

# Efficient Digital Watermarking Algorithm Using Frequency Transform

BY

**Humayan Kabir**

ID:171-35-184

Department of Software Engineering (PC)

Supervised By

Nayeem Hasan

Lecturer (Senior scale), The Department of Software Engineering

Daffodil International University



Daffodil International University

Dhaka, Bangladesh

June, 2021

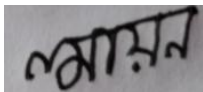
## **APPROVAL**

This thesis titled “Efficient Digital Watermarking Algorithm Using Frequency Transform”, submitted by Humayan Kabir to the Department of Software Engineering, Daffodil International University .

## DECLARATION

We hereby declare that we have taken this thesis under the supervision of  
Nayeem Hasan, Lecturer (senior), Department of Software Engineering,  
Daffodil International University (PC).

Humayan Kabir



Supervisor Signature



(Nayeem Hasan)



## **ACKNOWLEDGEMENT**

I would like to take this opportunity to express my gratitude to my supervisor Nayeem Hasan sir (senior lecturer, Dept. of Software Engineering ,Daffodil International University)for his generous guidance and patience given to me in the past seven months.His different kinds of help and stimulation, as well as his inspiring advice are extremely essential and valuable in my research papers.

Finally, I am deeply bound to my family for their unconditional love and support over the times during this pandemic.

This work is dedicated to my family and all of the teacher in my life for support and patience.

# LIST OF CONTENTS

<b>Approval</b>	<b>II</b>
<b>Declaration</b>	<b>III</b>
<b>Acknowledgement</b>	<b>IV</b>
<b>Abstract</b>	<b>I</b>
<b>1 Introduction</b>	<b>2</b>
1.1 Background	2
1.2 Research Objective	3
1.3 Contributions	4
1.4 The Structure of Thesis	5
<b>2 Literature Review</b>	<b>6</b>
2.1 Security in Multimedia Communications	6
2.2 Cryptography	9
<b>Chapter 3 :Novel Watermarking Schemes</b>	<b>12</b>
3.1 Watermark Preprocess	12
3.2 Simple image watermark	13
3.2.1 Binary image processing	15
3.2.2 Rgb2grayscale image processing	19
3.3 DCT(Discrete cosine Transform)	22
3.4 DWT(Discrete Wavelet Transform)	24
3.5 DFT(Discrete Fourier Transform)	26

<b>Chapter 4: Experimental Results</b>	28
4.1 Test on Robustness	28
4.2 Comparative Analysis between DCT & DWT Techniques	29
4.3 Overall Comparison	40
4.4 Test on Fidelity	41
4.5 Other Features of the Scheme	42
4. 6. Conclusion	43
<b>Chapter5: Conclusion</b>	45
<b>Bibliography</b>	47

### **LIST OF FIGURE**

Figure 2.1: Symmetric Cryptosystem	10
Figure 2.2: Asymmetric Cryptosystems	11
Figure 4.1: DCT watermark	30
Figure 4.2: DWT Watermark	31
Figure 4.3: The signal of DCT image processed	32
Figure 4.4: The original and reconstruction of DWT image processing	33
Figure 4.5: The denoise Signal with wavelet for the second input signal condition model	34
Figure 4.6: DCT and DWT embedding process.	35
Figure 4.7: DCT and DWT extraction process	36
Figure 4.8:DCT watermark original image and compressed image	37
Figure 4.9: DWT watermark original image and compressed image	38
Figure 4.10: Graph of DCT and DWT information loose and total information	39
Figure 4.11: Graph for DCT and DWT information loose	39
Figure 4.12: Comparison between JPEG quality factor	41
Figure 4.13: A conceptual illustration on the performance of the proposed scheme	43



## **LIST OF ABBREVIATIONS**

PSNR-Pick Signal noise Ratio

FM-Frequency Module

LL-Low Sub-band

HH-High Sub-band

MPEG-Moving Picture Experts Group

NC-normalize correlation

FFT-First fourier transform



## **Abstract**

There is a blast of data exchange on the internet and the large use of digital media. So, digital data owners can quickly and massively transfer multimedia documents through the Internet. It has cause intense interest in multimedia security and multimedia copyright protection. In this paper, a comprehensive approach protecting and managing image, audio and video copyrights with water-marking techniques is introduced. We propose a efficient digital water-marking scheme based on the scene change analysis, error correction code. Our digital water-marking algorithm is robust against the attacks of frame cascading, averaging and statistical analysis, which were not fixed effectively in the past. It started with a complete survey about current water-marking technologies. We have discovered that none of the existing schemes was admit of with-stand all attacks. Accordingly, we came up with the idea of embedding a single watermark of different parts into different images, audios and videos. Then we analyze the strength of different water-marking schemes. It optimizes the quality of the water-marked images, audios and videos. Also, our scheme allows blind recovery of the embedded watermark, which does not need the original images, audios and videos and the watermark is perceptually invisible.

# Chapter 1

## Introduction

With the rapid growth of the Internet and multimedia system the use of social media application like facebook,instagram,twitter and ring id here lot of memes,image,audio and video shares without of its copy rights.So people loose their authentic and creative work in this field so we can say it is un-ethical.Ethical way is everyone will claim the authentic and creative work efficiently.So that the real talent will not harressed in the particular way.We also ensure the real talent will get its reward after in this particular algorithm use so we can say that this efficient way we will get a solution for the data piracy.

### 1.1 Background

In computing, software piracy data authenticity is a gobal issue so that the data authentication remain in danger.Because the broadcasting monitoring ,copy protection ,copyrights protection and unauthorized access of the data still in danger for this Code is a 2-Dimensional barcode that can store different kinds of information such as a link, plain text, SMS text message, addresses, URLs, Geo-location, email, phone numbers or contact information. Watermarked Codes were introduced in Japan in order to track automobile parts but they became well known only when they were used as an advertising medium to distribute additional information to the users. When a user scans a Watermarked Code with his/her smartphone camera using the appropriate WatermarkedCode software reader, he/she can reach the additional information. Thus Watermarked Codes can be described as paper-based hyperlinks. This novel technology is now used in many new areas and according to latest measurements has been adopted by millions of smartphone users. This explosive growth in the last years indicates that that Watermarked codes are not just a momentary fashion but a very powerful and versatile tool for the future. Moreover, exploring the way that people face Watermarked Codes is a task that gave us great motivation. Analyzing and defining people's behavior is usually a difficult assignment. However, it is essential when we examine some aspects of the problem that are affected by the users' behavior. Furthermore, social engineering attacks, which are included in our research, are also based in human behavior..In this particular way if we can ensure the copy rights of creative work like image, audio and videos the real talent will not hamper in the efficient way.

## **1.2 Research objective**

In data authentication we proposed the schemes in watermarking so that in image processing we can process the original image for the author of its copyright protection and copy protection broadcasting method of copyright claim. Based on these, a new approach and procedures for multimedia security based on watermarking are proposed. As identical watermark is used within each motionless scene and independent watermarks are used for successive different scenes, the proposed method is robust in the method of frame dropping, averaging, swapping, interpolation and lossy compression. At the same time, error correcting code is pulled out from the audio, image and video channel and embedded in the audio channel, which provides extra information for recovery of extracted watermark. Moreover, the scheme allows blind repositioning of embedded watermark which does not need the original audio, image and video. This research can be continuous by applying this new developed scheme to specific environment or application and test its usefulness.

## **1.3 Contribution**

Our research work has the following contributions:

- To increase the robustness, the watermark strength of the scheme, we propose several approaches. The first one is the visual audio water-marking scheme. As videos consist of both video and audio channels, the wellness of our scheme can be boost by including an audio watermark work. Therefore, we embed error correcting codes of a video watermark as an audio watermark, which can refine the retrieved image watermark during watermark detection work efficiently.

- The second approach is another with different watermarking schemes. As no existing scheme is resistant against all attacks, we employ the robust scheme to embed different parts of a watermark into different scenarios. Thus, the proposed scheme is capable of resisting most of the common attacks.
- We proposed a new scheme which applies scene change detection and scrambled watermarks in audio, image and video. The scheme is powerful against frame dropping, as the same part of the watermark is embedded into the frames of image in order. For different scenarios, different parts of the watermark are used, making the scheme powerful against frame averaging and statistical analysis. This scheme is innovative in attacking the problems that are not solved effectively in the past.
- We compare the proposed scheme with the existing scheme in different regards and discuss the advantages and the disadvantages of our scheme.

Our talk cultivates an innovative idea in embedding different parts of a watermark according to scene changes, embedding its error correcting codes as an audio watermark in an efficient way. This address is never explored in literature, and its advantages are clear and significant. The usefulness of this scheme is verified through a number of experiments.

#### **1.4 The structure of thesis**

This paper is organized as 5 chapters. The next chapter introduces the issues related to multimedia security and different multimedia water-marking techniques, and a survey on current watermark techniques efficiently in order. Novel image water-marking scheme is described in chapter-3 and the experimental results in Chapter-4 are given in order. Finally, a conclusion would be given in chapter no-5.

## **Chapter 2**

### **Literature Review**

Now-a-days the digital media is easily to be reproduced due to the rapidly growth of internet and the multimedia technologies, this drives to emergency need to settle the security and copyright protection issues. Therefore, the field of digital water-marking increase extremely fast in these few years .

The purpose of a digital water-mark is to set auxiliary information into a digital signal by making small changes that are not noticeable to its intended receiver. For instance, in the case of multimedia water-marking, the hidden signal should not result in any visible or detectable distortions. Because the fixed signals enable invisible tags to be attached to digital documents, watermarks are strong tools that will play a role in solving the growing digital property identification problem.

This chapter overviews previous work in digital image water-marking and related fields. We first have a look of two popular security tools, digital signatures and cryptography. Then the principle and the techniques of digital water-marking are discussed. Besides, the important differences and the advantages that water-marking techniques provide over these keep going technologies are explained. Moreover, the important ingredients of video water-marking are presented. The following section reviews a number of techniques proposed in the literature. Then different water-marking algorithms are implemented and evaluated. Finally, a comparison among various video water-marking is given.

## **2.1 Security in Multimedia Communications**

Security in social media or multimedia communication is very essential in this era of communication. Because the main watermark theory is we know that the copy rights authenticity to claim author. And the digital water-marking theory express that bits of patterns of audio, images and videos which provides of the digital copy rights .this digital copy rights is now in danger because the unauthorized share of memes and images is day by day grow fast so to secure we can improve the process we want to create the efficient way by implementing a digital algorithm.

## **2.2 Cryptography**

Cryptography is the first technology that content owners would turn to. It is the most probably the most common method of protecting digital documents and certainly one of the best developed as a science. Before delivery, the content is encrypted and the a decryption key is provided only to those who have permission to access the legitimate copies of the content. Then, the encrypted file can be made available through the Internet, but would be useless to a pirate without appropriate key. After encrypted, the structure of the message is changed. It is meaningless and unintelligible unless it is decrypted .

