A
Dissertation
On

Application of Database Watermarking in Watermarking Digital Images

Submitted in Partial Fulfillment of the Requirement

For the Award of the Degree of

Master of Technology

in

Computer Science and Engineering

by

Gunjan Gaba
Roll No. 2K13/CSE/05

Under the Esteemed Guidance of

Mr. Manoj Kumar
Associate Professor

Computer Science & Engineering Department, DTU

COMPUTER SCIENCE & ENGINEERING DEPARTMENT

DELHI TECHNOLOGICAL UNIVERSITY

DELHI - 110042, INDIA

2013-2015

ABSTRACT

With the tremendous growth in internet technologies and its usage, Digital Watermarking has been widely applied to multimedia documents for the purpose of ownership protection and hiding information. Digital watermarking has emerged as a feasible solution to provide protection from copyright, detection of tampering, traitor tracing. But robustness is a big challenge due easily available multimedia manipulation tools. Here, we present an effective watermarking technique for digital images that is robust against various attacks. We present an approach which embeds a watermark into the image pixels. To embed the watermark the original image is modified slightly by the embedding algorithm to obtain the final watermarked image. This modification cannot be detected by human eye. The proposed system controls embedding and extracting of watermark according to the key and message digest algorithm. Watermark cannot be detected by those who do not possess the key, or do not have access to it. The proposed approach is application of watermarking technique used for databases previously.

ACKNOWLEDGEMENT

First of all, I would like to express my deep sense of respect and gratitude to my project supervisor Manoj kumar for providing the opportunity of carrying out this project and being the guiding force behind this work. I am deeply indebted to him for the support, advice and encouragement he provided without which the project could not have been a success.

Secondly, I am grateful to Dr. OP Verma, HOD, Computer Science & Engineering Department, DTU for his immense support. I would also like to acknowledge Delhi Technological University library and staff for providing the right academic resources and environment for this work to be carried out.

Last but not the least I would like to express sincere gratitude to my parents and friends for constantly encouraging me during the completion of work.

Gunjan Gaba

University Roll no: 2K13/CSE/05

M.Tech (Computer Science & Engineering)

Department of Computer Science & Engineering

Delhi Technological University

Delhi – 110042

Computer Science & Engineering Department
Delhi Technological University
Delhi-110042
www.dtu.ac.in

CERTIFICATE

This is to certify that **Gunjan Gaba (2K13/CSE/05)** has carried out the major project titled**"Application of Database Watermarking Technique For Image Watermarking"** as a partial requirement for the award of Master of Technology degree in Computer Science and Engineering by **Delhi Technological University.**

The major project is a bonafide piece of work carried out and completed under my supervision and guidance during the academic session **2013-2015**. The matter contained in this report has not been submitted elsewhere for the award of any other degree.

Date ……

(Project Guide)

Manoj Kumar

Associate Professor

Department of Computer Science & Engineering

Delhi Technological University

Bawana Road, Delhi-110042

Table of Content

List of Figures

List of Tables

CHAPTER 1
INTRODUCTION

The recent development of networked multimedia systems and distribution of digital images and graphics data type has led to the requirement of electronic watermarking for copyright protection, forgery detection and to know that image has been intercepted and replaced. The method used for embedding watermark is content based which embeds watermark in image based on its content. For example, sharing of images related to weather, professional photography, medical, social networking sites, scientific, etc. is frequently performed. So, there is a great need for providing security to images to discourage illegal copying, modification and dispersement in today's internet dependent application environment. In this context, it is necessary to embed an invisible image watermark on colour images [1].

Watermarking provides solutions to lots of the problems faced in the distribution of different multimedia objects such as text, digital images, and audio [2]. Similarly, watermarking is very effective in protection of large relational databases [3]. Digital watermarking technique is successfully applied to protect the different multimedia works and software products. Similarly, watermarking in database has been proposed for security and control of large databases. Secure authentication is also needed for watermarking binary images, so that it cannot be forged by unauthenticated people [4,5]. However, there are many differences between relational database and digital images. Firstly, a relational database table have many attributes and tuples, and there is no certain ordering between tuples and attributes of relational table and there exist no such tuples and attributes in image or other multimedia object. Secondly, database maintaining operators can easily change those tuples unlike any other type of multimedia object, but nowadays image manipulation tools is also easily available. Moreover, processing of database tuples depends upon logical set operational languages like SQL. So database watermarking must be capable of real-time update and blind detection and cannot directly adopt other methods of multimedia watermarking. It is more difficult to ensure the robustness of database watermarking [6], but if robustness is achieved in frequently changing databases the similar technique could be applied to images to achieve desired

properties [7]. However, the relational database's data can tolerate very little distortion and further increasing the amount of distortion can cause the values to become absurd, but the same is not applicable for digital images, if LSB's of few pixels are changed [8] still the images can still be useful.

In recent years, considerable research has been done on authentication based digital watermarking. Jae-Woo Lee did study on copyright protection using authentication key based on digital watermarking [9]. In 2002, Liu Tong did a survey on Digital Watermarking based Image authentication Techniques [10]. Jiang bin Zheng, David dagan Feng proposed multi channel framework for image watermarking [11], which aims at synchronising attacked watermarking signal and original embedded watermarking signal without considering the geometric transformations that the watermarking image undergoes. Sarabjeet S. Bedi and Shekhar Verma did research in secure watermarking scheme for images, they tried to embed watermark obtained by applying hash function to user key into blocks of size 4 by 4[12]. Many other researchers in watermarking have also done a lot of efforts to promote the development of image watermarking [13-24], yet there are still shortcomings in current study. The robustness of watermarks is too weak to resist different conventional image manipulation operations and illegal watermark attacks, such as blurring, cropping, and so on. As a result, improving the robustness of digital image watermarking is a very difficult and significant work.

1.1 Motivation

The motivation for image watermarking is to protect images,(e.g, parametric specifications, life sciences data and surveys), from pirated copies and tampering. A watermark is considered as any kind of information that is embedded into underlying data for tamper detection, localization, ownership proof, and/or traitor tracing purposes. Watermarking techniques for databases complement the Database Protection Act and they have become increasingly important as people have realize that "the law is not able to provide sufficient protection to the comprehensive, commercially and publicly useful databases which are at the heart of the information economy", development of these watermarking techniques led to increased research in image watermarking and focus on new techniques for images.

1.2 Research Objective

The objective of this work is to present a technique for digital image watermarking based on technique used for watermarking relation databases that provided a high robustness that can resist various conventional database operations and illegal watermark attacks, such as deletion, addition, modification and so on and provides the same robustness for digital images when image undergoes various modifications like cropping, blurring including median and guassian blur .The algorithm used will be explained in the forthcoming chapters with the experimental results.

1.3 Scope of work

Here, the method of protecting image copyright with key based watermarking is studied only on Portable Network Graphics (png) images, the technique used also uses cryptographic hash function MD5. In the future, we should expand our studies to other image formats. Here few image manipulation filters have been used like Gaussian blur, median blur and cropping. But the same technique can be checked after applying other image manipulations. The technique proposed embeds an invisible watermark in image, which is based on key used. The key used will decide which pixels of image must be watermarked and with what value they must be changed. The key must be different for all images and various parameters can be used for deciding the key for a particular image.

1.4 Organization of thesis

In this chapter, I have highlighted the concept of image watermarking, motivation to do this thesis, my objective, and scope to do the work in same field. Chapter 2 provides a detailed picture of image watermarking technique employed and the prior work done till date. In chapter 3 I have presented the proposed scheme, along with little information about the library used to carry out research. Chapter 4 includes the implementation details and experimental results. Chapter 5 concludes the thesis, and Finally Chapter 6 discusses the future scope in current work.

CHAPTER 2

LITERATURE REVIEW

Digital watermarking has two basic processes: watermark embedding or insertion and watermark detection or extraction or recovery, as shown in Figure 1. For inserting watermark, a key is used to insert watermark information into an original image leading to production of the watermarked image for publication or distribution. The key used can be same or different for all images, but together with watermark insertion process it must embed the watermark differently. With appropriate key and watermarking algorithm information, a watermark extraction process can be implemented on any doubtful image so as to check whether or not a genuine watermark can be detected. A doubtful image can be any watermarked image or naive image, or a mixture of them under various database attacks. Digital watermarking is used widely for copyright protection and checking integrity and authenticity of images. Many watermarking techniques have been proposed, but those having less cost in terms of both economical (using open source software mainly, less memory) and time(less complex) and which are robust are successful and frequently used. Basic watermark embedding and extraction scheme is shown below.

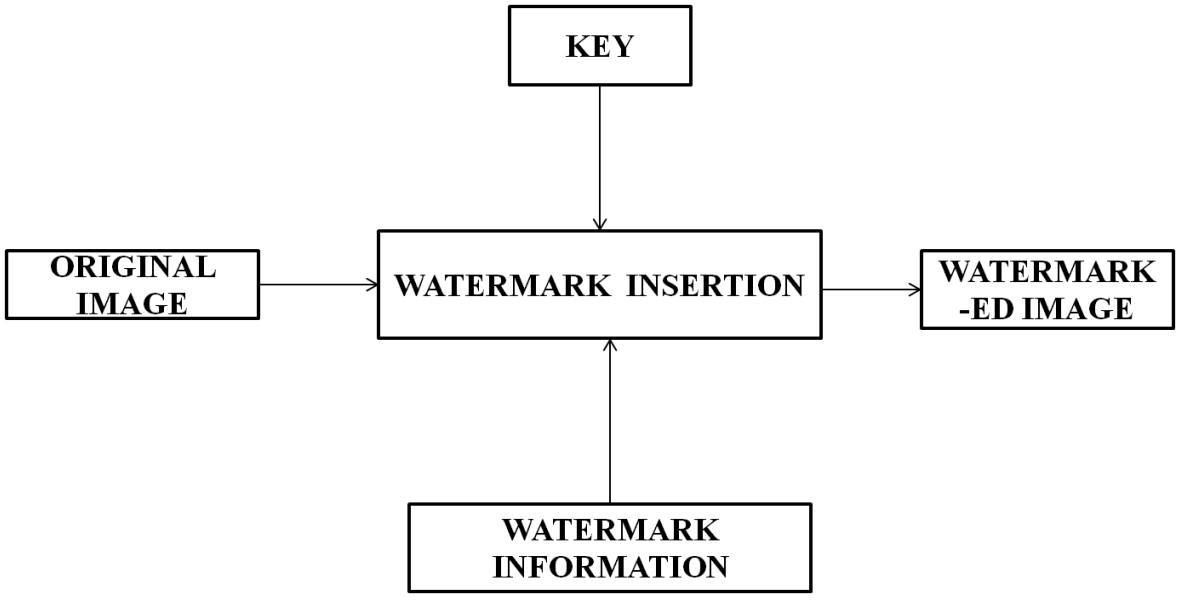

Figure 2.3: Basic Watermark Insertion or Embedding Process.

