

HISTOGRAM BASED WATERMARKING USING ENTROPY TECHNIQUE IN DIGITAL IMAGES

DISSERTATION

Submitted in partial fulfillment of the
Requirement for the award of the
Degree of

MASTER OF TECHNOLOGY

IN

Electronics and Communication Engineering

By

Shivani Kashyap

Under the guidance of

Mr. Mandeep Singh Saini

Assistant Professor



L LOVELY
P ROFESSIONAL
U NIVERSITY

School of Electronics and Communication

Lovely professional University

JALANDHAR, PUNJAB

APRIL 2015

School of: Electronics & communication

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: shivani

Registration No: 11308407

Batch: 2013

Roll No. 55

Session: 2013-2015

Parent Section: EE E2308

Details of Supervisor:

Designation: A.P.

Name: Mandeep Singh

Qualification: M.Tech

U.ID: 16853

Research Experience: 2 years

SPECIALIZATION AREA: _____ (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. Histogram digital image watermarking using entropy technique
2. Invisible watermarking by using interpolation technique
3. To increase robustness of invisible digital watermarking using frequency domain technique.

Signature of Supervisor

PAC Remarks:

Approved

APPROVAL OF PAC CHAIRPERSON:

Signature:

Date:

*Supervisor should finally encircle one topic out of three proposed topics and put up for a approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

DECLARATION

I hereby declare that the dissertation proposal entitled, “**HISTOGRAM BASED WATERMARKING USING ENTROPY TECHINQUE IN DIGITAL IMAGES**” submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date:

Investigator

Shivani Kashyap

Regn No.:-11308407

ACKNOWLEDGEMENT

First of all, I would like to express my gratitude to **Mr. Mandeep Singh Saini**, Department of Electronics and Communication Engineering, Lovely Professional University, Jalandhar for his continuous guidance and support throughout this report work. I am truly very fortunate to have the opportunity to work with him. Next, I wish to thank my gratitude to entire faculty as well as staff of the Department and then friends who devoted their valuable time and helped me in all possible ways towards successful completion of this work. I thank all those who have contributed directly or indirectly to this work. Lastly, I would like to thank my parents for their years of unyielding love and encourage. They have always wanted the best for me and I admire their determination and sacrifice.

Shivani kashyap

(Lovely Professional University)

ABSTRACT

With the wide use of internet, digital media are widely used. Digital media are easily and illegally destroyed, copied and changed. So there is a need of transmitting the data securely and confidentially and for this we need an effective data hiding scheme. This is where watermarking system comes in existence. Digital Watermarking is the technique which allows an owner to add hidden copyright notices, image, and signature, audio, video or other messages to digital media. If the media is copied by an unauthorized user, then the information embedded in digital media is also carried in the copy. Image watermarking means to embed visible or invisible information in an image that identifies the genuine owner. Several techniques for embedding a watermark into digital media have been developed so far each of which has its own advantages and limitations. Among these, this thesis work deals with developing the watermarking scheme for digital images. Here we deal with invisible watermarking. In this thesis work we mainly focus on better image quality and to retain the integrity of the watermark after being embedded into the original image and reduce perceptual degradation. Here we can increase robustness against attacks by pre-processing the image using techniques of interpolation and histogram equalization. After pre-processing entropy is calculated in different domains like grey scale, DCT and DWT to check high entropy value for watermark insertion as high entropy area would be less sensitive to attacks and provide robustness and guaranteed invisibility. It is proved analytically and shown experimentally that the peak signal to noise ratio (PSNR) of the watermarked image versus original image is guaranteed to be above 80 db.

Keywords:- Digital watermarking, histogram equalization, Interpolation, entropy technique, secret key.

CERTIFICATE

This is to certify that **Shivani Kashyap** has completed M.Tech dissertation proposal titled **“HISTOGRAM BASED WATERMARKING USING ENTROPY TECHINQUE IN DIGITAL IMAGES”** under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation proposal is fit for the submission and the partial fulfillment of the condition for the award of M.Tech in Information Technology.

Date:

Signature of Advisor:

Name: Mandeep Singh Saini

UID: 16853

ACKNOWLEDGEMENT

The report has been written with the kind guidance and support of my mentor. The satisfaction and happiness that accompanies the successful completion of any task would be incomplete without mentioning the names of people who made it possible, whose constant guidance and encouragement crowns all efforts with our success.

I would like to express my deep gratitude and thanks to my mentor **Mr. Mandeep Singh Saini**, Ass. Professor, Lovely Professional University, Phagwara, Punjab for their help and guidance throughout my dissertation work. I have received an enormous amount of valuable advice and knowledge from her that helps me a lot in my work. Thank you, **Mr. Mandeep Singh Saini**, for providing me motivating support in my research work.

TABLE OF CONTENTS

Chapter-1 Introduction.....	1
1.1 Different data hiding technique background.....	2
1.1.1 Cryptography.....	3
1.1.2 Steganography.....	5
1.1.3 Watermarking.....	6
1.2 Need of watermarking in digital media.....	6
1.3 Types of digital watermarks.....	7
1.3.1 According to watermarking domain.....	7
1.3.2 According to type of document.....	8
1.3.3 According to human perception.....	9
1.4 Watermarking techniques.....	12
1.4.1 Spatial domain watermarking.....	12
1.4.2 Frequency Domain watermarking.....	13
1.5 Application areas of digital watermarking.....	14
1.5.1 Copyright protection.....	14
1.5.2 Copy protection.....	15
1.5.3 Broadcasting monitoring.....	15
1.5.4 Fingerprinting.....	15
1.5.5 Annotation applications.....	16
1.6 Characteristic of watermarking schemes.....	17
1.7 Interpolation technique.....	17
1.8 Histogram equalization.....	18
1.9 Pixel region.....	19
1.10 Entropy technique.....	21
Chapter -2 Literature Review.....	22
Chapter-3 Present work.....	26
3.1 Problem and formulation.....	26
3.2 Work methodology.....	27
3.3 Digital watermarking process.....	28

3.3.1 Embedding technique.....	28
3.3.2 Retrieval technique.....	30
3.4 Evaluation parameters.....	32
3.4.1 Need of evaluation parameter.....	32
3.5 Development tool (MATLAB).....	33
3.6 Scope of study.....	34
Chapter-4 Result and discussion.....	35
4.1 Result.....	35
4.2 Performance evaluation or analysis.....	36
Chapter-5 Conclusion and future work.....	47
5.1 Conclusion.....	47
5.2 Future scope.....	48
References.....	49

LIST OF FIGURES

Fig. 1.1:- Securing confidential data using encryption.....	3
Fig 1.2:- Securing confidential data using steganography.....	5
Fig 1.3:- watermark on a bank currency note.....	6
Fig 1.4:- Classification of watermarking.....	7
Fig 1.5:- Embedding.....	8
Fig 1.6:- Extraction.....	9
Fig 1.7:-Visible watermarking.....	10
Fig 1.8:-Invisible watermarking.....	11
Fig 1.9:- DCT frequency band.....	13
Fig 1.10:- Wavelet watermarking.....	14
Fig 1.11:- Wavelet decomposition.....	14
Fig 1.12:- Equalized Histogram image.....	18
Fig 1.13:- Original image and its histogram.....	19
Fig 1.14:- Histogram and its histogram equalization.....	19
Fig 1.15:- Find the pixel of particular region of a image.....	20
Fig 1.16:- Finding pixel of lena image.....	20
Fig 1.17:- Final pixel region.....	20
Fig 3.1:- Formulation of problem.....	26
Fig 3.2:- Steps to embed the watermarking and to get the watermarked image.....	28

Fig 3.3:-Retrieval technique.....	31
Fig 4.1:-Original image and watermark image.....	36
Fig 4.2:-Graphical representation of PSNR of different original images.....	37
Fig 4.3:- Image watermark embedding.....	38
Fig 4.4:- Image watermark extraction.....	39
Fig 4.5:- Original image.....	39
Fig 4.6:- Histogram equalized image.....	40
Fig 4.7:-Histogram of DWT without Histogram equalization.....	40
Fig 4.8:- Histogram of DWT domain with Histogram equalization.....	41
Fig 4.9:- Histogram of watermark image after Histogram scaling.....	41
Fig 4.10:- Original boat image.....	43
Fig 4.11:- Histogram equalized boat image.....	43
Fig 4.12:- Baboon watermark.....	44
Fig 4.13:- Histogram of DWT domain without histogram equalization.....	44
Fig 4.14:- Histogram of DWT domain with histogram equalization.....	45
Fig 4.15:- Histogram of watermark image after histogram scaling.....	45
Fig 4.16:- Watermark final image.....	46

LIST OF TABLES

Table I:- PSNR comparison of original images with watermark image.....	37
Table II:- Comparison table.....	42

LIST OF ABBREVIATIONS

LSB: - Least Significant Bit

DCT: - Discrete Cosine Transform

DWT:-Discrete Wavelet Transform

Rbio:- Reverse bio-orthogonal

PSNR:- Peak Signal To Noise Ratio

CHAPTER 1

INTRODUCTION

The success and rapidly growth of the digital devices and Internet has briefly changed our society daily life style by making the capture, transmission and storage of digital data extremely easy and convenient. But it raises a big problem that is how to secure our data from the attacker when we are transmitting our files through internet. Digital media provides many distinct blessing as compare to analog family, or in other words digital media offers various blessing as compare to analog family that is high flexibility, high quality, easy editing and accuracy etc.

Now days, technology is developing more and more fast, it is playing an important role in people life and work. With the rapid development of networks and digital technology, we widely use the internet and digital signal to transmit information. But in transmission when we transmitting information then copying is easy because one can easily find out the exact discrete locations to be changed.

So this issue that is copying has become problematic in many areas. Due to this music and video industries loses lots of money by illegal downloading and coping. For solving this problem there is digital watermarking is used. From the above this reasons digital watermarking becomes attractive research topic. Digital watermarking provides copyright protection or more security and data authentication. In digital watermarking the secret information or message is added into digital media that is audio, video, text or images files etc. Digital information may be kept expeditiously, with a really prime excellence or quality, or it may be arranged terribly and simply by victimization computers. What is more, digital information may be transmitted in an exceedingly quick and cheap method through digital communication networks while not losing excellence or quality.

As an example, if we tend to visit <https://www.wallpaper.com>, we tend to observe that each one the wallpaper pictures are created by the house owners, which are their holding Right (HR). Any user will transfer the wallpapers. Now, consider that a user

downloads (the pictures or the photographs) and posts those images (either after modifying or original) on his/her web site.

Three problems might arise during this situation:

- However can the owner of wallpaper.com recognize that there's an added internet server on WWW posting their wallpapers?
- If the owner is aware of concerning this reality, wherever shall he visit to create a complaint?
- The last however vital issue is that if 1st 2 issues are resolved, how will be the owner will prove the ownership on the wallpaper images posted on another server?

The first issue is said to network technologies and involves problems like web crawler and pattern matching etc. Second issue is said to the international copyright laws and is another terribly tough issue. This thesis work will not deal with these a pair of problems.

This thesis covers the third issue, the authentication i.e. a way to prove the ownership?

The above problem may be solved by adding some possession or ownership information into the transmitted information, which can be extracted later to prove the possession or ownership. This idea is enforced in bank currency notes embedded with the watermark that is employed to prove the originality of the note. An equivalent watermarking construct is also employed in transmission digital contents for checking the genuineness of the first content. To start with a fast background of watermarking, 1st we tend to gift the history of information hiding and connected terminologies. Then, we'll travel to a discussion on the watermarking, needs that watermarking system should meet, sorts of the watermarking, applications and so varied attacks on a watermarking system.

The digital watermark is then introduced to solve this problem. There are two typical technologies have been developed from where copyrighted material can be protected by illegal duplications. One method is key-based cryptographic technique which provides appropriate security during the transmission process, but once the encrypted data is decoded, the control of redistribution and its spread fails.

1.1 DIFFERENT DATA HIDING TECHNIQUE BACKGROUND

There are several techniques used for copyright protection and several purposes. For information hiding several techniques are used in digital media. Cryptography and steganography these are the two basic methods of information hiding and digital watermarking is then derived from steganography. The cryptography means secret writing whereas steganography means cover writing.

1.1.1 Cryptography

- Protecting the digital content of the media.
- In cryptography hiding the contents of a message from an attacker, but do not hide the existence of the message.
- With the help of key the message is decrypted at the receiver end, or the message is encrypted before the transmission.
- No one can access the contents without having the true key.
- The message or information is protected before the transmission but after decryption the information becomes unprotected and it can be copied and distributed.
- The message is called plaintext and after encryption the message is called cipher text.