There are two kinds of crypto systems: symmetric and asymmetric . Symmetric crypto systems use the same key, known as the secret key, to encrypt and decrypt a message, and asymmetric crypto systems use one key, named as public key, to encrypt a message and a different key, named as private key, to decrypt it. Asymmetric cryptosystems are also called public key crypto systems .

Symmetric crypto systems have a problem: "how do you transport the secret key from the sender to the recipient securely and in a tamper proof fashion?" . If you



could send the secret key securely, in theory, you then would simply use that secure channel to send your message instead of encrypting your message with symmetric cryptosystem. All the time, trusted couriers are used as a solution to this problem.

One example using symmetric crypto system is shown in Figure 2.1. Humayan and Kabir want to communicate in secret, while

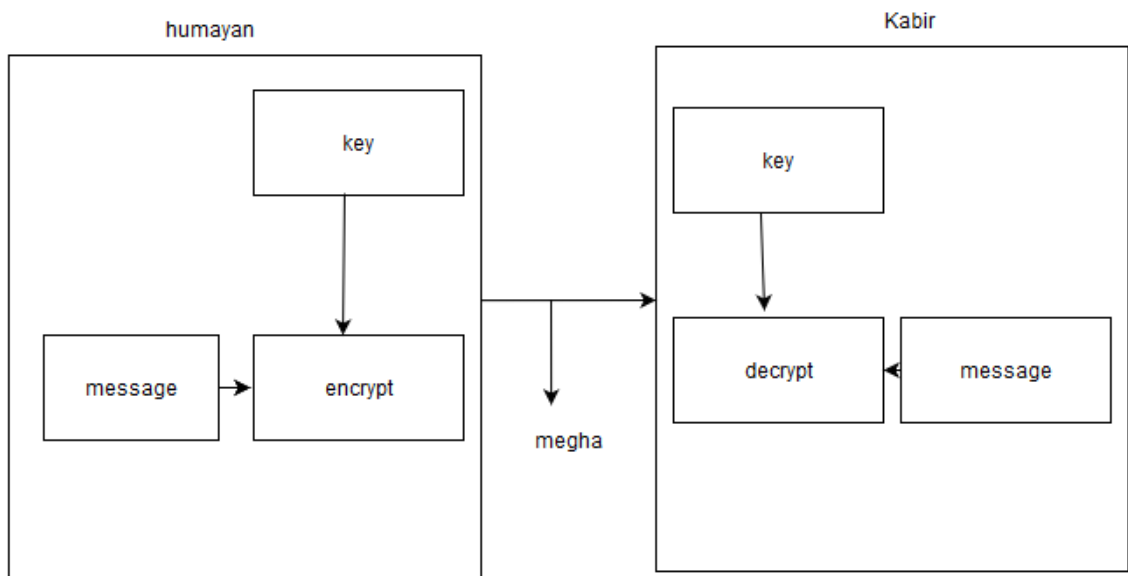


Figure 2.1: Symmetric Cryptosystem

Megha wants to eavesdrop. Humayan and kabir could be military jets, online businesses or just friends trying to have a private conversation. They cannot stop megha listening to their radio signals, so they can keep communication by using cryptography.

Asymmetric crypto system is another more efficient and reliable solution, such as RSA, which is the popular security tool . Asymmetric crypto systems is different,

because it splits the key up into a public key for encryption and a secret key for decryption. It's not possible to determine the secret key from the public key.

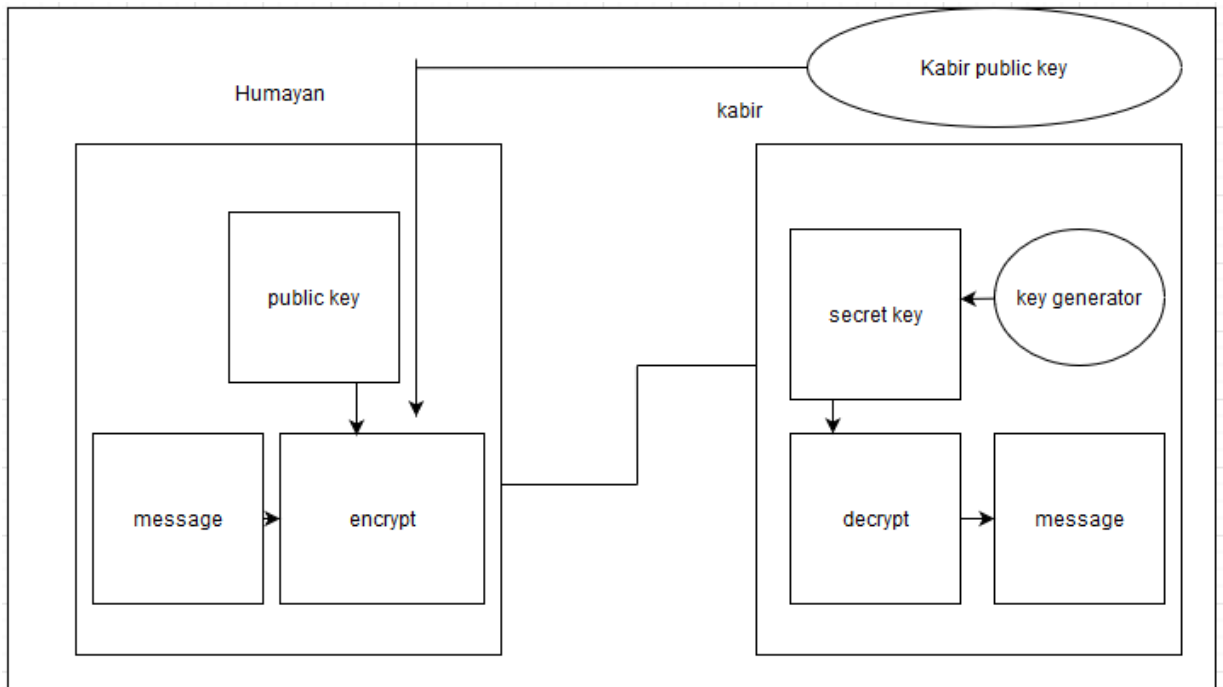


Figure 2.2: Asymmetric Cryptosystems

In the Figure 2.2, Kabir creates a pair of keys and tells everyone, including Megha, her public key, while only she knows her secret key. Anyone can use Humayan's receive key only he will use the key of the process in this way and decrypted message will be processed encryprd in this way .All messages will be encrypted to decrypted in the better way.

# Chapter 3

## Novel Watermarking Schemes

In this chapter, we will compressed image the original image in novel watermarking propess like the original water-marked image,RGB2gray image processing,discrete cosine teansform ,discrete fourier transform and the discrete wavelet transform.we also see here some of source code also in the method.This novel water-marking schemes shows that the real image processing way.

### 3.1 Watermark Preprocess

A watermark is scrambled into different subsmall parts in a preprocess, and they are embedded to different scenes so that the scheme can resist a number of attacks to to the video. A 256-grey-level image is used as the watermark, so 8 bits can represent each pixel sequence. The watermark is first scaled to a particular size as follows:.

$$2n \leq m, n > 0 \dots\dots\dots (3.1)$$

$$p + q = n, p, q > 0 \dots\dots\dots (3.2)$$

where  $m$  is the number of scene changes and  $n, p, q$  are positive integer number.

The size of the watermark is represented as given below:

$$64 \cdot 2p \times 64 \cdot 2q \dots\dots\dots (3.3)$$

Then the watermark is divided into  $2 \cdot \pi$  small images with size  $64 \times$

64. Figure 3.2 shows the procedure of the watermark.

In the other step ,we will apply watermark process in a original image to large gray ratio image for the better image authentication so that the author can claim the right of its authenciticity.Our proposed schmes shows that the change of image after

watermark.

### **3.2 Simple image watermark**

Now we want a picture to make it simple watermark is given below:

#### **Source code**

```
cman=imread('2.png');  
logo=imread('10.png');  
graycman=rgb2gray(cman);  
graylog=rgb2gray(logo);  
amsg=uint8(graylog);  
[r,c]=size(amsg);  
Msg=zeros(r,c);  
fori=1:r
```

**Original image:**



**Image after processed:**



### **3.2.1 Binary image processing**

Now we want to make a picture into binary image processing method:

Source code:

```
for j=1:c
```

```
bmsg=dec2bin(msg(i,j),8);
```

```
cmsg=str2double(bmsg);
```

```
msg(i,j)=bitget(cmsg,8);
```

```
end
```

```
end
```

```
ahst=uint8(graycman);
```

```
[R,C]=size(ahst);
```

```
for k=1:R
```

**Original image:**



**Image after processed:**



### **3.2.2 Rgb2grayscale image processing**

**Source code:**

```
function out=jpeg_scan(N,M);  
scan_order = zeros(N,M);  
scan_order(1,1) = 1;  
diag_down = 1; x = 1; y = 2;  
for k = 2:N*M,  
scan_order(x,y) = k;
```



```

ifdiag_down==1, y=y-1;x=x+1; end;

ifdiag_down==0, y=y+1;x=x-1; end;

if y>N, y=N; x=x+2; diag_down=1; end;

if x>M, x=M; y=y+2; diag_down=0; end;

if y<1, y=1; diag_down=0; end;

if x<1, x=1; diag_down=1; end;

end;

out=scan_order;

%host image

host=imread('Lena512.bmp');

yCbCr = rgb2ycbcr(host);

Y = double(yCbCr(:,:,1));

[xm,xn] = size(Y);

scan_order = jpeg_scan(xm,xn);

% call watermark image (grayscale image)

watermark = imread('logo.bmp');

Wm= ?????

%transform Y component of host image to DCT

Y_dct = dct2(Y);

temp = Y_dct(:);

zz_dct_koeff = temp;

zz_dct_koeff(scan_order(:)) = temp;

V = zz_dct_koeff(L+1:L+n);

V = V + a*abs(V).*Wm;

zz_dct_koeff(L+1:L+n) = V;

```

```
temp = zz_dct_koeff(scan_order(:));  
Yx_dct = reshape(temp,xm,xn);  
Yx = uint8(idct2(Yx_dct));  
yCbCr(:, :, 1) = Yx;  
wtm = ycbcr2rgb(yCbCr);  
imwrite(wtm,'watermarked_image.bmp','bmp')  
figure(1);imshow(host);title('HostImage')  
figure(2);imshow(wtm);title('WatermarkedImage')
```