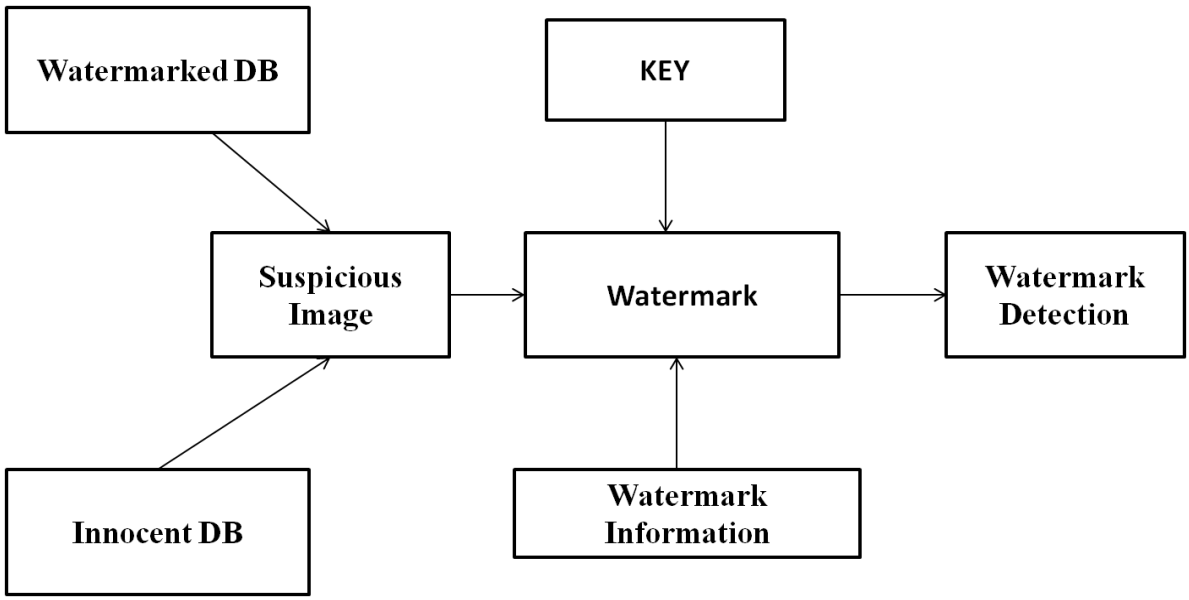

Figure 4.2: Basic Watermark Detection Process.

Image watermarking techniques can be categorized into two categories:

- Robust watermarks: Image manipulation or attacks both incidental and intentional do not change the watermark embedded and hence these watermarks can be used for protecting copyrights and ownership assertion.
- Fragile watermarks: Basic image manipulation procedures change the watermark embedded and hence these watermarks can be used to check the integrity of image and authenticity of content. They are also known as authentication watermarks.
- Semi-Fragile watermarks: These watermarks are used for authentication of image and are generally robust against incidental attacks, but fragile against intentional attacks.

In my proposed scheme I have proposed a new authentication based watermarking scheme which is application of database watermarking technique.

The Authentication watermarks that are embedded in our Images must have following properties:

1. These watermarks must be Invisible for human eye perception, watermarked and original image must be perceptually similar.

2. Watermark embedded must be secure against unauthorized removal, unauthorized embedding and unauthorized detection. When unauthorized removal is done, watermark should not be removed and when unauthorized embedding is performed watermark should be fragile or semi-fragile, and it should be imperceptible for unauthorized detection.
3. These watermarks must be of low complexity, the cost of embedding and extracting the watermark must be less both in time and economic cost.
4. The watermark embedding and extraction can only be performed by legitimate people.
5. The watermark must be able to do copyright protection, content authentication and broadcast monitoring.

2.1 Inserting watermark in relational database

This research work describes a robust technique for hiding watermark in database, the watermark is hidden in database based on a key and density control parameter, and is hidden in database attributes fractional parts.

The watermark embedding process is described below:

- Few parameters like secret key ƙ, gap parameter ȳ, total marked tuples ε, total attributes α, total tuples τ, total bits available for modification β are known and private to owner of database.
- The embedding process includes use of a cryptographic pseudorandom sequences.
- The tuple is selected based on the secret key and value of gap parameter(ȳ). For each tuple, primary key of that tuple and secret key(ƙ) are concatenated and it is input as seed to pseudorandom sequences. If the modulus ȳ of that random no. obtained from sequence value is zero then that tuple is selected for hiding the watermark.
- After selection of tuple, particular attribute is selected by taking mod of random sequence no. obtained with total no. of attributes(α).

- Finally bit index to be modified in selected attribute is selected by taking mod of random sequence no. obtained with total no. of bits available at least significant position(β).
- After selection of bit it is set as 0 or 1 depending upon whether even or odd attribute is selected. If attribute is even bit is set as 0 otherwise it is set as 1.

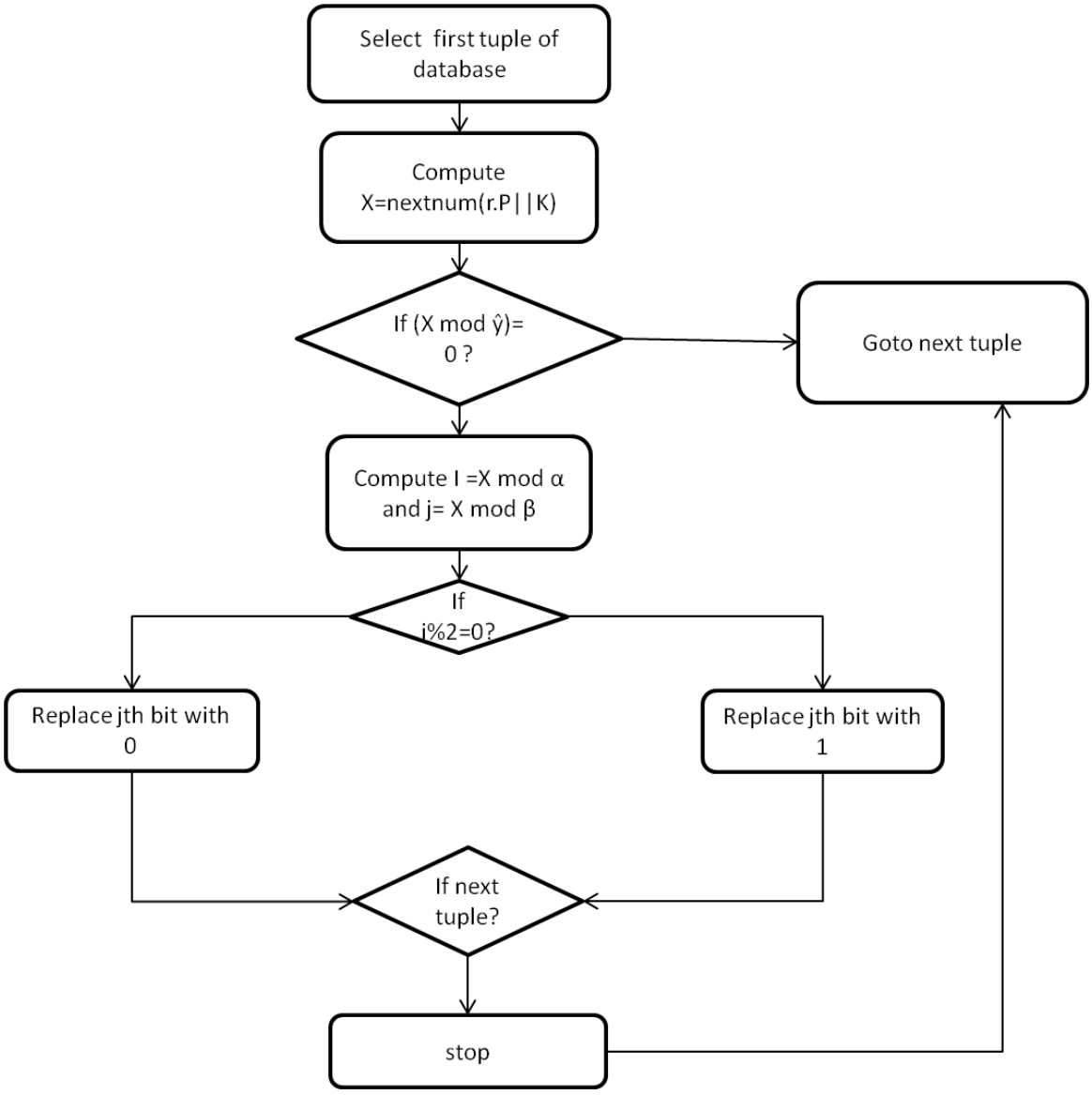

Figure 2.3: Watermarking relational database.

Algorithmically it can be represented as:

1. For each tuple r in Relation do
2. Compute X = nextnum(r.P||K)
3. If ((X mod ȳ)equals 0) then // mark it
4. Compute i = X mod α // mark i^{th} attribute.
5. Compute j = X mod β // mark j^{th} bit.
6. If (i is even) then
7. Replace j^{th} bit with 0
8. Else
9. Replace j^{th} bit with 1
10. Return Relation.

