# A Tamper Localization Approach for Reversible Watermarking Algorithm Based on Histogram Bin Shifting

*Thesis submitted in partial fulfillment*

*of the requirements for the degree of*

**Master of Technology**

*in*

**Computer Science and Engineering**

*by*

**Awadhesh Kumar Yadav**

**(Roll No: 213CS2176)**

*under the guidance of*

**Prof. Ruchira Naskar**

**Department of Computer Science and Engineering**
**National Institute of Technology, Rourkela**
**Rourkela-769 008, Odisha, India**
**May, 2015.**

Department of Computer Science and Engineering
**National Institute of Technology Rourkela**
Rourkela-769 008, Odisha, India.

# Certificate

This is to certify that the work in the thesis entitled " ***A Tamper Localization Approach for Reversible Watermarking Algorithm Based on Histogram Bin Shifting***" submitted by ***Awadhesh Kumar Yadav*** is a record of an original research work carried out by him under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of Master of Technology in Computer Science and Engineering, National Institute of Technology, Rourkela. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

**Prof. Ruchira Naskar**
Assistant Professor
Department of CSE
National Institute of Technology
Rourkela-769008

Place: NIT,Rourkela-769008
Date: 25 - 05 - 2015

# Acknowledgment

First of all, I would like to express my deep sense of respect and gratitude towards my supervisor Prof. Ruchira Naskar, who has been the guiding force behind this work. I want to thank her for introducing me to the field of Multimedia Security and giving me the opportunity to work under her. Her undivided faith in this topic and ability to bring out the best of analytical and practical skills in people has been invaluable in tough periods. Without her invaluable advice and assistance it would not have been possible for me to complete this thesis. I am greatly indebted to her for constant encouragement and invaluable advice in every aspect of my academic life. I consider it my good fortune to have got an opportunity to work with such a wonderful person.

Secondly, I would like to thank Prof. Banshidhar Majhi for his invaluable suggestions, and encouragements during this research period.

I wish to thank all faculty members and secretarial staff of the CSE Department for their sympathetic cooperation.

During my studies at N.I.T. Rourkela, I made many friends. I would like to thank them all, specially AB Saxena and Rahul sir for all the great moments I had with them.

When I look back at my accomplishments in life, I can see a clear trace of my family's concerns and devotion everywhere. My dearest mother, whom I owe everything I have achieved and whatever I have become; my beloved father, for always believing in me and inspiring me to dream big even at the toughest moments of my life. At last but not least my brother and sisters; who were always my silent support during all the hardships of this endeavor and beyond.

*Awadhesh Kumar Yadav*

# Abstract

Reversible watermarking is a process which is used to authenticate the multimedia content. It checks the integrity of the digital data in order to recover the original data without any distortion. Industries like as medical services, military organization and legal services which are dealing the sensitive data where the minimal alteration is difficult to be tolerated is the application domain of Reversible watermarking. In this thesis, we have proposed a Tamper localization approach for histogram bin shifting based Reversible watermarking algorithm, where original image can be obtained from the watermarked image without any distortion. Tamper localization approach finds out the tampered region of the image, which is used for the selective rejection of the cover image. General application of reversible watermarking procedure says that the entire image gets rejected at receiver side due to the hash mismatch and authentication failure.

By using our approach when the hash mismatch occurs the selected part of the image is rejected. This will reduce the re-transmission overhead on the communication channel and limited bandwidth is required due to small sub-part of re-transmission of the image. Here we are taking the advantage of the multiple minimum and maximum points of the histogram for embedding purpose. This will increase the embedding capacity. We have embedded the hash into smaller sub-part of the image until embedding is possible. The hash is generated through the some known cryptographic hash function such as SHA or MD5. This will help us to find out the tampered region at the receiver end while extracting the hash, in the case of hash mismatch occur in cover image which will lead to selective rejection of the cover images.

# Contents

# List of Figures

# Chapter 1

# Introduction

Due to increasing of the internet uses and accessibility of digital multimedia content it has became very easy to manipulation of digital content, malicious tampering and copying of software and hardware [15]. It is very difficult to detect the illegal reproduction of multimedia content. From the past decade the Digital Right management is the active field which is used in aiming to stop the theft and tampering of the digital multimedia data. The basic goal of DRM is to detect and possibly prevent the unauthorized access of content of intellectual property rights. DRM is the best and methodological approach for the prevention of the multimedia content. The main idea behind the use of DRM is to protect the unauthorized access of multimedia content.

Digital watermarking [6] is a technique which is used in various documents like as bank notes, postage stamp and legal documents in order to discourage the counterfeiting problem [1]. it is used for the purpose of ownership and copy protection. The reversible watermarking is the extension of digital watermarking. In the reversible watermarking the watermark is extracted and authenticated at the receiver end. If the embedded watermark and hash matches then the image is accepted. In the case of hash mismatch the entire image is get rejected at the receiver side that will lead to authentication failure. This chapter introduces the importance of digital watermarking for the protection of digital multimedia content [15].

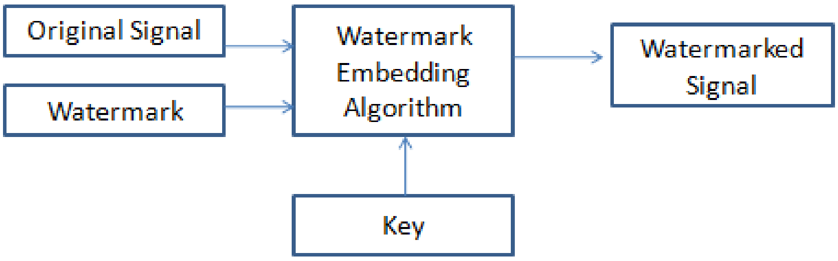


Figure 1.1: Block diagram of General Watermark Embedding System

## 1.1 Digital Watermarking

Digital watermarking [2] is a process in which watermark is embedded into a noise-tolerant signal like as audio or image data. Generally it is used to identify the ownership and copyright. Watermarking is a technique of hiding digital information into the original content. Digital watermarking has several advantages over the traditional encryption system. The traditional security system like as encryption is not able to provide the sufficient protection because they are not able to prevent the unauthorized redistribution and not able to detect the modification once when the original information is encrypted.

Digital watermarking is used for the verification and integrity of the original content [7]. Now days it is prominently used in the tracing, postage stamp and banknote authentication. The watermark embedded into the multimedia content is a logo or a random sequence of an integer bits which is predefined. The Watermark is embedded by some selected bin into the images. This embedded watermark is known by both sender and receiver. To provide some additional security the watermark is embedded through the some secret key. The embedded watermark should persist if is attacked by some common media attack, in order to check its integrity.

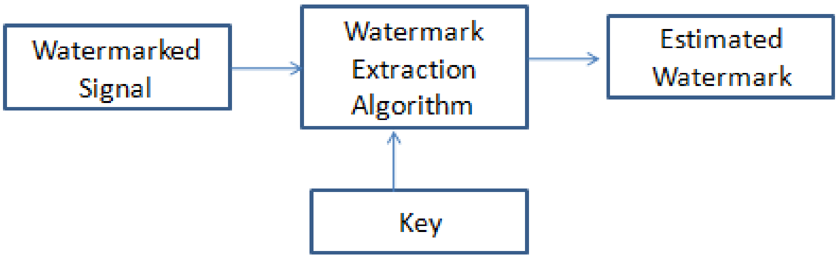


Figure 1.2: Block diagram for Watermark Detection

## 1.2 Reversible Watermarking

The reversible watermarking is the data hiding technique, which is used to recover the original image without any distortion from the watermarked image [8]. The Reversible watermarking procedure is also known as invertible or loss-less data recovery algorithm. The main application field of the reversible watermarking is that scenario whether the originality of the content is needed in order to make a decision on that information basis.

In the reversibly watermarking technique there are two phases one is sender and the second one is receiver. At the sender side we embed the watermark into the original cover image and that reversibly watermarks image is sent to the receiver side. At the receiver side the watermark is extracted and the original cover image is restored. In the next step the watermark and embedded hash is computed. If both Hash and watermark are the same as it was used for embedding, then it is accepted otherwise it is rejected.

Reversible watermarking is a technique for the digital images which is used for the verification of the image integrity, tamper localization and the reconstruction of the original images [4]. For the verification of the integrity of the image we embed the watermark into the original cover image after selecting the LSB of the original cover image, while embedding the watermark into the cover image it is take for consideration that the embedded watermark should be lesser or equal to the highest bin. If the to be embedded watermark is greater than the highest bin it will show the overflow problem. While on the second hand there will be distortion in the original cover image.

In this way we can say that to obtain the reversibility the modified value of original LSBs should avoid the underflow/overflow problem. If there is no tampering in the image then the restored and original image will be the same. The process of reversibility is shown in the following.

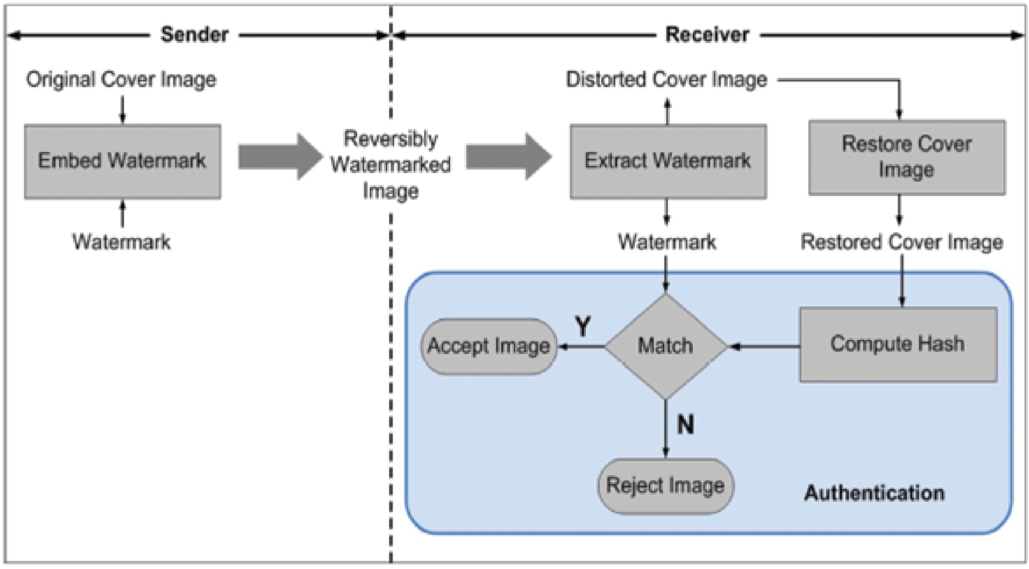


Figure 1.3: General Procedure of Reversible Watermarking System

### 1.2.1 Applications of Reversible Watermarking

The areas where 100 percent recovery of the original image is required, is the main area of reversible watermarking.

- Legal Services.
- Medical diagnosis.
- Broadcast monitoring.
- Copy-right protection.
- Military organization.

## 1.3 Motivation and Problem Description

The basic aim of reversible watermarking algorithm is to embed the secret massage into the cover image by modifying the pixel values and unlike the traditional cover data hiding. The embedded watermark and the original image are to be completely recoverable from the watermarked content. Reversible watermarking technique is the advance version of digital watermarking which is based on loss-less data compression technique.