**Original image:**



**Image after processed:**



### 3.3 DCT(Discrete cosine Transform)

**Original image:**

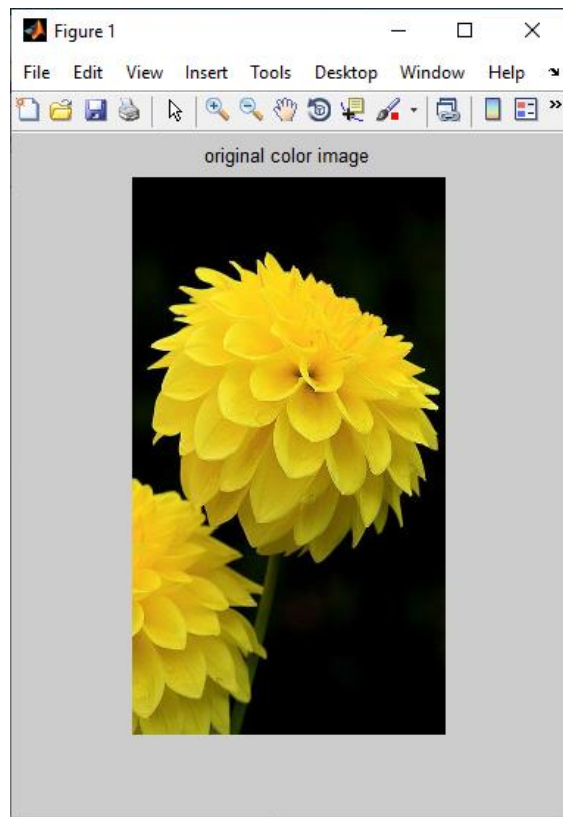


**Image after processed:**

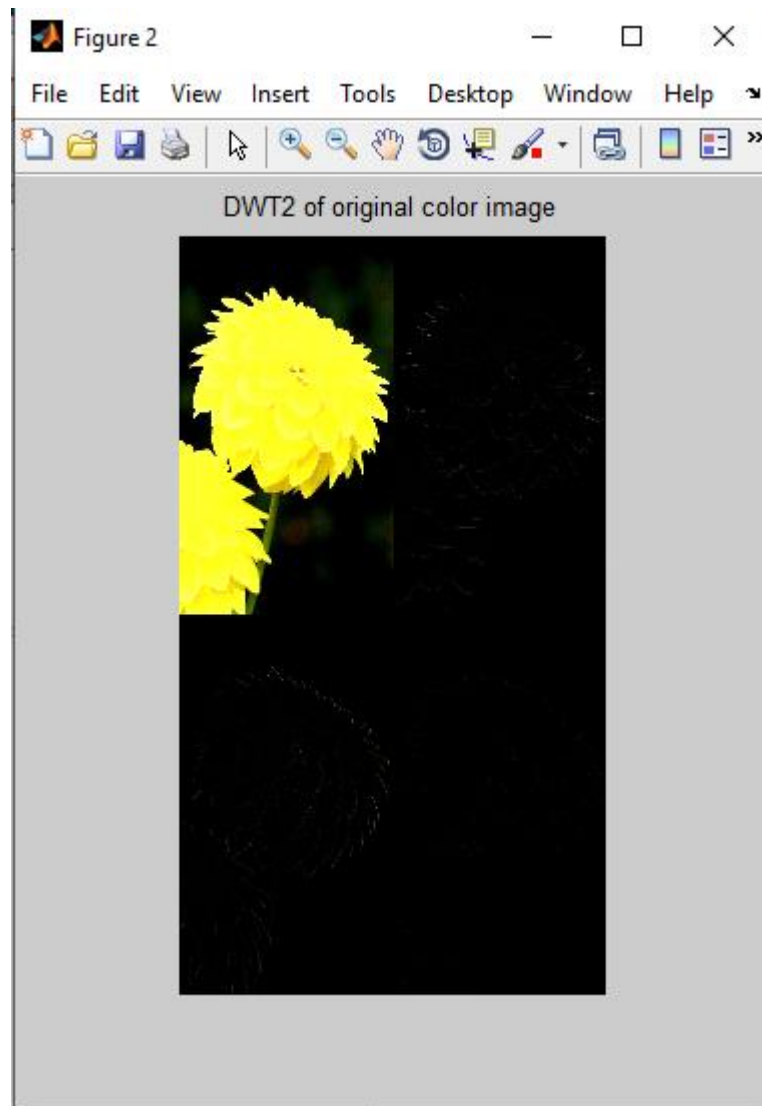


### 3.4 DWT(Discrete Wavelet Transform)

**Original image:**



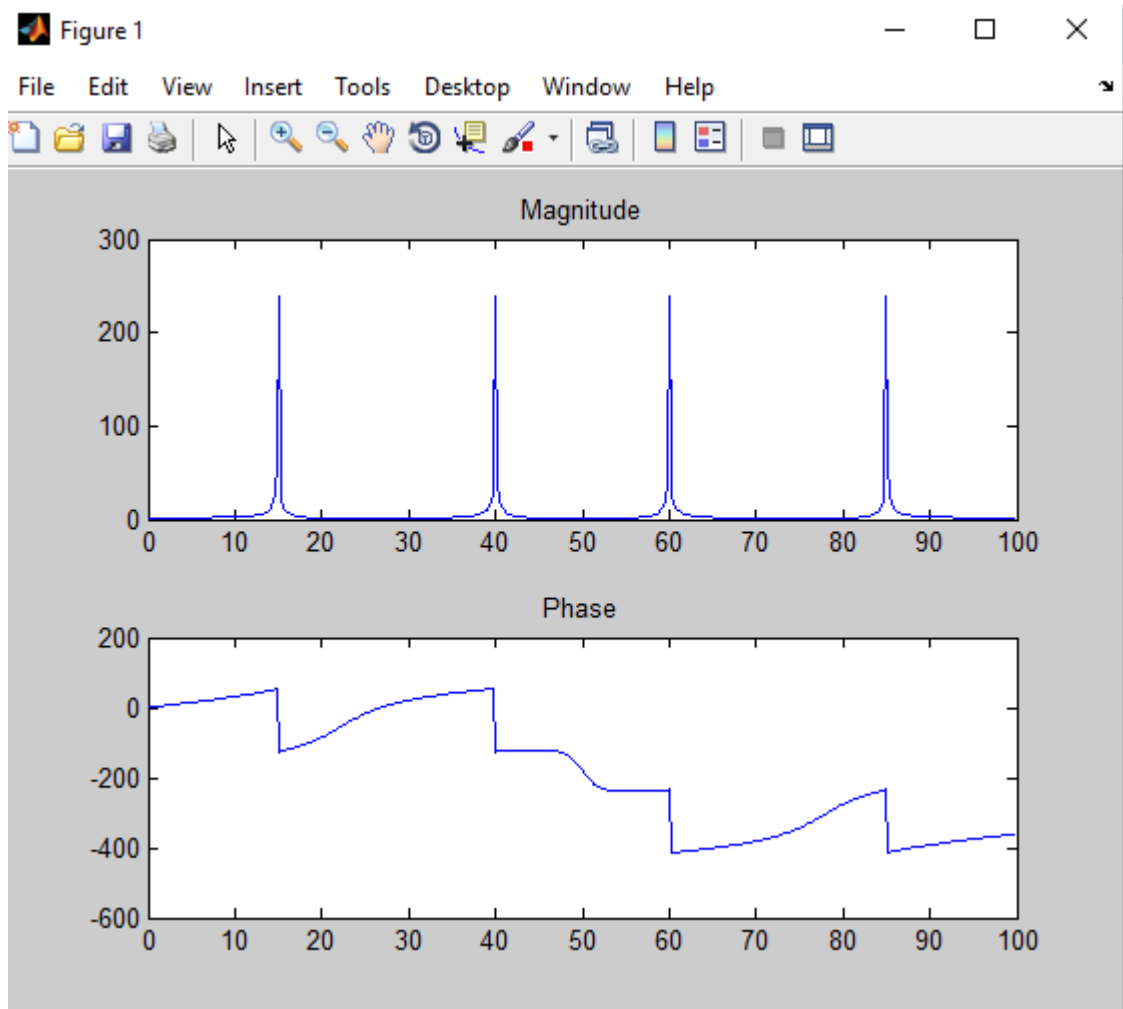
**Image after processed:**





### 3.5 DFT(Discrete Fourier Transform)

Image after processed:



## **Chapter 4**

### **Experimental Results**

In this chapter, we present our experimental results on the scene-based water-marking scheme, the hybrid water-marking scheme and the GA-based water-marking scheme. The chapter are mainly divided into two types: test on robustness in efficient way and test on fidelity in efficient way. In the following sections, we present the implementation detail of proposed schemes and the experimental results which we found.

#### **4.1 Test on Robustness**

In this section, the robustness of the scene based water-marking scheme and the hybrid water-marking scheme is tested. To implement the proposed water-marking scheme, the software Virtual-Dub is employed efficiently. The performance of the new video water-marking scheme is evaluated through several experiments: the experiment with various dropping ratio, the experiment with the various number of frame colluded efficiently, the experiment with the various quality factor of MPEG, and the test of Robustness with Stir-Mark 4.0. Another DWT (discrete wavelet transform)based water-marking scheme, which embeds an identical watermark in all frames , is implemented to compare with the proposed scheme. A video clip with 1526 frames of size 352 x 288 is used in our experiment way. The video consists of 10 scene changes in the frame. The experiments are done on a desktop computer with Pentium 4 CPU(central processing unit) 2.00GHz and 512MB RAM.

Distinguishable attacks, including frame dropping, frame averaging, lossy

compression, and Stir-Mark 4.0 , are carried out to the water-marked video to test the robustness of our scheme. The audio channel is also attacked by adding some noises into it after water-marking. After extracting and refining the watermarks, a quantitative measurement is required to provide an objective judgment of the extraction fidelity in water-marking efficiently. Therefore, a similarity measurement of the extracted and the referenced watermarks can be defined

NC values are retrieved when the water-marked video is facing different attacks in a way . The experimental results are described in detail in the following sections is given .