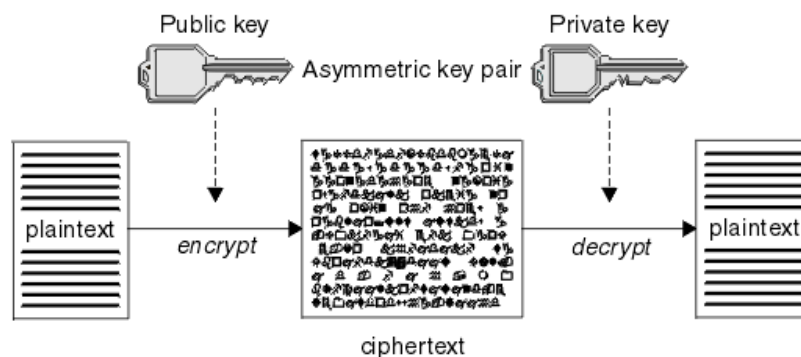


Figure 1. 1 Securing confidential data using encryption[23]

I. Classical cryptographic Techniques

❖ Symmetric Technique

- One of the oldest and most secure encryption technique, it is also known as private key cryptography.
- Private key is used for the security purpose. Basically key is used for encryption and decryption of data, with the help of key data remains secure and no one can read the coded message.
- Message is changed into cipher text with the help of key when the sender encodes it, and at receiver side the same key is used when the message is decoded that is same key are used at the both side.
- People can be use this encryption method as either a stream cipher or block cipher depending on the amount of data being encrypted or decrypted at a time.
- A stream cipher encrypts data one character at a time as it is sent or received, while a block cipher processes fixed chunks of data.
- Common symmetric encryption algorithms include Caesar cipher algorithm, Data encryption standard (DES), Advanced encryption standard (AES), and International data encryption algorithm (IDEA).

❖ Asymmetric Technique

- Asymmetric technique is more secure than symmetric technique. Asymmetric technique is also known as public cryptography.
- Two keys are used for encryption and decryption in asymmetric technique that is Private Key or public key.
- The use of two keys overcomes a major weakness in symmetric key cryptography, since a single key does not need to be securely managed among multiple users.
- In asymmetric technique public key is freely available to everyone and used to encrypt message before sending them. RSA method is used in the public key encryption.

1.1.2 Steganography

- Steganography is a cover writing in which secret data is embedded into the carrier in such way that only carrier is visible which is sent from transmitter to receiver without scrambling
- In steganography all kinds of digital knowledge that is video, audio, pictures and text documents are used as a cover medium.
- In steganography, the message is embedded into the digital media rather than encrypting it in such a way that nobody except the sender and the intended recipient can even realize that there is a hidden message.
- The digital media content, called the cover, can be determined by anybody; but, the message hidden in the cover can be detected by only the person having the actual key. Thus steganography actually relates to covering point-to-point communication between two parties. That's why steganography methods are usually not robust against modification of the data. Thus, steganography is a region that is, additional or less, a Hide-&-Seek game.
- Watermarking and fingerprinting these two techniques are very closely to related to steganography.

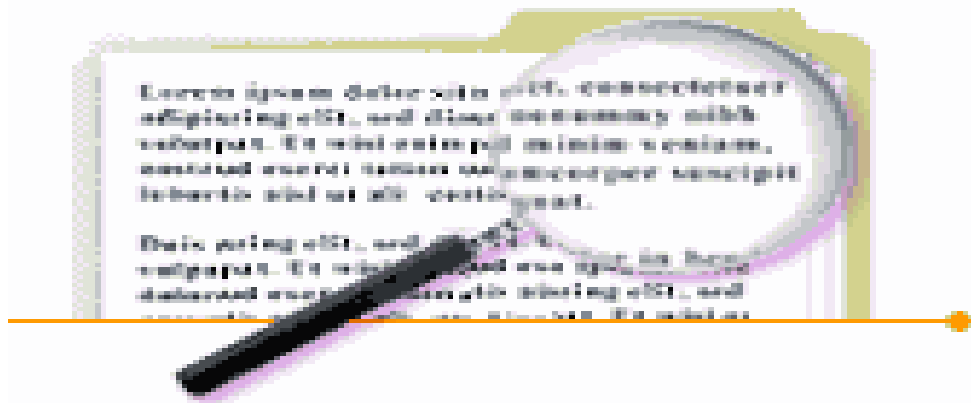


Figure 1. 2 Securing confidential data using steganography[22]

1.1.3 Watermarking

- Watermarking is a computer-aided information and this computer aided information is hiding in a carrier signal. Watermarks may be used to verify the authenticity or the integrity of the carrier signal or to show the identity of its owner.
- It is prominently used for tracing copyright infringements and for banknote authentication. Watermarking tries to control the robustness at top priority, or watermarking and fingerprinting these techniques are very closely related to steganography.
- Digital watermarking is a copyright protection and here watermark could be a message, information, data, images or any type of symbol which is embedded in the digital content and can be detected or extracted later. Watermark can be embedded in the digital contents visible or invisible form.



Figure 1. 3 Watermark on a bank currency note[24]

1.2 NEED OF WATERMARKING IN DIGITAL MEDIA

- The development of various digital media in multimedia system has developed many multimedia technologies and this technology and this technology can be protected by copyright ownership and cannot be use without any permission of the owner. So that is why Digital watermarking is one best technology that protects digital media (images, audio and video) from illegal manipulations.
- During the past year, copyrighted materials can be protected by using watermark. By using watermark in digital media no one can use the data (images, audio and video) without any permission of owner. To solve this reason the digital watermark is

introduced. There are various technologies have been developed from where copyrighted material can be protected by illegal duplications. One of them is key-based cryptographic technique which provides appropriate security level during the transmission.

1.3 TYPES OF DIGITAL WATERMARKS

Prof. S. Mohanty et al.[12] presents a very good classification of watermarking areas in his paper. In this type of watermarking is based on embedding, perception, cover medium an application domain. Figure 1.4 describes the different types of classification of watermarking.

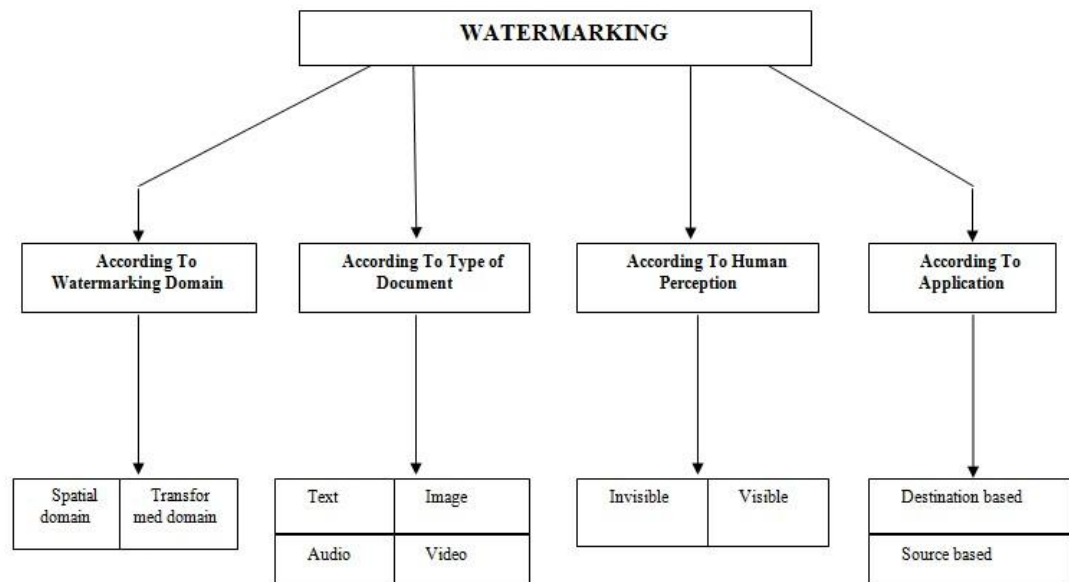


Figure 1. 4 Classification of watermarking

1.3.1 ACCORDING TO WATERMARKING DOMAIN

I. Spatial domain: In spatial domain there is a direct manipulation of the pixels in an picture to hide the watermark. No transformation is applied in the host signal and this technique there is limited robustness.

II. Transformed technique: In transformed domain there is a modification in the Fourier transform of an image. In this domain the watermark is insert into frequency coefficients of transformed image using different types of transform techniques (DCT and DWT).Watermark in frequency domain has proved to be more robust and compatible than the spatial domain.

1.3.2 ACCORDING TO TYPE OF DOCUMENTS

I. Image watermarking

❖ Embedding

A binary data sequence that is watermark is added into original signal or key is also used there. The information embedding imposes small signal changes, determined by the key and the watermark, to generate the watermarked signal.

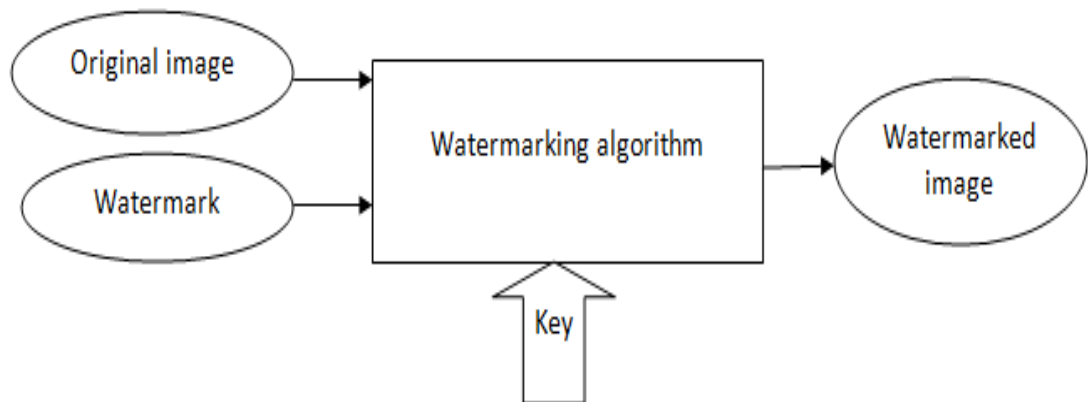


Figure 1.5 Embedding

❖ Extraction

- The watermark so that changes can be later observed with the use of the key to ascertain the embedded bit sequences. The process is called watermark extraction. The principal design challenges are in embedding the watermark so that it reliably fulfills its intended task.
- For copy protection applications, the watermark must be recoverable even when the signal undergoes a reasonable level of distortion, and for tamper assessment applications. The security of the system comes from the uncertainty of the key. Without access to this information, the watermark cannot be extracted.

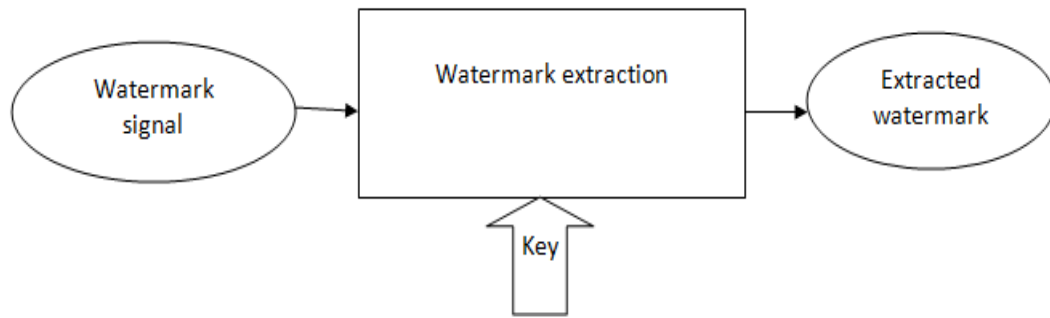


Figure. 1.6 Extraction

II. Video watermarking: To control the video applications the watermark or any type of symbol is added in it.

III. Audio watermarking: To control the audio applications the watermark is added into it.

Due to illegal copying or downloading of the contents people or owner loses lots of money. To overcome this problem the watermark is applied into media contents.

IV. Text watermarking: In text watermarking the watermark is embedded into various text files, PDF, DOC etc. The watermark or a bit character is added into the font shape and line spaces.