The reversible watermarking is not only used for the protection of digital multimedia content but also used for the authentication of the content. Reversible watermarking has the several advantage compare to the traditional encryption and digital signature. The reversible watermarking scheme supports the embedding watermarking and prevents to easy separation of watermark from the adversary, while on the other hand in the digital signature is attached to the file with its header. It is easy to delete by the modifying the files or it can be changed by format conversion. The encrypted multimedia content when once they are decrypted there is no further protection against the manipulations.

The reversibly watermarking technique is very useful to find the location of tampering. It is able to detect the location and manipulation of multimedia content where it is done. The embedded watermark is imperceptible so it is not a problem to those people who are not aware of the watermarking [9]. However in the digital signature it is very difficult to detect where the modification has done due to the encrypted signal in the digital images. In Chapter 2 we have discussed the property of the reversible watermarking in details. In general the reversible watermarking should posses the following property [17] Information hiding, Copy protection and tamper localization. The different application emphasizes the different property of reversible watermarking.

### 1.3.1 Copy Protection

In the reversible watermark technique the watermark is used to prevent or discourage the copying and of the multimedia content. Watermark is used to prove the ownership of the certain certificate that they are created by certain user. Legal documents and Broadcasting channels use this technology so that commercials add can be verified and monitored. While using this technique robustness is the important characteristics of the watermark. It should not be easily removed if it is attacked by the some common attack by the adversary.

### 1.3.2 Tamper Detection and Authentication

When there is the need of evidence it should be able to detect the tampering and authentication. The tampering method in the reversible watermarking algorithm finds out the tampered region in the image. At the receiver end the watermark and hash is computed in order to check the integrity of original content. If the mismatch is occurring then it is considered that there is tampering done in the content. For the detection of tampering some special technique is used to verify the content likes as small module checking. By using some loss-less compression technique like as Run Length encoding is used to prevent the multimedia content. It is hard to decode this watermark by adversary.

### 1.3.3 Information Hiding

Watermarking is used for the securely annotate content, like as medical record of disease for privacy protection. The hidden information should be in such a way that is can't be accessed without any prior permission or right, only authorized personnel should be allowed to access the sensitive information. Accuracy and security is the important features for these types of the applications.

## 1.4 Thesis Contribution and Organizations

The objective of this thesis work is to improve the performance of Reversible watermarking by the tamper localization approach. We have proposed an approach to detection of tampered region in the image, using our approach it is easy to reject the selected part of the image due to the hash mismatch and authentication failure. It will reduce the transmission overhead on the communication channel.

Chapter 2 provides background for Digital watermarking and Reversible watermarking technology. It identifies current models in designing a watermarking system and presents the properties that a generic digital watermarking system should have. Furthermore, it describes the applications that this thesis aims to address. The general features of reversible watermarking are also presented in this chapter. The subsequent chapters present the watermarking techniques developed by this work.

1. In Chapter 3, Reversible watermarking based on the Histogram Bin Shifting is presented. We propose an image authentication method to check the integrity of the content. For embedding the watermark in the images we take the advantage of minimum and maximum point of the histogram. Generally the watermark is embedded into the lowest bin of the histogram, because using this point there will be the high embedding capacity. Here is our method we have used the zero point and the maximum point.

2. In Chapter 4, An approach for Tamper localization in Reversible watermarking scheme is presented. Since repeated use of the same watermark is vulnerable to estimation and forgery, there is a great need for a watermarking scheme which incorporates a description of the original signal to guard against copy attacks. An image hashing function for content based watermark generation is proposed in this chapter. It is based on the combination of loss-less compression technique like as Run Length encoding and the Radon integer transform. By using this approach we are able to detect the exact location of tampering. The image region where the tampering has been done, that will be rejected at the receiver end.

3. In Chapter 5, we have presented our Experimental Results. By following our proposed method it is easy to detect the point in the image where the tampering has been done. It will allow the selective rejection of the cover image because of the non

correctable hash value. Watermark embedding introduces distortions in the original signal. For some applications, distortions are undesirable no matter how small they are. We have proposed a tamper localization approach for reversible watermarking technique. In the proposed method we first use the minimum and maximum point of the histogram to embed the watermark. We embed the watermark into the smaller subpart of the image until the embedding is possible. The advantage of our method is that there will be less re-transmission overhead over the communication channel.

Reversible watermarking is especially valuable in as of recently created e-Health Programs, for example, Ontario government treatment Smart Systems for Health Agency, in which private patient data needs to be securely put away and secured. The theory concluded in Chapter 5. It summarizes the Tamper localization advantages of the reversible watermarking techniques presented and proposes possible directions to address for improving the algorithms developed in this work.

4. In Chapter 6, we have presented the Conclusion and Future work. In this chapter we have concluded a tamper localization approach for histogram bin shifting based reversible watermarking. This thesis work may be extended mainly into two area. In the first area the reversible watermarking technique can be improved for the betterment of embedding capacity. This may address to the increasing of the embedding capacity. The second one the tamper localization approach may be enhanced by doing some special operation to the every bin of the histogram image.

# Chapter 2

# Background

This chapter exhibits a review of the digital watermarking and reversible watermarking innovation. It provides the vital material that is required in comprehension of different segments reversible advanced watermarking. Besides, it gives the overview about the impediments in current works and highlights some of the features which this proposal plans in the thesis to address.

## 2.1 History of Watermark

The watermarking system has been developed from the different streams like as cryptography and steganography [15]. The meaning of cryptography is secret writing and the steganography is Greek word which having the meaning of the cover writing.

The cryptography is the method of sending of massage into the distinct form, so the intended receiver can disguise the massage and can read it. The plain text is called the intended massage and the cipher text is called as the disguised massage. The process of changing the plaintext into the cipher text is called the encipherment or encryption and its reversible process is called as the decipherment or decryption. The encryption method is used to protect the original content for the transmission of the data.

Steganography [6] is the art of concealing the massage that should be undetectable. Actually there is no specific way for the steganography. It refers to the secret writing of the massage. Some special kind of the technique is used to write the massage. In this technique the massage is written into some diagonal, vertical or horizontal form. In the old time the onion juice, milk or sympathetic inks are used to write these types of massages, after some chemical affected sympathetic inks were used for writing. This technique was used during the World War one and two. In the ancient time military organization and diplomatic rulers were using this technique. For the secure transportation of theses massages sheets were rolled into the balls and covered with the waxes to covey the massage through the messenger.

## 2.2 Introduction

Steganography is the science that includes conveying mystery information in a suitable multimedia carrier, e.g., picture, sound, and feature documents. It goes under the supposition that if the information is noticeable, the purpose of assault is clear, subsequently the objective here is dependably to disguise the very presence of the implanted information. Steganography has different helpful applications. The information is hided is such a way that it should not be visible by seeing in the normal way, some special technique are used to hide the secrert information. Some special technique is used to read this massage like as putting some lights and making some angles while reading such type of information.

The ultimate goal of the steganography is that it should be undetectable, robustness and able to conceal the information. These are the factor that separate it from the other technique like that watermarking and cryptography. This chapter provides the cutting edge review and analysis of different steganography technique alongside some basic benchmarks from literature. This paper gives a cutting edge audit and examination of the distinctive existing routines for steganography alongside some basic benchmarks and rules drawn from the writing. This paper concludes up with a few suggestions and support for the article to embedding of the information. Steganalysis, which is the investigation of attacking steganography, which is further discussed in this chapter. The three techniques which are associated to each other are steganography, watermarking and watermarking. The following Figure shows the traditional procedure of the information hiding, in the next the table gives the comparison of these technique.

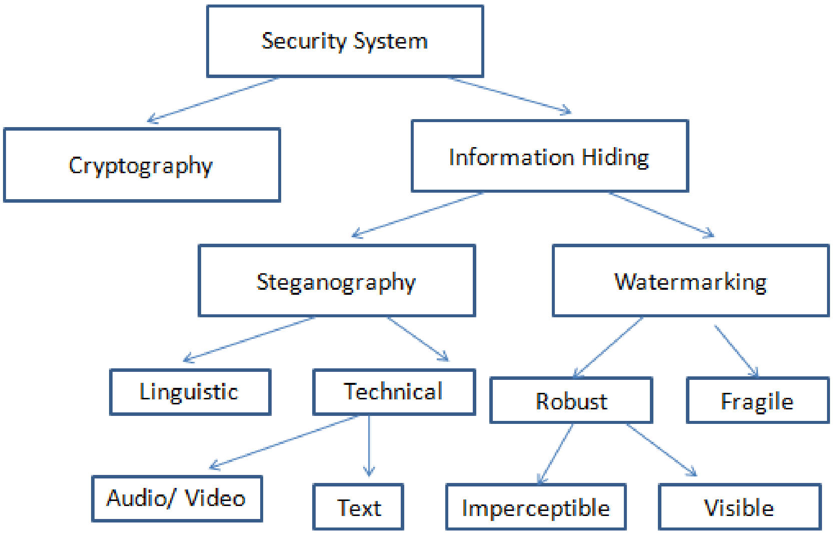


Figure 2.1: The different Embodiment method of Information hiding

## 2.3 Comparison among Steganography,Watermarking and Encryption.

| Method/Criterion | Steganography | Working method | Encryption method |
|---|---|---|---|
| Carrier | The digital media | Mainly image/audio | Mostly text sometimes image files |
| Secret data | Embedding | Watermarking | Plain text. |
| Key | not necessary | Not necessary | Needed |
| Authentication | Complete retrieval of data | Data usually achieved through cross | complete retrieval of data is needed |
| Objective | Hidden communication | Copyright preserving | Data protection and integrity |
| Result | Stegano-cover | Watermarked-cover | Cipher-text |
| concern | capacity | Robustness | Robustness |

## 2.4 Digital Watermarking

The term watermarking is regularly identified with data concealing. The watermarking offers numerous procedures and properties. Their disparities rely upon the configuration logic and the particular applications. Information hiding is not only the property of watermarking but also used to keep the information secrecy. This way we can say that, the term data concealing regularly covers both steganography and watermarking. Steganography is the specialty of disguising data [25]. One of the differences between the steganography and watermarking is that a watermark usually conveys the possession data and keeps the ownership information though steganography is utilized to convey the information between two or more parties. Likewise, a watermark may need to survive to certain attacks when the cover document is harmed. In generally we can say that the watermarking procedure for the multimedia data needed the different methodology. For watermarking the images, audio and video different technique is used. To address the digital watermarking problem in the communication channel many models has been developed. The model based on the communication channel is shown in the following figure, where the watermarked massage is transmitted over the noisy communication channel. In this phase the watermarked massage is decoded to the receiver end to check the integrity of the massage.