#### 4.2 Comparative Analysis between DCT & DWT Techniques

In DCT and DWT We found the difference as given below:

DCT:

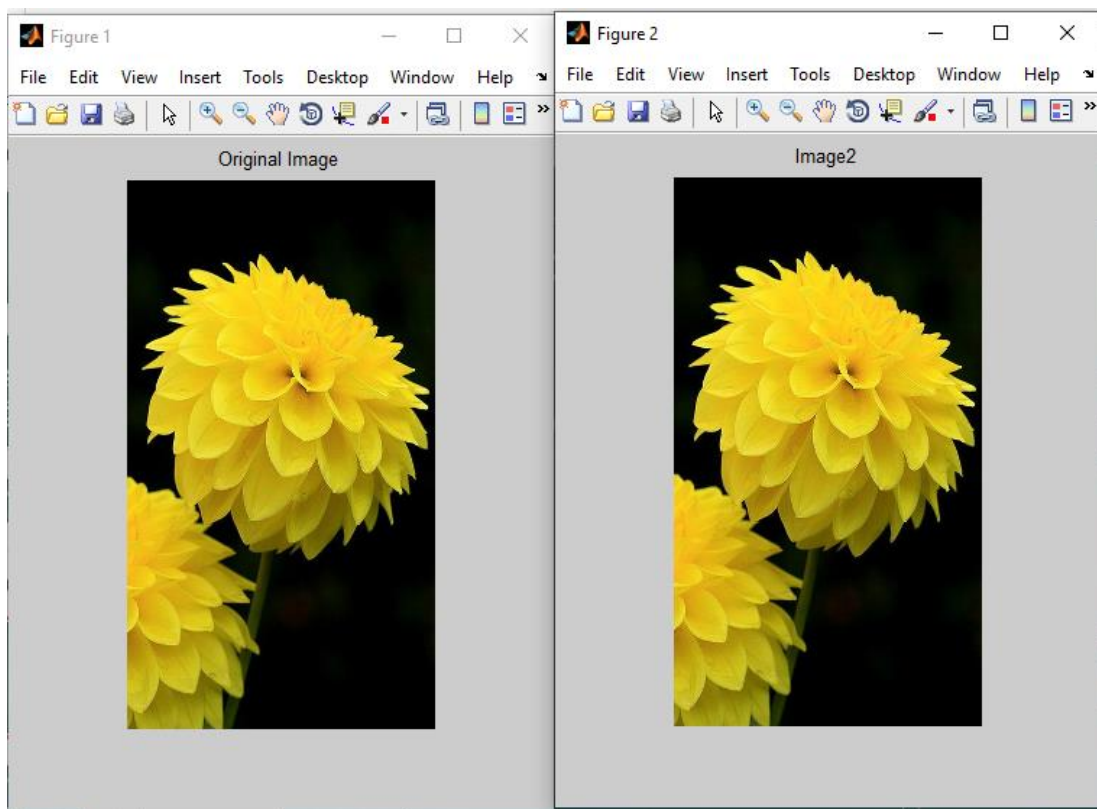


Figure 4.1:DCT watermark

DWT:

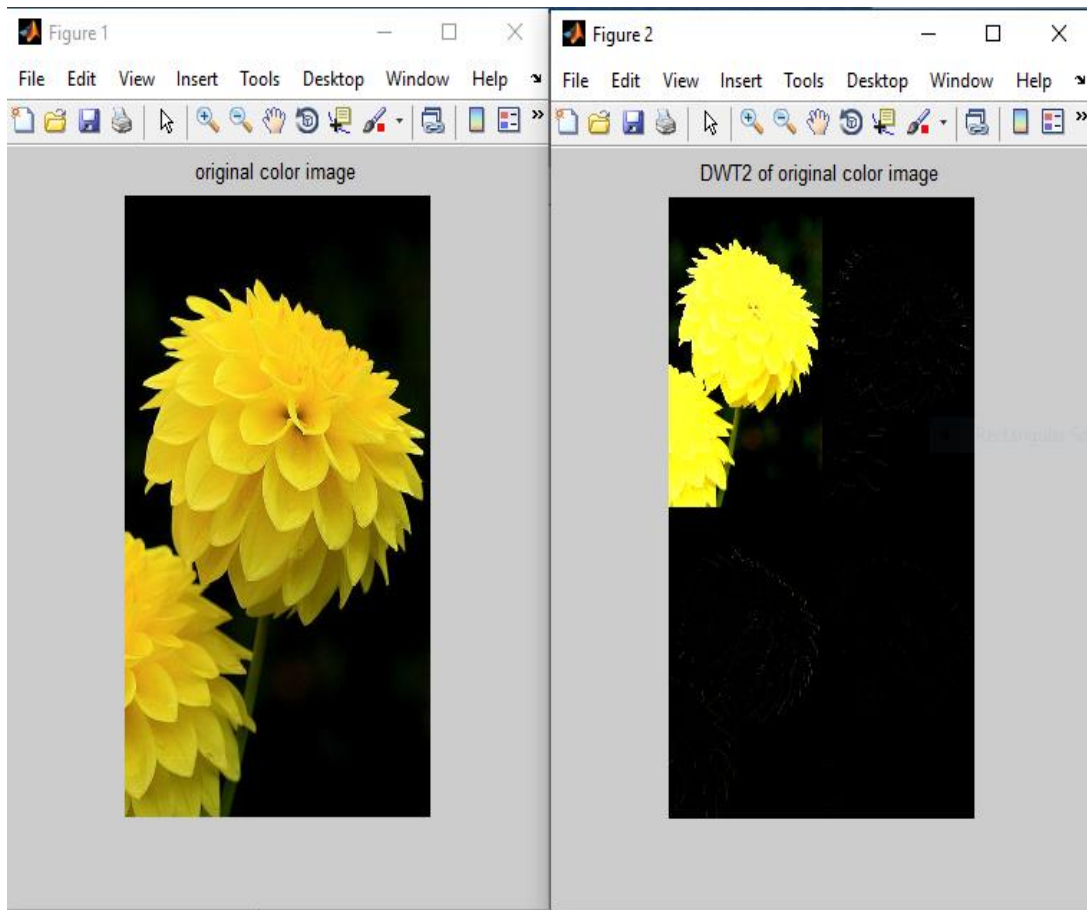


Figure 4.2: DWT Watermark

Analysis of the reflected signal received back by the radar by using Discrete Wavelet Transform (DWT) give performance is better than using Discrete Cosine Transform (DCT), especially in eliminating noise efficiently after processed the image.

