UNIVERSITY OF GAZİANTEP

GRADUATE SCHOOL OF

NATURAL & APPLIED SCIENCES

A NEW APPROACH FOR VIDEO WATERMARKING

M.Sc. THESIS

IN

ELECTRICAL AND ELECTRONICS ENGINEERING

BY

ALISHER ABDULKHAEV

FEBRUARY 2016

A new approach for Video Watermarking

M.Sc. Thesis

in

Electrical and Electronics Engineering

University of Gaziantep

Supervisor

Assis. Prof. Dr. Sema Koç KAYHAN

by

Alisher ABDULKHAEV

February 2016

REPUBLIC OF TURKEY
UNIVERSITY OF GAZIANTEP
GRADUATE SCHOOL OF NATURAL & APPLIED SCIENCES
ELECTRICAL AND ELECTRONICS ENGINEERING DEPARTMENT

Name of the thesis: A New Approach For Video Watermarking

Name of the student: Alisher ABDULKHAEV

Exam date: 03/02/2016

Approval of the Graduate School of Natural and Applied Sciences.

Prof. Dr. Metin BEDİR

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Prof. Dr. Ergün ERÇELEBİ

Head of Department

This is to certify that I have read this thesis and that in my consensus opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Sema Koç KAYHAN

Supervisor

Examining Committee Members:

Signature

Prof. Dr. Nuran DOĞRU .....

Assist. Prof. Dr. Sema Koç KAYHAN .....

Assoc. Prof. Dr. Muhammet Fatih HASOĞLU .....

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Alisher ABDULKHAEV

ABSTRACT

A NEW APPROACH FOR VIDEO WATERMARKING

ABDULKHAEV Alisher
M.Sc. in Electrical and Electronics Engineering
Supervisor: Assis. Prof. Dr. Sema Koç KAYHAN
February 2016
66 pages

Abstract

Digital Watermarking plays a significant role in data authentication and proof of ownership. In this study, a novel approach for Video Watermarking is proposed, in which the Genetic Algorithm is used to optimize the parameters of digital video watermarking scheme. One of the most straightforward watermarking method is LSB (Least Signifiant Bit) in which watermark is embedded into least significant bit of host media. Our work is based on LSB watermarking method. Although, standard LSB watermarking is good choice for data embedding, it is not robust against bit-deletion, gaussian, median filtering attacks. We use genetic algorithm to select the most optimum bit plane during the embedding process and the watermark is embedded into optimum (6th,7th or 8th) bit of host video frames, to overcome above mentioned attacks' degradations. Decision is done with respect to Peak Signal Noise Ratio (PSNR) of watermarked frame and Normalized Cross Correlation (NCC) values of the original and extracted watermark. Experiments are performed for various watermarks, host video, and a set of Genetic Algorithm parameters, such as population size, number of iteration, tournament range. Results suggest that modified LSB watermarking scheme is more robust to bit-plane deletion, gaussian, median filtering and other similar attacks.

Key Words: LSB; Genetic Algorithm, video watermarking; PSNR; NCC.

ÖZET

VİDEO DAMGALAMA İÇİN YENİ BİR YAKLAŞIM

ABDULKHAEV Alisher
Yüksek Lisans Tezi, Elektrik-Elektronik Mühendisliği Bölümü
Tez Yöneticisi: Yrd. Doç. Dr. Sema Koç KAYHAN
Şubat 2016
66 sayfa

Dijital Damgalama veri doğrulama ve sahiplik ispatı gibi alanlarda çok önemli bir role sahiptir. Bu çalışmada Video Damgalama için yeni bir yaklaşım öngörülmüştür. Damgalama parametrelerinin optimizasyonu için Genetik Algoritma kullanılmıştır. Literatürde dijital damgalama ile ilgili birçok yayın mevcut olup, aralarındaki en basit olanı En Az Anlamlı Bit metodudur. En Az Anlamlı Bit algoritmasında, damga ana verinin en az anlamlı bitine gömülmektedir. Her ne kadar LSB metodu video damgalama için en uygun seçim olsa da, bit düzleminin silinmesi, gausyen filtre, medyan filtre gibi ataklara karşı dayanıklı değildir. En uygun bit düzlemi seçimi için Genetik algoritma kullanılmıştır ve sonuç olarak gömülecek olan damga video karelerinin en uygun bit düzlemine (6., 7. veya 8.) gömülmüştür. Böylelikle, olası ataklara karşı dayanıklılığının artırılması öngörülmüştür. Seçim aşamasında damgalanmış video karelerinin Tepe Sinyal Gürültü Oranı (PSNR) ve orijinal damga ile çıkartılan damga arasındaki Normalize Edilmiş Çapraz Korelasyon (NCC) değerlerine göre karar verilmiştir. Deneyler ana video, damga ve Genetik Algoritma parametreleri (populasyon büyüklüğü, iterasyon sayısı, turnuva aralığı) değiştirilerek yapılmıştır. Sonuçlar, sunulan/değiştirilen LSB yönteminin bit düzleminin silinmesine, medyan filtrelemeye ve gausyen filtrelemeye karşı dayanıklı duruma geldiğini göstermiştir.

Anahtar Kelimeler: LSB, Genetik Algoritma, video damgalama, PSNR, NCC.

To My Mother and Uncle;

Iroda and Sanjarbek,

To My Sister and Brother;

Gulshana and Abdulaziz.

ACKNOWLEDGEMENTS

This work would not have been possible to finish without support of my mother, sister and brother, Iroda, Gulshana and Abdulaziz over past years. Thanks a lot for them!

I would like to thank my advisor, Assis. Prof. Dr. Sema Koç KAYHAN, for giving me this opportunity to work with her. It has been a rewarding experience.

Also I would like to thank my M.Sc. head of committee Prof. Dr. Ergün ERÇELEBİ for his support and guidance.

Special thanks to my friends Saad Elhashmi Allagwail, Mrwan Margem and Kadir Işık to whom I owe a lot.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF SYMBOLS/ABBREVIATIONS

DWT	Discrete Wavelet Transform
DFT	Discrete Fourier Transform
dB	Decibel
DCT	Discrete Cosine Transform
HVS	Human Visual System
GA	Genetic Algorithm
NN	Neural Network
ANN	Artificial Neural Network
PSNR	Peak Signal Noise Ratio
NCC	Normalized Cross Correlation
F	Fitness Function
RNN	Recurrent Neural Network
CNN	Convolutional Neural Network

CHAPTER 1

INTRODUCTION

Watermarking is one of data hiding methods. Data hiding is, mainly, used for secure communication between two of people or more. Data hiding is used for hiding or protecting any information in different methodologies. There are some kinds of data hiding exist: cryptography, steganography, fingerprinting, and watermarking. Of course, each of above methods are very useful for a specific purpose. In this thesis, we handled a noval approach for digital video watermarking. Since, nowadays communication on social networks becomes very widespread, we may need to do something to prove ownership of our videos, photos or any other kind of digital files. It is very crucial to avoid any modification on our digital files by other users.

In literature, some review papers about data hiding were published [1-3]. On the other hand, some other review papers about specific data hiding methods such as; watermarking [4-7], steganography [8,9], fingerprinting [10], cryptography [11] are available. Brief explanations of these data hiding methods are as follows: watermarking – is the embedding the data into cover signal in order to prove ownership or detecting the tamper [1], steganography – main aim in steganography is writing hidden messages that existance of message can be found by receiver and sender only [1], fingerprinting – is making the content unique for specific receiver person by taking each copy of content [1], cryptography – is the practice and learning techniques for secure communication in the presence of third parties [1].

In watermarking, there are a lot trade-off between choosing watermarking parameters. Because we need that our watermarked image/video to be both robust and imperceptible. The most prominent trade-off in watermaking is between robustness and imperceptiblity. From this point of fact, we have to leverage while choosing the watermark which we are going to embed into out digital data. It is a challenge to select the most suitable watermark in order to meet a need. If we select such a watermark that is very robust against any attacks, and not imperceptible, then

it would not be suitable, because the goal behind watermarking is to be able to prove ownership, therefore it should be both robust and imperciple. However, if we embed such a watermark that is imperceptible, and not robust against attacks (median filtering, gaussian filtering, bit-plane deletion, etc.), then in this case, also, it would not fit its purpose. Therefore, we should select the optimum matermark, optimum methodology for embedding the watermark, and optimum space (spatial domain, frequency domain, or wavelet domain) in which we perform watermarking procedure. It is appreciated that it is a challenge to choose above options, and it would be possible by the using of optimization methods.

If there is an issue about any kind of trade-offs then the first thing that comes to mind is, of course, optimization methods. Because, unlike humans, optimization methods can find the most optimum value of a function, that is called fitness function. It will be possible to optimize a problem, if and only if we have a fitness (error) function.

In order to be able to use such kind of optimization methods, GA and NN, we need to find the suitable error/fitness function. It is also challenging task.

In this thesis, a noval video watermarking method is presented using optimization methods. And the results are mentioned in chapter 6.