The extraction process is described below:

- Parameters like secret key ƙ, gap parameter ȳ, total attributes α, total bits available for modification β are required to extract the hidden curve from the database.
- Selection of tuple is based on value of ȳ and secret key. For every tuple, primary key of that tuple is concatenated with secret key and is given as seed to pseudorandom sequences. If mod ȳ of obtained random number(X') is zero then that tuple is the marked tuple.
- For extracting the particular bit marked in particular attribute, the random no. (X') mod is first obtained with total no. of attributes to select particular attribute and then is X' mod is obtained with total no. of bit positions available for modification (β) to get the particular bit.
- After getting that bit (β) its value is checked based on attribute position that whether its 1 or 0. If it is same as watermarking insertion algorithm would have made it then given bit has watermark in it and is counted to know about total no. of watermarked bits correctly detected.

2.2 Watermarking Techniques for digital images

2.2.1 Spatial Domain

Here information is inserted directly into image, algorithms included are:

(a) LSB (least significant Bit) : it is simplest approach and since least significant bits consists of less relevant information, any changes in these bits do not cause visible changes ,so information is embedded in these bits.

(b) ISB (intermediate significant Bit): in this technique best position of watermarked pixel from edge of range and from middle of range is found out, so that we can protect watermark attack from various kinds of attacks and can keep the watermark image to minimum distortion.

(c) Patchwork: Information is embedded in brightness of pixels thus changing statistical properties of image, it first selects random no. of pairs of pixel points and difference from Gaussian distribution of those pixels is taken as zero. Finally, brightness of one of the pixel is increased by one and that of other is reduced by 1 so that average brightness will not change but distribution center may change.

2.2.2 Transform Domain

In this technique transform coefficients are used to embed the watermark, since watermark is spread in whole image these techniques are very robust.

(a) DCT (discrete cosine transform): due to its robustness property it is widely used in digital image watermarking, but drawback of using these techniques is they have low watermarking capacity. DCT coefficients are divided into four categories: DC coefficient, low frequency coefficient, mid frequency coefficient and high frequency coefficient. All have different capacity and robustness.

(b) DWT (discrete wavelet transform): it separates the frequency detail, which is decomposition in multi resolution. Single decomposition divides the image into four sub images of quarter size into low frequency approximate sub image, horizontal, vertical and diagonal high frequency sub image.

2.3 Multichannel image watermarking framework

For single channel image watermarking it is difficult to do correlation between manipulated watermarked image and watermarking signal, so it is difficult to extract the watermarks in geometric transformed images. So, a framework which synchronizes these two signals automatically is proposed, it does not resolve any geometric transformations that the image undergoes.

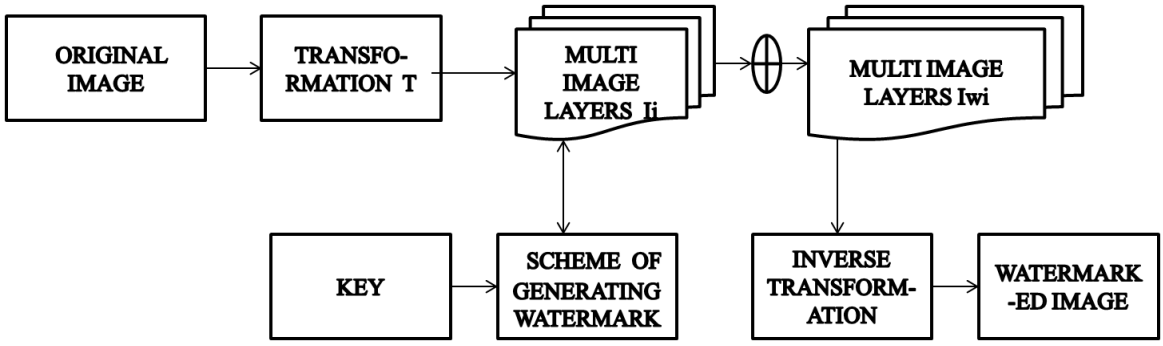

Figure 2.4: Multichannel image watermarking framework

In this case,

G : Watermarking template generation function.

W_t : Generated watermarking template,

I_j : Input image channel data.

Here the main requirement is that W_t should be satisfied with normal distribution and zero mean, and this template is embedded into one or more channels of original image data.

$$I_{wi} = I_i + W_t \quad (2)$$

If both I_{wj} and I_j undergo geometric transformation attack D then

$$I_{J'} = D.\ I_j \quad (3)$$

$$I_{wi'} = D.\ I_{wj} \quad (4)$$

Using attacked image channel $I_{J'}$, the watermarking template is obtained as

$$W_{t'} = G.\ I_{J'} \quad (5)$$

Substituting (3) in (5), we get

$$W_{t'} = G.D.I_{J.} \quad (6)$$

If watermarking template generation scheme (G) and geometric transformation D are such that $G.D=D.G$ substituting $G.D$ in equation (6), we get

$$W_{t'} = G.D.I_J = D.G.I = D.Wt$$

Hence proved that watermarked image and watermarking generation algo undergo the same geometric transformation and hence self synchronization is achieved.

In above scheme it is proved mathematically that both watermarking template and watermarked image undergo same transformation and undergo self-synchronization.

2.4 Authentication watermarking for binary image security

Watermark insertion process:

1. Binary image to be watermarked B is taken along with logo L to be inserted.
2. Pseudo random number generator is used for generating random locations R inside B.
3. All pixels belonging to R are cleared getting B* and fingerprint of B* is computed H=H (B*).
4. H is exclusive-ored with L to get marked fingerprint H' and H' is encrypted with secret or public key to get digital signature S.
5. And S is embedded in R to get B'.

Watermark extraction process:

1. Let Y' be image having watermark, same pseudo random no. generator is used with same seed to generate same random locations R.
2. Again Y* is obtained by clearing R location in Y and its fingerprint is calculated H=H(Y*).
3. Decrypt the pixels present in Y to get decrypted data D, which is ex-ored with H, and a check image C is obtained. If C and L are same, the watermark has been verifies otherwise it is modified.

2.5 Scheme for Watermarking Images in Spatial Domain Securely

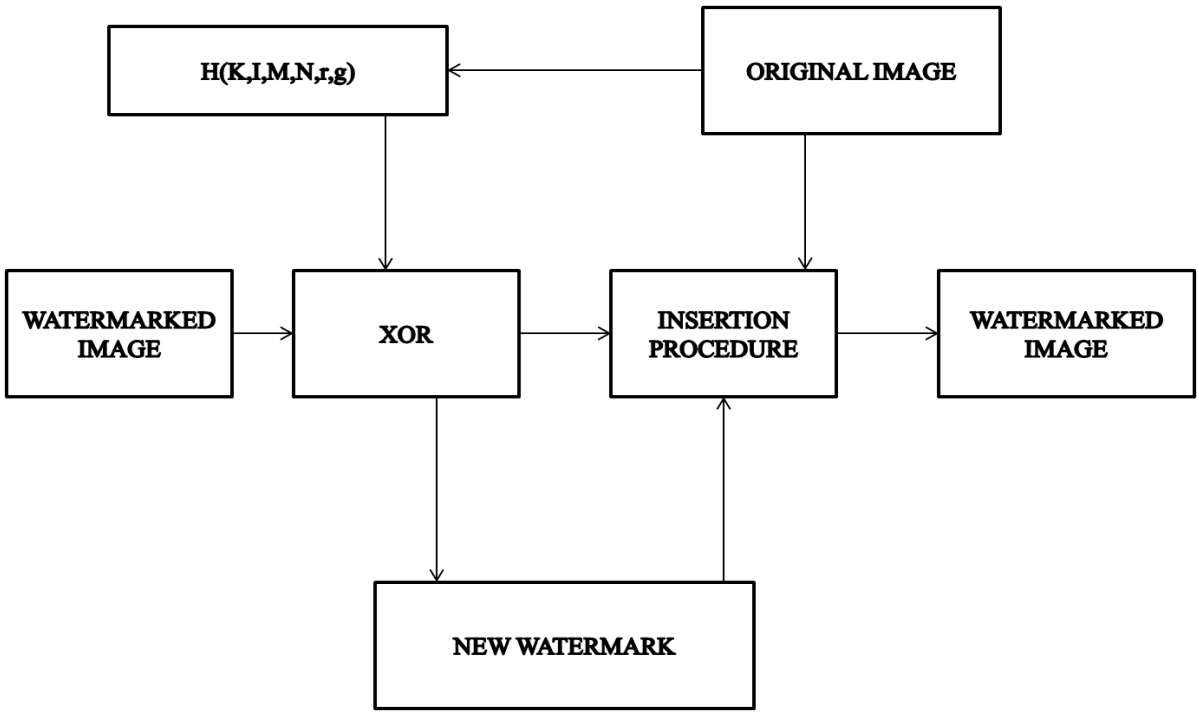

Figure 2.5: inserting watermark in images in spatial domain securely

Proposed watermark insertion scheme is shown above.

In this scheme original image (I^0) is taken and divided into two non overlapping independent blocks b^h (high level) and b^l_r (low level) partition, r is index of each block. For each rth block of watermarked image b_r^w hash is computed as $H(K,I,M,N,R,g^m_r)$, a string of bits is called user key K, Image Index is I, Image width is M, Image height is N, R is image index and g^m_r is mean value of pixel intensity of corresponding block, new watermark is obtained by XORing hash value obtained with with watermark image block and then insertion procedure is used to embed the watermark into original image to get watermarked image based on local statistics of pixel intensities of each block.