1.3.3 According to human perception

In this human perception the digital watermarking having a two different types: Visible watermarking and invisible watermarking.

I. Visible watermarking



Original image

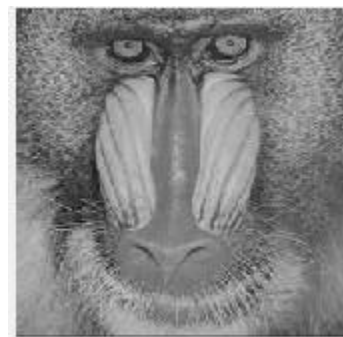


image watermark



Final watermark image

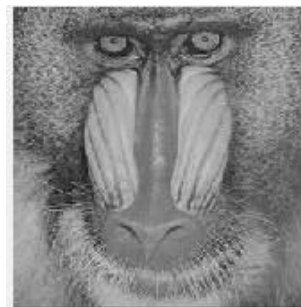
Figure 1.7 Visible watermarking

- The information or message is visible in the digital media. This process is called visible watermarking; here information is visible in the picture or video. Typically, the information is text, logo or image which identifies the owner of the media.
- Visible watermarks change the signal altogether such that the watermarked signal is totally different from the actual signal, Stock photography agencies often add a watermark in the shape of a copyright symbol ("©") to previews of their images, so that the previews do not substitute for high-quality copies of the product included with a license.
- When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark. Figure 1.7 shows the visible watermarking.

II. Invisible watermarking



Original image



watermark image



Final watermarked image

Figure. 1.8 Invisible watermarked image

- In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it is not visible. Invisible watermarks do not change the signal to a perceptually great extent, i.e. there are only minor variations in the output signal.
- An example of an invisible watermark is when some bits are added to an image modifying only its least significant bits. While the addition of the hidden message to the signal does not restrict that signal's use, it provides a mechanism to track the signal to the original owner.
- It is to protect digital media by fingerprinting each copy with the purchaser's information. If the purchaser makes illegitimate copies, these will contain his name. Fingerprints are an extension to watermarking principle and can be both visible and invisible.

1.4 WATERMARKING TECHNIQUES

1.4.1 Spatial (space) Domain Watermarking

In spatial domain there is a direct manipulation of pixels in an image to hide the watermark. No transformation is applied in the host signal and this technique has limited robustness. Spatial domain watermarking is a spread spectrum approach in which a watermark such as an image or any type of symbol is embedded or added by modifying pixel values.

There are some common spatial domain that are patchwork, texture, LSB and block coding etc. in this domain there is limited robustness, due to this it is difficult to add watermark in this technology and it cannot survive under attacks that is low pass filtering, lossy compression etc. in this domain the limited information can be embedded.

I. LSB watermarking

LSB watermarking is one of the earliest techniques used for watermarking. Embedded watermark image is found by alternation of certain bits of digital image which are selected based on secret key.

Advantages

- High Watermark channel capacity.
- Algorithm has less computational complexity.

Disadvantages

- No robustness.
- Search Space is huge.
- Weak against D/A and A/D.

1.4.2 Frequency Domain Techniques

Frequency domain modifying the Fourier transform of an image. In the frequency domain the watermark is inserted into frequency coefficients of transformed image using any kind of transform technique such as DCT and DWT. When we added watermark in frequency domain then there is more robustness and compatible to proper image compression standards.

I. DCT:- It basically express a sequence of many data points that is sum of cosine function and oscillating at different frequency. DCT is a general orthogonal transform for signal processing and digital image processing. In this it having a advantages such as small bit error rate, compression ratio, good information integration ability and good synthetic effect of calculation complexity.

DCT converts images from spatial to frequency domain. In this high frequency correspond the pixel value changing rapidly so in this area the imperceptibility increases and robustness decreases, whereas at the low frequency correspond the pixel

value changing slowly and in this area there is robustness increases and imperceptibility decreases.

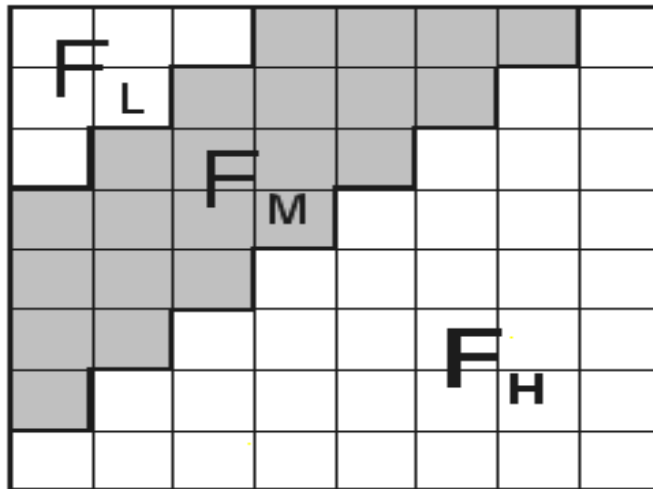


Figure 1.9 DCT Frequency band[14]

DCT has a strong energy compaction property so high frequency corresponds to rapidly changing pixel values and Low frequency correspond to slowly changing pixel values. DCT is used to compress JPEG images and can be used as part of a information hiding technique.

II. DWT:- DWT is a fast and simple transformation technique which translate an image from spatial domain to transform domed or frequency domain. DWT separate an image into the different resolutions and watermark can be embedded into this reason when once the image has been separated. DWT provides a no. of powerful image processing algorithms including noise reduction, compression and edge detection. In DWT if we are added CDMA spread spectrum then it increases the security level in watermark. DWT also survive under attacks such as image altering and conversion. Computer science, engineering, mathematical these are the basic application where DWT is used.

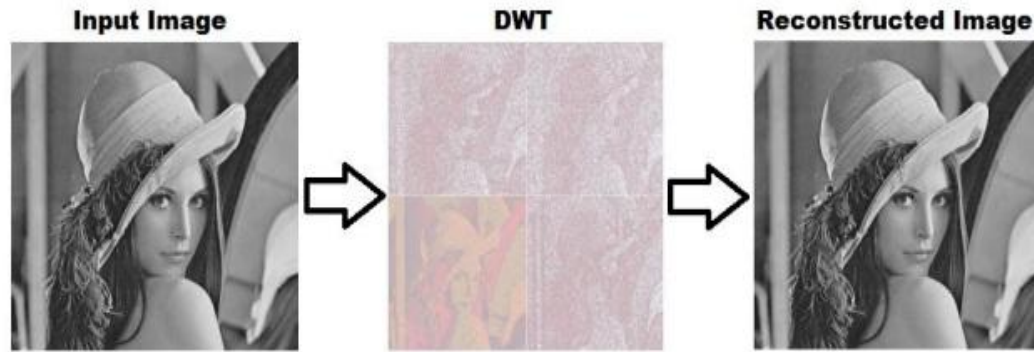


Figure 1.10 Wavelet watermarking[14]

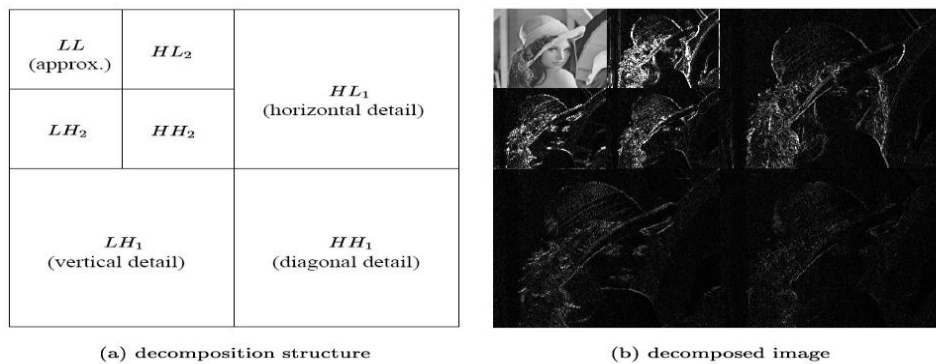


Figure 1.11 Wavelet decomposition[14]

1.5 Application areas of Digital Watermarking

Watermarking techniques may be relevant in the following application areas:

1.5.1 Copyright Protection

The primary use of watermarking is where an organization wishes to assert its ownership of copyright for digital objects. This application is of great interest to ‘big media’ organizations, and of some interest to other vendors of digital information, such as news and photo agencies. These applications require a minimal amount of information to be embedded, coupled with a high degree of resistance to signal modification (since they may be subjected to deliberate attack).

For example, now a days, a news channel “AAJ-TAK” is showing the animal’s clips (which are already shown on “Discovery” Channel) by hiding the Discovery channel’s logo on the video clips. As per the law, The AAJ-TAK should show the curtsey-sign and should pay the copyright fee to the Discovery channel. In such cases, there is a

strong need of watermarking as once the digital data is broadcasted, anybody else can start selling it without paying the IPR value to its owner.

1.5.2 Copy Protection

Watermarking can be used as a strong tool to prevent illegal copying. For example, if an audio CD has a watermark embedded into it, then any of the system (Hardware like DVD, or software) cannot make a copy of it, and even if it copies, the watermark data will not get copied to new duplicate audio CD. Now the duplicate CD can be easily found because it does not have watermark data. Some schemes have attempted to satisfy more complex copy protection requirements.

An early example is the Serial Copy Management System (SCMS), introduced in the 1980s, which enabled a user to make a single digital audio tape of a recording they had purchased but prevented the recording of further copies (i.e. second generation) from that first copy. The scheme failed ultimately because not all manufacturers of consumer equipment were prepared to implement the scheme in their products.

1.5.3 Broadcasting Monitoring

There are several types of organizations and individuals interested in monitoring the broadcast of their interest. For example, advertisers want to ensure that they receive the exact airtime that they have purchased from broadcasting firms. Musicians and actors want to ensure that they receive accurate royalty payments for broadcasts of their performances and copyright owners want to ensure that their property is not illegally rebroadcast by pirate stations.

1.5.4 Fingerprinting

If monitoring and owner identification applications place the same watermark in all copies of the same content, it may create a problem. If out of n number of legal buyers of a content one starts selling the contents illegally, it may be very difficult to catch who is redistributing the contents without permission. Allowing each copy distributed to be customized for each legal recipient can solve this problem. This capability allows a unique watermark to be embedded in each individual copy.

Now, if the owner finds an illegal copy, he can find out who is selling his contents by finding the watermark which belongs to only singly legal buyer. This particular

application area is known as fingerprinting. This is potentially valuable both as a deterrent to illegal use and as a technological aid to investigation.

1.5.5 Annotation Applications

In this applications area, watermarks convey object-specific information (“feature tags” or “Captions”) to users of the object. For example, patient identification data can be embedded into medical images. These applications require relatively large quantities of embedded data. While there is no need to protect against deliberate tampering.

1.6 CHARACTERISTIC OF WATERMARKING SCHEMES

Imperceptibility: In terms of watermarking, imperceptibility means that after inserting the watermark data, cover medium should not alter much. In other words, the presence of the watermark data should not affect the cover medium being protected.

If a watermarking scheme does not ensure this requirement, it may happen that after inserting a watermark data in a cover medium (say an image), image quality may alter which the owner of the image will never like that a protecting mechanism modifies his work.

Robustness: Robustness of the watermark data means that the watermark data should not be destroyed if someone performs the common manipulations as well as malicious attacks. It is more of a property and also a requirement of watermarking and its applicability depends on the application area.

Fragility: Fragility means that the watermark data is altered or disturbed up to a certain extent when someone performs the common manipulations & malicious attacks. Some application areas like temper detection may require a fragile watermark to know that some tempering is done with his work.

Some application may require semi-fragility too. The semi-fragile watermark comprises a fragile watermark component and a robust watermark component i.e. semi-fragile watermarks are robust to some attacks but fragile to others attacks.

Resilient to common signal processing: The watermark should be retrievable even if common signal processing operations are applied to the watermarked cover medium data.

These operations include digital-to-analog and analog-to-digital conversion (i.e. taking the printout of an image and then scan it to create another digital copy of the image), re-sampling, re-quantization (including dithering and recompression), and common signal enhancements such as image contrast, brightness and color adjustment, or audio bass and treble adjustment, high pass and low pass filtering, histogram equalization of an image.

Resilient to common geometric distortions (image and video data): Watermarks in image and video data should also be immune from geometric image operations such as rotation, translation, cropping and scaling. This property is not required for audio watermarking.