The organization of the thesis is described as follows: the first Chapter is the introduction of the thesis, where the problem statement and scope of the thesis background have been described step by step. In Chapter 2, general description of data hiding is mentioned in detail. In Chapter 3, common types of watermarking and methods of watermarking are mentioned with their pros and cons. Afterwards usage areas of those methods are also given. In Chapter 4, Genetic Algorithm and its parameters' importances are stated, subsequently a little discussion about fitness function is proposed, then Neural Network is stated and discussed about its properties and advantages. In Chapter 5, the previous two chapters are combined together, watermarking using optimization methods is discussed. GA and NN based watermarkings are compared. Experimental results are given in Chapter 6. Then, discussions are done based on experimental results. In the final Chapter, Chapter 7, conclusion of overall subjects in this thesis is stated. Consequently, future work that we wish to do is stated in this line of work.

CHAPTER 2

DATA HIDING

Although data hiding has become center of attraction in communication in recent years, its history is based on a long time ago – ancient ages. It is appreciated that data hiding was the need of people, it will continue to be the need of people, too. Because, it is always very crucial requirement in our daily life. One can need to hide his personal informations from other people. So, data hiding maintaining its necessity but in different ways. For instance, first data hiding was implemented in ancient ages, in form of tattoo to scalp of slave [12]. In the later years, Romans communicated in the written form, by using ink generated from liquids, such as juice and milk. Trithemius, have written a book named "Steganographia" in 1500s. And after that time, data hiding has been used, and has come up to today. In II. World War, Germans have developed a micro-pointing device. Using this device, they did a communication between each other, by reducing the size of a message to the point size. The receiver could get the message by combining those points together [12].

Nowadays, data hiding appeared in the form of digital. In [13] Prisoners' Problem is stated (Figure 2.1). In that problem, data hiding was used to communicate that will not arouse suspicion to third party. And some other data hiding algorithms and methods are enhanced.

Data hiding is mainly divided into two seperate subtitle: Steganography and Watermarking. Both of these subtitles require some properties while implementing data hiding. These requirements can be explained as shown in Figure 2.2.

2.1. Steganography

Steganography means "covered writing" and originated from Greek. It is such kind of a science that hides the communication. Therefore, a steganographic system embeds hidden message (it may be any kind of message; text, picture, etc.) in unremarkable cover media, in this manner the idea "not to arouse an eavesdropper's

suspicion" intends. Earlier, people used hidden tattoos or invisible ink to convey steganographic content. Nowadays, easy-to-use communication channels, for steganography, are provided by means of computer and network technologies. In steganography, embedding (hidden message) process is provided, primarily, by identifying a cover medium's redundant bits (that bits should not destroy medium's integrity when they are modified in order to embed information). By replacing those redundant bits with the bits of hidden message, stego medium is created. Stego medium means special form of media that contains a hidden message [14].

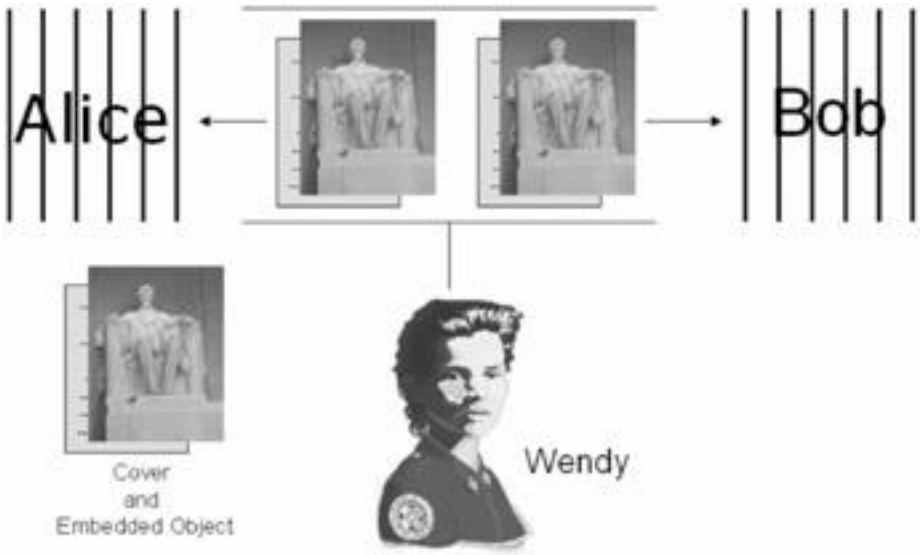


Figure 2.1 Prisoners' Problem

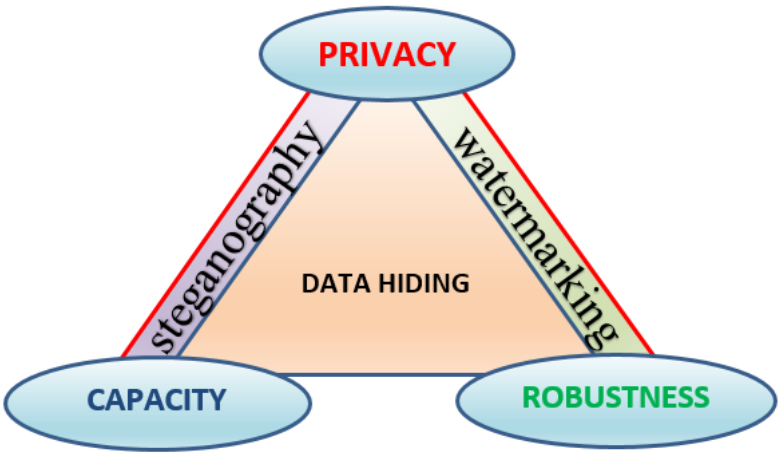


Figure 2.2 Triangle of main requirements in data hiding

2.1.1 Steganalysis

In steganography work, main issue is to embed the hidden message into cover data in different purposes. I am saying “in different purposes”, because steganography can be used both with positive and negative aims. Because of its privacy, some thieves or persons who threaten national security can use it in order to communicate between each other, while keeping their communication in secret. But, in response to this, one can use steganography in order to ensure the government against threats or to ensure the security of a company, web site of a company against hackers. In this connection, we may have to recognize if there exist any steganography in data we received. As I mentioned previously, the usage of data hiding is very flexible. It can be used for evil purposes, or it can be very beneficial in some cases to catch malicious people. At this point, one can ask a question “Is it possible to detect or recognize if there exist any steganography in data or not?”. So, the answer to this question is “steganalysis”. Steganalysis is the method of detecting the existence of the secret communication. Thus, the steganographer (data hider) and steganalyst (detector of steganography) are like two eternal competitors - one always tries to defeat the other. Thus, detecting the steganography is very important as is the case for steganography, too.

As shown in Figure 2.3 when we encounter in such a situation that we receive a data, but we need to test if this data contains any hidden message or not, then we have to be sure about perceptual transparency of image in this case. Afterwards, if we are sure about its perceptual transparency, i.e. if we ensure that it does not contain any hidden message, then give up about testing this content of the. But if we are not sure at all, or even if we do not suffirance about any kind of hidden communication, then we should check the content of data and focus on task that is called steganalysis.

As every data hiding methods include their own features, or properties, steganography also has to meet some requirements, or in other words it should fulfill some features. Features can be in trade-offs between each other. These features are briefly explained in next subsections; capacity and security.

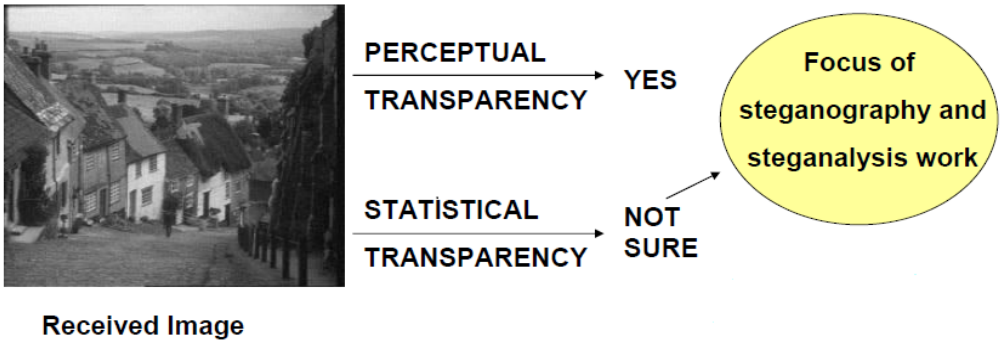


Figure 2.3 The main and rough scheme of steganalysis

2.1.2 Capacity

Capacity of steganography describes the amount of information that can be hidden into data. Capacity is one of the priority needs of steganography. The more information embedded means more succesfull steganography has done. Because, we are seeking to send as more as possible information, while keeping security at highest point in secure communications.

2.1.3 Security

Security of steganography describes the eavesdropper's inability to detect the information or embedded message. Security is the second priority need of steganography, while the first was capacity. However, high capacity may subject to security failure. So, there is a huge trade-off between capacity and security requirements of steganography. Because of our title of thesis is not related with "steganography" we are not going to keep analysing bout these parameters of steganography.

2.1.4 Robustness

Finally, robustness of a steganography stands for ability of steganography to withstand against attacks before an adversary can destroy embedded information. Robustness requirement is sought more in watermarking rather than steganography. Since, robustness of data hiding is introduced in more detail in next section.