Watermark extraction scheme:

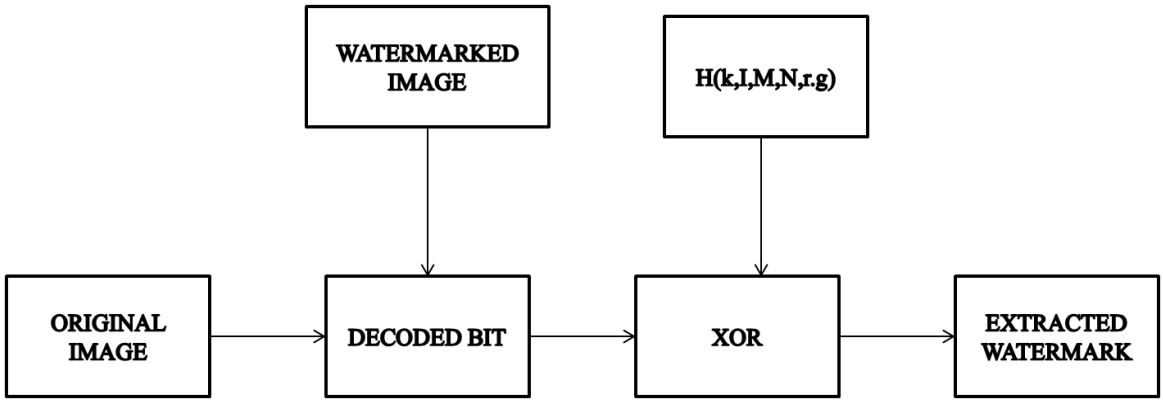

Figure 2.6: Extracting watermark from images in spatial domain securely

The extraction process is simple and it requires original image, user key and image index. Then sum of intensity values of original and watermarked image block is done. The extracted bit comes out to be 0 if sum of intensity value of original image is greater than watermarked image otherwise it comes out to be 1. Finally these bits when combined together form the final watermark of size i*j pixels.

2.6 Authentication Key Based Digital Watermarking for Copyright Protection

Below figure shows how authentication and digital watermarking can be clubbed together. The various steps are listed below:

1. Before requesting application server for multimedia document, client requests authentication server for authentication key.
2. After getting the client request, authentication server generates authentication key for client using Randomize (), gives the key to client and notifies application server about client authentication key.
3. Client then request application server for document, but before giving the document to client the application server generates watermark for the document using client key and insert that watermark into the document.
4. Finally, responds to client using multimedia document.

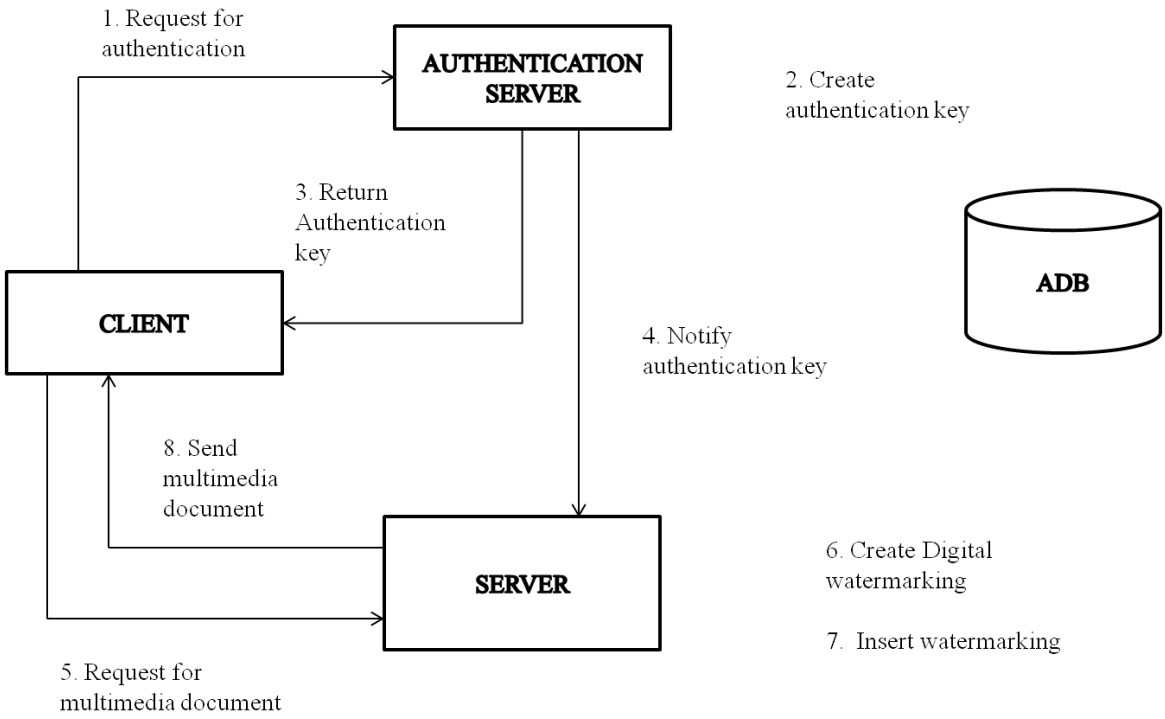

Figure 2.7: Authentication key based watermarking for copyright protection.

CHAPTER 3

PROPOSED APPROACH

The proposed system embeds a watermark into digital image pixels using an embedding algorithm. Embedding algorithm utilizes the physical location of pixel and a key, which provides control for the hiding and recovery processes, restricting extraction by those who do not possess the key, or do not have access to it. The proposed approach is an application of watermarking approach used in database. The Embedding process and extraction process along with library which is used for carrying out the work is explained here.

3.1 Embedding Process

- The watermark which is to be embedded in the digital image is selected according to two parameters: key and physical location of pixels, so the watermark embedded depends upon the size of image.
- The embedding process includes selecting particular pixels for modification for watermarking.
- The pixel is selected based on the secret key and its x and y coordinates. For each pixel, physical location of that pixel and secret key are concatenated and its hash is calculated, let's say that the hash comes out to be K. If the modulus alpha (density parameter) of that hash value (K) is zero then that pixel is selected to hide the watermark.
- After Selecting a particular pixel ,it is decided that which color panel(BGR) of that pixel must be watermarked if image is colored image otherwise for gray scale images we have only one panel ,and modification is done in that panel only. The panel selection is done by finding modulus beta (β) of hash value (K) obtained in above step with 3. Based on beta value (β), which can be either 0, 1 or 2 particular color panel is selected.
- Once selection of colored panel is done, location of bit for watermark in that panel is selected. The location is selected from last four bits of that panel, this location is

also selected based on calculating modulus gamma (ϒ) of hash value with 4. Based on gamma value (ϒ), which can be 0, 1, 2 or 3 bit position from last bits are selected respectively.

- Then finally after selection of particular pixel, particular panel and particular bit position, with which value that pixel must be changed is selected. This selection is done based on taking modulus of hash value with 2. If modulus comes out to be 0, that particular bit position is replaced with 0 or cleared, otherwise if it comes out 1, that bit position is replaced with 1 or set.

The proposed watermark embedding can be shown as:

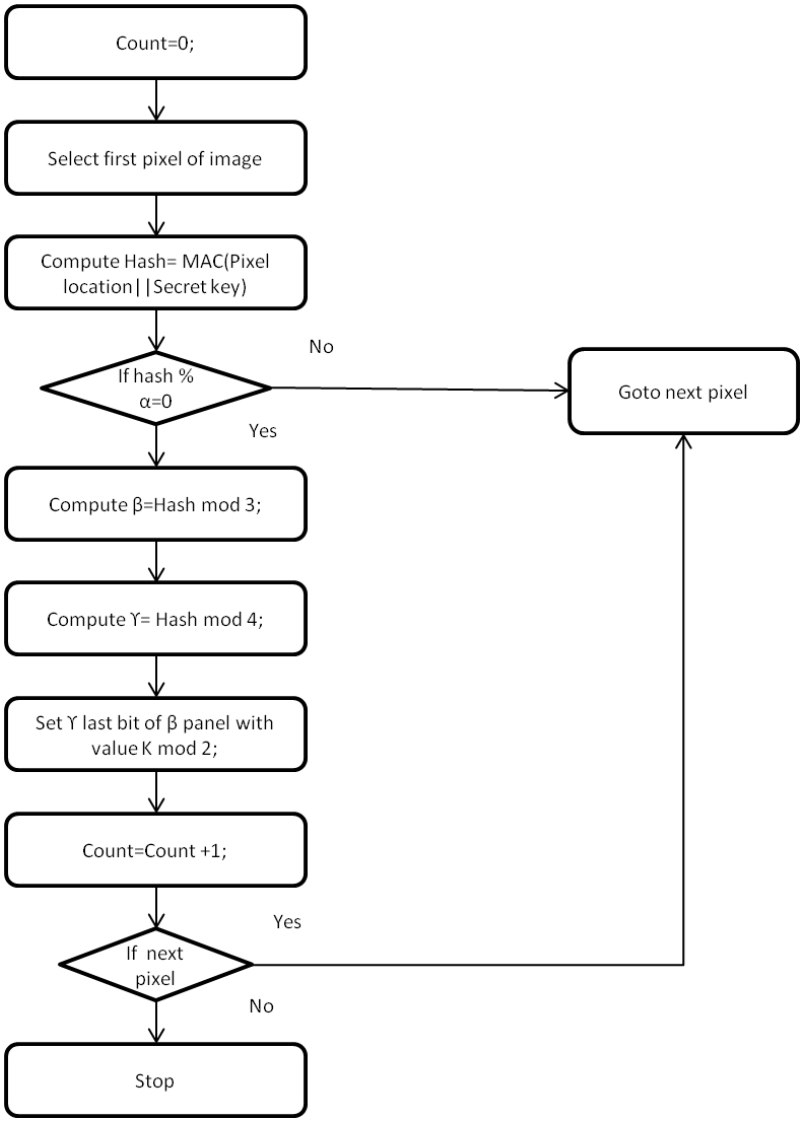

Figure 3.1: Proposed watermark embedding process

In above flowchart, count represents total no. of pixels having watermark.Algorithmically the same can be represented as:

1. Count=0;
2. For each pixel in image do
3. Compute hash K=MAC(x|y|key)
4. If (K mod α) equals 0, then pixel is marked
5. β=K mod 3;
6. ϒ=K mod 4;
7. Set ϒ last bit of β panel of selected pixel with value K mod 2;
8. Count=Count+1;
9. end

3.2 Extraction Process

- Extraction process consists of counting the no. of pixels that still have watermark after the image undergoes manipulation.
- During extraction, the pixel is selected based on the secret key and its x and y coordinate. For each pixel, location of that pixel and secret key are concatenated and its hash is calculated. If the modulus alpha of that hash value is zero then that pixel has the watermark.
- After getting the watermarked pixel, the value of gamma bit in beta panel is checked if it comes out to be same as modulus of hash value with 2, then this pixel is match, And count of watermarked pixels is incremented.