Robust to subterfuge attacks (collusion and forgery): In addition, the watermark should be robust to collusion attack. Multiple individuals, who possess a watermarked copy of the data, may collude their watermark copies to destroy the watermark presence and can generate a duplicate of the original copy. Further, if a digital watermark is to be used in litigation, it must be impossible for colluders to combine their images to generate a different valid watermark.

Unambiguousness: Retrieval of the watermark should unambiguously identify the owner. Furthermore, the accuracy of owner identification should not degrade much in the case of an attack.

1.7 INTERPOLATION TECHNIQUE

Interpolation is the process of using known data to estimate value at unknown location, or basically it provide a good perceptual quality from known sample values.

Interpolation is the technique from which the images are improved.

Interpolation is a basic tool used extensively in tasks such as rotating, zooming, geometric correction and shrinking. In interpolation technique there are various different types of methods and each resulting in different look to the final image.

Older methods of linear interpolation somewhat addressed this problem. By finding mean pixel value between neighboring pixels, one was able to produce an exact copy of Blurred edges and smoothed details.

Bilinear re-sampling uses the values of the four Surrounding pixels and new pixel values are calculated by weighting the averages of the four closest pixels based on distance. The new pixel value is determined by calculating a weighted average of the four closest pixels (2x2 arrays) based on distance. However, bilinear interpolation seems to work better for image improvement rather than image enlargement. A digital image is not an exact snapshot of reality; it is only a discrete approximation.

1.8 HISTOGRAM EQUALIZATION

Histogram equalization is a technique for adjusting image intensities to enhance contrast. Histogram modeling techniques provide a sophisticated method for modifying the dynamic range and contrast of an image by altering that image such that its histogram intensity has a desired shape. Histogram equalization employs a monotonic, non-linear mapping which re-assigns the intensity values of pixels in the input image such that the output image contains a uniform distribution of intensities (flat histogram).

Histogram equalization is the method which increases the global contrast of various images or it simply adjusting image intensities to enhance contrast. It produces unrealistic effects in photographs, and used for scientific images such as satellite, thermal and X-Ray images.

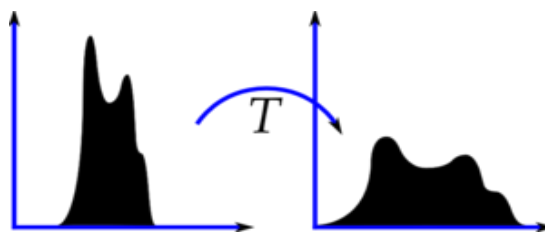


Figure 1.12 Equalized histogram image[10]

The method is useful in images with backgrounds and foregrounds that are both bright or both dark. In particular, the method can lead to better views of bone structure in x-ray images, and to better detail in photographs that are over or under-exposed.

For example:-

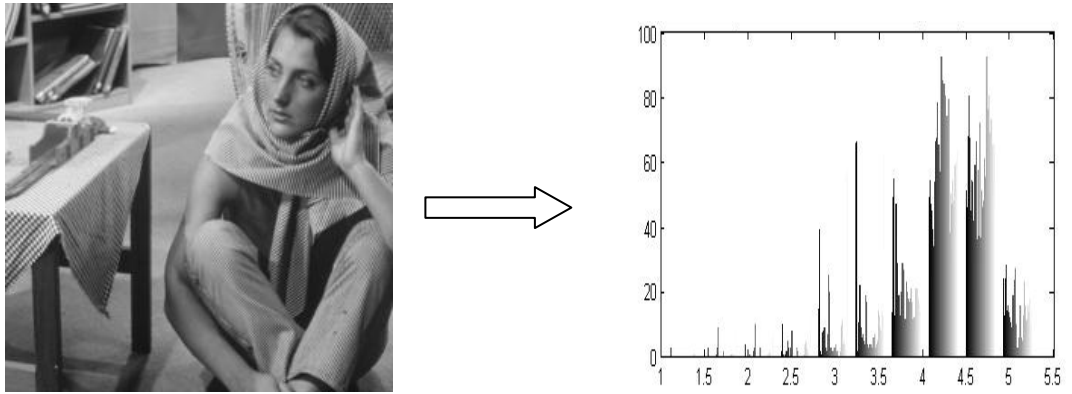


Figure 1.13 Original image and its histogram

HISTOGRAM EQUALIZATION:-

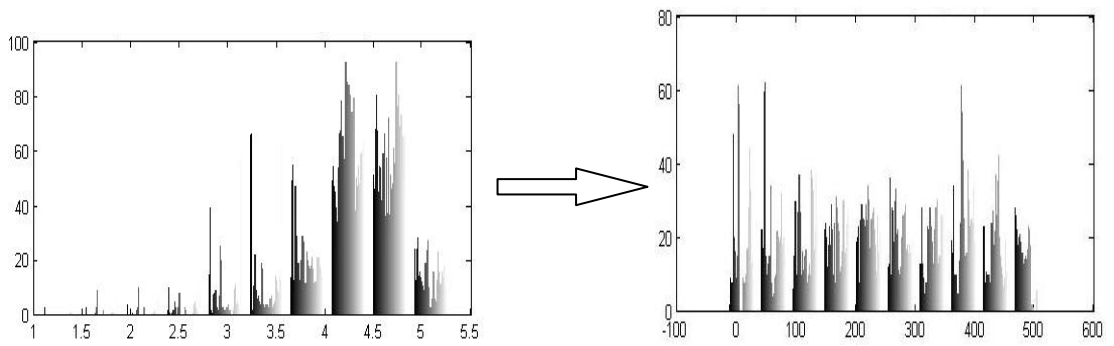


Figure 1.14 Histogram and its histogram-equalization image

1.9 PIXEL REGION

i. Finding the pixels of particular region of a image

Code:-

```
a=imread('lena.jpg');
```

```
Vals=impixel(a)
```

```
Vals =
```

```
215 215 215
```




Figure 1.15 Find the pixels of particular region of a image

ii. Finding all the pixel of image

Code:-

```
a=imread('lena.jpg');
s=imshow(a);
z=impixelregion(s);
```



Figure 1.16 Finding pixel of lena image

	B: 4	B: 12	B: 35	B:132	B: 62
	R: 0	R: 2	R: 67	R:148	R: 55
	G: 0	G: 2	G: 67	G:148	G: 55
	B: 0	B: 2	B: 67	B:148	B: 55
	R: 4	R: 41	R: 78	R:138	R: 55
	G: 4	G: 41	G: 78	G:138	G: 55
	B: 4	B: 41	B: 78	B:138	B: 55
	R: 26	R: 80	R: 57	R:101	R: 84
	G: 26	G: 80	G: 57	G:101	G: 84
	B: 26	B: 80	B: 57	B:101	B: 84

Figure 1.17 Final pixel region

1.10 ENTROPY TECHNIQUE

Entropy is a measurement of uncertainty, the area with large entropy keeps balance between robustness and transparency as a result. In information theory, entropy is a measure of the uncertainty in a random variable. Image entropy is a quantity which is used to describe the business of an image that is the amount of information which must be present in the image. Low entropy images, such as those containing a lot of black sky, have very little contrast and are venerable to attacks. An image that is perfectly flat will have entropy of zero. Consequently, they can be compressed to a relatively small size.

In order to keep effectiveness of media content communication, the area with more information provides high robustness. For another, the area with great uncertainty provides excellent masking effect, leading to high transparency. While the entropy is a measurement of uncertainty, the area with large entropy keeps balance between robustness and transparency as a result.

Formula to calculate the entropy value:

$$Entropy = -\sum_i P_j \text{Log}_2 P_j$$

In the above expression, P_i is the probability that the difference between 2 adjacent pixels is equal to i , and Log_2 is the base 2 logarithm.

CHAPTER 2

LITERATURE REVIEW

(BASE PAPER) Simi Elizabeth Chacko et al.[1] This paper describes the interpolation technique which is used for data hiding method,

- Here firstly calculates the interpolation error and then hide the secret information or data into the residual histogram.
- This paper describes two techniques Interpolation and Histogram shifting, from these two techniques the residual image is obtained.
- The advantage of this technique is compared to other hiding technique that is higher image quality and computational cost.
- In this paper the experimental results having a higher quality as compare to other hiding technique, and this image quality is evaluated in terms of PSNR.

Yana Zhang et al.[2] This paper describes the dissymmetric digital watermarking framework lived on media content communication and in the digital watermarking the essence of information is transmitted.

- In this paper entropy technique is used and this technique maintains or balance watermarks that are it maintain watermarks robustness and imperceptibility.
- In this paper the entropy is calculated into three different domains and finally shows the higher quality domain.

Sapana S.Bagade et al.[10] In this paper the authors presents the histogram equalization for image enhancement in image processing.

- Two techniques are described here: Image enhancement and histogram equalization technique.

G.coatrievx et al.[9] Presents the watermarking in healthcare systems. In this paper the watermarking provides security in instruments and medical information and also securely sharing and handling the medical images.

Yusnita Yusof et al.[6] In this paper author presents the overview of digital watermarking.

- History of watermarking, Types of digital watermarking, data hiding techniques, frequency domain (DWT).

Radhika v.totla et al.[14] Presents the both methods DCT and DWT based algorithm for watermarking in digital images.

- And also compare the imperceptibility and robustness in both methods and apply attacks such as resizing, rotating and cropping.

Hamza A.Ali et al.[11] In this paper the histogram technique is used.

- Here firstly the image carrier signal segmented or divided into blocks and then histogram technique is used and for each block the histogram is drawn.
- Due to this there is occurrence of peak frequency signal is identified in the given image.
- Finally watermark are used and applied at peak frequency signal.
- This technique is secure against different types of attacks that is resizing, noise or rotation.

Zhicheng Ni et al.[8] In this paper when the data is extracted after the hidden then there is original picture recovered back without any distortion.

- And this is only possible by the reversible data hiding algorithm.
- PSNR is calculated between the original picture and watermarked picture and in this paper the experimental result is above than 48 db.

Abduljabbar shaamala et al[16] Presents the study of the genetic watermarking Robustness under DCT and DWT Domains.

- In this paper watermarking is based on genetic algorithm and studying the effect of DWT and DCT.
- And the result is calculated which is based on numerical correlation. Numerical correlation is used to measure of robustness. It calculates the difference between the embedding and extracting watermark.

B Manoj kumar et al. [19] proposed a novel invisible and blind watermarking scheme for copyright protection against piracy of digital images. The proposed watermarking

scheme embeds a binary watermark image invisibly into a host image for protecting its copyrights.

- For every 2x2 block of the host image, a watermark pixel is embedded using the proposed approach. As the proposed watermarking scheme is blind, the extraction of watermark requires only the watermarked image and it doesn't demand the original image or any of its characteristics. The experimental results have demonstrated the efficacy of the proposed watermarking scheme.

P.Mohanty et al.[12] Presents digital watermarking and its review.

- Here the author describe Types, applications, attacks and also describe the various hiding techniques.

Franklin Rajkumar.V et al. [18] In this paper the Hadamard transformation algorithm is used. In this paper firstly original images is converting from spatial to transform domain and the watermark that is entire image or pattern is embedded into original image. And here the computational complexity is reducing by the hadamard transformation.

A.V. Subramanyam et al. [7] In this paper the stream cipher is used for encryption algorithm.

- Two techniques are used embedding and extraction.
- In this paper the robustness, embedding capacity, perceptual quality and security of the proposed algorithm is investigated in details.
- Different types of watermarking schemes are used.

Xianting Zeng et al. [3] In this paper the different types of scan paths are described.

- Reversible data hiding scheme are defined and also showing that more data can be hide into original image due to reversible data hiding technique.
- Increases data hiding capacity through multi layer embedding.
- For embedding process we can add more data into the original image as compared to the histogram shifting by selecting the best scanning path.

- PSNR is calculated between the original images or watermarked image and here the author show experimentally result more than 30 db.

Mohamed Radouane et al.[15] In this paper the author presents the LSB substitution method and entropy technique.

- In this paper the author introduce an algorithm of digital watermarking based on embedding watermark into sub images with LSB technique. Or in embedding process the watermark is added into specifies image blocks and selection of blocks are based on entropy value, and also calculated PSNR value.

3.1 PROBLEM AND FORMULATION

The problem statements consist of embedding the watermark in reverse bi-orthogonal DWT wavelet coefficient of the image. The watermark image was to be made secure with the aid of watermarking.