2.2. Watermarking

Watermarking is another branch of data hiding after steganography. The main task in steganography was to embed message into cover data, to protect the message itself. Therefore, security, information about existence of hidden message, is sought in steganography. Whereas, in watermarking; some informations (message, image, logo or signature) embedded into cover data (image, audio signal, video or any other type of media) in order to protect that cover data, not embedded message itself. Since, in watermarking, robustness becomes the most important requirement. Here, the main trade-off occurs between perceptibility and robustness. Capacity feature is not sought in watermarking tasks. Security, robustness and percetibility features are sought properties of watermarking. These requirements are stated in detail in Chapter 3.

Earlier, watermarking procedure was done in different cases. One of application areas of watermarking was printing images on money notes. Watermarks on money notes is shown in Figure 2.4. This figure explicitly represents the watermarks; it is invisible, or let's say not fully visible in normal cases, but it becomes visible when we look to it under light. This embedded watermark protects the money's originality. Thus banks and people can avoid forgery.

Figure 2.4 The basic watermarking from daily life.

Watermarking can also be applied to physical objects, examples include: fabrics, banknotes, and product packaging. By using special, invisible kind of inks and dyes that materials can be watermarked. Nowadays, as technology has developed and internet became convenient communication channel among people, digital watermarking appeared. Today when we deal with watermarking, actually we refer to digital watermarking. In Figure 2.5 the main scheme of watermarking procedure is shown. The main task of watermarking is withstand against noises or attacks in transmission part, so it can be transmitted without any distortions.

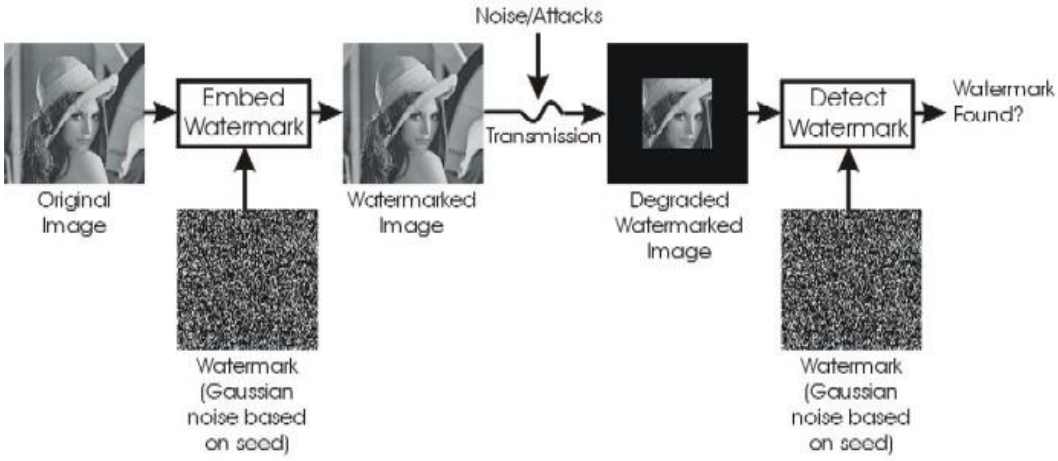


Figure 2.5 Scheme of classical watermarking procedure: Embedding, Transmission and Detection/Extraction of embedded watermark.

CHAPTER 3

DIGITAL WATERMARKING

3.1. Overview

The advent of the Internet has resulted in many new opportunities for the creation and delivery of content in digital form. Communications via Internet becomes very widespread, and also applications include electronic advertising, realtime video and audio delivery, digital repositories and libraries, and Web publishing. An important issue that arises in these communication and applications is the protection of the rights of all participants. Social media provided great opportunity in communication with each other, sharing photos, videos, audios. As these opportunities increases, of course, some security precautions should be considered in order to avoid any forgery. This task considered to be solved using digital watermarking. Social media services can be listed as follows:

- YouTube,
- Twitter,
- Facebook,
- Flickr,
- Google Plus, etc.

Digital watermark was first discovering in 1992 by Andrew Tirkel and Charles Osborne [15]. Digital watermarking is similar to waterking technique which embeds hidden message into digital data rather than papers, banknotes, etc. Basically, watermarking is the process of hiding authentication information in order to prove ownership. Digital version of watermarking, digital watermarking, is the process of hiding **digital information** into a **digital signal** through certain algorithm. Abovementioned digital information can be some text, author's serial number, company logo, images with some special importance. Again, abovementioned digital signal can be an image, a video or an audio signal. The main goal is to ensure the security, data authentication, prove of ownership and copyright protection [16].

As is predictable, there can be implemented so many different algorithms in order to both embed and extract the watermark into/from digital data. Types, properties, requirements of digital watermark and different watermarking algorithms are discussed in next subsections respectively. In the last subsection performance metrics, which are very crucial to decide if the watermarking process meets our needs or not, are stated.

3.2. Types of Digital watermark

Watermarking techniques and watermarks can be classified into different classes in various ways. Because, there are to many aspects in order to implement the watermarking process, or judge its requirements. In Figure 3.1 this classifications are shown obviously.

3.2.1. Domain

Digital Watermarks can be divided into two categories according to working domain as Spatial Domain Watermarking and Frequency Domain Watermarking.

3.2.1.1. Spatial Domain Watermarking

In Spatial Domain Watermarking, the hidden message – watermark, is added to the pixels of still images, or pixel values of frames of videos. Spatial Domain Watermarking is very straightforward, but may not be robust against attacks, and it is difficult task to make it invisible. The most popular Spatial Domain Watermarking is Least Significant Bit (LSB) watermarking. In LSB watermarking, watermark's bits are embedded into Least Significant Bit of host data. It means if an image was encoded with 8 bits, watermark's bits will be embedded into 8^{th} bit of host image or frames of videos. It is very easy way of watermarking, but it is fully invisible, while 8^{th} bit of image is not perceptible by Human Visual System (HVS). While it is fully invisible, because of trade-off between perceptibility and robustness, it is not robust against attacks, such as bit deletion, mean filtering, etc., at all. One more crucial advantage Spatial Domain Watermarking owns; it's computation time is very low. Because, not watermark nor host data is tranformed into another domain. Low Computational complexity is very crucial in real-time applications, since transforming an image into Fourier Domain (Frequency Domain) is computationaly more expensive. So, it affects

the speed of real-time applications. This computational complexity is discussed in detail in the following subsection 3.2.1.2.

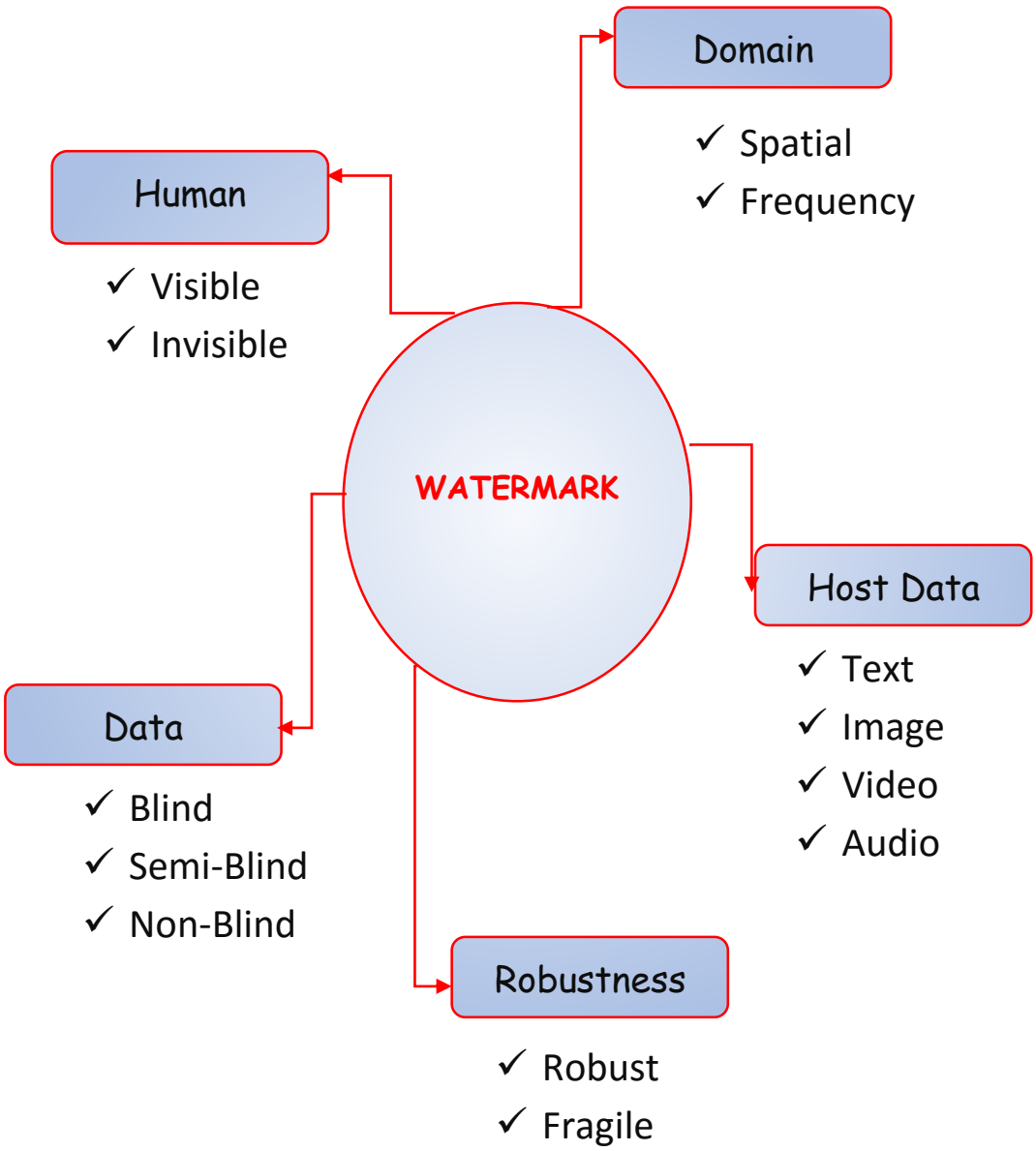


Figure 3.1 Classification of Digital Watermark

3.2.1.2. Frequency Domain Watermarking

In Frequency Domain Watermarking, embedding is done after taking transforms of host data and watermark. By transforming the host data and the watermark we get frequency domain versions of them. Afterwards, embedding procedure is done in frequency domain. There are some sub-domains in the field of frequency domain watermarking: Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT).