The proposed watermark extraction can be shown as:

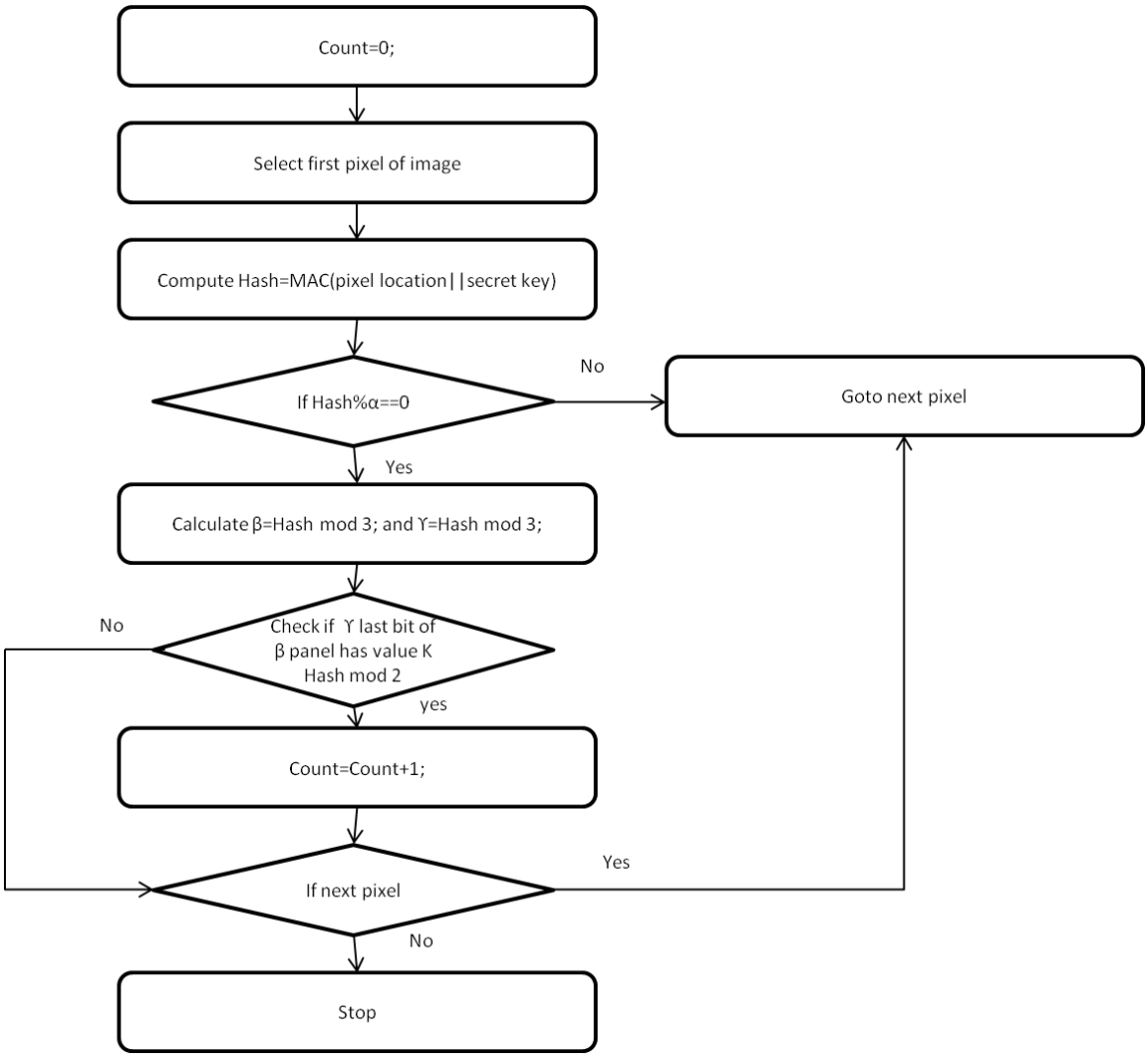

Figure 3.2: Proposed watermark extraction process

1. Count=0;
2. For each pixel in image do
3. Compute hash K=MAC(x|y|key)
4. If (K mod α) equals 0, then pixel is marked pixel
5. β=K mod 3;
6. ϒ=K mod 4;
7. Check if ϒ bit of β pixel has value K mod 2;
8. If yes then Count=Count+1;
9. End
10. Count the total no. of pixels having watermark they must be same as marked.

After embedding of watermark in images, histogram of the original and watermarked image are calculated and these histograms are compared based on four different matrices.

Histogram is generally intensity of image pixels represented graphically. Histogram can be calculated on any other feature as well, but in my work I have considered pixel intensities in different channels. When watermark is embedded the pixel intensities undergo slight modification. These modified and original pixel intensities are compared using four different functions or methods, each method taking into account the Histogram **OH1** and W**H2** of original and watermarked image repectively.

Method 1: Correlation (CV_COMP_CORREL)

$$d(\mathbf{OH1,WH2}) = \frac{\sum_I (\mathbf{OH1} - \mathbf{OH1}')(\mathbf{WH2} - \mathbf{WH2}')}{\sqrt{\sum_I (\boldsymbol{OH1} - \boldsymbol{OH1}')2(\boldsymbol{WH1} - \boldsymbol{WH2}')2}}$$

where OH'= $\frac{\mathbf{1}}{\boldsymbol{M}} \sum_J \boldsymbol{OH}$

The output of correlation is between [-1,1] , where 1 represents perfect match and -1 represents no match at all.

Method 2: Chi-Square (CV_COMP_CHISQR)

$$d(\mathbf{OH1,WH2}) = \sum_i \frac{(\mathbf{OH1} - \mathbf{WH2})(\mathbf{OH1} - \mathbf{WH2})}{\boldsymbol{OH1}}$$

In Chi-Square, 0 represents perfect match, low score is better than high score and no correlation can be anything.

Method 3: Intersection (CV_COMP_INTERSECT)

$$d(\mathbf{OH1,WH2}) = \sum_i \mathbf{min}(\boldsymbol{OH1}, \boldsymbol{WH2})$$

Good match is represented by high score ,bad match by low score and for histograms which have been normalized 1 is perfect match and 0 is total mismatch.

Method 4: Bhattacharyya distance (CV_COMP_BHATTACHARYYA)

$$d(\mathbf{OH1,WH2}) = \sqrt{\mathbf{1} - \sum \frac{\sqrt{OH1(i).WH2(i)}}{\sum OH1(i) \sum WH2(j)}}$$

good match means low score ,bad match means high score perfect match means 0 and total mismatch means 1.

The values that are obtained after comparing histogram of original and watermarked image are shown in tabular form in result section.

After extraction is done, the watermark is checked for robustness, geometric transformation of cropping is applied to image and filters like blurring are applied. The corrupted image is checked for the degree of accuracy with which watermark can be extracted after applying transformations. Median blur and guassian blur are explained below, how they modify watermarked image.

Median Blur: It is digital filtering technique, which is used for noise reduction in images, to improve later processing results. It preserves edges while removes noise, and is widely used, while processing the signal it replaces each pixel with the median of its neighbours.

Gaussian Blur: In this technique the image is blurred using guassian function, and it seems like we are viewing the image through a translucent screen. It is generally pre-processing step to enhance image structure in computer vision. Values from this filter are used to apply a convolution matrix which is build from original image.

To access pixel values I have used a library called OpenCV (Open Computer Vision).
OpenCV is an open source library and is available on:
http://sourceforge.net/projects/opencvlibrary/
The installation steps are mention at URL:
docs.opencv.org/doc/tutorials/introductionlinux-install/linux-install.html#linux-installation
In OpenCV image is stored as matrix MAT
Mat imagee;
imagee = **imread**("imagename.fmt",cv_load_image_color);
: imread is the function used to read the image the image.

namedWindow();

: Before showing the image, a window needs to be created using function

imshow("imagename",imagee);

: it is the function used to display image.

imwrite("imagename.fmt", imagee);

: it is the function used to write image back to disc.

Two for loops can be used to access pixels in image, one for loop for accessing pixels row wise and another for accessing pixels column wise, OpenCV stores pixels in BGR order for colour images:

```
For (int i=0;i < imagee.rows ;i++)
For (int j=0;j< imagee.col; j++)
    Imagee.at<cv::Vec3b>(r1,c1)[k] = newval;
```

Where k defines particular colour panel or channel.

For greyscale images there is single channel only and its pixels can be accessed as:

```
For (int i=0;i < imagee.rows ;i++)
For (int j=0;j< imagee.col; j++)
    Imagee.at<uchar>(r1,c1) = newval;
```

For blurring the image following functions are used:

blur(imagee ,dst, size(i,i));

medianBlur(imagee, dst, i); // for median blurring the image

GuassianBlur(imagee,dst,size(i,i),0,0); //for guassian blur

For calculation of histogram following function is used :

void calcHist(const Mat* images, int no_of_images, const int* channels, InputArray mask, OutputArray hisst, int Dims, const int* histSize, const float * ranges, bool uniform = true, bool accumulate = false)

For calculating hash value of pixel position concatenated with key, i have used MD5, which calculates 128 bit hash value.

