239	-0.0254	intact	decoded
	Instance2	36.4239	-0.0187	intact	decoded
	Instance3	36.4239	0.0145	intact	decoded
resizing	**90%**	36.4239	0.9814	corrupt	decoded
	75%	36.4239	0.9818	corrupt	decoded

Discussion

From the above tables it is clearly shown that this mythology given in this project work is quite robust against various attacks mentioned in above tables. In most of the attacked instances, information is decoded successfully and authenticity of author is proven. For noise attacks in most of cases text watermark get corrupted but information is decoded successfully from image watermark which is nothing but encoded QR code of text watermark same for the resizing attacks. But for cropping attack image watermark is get corrupted to large extent shown by low NC values; hence information is decoded using text watermarks. But some of the attacks corresponding to higher density like in Gaussian noise or poisson noise, information could not be decoded successfully that mean this method is robust up to some level of noise and it is meaningful in the sense that imposing large noise mean degrading the beauty of digital image which in some application attacker have no use of like for professional photographs. For improving more robustness more redundant watermarks can be embedded but it will result into low imperceptibly of watermarked image.

5.4 Implementation and Results for Dataset 2

5.4.1 Implementation

In the below Figure 5.4.1, cover image and watermark image, also called payload image of dataset 2 is shown. Apart from payload image, 3 copies of 50 characters long text watermark and 3 copies of their corresponding CRC-16 code is also embedded. Redundancy is imparted to improve the robustness for text watermark.

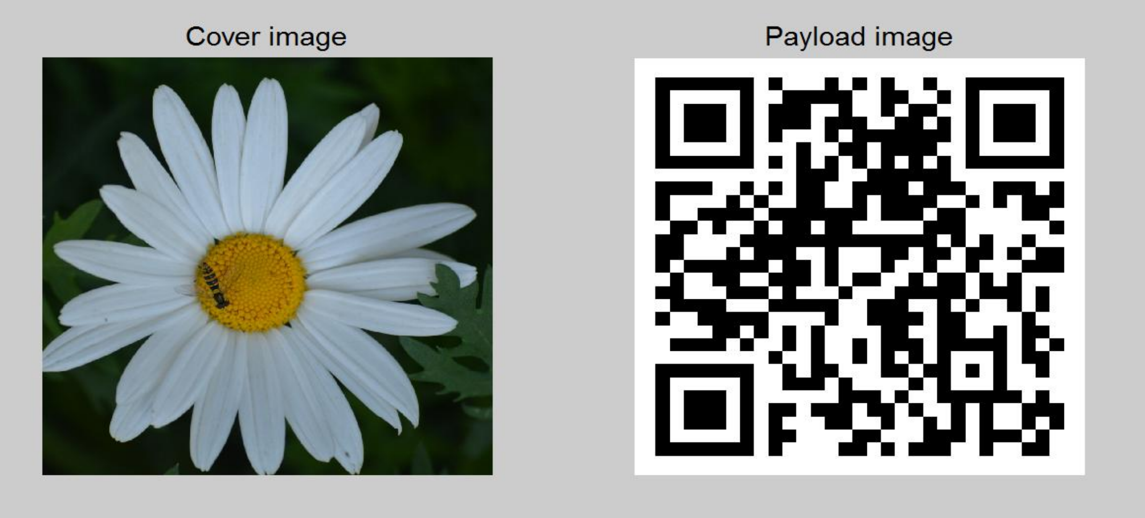


Figure 5.4.1 Dataset 2

For watermark embedding process, in Figure 5.4.2, 1 level DWT is applied to transform the image into frequency domain and separate its component into 4 sub-bands HH, HL, LH and LL respectively. HH being the first sub-band and contains maximum information. On HH sub-band again 2 level DWT is applied to divide it further into 4 sub-bands HH1, HL1, LH1 and LL1 which are shown in below Figure 5.4.3. HH1 again contains the maximum information of HH sub-band. In this HH1 sub-band 'image watermark' which QR code are embedded.