Watermarking schemes that operate in a transform space are increasingly common, as these schemes posses a number of desirable features such as:

- By transforming spatial data into another domain, especially into frequency domain, statistical independence between pixels as well as high-energy compaction can be achieved.

- The watermark spreads to entire image when inversely transformed from frequency domain into spatial domain, which makes the watermark hard to detect, decode or read the message by others rather than owner(s).

- One can embed the watermark into the least noticeable areas of host signal, adaptively. These area may be textured area, middle frequencies of frequency domain rather than high or low frequencies.

- Embedding watermark into significant area of host signal can be provided with transform domain methods of watermarking. Also, transform domain watermarking is more robust against attacks and degradations. While, it provides robustness of watermark it also maintains imperceptibilty, which very crutial for human sensory system.

- Cropping may be a serious threat to any spatially based watermark but is less likely to affect a frequency-based scheme. Since watermarks applied to the frequency domain will be dispersed over the entirely of the spatial image upon inverse transformation so we can retrieve part of the watermark.

- Lossy compression usually discards components of a signal that are perceptually unseen or perceptually unimportant. This sorting, separating unimportant

components from important ones, takes place in frequency domain. In fact, matching the transform with compression transform may result in better performance of the data-hiding schema (i.e., DCT for JPEG, Wavelet for JPEG-2000).

- ❖ Frequency domain is very suitable for HVS characteristics [18].

Advantages of Frequency Domain Watermarking are stated above. But still there is a huge obstacle in application area. This obstacle is computational complexity of transforming a digital data into another domain, for instance into Frequency Domain by DFT. A computational cost of DFT of **"N"** dimentional signal is [18]:

$$O\ (N*\log(N)) \qquad (3.1)$$

In 3.1 O (Big O), indicates the computational cost of expression inside the paranthesis. Since, an image dimension is NxN ($=N^2$), then computational complexity of DFT becomes:

$$O\ (N^2*\log(N^2)) \qquad (3.2)$$

As is obvious in 3.2, computational cost increases exponentially as "**N**" increases, i.e. as image dimension increases. This is the main drawback of this kind of watermarkings.

A brief explanation of sub-domain frequency watermarkings are given below.

- DFT – Discrete Fourier Transform: Signals can be expressed as the integral of sine and/or cosine multiplied by a weighting function. This weighting function makes up the coefficients of the Fourier Transform of the signal [19]. In DFT watermarking bits of watermark are embedded into Fourier coefficients – usually into middle frequences. In this way, embedded watermark is not perceptible by human eyes. Because, human eye is not sensitive to changes in middle frequencies in the image.
- DCT – Discrete Cosine Transform: Takes the real components of DFT coefficients. In terms of property, the DCT has a strong energy compaction property. The most crucial advantage of DCT is based on the fact that majority of signal information is concentrated in a few low-frequency components of the DCT. The JPEG compression technique utilizes this property to separate

and remove insignificant high frequency components in images [19]. While, compression standarts (JPEG for images, MPEG for videos) are commonly used, it is judicious to design a watermarking method solely for JPEG and MPEG compressed data. DCT watermarking is used to watermark such, compressed, files.

In Figure 3.2 watermark embedding and extracting procedures, in DCT, are shown.

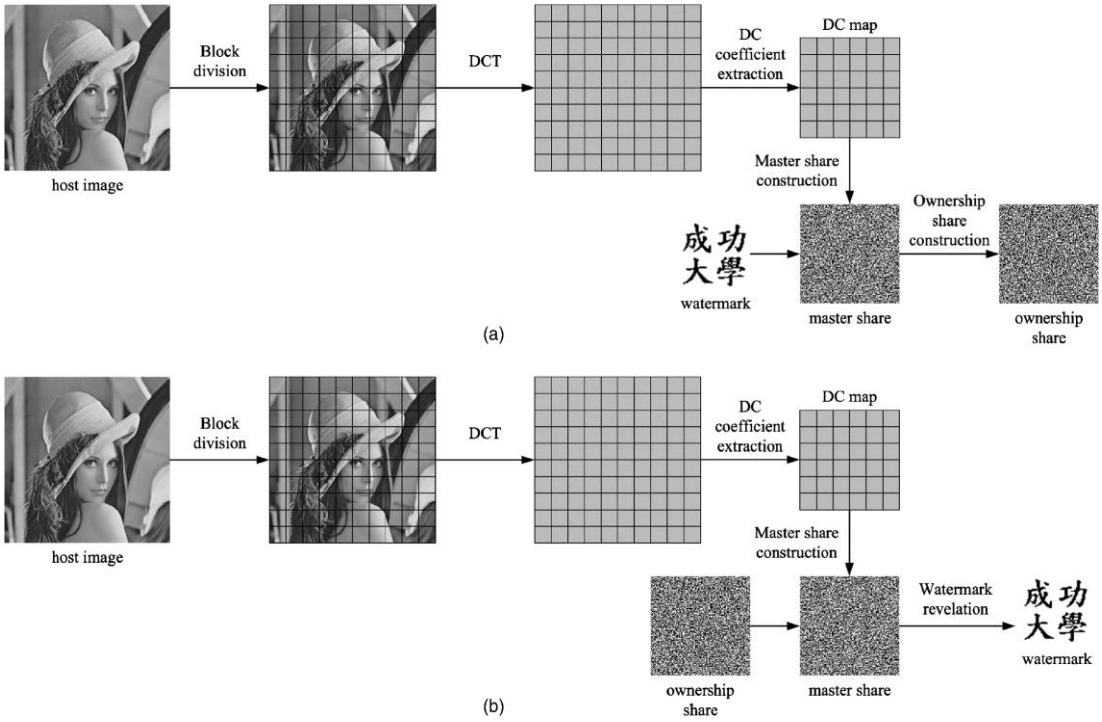


Figure 3.2 DCT watermarking scheme: (a) Procedure of embedding a watermark into image;
(b) Procedure of extracting a watermark from watermarked image.

- DWT – Discrete Wavelet Transform: is something between spatial and frequency domain. It captures both frequency and location information (location in time). DWT decomposes the image into four parts as LL, HL, LH, HH. DWT decomposition of an image is shown in Figure 3.3. Letters stand for applying either low pass or high pass filter operation to the rows and to the columns of an image, respectively.

LL: Lowest Resolution level. It looks like approximative original image.

HL: Consists details of an image, horizontal high frequencies

LH: Consists details of an image, vertical frequencies.

HH: Represents high frequencies.Watermark is embedded into cover signal by modifying these high frequency coefficients. General scheme of DWT watermarking is shown in Figure 3.4.

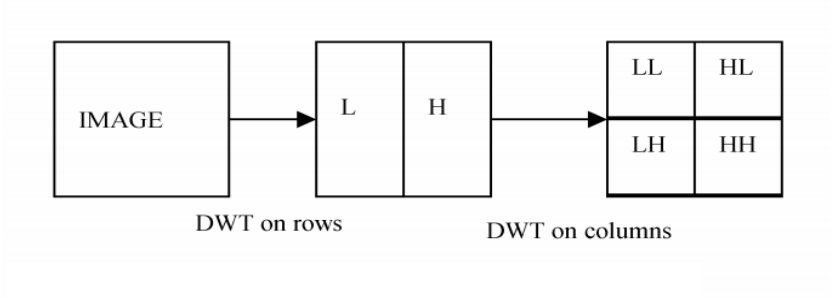


Figure 3.3 DWT decomposition of image

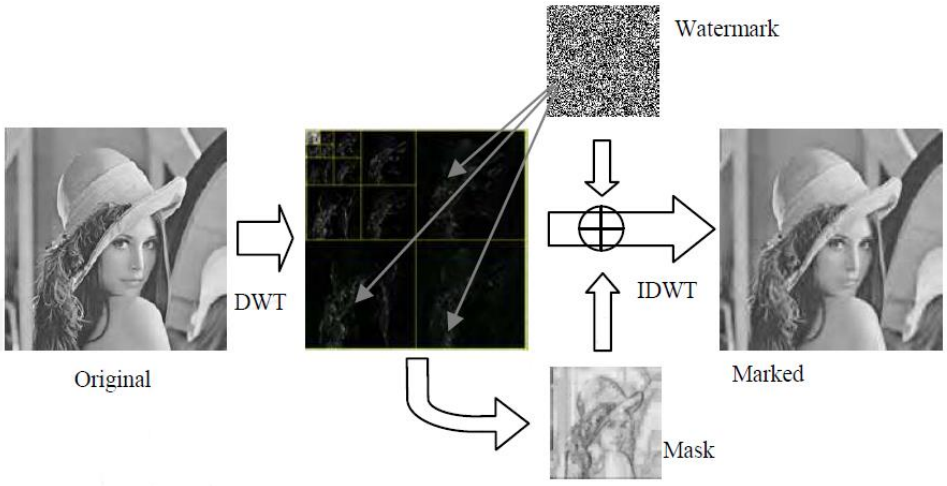


Figure 3.4 Scheme of DWT watermarking.