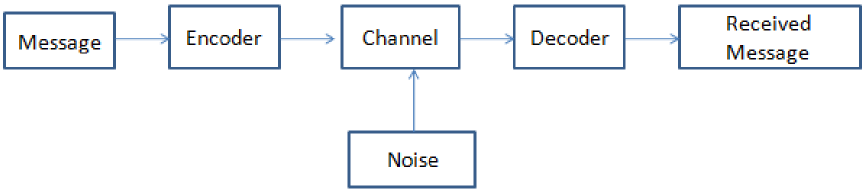


Figure 2.2: Block diagram of a Communication Channel

The problem is here that to design such a channel encoder and decoder which can ensure the correct detection of watermark at the receiver end. In this model assumption is that the original signal and the watermark are independent of one another. However, this is usually not the case because the embedding algorithm is generally dependent on the cover signal. For example, watermarking of images and audio requires different methodologies [26]. Therefore, the channel encoder can be modified to incorporate side information from the cover signal.

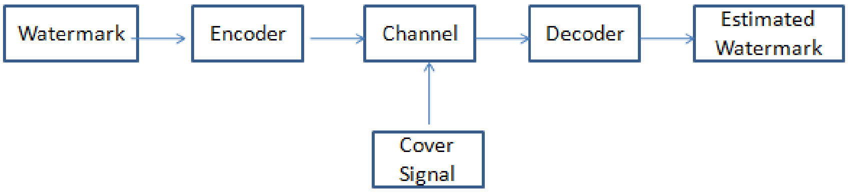


Figure 2.3: Block diagram of a Watermarking System analogous to Communication Channel

The watermark embedding algorithm is the most robust and effective. Watermarking methods which target specific applications, such as image authentication method that is robust against various attacks is an example of this class of watermarking system.

## 2.5 Evaluation of Watermarking System

A watermarking framework has various necessities. Clearly, difference applications have distinctive concerns; consequently, there is no set of properties that all watermarking frameworks need to fulfill. This section highlights the common assessment techniques used for watermarking frameworks and shows why they are essential.

### 2.5.1 Perceptual Transparency

Embedding extra information into the original images will lead to the degradation in image quality. In many applications, such as transmission of the watermarked image, it is often undesirable to have perceptual distortions. The watermark is truly imperceptible if humans cannot distinguish between the original cover image and watermarked image.

The watermark should not be visible by human visible system. If the embedded watermark media is visible it is easy to make forge such type of the watermark. The best way to evaluate invisibility of watermark is to conduct test where both original and watermarked signals are presented to human subjects. However, due to the high volume of test images, subject tests are usually impractical. The most common evaluation method is to compute the peak signal-to-noise ratio (PSNR) between the host and watermarked media.

### 2.5.2 Security and Effectiveness

The digital watermarking system is the dependable upon the input multimedia content. The term effectiveness is generally considered that it should be able to detect the watermark embedding process. When the watermark is applied to the multimedia content it should not be extracted without a correct user key. The term security refers to that the location of embedding of the watermark should be undetectable. One of the major goal of the digital watermarking is to protect the multimedia content from the illegal use and distribution.

### 2.5.3 Unambiguous

Once the watermark is embedded, while extracting of this watermark at the receiver end, it should be able to identify the owner. In addition, the accuracy of owner identification will degrade gracefully under the tampering attacks. Unauthorized removal of the watermark will lead to the rejection of the content at the receiver end. The goal of watermark is to make undetectable to this.

### 2.5.4 Tamper Verification

The watermark media is send through the some communication channel, if the communication channel is prone to the attack then it should be able to detect the tampered region of the content. The tampering operation on the multimedia content is used to detect the copyright protection.

### 2.5.5 Robustness

Robustness is the one of desirable property of the digital watermarking system. The watermark must be still presented if it is attacked by some common attack. Robustness refers to ability of detector to detect the watermark after the distortion. If the format, version and some changes is done on the multimedia content it should be able to detect the watermark. Although it is difficult to make watermark completely robust against all the signal processing attack, but protect to watermark some lossless compression and conversion technique is used to make it robust.

## 2.6 Target Applications

The watermarking technique and its requirement mainly depend upon the target applications. This section discuss about proposed method application: those are content authentication and privacy protection, which are discussed later in this section.

### 2.6.1 Content Authentication

Due to rapid increasing in technology the manipulation of digital multimedia content has became easier. The originality of content has become difficult to manage. Content authentication is needed in the case of forgery whether the integrity is important key for it. Integrity is needed to for the protection of multimedia content. Many techniques are used for the protection of content. The content are protected using some special technique like as watermarking, digital signature where the original contents are attached to this procedure. If the contents are changed then it should be able to detect its originality.

The drawback of some traditional cryptography method is that the attached signature with this massage is not robust. The manipulation can be done using the some common attack like as format changes and signal attack. The overcome of this problem is digital watermarking. The digital watermark where the signature of massage is embedded into original file, while using this approach it is not possible to remove the signature from the massage. There is no need of transmit the and store it separately. The Watermarking fill the gap between these two methods.

### 2.6.2 Privacy Protection

The medical industries deal with sensitive information where the personal information is stored in the electronic form. This sensitive information must be protected from the unauthorized use of it. There should be privacy protection and control access of these data. If we go the protection of these data through the watermarking it reduces the chance of being manipulation and alteration of it. It also provides the control access of the data. A loss-less watermarking system is used for the protection of such data from unauthorized retrieval.

Digital watermarking procedure is widely known for the authentication which is reported in this background survey.The traditional watermarking procedure suffers from the some drawback, while appending the signature with the massage it increases the size of the file and it is also can be removed from the massage. This procedure is not able to detect the manipulation. The digital watermarking is the overcome of the above problem. The watermark is known as the recognizable image pattern [23]. It appears on the various lights. It appears in lightness/darkness. When a transmitted light is put on this watermark appears. Basically watermarks are two types which are visible watermark and invisible watermark. The visible watermark can be seen by the human naked eyes [28]. It is visible to human visible system. When the light is transmitted on this it became visible. The invisible watermark is not visible to human visible system. It is embedded using some special technique like as histogram bin shifting. Due to security reason the invisible watermark should not be able to identify through human visible system. The invisible watermark is kept as backup for the visible watermark for the case of authentication purpose.

Watermark is used in many documents like as postage stamps, documents, currency. It is used to discourage the counterfeiting problem. The advantage of the digital watermarking is that after embedding of the watermark the file size remains intact. The watermarking scheme is very sensitive to detect the tampering; while some modification has been done on the content it is able to detect the tampering. It is used to authenticate the integrity of the content. A good authentication system should posses the following properties which are tamper detection, tamper localization and perceptual transparency. Tampering identification is one the main property of the watermarking, in this the watermark are embedded which are invisible to human eyes. Any alteration did on the multimedia content can be found out while decoding this watermark at the receiver end. This watermarking technique is used in the military organization, legal services and those industries which are dealing the sensitive information. The techniques which are used in the application are not robust to detect the slight modification [14]. These watermarking system are called the fragile watermarking system.

The aim of reversible watermarking is to embed the secret massage into the multimedia content. The performance of reversible watermarking is evaluated in the ability to detect the of modification. Basically the loss-less compression technique is used to embed the watermark. The histogram based methods is used to embed the watermark in which some bins are shifted to create the some space for embedding. After creating the spaces the in these empty bins the watermark is embedded. For embedding the watermark we take the advantage of the minimum and maximum points of the histogram of the images. This scheme utilizes the zero point of the histogram by choosing this point we can embed the more bit in that empty bins. In the next chapter 3 the histogram bin shifting for reversible watermarking method is described.

## 2.7 Attacks on Watermarking

The basic aim of any watermarking is to provide some degree of security that can negate the some attack. Here we have mentioned some kind of weakness of the watermarking system [8]. These methods find out the some weakness of the watermarking system and address some solution to these problems that affect the current watermarking system procedure. In the watermarking segment if the attack is in processing of the communication of information it is easy to find out these types of attacks [10]. In this system of communication the owner of content tries to send the data to receiver thinking that there is sufficient high data quality, while on the other hand the adversary tries to impair watermark communication between these two parties. Therefore the communication system may be the game between these two party sender and receiver. The modeling of the communication system and resisting of attack may be the solution of these problems.

### 2.7.1 Classification of Attacks

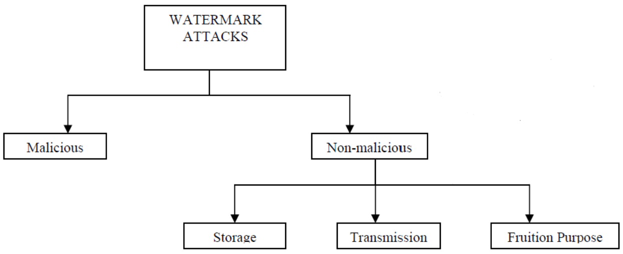


Figure 2.4: General Classification of Watermark Attacks on the Basis of Intent

There are basically two types of attack on the watermarking, the first one is On the Basis of Intent and the second one is the malicious attack. On the Basis of Intent attack is categorized as the non malicious attack. This type of the attack is called as the unintentional attack. The aim of the attacker is just to obtain the information. Many strategies are used to achieve the massage. In this the adversary illegally tries and uses the content of the massage. It is form of the passive attack. The other type of attack is the malicious attack. The basic goal of attacker is to harm down the watermark and make it to unrecoverable. The malicious attack is said to be blind because the adversary tried to remove the watermark from the media. The adversary estimates the copy of content and adds some noise to media. The adversary nullifies the effectiveness of the watermark.

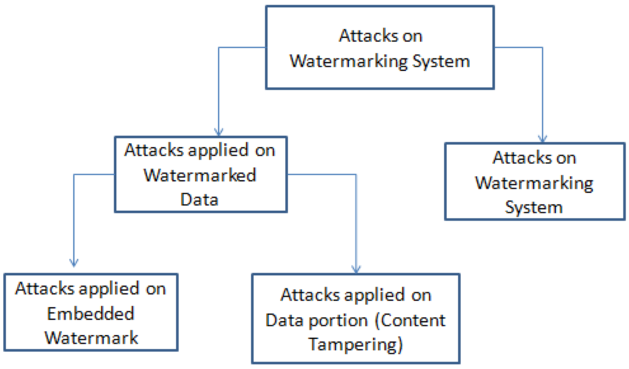

Attacks on Watermarking System
Attacks applied on Watermarked Data
Attacks on Watermarking System
Attacks applied on Embedded Watermark
Attacks applied on Data portion (Content Tampering)

Figure 2.5: Classification of Watermark Attacks on the Basis of Attacking Target

## 2.8 Observations

| Method | Descriptions |
|---|---|
| Spatial domain | • Not robust against the lossy compression.<br>• Not robust against rotation and cropping.<br>• Not robust against the noise.<br>• Mainly works on the BMP format. |
| DCT based domain technique | • Less prone to attack.<br>• Robust against rotation and cropping.<br>• Double compression of the file.<br>• No robust against noise.<br>• Works only on the JPEG format. |
| Watermarking technique | • Embedding of watermark for security.<br>• Embedding space used for robustness.<br>• Resistance to loss compression.<br>• Embed secret data for with secret key.<br>• Provide security for statistical attack. |

## 2.9 Chapter Summary

in this way we can say that embedded watermark should be perceptual transparent, it should not be visible to human visible system. It will be imperceptible if human naked eyes cannot differentiate between the watermarked image and original cover image. Once the watermark is embedded while extracting this watermark it should be able to identify the owner. Watermark should also be unambiguous, unauthorized removal of the watermark will lead to the authentication failure. One of the major property of watermark is that is should be able to detect the tampering in multimedia content. These are the desirable property of the watermark which is concluded in this section.