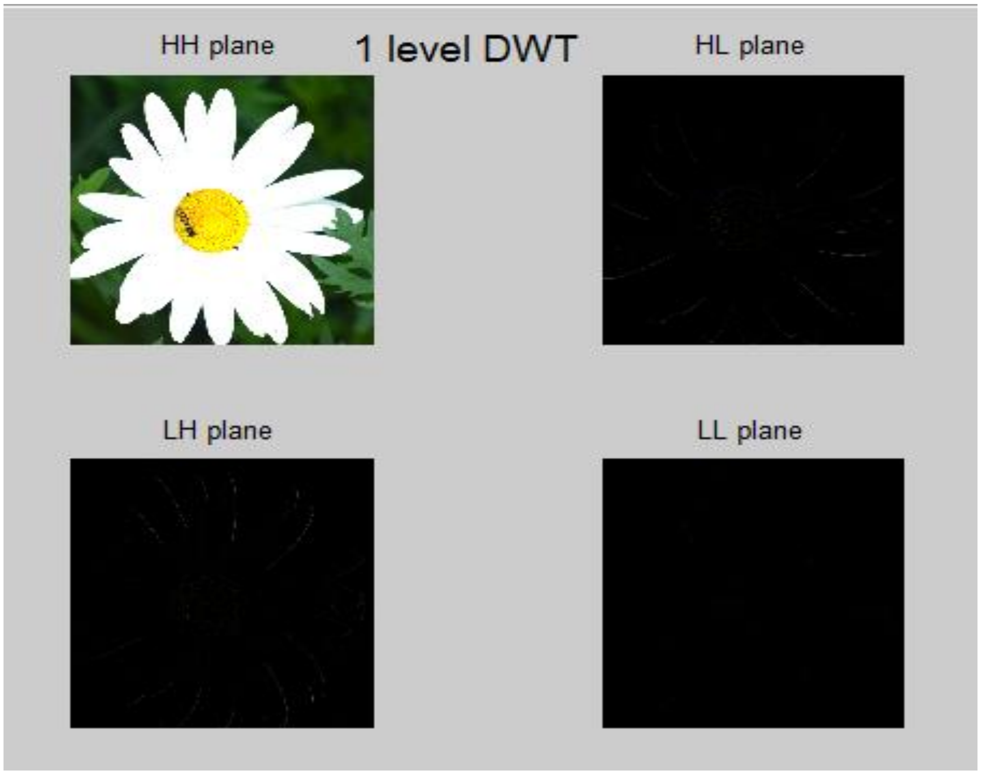


Figure 5.4.2 1 level DWT of cover image

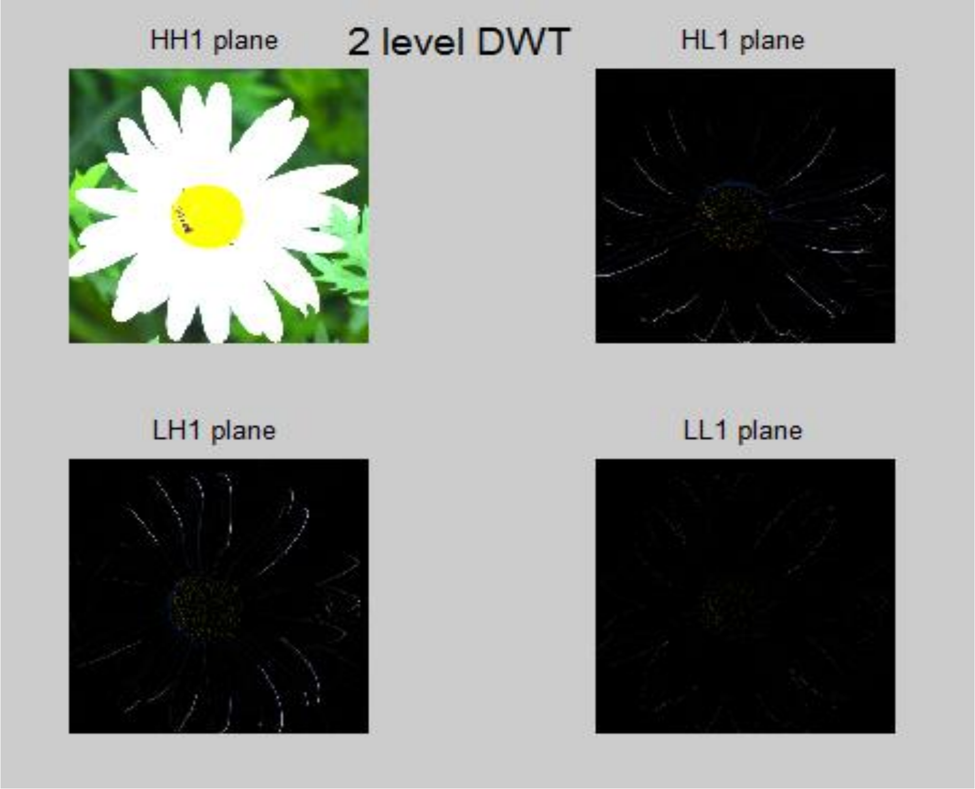


Figure 5.4.3 2 level DWT of cover image

In Figure 5.4.4, HH1 sub-band is shown before embedding image watermark and after embedding watermark and the perceptibility of watermark in even in HH1 sub-band is very low.

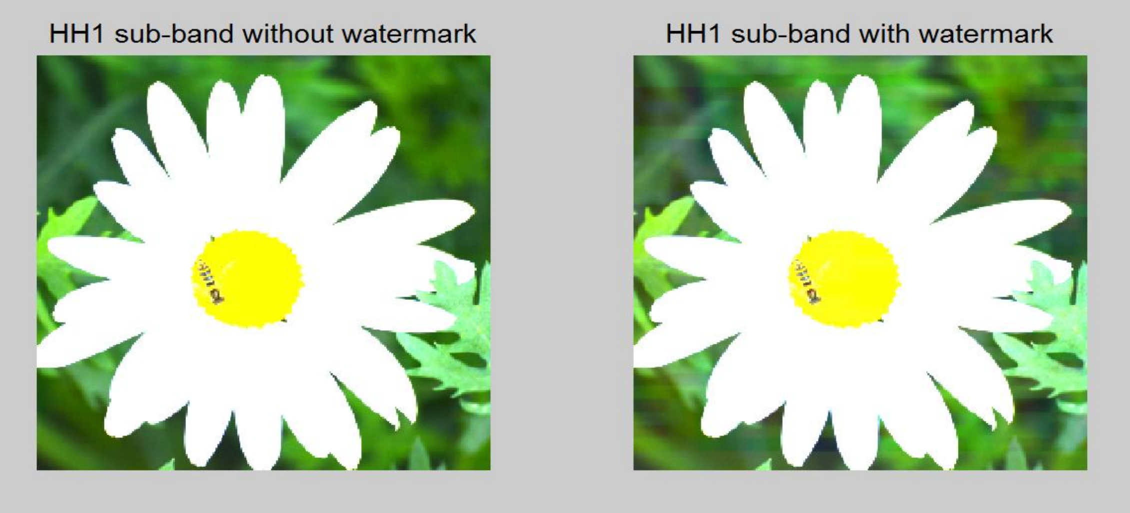


Figure 5.4.4 HH1 sub-band with or without image watermark

After embedding image watermark in HH1 sub-band inverse DWT is applied on HH sub-bands to obtained HH sub-band back again. After that blue colour component of HH sub-band is get separated and divided into four blocks and in first three blocks, 3 identical copies of text watermark which is shown as ‘Second Watermark’ in above table are embedded. And 3 identical copies of computed CRC-16 code of second watermark is also embedded in blue component of HH sub-band but in random locations. After embedding all three watermarks inverse DWT is performed to obtain the watermarked image which is shown below in the Figure 5.4.5.

Figure 5.4.5 Watermarked Image

In watermark extraction process, the original cover image is used along with watermarked image to extract ‘image watermark’, but for text watermark there is no need of original cover image. Image watermark is extracted by transforming both images to 2 level DWT and to HH1 sub-bands of both the images are obtained which are being compared to extract ‘image watermark’. Text watermarks which are 3 identical copies of authentication information and 3 identical copies of its CRC-16 code are extracted from blue component of HH sub-band of watermarked image after applying 1 level DWT on watermarked image. Extracted CRC-16 code is compared with computed CRC-16 codes of all other watermarks after extraction and intactness of authentication information is proved accordingly. In below Figure 5.4.6 extracted image watermark and cover image left behind after watermark extraction is shown.

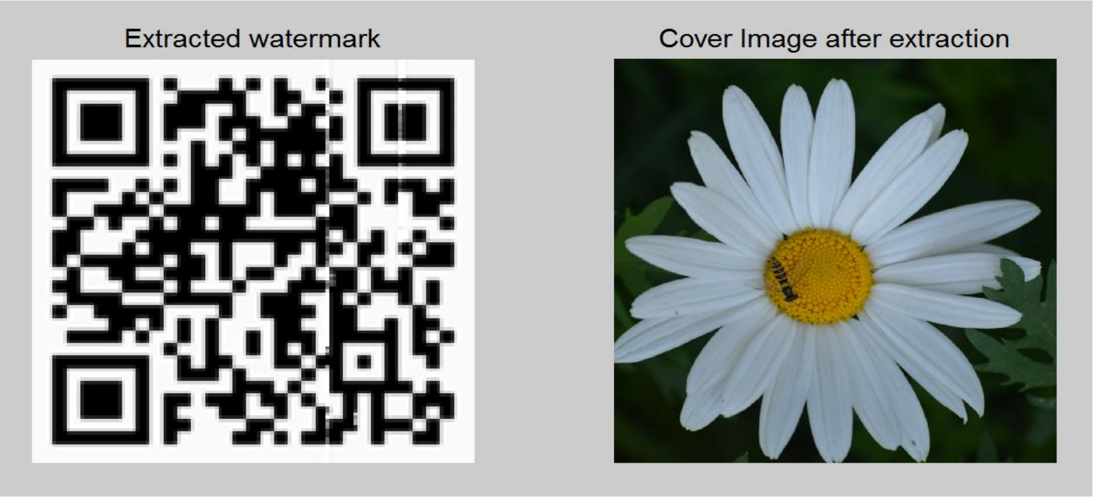


Figure 5.4.6 Extracted Image watermark

In the below Figure 5.3.7, watermarked image is shown exposed to various noise attacks such as ‘salt & pepper noise’, ‘speckle noise’, ‘Gaussian noise’ and ‘poisson noise’.