3.2.2. Human Perception

Perception property is one of the crucial property of Digital Watermarks. Because, we need that our embedded watermark be both robust against attacks and invisible for human. In this perceptron digital watermarks are divided into two classes as visible and invisible. Of course, invisible is more preferred one, but in some cases it is not exactly needed. If our watermark is visible and robust enough, then it is not needed to

make a watermark invisible. Therefore, chosing either visible or invisible watermarking is depends on application area and purpose of use. In Table 3.1 main differences, pros and cons of both visible and invisible watermarks are listed.

Table 3.1 Visible Watermarking vs. Invisible Watermarking.

	Invisible Watermarking	**Visible Watermarking**
Watermark Perceptibilty	Imperceptible distortion	Visual pattern
Extraction	Explicit extraction module	Direct Viewing
Protection	Passive	Active
Robustness	Intentional attacks and/or signal processing	Watermark removal (with some distortios at cover media)
Current Research Status	Hot	Only few papers

3.2.2.1. Visible

Visible Digital Watermarks are very straightforward to understand and easy to embed into cover data. For example, if you watch any news channel, you will quite often see their logo embedded into some corner of the screen to show that this particular video being transmitted to your TV did come from that news station. Also, if you happen to come across a website that sells music online, they may have sample music file that is a whole music, but also includes some phrase or note in different places that you can noticeably hear. Both of those are considered visible digital watermarking because you can “see” them—for the case of audio, because you can hear it and identify the

watermark. In Figure 3.5, example of visible watermark is shown. While embedding visible watermark into an image or any kind of signal, one of the most important things we need to pay attention is; not to disrupt the original signal's details. It means, host signal should not be rendered useless by the watermark that was embedded into signal. The other thing that we should pay attention while embedding visible watermark is; robustness. What we deal with robustness is; watermark should not easily removed from the signal without any distortion in the signal. Let's say one has removed the watermark from the signal, then he/she should not use that signal because of distortions. Let's wrap this analogy; robustness of visible watermark is proportional to it's distortion after removing watermark from the host signal.

Figure 3.5 Visible Watermark: ABC NEWS channel

3.2.2.2. Invisible

The other class of digital watermark in terms of human perception is invisible watermark. The main idea in invisible watermark is not to arouse suspicion that there

exist any watermark. Because of trade-off between robustness and imperceptibility, invisible watermark tends to be less robust compared to visible watermark. Expected and intended task is to propose both imperceptible and robust watermark. This challenge can achieved by propose such a watermark, that is suitable for HVS and invariant against some kind of attacks. As previously described, there is a trade-off between robustness and imperceptibility. But in application area there is a parameter, namely computational complexity, that is also very crucial in real time applications. We can imagine that now we have a trade-off between robustness, computational complexity and imperceptibility. This thesis deals with noval digital watermarking that is imperceptible, computationally cheaper, and robust against some kind of attacks (not all kind of attacks!). Imperceptibility was obtained using LSB watermarking; less computational complexity was achieved by embedding the watermark in spatial domain; and finally robustness against some kind of attacks was ensured by embedding the watermark into 6^{th}, 7^{th} or 8^{th} less significant bit of frames in a video. This phenomena was described in details in Chapter 5 – Watermarking with optimization methods.

3.2.3. Host Data

There are four types of digital watermarking, based on host data differences, to identify the originality copyright owner(s) of the content: an image, a plain text, an audio, a video or a combination of some of them or all. These types of digital watermarking are emerged because we may need to embed a watermark into different types of signals, or into combination of some of them. The main idea is the same in these types of watermarkings, but according to structure of cover signals, watermarking procedure varies in some sense.

3.2.3.1. Text Watermarking

Digital Text Watermarking is the procedure that embeds a digital watermark into a text based digital document that carries information unique to the copyright owner or to the creator of the document. Text is widely used type of signal in communication in internet. So text watermarking reveals in order to protect text. As other types of host data based digital watermarks use redundant bits in order to be able to embed a watermark, in text based digital watermark we should find some redundancy in text

documents. The binary nature, line or word patterning, text meaning, structure of the text, style, language rules, are some of the exclusive properties of text documents. These properties can be exploited during watermarking a text document. The size of text plays a huge role in digital text watermarking, because the bigger size of the text causes embedding the more information. Another property of Digital Watermarking, called “Capacity”, is the amount of data that can be embedded into digital signal; the more capacity means the better watermarking. All properties of Digital Watermark are discussed in details in Subsection 3.3.

In literature, some researches worked on text based digital watermarking. These works can be classified into three classes according to text watermarking approaches as semantic based approach, syntactic based approach and image based approach. In the following paragraphs a brief explanations of text watermarking approaches are stated.

In image based digital text watermarking, watermark is embedded into text by changing the visual view of the text; shifting the line or shifting the word position to the right/left or upward/downward, etc. according to watermarks content.

In syntactic based digital text watermarking, watermark can be embedded by applying syntactic transformation on structure of text. Syntactic of a text means, set of rules, principles, and processes that govern the structure of sentence in a given language.

In semantic based digital text watermarking, to embed the watermark semantic structure of the text is used. Verbs, nouns, prepositions, acronyms, grammer rules, sentence structure, word spellings are exploited in order to embed a watermark into text document [20].

3.2.3.2. Image Watermarking

In image watermarking we need to find some redundancies in image data, as is the case in all watermarking schemes. Redundancy in an image can be described as the part of the image that is unseen to HVS. If we deal with frequency domain, redundancies in frequencies can be high frequency components of Fourier Transform for example. Small changes in high frequencies are not visible for humans. But in compression techniques such as JPEG, high frequencies are tend to discarded in order to dicrease the size of an image. So the idea to embed the watermark in high

frequencies does not make sense at all. On the other hand, changes in low frequencies are easily detectable by human eyes. Hereby, in frequency domain image watermarking, reasonable embedding procedure is embedding the watermark into middle frequencies, that are neither discarded while compressing the image nor visible by human eyes.

If we deal with spatial domain image watermarking, requirements are both imperceptibility and robustness. In the spatial domain, image contains bit planes, usually 8 bit planes, that creates a whole gray or RGB image when placed one after another. Gray image contains one channel, while RGB image contains three channels each consisting 8 bit planes. Redundancy in spatial domain images can be thought by making analogy that which part of image, or which bit plane of an image, is not perceptible to human eyes. Of course, the Least Significant Bit, i.e. 8^{th} bit, is less perceptible in image signals. So, it can make sense that embedding to LSB is enough to success embedding task. But, there is a drawback of this technique. This drawback is, when watermark is embedded into LSB of an image, it becomes less robust against attacks (like bit deletion, median filtering, etc). On the other hand, embedding the watermark into Most Significant Bit (MSB) causes visual degradations in the watermarked image. These are main logic frames in digital image watermarking. In literature exist a lot of papers for digital image watermarking, some of them are given in [21-23].

3.2.3.3. Video Watermarking

Digital Video Watermarking is the same with Digital Image Watermarking in some sense. Because video signal consists of video frames, which are semantically the same with images. Digital Image Watermarking requirements are also valid for Digital Video Watermarking, but video hold an additional property rather than still images which is time dimension. If a video is encoded with 30 fps (frames per second), then there exist 25 frames (equivalent with still images) in one second of video. Therefore, we need to make analogy from digital image watermarking to digital video watermarking in terms of finding a redundancy to be able to embed a watermark. Time dimension of a video, or in other words temporal property of a video is very crucial thing that has to be considered. Consecutive frames causes visual degradations if successive frames are not similar with each other, i.e. embedding a watermark into

some of frames rather than all, causes visual distortion in digital video signal. In this manner, imperceptibility of watermarking procedure would not provided. However, video signal contains more redundant data compared to still images.

Digital Video Watermarking can be done in spatial domain, frequency domain at raw video signal or in compressed video signal. There are a lot of papers published to provide video watermarking into compressed video like MPEG, H.262, H.263, H.264, HEVC/H.265 etc. [24-26]. And also exist raw video watermarking algorithms in the literature [27].

3.2.3.4. Audio Watermarking

Digital Audio files are particularly the most abused for copyright infringements because they can be downloaded and copied with ease. Audio watermarking schemes rely on the imperfection of the human auditory system. Human ears are more sensitive to other sensory organs, so it is a challenge to design good audio watermarking scheme [28]. Digital audio watermarking should be carefully chosen considering the following properties of watermarking; robustness to signal processing, perceptual quality, bit rate, watermark security, and computational complexity. As in the previous host data based watermarkings, it is expected to find some redundancies in audio signal, it may be high frequency audio signals that are not reliable from human ears.