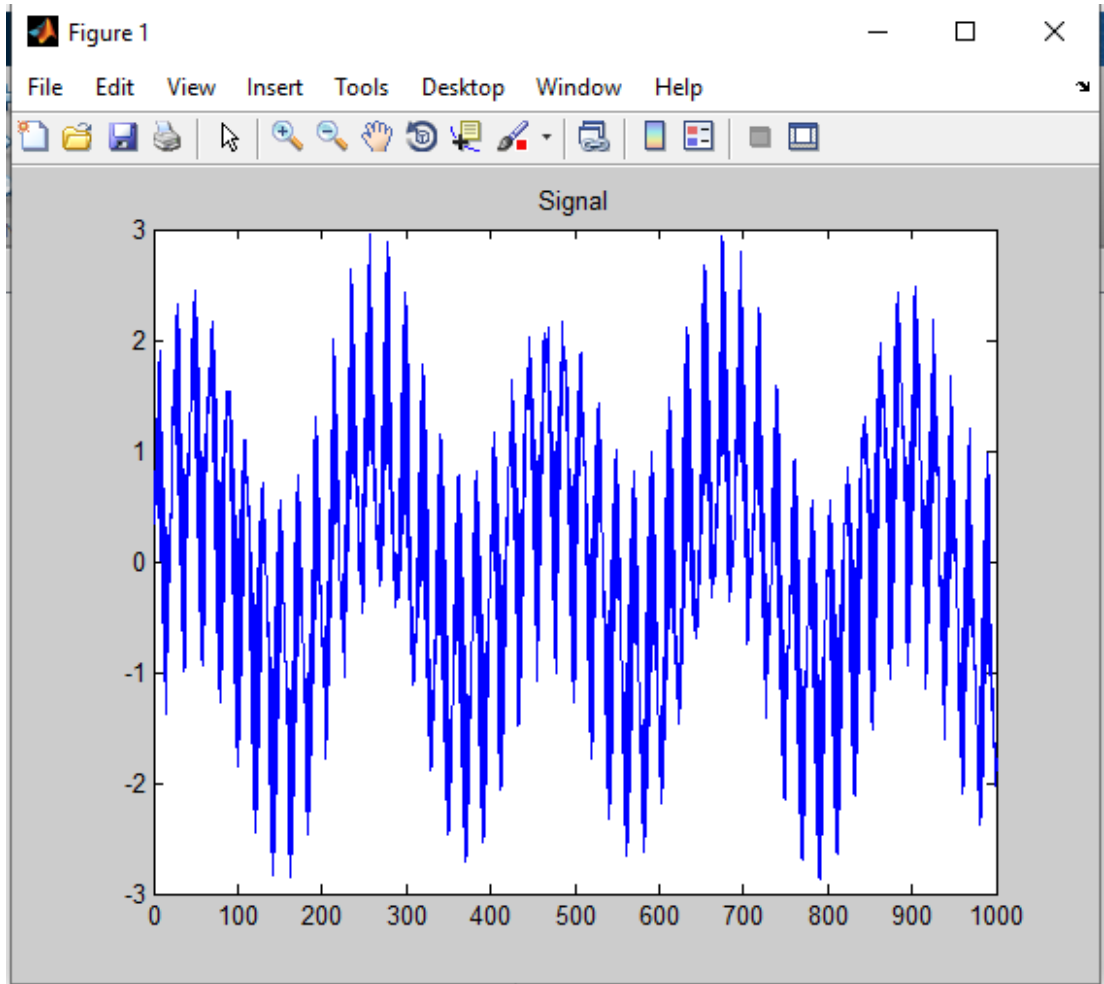


Figure 4.3: The signal of DCT image processed

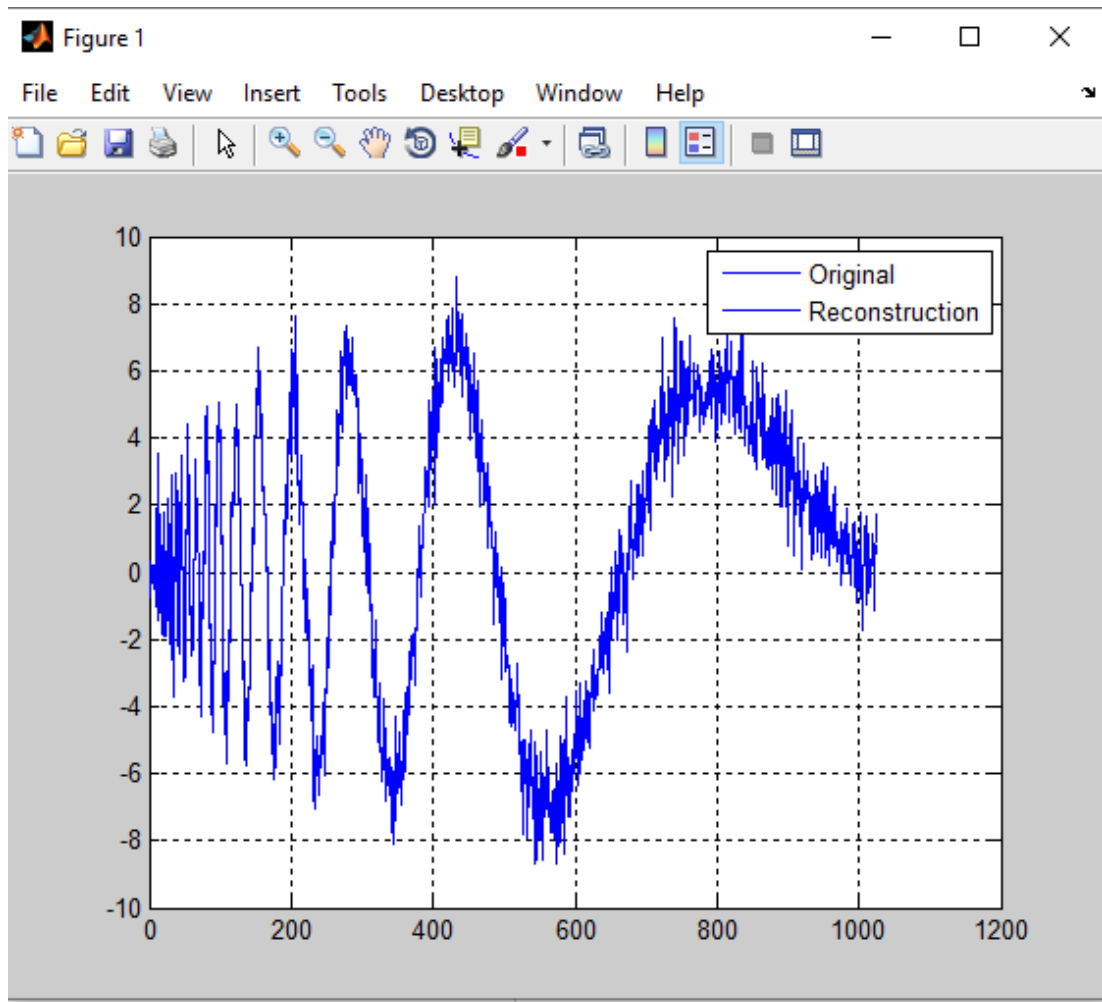


Figure 4.4: The original and reconstruction of DWT image processing

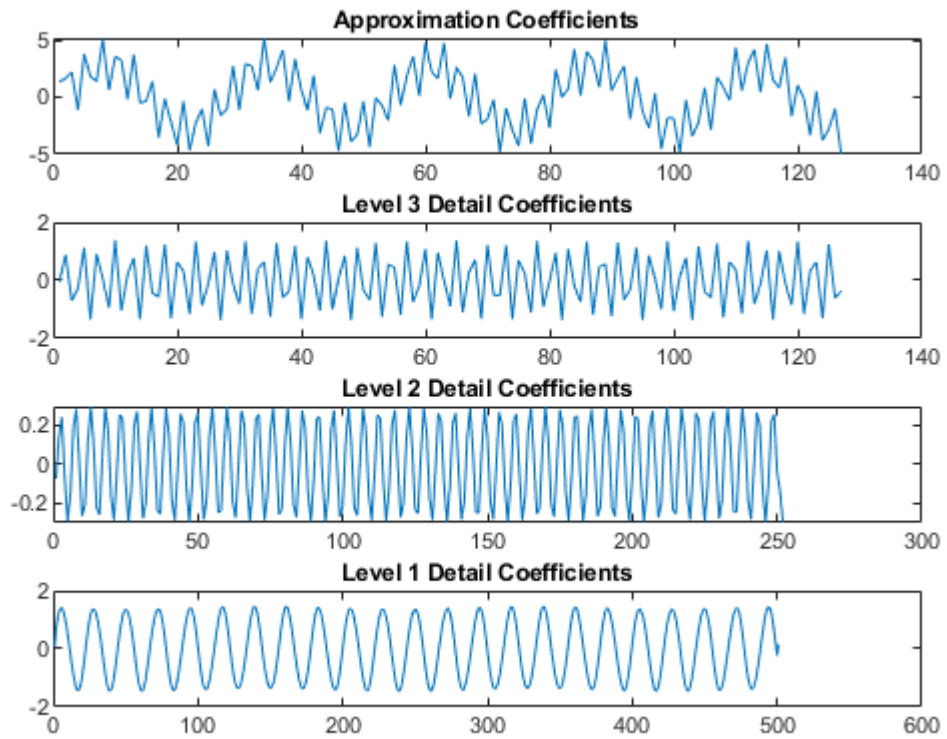
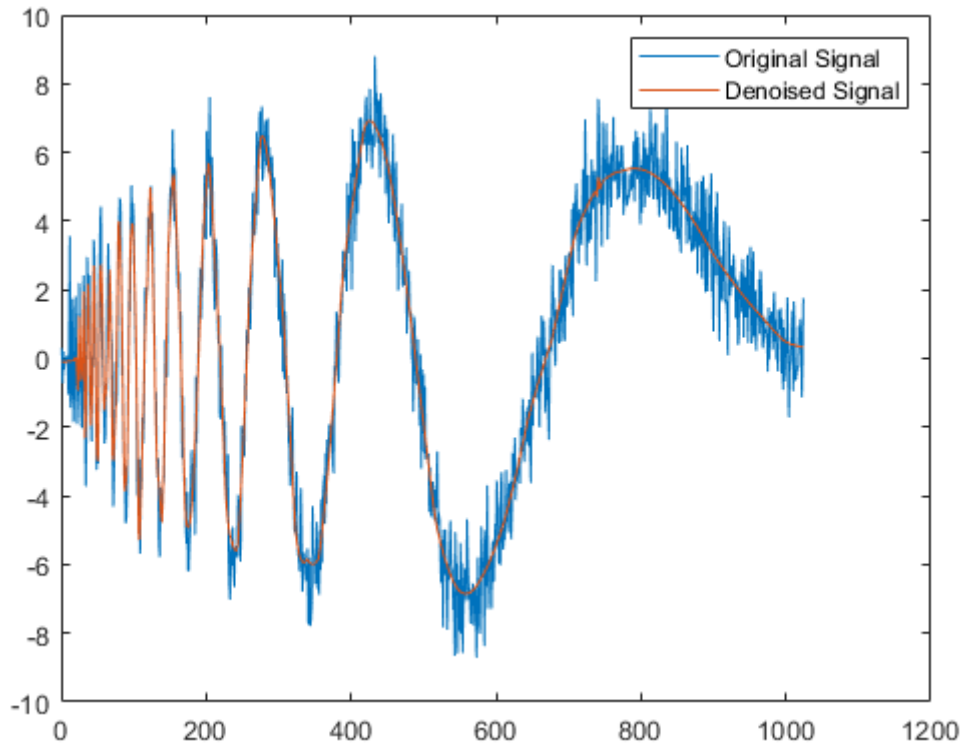


Figure 4.5: The de noise Signal with wavelet for the second input signal condition model



### THE COMBINED DCT-DWT ALGORITHM:

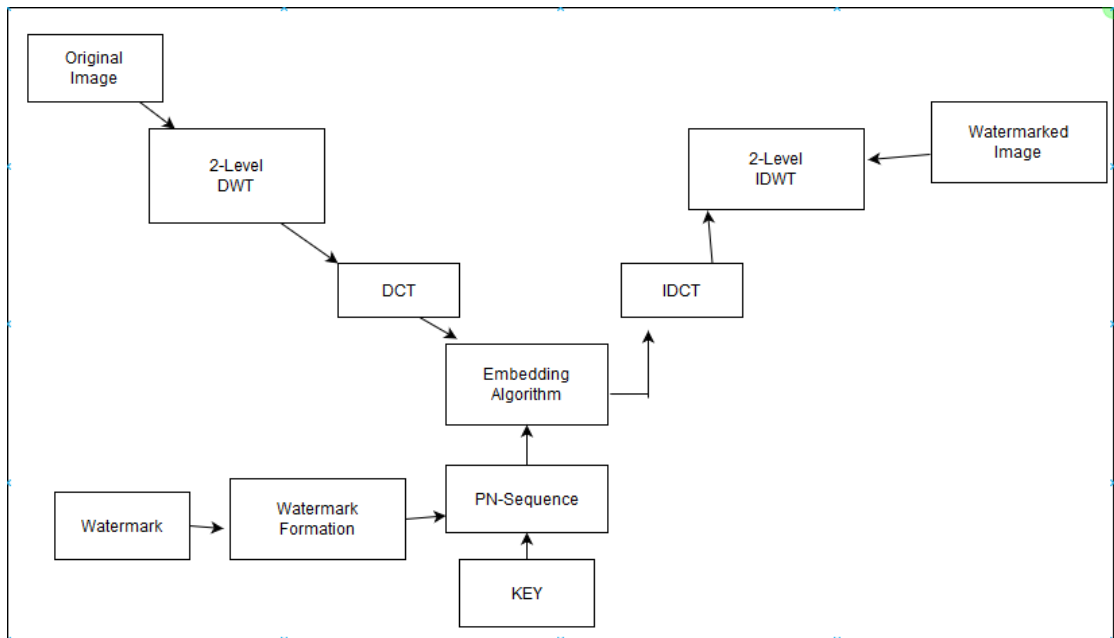


Figure 4.6: DCT and DWT embedding process

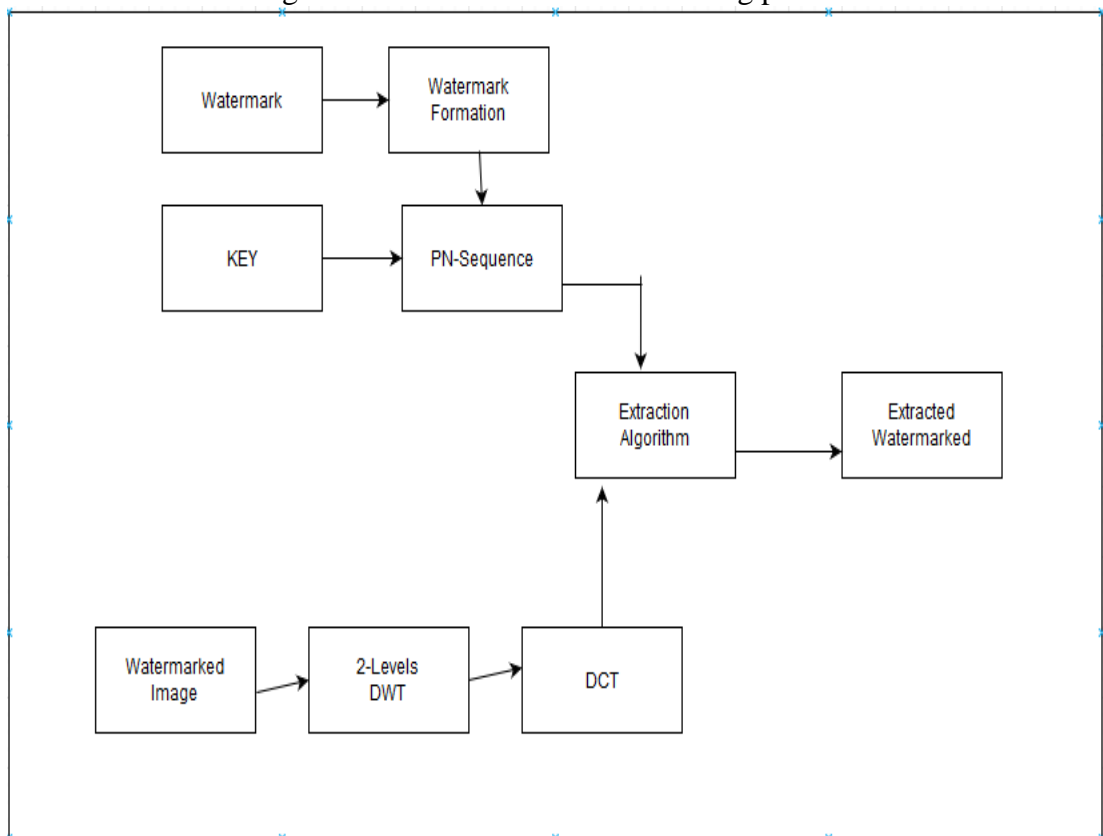


Figure 4.7: DCT and DWT extraction process

Here we have five steps to extracted an image in DCT through DWT.the five is we see in the below:

STEP 1: Apply the 2-level DWT into a water-marked image and divided the image into multi subband like LL1,HH1,HL1,LH1.