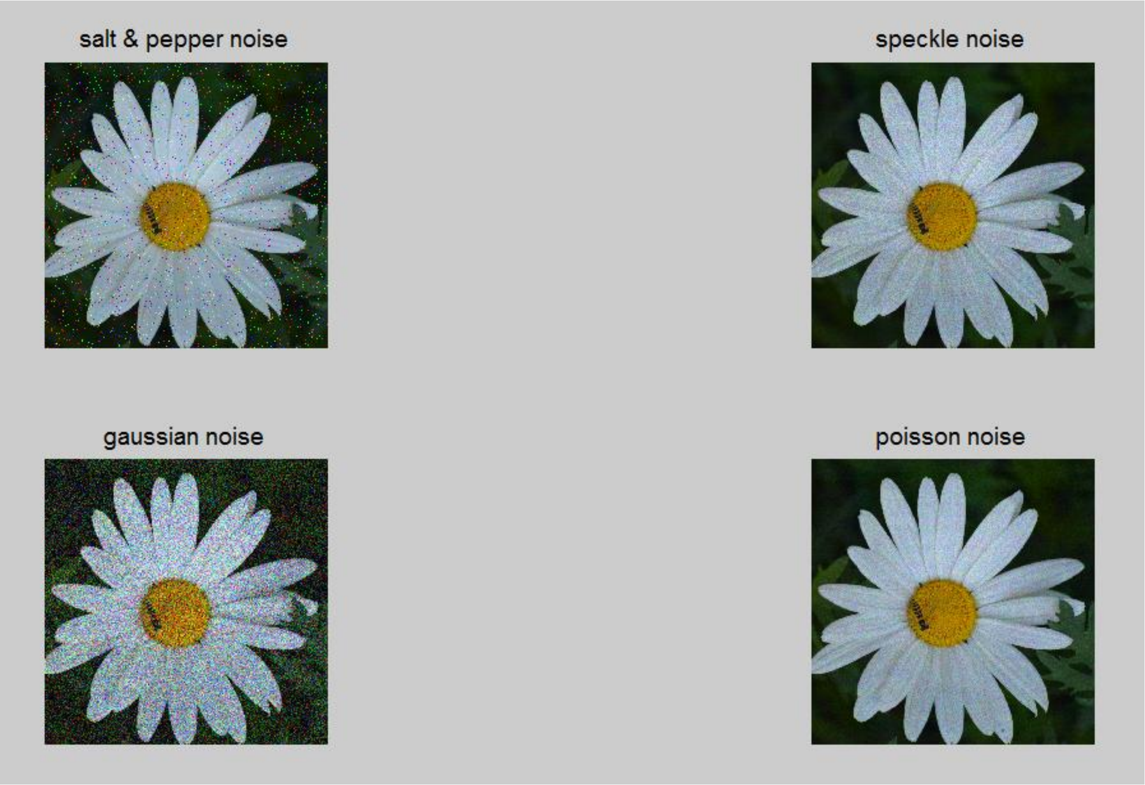


Figure 5.4.7 Watermarked Image exposed to various noise attacks

In the below Figure 5.4.8, watermarked image is shown exposed to cropping attacks labelled as Instance 1, Instance 2 and Instance 3 corresponding to these results are shown in next section.

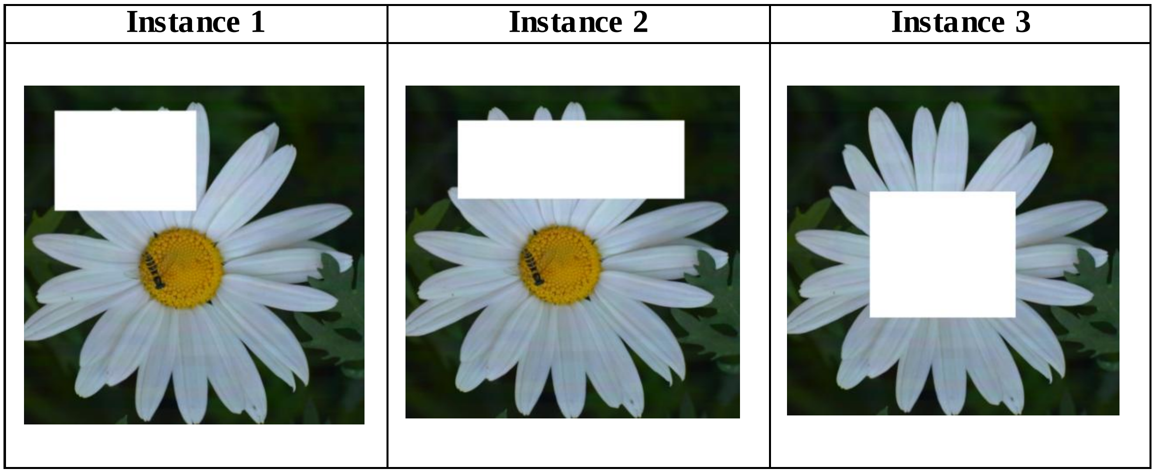


Figure 5.4.8 Watermarked Image exposed to cropping attacks

5.4.2 Results and discussion

Watermarked image is exposed to various attacks listed in below tables and then watermarks have been extracted. The status of watermarks like NC value of 'image watermark' , status of 'text watermark' if at least one watermark is intact then the value to corresponding cell is 'intact' otherwise 'corrupt' and finally information status is mentioned in the below tables weather information is decoded or not after being exposed the watermarked image to listed attacks. If information status is decoded that mean authentication information is decoded successfully and it will authenticate the digital content.

Table 5.4.1 shows the results corresponding to gain factor value = 0.1 for dataset 2.

Table 5.4.1 Results for dataset 2 corresponding to gain factor= 0.1

Attacks		NC value, text watermark and information extraction status corresponding to various attacks			
		Gain factor=0.1			
		PSNR	NC (for image watermark)	Text Watermark Status	Information Status
Without attack		34.5688	0.9826	intact	decoded
salt and	**d=0.001**	34.5688	0.9775	intact	decoded

pepper noise	**d=0.002**	34.5688	0.9719	intact	decoded
	d=0.003	34.5688	0.9658	intact	decoded
speckle noise	**v=.001**	34.5688	0.9793	intact	decoded
	v=.002	34.5688	0.9769	intact	decoded
	v=.003	34.5688	0.9731	intact	decoded
gaussian noise	**v=.0003**	34.5688	0.9769	intact	decoded
	v=.001	34.5688	0.9607	intact	decoded
	v=.002	34.5688	0.9346	corrupt	decoded
poisson		34.5688	0.9626	corrupt	decoded
cropping	**Instance1**	34.5688	0.0093	intact	decoded
	Instance2	34.5688	-0.0462	intact	decoded
	Instance3	34.5688	0.0336	intact	decoded
resizing	**90%**	34.5688	0.9816	corrupt	decoded
	75%	34.5688	0.9818	corrupt	decoded

Table 5.4.2 shows the results corresponding to gain factor value = 0.09 for dataset 2.

Table 5.4.2 Results for dataset 2 corresponding to gain factor= 0.09

Attacks		**NC value, text watermark and information extraction status corresponding to various attacks**			
		Gain factor=0.09			
		PSNR	**NC (for image watermark)**	**Text Watermark Status**	**Information Status**
Without attack		35.4953	0.984	intact	decoded
salt and pepper noise	**d=0.001**	35.4953	0.9782	intact	decoded
	d=0.002	35.4953	0.9723	intact	decoded
	d=0.003	35.4953	0.9658	intact	decoded
speckle noise	**v=.001**	35.4953	0.9807	intact	decoded
	v=.002	35.4953	0.9774	intact	decoded
	v=.003	35.4953	0.9744	intact	decoded
gaussian noise	**v=.0003**	35.4953	0.978	intact	decoded
	v=.001	35.4953	0.9617	intact	decoded
	v=.002	35.4953	0.9339	corrupt	decoded
poisson		35.4953	0.9635	corrupt	decoded
cropping	**Instance1**	35.4953	0.0168	intact	decoded
	Instance2	35.4953	-0.0348	intact	decoded
	Instance3	35.4953	0.0436	intact	decoded
resizing	**90%**	35.4953	0.983	corrupt	decoded
	75%	35.4953	0.9833	corrupt	decoded

Table 5.4.3 shows the results corresponding to gain factor value = 0.08 for dataset 2.