Digital audio watermarking techniques can be listed as follows, but details will not be mentioned in this thesis:

1. Spread Spectrum watermarking
2. Amplitude modification
3. Replic method
4. Dither watermarking
5. Self-Marking method.

3.2.4. Data Extraction

Digital Watermarking procedure consists of three steps; embedding, transmission, and extraction. In embedding part, watermark is designed, and embedded into cover media.

At transmission part, the watermarked signal will be transmitted to somewhere, or will be uploaded into internet. In transmission part there may be attacks, noises, or intentional signal processing may be implemented in order to detect a watermark or at least to destroy cover media's content to avoid healthy extraction of watermark from watermarked media. Extraction part is very crucial to prove ownership, in this stage watermarked signal expected to be not degradated by noises, any kind of attacks. Watermarking stages are shown in Figure 3.6 in general.

Watermarking systems are classified as non-blind, semi-blind and blind watermarkng according to whether the original media is needed or not to extract the watermark from watermarked media [29].

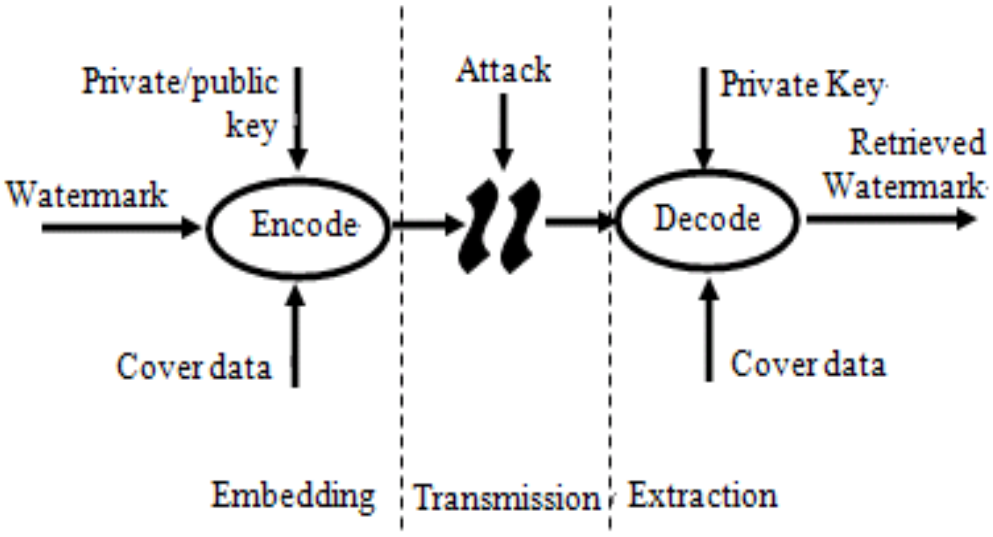


Figure 3.6 General stages of Digital Watermarking

3.2.4.1. Non-Blind Watermarking

Non-Blind Watermarking needs the original media in extraction stage. Main disadvantage of non-blind watermarking is difficulty of carrying the original media

always to be able to prove ownership, or in general to extract the embedded watermark. This causes the limitations at usage of non-blind watermarks.

Watermark extraction is done by computing the differences between original media and watermarked media, in this manner watermark can be extracted and it can be used as it is expected in ownership proof, content identification, etc.

3.2.4.2. Semi-Blind Watermarking

Semi-blind watermarking schemes do not need the original media, but it requires the watermark itself or any other side information like private key. Private key may be a secret password that is unique for media's owner. Watermark can be extracted by the help of this secret private key.

3.2.4.3. Blind Watermarking

Blind Watermarking does not need neither original media nor watermarks itself at extraction stage. Blind watermarking schemen can be achieved by embedding the watermark according to fixed algorithm. At extraction or decoding stage watermark can be easily extracted by the help of that algorithm that was used in embedding or encoding stage. Proposed noval digital video watermarking in this thesis belongs to blind watermaking. Blind watermarking scheme was developed by embedding the watermark into different bit-planes of video frames using genetic algorithm. By running the same genetic algorithm at the extraction stage, watermark can be obtained, in other words bit-planes can be find again at which the watermarks were embedded.

3.2.5. Robustness of Watermarking Schemes

Robustness plays a huge role at transmission stage, because embedded watermark has to stand up to attacks or intentional signal processings. In this point of view digital watermarks divided into two categories as Fragile and Robust Watermarks.

3.2.5.1. Fragile

Briefly saying, fragile digital watermarks are not robust against attacks such as bit deletion, frame averaging, mean filtering, geometric attacks, or any noises. If there is

no threatening exist in transmission stage, then fragile digital watermarks can be used if it provides advantages in terms of computational complexity.

3.2.5.2. Robust

In recent researches are at progress in the direction of designing robust digital watermarking. Ideal digital watermink scheme has to be robust against any imaginable attacks. In literature, proposed papers solved this robustness against some attacks; geometric attacks [30], filtering attacks [31], frame attacks [32], etc.

3.3. Properties of the watermark

There are a lot properties that should be provided in order to design an ideal digital watermark. Some of properties will be explained briefly below.

- *Robustness:* The robustness is the ability of detecting the watermark after some signal processing modification such as spatial filtering, scanning and printing, lossy compression, translation, scaling, and rotation [33], image enhancement, cutting, etc.
- *Imperceptibility (*Sometimes called *Fidelity* or *Invisibility)*: is the similarity between original media and watermarked media, in other words visual insignifacance of watermark. This property is very crucial for not to arouse a suspicion.
- *Computational Complexity or Cost:* computational complexity adresses the speed of embedding and extracting of watermark. Desired digital watermarking should be as low as possible in terms of computational complexity or cost.
- *Security:* Ability to resist against intentional degradations that cause the change in visual view or changes the purpose of embedding the watermark.
- *Capacity (Payload):* Capacity of digital watermark indicates the number of possible bits embedded into a digital signal. This property is concerned with Robustness and Imperceptibility. Because, embedding more information may cause to low imperceptibility, or may not be as robust as it was intended.

3.4. Performance metrics

Performance metrics are very crucial in order to judge the goodness, robustness, imperceptibility of designed watermark. There are two categories of performance measurements: Full-Reference Quality Metrics and No-Reference Quality Metrics.

Full-Reference Quality metrics measures the amount of change between original media and watermarked media using the similarity. This metrics is used when both original and watermarked media exist.

On the other hand, if there is only one document exists, then No-Reference Quality metrics are used. This quality metrics evaluates the quality of that media/signal [12].

X_i – original signal

$X_i^{'}$ – watermarked signal

M – Number of samples in the signal

- *Mean Square Error (MSE):*

$$MSE = \frac{1}{M}\sum_{i=1}^{M}(x_i - x_i')^2 \qquad (3.3)$$

- *Peak Signal Noise Ratio (PSNR):* Max variable indicates the possible maximum value that signal may take. Unit of PSNR is decibel – dB.

$$PSNR = 10\ log\frac{MAX^2}{MSE} \quad (3.4)$$

- *Normalised Cross-Correlation (NCC):*

$$NCC = \frac{\sum_{i=1}^{M} x_i * x_i'}{\sum_{i=1}^{M}(x_i)^2} \qquad (3.5)$$

- *Average Difference (AD):*

$$AD = \frac{\sum_{i=1}^{M}(x_i - x_i')}{M} \qquad (3.6)$$

- *Structural Content (SC):*

$$SC = \frac{\sum_{i=1}^{M} {x_i}^2}{\sum_{i=1}^{M}(x_i')^2} \qquad (3.7)$$

- *Maximum Difference (MD):*

$$MD = Max(|x_i - x_i'|) \qquad (3.8)$$

- *Normalized Absolute Error (NAE):*

$$NAE = \frac{\sum_{i=1}^{M}|x_i - x_i'|}{\sum_{i=1}^{M}|x_i|} \qquad (3.9)$$

CHAPTER 4

OPTIMIZATION METHODS

Some problems may be solved by straightforward mathematical calculations, or by using linear algebra. Let's think N (≤10) equations with N (≤10) unknown variables. To solve this problem we have to solve a matrix with dimensions of N-by-N. This problem may be solved by hands, or using computers. Actually solving this kind of problems is equivalent with making a search in N^2-dimensional space. It is okay while N is small enough, but when it gets larger and larger, then it will becomes somehow impossible to solve it by hands, or even by using computers because of its high computational cost. Actually computers can solve, make search in N^2-dimensional (note that N is big number) space and find the actual solution, but it takes lots of time. In order to overcome this drawback, there exist heuristic methods to find the near actual solution of the problem. Optimization methods make this search for us, and surprisingly find the very close solutions to actual solutions. There are two main and widespread optimization methods exist in the literature: Genetic Algorithms and Neural Network.

4.1. Genetic Algorithms - GA

John Holland was invented GA in the early 1970's. Genetic Algorithm is the search heuristics that mimics the natural selection. Genetic Algorithm was inspired from nature, and seeks for best/optimal solution for the problem. Genetic Algorithm represents an intelligent exploitation of historical information at determining the search direction in the search space. The basic techniques of the GAs are designed to simulate processes in natural systems necessary for evolution. Competition between individuals provides that fittest individuals dominate the weaker ones.