STEP 2: Divided the subband into (4x4) HL1 method.

STEP 3: Apply DCT into muti bands co-efficient of extraction algorithm .

STEP 4: Regenerate the two psedorandom sequence (PN-1,PN-0) in this process.

STEP 5: Recontract the watermarked image into the multi bands watermarked extracted method.

**DCT and DWT information loose after the image is being processed:**

**Original Image**



Logo

**Compressed Image**



Logo



Baby



Baby



Penguins



Penguins

Figure 4.8: The DCT watermark original image and compressed image

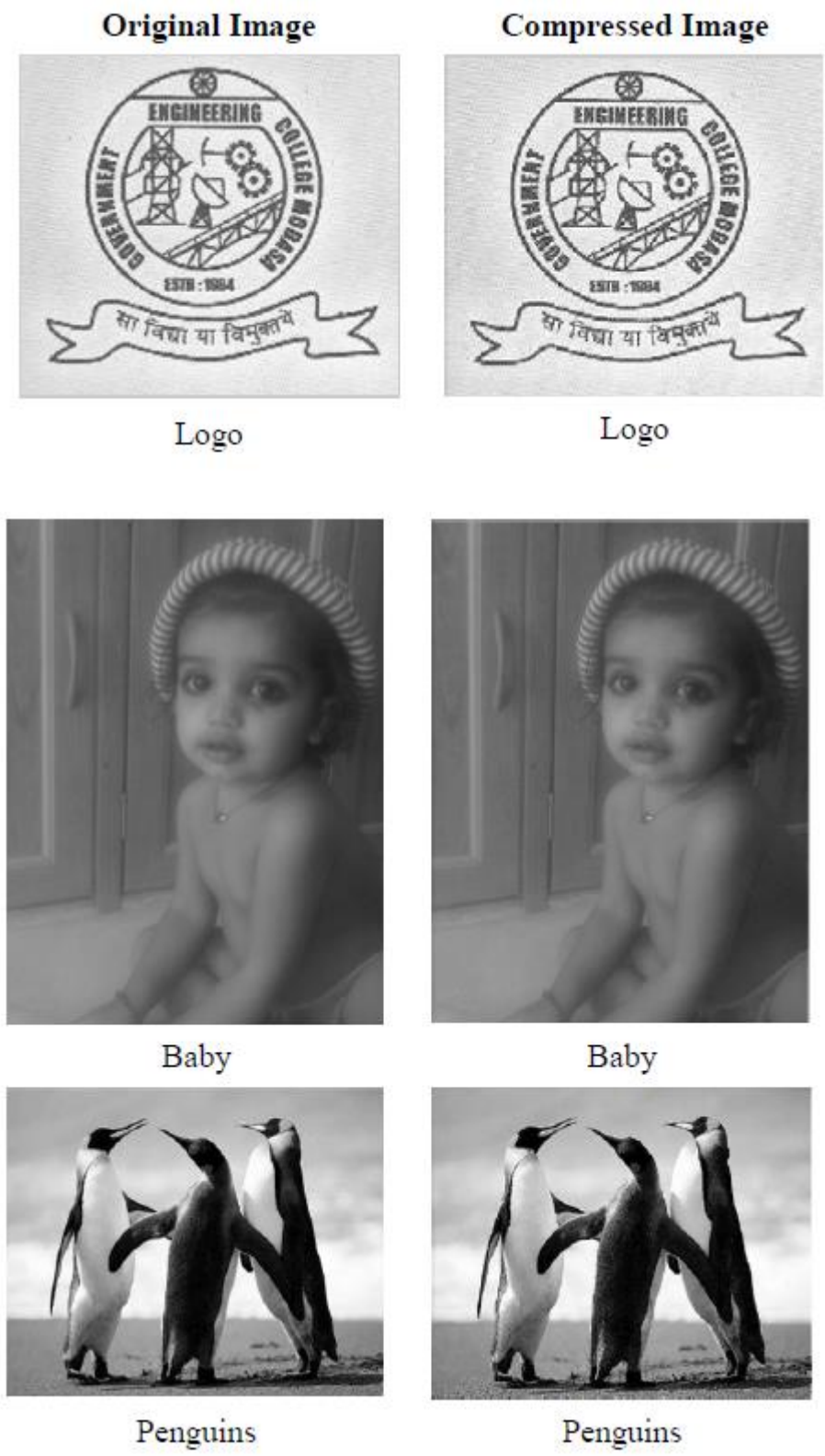


Figure 4.9: DWT watermark original image and compressed image

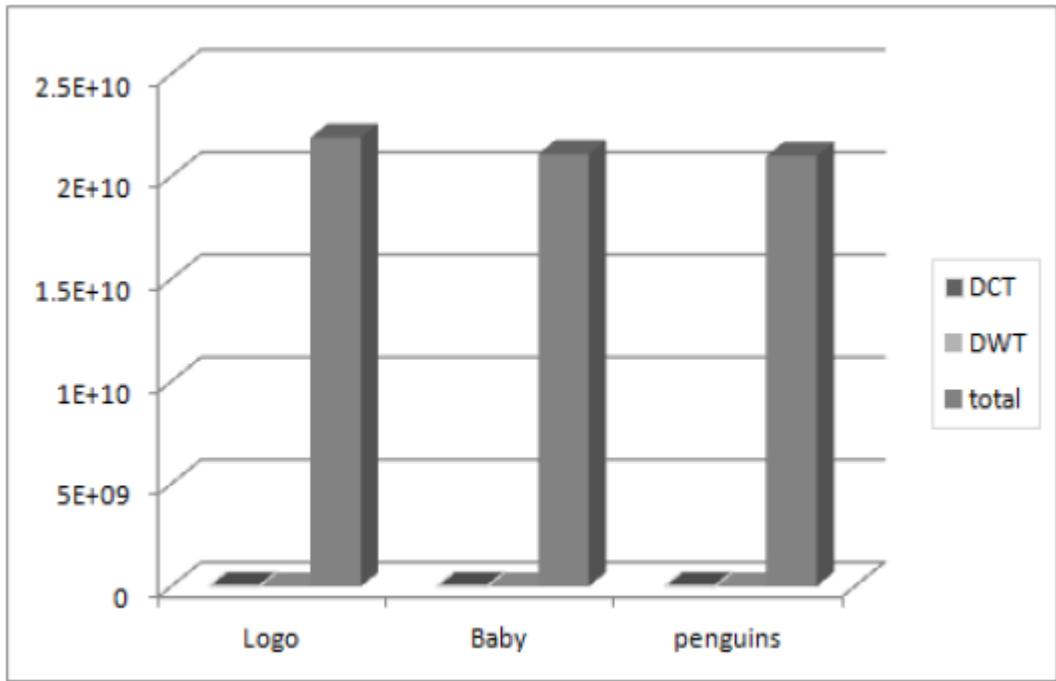


Figure 4.10: Graph of DCT and DWT information loose and total information

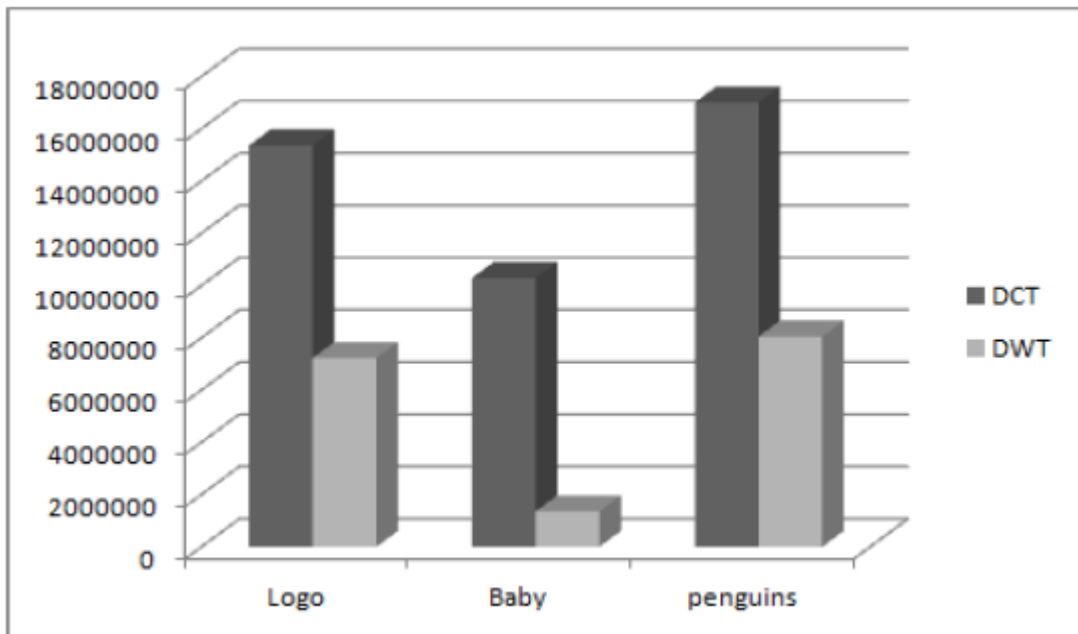


Figure 4.11: Graph for DCT and DWT information loose

We can conclude that picture of baby, logo and penguins the first one is original image and the second one is the compressed image created in matlab. In real world we cannot find no change of the images but in DCT and DWT water-marked process we can see the chart the imformation loose and the total information in figure

number 4.10 DWT and DCT watermark are same but the total information is very high. In figure number 4.11 we can see that baby, logo and penguins information loss of DCT is higher than the DWT watermark process. We cannot get all original data in both processes but we get much more data in DWT as compared to DCT water-marking process. So again we can say that the DWT or the wavelet frequency transform is better than the cosine frequency transform.

### **4.3 Overall Comparison**

From the above results, the effectiveness of the scene based hybrid schemes are demonstrated in a row. The scene based water-marking scheme achieves higher NC (normalized correlation) values when attacks based on video properties are launched. This indicates that the water-marking scheme works well by applying scene change detection with muddled water-marks. The performance of the scheme is further improved by combining with an audio water-mark, especially when the video water-mark is corrupted, such as the attack by lossy compression. When the audio channel is also attacked, the error correction information is altered. The overall performance, however, still shows improvement in water-marking. The robustness of the scheme is also raised by engaging other hybrid approaches in water-marking schemes.