# Chapter 3

# Reversible Watermarking Algorithm based on Histogram Bin Shifting

The reversible data hiding algorithm is used to recover the original images, from the watermarked image without any distortion after the authentication. This approach of the reversible watermarking utilizes the minimum and maximum points of histogram of the image. The histogram gray scale values are slightly modified to embed the watermark in the image histogram [20]. Data hiding process refers to the hide the information into the cover media. The reversible watermarking technique should satisfy the criterion like as lossless, distortion free and invertible data hiding [12]. This criterion should be fulfilled while extraction of the data at the receiver ends.

## 3.1 Reversible Watermarking

The reversible watermarking technique is first used in the spatial domain technique. In this spatial domain technique it uses the modulo 256 addition technique to embed the hash into the cover image. It is used for the authentication purpose. The embedding formula for this approach is the following.

Iw = ( I+w)mod 256.

Where I= Original image.

Iw = Watermarked image.

W= W(H(I).K).

W = Watermark.

H(I) = Hash function applied on the image.

K= Secret key.

The purpose of using the Modulo 256 addition is to prevent the overflow and underflow condition and to achieve the reversibility. The reason for using this method is that because the gray scale value flips between the 0 and 255.

The other reversible watermarking technique is loss-less compression technique. In this technique some bits are compressed to leave the space to embed the watermark in the image, this is done because the book-keeping information of data is also hidden in the image [24]. The goal of the watermarking technique is to authenticate the information so hidden data are limited. It is also base on the modulo 256 addition technique, because of following this approach it suffers from the salt and pepper noise [18]. In this way we can say that this technique is not useful in many applications. This method is valid till to all those data hiding technique which uses the modulo 256 addition for reversibility.

The reversible watermarking technique which is best suitable for embedding of large amount of data is presented in this chapter [27]. It divides the image into non overlapping of blocks to embed the watermark. In order to achieve the reversibility in data hiding scheme the histogram modification technique is used. It is used to prevent the overflow and underflow of the data in the image [11]. This algorithm uses the zero or minimum point of the histogram to embed the watermark in the image. This technique can be applied virtually to all the standard images. Here in the our thesis we have taken all the images from the standard image database like as SIPI image database, CorelDraw and UGR image database.

## 3.2 Histogram Bin Shifting based Reversible Watermarking

Here in the reversible watermarking based on the histogram bin shifting for the embedding algorithm we are taking one zero point and one peak point [13]. The procedure of embedding the watermark into the image is the following.

1. In the histogram of the given image we first find out the zero point and the maximum point. A zero point says that at the particular gray-scale value having no pixels. In our case this value is h (255) as shown in the histogram. The peak point indicates the gray-scale value having the highest frequency. The maximum number of pixels is associated with this gray-scale value, that point in mine case is h (154). Here the aim of the finding the maximum and minimum point as to increase the embedding capacity as much it may be possible. The maximum number of watermark bit that can be embedded in the image may be equal or lesser than the peak point. If we go for the embedding more than the peak point then there will be distortion in the images. Then we can say that the embedding capacity more than the highest bin is not possible.

2. The complete image is scanned in the some particular sequential order like as column by column or row by row or left to right or right to left, it does not matter in which order image is scanned. The gray-scale value from the minimum point to maximum point is incremented by one unit to the right side leaving the maximum bin empty for embedding the watermark in the maximum bin. This step is used to make the maximum bin empty. The reason for shifting the histogram to the right hand is that the minimum point is the right side to the maximum point. In some case this may be to the left side.

3. The complete image is scanned the same again in that particular order as it was previously done. While scanning the image if the pixel value to the maximum point like as h(154) is encountered and the to be embedded bit sequence is one, the pixel value is counted and it is incremented by one. In the other case if the to be embedded bit sequence is zero then its value remain unchanged. The pixel values remains intact. This process is done till the complete image is scanned.

These three method who are presented above complete the data embedding process. In this way we can say that the data embedding process utilizes the minimum and

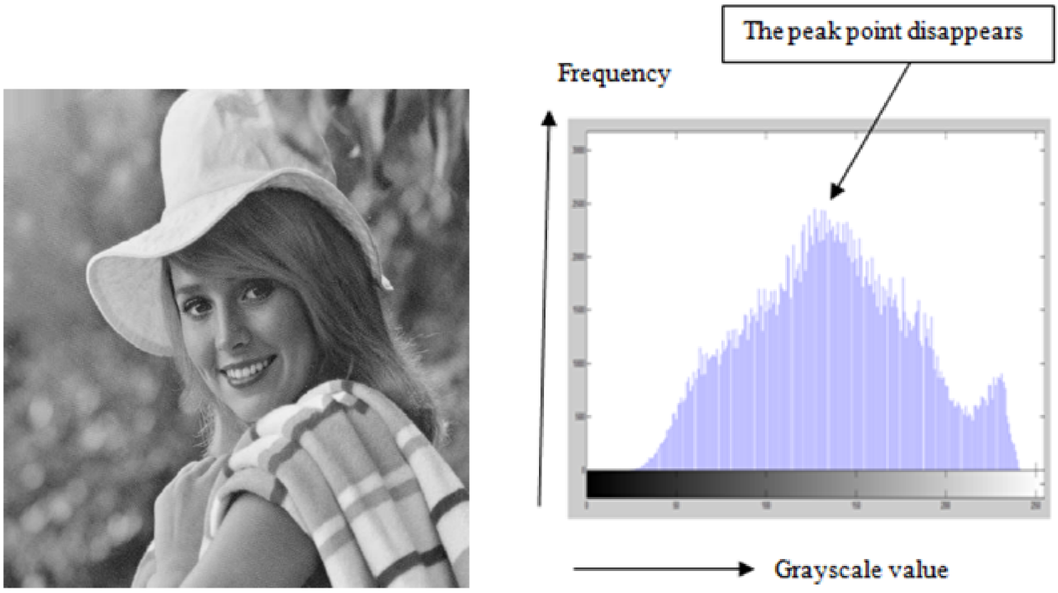


Figure 3.1: Lena Image 512x512x8 and Histogram of the Lena image

maximum points. Further steps are the following.

## 3.3 Embedding Algorithm

We know that the zero point may not be exists in the case of every images. Here we are taking the concept of the minimum point [28]. This point shows that there are the minimum number of the pixels which are associated with that gray-scale value.For the MxN image in which each pixel gray-scale value $\epsilon(0, 255)$.Further steps are the following.

**Step 1:** Generate the histogram of the image H(x).

**Step 2:** In the generated histogram of H(x) find out the minimum and maximum point of the histogram in which the maximum point h(a) a $\epsilon(0, 255)$(0,255) and the minimum point h(b) b $\epsilon(0, 255)$ (0,255).

**Step 3:** The minimum point h(b) in the given image if h(b) ¿0 then find out the co-ordinate of those pixels and set this value as h(b)=0.

**Step 4:** Shift the whole part of the histogram to the right hand side by one unit leaving the maximum bin empty. This process is done to make the spaces for the embedding.

**Step 5:** The image is scanned in the particular sequential order, while scanning the image if the pixel value with the maximum value h(a) is encountered and the to be embedded bit sequence is one, the pixel value is counted as one and the pixel value is incremented by a+1. This step is equivalent to the consideration of the frequency. If the to be embedded bit is zero then its value of pixel to that gray-scale value remains unchanged. Following this approach we embed the watermark bit sequence in the images.

### 3.3.1 Embed Watermark

1. For MxN image, each pixel x $\epsilon(0, 255)$(0,255).
2. Generate H(x)← mxN image.
3. Find Min point h(a)← H(x).
4. Max point h(b)← H(x)
5. If h(b) is greater than zero, then then set h(b)=0.
6. H(x)← H(a)+1.
7. If to be embedded bit=1.
8. Then H(x)= a+1.
9. Otherwise H(x)← a.
10. End.

### 3.3.2 Flow Chart for Data Embedding Algorithm

In the given image first we plot the histogram of the image and the counter value is initialized to one. In the next step we find out the maximum and minimum point of the histogram [19]. After this we check the embedding payload, if it is enough then we embed this into the image. If the to be embedded payload is not enough then the counter value is incremented by one and the to be embedded bit is checked if it is enough then it is embedded [29]. Although if it is not enough then it lead to the failure.

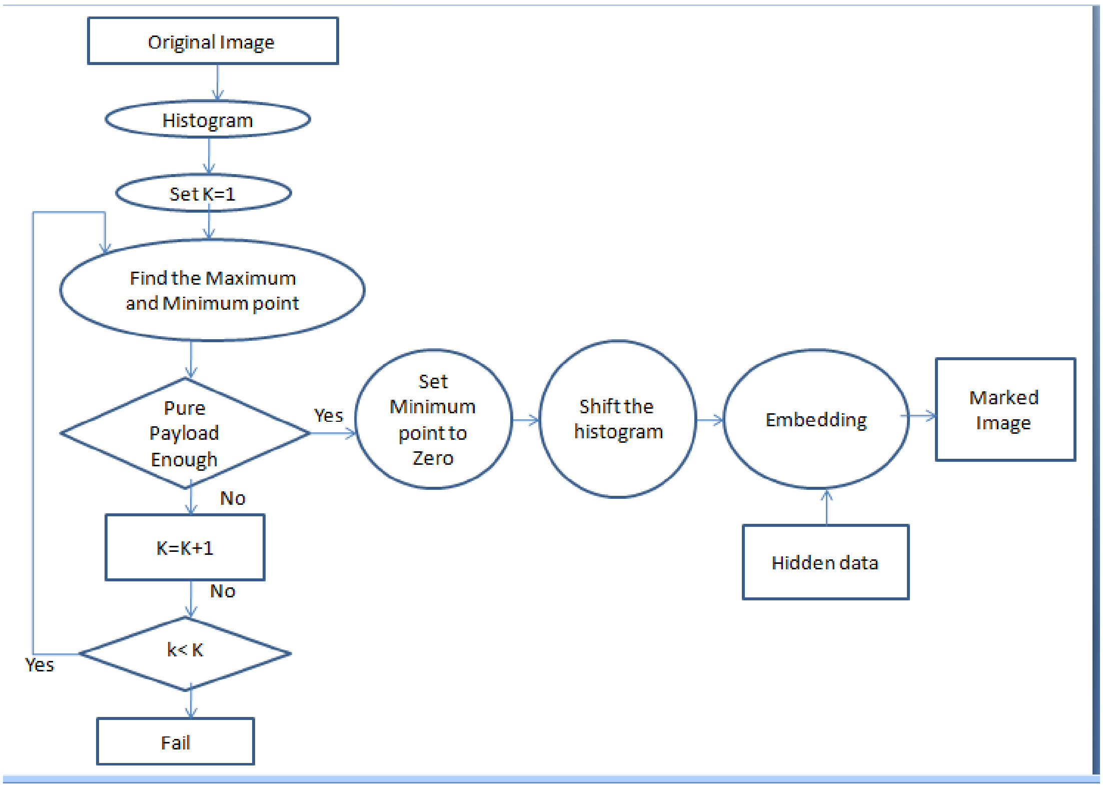


Figure 3.2: Flow chart for Data Embedding Algorithm

After finding the minimum and maximum point of the histogram, if the minimum point is not zero then the minimum point is set to be zero and the histogram value is shifted to make space for embedding. In the next step embedding is done in the histogram and the given original image is watermarked.