Table 5.4.3 Results for dataset 2 corresponding to gain factor= 0.08

Attacks		**NC value, text watermark and information extraction status corresponding to various attacks**			
		Gain factor=0.08			
		PSNR	**NC (for image watermark)**	**Text Watermark Status**	**Information Status**
Without attack		36.3922	0.9825	intact	decoded
salt and pepper noise	**d=0.001**	36.3922	0.9744	intact	decoded
	d=0.002	36.3922	0.9666	intact	decoded
	d=0.003	36.3922	0.9562	intact	decoded
speckle noise	**v=.001**	36.3922	0.9779	intact	decoded
	v=.002	36.3922	0.9731	intact	decoded
	v=.003	36.3922	0.9693	intact	decoded
gaussian noise	**v=.0003**	36.3922	0.9738	intact	decoded
	v=.001	36.3922	0.9497	intact	decoded
	v=.002	36.3922	0.9112	corrupt	Not
poisson		36.3922	0.9523	intact	decoded
cropping	**Instance1**	36.3922	0.0226	intact	decoded
	Instance2	36.3922	-0.0455	intact	decoded
	Instance3	36.3922	0.0293	intact	decoded
resizing	**90%**	36.3922	0.9814	corrupt	decoded
	75%	36.3922	0.9816	corrupt	decoded

Discussion

It is clearly shown in tables above that the mythology given in this project work is quite robust against various attacks mentioned in above tables. In most of the attacked instances, information is decoded successfully and authenticity of author is proven. For noise attacks in most of cases text watermark get corrupted but information is decoded successfully from image watermark which is nothing but encoded QR code of text watermark same for the resizing attacks. But for cropping attack image watermark is get corrupted to large extent shown by low NC values; hence information is decoded using text watermarks. But some of the attacks corresponding to higher density like in Gaussian noise, information could not be decoded successfully that mean this method is robust up to some level of noise. But it can cope up with other attacks mentioned above in the tables. For improving more robustness more redundant watermarks can be embedded but it will result into low imperceptibly of watermarked image.

5.5 Implementation and Results for Dataset 3

5.5.1 Implementation

In the below Figure 5.5.1, cover image and watermark image, also called payload image of dataset 1 is shown. Apart from payload image, 3 copies of 50 characters long text watermark and 3 copies of their corresponding CRC-16 code is also embedded. Redundancy is imparted to improve the robustness for text watermark.

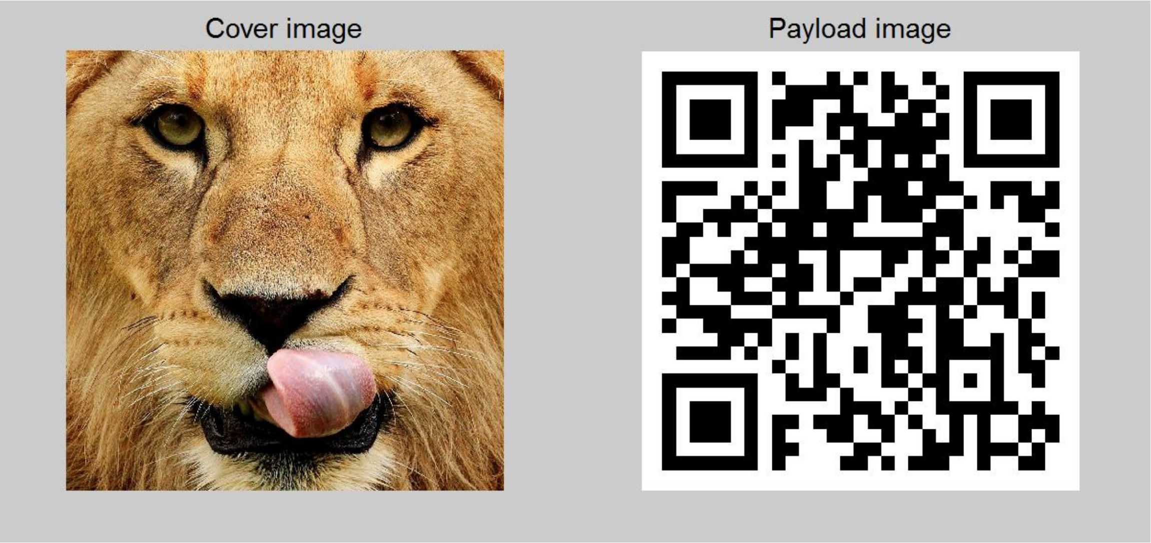


Figure 5.5.1 Dataset 3

For watermark embedding process, in Figure 5.5.2, 1 level DWT is applied to transform the image into frequency domain and separate its component into 4 sub-bands HH, HL, LH and LL respectively. HH being the first sub-band and contains maximum information. On HH sub-band again 2 level DWT is applied to divide it further into 4 sub-bands HH1, HL1, LH1 and LL1 which are shown in below Figure 5.5.3. HH1 again contains the maximum information of HH sub-band. In this HH1 sub-band 'image watermark' which QR code are embedded.