MD5 is cryptographic hash function designed by Ron rivest ,it is used to verify data integrity and can work on message of any length, it is considered to be unique to a particular data as fingerprint is unique to an individual

CHAPTER 4

RESULTS

4.1 Environmental Setup

The following configuration has been used while conducting the experiments:

Hardware Configuration

Processor	: Intel core i5
Processor Speed	: 2.40 GHz
Main Storage	: 4.00 GB
Hard Disk Capacity	: 320 GB

Software Configuration

Operating System	: Linux
Language used	: C++
IDE used	: Netbeans
Library used	: OpenCV

4.2 Results of application of Watermarking on Images

The scheme was applied on a sample image of 512* 512 pixels.

For image

a) baboon.png

- Secret Key = kite
- $\alpha = 5$

b) Lena.png

- Secret Key = kitten
- $\alpha = 5$

c) Barabara.png

- Secret key = commit
- $\alpha = 5$

After hiding the watermark in the image, the image is subjected to modification like cropping, median blur and guassian blur.

4.2.1 Results after applying the watermark in image

Secret Key used: “kite”.

No. of pixels Watermarked: 49236

Figure 4.1: baboon.png before watermarking.

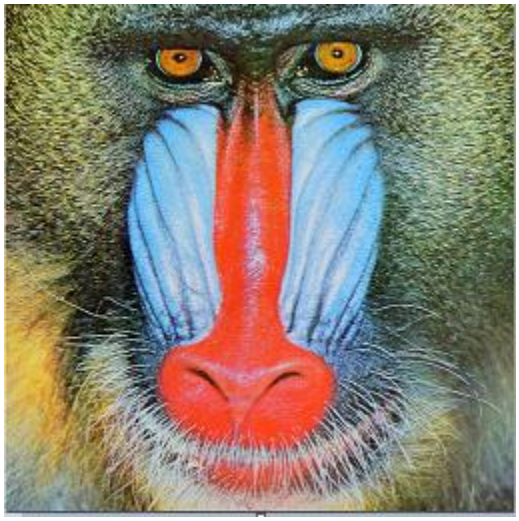

Figure 4.2: baboon.png after watermarking

Secret Key used: “kitten”.

No. of pixels watermarked: 49293

Figure 4.3: lena.png before watermarking

Figure 4.4: lena.png after watermarking

Secret Key used: “commit”.