## 3.4 Extraction Algorithm

For the given image we have the maximum point is a and the minimum point is b. The watermarked image MxN where the pixels gray-scale value x $\epsilon(0, 255)$. The procedure for extracting the watermark is the following.

Step 1: Scan the watermarked image same sequential order as the embedding was done.

If the pixel with the gray-scale a+1 is encountered then the watermarked bit 1 is extracted, on the other hand if the pixel value a is encountered then the bit zero is extracted.

Step 2: In the next step we scan the image once again in same particular order for any pixel whose gray-scale value x $\epsilon(0, 255)$[a,b] is encountered then value is subtracted by the 1. In this way we obtain the original cover image from the watermarked image. If there is no modification in the image we gets the original image and it will support the integrity of the image. This will lead to the authentication of the image.

### 3.4.1 Extract Watermark

1. For MxN image where x $\epsilon(0, 255)$(0,255).
2. If H(x) $\leftarrow$h(a)+1.
3. ]Then H(x) $\leftarrow$(a)-1.
4. Find h(b) $\leftarrow$ minimum of h(b).
5. Authenticate the watermark.
6. Original cover image is found.
7. End.

### 3.4.2 Flow Chart for Extraction Algorithm

The watermarked image is scanned in that particular order as the embedding was done in the original cover image. In the next phase the embedded data are extracted and histogram is shifted back. After shifting the histogram back the minimum point of the histogram is restored and the watermark is authenticated. This way the original cover image is recovered. This is the procedure of the extraction of the watermarked from the watermarked image.

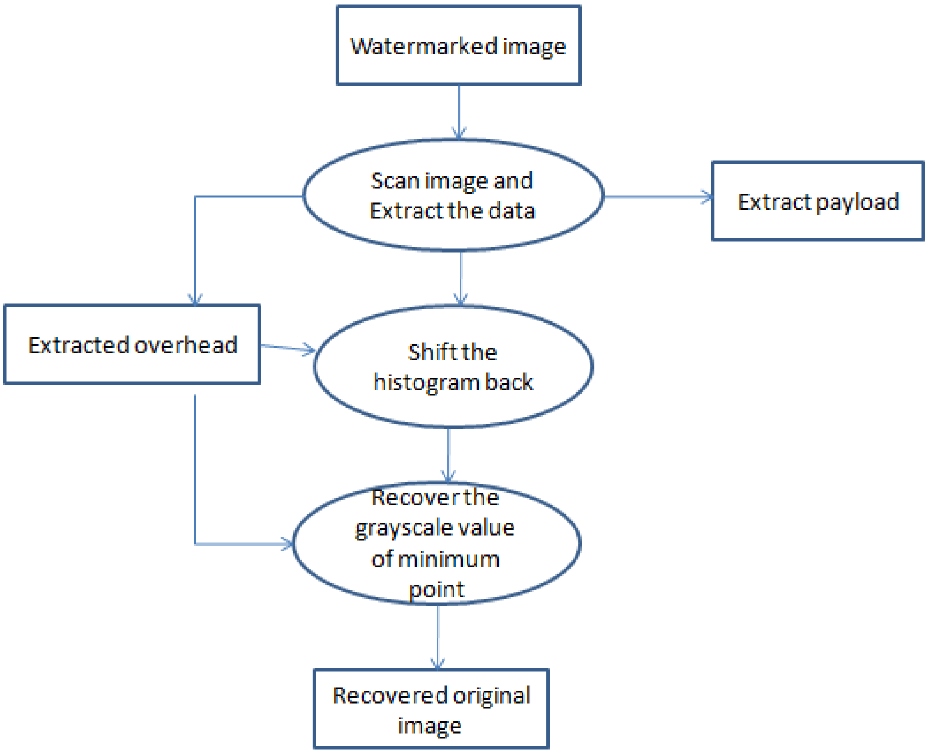


Figure 3.3: Flow chart for Data Extraction Algorithm

## 3.5 Proposed Enhancement for Reversible Watermarking Algorithm based on Histogram Bin Shifting

In this method we have proposed an enhancement to the reversible watermarking based on histogram bin shifting [5]. It enhances the embedding capacity of the watermark in the images. Basically in the reversible watermarking algorithm has two states, in which one is sender and second one is the receiver. In the first phase the watermark is embedded into the original cover images after watermarking these images it is send to the receiver end. At the receiver end the watermark is extracted and hash is computed. If the extracted hash and the watermark matches then the image is accepted at the receiver end. In the case of hash mismatch it leads to the authentication failure then the image is rejected at the receiver end. This way we know that the embedding information is based on the shifting of the pixels. To embed the watermark in the shift the pixels gray-scale to create some spaces to embed the watermark. The points which are left or right to maximum point those points are chosen for the embedding.

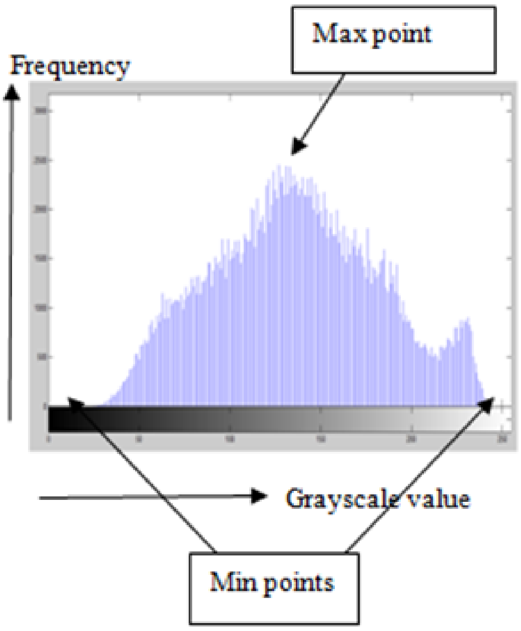


Figure 3.4: Histogram of the Image

Here in this approach we are taking the advantage of the multiple minimum points. By choosing multiple minimum or zero points the embedding capacity is improved. But in this case that minimum point is taken which is close to the maximum point, because taking this point there will be the minimum distortion in the image. This is also one of the desirable properties of the reversible watermarking. In the above histogram we have taken 512x512x8 image where the two minimum points are shown.

## 3.5.1 Histogram Bin Shifting

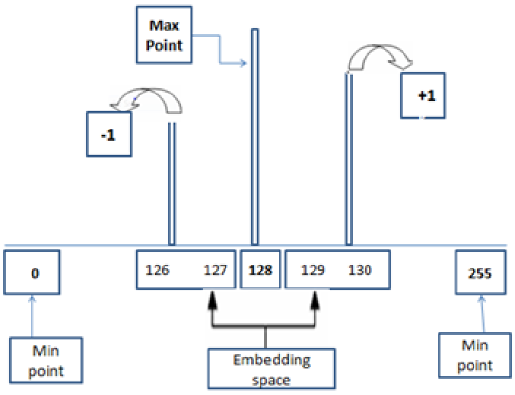


Figure 3.5: Histogram Bin Shifting Mechanism

In this approach of the histogram bin shifting the histogram bins are shifted to left or right to create some spaces for embedding. The bins value are shifted to left or right by one unit to create some spaces for embedding [28]. At the receiver end the original image is easily get retrieved if we know the minimum point and the embedding information which were used for the embedding purpose before the watermarking. The procedure for creating the space and embedding of watermark is shown in the above Figure.

### 3.5.2 Embedding Algorithm

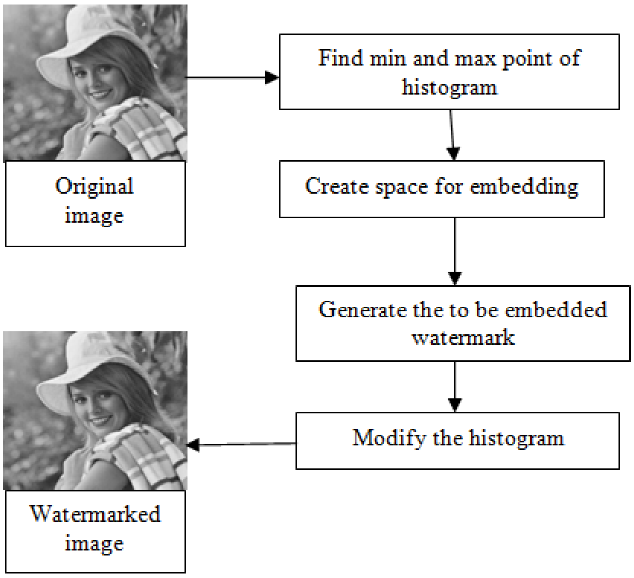

Original image
Find min and max point of histogram
Create space for embedding
Generate the to be embedded watermark
Modify the histogram
Watermarked image

Figure 3.6: Procedure of Data Embedding Algorithm

In this procedure of embedding the minimum and maximum point is selected for embedding the watermark in the histogram. After that histogram is shifted left or right according to the minimum point. In the next step the watermark is generated through the well known cryptographic hash function and they are embedded into the image histogram. This way the histogram is modified and image is marked. Watermarked image is send to the receiver end.

### 3.5.3 Extraction and Recovery Algorithms

The procedure of extraction and recovery is shown in the following Figure. At the receiver end from the watermarked image the maximum point is selected. After selecting the maximum point the watermark is extracted and we find the embedded location and minimum point is restored. In the next step the watermark and the hash is computed, after the authentication of the hash and watermark image is accepted. In this way histogram is shifted back and the original image is recovered.

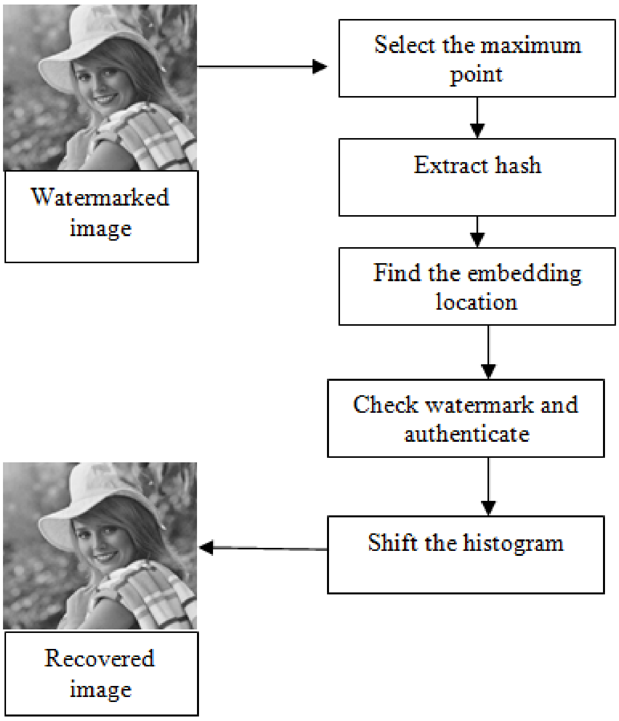


Figure 3.7: Extraction of Watermark and Recovery process

## 3.6 Chapter Summary

In this way we can say that the reversible watermarking is need of secure multimedia content. The watermark is needed for checking the integrity of the massage. Histogram bin shifting us used to embed the watermark in the images. By following this approach the embedding capacity is improved, this will lead to security of the content. The minimum and maximum point plays the very important role in the embedding of watermark in the image.