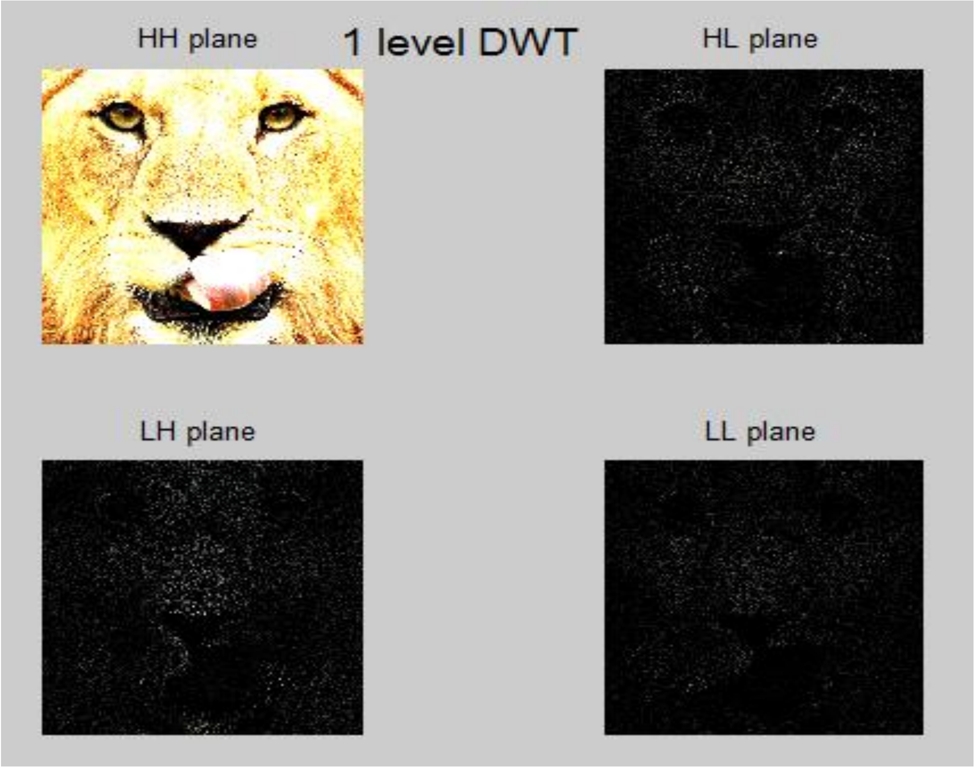


Figure 5.5.2 1 level DWT of cover image

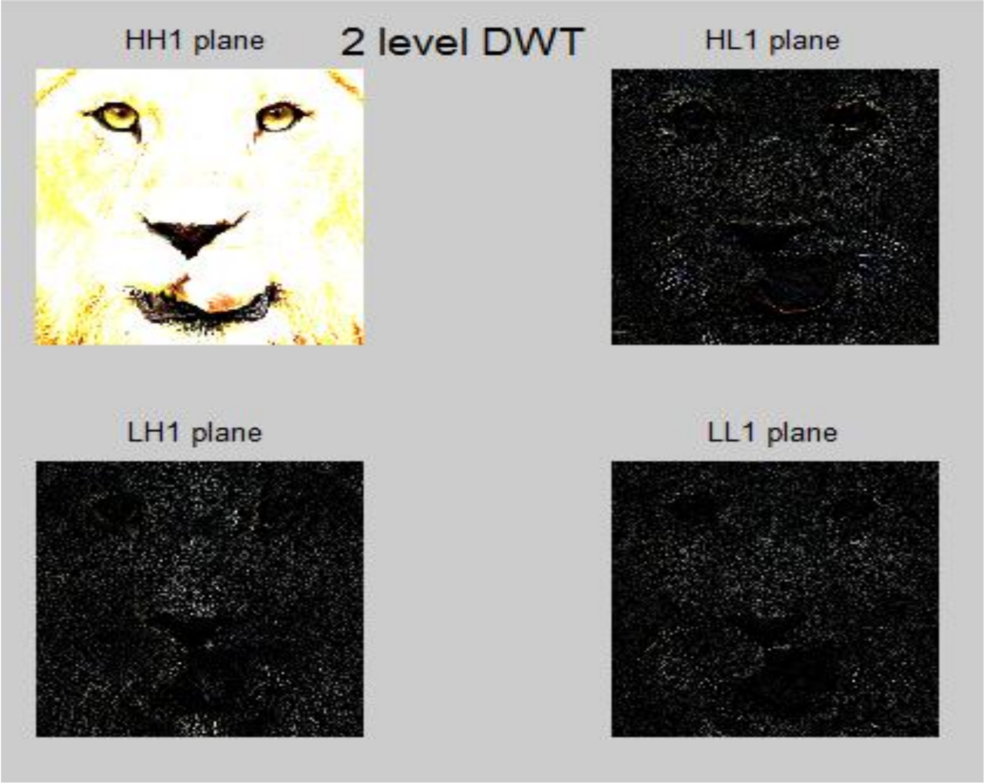


Figure 5.5.3 2 level DWT of cover image

In Figure 5.5.4, HH1 sub-band is shown before embedding image watermark and after embedding watermark and the perceptibility of watermark in even in HH1 sub-band is very low.

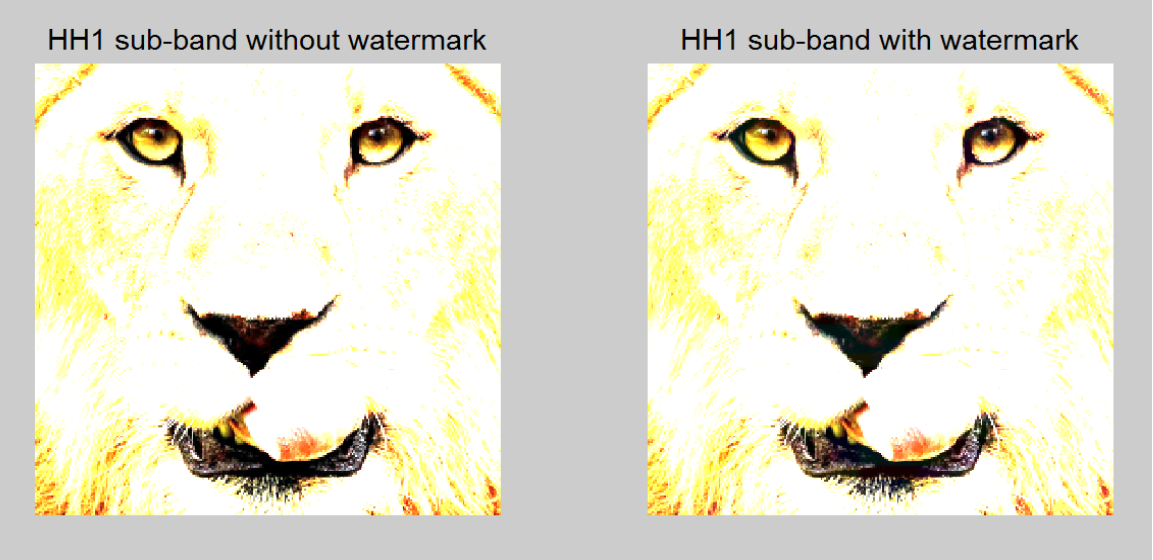


Figure 5.5.4 HH1 sub-band with or without image watermark

After embedding image watermark in HH1 sub-band inverse DWT is applied on HH sub-bands to obtained HH sub-band back again. After that blue colour component of HH sub-band is get separated and divided into four blocks and in first three blocks, 3 identical copies of text watermark which is shown as ‘Second Watermark’ in above table are embedded. And 3 identical copies of computed CRC-16 code of second watermark is also embedded in blue component of HH sub-band but in random locations. After embedding all three watermarks inverse DWT is performed to obtain the watermarked image which is shown below in the Figure 5.5.5.