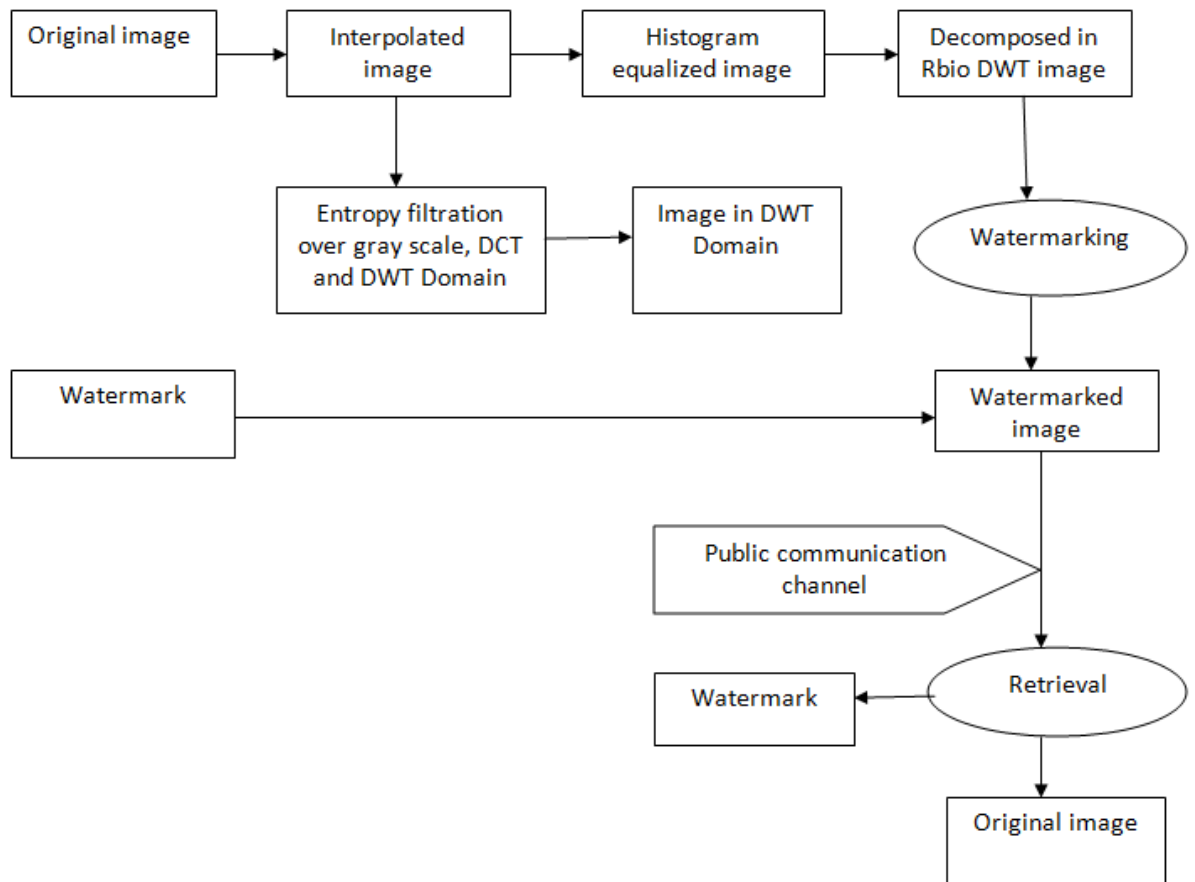


Figure 3.1 Formulation of problem [17]

Here, the entropy based method is proposed for invisible watermarking in still grey scale images using discrete wavelet transform and histogram equalization. The original image is chosen where we want to embed the watermark for copyright protection. And embedding is done in such a way so that it is invisible to others. To embed the watermark, we firstly improve the quality of image and then calculate entropy of the original image in different domains because maximum randomness or uncertainty

leads to better embedding of watermark and enhance robustness against attacks. Also in this proposed work secret key is embedded to enhance more security.[17]

3.2 WORK METHODOLOGY

The proposed technique is based on interpolation, Entropy calculation, histogram equalization and reverse bi-orthogonal DWT (discrete wavelet transform) domain. The original image is of 256*256 and watermark should be either equal to size of original image or less than that of the size of original image. During communication the security and robustness is important and it is provided by DWT domain.

In histogram of equalized image of DWT coefficients the watermark is added. In our proposed system we first implement interpolation over the original image using bilinear interpolation on the interpolated image we apply entropy filtration in order to find which domain is better for embedding the watermark. So we find that out of grey scale, DCT and DWT.

DWT domain has highest entropy so for embedding DWT is chosen as it is more secure and less vulnerable to attacks and the PSNR in DWT domain over actual picture is higher than other domain and. After that we do histogram equalization on the interpolated image to get the histogram equalized image and then we can apply reverse bi-orthogonal DWT wavelet to insert the watermark. Then again we can decompose the watermark by using R-bio wavelet and multiply the values of pixels of watermark by the factor alpha in order to insert the watermark uniformly anywhere in the histogram equalized image.

The proposed work achieve quite interesting finding. The watermarked image over the equalized image, PSNR always comes out more than 80 for different images. Due to this our watermark is done with higher invisibility and secondly the security is provided while transmitting the image over the internet or communication channel.

3.3 DIGITAL WATERMARKING PROCESS.

3.3.1 Embedding method

In original image the watermark is embedded by calculating entropy value so that we can find which area has maximum uncertainty or randomness in order to insert watermark so that it is invisible to others. While embedding we can first improve the quality of image and also remove the pixel errors based on bi-linear interpolation.

Following flow chart shows the complete embedding procedure to insert the watermark into the equalized image:

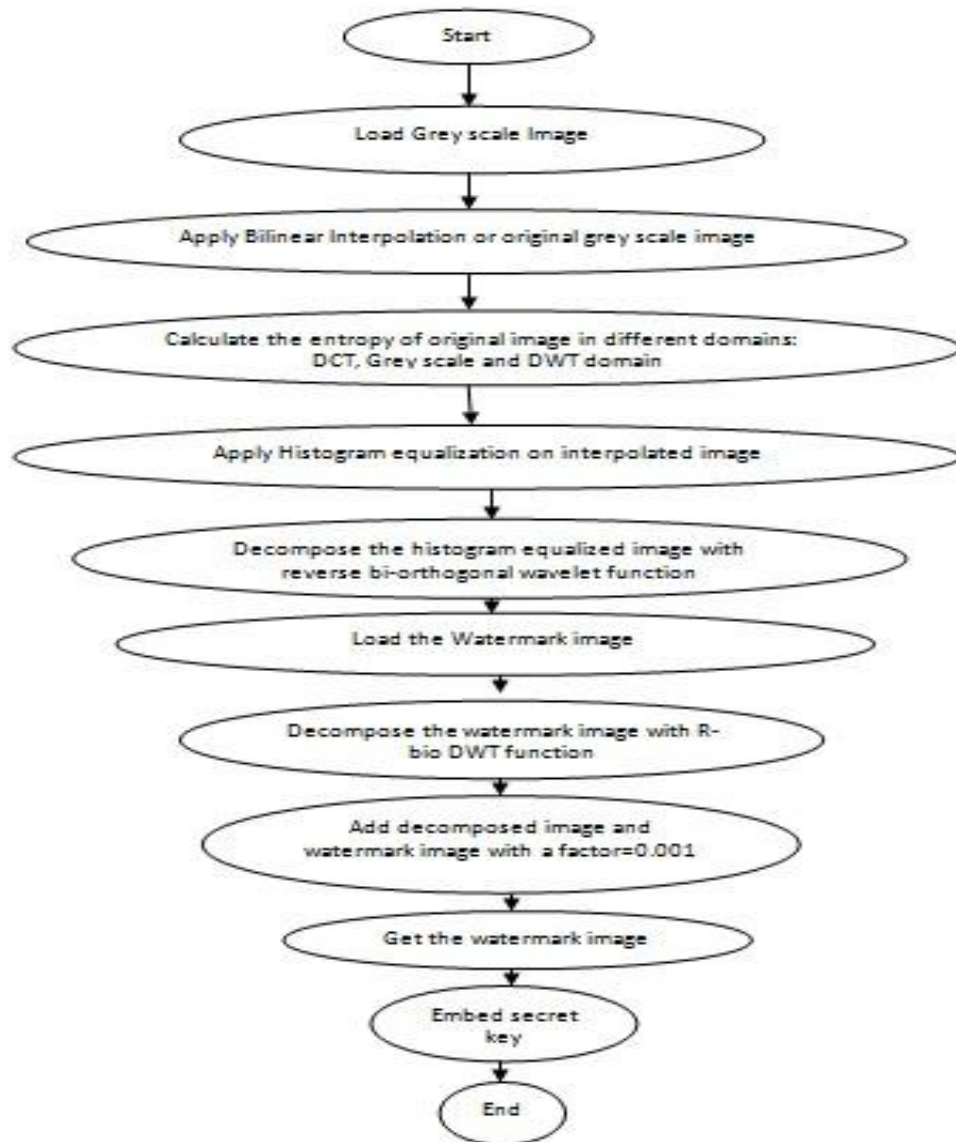


Figure 3. 1 Steps to embed the watermark and to get the watermarked image

1. Original Image:

The gray scale original image of size 256*256 is chosen and format of any type i.e. jpg, png, tiff, etc is chosen.

2. Interpolation image:

By using interpolation technique the gray scale image that is original picture is converted into interpolated image by using bilinear interpolation technique where the pixel value is guessed by using the pixel values 4 neighborhood pixels and taking the average weightage and remove pixel error and enhance image quality.

3. Entropy calculation:

Now calculate the entropy value of the interpolated image in different domains to check which domain is better in order to insert the watermark as high entropy value leads to increased invisibility and less vulnerable to attacks. Now the maximum entropy value and high PSNR comes in DWT domain.

4. Histogram equalized image:

Now we equalized the interpolated image so that the intensity value of the outcome image contains the uniform distribution of intensities which enable us to embed the watermark easily in any part of the image.

5. Decomposition with R-bio(reverse bi-orthogonal) wavelet:

For decomposition of the histogram equalized image and watermark image we have chosen R-bio 6.8 wavelet function. Decomposition of both image is done at level 1 by applying the scaling and wavelet functions on low pass filters. There is an advantages that is less computation time for embedding or also increasing robustness and invisibility by applying DWT domain.

6. Watermark image:

Now load the watermark image which is of the size equal to original image or less than that of the size of original image.

7. Watermarked image:

Now add the decomposed watermark image into decomposed histogram equalized image with factor $\alpha=0.001$.

8. Embedding secret key:

We embed the secret key by using the cipher code algorithm. This is the technique of symmetric key insertion in watermarked image before sending it over the public communication channel.

❖ Steps for embedding algorithm:

Step 1. Original image that is gray scale picture of 256*256 is chosen and format of any type like png, tiff, and jpg is considered.

Step2. Applying interpolation on original image to get interpolated image

Step 3 Calculate the entropy of the image in different domains i.e gray scale DCT and DWT domain.

Step 4. Now apply a histogram equalization on interpolated image to get a histogram equalized image.

Step 5. Decompose the histogram equalized image using reverse bi-orthogonal DWT as entropy value is higher in this domain.

Step 6. Also decompose the watermark image with reverse bi-orthogonal DWT wavelet function.

Step 7. Embedded the watermark into the histogram equalized image by using a factor=0.001 to get watermarked image.

Step 8. Now add the secret key into the watermarked image while transferring it over the communication channel.

3.2.2 Retrieval Technique

For retrieval purpose if the secret key which is embedded or applied to the watermarked image and this watermarked image is known before sending it over the public communication. After retrieval we get the image which we insert into equalized image from this we can secure an image or it is a copyright protection.

Below flowchart depicts, retrieval of invisible watermark from the watermarked image. Watermark is than extracted using inverse of R-bio (reverse bi-orthogonal) DWT wavelet. Retrieving the watermark in such a way that it does not leads to harm the integrity.