# Chapter 4

# An Approach for Tamper Localization in Reversible Watermarking

In this chapter we have proposed a tamper localization approach for detection of tampering in the reversible watermarking technique [22]. The need of tamper localization against the forgery in the reversible watermarking plays a very important role in this scheme. The content dependent watermarking scheme is also able to detect the forgery. Our proposed approach is able to detect the exact location of the tampering. Here we are using the hash based function to generate the watermarks [3]. It is the combination of random integer function which produces the random numbers. The property of being random it is not easy for adversary to find out these sequence numbers.

## 4.1 Preliminaries

The reversible watermarking algorithm embeds the watermark for protection of the multimedia contents [16]. While at the receiver end the decoder rely the knowledge of this watermark that they are in order and make the authentication on the basis of correctness of this watermark. The correctness of the watermark is the serious concern for protection of the watermark. The possible way to detection of the tampering in the reversible watermarking is the checking of the integrity of the watermark. At the receiver end watermark is compared with the original one. If it validates the originality of the watermark then it is said that tampering is not done in the images. In the approach the image is watermarked using the hash function and the help of the key. After watermarking the image it is send to the receiver end. On the watermarked signal

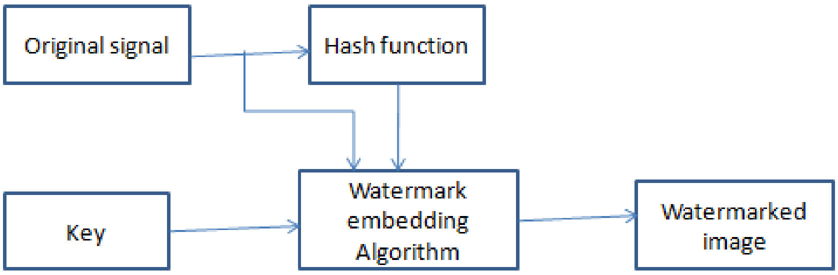


Figure 4.1: Watermark Embedding

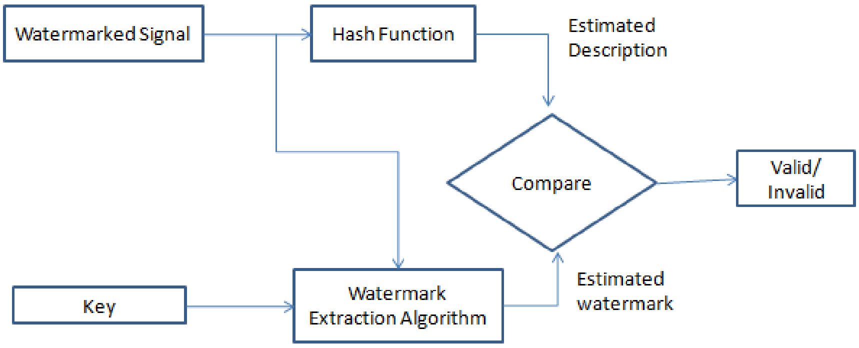


Figure 4.2: Detection System using of Hash function

the hash function and key is applied and the watermark is extracted, then it compared with the existing watermark and embedded watermark. If both watermark matches to each other then the image is accepted at the receiver end. This approach validates the watermark for the acceptance of the image.

## 4.2 Existing Work and Limitations

The challenge in the reversible watermarking is that the watermark should persist during the transmission and format changes. The general convention of reversible watermarking says that the entire image is get rejected at the receiver end due to the authentication failure. When the hash mismatches occur then it lead to the authentication failure. There is no particular ways who can detect the exact location of tampering. Our proposed method that is presented in this chapter is able to detect the exact location of the tampering. In our method we are embedding the watermark in the image with the help of the hash function. The hash function generates the bit sequence of watermark which is embedded into the image. For the tamper localization approach

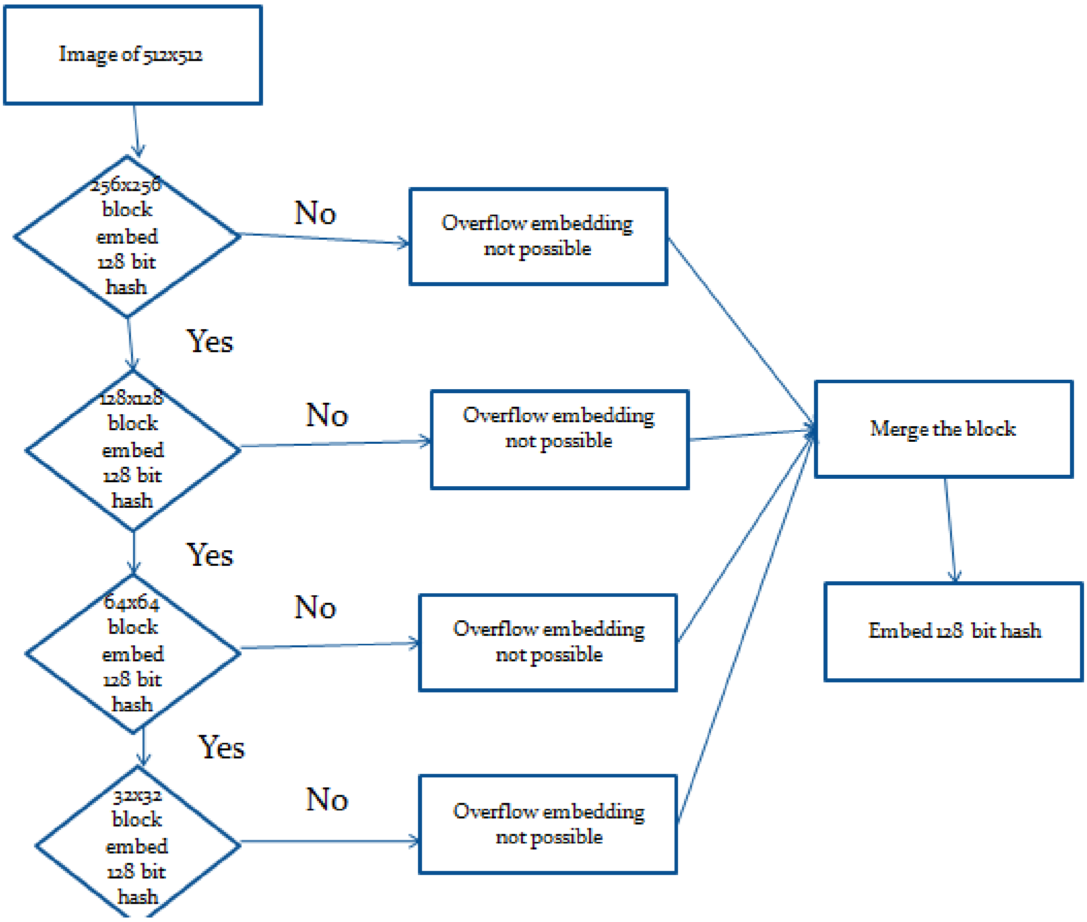


Image of 512x512
256x256 block embed 128 bit hash
No
Overflow embedding not possible
Yes
128x128 block embed 128 bit hash
No
Overflow embedding not possible
Merge the block
Yes
64x64 block embed 128 bit hash
No
Overflow embedding not possible
Embed 128 bit hash
Yes
32x32 block embed 128 bit hash
No
Overflow embedding not possible

Figure 4.3: Block Merging Technique

in the reversible watermarking we go for the block division approach. In the block division approach we divide the image into smaller block size up to embedding is possible. The blocks where the embedding is not possible those blocks are merged into one blocks. After merging the blocks the watermark is embedded into the merged block [21]. This approach helps us to find out the tampering in the image, while the embedded watermark is extracted is on the receiver end.

Although this technique is not much efficient to detect the tampering which done in the during the transmission [24]. It is not able to detect the exact location of the tampering. The method which we have proposes in this chapter is able to detect the exact location of tampering. By following our approach it is able to detect the tampered region in the image. This way we can say that our method is more efficient than the existing method.

## 4.3 Proposed Method for Tamper Localization

The general consideration of reversible watermarking is that the entire image is get rejected in the case of authentication failure. When the hash mismatch occurs the complete image is rejected at the receiver end. The solution of this problem is proposed in this section. By following our approach there will be the selective rejection of the cover image. The selected part of the image will be rejected due to the hash mismatch and authentication failure. In our proposed method we have selected the two private key for prevention of unauthorized access of the images.

The first key used here is to encrypt the hash value. This key compresses the hash value without losing its integrity. He we are using the loss-less compression technique that is Run Length encoding. This technique runs over the data. Without losing data integrity it compress the repetition of the data. The repeated data are counted to single bit and it is represented to one bit. This method takes the advantage of the repetition of bits; many consecutive elements are counted to one. The second key is used to generate the random sequence of the integers. It generates the random bit of integers; it is quite easy to adversary find out the same bit sequence to decrypt the information.

### 4.3.1 An Approach for Tamper Localization

For ease of embedding and extraction of watermark, for tamper localization we divide the cover image uniformly into equal sized blocks. In the proposed approach if the block size is smaller with the embedded hash then the location of tampering is be more accurate. The embedding process is carried out on the sub-part of the image as long as it is possible. While extracting this watermark it is easy to find out the tampered block with exact location of tampered image region.

Here we are using 128 bit MD5 hash to embed into the complete cover image. The purpose of using 128 bit MD5 hash is primarily security feature enhancement due to its key nature. It supports the pre-image resistance and collision resistance. This is discussed in detail in the following section.

### Resolution of Tamper Localization

The smaller tamper localization of blocks, there will be higher accuracy of locating the the tampered region. This is happening due to the smaller part of the image is embedded with the watermark, while extracting these watermark at the receiver end if there is hash mismatch these selected block will be rejected at the receiver end.

### Uniformity in Block Sizes

If there is uniformity in the block sizes then it will be easy to embedding and extraction of the watermark. In this approach we have divided the cover image into equally size of blocks through the complete image region. This approach is uses in the reversible watermarking in order to make ease of it. The uniformity of blocks is maintained by embedding the equal size of the hash bit into the complete cover image. We know that there are some regions in the image blocks in which we can embed more number of bits while on the other hand there are some blocks in which embedding may not be possible due the limitation of embedding capacity.

The main goal of any reversible watermarking algorithm is that it should be able to restore the original cover image back to its original form. The addition retrieval information is needed in order to get the reversibility of the image. Hence we can say that the uniformity of the blocks is needed to find out the tampered region in the images.

## 4.4 Using 128 bit MD5 Hash

To generate the hash value we use the some well known cryptographic hash function. We can use the SHA or MD5 hash algorithm. Here we are using the 128 bit hash function to generate the random sequence of the integers. The reason for using this approach is mentioned below.