Some search algorithms may work well in small-spaces like linear programming, depth-first search, brute-force search, breath-first search. But in a large space GA provides a significant benefits over those search algorithms.

Why Genetic Algorithm

The most important and evident feature of genetic algorithms is, there no need to any information about of the problem or information about nature of search space in which searching procedure is performed. In order to reach the solution, no needs to make complex numerical calculations. GA performs global search rather than local search for finding the optimal solution. Surprisingly, GA are able to find the global optimum (near optimum) point/solution in the complex multi-dimensional search space. And another advantage of GA is that it can work with many parametes, so can be operated using parallel computers, GPU's may be used in order to run GA due to GPUs can make parallel computations in a time [34].

How does GA work

Each individual represents a point in a search space and a possible solution. The individuals in the population are then made to go through a process of evolution.

GAs are based on an analogy with the genetic structure and behaviour of chromosomes within a population of individuals using the following foundations:

- Individuals in a population compete for resources and mates.
- The most successful individuals in a competetion will produce more children compared to poorly successful ones.
- Genes from `good' individuals keep progress throughout the population. Sometimes the better child may be created from two worse parents.
- In this manner, each generation after each selection become more suitable to environment.

Flow chamber and evolution cycles of GA are shown below in Figure 4.1 and Figure 4.2.

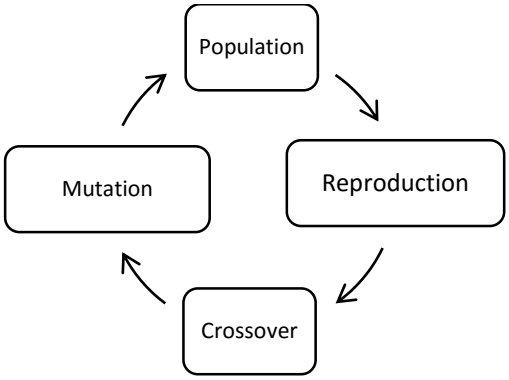


Figure 4.1 Flow Chamber

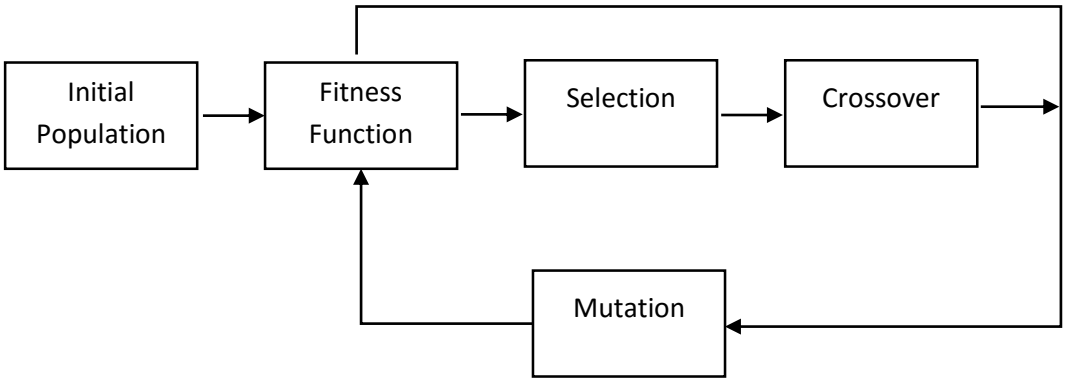


Figure 4.2 Genetic algorithms evolution cycles

Operators of GA

Each generation in the population represents a possible optimal solution to a problem that has to be solved. Each individual is coded with binary numbers: “0”s and “1”s. Individuals in GA are analogous to chromosomes and variables are similar to genes. Fitness score of each individual is assigned as expected solution that indicates the abilities of that individual to compete among other individuals. The individual with the optimal (or generally near optimal) fitness score is sought. The GA aims to use selective `breeding' of the solutions to produce `children better than the parents by combining information from the chromosomes.

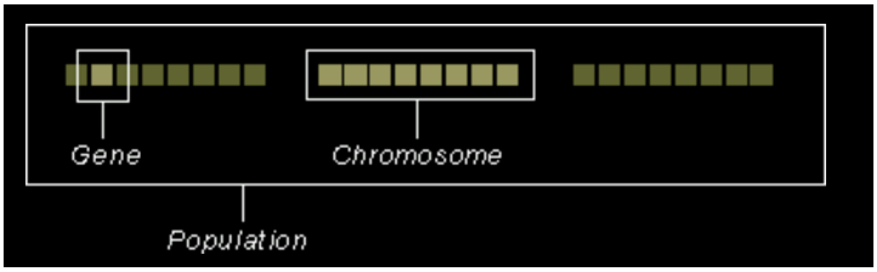


Figure 4.3 Population representation in GA.

The GA saves a population of n (n is determined by the user, can be tuned) chromosomes (solutions) by looking for thier fitness values. Parents are selected to mate, on the basis of their fitness, producing children via a reproductive plan. Hereby, GA gives more opportunity to reproduce to highly fitted solutions, so children tend to carry the properties of each parent. So, stronger individuals tend to live, while weaker ones are subjected to die. Dead individuals are replaced with new individuals (solutions), new As parents mate and produce children, room must be made for the new arrivals since the population is kept at a static size. Individuals in the population die and are replaced by the new, randomly or based on historical information, generated solutions. In this way it is hoped that over successive generations better or optimal solutions occurs while worse solutions die out.

New generated solutions are created based on the historical informations as containing more good genes than a previous one. Consequently, each successive generation tend to contain more good `partial solutions' than previous generations. Eventually, GA will stop running when population can not generate the different, in terms of fitness, children than previous ones. Stop running means that algorithm has converged to a (near) optimum solution.

After randomly generating the initial population , GA proceeds to evolve the following three operators:

1. **Selection –** provides the survival of the fittest one,
2. **Crossover –** represents mating between individuals,
3. **Mutation –** introduces random modifications.,

- **Fitness Function and Selection:** Fitness function should be determined in order to be able to use GA optimization method. Fitness function measures the fitness of each

individuals. From other point of view, fitness function summarizes how to close a given design solution is to achieving the set aims. After looking at all the fitness values of individuals in the population is checked according to termination criteria. If the termination criterion is satisfied, the genetic algorithm tends to stop.

Key idea of selection operator: gives chance to better individuals to pass on their genes to the next generation. The goodness of each individual depends on its fitness. Fitness of individuals are defined by objective function or by a subjective judgement.

- **Crossover:** Two individuals are selected from the population based on a logic of one of selection methods. Crossover part of binary strings of two individuals are chosen randomly. Values of those selected parts of strings are swapped. These newly generated binary strings are called new children generated by performing crossover operator and putted into next generation of the population. So next generation tends to be more fitted than old one. In Figure 4.4 crossover operation is shown.

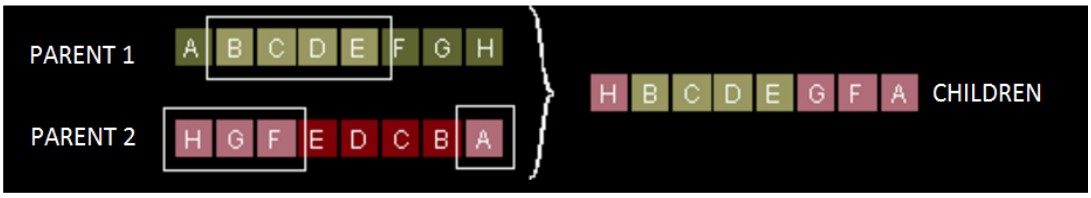


Figure 4.4 Crossover Operator.

- **Mutation:** In mutation, a portion of new individuals' bits are shuffled with a low probability. Analogy of mutation in GA to search algorithms is randomly walk in searh space with low probability, i.e. walk in search space randomly very rarely [35-37].

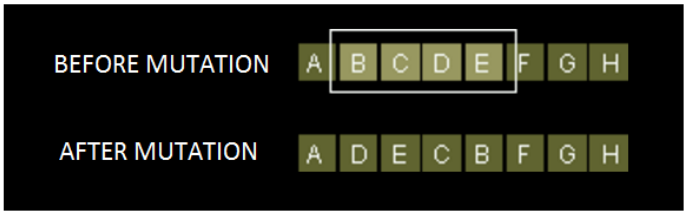


Figure 4.5 Mutation Operation.

4.1.4 Pseudo-Code of GA

1. Initialize the population randomly (t)
2. Assign a fitness function to population (t)
3. repeat
    1. Make selection of parents from generated population (t)
    2. Perform crossover operation on parents and create a population (t+1)
    3. Make mutation for population (t+1)
    4. Evaluate the fitness function's value for population (t+1)
4. until iteration number reaches the maximum number OR best individual is good enough as expected

4.2. Neural Networks (NN)

Neural Networks is the most widely used optimization method in recent years. Neural Networks were inspired from neural network structure of human brain. NN sometimes named as Artificial Neural Networks (ANN), as it acts artificially. In last recent years, so many researches have focused on NN/ANN to solve big problems, make a seacrh in a big search space, or even to make machines intelligent. By NN algorithms machine can make a classification or regressiion on image datasets, can make decision what kind of objects exist in the image, can perform scene recognition, can extract features from a set of images or from set of audio signals, can make classification of given images to which class does it belongs. Neural Networks are very closely used in research areas as: Artificial Intelligence and Machine Learning.