No. of pixels watermarked: 48790

Figure 4.5: barbara.png before watermarking

Figure 4.6: barbara.png after watermarking

4.2.2 Histogram of original images and their corresponding watermarked images.

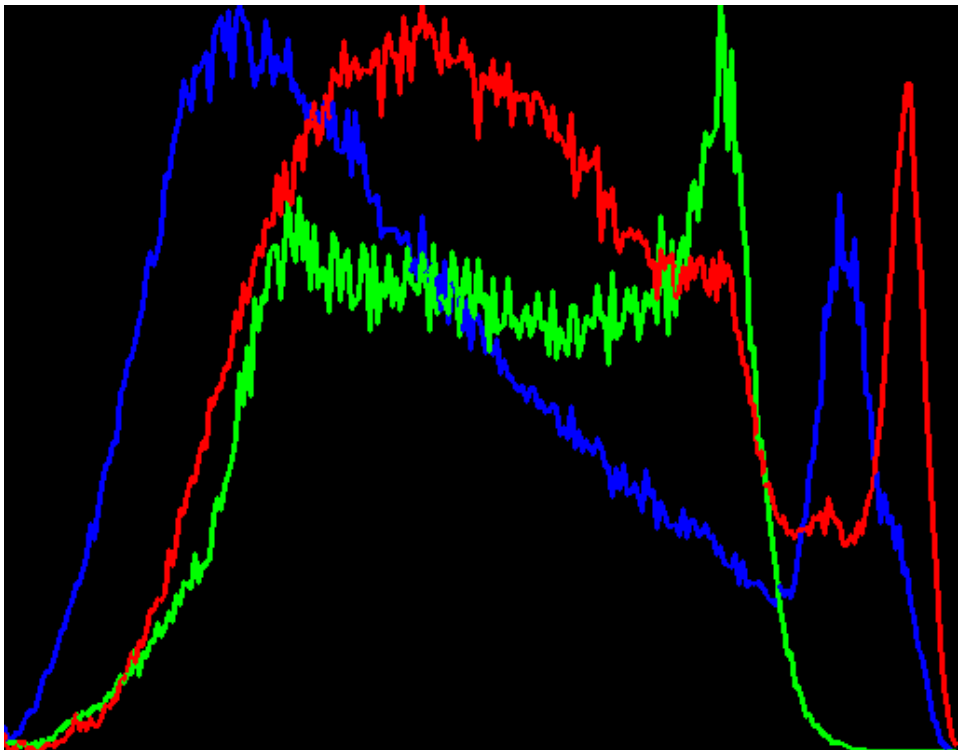

Figure 4.7: Histogram of baboon.png before watermarking

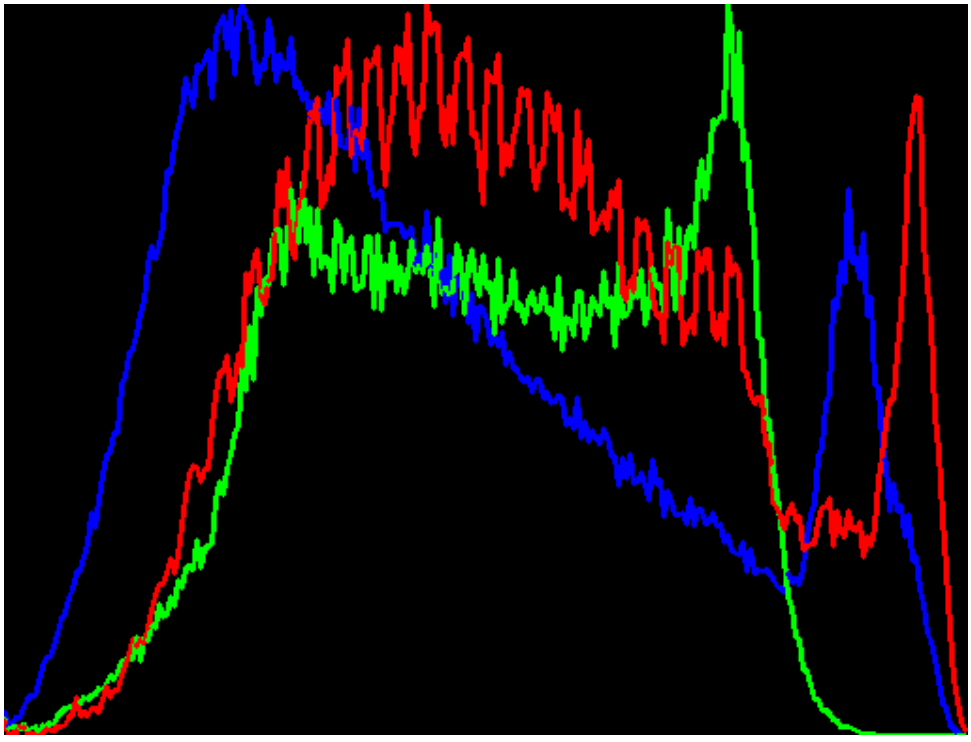

Figure 4.8: Histogram of baboon.png after watermarking

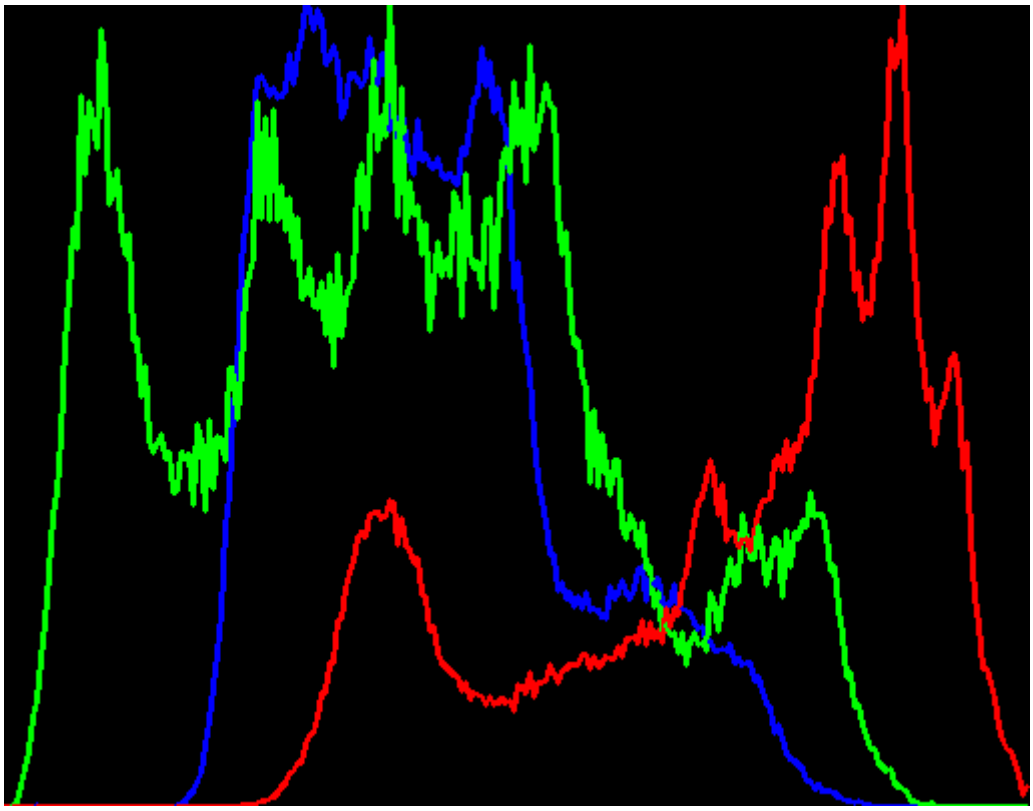

Figure 4.9: Histogram of lena.png before watermarking

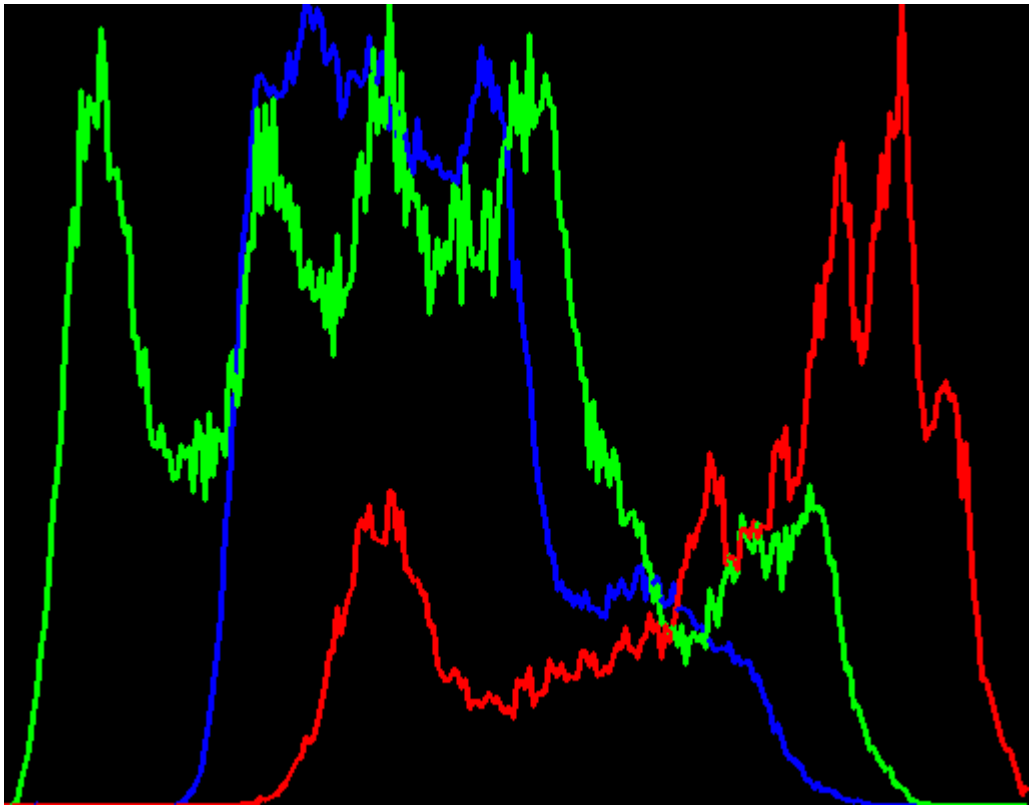

Figure 4.10: Histogram of lena.png after watermarking

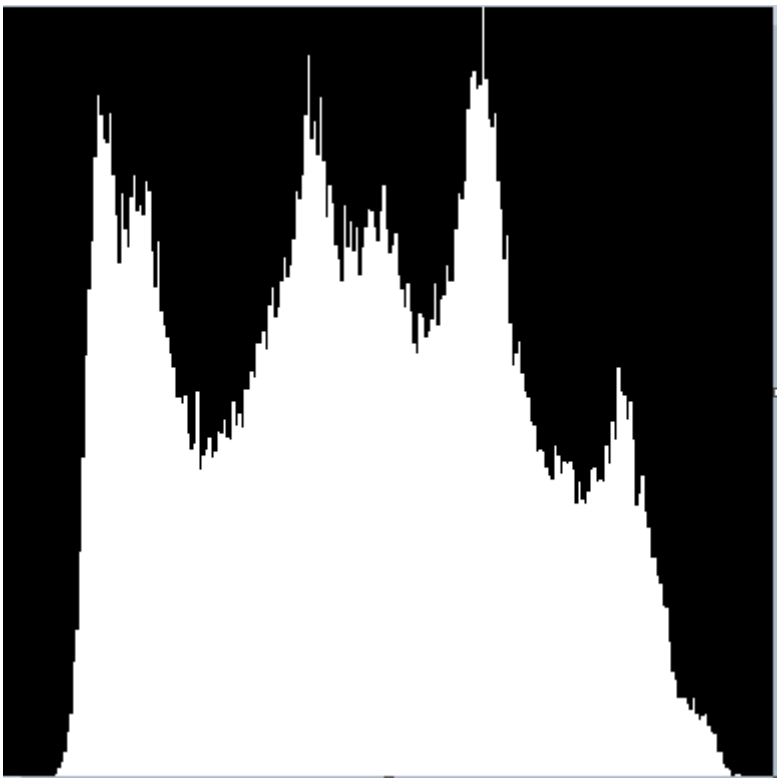

Figure 4.11: Histogram of barbara.png before watermarking

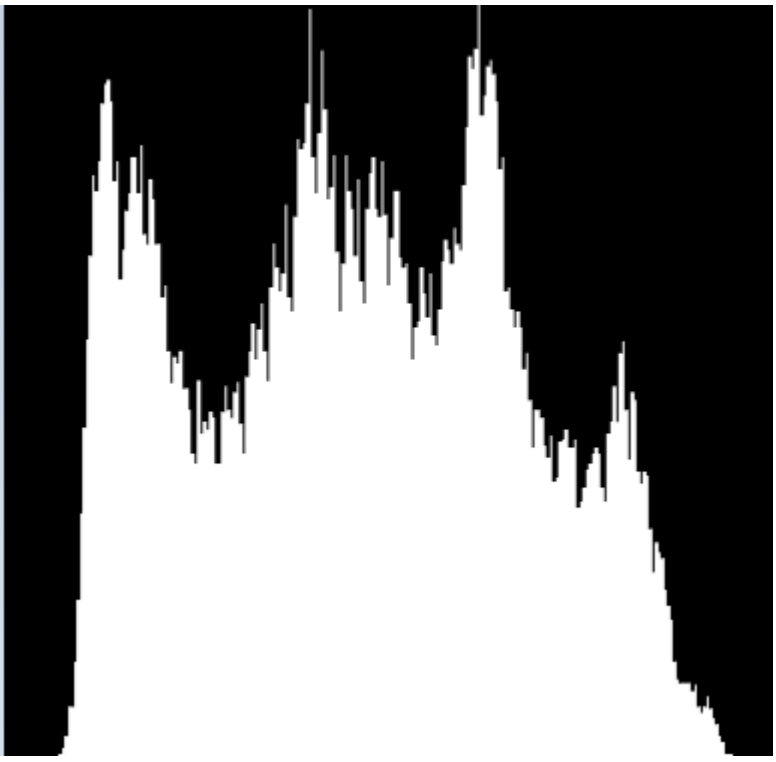

Figure 4.12: Histogram of babara.png after watermarking

4.2.3 Comparison of histograms of Original and Watermarked images.

	Baboon.png	Lena.png	Barbara.png
Correlation	1.000000	1.000000	1.000000
Chi-Square	0.000000	0.000000	0.000000
Intersection	152.409301	45.322269	39.114622
Bhattacharyya distance	0.000000	0.000000	0.000000

Table 4.1: Results after comparing histogram using different methods

It can be seen from above table that histograms of original and watermarked image have a very good match. Value 1 for correlation and value 0 for both Chi-Square and Bhattacharya distance proves the same. Similarly high value of Intersection also favours that images does not undergo high modification.

4.2.4 Results after cropping the image

Original image	Size of cropped image	Cropped image/original image	Pixels watermarked in original image(o)	Watermarke-d Pixels in cropped image(c)	Ratio c/o
baboon.png	128*128	0.0625	49236	3074	0.0624
	256*256	0.25	49236	12366	0.2511
	384*384	0.5625	49236	27615	0.5608
lena.png	128*128	0.0625	49293	3057	0.0620
	256*256	0.25	49293	12346	0.250
	384*384	0.5625	49293	27788	0.5637
barbara.png	128*128	0.0625	48790	2990	0.0612
	256*256	0.25	48790	12132	0.248
	384*384	0.5625	48790	27497	0.5635

Table 4.2: Ratio of pixels that can be retrieved after cropping

Above results after cropping the image in various amounts like keeping $\frac{1}{16}$, $\frac{1}{4}$, or $\frac{3}{4}$ also keeps the watermarked pixels in almost same fraction. So it shows that our watermarking algorithm is robust against cropping.

4.2.3 Results after applying Median Filter

No. of pixels watermarked in original image(o)	Window size of median filter	Watermarked pixels in blurred image(b)	Ratio b/o
49236	5	26380	0.536
49236	7	25790	0.524
49236	9	25765	0.523
49236	11	25441	0.517
49236	13	25490	0.518
49236	15	25362	0.515
49236	17	25299	0.514
49236	19	25326	0.514
49236	21	25269	0.513
49236	23	25272	0.513
49236	25	25408	0.516
49236	27	25200	0.512
49236	29	25045	0.509
49236	31	25157	0.511
49236	33	25175	0.511
49236	35	25134	0.510
49236	37	25264	0.513

Table 4.3: Effect of applying median filter to baboon.png

No. of pixels watermarked in original image(o)	Window size of median filter	Watermarked pixels in blurred image(b)	Ratio=b/o
49293	5	26983	0.547
49293	7	26310	0.534
49293	9	25860	0.525
49293	11	25626	0.520
49293	13	25494	0.517
49293	15	25530	0.518
49293	17	25447	0.516
49293	19	25128	0.510
49293	21	25288	0.513
49293	23	25324	0.514
49293	25	25403	0.515
49293	27	25204	0.511
49293	29	25081	0.509
49293	31	25142	0.510
49293	33	25203	0.511
49293	35	25076	0.508
49293	37	25016	0.507