### Pre-image Resistance

According to the pre-image resistance property the hash function it implies that for a given hashed value, it is not easy for adversary to compute the pre-image of the hash.

In mathematical order we can say that, a hash value function h, is said to be pre-image resistance if the given value of Z=h(x).
For same x it is difficult to compute the value of any $x'$ such that h$(x')$ =Z. This is not quite possible for adversary to find out both value should be the same.

### Collision Resistance

Property of collision resistance hash function implies that when two value x and $x'$ are such that x is not equal to $x'$. It will be difficult for adversary to find out the value like h(x) = h$(x')$. It is not easy to adversary to find the collision for which value is different. This way we can say that using this approach it will not be easy to adversary to find out these values. Here some special type of technique is used to protect the data. After generating these values we use the other secret key which is used to compress this value. A loss-less data compression technique like as Run Length encoding is used here.

## 4.5 Procedure for Embedding Hash

To embed the hash into the cover image we divide the cover image into the smaller block size and embed the hash into the smaller block size up to embedding is the possible. The algorithm for embedding the hash into smaller block size is the following.

### Procedure

Step 1: Divide the cover image into uniform tamper localize blocks.

Step 2: For each block B do.

Step 3: Compute hash H $\leftarrow$Hash B.

Step 4: Embed H into B.

Step 5: If embedding hash into block B is not possible, then.

Step 6: Find (min, max) pair of gray scale values in block B.

Step 7: Embed hash into every block B.

Step 8: End.

This is the procedure of embedding hash into the image. For embedding the hash into the smaller sub part of the image, we take account of the maximum and minimum points. With the help this point the embedding is done into the smaller sub part of the image.

Here we have taken (512X512X8) image as shown in the following Figure We have embedded 128 bit hash on this block. After that we have divided the cover image into (256x256) equal size of blocks and embed 128 bit hash on this. Further we have divided image into (128x128) block sizes and embedded hash on this. Repeating the same process we have found that while embedding the hash into (32x32) blocks, there are some blocks where embedding is not possible. These blocks are in close neighborhood of each other due to the high correlation between the image pixels.

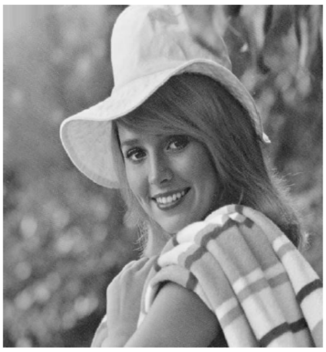


Figure 4.4: Grayscale Image of 512x512x8

Those blocks where embedding is not possible, we find out the more pairs of maximum and minimum points. After finding the more pair of maximum and minimum value we have embedded 128 bit hash on those block where embedding was not possible. This way we have embedded hash into every (32x32) blocks of the cover image. For this image up to this block size is possible. The embedding of the watermark into the smaller block size vary for different images. In some blocks it may be (64x64) or higher or it may be less. The embedding of watermark depends on the image embedding capacity, due to every image have different characteristics. It totally depends upon the image features.

## 4.6 Extraction and Authentication

In this phase of extraction and authentication the watermarked image is extracted at the receiver end. After extracting the watermark the hash value is computed. If the embedded watermark and hash value is the same then the image is authenticated and accepted to the receiver end. In the case of hash mismatch it leads to the authentication failure. The block where hash mismatch occur that block is rejected.

### Procedure

1. Divide the cover image into tamper localization blocks of (32x32) pixels
2. For each unit block B do,
3. Extract watermark from pixel [B (1, 2)...... B(32,32)]
4. Restore pixel [B(1,2).......B(32x32)]
5. Separate hash H← 128 bit hash P(1,128)
6. For each block B do same
7. If H! =Hash(B) then
8. Reject B;

In this the image is divided into the (32x32) block sizes. For each block we extract the watermark from each block. Then the pixel values are restored at the receiver end and hash is separated from that watermarked image. In the next step hash value is computed. If the hash mismatch occur then it is rejected otherwise it is accepted if the hash matches.

## 4.7 Chapter Summary

In order to locate the tampering in the image we use the block division approach. We embed the watermark 128 bit Hash into the smaller block sizes. This step is done until the embedding is possible. These watermark are extracted at the receiver end in order to authenticate the image. If the embedded watermark and hash matches at the receiver then it accepted. In case of hash mismatch it is rejected at the receiver end. Our proposed method gives the selective rejection of the cover images.

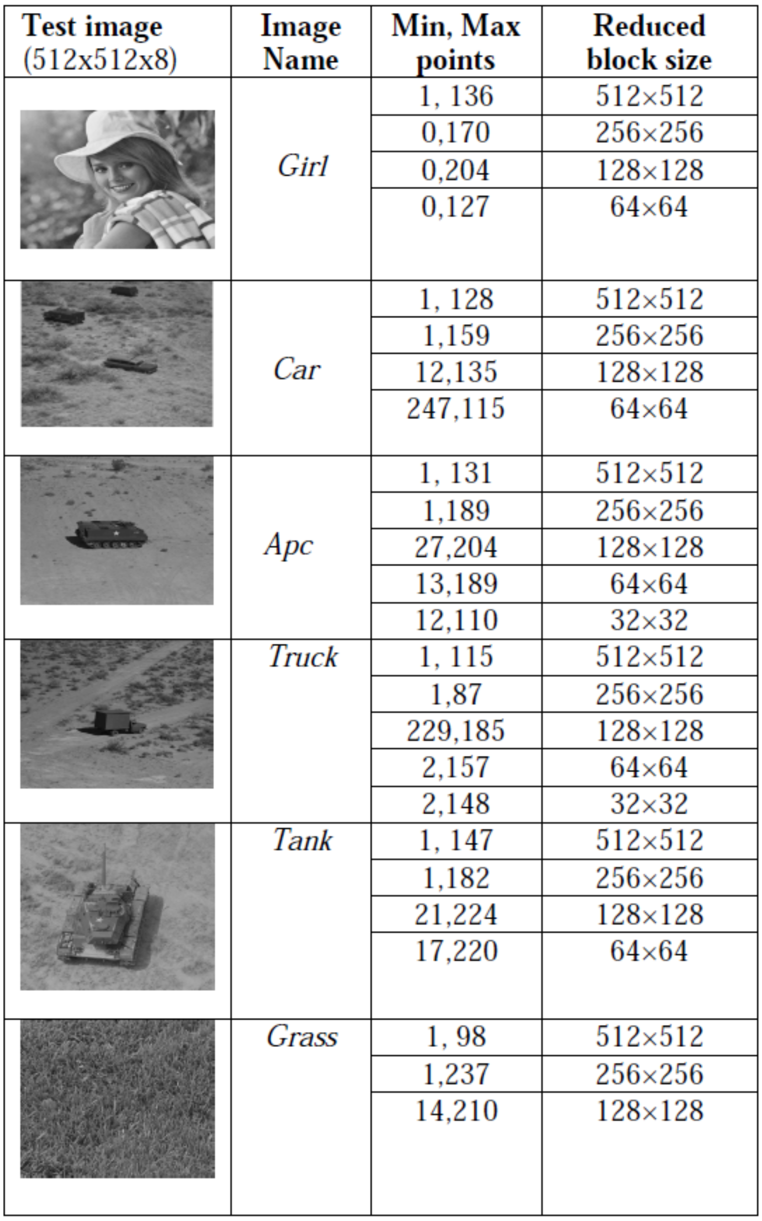
# Chapter 5

# Experimental Results

The proposed scheme succeeds to achieve tampered block detection accuracy. In other words, the exact block(s) containing the region(s) of tamper, is(are) the only one(s) to be rejected at the receiver end. The proposed scheme has been implemented using the Image Processing Toolbox of MATLAB 2014. Here we present our experimental results for a set of six (512×512×8) standard test images. The results are presented in the following Table.

Here we are embedding the watermark into the complete cover image. In the 512x512 image we have embedded the watermark. Here we are using the 128 bit hash into the complete cover image. After embedding the hash into 512x512 we have embedded hash into the block size of 256x256. Doing the same approach we will go to the smaller block size until embedding is possible. There are some blocks where embedding is not possible. Those blocks where embedding is not possible, for those blocks we will take the advantage of multiple minimum and maximum points. By choosing these points we will embed the hash into those blocks. At last there are some blocks where embedding is not possible. These blocks are the minimum level of achievable where the embedding is possible. This way we can say that we have embedded hash into the smallest block size. We extract the hash at the receiver end, if the hash matches then it is authenticated and accepted to the receiver end. In the case of hash mismatch occur that particular block will be rejected and retransmission of that block is needed.

In below Table, we have presented tamper localization blocks, up to the minimum possible level of decomposition, so as to embed 128 bit watermark. Table also presents



| Test image (512x512x8) | Image Name | Min, Max points | Reduced block size |
|---|---|---|---|
| | *Girl* | 1, 136 | 512×512 |
| | | 0,170 | 256×256 |
| | | 0,204 | 128×128 |
| | | 0,127 | 64×64 |
| | *Car* | 1, 128 | 512×512 |
| | | 1,159 | 256×256 |
| | | 12,135 | 128×128 |
| | | 247,115 | 64×64 |
| | *Apc* | 1, 131 | 512×512 |
| | | 1,189 | 256×256 |
| | | 27,204 | 128×128 |
| | | 13,189 | 64×64 |
| | | 12,110 | 32×32 |
| | *Truck* | 1, 115 | 512×512 |
| | | 1,87 | 256×256 |
| | | 229,185 | 128×128 |
| | | 2,157 | 64×64 |
| | | 2,148 | 32×32 |
| | *Tank* | 1, 147 | 512×512 |
| | | 1,182 | 256×256 |
| | | 21,224 | 128×128 |
| | | 17,220 | 64×64 |
| | *Grass* | 1, 98 | 512×512 |
| | | 1,237 | 256×256 |
| | | 14,210 | 128×128 |

Figure 5.1: Embedding Capacity achievable in Smaller Block size

the histogram minimum and maximum points, for the entire cover image, as well as for each of the reduced blocks. The experimental results have been presented for each of the test images. The embedding capacity which is achievable in smaller block size is shown in the Figure 5.1. This shows the smallest block size which can be achieved by the embedding of 128 bit hash.

These images has been taken from the standard image database like as USC-SIPI image database, CVG-UGR image database and USF-DM image database. This is very useful to taking the images from standard image database. There exist a high correlation between the image pixels. Most of time adjacent pixel possess the same property. While dividing these images into smaller sub-part of the images although we get a good standard image for our applications.

The implementation of our proposed scheme we are using 128 bit Hash, which is generated through cryptographic hash function. This approach shows the tamper localization blocks. For the tamper localization of blocks we are using the 512x512 Lena image. The tamper localization for any images varies according to the watermark embedding capacity. For different type of images the embedding capacity differs and it depend on the pixel of images. For embedding the hash into the images we take the advantage of having multiple minimum and maximum points. By using these points the embedding capacity is increases. Here we shift the histogram of the image to make some space for embedding. In these spaces we embed the watermark into the image. The embedding of the watermark is equal to maximum frequency of the Bin or it may be less. The embedded hash should not be more than the maximum bin; otherwise there will be distortion in the images.