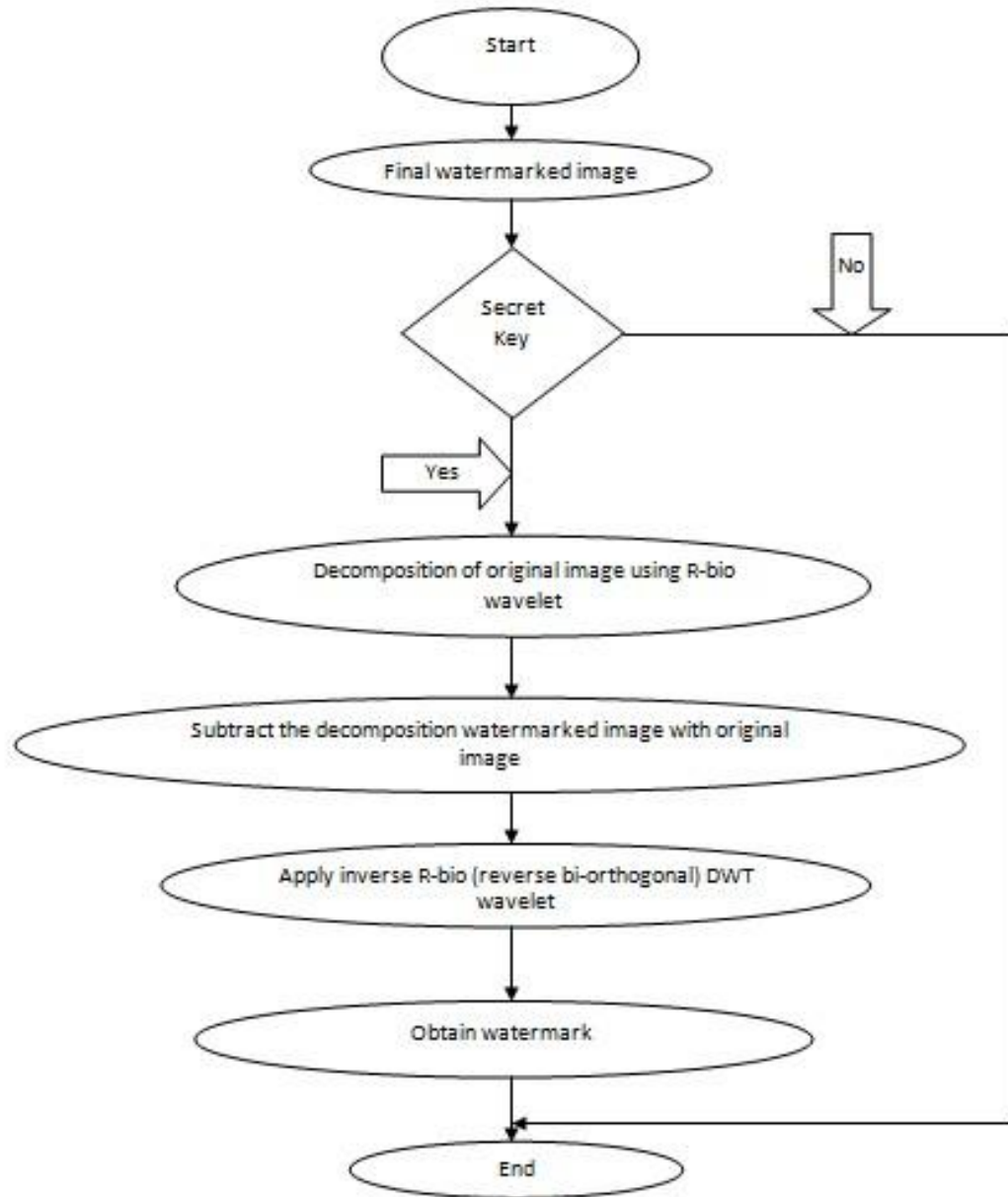


Figure 3. 3 Retrieval technique

1. Extraction of Watermark from the Watermarked image:

At the destination the watermarked image is received over the open channel. Any intruder will only be able to see it when an intruder interferes in the communication or transmission process, and the watermark image which is embedded in it cannot be extracted.

2. Enter Secret key

In order to extract the watermark Caesar cipher code which is applied for encryption at the sender side is used for decryption at other side. We can add the key which is decrypted by shifting that key by 3 value.

3. Decomposition of watermarked and original image

Both the images are decomposed by using reverse bi-orthogonal wavelet in order to extract the watermark.

4. Extract watermark

Now subtract the watermarked image with histogram equalized image to get watermark. And finally the watermark is extracted.

I. Steps for Retrieval Algorithm

Step 1. Receive the watermarked image through public channel

Step 2. Enter the secret key to extract the watermark. If entered key is incorrect than watermark is not extracted else go to step 3.

Step 3. Decomposed the watermarked image with R-bio wavelet.

Step 4. Also decomposed the histogram equalized image with R-bio wavelet.

Step 5. Subtract the watermarked image with histogram equalized image.

Step 6. Applying inverse R-bio DWT on subtracted outcome

Step 7. Finally display the watermark.

3.4 Evaluation Parameters

To check the performance of the proposed technique several parameters are used. Parameters evaluate the technique in terms of hiding capacity, and calculate PSNR between original picture and watermark picture and show the quality of watermarked picture.

3.4.1 Need of Evaluation Parameters

- 1.. Find the error between original and watermark picture.
2. Comparing the original picture or image with watermarked picture or image and measure its quality.
3. PSNR(Peak signal to Noise Ratio)

In this it is basically measure the quality of the image by comparing the original picture or image with the watermarked picture or image.

$$PSNR = 10 * \log \left(\frac{255^2}{MSE} \right)$$

3.5 DEVELOPMENT TOOL (MATLAB)

The name of MATLAB stands for Matrix laboratory. MATLAB is a high-performance or high level language for technical computing. MATLAB allows you to solve many technical computing problems. It is a program for analyzing images and data or doing Numerical computation. MATLAB environment to solve particular classes of problems or solving linear algebra type problems faster than other languages. MATLAB is used in various applications such as control systems, image processing, signal processing, fuzzy logic, simulation, communications and many others. From MATLAB we can solve technical computing problems and it is more faster than other traditional programming languages such as FORTRAN, C and C++

I. MATLAB various parts:

- Graphics
- Mathematical function library
- External interfaces
- Desktop tools and development environment
- The languages

II. MATLAB FEATURES:

- MATLAB is a high level language.
- MATLAB Provides strong mathematical and numerical support for the implementations of advanced algorithm.
- Analyzing data from 2-D and 3-D graphics functions.
- Environment for controlling and managing the data, code and files.
- Solving the problems faster than the other languages.

III. MATLAB STANDARD WINDOWS:

Command Window:- In this window we can write or execute the commands.

Workspace Window:- In this window load the variable from the files and to clear variables.

Show the current variables and also allows editing the variables, opening array editor by double click.

Current Directory Window:- In this window the MATLAB files in current folder and show current directory. Provides with a handy way to change folders and to load files.

History Window:- Shows previously executed commands.

In this window we can re-execute commands by double-clicking.

IV. MATLAB help

- Learning the MATLAB commands in a powerful way from the MATLAB help.
- MATLAB help option is present on the top of the window.
- In this it explains the commands with examples.
- In the search box we can search any command.
- It contains theoretical background or also shows the demonstration implementations.

3.6 SCOPE OF STUDY

- In our research we deal with invisible watermarking.
- In this thesis work we are mainly focus on better image quality and to retain the integrity of the watermark and after being embedding into the original image and reduce perceptual degradation.
- In our research we are going to increase robustness by using interpolation and histogram equalization.
- The main task of our dissertation is solving the two issues that we face copyright protection in the images and increase the quality and the security.

CHAPTER -4

RESULT AND DISCUSSION

4.1 RESULT

- The proposed algorithm deal with image watermarking.
- The proposed technique has been applied to grey scale images of size 256*256 and is of the image format png, tiff, bmp, jpg. Also the watermark which is to be embedded is of the size equal to or less than original image.
- This technique is applied into the different images and the same watermark image.
- The proposed technique can hide entire watermark directly in to the equalized image
- The research work also to retain the integrity of the watermark image after being embedded into the original image.
- Hiding information in the DWT coefficients results in less computation time and more security and more invisibility.
- The evaluation of the algorithm is calculated in terms of PSNR.
- The research has resulted in better PSNR value and with the help of secret key here we can enhance the security level.
- Adding of watermarking has made the technique more secure for public communication channel. For the protection the watermark is used and after that it shows the identity of the owner, because any intruder is trying to copy the contents during the transmission.
- The technique used here the entropy to check maximum randomness area which guarantees maximum invisibility and is less vulnerable to attacks.
- The quality of image is also increased by histogram equalization technique.
- The technique also use secret key for encryption while sending the copyright data or image over the public communication channel.
- In comparison with other well-known techniques our technique shows better results in terms of PSNR.
- This technique increases the robustness also.

4.2 PERFORMANCE AND ANALYSIS

I. For the performance analysis we use images of Lena, Boat, Lady as original image and Baboon as watermark image.



a) Lena



b) Boat



c) Lady



d) Baboon

Figure 4.1 ((a)-(c)) are the original images and (d) watermark image.[17]

II. For the performance analysis we use different original images and same watermark image of baboon to get watermarked picture or image and comparing PSNR of different original images and watermarked images as shown in Figure 4.1

Then enhance the image quality after that find the domain then same images are used to check the different value of PSNR here it check the clarity or quality of image between the original picture or image and the watermarked picture or image. By applying histogram based technique we get different values of PSNR.







ORIGINAL IMAGE	WATERMARK IMAGE	PSNR IN DIFFERENT DOMAIN	PSNR OF WATERMARKED IMAGE
		GRAYSCALE 48.698 DCT 47.864 DWT 49.541	86.410
		GRAYSCALE 51.434 DCT 50.5095 DWT 52.359	84.660
		GRAYSCALE 47.807 DCT 47.002 DWT 48.622	88.176

Table I PSNR comparison of original images with watermark image.[17]

The Table I. shows that maximum PSNR value comes while we insert the baboon as a watermark into the original image (Boat).

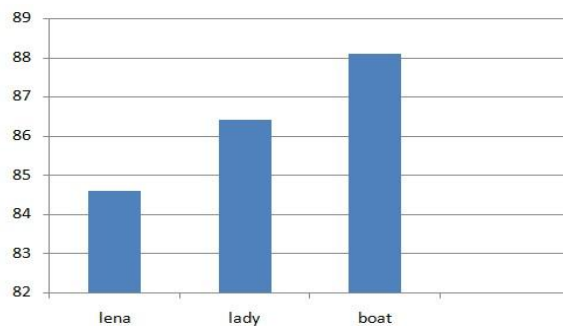


Figure 4.2 The graphical representation of PSNR of different original images.[17]

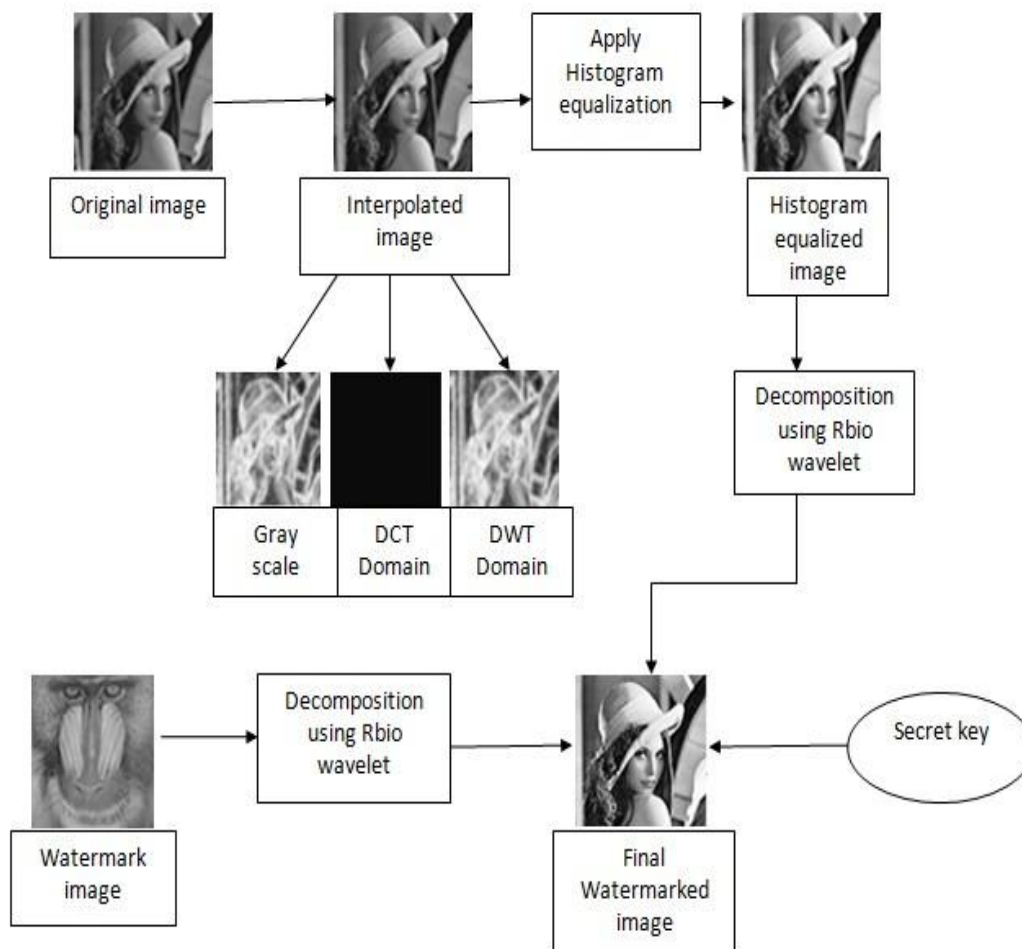


Figure 4.3 Image watermark embedding.[17]

Figure 4.3 To show the results we take original image of Lena with watermark of Baboon, and then this baboon image is embedded or added into the original image (lena) and get finally watermarked picture or image. This watermarked image is then transmitted over a public communication channel.