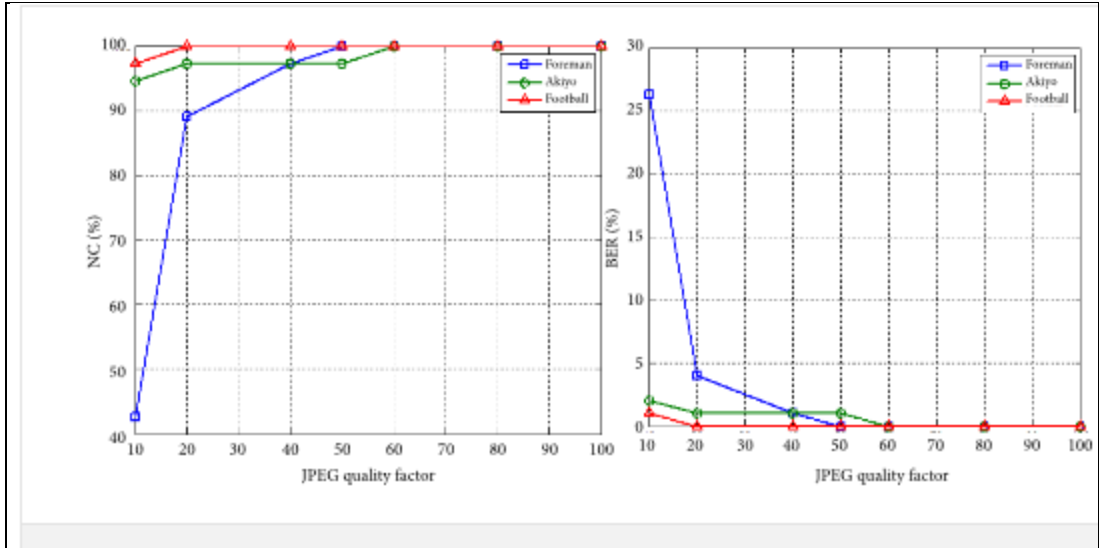


Figure 4.12: Comparison between the JPEG quality factor

#### 4.4 Test on Fidelity

In this section, we focus on that evaluating the performance of the GA-based Watermarking Scheme. In the experiment, we prove that the fidelity enhancing an effectiveness of the proposed optimization process. The GA-based water-marking scheme is implemented with GA-lib in order. To evaluate the fidelity of the water-marking scheme, the peak signal to noise the ratio (PSNR) and maximum absolute difference (MAD) is used. Using the same set of test images, different image enhancement algorithms can be compared systematically to identify whether a particular algorithm produces better results efficiently. The metric under investigation is the peak signal to noise ratio(PSNR). If we can show that an algorithm or set of algorithms can enhance a degraded known image to more closely resemble the original in order, then we more accurately conclude that it is a better algorithm. PSNR equation is below

$$PSNR = 20 \log_{10} \left( \frac{MAX_f}{\sqrt{MSE}} \right) \dots\dots\dots 4.1$$

The performance of the GA-based video water-marking scheme is evaluated through several experiments with an different number of generation in the GA-optimization process. Then, the quality of the video is evaluated with PSNR(pick signal noise ratio) and MAD. The quality of the video water-marked by the scene based water-marking scheme and the hybrid water-marking scheme are also evaluated, and compared with the GA-based scheme in order. In the experiment, two

video clips are used from the frame. One of the video clips has 1526 frames of size 352 x 288 and it consists of 10 scene changes respectively. Another video clip has 4236 frames of size 352 x 288 and it consists of 22 scene changes in a row. The experiments are done on a desktop computer with Pentium 4 CPU 2.00GHz and 512MB RAM.

#### **4.5 Other Features of the Scheme**

Our proposed the scheme that is an invisible water-marking scheme. In the scene based water-marking scheme, as low frequency sub-band DWT(discrete wavelet transform) coefficients are not water-marked and image energy is concentrated on the lower frequency wavelet coefficients, the watermark is perceptually invisible. If these coefficients are altered, however, the perceptual quality will be affected . Additionally, retrieval of the embedded watermarks does not need the original video in the frame, i.e. a blind water-marking scheme. This is an important performance feature of the scheme since it takes a long time to transmit, store, and process the original video water-marking.

The experiments show that the proposed scheme is robust(not fragile) to most of the existing attacks, however, there are still some weak-nesses in our scheme. The

computation time of the GA-based scheme is rather long if the number of GA generation applied is large or the number of the scene change of the video increases in the frame. Also, when the encoding method is applied again with another watermark process, the proposed scheme is not robust against the scheme.

#### 4. 6. Conclusion

From the experiment, we can prove that our proposed scheme enhances two of three prescribed water-marking requirements, robustness and fidelity are mainly. The robustness enhancement provided by hybrid scene based water-marking scheme and the fidelity enhancement provided by the GA-based water-marking scheme are important steps toward a perfect water-marking scheme.

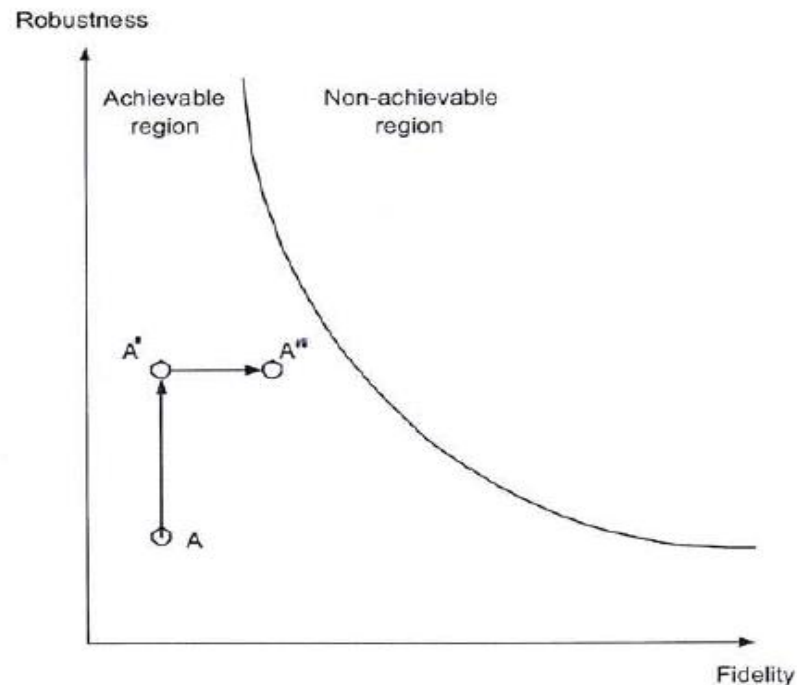


Figure 4.13: A conceptual illustration on the performance of the proposed scheme

Figure 4.13 shows a conceptual illustration. When there are two orthogonal axes, robustness and fidelity in water-marking. The robustness is indicated by the power of



the watermark, and the fidelity can be represented by quality index respectively. Moreover, the curve represent the best robustness under the fidelity performance constrain in watermark. To optimize the performance of a water-marking scheme, we try to move the point towards the curve respectively.

The point **A** represents the performance of 'a' scene based water-marking scheme. By applying the hybrid approaches, the robustness of the scheme is improved and moves the point to '**A**'. When the water-marking scheme is further enhanced by GA, i.e. increase the fidelity the scheme, the point moves along the fidelity axes in a row . Thus, it moves towards **A''**. Therefore, our proposed scheme is approaching to the "optimal" embedding configuration.

## Chapter 5

### Conclusion

This thesis investigates the knowledge of digital image water-marking techniques for secure multimedia creation and delivery. After noticing the significance of the multimedia security and image water-marking in now-a-days Internet world and reviewing the state of the arts technologies of the audio water-marking, image water-marking and video water-marking, an original hybrid digital video water-marking scheme with scene change analysis, error correcting code and GA optimization is proposed. The process of this extensive video water-marking scheme, including watermark preprocessing, video preprocessing, watermark embedding, and watermark detection, is narrated in detail. Experiments are conducted to express that our scheme is robust against attacks by frame dropping, frame averaging, and statistical analysis, and the robustness against the image processing attacks is tested with Stir-Mark benchmark. Moreover, the fastness of the scheme is evaluated.

Our approach cultivates an innovative idea in:

- (1) embedding various parts of a watermark according to scene changes,
- (2) embedding its bug correcting codes as an audio watermark,
- (3) applying a hybrid address to the proposed scheme, and
- (4) employing the GA algorithm to add to the fidelity. This approach is never explored in literature, and its dominance are clear and notable. The effectiveness of this scheme is proved through a number of experiments.

To finish our work, we contribute the followings:

- We have done a complete survey on the current water-marking technologies.

- We prefer a scene based water-marking scheme. The scheme is robust against the frame equating to the frame dropping, frame. We propose a optical audio hybrid water-marking scheme. The robustness of our scheme can be added to by including an audio watermark. We embed error correcting codes of a video watermark as an audio watermark and refine the redeemed watermark during watermark detection.
- We propose a hybrid approach with various water-marking schemes. We recruit the hybrid scheme to embed different parts of a watermark into various scenes. There are various ways to embed the watermarks.

We propose a GA based water-marking scheme increase integrity, i.e. the media class index, of the water-marking scheme. By employing GA, we can optimize the combination of the watermark and scenes in the video.

- Experiment has been done on these novel video water-marking schemes to test and show its Effectiveness. The robustness of our approach is organised using the criteria of the latest Stir-Mark test.

## Bibliography

- [1] Jiang Xuehua” Digital Watermarking and Its Application in Image Copyright Protection”, School of Engineering, Linyi Normal University, Linyi, Shandong, 276000, China.
- [2] Sumedh P. Ingale<sup>1</sup>, Prof. C. A. Dhote<sup>2</sup>” Digital Watermarking Algorithm using DWT Technique”, <sup>1</sup>Prof. Ram Meghe Institute Of Technology and Research, Badnera, Amravati SantGadgebaba Amravati University, Amravati, Maharashtra, India –444701<sup>2</sup>Prof. Ram Meghe Institute Of Technology and Research, Badnera, Amravati .SantGadgebaba Amravati University, Amravati, Maharashtra, India – 444701.
- [3] Hai Tao\*<sup>1</sup>, Li Chongmin\*<sup>2</sup>, Jasni Mohamad Zain<sup>1</sup>, Ahmed N. Abdalla<sup>3</sup>” Robust Image Watermarking Theories and Techniques: A Review”, <sup>1</sup>Faculty of Computer System and Software Engineering, University Malaysia Pahang, Malaysia<sup>2</sup> Department of mathematics and information, Qinghai Normal University, China<sup>3</sup>Faculty of Electrical and Electronic Engineering, University Malaysia Pahang, Malaysia.
- [4] Mohamed A. Suhail, *Member, IEEE*, and Mohammad S. Obaidat, *Senior Member, IEEE* “Digital Watermarking-Based DCT and JPEG Model”
- [5] Christine I. Podilchuk and Edward J. Delp” Digital watermarking and its applications”.
- [6] Pooya Monshizadeh Naini” Digital Watermarking Using MATLAB”, Pooya Monshizadeh Naini, *University of Tehran, Iran*.
- [7] Xin Li, Xingjun Wang, Anqi Chen and Linghao Xiao” A Simplified and Robust DCT-based Watermarking Algorithm”, Department of Electronic