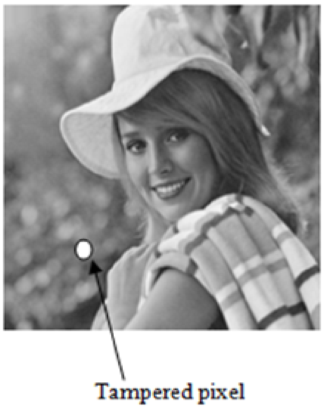


Figure 5.2: Modified pixel of the Watermarked image

In the given image if any pixel is tampered then our proposed method is able to detect exact location of tampering. Then the selected part of the image will be retransmitted by the sender. It will reduce the bandwidth requirement and solve the problem of re-transmission of the image. This way we can say that our method is most suitable for the selective rejection of the cover images.

By following our approach there is no block which is going to be falsely rejected. There is 100% accuracy while rejection of the tampered blocks. The false rejection rate by our proposed scheme is 0%. At the receiver end while extracting the hash only the tampered block is going to be rejected. If somewhere tampering is done in the original cover image particularly that block is going to be rejected. The false acceptance and rejection rate by our proposed scheme is 0%. We have tested our result on six different types of images, although in the case of tampering there is no block which is going to be falsely rejected. This we can say that our proposed method is able to detect the exact location of tampering.

In the reversible watermarking the exact restoration of the image without distortion is required. We know that the reversible watermarking being fragile it is vulnerable to attacks. The trivial tampering attack can be done by some adversary. At the receiver end the image is rejected due to the changes or tampered of the pixels. This will lead to the rejection of complete cover image. Although even single pixel of image is tampered, then the complete cover image will be rejected at the receiver end due to authentication failure. Then the re-transmission of the cover image is needed.

The proposed method is based on the block authentication of the image. By this approach we compute the hash of each and every block which is achievable through the embedding of the watermark up to the smallest block size. The hash is computed individually of every unit block at the receiver end. The integrity of every block is checked. The extracted watermark is computed with the original watermark. If both embedded and extracted watermark matches to each other then it is authenticated and accepted. The hash mismatch indicates that the tampering was done during the transmission. By our proposed method even a single bit is tampered of the cover image it will be detected and this method will localize the tampered blocks. That particular block where the tampering is done that block will be re-transmitted to the receiver. The tampering in one block does not reject to the another block in the case of authentication failure.

The situation when the communication channel is too noisy and busy, it is not quite feasible the repeated re-transmission of images. This situation will create the form of Denial of services attack, because when it will be needed it will be unavailable. We have proposed the solution of this problem in the form of selective rejection of the cover image. The selected part of the image where the tampering is done, there will be selective rejection of that block. By following our proposed method there will be minimal overhead over the communication channel. Due to selected transmission of the cover image limited bandwidth is required. In this way we can say that the performance of reversible watermarking is improved by our proposed method of tamper localization.

Our proposed method uses the secret key to embed the hash into the cover image. Here we are using the 128 bit hash to embed the watermark into the cover image. This function generates the sequence of random bit integers. Using this approach it will not be quite possible for adversary to find the same value of hash as it was used for the embedding. The second key is used to compress this value which was generated by the hash function. The loss-less compression technique is used here. In our approach we are using Run Length Encoding scheme to compress the bits. Due to its keyed nature it will not be easy to adversary to guess the same value as it was used during the embedding of watermark. This way we can say these watermark can be extracted with the same key at the receiver end with the authentic user. The special case when the hash values are modified by the adversary, then there is no idea at the receiver end that the hash value has been changed. But the key nature of this method is able to detect the tampering done by the adversary.

# Chapter 6

# Conclusion and Future work

## 6.1 Conclusion

In this thesis we propose a tamper localization approach for histogram bin shifting based reversible watermarking. The proposed approach finds the exact location of tampering. This allows the selective rejection of cover image where tampering is done. Subsequently, the proposed approach optimizes the number of cover image retransmissions requirement, hence the transmission overhead on the communication channel is reduced considerably.

In the proposed approach location of minimum and maximum points, is not of any concern. The mere presence of minimum and maximum points is sufficient. In those special cases, where the histogram of the image is horizontal, that is, all the pixel grayscale values are more or less equal; it is not possible to find out the maximum and minimum points. In this case we would have numerous minimum as well as maximum points. Hence the proposed approach fails in such cases.

## 6.2 Future Work

This thesis work may be extended mainly into two area. In the first area the reversible watermarking technique can be improved for the betterment of embedding capacity. This may address to the increasing of the embedding capacity. The second one the tamper localization approach may be enhanced by doing some special operation to the every bin of the histogram image.

### 6.2.1 Future Research Direction for the Reversible Watermarking Algorithm

The future research can be carried out the three different area, which are categorized as the following.

The problem of this approach is that the original image statistics is computed and stored before sending this. The transmission medium should be secure so that it can be prevented from the adversary. The other drawback is that watermarking cannot be estimated by the statistics. One of the possible solutions of this problem is that there is the need of the filter at the receiver end who can remove the added noise. Generally the added noise depends upon the communication channel. If the communication channel is too noisy then it may affect the communicated content. However it should be possible at the receiver end to authenticate the originality of the content.

The embedded watermark in the reversible watermarking should be persisted although it is attacked by the some common media attack. It should not be possible for adversary to detect and tamper the watermark from the watermarked media. It should be survive although if it is attacked. This property of robustness says that watermark still be presented if some common attack is done to achieve the information of contents.

Sometimes it is not only needed to know whether image has been tampered, but also it is desirable to know the exact location of tampering in the images. Some efficient robust hash function may be used to detect the tampering in the images. This approach should be able to detect the exact location of the tampering.

# Bibliography

[1] Muhalim Mohamed Amin, M Salleh, S Ibrahim, Mohd Rozi Katmin, and MZI Shamsuddin. Information hiding using steganography. In *Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on*, pages 21–25. IEEE, 2003.

[2] Donovan Artz. Digital steganography: hiding data within data. *internet computing, IEEE*, 5(3):75–80, 2001.

[3] Walter Bender, Daniel Gruhl, Norishige Morimoto, and Anthony Lu. Techniques for data hiding. *IBM systems journal*, 35(3.4):313–336, 1996.

[4] Mehmet Utku Celik, Gaurav Sharma, A Murat Tekalp, and Eli Saber. Reversible data hiding. In *Image Processing. 2002. Proceedings. 2002 International Conference on*, volume 2, pages II–157. IEEE, 2002.

[5] E Chrysochos, V Fotopoulos, AN Skodras, and M Xenos. Reversible image watermarking based on histogram modification. In *Proc. 11th Panhellenic Conf. Informatics (PCI 2007)*, pages 93–104, 2007.

[6] Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, and Ton Kalker. *Digital watermarking and steganography*. Morgan Kaufmann, 2007.

[7] Ingemar J Cox, Matthew L Miller, Jeffrey Adam Bloom, and Chris Honsinger. *Digital watermarking*, volume 53. Springer, 2002.

[8] Jen-Bang Feng, Iuon-Chang Lin, Chwei-Shyong Tsai, and Yen-Ping Chu. Reversible watermarking: current status and key issues. *IJ Network Security*, 2(3):161–170, 2006.

[9] L Ganesan et al. Some studies on data hiding using watermarking for authentication and security. 2013.

[10] Jiwu Huang and Yun Q Shi. Adaptive image watermarking scheme based on visual masking. *Electronics letters*, 34(8):748–750, 1998.

[11] Jiwu Huang and Yun Q Shi. Embedding gray level images. In *Circuits and Systems, 2001. ISCAS 2001. The 2001 IEEE International Symposium on*, volume 5, pages 239–242. IEEE, 2001.

[12] Jiwu Huang and Yun Q Shi. Reliable information bit hiding. *Circuits and Systems for Video Technology, IEEE Transactions on*, 12(10):916–920, 2002.

[13] JinHa Hwang, JongWeon Kim, and JongUk Choi. A reversible watermarking based on histogram shifting. In *Digital Watermarking*, pages 348–361. Springer, 2006.

[14] Xiangui Kang, Jiwu Huang, and Yun Q Shi. An image watermarking algorithm robust to geometric distortion. In *Digital Watermarking*, pages 212–223. Springer, 2003.

[15] Stefan Katzenbeisser and Fabien Petitcolas. *Information hiding techniques for steganography and digital watermarking*. Artech house, 2000.

[16] Sang-Kwang Lee, Young-Ho Suh, and Yo-Sung Ho. Reversiblee image authentication based on watermarking. In *Multimedia and Expo, 2006 IEEE International Conference on*, pages 1321–1324. IEEE, 2006.

[17] Bin Li, Junhui He, Jiwu Huang, and Yun Qing Shi. A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing*, 2(2):142–172, 2011.

[18] Xiaoping Liang. Reversible authentication watermark for image. In *Proceedings of the World Congress on Engineering and Computer Science*, pages 22–24. Citeseer, 2008.

[19] Chia-Chen Lin, Wei-Liang Tai, and Chin-Chen Chang. Multilevel reversible data hiding based on histogram modification of difference images. *Pattern Recognition*, 41(12):3582–3591, 2008.

[20] Pasunuri Nagarju, Ruchira Naskar, and Rajat Subhra Chakraborty. Improved histogram bin shifting based reversible watermarking. In *Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on*, pages 62–65. IEEE, 2013.

[21] Ruchira Naskar and Rajat Subhra Chakraborty. A generalized tamper localization approach for reversible watermarking algorithms. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, 9(3):19, 2013.

[22] Ruchira Naskar and Rajat Subhra Chakraborty. Reversible watermarking: Theory and practice. *Case Studies in Secure Computing: Achievements and Trends*, page 311, 2014.

[23] Zhicheng Ni, Yun Q Shi, Nirwan Ansari, Wei Su, Qibin Sun, and Xiao Lin. Robust lossless image data hiding. In *Multimedia and Expo, 2004. ICME'04. 2004 IEEE International Conference on*, volume 3, pages 2199–2202. IEEE, 2004.

[24] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su. Reversible data hiding. *Circuits and Systems for Video Technology, IEEE Transactions on*, 16(3):354–362, 2006.

[25] Christine I Podilchuk and Edward J Delp. Digital watermarking: algorithms and applications. *Signal Processing Magazine, IEEE*, 18(4):33–46, 2001.

[26] Vidyasagar M Potdar, Song Han, and Elizabeth Chang. A survey of digital image watermarking techniques. In *Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on*, pages 709–716. IEEE, 2005.

[27] Yun Q Shi, Zhicheng Ni, Dekun Zou, Changyin Liang, and Guorong Xuan. Lossless data hiding: fundamentals, algorithms and applications. In *Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium on*, volume 2, pages II–33. IEEE, 2004.

[28] Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang. Reversible data hiding based on histogram modification of pixel differences. *Circuits and Systems for Video Technology, IEEE Transactions on*, 19(6):906–910, 2009.

[29] Jun Tian. Reversible data embedding using a difference expansion. *IEEE Trans. Circuits Syst. Video Techn.*, 13(8):890–896, 2003.