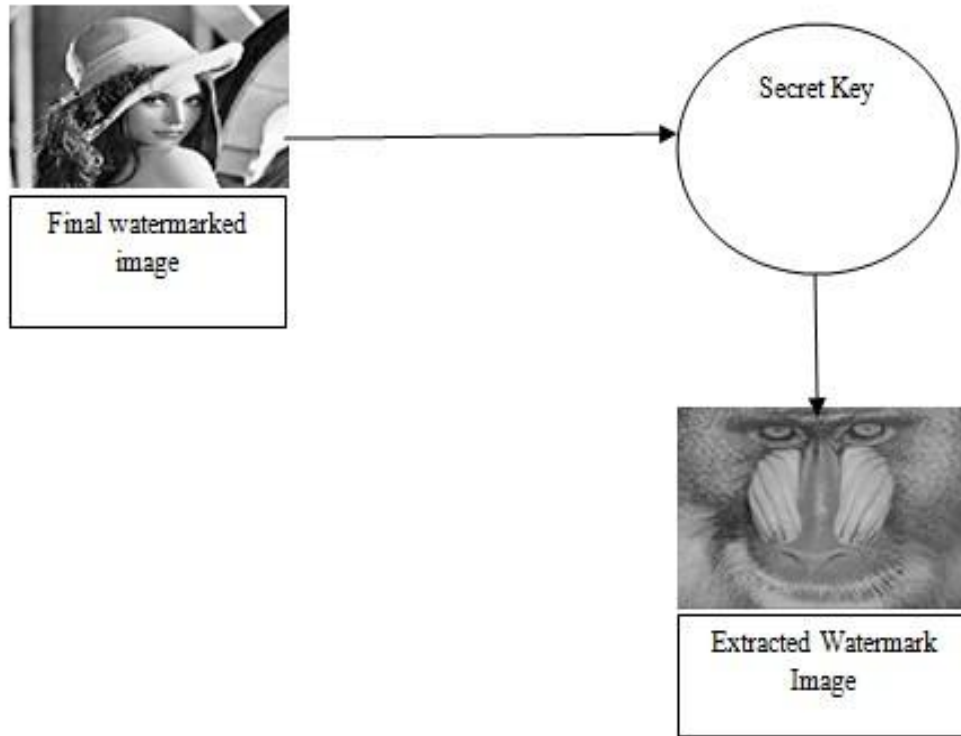


Figure 4.4 Image watermark extraction.[17]

Figure 4.4 shows the extracted watermark image of baboon extracted from the watermarked image.

III. Histogram Equalized Image and Histogram Process



Figure 4.5 Original image lena



Figure 4.6 histogram equalized lena image

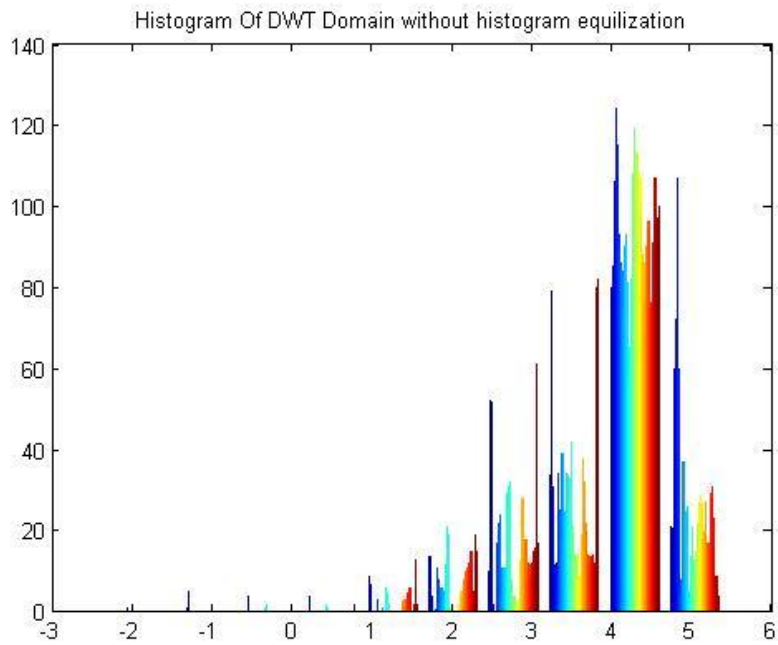


Figure 4.7 Histogram of DWT domain without histogram equalization.[17]

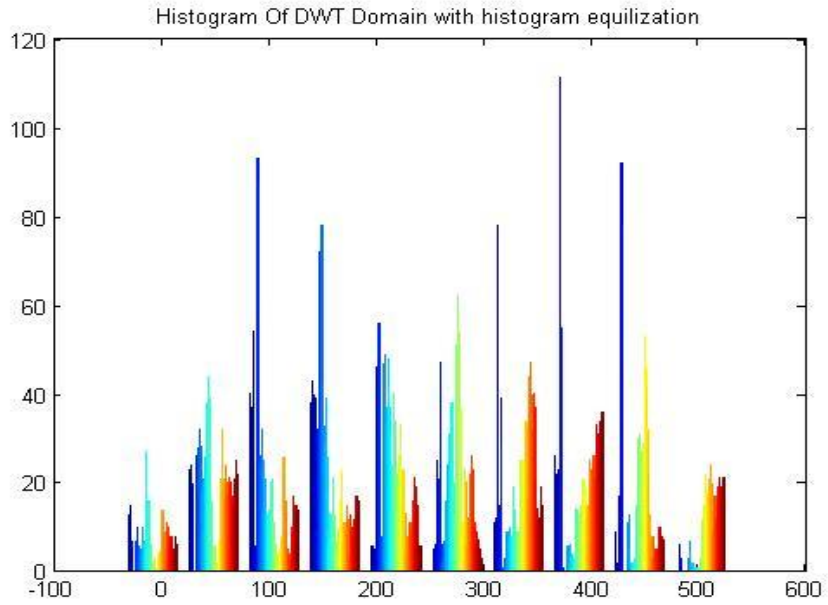


Figure 4.8 Histogram of DWT domain with histogram equalization.[17]

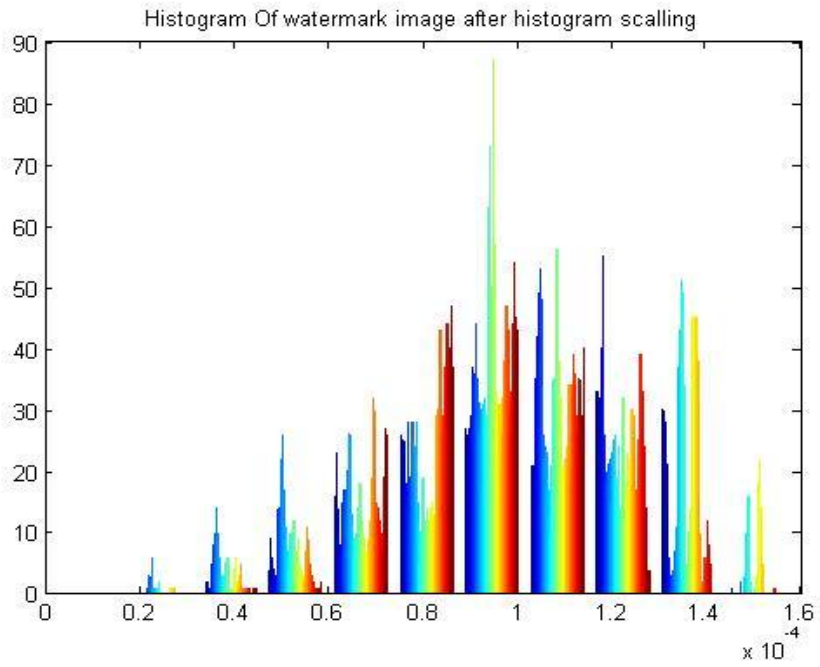


Figure 4.9 Histogram of watermark image after histogram scaling.[17]

IV. Comparison Result with Different Authors

Comparison result of lena and baboon in terms of quality. The proposed approach is compared with different authors to show our better results as specified below. As the PSNR of different authors are compared and it is found that our work is better among all.

Schemes	Lena Image	Baboon Image
	Quality (PSNR)	Quality (PSNR)
J.Hwang	48.22	48.20
C.C. Lin	46.22	47.61
P.Tsai	51.33	52.95
Lixin Luo	48.82	48.36
Simi Elizabeth chacko	68.59	68.53
Proposed	84.66	83.17

Table II. Comparison table.[17]

Comparison result lena and baboon in terms of quality. The proposed approach is compared with different authors to show our better results[1].

❖ **ANOTHER CASE**

Another results we take original image of boat with watermark of Baboon and this baboon image is embedded in it that is the baboon watermark image is embedded into the original (boat) and get finally watermarked picture or image. This watermarked image is then transmitted over a public communication channel.