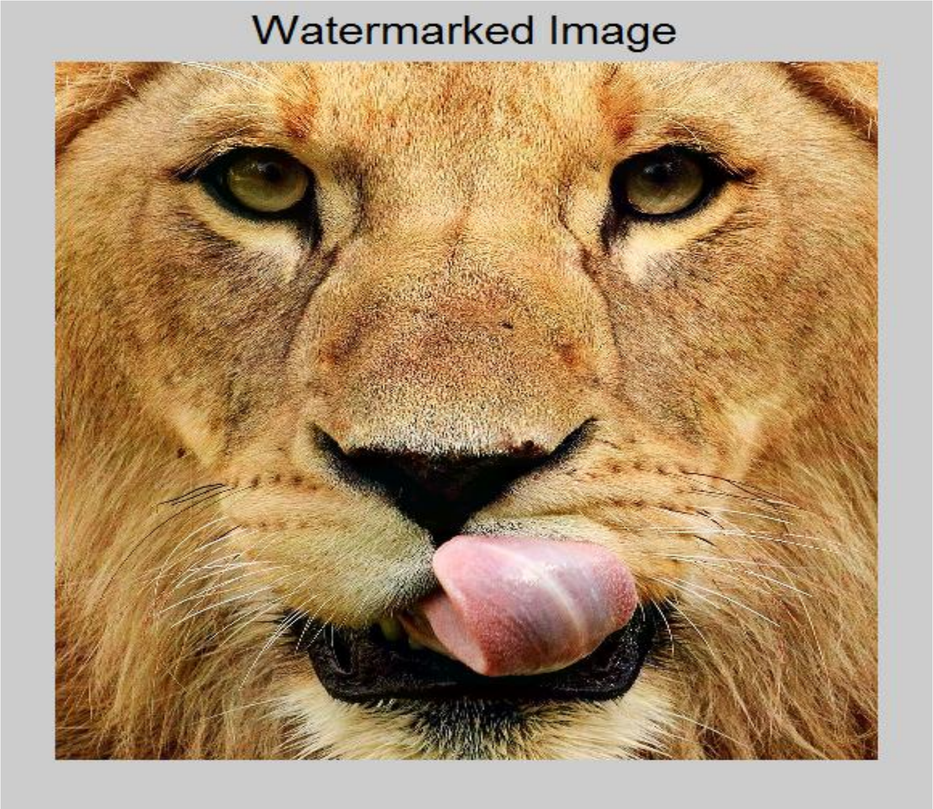


Figure 5.3.5 Watermarked Image

In watermark extraction process, the original cover image is used along with watermarked image to extract ‘image watermark’, but for text watermark there is no need of original cover image. Image watermark is extracted by transforming both images to 2 level DWT and to HH1 sub-bands of both the images are obtained which are being compared to extract ‘image watermark’. Text watermarks which are 3 identical copies of authentication information and 3 identical copies of its CRC-16 code are extracted from blue component of HH sub-band of watermarked image after applying 1 level DWT on watermarked image. Extracted CRC-16 code is compared with computed CRC-16 codes of all other watermarks after extraction and intactness of authentication information is proved accordingly. In below Figure 5.5.6 extracted image watermark and cover image left behind after watermark extraction is shown.

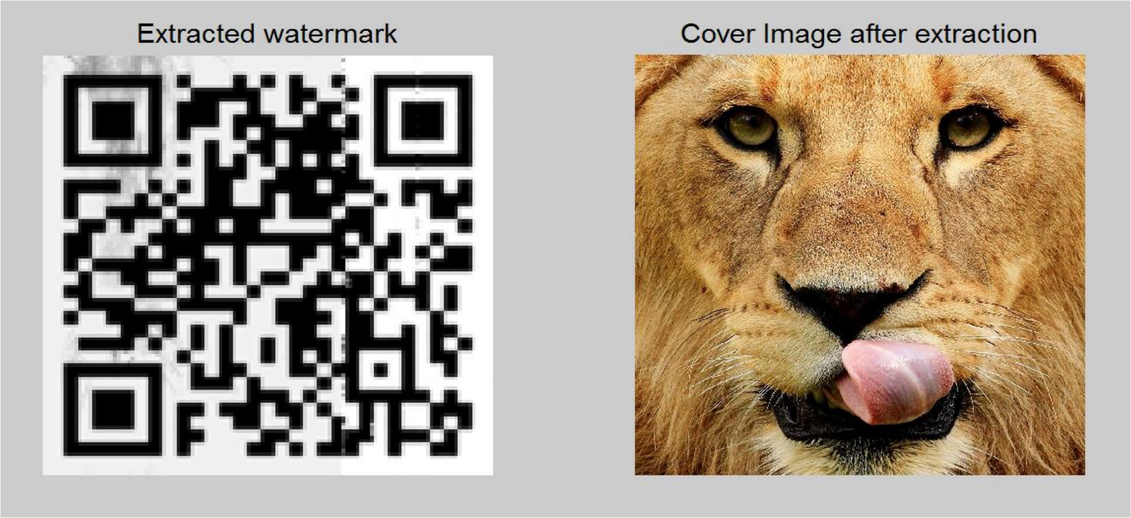


Figure 5.5.6 Extracted Image watermark

In the below Figure 5.3.7, watermarked image is shown exposed to various noise attacks such as ‘salt & pepper noise’, ‘speckle noise’, ‘Gaussian noise’ and ‘poisson noise’.

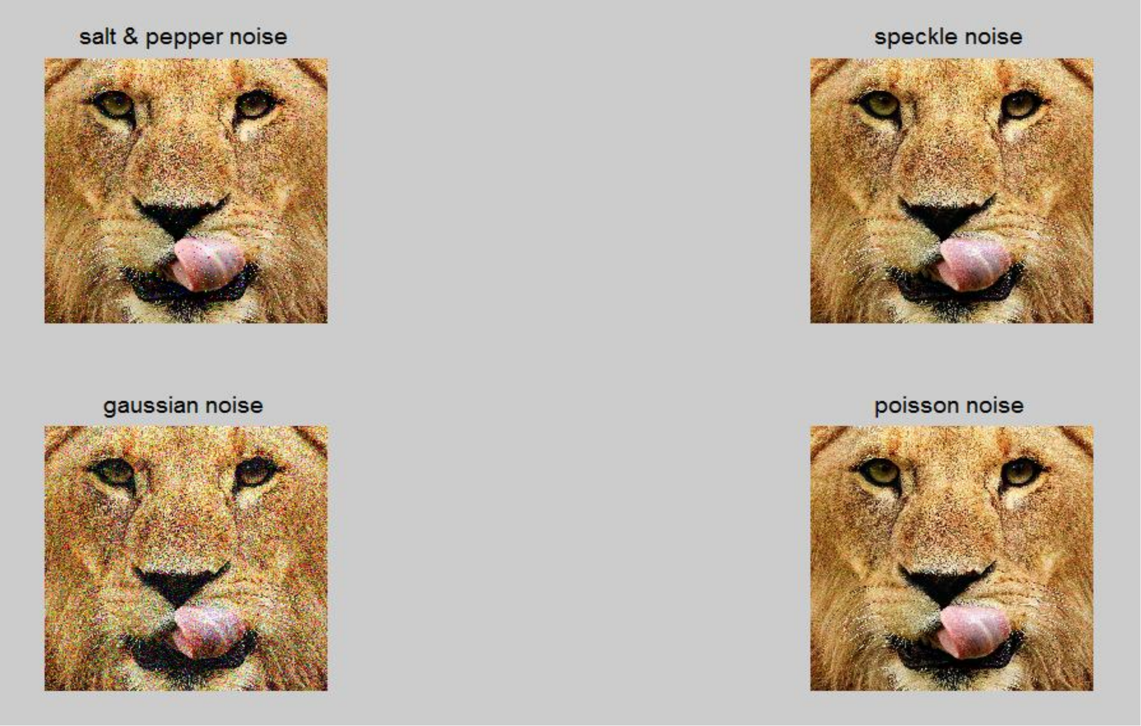


Figure 5.5.7 Watermarked Image exposed to various noise attacks

In the below Figure 5.5.8, watermarked image is shown exposed to cropping attacks labelled as Instance 1, Instance 2 and Instance 3 corresponding to these results are shown in next section.

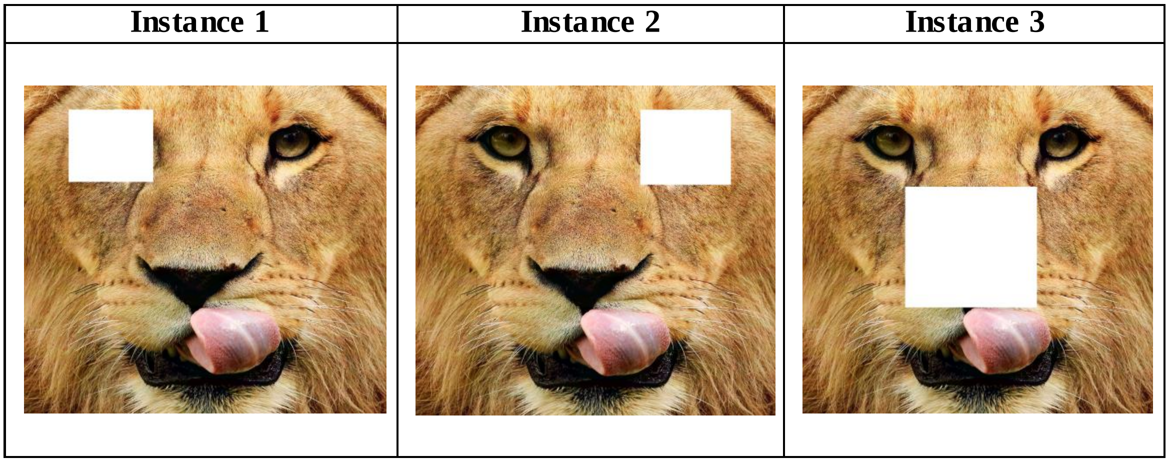

Instance 1 Instance 2 Instance 3

Figure 5.5.8 Watermarked Image exposed to cropping attacks

5.5.2 Results and discussion

Watermarked image is exposed to various attacks listed in below tables and then watermarks have been extracted. The status of watermarks like NC value of 'image watermark' , status of 'text watermark' if at least one watermark is intact then the value to corresponding cell is 'intact' otherwise 'corrupt' and finally information status is mentioned in the below tables weather information is decoded or not after being exposed the watermarked image to listed attacks. If information status is decoded that mean authentication information is decoded successfully and it will authenticate the digital content.