Table 4.4: Effect of applying median filter to lena.png

No. of pixels watermarked in original image (o)	Window size	No. of pixels watermarked in blurred image (b)	Ratio=b/o
48970	5	26773	0.547
48970	7	25780	0.526
48970	9	25355	0.518
48970	11	25253	0.516
48970	13	25211	0.515
48970	15	24814	0.507
48970	17	24815	0.507
48970	19	24925	0.509
48970	21	24885	0.508
48970	23	24859	0.508
48970	25	24994	0.510
48970	27	24932	0.509
48970	29	25037	0.511
48970	31	24861	0.508
48970	33	24934	0.509
48970	35	25077	0.512
48970	37	25259	0.516

Table 4.5: Effects of applying median filter to Barbara.png

4.2.5 Results after applying Guassian filter.

No. of pixels watermarked in original image (o)	Window size of Gaussian filter	No. of pixels watermarked in blurred image (b)	Ratio=b/o
49236	5	24646	0.500
49236	7	24460	0.497
49236	9	24502	0.497
49236	11	24663	0.500
49236	13	24669	0.501
49236	15	24590	0.499
49236	17	24775	0.503
49236	19	24583	0.499
49236	21	24689	0.501
49236	23	24858	0.504
49236	25	24467	0.497
49236	27	24638	0.500
49236	29	24576	0.500
49236	31	24466	0.497
49236	33	24664	0.500
49236	35	24565	0.499
49236	37	24514	0.498

Table 4.6: Effect of applying guassian filter to baboon.png

No. of pixels watermarked in original image (o)	Window size of Gaussian filter	No. of pixels watermarked in blurred image (b)	Ratio=b/o
49293	5	24753	0.502
49293	7	24822	0.503
49293	9	24591	0.499
49293	11	24599	0.499
49293	13	24650	0.500
49293	15	24641	0.500
49293	17	24759	0.502
49293	19	24702	0.501
49293	21	24549	0.498
49293	23	24505	0.497
49293	25	24624	0.499
49293	27	24534	0.497
49293	29	24466	0.496
49293	31	24426	0.495
49293	33	24653	0.500
49293	35	24560	0.498
49293	37	24726	0.501

Table 4.7: Effect of applying guassian filter to lena.png

No. of pixels watermarked in original image (o)	Window size of Gaussian filter	No. of pixels watermarked in blurred image (b)	Ratio=b/o
48970	5	24408	0.498
48970	7	24432	0.499
48970	9	24261	0.495
48970	11	24523	0.500
48970	13	24380	0.498
48970	15	24451	0.499
48970	17	24261	0.495
48970	19	24180	0.494
48970	21	24498	0.500
48970	23	24471	0.498
48970	25	24239	0.495
48970	27	24561	0.501
48970	29	24322	0.497
48970	31	24503	0.500
48970	33	24437	0.500
48970	35	24321	0.495
48970	37	24287	0.496

Table 4.8: Effect of applying guassian filter to Barbara.png

The above results in tabular form show that after blurring the image to very large extent or using large window size almost half of watermarked pixels remain intact for both Guassian and Median Blur. However this value remains constant for small window size as well as large window size.

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

A new approach of digital image watermarking based on application of database watermarking has been presented and the insertion and extraction watermarking algorithms are discussed in detail. In database watermarking beizer cubic curve was inserted in attributes fractional value and extracted after performing various database operations like insertion and deletion of records. The approach was quite robust and Our goal has been to ensure that our watermarking approach is also robust for watermarking digital images. We discussed our approach's robustness analytically and quantitatively. However, the persistency of the watermark after various malicious and benign modifications, as a sub problem, may be evaluated by performing various image manipulations. This evaluation process may sound convincing, but it is application-specific and cannot be generalized very well. The approach discussed has very low cost both in terms of time and money and does not require many resources , cryptographic hash function is used to embed the watermark in image pixels. The physical location of pixels, value of key and α (the density parameter) play major role in deciding which pixels must be selected. All these parameters can be set by watermark generating entity based on image to be watermarked.

Since key based watermarking is new to field of watermarking and can provide more secure and robust watermarking techniques. The cryptanalysis of these watermarks need to be done in order to know about the percentage of security they can offer and this cryptanalysis along with enhancement of key generation process, taking into consideration the buyer specific key and image attributes must be performed. Apart from that, this watermarking scheme can be applied to all image types including jpeg, tiff and can be checked for different types of image manipulations and image compression. A server that stores the key for different images can be taken into account and since image is watermarked with different keys for different clients, a client distributing the copies of watermarked image can be tracked easily so it helps in theft protection and security of

digital images. The scheme can be employed in securing images posted on various social networking sites nowadays

References

1) Soumik Das, Pradosh Bandhopadhyay, Shauvik Paul, Arindam Sinha Ray and Dr. Monalisa Banerjee, "A new introduction towards invisible Image Watermarking on color image" International Advance Computing Conference, (IACC),IEEE 2009.

2) I. Cox, M. Miller, J. Bloom and C. Honsinger, "Digital Watermarking", Academic Press, USA 2002.

3) R. Sion, M. Atallah and S.Prabhakar, "Rights Protection for Relational Data", Transactions on Knowledge and Data Engineering, vol. 16, no.12, IEEE 2004, pp. 1509-1525.

4) Hae Yong Kim, Amir Afif, "Secure Authentication Watermarking For Binary Images", Proceedings of the XVI Brazilian Symposium on Computer Graphics and Image Processing, IEEE 2003.

5) R. Chamlawi, A. Khan, I. Usman, "Authentication and recovery of images using multiple watermarks", Computers & Electrical Engineering 36 2010, 578–584.

6) Zhiyong Li, Junmin Liu and Weicheng Tao, "A Novel Relational Database Watermarking Algorithm Based on Clustering and Polar Angle Expansion", International Journal of Security and Its Applications, Vol. 7, No. 2, March, 2013

7) Mohammad Abdullatif, Akram M. Zeki, Jalel Chebil, Teddy Surya Gunawan, "Properties of digital image watermarking",9th International Colloquium on Signal Processing and its Applications, IEEE 2013.

8) Khalid A. Darabkh, Iyad F. Jafar, Raed T. Al-Zubi, Mohammed Hawa, " An improved image least significant bit replacement method", MIPRO 2014.

9) Jae-Woo Lee, "A policy of copyright protection using authentication key based on Digital watermarking", International Conference on Multimedia and ubiquitous Engineering, IEEE 2007.

10) Liu Tong, Qiu Zheng-ding, "The Survey of Digital Watermarking-based Image Authentication Techniques", IEEE 2002.

11) Jiang-bin zheng, David dagan feng, Rong-chun zhao," a multi-channel framework for image watermarking". Fourth International Conference on Machine Learning and Cybernetics, IEEE 2005.

12) Sarabjeet S. Bedi, and Shekhar Verma, "A Design of Secure Watermarking Scheme for Images in Spatial Domain",IEEE 2006.

13) Rakesh Agrawal, Peter J. Haas, Jerry Kiernan," Watermarking relational data: framework, algorithms and analysis" The VLDB Journal, Springer 2003.

14) A Umaamaheshvari and Dr K Thanushkodi." Robust Image Watermarking Based On Block Based Error Correction Code", International Conference on current Trends in Engineering and Technology, ICCTET'13, IEEE 2013.

15) Qing Liu and Jun Ying," Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis",Symposium on electrical & Electronics Engineering (EEESYM),IEEE 2012.

16) Haohao Song, Zihua Qiu, Jian Gu," A Novel Semi-fragile Image Watermarking Scheme Based on Wavelet", IEEE 2010.

17) HUA Yuning WANG A-na WU Bo," An Algorithm for Image Authentication Based on Fragile Watermarking", IEEE 2010.

18) Tan Yuxi, Tang Lei, Gao Zhinian," A Rotation Resistant Image Watermarking Algorithm via Circle", Eighth International Conference on Computational Intelligence and Security, 2012.

19) Meryem Benyoussef, Samira Mabtoul, Mohamed El marraki, Driss Aboutajdine," Medical Image Watermarking for Copyright Protection Based on Visual Cryptography", IEEE 2014.

20) Pradosh Bandyopadhyay, 2 Soumik Das, 3 Shauvik Paul," A Dynamic Watermarking Scheme for Color Image Authentication", International Conference on Advances in Recent Technologies in Communication and Computing, 2009.

21) Wei-Fan Hsieh, Pei-Yu Lin, "Analyze the Digital Watermarking Security Demands for the Facebook Website", Sixth International Conference on Genetic and Evolutionary Computing, IEEE 2012.

22) Dr.M.A.Dorairangaswamy, B.Padhmavathi," An Effective Blind Watermarking Scheme for Protecting Rightful Ownership of Digital Images", IEEE 2009.

23) Neeraj Bhargava, M.M. Sharma, Abhimanyu Singh Garhwal and Manish Mathuria,"Digital Image Authentication System Based on Digital Watermarking", International Conference on Radar, Communication and Computing (ICRCC), IEEE 2012.

24) Jiang Xuehua," Digital Watermarking and Its Application in Image Copyright Protection", International Conference on Intelligent Computation Technology and Automation, IEEE 2010.

25) Dr.M.A Dorairangaswamy," Protecting Digital-Image Copyrights: A Robust and Blind Watermarking Scheme", IEEE 2009.

26) Sudip Ghosh,Subhojit Chatterjee," A New Algorithm On Wavelet Based Robust Invisible Digital Image Watermarking for Multimedia Security"in Electronic Design, Computer Networks and Automated Verification (EDCAV), IEEE 2015

27) Jiaming He, Hongbin Zhang," Digital Right Management Model Based on Cryptography and Digital Watermarking" International Conference on Computer Science and Software Engineering, IEEE 2008

28) Keta Raval, Sameena Zafar,"Digital Watermarking with Copyrigh Authentication for Image Communication", International Conference on Intelligent Systems and Signal Processing (ISSP), IEEE 2013.

29) Munesh Chandra, Shikha Pandel, Rama Chaudhary," Digital Watermarking Technique for Protecting Digital Images", Computer science and information technology (ICCSIT), IEEE 2010.