Figure 4.10 Original boat image



Figure 4.11 Histogram equalized boat image

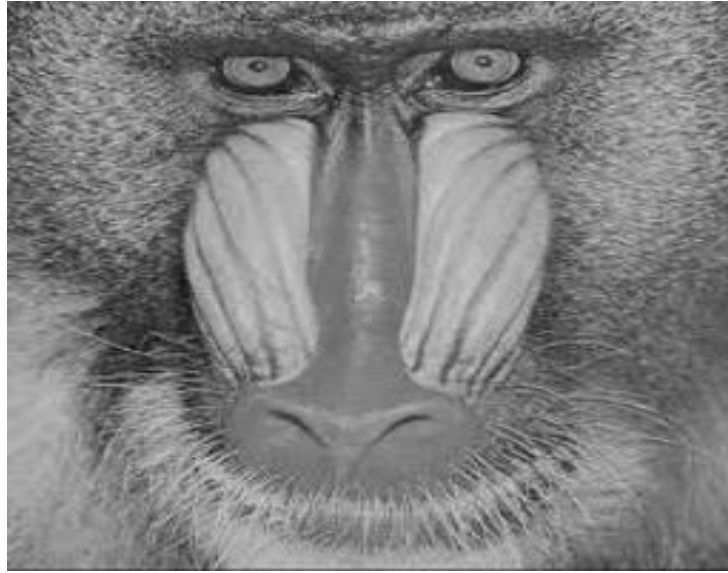


Figure 4.12 Baboon watermark

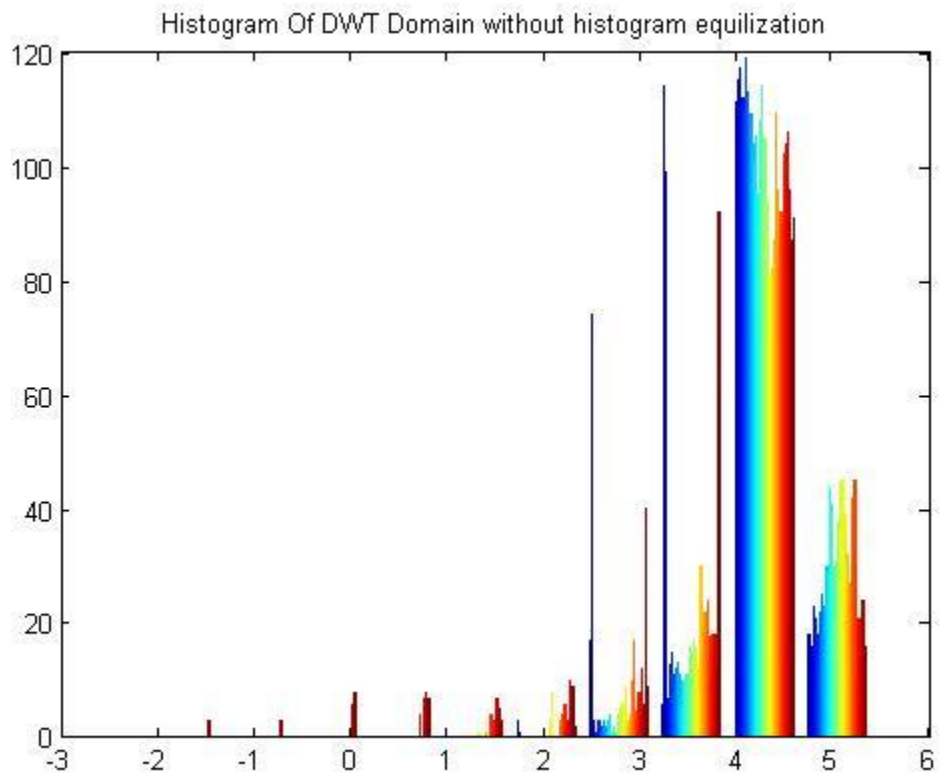


Figure 4.13 Histogram of DWT domain without histogram equalization

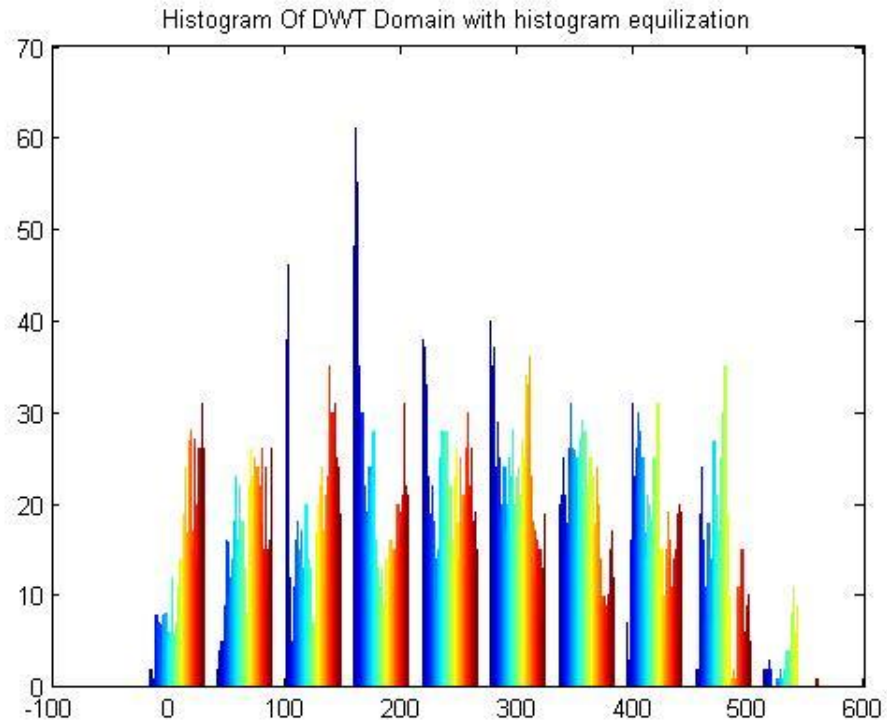


Figure 4.14 Histogram of DWT domain with histogram equalization

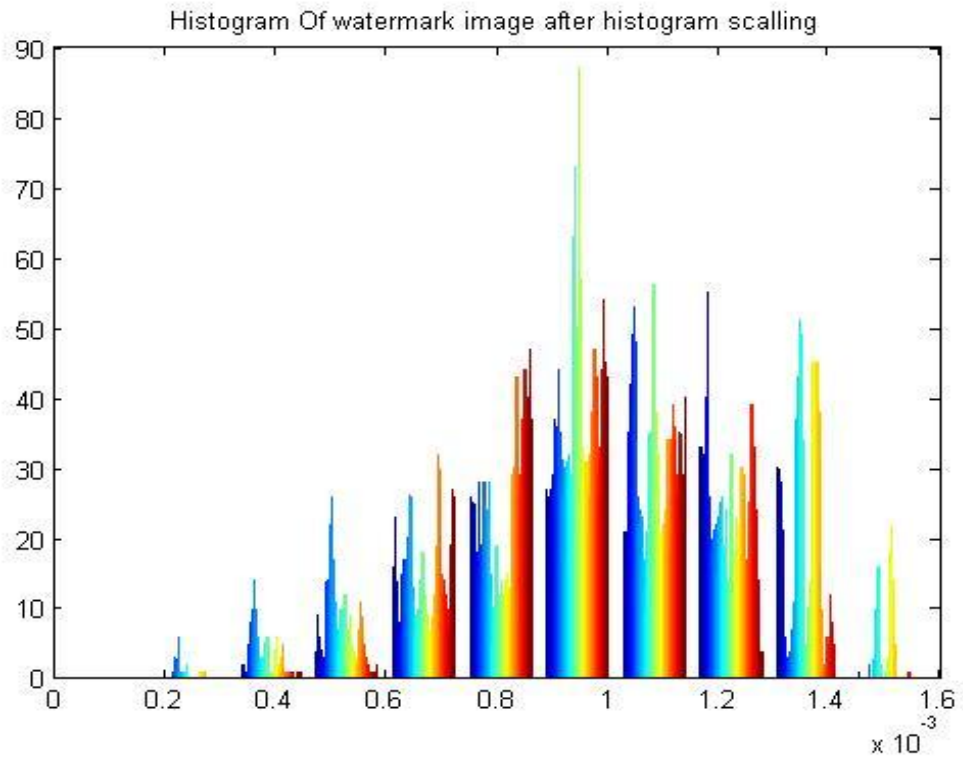


Figure 4.15 Histogram of watermark image after histogram scaling



Figure 4.16 Watermark final image

5.1 CONCLUSION

The watermarking is used to transfer copyright information over open channel. The technique proposed here is based on interpolation, histogram equalization, entropy filtration and Rbio DWT. The invisible watermark is added to the original image to make it more protected. The integrity of the data embedded in the original image retains. It is observed that the proposed techniques comes up with a good PSNR(Peak Signal to Noise Ratio) and enhanced security and also the secret key by the user or authorized person is added and is used at another side when one want to extract the hidden data(watermark) from the original image.

If anyhow the key entered by the user is wrong then user is not able to extract the watermark. Any intruder cannot find that there is some watermark is added into the original image and when trying he/she fails and would not be able to copy it or extract anything.

In methodology we adopted here for the implementation of proposed algorithm. And also we discuss the results of our proposed algorithm and findings shows that as far as existing literature is concerned, we have achieved better quality. We have used Rbio wavelet for decomposition of the image and provides much better results. Also we have calculated PSNR for different values of alpha and finding shows that at value of alpha=0.001, the PSNR of image is maximum.

If we further trying to reduce the value of alpha, the PSNR of the image does not show any significant improvement that's why we take the value of alpha=0.001 and at this time the value of PSNR is approximately equal to 88.17.

And also we enhance the quality of the image by removing its noise by using histogram equalization, interpolation so far none of the researchers had been focused on this side of watermarking.

5.2 FUTURE SCOPE

- In future we can improve the results if there is any other algorithm is better than which we are using.
- And also adding different types of noise in different domains and comparing the results and showing more robustness of watermarking.
- In future the same technique can be extended by applying different transforms to both original image as well as watermark and thus the robustness of algorithm can be verified.

REFERENCES

- [1] Simi Elizabeth Chacko Thusnavis Bella Mary.I Newton David Raj.W, “Embedding Invisible Watermark in Digital Image Using Interpolation and Histogram Shifting”,IEEE trans,2011.
- [2] Yana Zhang, Qiu Yang & Chen Yang, Qi Zhang, “A Universal Entropy Masking Model in Digital Watermarking System”,IEEE trans, 9th International Conference on Fuzzy Systems and Knowledge Discovery, 2012.
- [3] Xianting Zeng, Lingdi Ping & Zhuo Li, “ Lossless Data Hiding Scheme Using Adjacent Pixel Difference Based on Scan Path”,IEEE trans, VOL. 4, NO. 3, JUNE 2009.
- [4] Yu Chee Tseng, Hsiang Kuang Pan, “A Secure Data Hiding Scheme For Binary Images”, IEEE TRANSACTION ON COMMUNICATION, VOL.50, NO.8, AUGUST2002.
- [5] Fabien A. P. Petitcolas, Ross J. Anderson, Markus G.Kuhn,“Information hiding A Survey”,IEEE,VOL.87,NO.7,JULY 1999.
- [6] Yusnita Yusof, Othman O. Khalifa, “Digital Watermarking For Digital Images Using Wavelet Transform”,IEEE International Conference On Telecommunications and Malaysia International Conference on Communications,14-17 May 2007.
- [7] V. Subramanyam, Sabu Emmanuel & Mohan S. Kankanhalli, “ Robust Watermarking of Compressed and Encrypted JPEG2000 Images”, IEEE TRANS, VOL. 14, NO. 3, JUNE 2012.
- [8] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, & Wei Su, “Reversible Data Hiding”, IEEE trans, VOL. 16, NO. 3, MARCH 2006.
- [9] G.Coatrieux, L.Lecornu,“A Review of Image Watermarking Applications in Healthcare”,IEEE.
- [10] Sapana S. Bagade,“Use of Histogram Equalization in Image processing for Image Enhancement”,International Journal of Software Engineering Research and Practices , VOL.1, Issue 2 April,2011.
- [11] Hamza A. Ali & Sama’a A. K. khamis, “Robust Digital Image Watermarking Technique Based on Histogram Analysis”WCSIT trans, VOL. 2, No. 5, 163-168, 2012
- [12] Saraju P.Mohanty, “Digital Watermarking Tutorial Review”,1999.

- [13] S.M. Rafizul Haque, "Singular Value Decomposition and Discrete Cosine Transform Based Image Watermarking", Master Thesis, Computer Science, and Thesis no: MCS-2008:8, January 23, 2008.
- [14] Radhika v. Totla, K.S. Bapat, "Comparative Analysis of Watermarking in Digital Images Using DCT and DWT", International Journal of Scientific and Research Publications, VOL. 3, Issue 2, February 2013.
- [15] Mohamed Radouane, Tarik Boujiha, Rochdi Messoussi, Nadia Idrissi, Ahmed Roukh, "A Method of LSB substitution based on image blocks and maximum entropy", International Journal of Computer Science Issues, VOL. 10, Issue 1, No 1, January 2013.
- [16] Abduljabbar Shaamala, Azizah A. Manaf, "Study of the effected Genetic Watermarking Robustness Under DCT and DWT Domains", IJNCAA, 2012, pp. 353-360.
- [17] Shivani kashyap, Mandeep singh saini, "Histogram Based Watermarking Using Entropy Technique In Digital Images", IJARECE, VOL. 4, issue 3, March 2015, pp. 666-670.
- [18] Franklin Rajkumar.V Manekandan.GRS V.Santhi, "Entropy based Robust Watermarking Scheme using Hadamard Transformation Technique", international journal of computer application, VOL. 12, January 2011, pp. 14-21.
- [19] B. Manoj kumar, "Novel Invisible And Blind Watermarking Scheme For Copy Right Protection Of Digital Images", IJERT, VOL. 1 Issue 7, September – 2012, pp. 1-7.
- [20] http://www.encryptionanddecryption.com/algorithms/asymmetric_algorithms.html.
- [21] Chiou Ting Hsu and Ja Ling WU, "Mutiresolution Watermarking for Digital Images", IEEE Transaction On Circuits And Systems Ii, Analog And Digital Signal Processing, VOL. 45, No. 8, August 1998.
- [22] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.
- [23] http://www.encryptionanddecryption.com/algorithms/asymmetric_algorithms.html.
- [24] Prabhjot kaur chahal, Jaasveen kaur, Pallwinder singh, "Digital watermarking on bank note", IJSCE, vol. 3, issue 6, January 2014, pp. 38-41.