Table 5.5.1 shows the results corresponding to gain factor value = 0.1 for dataset 3.

Table 5.5.1 Results for dataset 3 corresponding to gain factor= 0.1

Attacks		NC value, text watermark and information extraction status corresponding to various attacks			
		Gain factor=0.1			
		PSNR	NC (for image watermark)	Text Watermark Status	Information Status
Without attack		34.5952	0.9812	intact	decoded
salt and pepper noise	d=0.001	34.5952	0.9758	intact	decoded
	d=0.002	34.5952	0.969	intact	decoded
	d=0.003	34.5952	0.9626	intact	decoded

speckle noise	**v=.0001**	34.5952	0.9792	intact	decoded
	v=.0003	34.5952	0.9765	corrupt	decoded
	v=.001	34.5952	0.9687	corrupt	Not
gaussian noise	**v=.0001**	34.5952	0.9777	corrupt	decoded
	v=.0002	34.5952	0.9746	corrupt	decoded
	v=.0003	34.5952	0.9717	corrupt	decoded
poisson		34.5952	0.9313	corrupt	Not
cropping	**Instance1**	34.5952	0.0385	intact	decoded
	Instance2	34.5952	0.0116	intact	decoded
	Instance3	34.5952	0.0477	intact	decoded
resizing	**90%**	34.5952	0.979	corrupt	decoded
	75%	34.5952	0.9805	corrupt	decoded

Table 5.5.2 shows the results corresponding to gain factor value = 0.09 for dataset 3.

Table 5.5.2 Results for dataset 3 corresponding to gain factor= 0.09

Attacks		**NC value, text watermark and information extraction status corresponding to various attacks**			
		Gain factor=0.09			
		PSNR	**NC (for image watermark)**	**Text Watermark Status**	**Information** Status
Without attack		35.5238	0.9834	intact	decoded
salt and pepper noise	**d=0.001**	35.5238	0.9778	intact	decoded
	d=0.002	35.5238	0.9715	intact	decoded
	d=0.003	35.5238	0.9656	intact	decoded
speckle noise	**v=.0001**	35.5238	0.9814	intact	decoded
	v=.0003	35.5238	0.9789	corrupt	decoded
	v=.001	35.5238	0.9713	corrupt	Not
gaussian noise	**v=.0001**	35.5238	0.9798	corrupt	decoded
	v=.0002	35.5238	0.9766	corrupt	decoded
	v=.0003	35.5238	0.9736	corrupt	decoded
poisson		35.5238	0.931	corrupt	Not
cropping	**Instance1**	35.5238	0.0401	intact	decoded
	Instance2	35.5238	0.0021	intact	decoded
	Instance3	35.5238	0.0543	intact	decoded
resizing	**90%**	35.5238	0.9811	corrupt	decoded
	75%	35.5238	0.9828	corrupt	decoded

Table 5.5.3 shows the results corresponding to gain factor value = 0.08 for dataset 3.

Table 5.5.3 Results for dataset 3 corresponding to gain factor= 0.08

Attacks		**NC value, text watermark and information extraction status corresponding to various attacks**			
		Gain factor=0.08			
		PSNR	**NC (for image watermark)**	**Text Watermark Status**	**Information Status**
Without attack		36.4256	0.9828	intact	decoded
salt and pepper noise	**d=0.001**	36.4256	0.975	intact	decoded
	d=0.002	36.4256	0.9672	intact	decoded
	d=0.003	36.4256	0.957	intact	decoded
speckle noise	**v=.0001**	36.4256	0.9805	corrupt	decoded
	v=.0003	36.4256	0.9775	corrupt	decoded
	v=.001	36.4256	0.9669	corrupt	not
gaussian noise	**v=.0001**	36.4256	0.9781	corrupt	decoded
	v=.0002	36.4256	0.9739	corrupt	decoded
	v=.0003	36.4256	0.9694	corrupt	decoded
poisson		36.4256	0.9125	corrupt	not
cropping	**Instance1**	36.4256	0.0205	intact	decoded
	Instance2	36.4256	-0.0102	intact	decoded
	Instance3	36.4256	0.0482	intact	decoded
resizing	**90%**	36.4256	0.9799	corrupt	decoded
	75%	36.4256	0.9821	corrupt	decoded

Discussion

From the above tables of dataset 3 in a same way is clearly shown as for dataset 1 and dataset 2 that this mythology given in this project work is quite robust against various attacks mentioned in above tables. In most of the attacked instances, information is decoded successfully and authenticity of author is proven. For noise attacks in most of cases text watermark get corrupted but information is decoded successfully from image watermark which is nothing but encoded QR code of text watermark same for the resizing attacks. But for cropping attack image watermark is get corrupted to large extent shown by low NC values; hence information is decoded using text watermarks. But some of the attacks corresponding to higher density like in Gaussian noise, speckle or poisson noise, information could not be decoded successfully that mean this method is robust up to some level of noise. For improving more robustness more redundant watermarks can be embedded but it will result into low imperceptibly of watermarked image.

CHAPTER 6

CONCLUSION

From the results shown in chapter 5 it is clearly shown that this mythology given in this project work is quite robust against various. In most of the attacked instances, information is decoded successfully and authenticity of author is proven. For noise attacks in most of cases text watermark get corrupted but information is decoded successfully from image watermark which is nothing but encoded QR code of text watermark and same for the resizing attacks. But for cropping attack image watermark is get corrupted to large extent shown by low NC values; hence information is decoded using text watermarks. But some of the attacks corresponding to higher density like in Gaussian noise or poisson noise, information could not be decoded successfully that mean this method is robust up to some level of noise and it is meaningful in the sense that imposing large noise mean degrading the beauty of digital image which in some application attacker have no use of, like for professional photographs. For improving more robustness more redundant watermarks can be embedded but it will result into low imperceptibly of watermarked image.

REFERENCES

[1] M. Durvey and D. Satyarthi,"A Review Paper on Digital Watermarking," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),* July-August 2014, Volume 3, Issue 4.

[2] M. Abdullatif, A. M. Zeki, J. Chebil and T. Surya Gunawan,"Properties of Digital Image Watermarking," *IEEE 9th International Colloquium on Signal processing and its Applications,* March 2013, kuala Lumpur, Malaysia, pp. 235 - 240.

[3] P. Mishra and B. Thankachan, "Highly Secure Method for Image Transmission Using Partition and Multi Encryption Technique," *International Journal of Science and Research (IJSR),* July 2013, India, Volume 2, Issue 7, pp. 347-350.