Engineering Graduate School at Shenzhen, Tsinghua University, Shenzhen, China

- [8] 1Khandve Ashwini B. 2Udhane Priyanka P. 3Parkar Shalaka B. 4Kulthe Sagar A” A Robust QR-Code Video Watermarking With DCT Domain”, BE Computer, PGMCOE, Wagholi. Pune.,Maharashtra.BE Computer, PGMCOE, Wagholi, Pune,Maharashtra.BE Computer, PGMCOE, Wagholi., Pune.,Maharashtra., BE Computer, PGMCOE, Wagholi., Pune.,Maharashtra.
- [9] Ali Al-Haj” Combined DWT-DCT Digital Image Watermarking”.Department of Computer Engineering, School of Electrical Engineering,Princess Sumaya University for Technology, PO Box 1928, Al-Jubeiha,11941 Amman, Jordan
- [10] Wu He-Jing“A DCT Domain Image Watermarking Method Based on Matlab”,Department of Computer Science & Electrical Engineering,East University of Heilongjiang, Harbin, China
- [11] Lalit Kumar Saini<sup>1</sup>, Vishal Shrivastava<sup>2</sup> “A Survey of Digital Watermarking Techniques and its Applications”M.Tech<sup>1</sup> Research Scholar, Professor<sup>2</sup> Department of Computer Science and Engineering, Arya College of Engineering. & Information Technology, Jaipur, India
- [12] Z. J. XU<sup>a</sup>, Z. Z.WANG<sup>b1\*</sup>, Q.LU<sup>c</sup>” Research on Image Watermarking Algorithm based on DCT”Shanghai Maritime University, Information Engineering College, Shanghai 200135, P .R.. China
- [13] P.W. Chan, M.R. Lyu and R.T. Chin ”A Novel Scheme for Hybrid Digital Video Watermarking: Approach, Evaluation and Experimentation,” submitted to *IEEE Transactions on Circuits and Systems for Video Technology*.

- [14] F. Petitcolas, M. Frederic Raynal, J. Dittmann, C. Fontaine, N. Fates, "A public automated web based evaluation service for watermarking schemes: StirMark Benchmark," In Ping Wah Wong and Edward J. Delp, editors, proceedings of electronic imaging, security and watermarking of multimedia contents III, Vol. 4314, San Jose, California, U.S.A., Jan. 2001. The Society for imaging science and technology (IS. and T.) and the international Society for optical engineering (SPIE). ISSN 0277-786X, <http://www.petitcolas.net/fabien/watermarking/stirmark/>.
- [15] K. Su, D. Kundur, and D. Hatzinakos, "Statistical Invisibility for Collusion-resistant Digital Video Watermarking," *IEEE Transactions on Multimedia* 2004
- [16] K. Su, D. Kundur, and D. Hatzinakos, "Spatially Localized Image dependent Watermarking for Statistical Invisibility and Collusion Resistance," *IEEE Transactions on Multi-media* 2004
- [17] K. Su, "Digital Video Watermarking Principles for Resistance to Collusion and Interpolation Attacks, , , Master of Applied Science thesis, University of Toronto, Sept. 2001.
- [18] I. Cox, M. Miller, and J. Bloom, "Digital watermarking," Morgan Kaufmann Publishers, Oct. 2001, ISBN 1-55860-714-5.
- [19] F. Litterio, <http://world.std.com/franl/crypto/>.
- [20] K. Su, D. Kundur, and D. Hatzinakos "Combined DWT-DCT Digital Image Watermarking *IEEE Transactions on Multimedia* 2004
- [21] Watermarking World, <http://www.watermarkingworld.org/>.

- [22] M. Kutter and F. Hartung, "Introduction to Watermarking Techniques," Proceedings Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, pp. 97-119, Dec. 1999.
- [23] H. Inoue, A. Miyazaki, and T. Katsura "An Image Watermarking Method Based on the Wavelet Transform", Kyushu Multimedia System Research Laboratory.
- [24] I. Cox, M. Miller, J. Linnartz, and T. Kalker, "A Review of Watermarking Principles and Practices" Proceedings Digital Signal Processing for Multimedia Systems, K.K. Parhi, T. Nishitani, eds., New York, New York, Marcel Dekker, Inc., pp. 461-482, 1999.
- [25] F. Petitcolas, "Watermarking Schemes Evaluation", IEEE Signal Processing Magazine, Vol. 17, pp. 58-64, Sept. 2000.
- [26] Y. Kim, K. Moon, and I. Oh, "A text watermarking algorithm based on word classification and interword space statistics," Proceedings Seventh International Conference on Document Analysis and Recognition 2003, pp. 775 -779, Aug. 3-6, 2003 .
- [27] R. Wolfgang, C. Podilchuk, and E. Delp, "Perceptual Watermarks for Digital Images and Video," *Proceedings of the SPIE/IS and T International Conference on Security and Watermarking of Multimedia Contents*, Vol. 3657, pp. 40-51, San Jose, CA, Jan. 25 - 27, 1999.
- [28] R. Wolfgang and E. Delp, "A Watermarking Technique for Digital Imagery: Further Studies," Proceedings of the International Conference on Imaging

Science , Systems, and Technology, pp. 279-287, Jun. 30 - Jul. 3' 1997.

- [29] D. Sachs, R. Anand, and K. Ramchandran, "Wireless image transmission using multiple description based concatenated codes," *Proceedings Data Compression Conference DCC 2000*, pp. 569, 2000.
- [30] A. Doufexi, A. Nix, D. Bull, "Robust wireless image transmission using jointly optimized modulation and source coding," *Proceedings IEEE Vehicular Technology Conference 2000, VTC 2000-Spring* Vol. 3, pp. 2039-2043, Tokyo, 2000.
- [31] M. Buckley, M. Ramos, S. Hemami, and S. Wicker, "Perceptually based robust image transmission over wireless channels," *Proceedings 2000 International Conference on Image Processing*, Vol- 2, pp. 128-131, 2000.
- [32] H. Bassali , J. Chhugani, S. Agarwal, A. Aggarwal, and P. Dubey, "Compression tolerant watermarking for image verification," *Proceedings 2000 International Conference on Image Processing*, Vol. 1, pp. 430-433, 2000.
- [33] L. Boney, A. Tewfik, and K. Hamdy, "Comparative Analysis between DCT & DWT Techniques of Image Compression," *Proceedings Third IEEE International Conference on Multimedia Computing and Systems*, pp. 473-480, Jun. 17-23, 1996.
- [34] C. Lu, M. Liao, and L. Chen, "Multipurpose audio watermarking," *Proceedings 15th International Conference on Pattern Recognition 2000*, Vol. 3, pp. 282-285, 2000.



# Appendix A

## LIST OF CONTENTS

<b>Approval</b>	<b>II</b>
<b>Declaration</b>	<b>III</b>
<b>Acknowledgement</b>	<b>IV</b>
<b>Abstract</b>	<b>I</b>
<b>1 Introduction</b>	<b>2</b>
2.1 Background	2
2.2 Research Objective	3
2.3 Contributions	4
2.4 The Structure of Thesis	5
<b>2 Literature Review</b>	<b>6</b>
2.1 Security in Multimedia Communications	6
2.2 Cryptography	9
<b>Chapter 3 :Novel Watermarking Schemes</b>	<b>12</b>
3.1 Watermark Preprocess	12
3.2 Simple image watermark	13
3.2.1 Binary image processing	15
3.2.2 Rgb2grayscale image processing	19
3.3 DCT(Discrete cosine Transform)	22
3.4 DWT(Discrete Wavelet Transform)	24
3.5 DFT(Discrete Fourier Transform)	26

<b>Chapter 4: Experimental Results</b>	28
4.1 Test on Robustness	28
4.2 Comparative Analysis between DCT & DWT Techniques	29
4.3 Overall Comparison	40
4.4 Test on Fidelity	41
4.5 Other Features of the Scheme	42
4. 6. Conclusion	43
<b>Chapter5: Conclusion</b>	45
<b>Bibliography</b>	47

## **Appendix B**

From the above results, the effectiveness of the scene based hybrid schemes are demonstrated in a row. The scene based water-marking scheme achieves higher NC(normalize correlation) values when attacks based on video properties are launched. This indicates that the water-marking scheme work well by applying scene change detection with muddled watermarks. The performance of the scheme is further improved by combining with an audio watermark, especially when the video watermark is corrupted, such as the attack by lossy compression. When audio channel is also attacked, the error correction information is altered row. The overall performance, however, still shows improvement in watermarking. The robustness of the scheme is also raised by engaging other hybrid approaches schemes.

## Appendix C

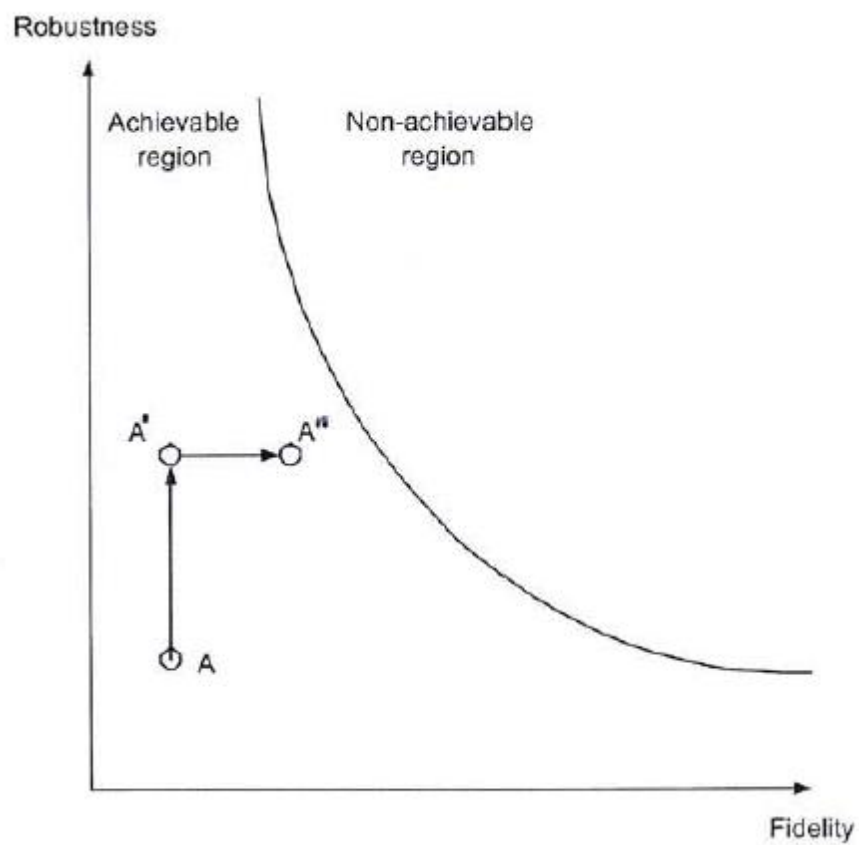


Figure 4.4: A conceptual illustration on the performance of the proposed scheme