[4] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," *Proceedings of the IEEE,* July 1999. Volume 87, Issue 7, pp. 1079 - 1107.

[5] P. Dabas and K. Khanna "A Study on Spatial and Transform Domain Watermarking Techniques," *International Journal of Computer Applications,* May 2013. Volume 71, Issue 14.

[6] M. Prajapati "Transform Based Digital Image Watermarking Techniques for Image Authentication," *International Journal of Emerging Technology and Advanced Engineering*, May 2014, Volume 4, Issue 5.

[7] M. Durvey and D. Satyarthi, "A Review Paper on Digital Watermarking," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),* July-August 2014, Volume 3, Issue 4.

[8] S. P. Mohanty "Digital Watermarking : A Tutorial Review," IIT Banglore, 1999.

[9] M. Yang, N. Bourbakis and S. Li, "Data, Image and Video Encryption*"* *IEEE Potentials,* 2004, Volume 23, Issue 3, pp. 28 - 34.

[10] P. Parashar and R. K. Singh, "A Survey: Digital Image Watermarking Techniques," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 2014, Volume 7, Issue 6, pp. 111-124.

[11] R. K. Megalingam, M M. Nair, R. Srikumar, V. K. Balasubramanian, V. Sarma and Venugopala Sarma, “Performance Comparison of Novel, Robust Spatial Domain Digital Image Watermarking with the Conventional Frequency Domain Watermarking Techniques,” *International Conference on Signal Acquisition and Processing*, 2010, pp. 349 - 353.

[12] S. Kumar and A. Dutta, “Performance analysis of spatial domain digital watermarking techniques,” *International Conference on Information Communication and Embedded Systems (ICICES)*, 2016, pp. 1- 4.

[13] N. S. Narawade. “Robust reversible watermarking using integration of histogram shifting and patchwork algorithm to improve quality and capacity,” *International Conference on Information Processing (ICIP)*, 2015, pp. 625 -630.

[14] M. Ejima and A. Miyazaki, “On the evaluation of performance of correlation-based watermarking techniques in the frequency domain,” *Proceedings. International Conference on Image Processing, 2002*, Volume 3 , pp. 457 - 460.

[15] M. Al Baloshi and M. E. Al-Mualla, “A DCT-Based Watermarking Technique for Image Authentication,” *IEEE/ACS International Conference on Computer Systems and Applications*, 2007, pp. 754 - 760.

[16] K. Deb, Md. Sajib Al-Seraj, Md. Moshiul Hoque and Md. Iqbal Hasan Sarkar, “Combined DWT-DCT based digital image watermarking technique for copyright protection,” *7th International Conference on Electrical and Computer Engineering*, 2012, pp. 458 - 461.

[17] R. Choudhary and G. Parmar, “A robust image watermarking technique using 2-level discrete wavelet transform (DWT),” *2016 2nd International Conference on Communication Control and Intelligent Systems (CCIS)*, 2016, pp. 120 - 124.

[18] K. Tomar, “A Review Paper of Different Techniques on Digital Image Watermarking Scheme For Robustness,” *International Journal of Advanced Research in Computer Science and Software Engineering*, February 2015, Volume 5, Issue 2, pp 900 - 904.

[19] E. El-Din Hemdan “Hybrid Digital Image Watermarking Technique for Data Hiding,” *IEEE 30th national radio science conference,* April 2013, pp. 220 - 227.

[20] M. C. Hernandez, M. N. Miyatake and H. M. P. Meana, “Analysis of a DFT-based watermarking algorithm,” *2nd International Conference on Electrical and Electronics Engineering*, 2005, pp. 244 - 247.

[21] A. K. Singh, N. Sharma, M. Dave and A. Mohan “A Novel Technique for Digital Image Watermarking in Spatial Domain,” *2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, 2012, pp. 497-501.

[22] R. Gayathri and Dr. V. Nagarajan, “Secure data hiding using Steganographic technique with Visual Cryptography and Watermarking Scheme,” *IEEE ICCSP conference*, 2015, pp. 118-123.

[23] B. Nassiri, R.Latif,A.Toumanari and F.M.R. Maoulainine, “Secure transmission of medical images by watermarking technique*,” 2012 IEEE International Conference on Complex Systems (ICCS)*, 2012, pp. 1 - 5.

[24] M. Rajawat and D S Tomar, “A Secure Watermarking and Tampering detection technique on RGB Image using 2 Level DWT,” *IEEE Fifth International Conference on Communication Systems and Network Technologies*, 2015, pp. 638 - 642.

[25] M. Moniruzzaman, M. Abul Kayum Hawlader and M. Foisal Hossain,“Wavelet Based Watermarking Approach of Hiding Patient Information in Medical Image for Medical Image Authentication,” *IEEE 17th International Conference on Computer and Information Technology (ICCIT)*, 2014, pp. 374 - 378.

[26] S. Bakhtiari, “JPEG Image Encryption with Elliptic Curve Cryptography,” *IEEE International Symposium on Biometrics and Security Technologies (ISBAST)*, 2014, pp. 144 -149.

[27] P. Gupta, “Cryptography based digital image watermarking algorithm to increase security of watermark data,” *International Journal of Scientific & Engineering Research*, September 2012, Volume 3, Issue 9.

[28] J. S. Bhalla and P. Nagrath, “Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm,” *International Journal of Scientific & Engineering Research Publications*, April 2013, Volume 3, Issue 4.

[29] S. Kaur and M. Lal, “An Invisible Watermarking Scheme Based on Modified Fast Haar Wavelet Transform and RSGWPT,” *Proceedings of IEEE 2015 RAECS UIET Panjab University Chandigarh*, 21 - 22 December 2015.

[30] A. Al-Haj, N. Hussein and G. Abandah, “Combining Cryptography and Digital Watermarking for Secured Transmission of Medical Images,” *2016 2nd International Conference on Information Management (ICIM)*, 2016, pp. 40 - 46.

[31] M. OUSLIM, A. Sabri and H. Mouhadjer, “Securing biometric data by combining watermarking and cryptography,” *IEEE 2nd International Conference on Advances in Biomedical Engineering*, 2013, pp. 179-182.

[32] K. Anusree and G. S. Binnu, “Biometric Privacy using Visual Cryptography, Halftoning and Watermarking for Multiple Secrets,” *IEEE National Conference on Communication, Signal Processing and Networking (NCCSN)*, 2014, pp. 1-5.

[33] Y. Han, W. He, S. Ji and Q. Luo, “A Digital Watermarking Algorithm of Colour Image based on Visual Cryptography and Discrete Cosine Transform,” *IEEE Ninth International Conference on P2P, Parallel Grid, Cloud and Internet Computing*, 2014, pp. 527-530.

[34] S. Ghosh, S. De, S. Prasad Maity and H. Rahaman, “A Novel Dual Purpose Spatial Domain Algorithm for Digital Image Watermarking and Cryptography Using Extended Hamming Code,” *IEEE Proceedings of International Conference on Electrical Information and Communication Technology (EICT 2015)*, 2015, pp. 167-172

[35] S. Kumar and A. Dutta, “A Novel Spatial Domain Technique for Digital Image Watermarking Using Block Entropy,” *IEEE Fifth International Conference on Recent Trends in Information Technology*, 2016, pp. 1 - 4.

[36] M. Malonia and S. K. Agarwal, “Digital Image Watermarking using Discrete Wavelet Transform and Arithmetic Progression,” *IEEE Students’s Conference on Electrical, Electronics and Computer Science (SCEECS)*, 2016, pp. 1 - 6.