Brief History of NN

Beginning of NN is based on 1940s years. McCulloch and Pitts [38] published a research article, in which showed that even simple types of neural networks could compute any arithmetic or logical function. Norbert Wiener and von Neumann worte

a book and research paper in which they suggest that the research into the design of brain-like computers might be interesting.

The 1950s and 1960s were the first golden age of NN. In 1957 and 1958 the first successful neuro-computer was developed by Frank Rosenblatt, Charles Wightman.

The 1970s were the quiet years. In early 1980s many Neurocomputing researchers became courageous to begin submitting proposals to explore the development of neuro-computers and of neural network applications.

In 1982 John Hopfield wrote a papers on neural networks [39] and persuaded hundreds of scientists, technologists to join the emerging field of neural networks.

Why Neural Networks?

There are some problem categories that they can not be as an algorithm. Computers can not solve Problems without an algorithm, so there arises a question about how to teach to solve these kind of problems to computers, that computers solve the complex problems or make search in large search space. Actually, computers can not learn anything, but humans can. NN were inspired from this point of view, structure of brain satisfies learning. Building similar system on computers may help us to teach something to computers.

Componens of Artifical Neural Networks

A technical neural network consists of simple processing units, the ***neurons***, and directed, weighted connections between those neurons. These connections carry an information about problem. NN can contains at least three layers: input layer, hidden layer, and output layer, or may contain N+2 layers: input layer, hidden layer # 1, hidden layer # 2, hidden layer # 3, ..., hidden layer # (N-1), hidden layer # N, and output layer. In each hidden layer there may exist any number of neurons. In input layer there have to number of neurons that equals to number input features. In output layer neurons number must be equal to number of classes in classification problems. However, in regression problems number of neurons in output layer have to be “1”. Components of classical Neural Network is given in Figure 4.8 with input layer, two

hidden layers, and uotput layer. Input layer consist of two neurons, each hidden layer consist of four neurons, and one neuron at output layer. Connections between layers are also shown.

Working principle of NN

There are two states in NN algorithm: training, cross validaton, test states.

In training state NN learns the weight (connections) values according to given input and given ground truth outputs. Training state contains feedforward and backpropagation parts; in feedforward network learns weights from given input, and at the output layer it predicts some output. Comparing this predicted output with ground truth labels, estimation error is evaluated. In this time, algorithm flows in reverse side named as backpropagation. In backpropagation part, given the estimation error at the output layer, goes back to input layer by dividing the errors equally to all neurons in all layers. Feedforward algorithm is shown in Figure 4.6, while backpropagation algorithm is shown in Figure 4.7.

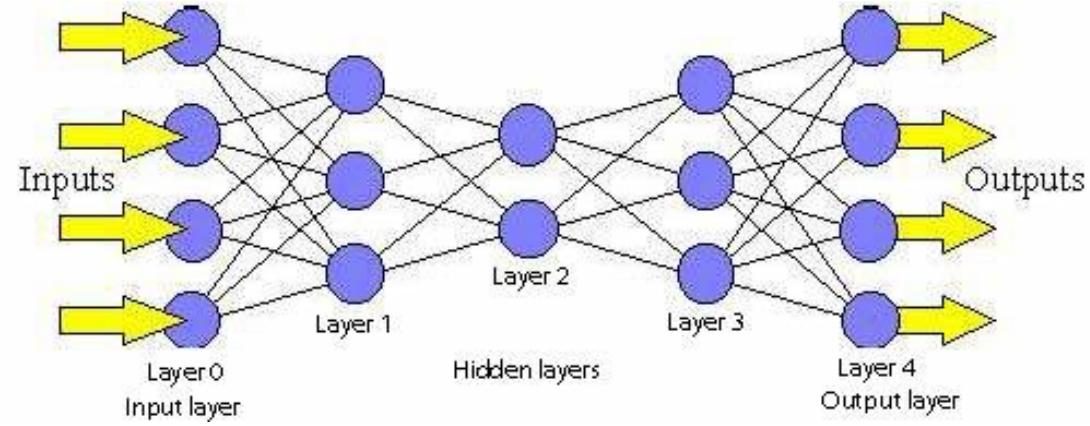


Figure 4.6 Feedforward Algorithm of NN.

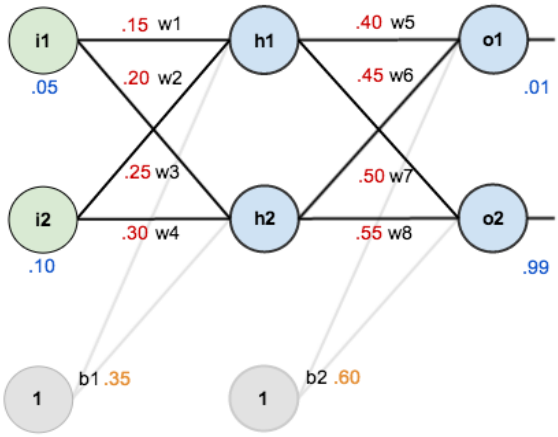


Figure 4.7 Backropagation Algorithm of NN.

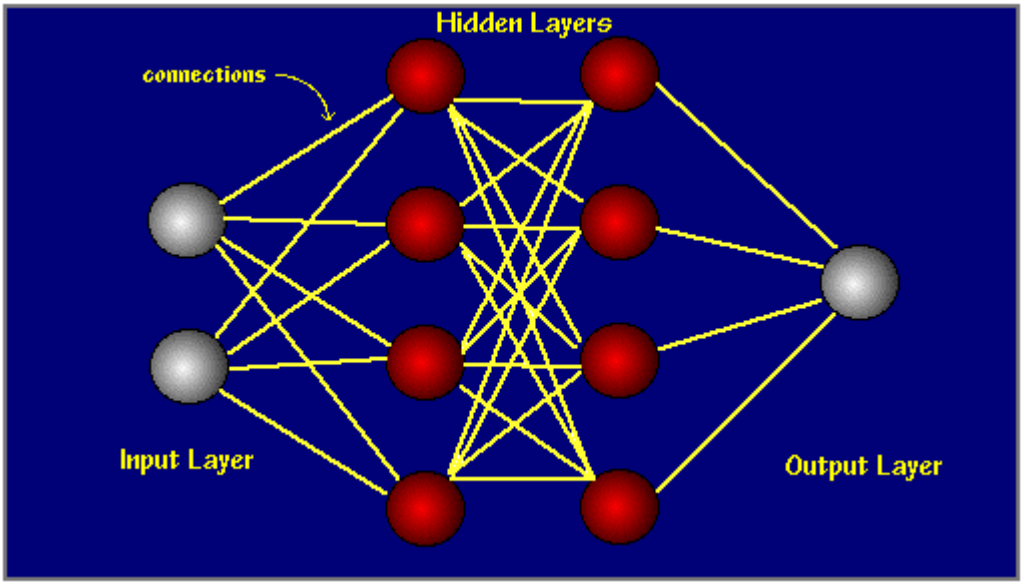


Figure 4.8 Components of classical Neural Network.

CHAPTER 5

WATERMARKING WITH OPTIMIZATION METHODS

Since there are a lot parameters in digital watermarking, and some trade-offs betwen parametes, then it is very hard to select the best parameters for specific purpose of use. This search of appropriate parameters is analogious to searching the solution in very big search space with several local minimas. To overcome this task we can use optimization methods to build a digital watermark algorithm. In the following paragraphs digital watermarking algorithms in the literature that used optimization methods will be described briefly. First four proposed works used Genetic Algorithms to optimize the parameters of Digital Watermarkings, while the last ones use the Neural Networks Algorithm.

1. An Oblivious and Robust Multiple Image Watermarking Scheme using Genetc Algorithm [40].

In this paper, a novel oblivious and robust image watermarking scheme using Multiple Desription Coding and Quantization Index Modulation is proposed. Genetic Algorithm is used to optimize performance metrics of watermarking that conflicts to each other; Peak-Signal-Noise-Ratio (PSNR) and Normalized Cross Correlation (NCC). Where PSNR measures inverse proportion of the amount of distortion introduced to the host image during embedding, while NCC measures the amount of similarity between original watermark and extracted watermarks. So, NCC indicated the robustness of watermarking algorithm, while PSNR refers to imperceptibilty of watermarking scheme. Because of trade-off between imperceptibility and robustness, that was stated above, there is a need to chose the optimum imperceptibilty and robustness value to achieve a good watermarking scheme. In this point of view, one can use optimization methods to optimize these two parameters. In this work, Genetic Algorithm is used to optimize PSNR and NCC values. Using GA, the optimum PSNR and NCC values chosen that yields a both imperceptible and robust watermarking scheme in image watermarking.

2. A Genetic Algorithm based Video Watermarking in the DWT domain [41].

To decompose the video into difference scenes, scene change analysis is used. Each frame of a video transformed to wavelet domain by Discrete Wavelet Transform (DWT). Watermark is represented with 8-bits planes and embedded into mid-frequency DWT coefficients. Genetic Algorithm is used in order to optimize the quality of the watermarked video. In this paper, watermark image is decomposed into parts and referred as chromosomes, and tried to decide which chromosome is suitable to which scene of the host video signal. To find the optimum coupling, GA is used as a search algorithm. In order to be able to use GA, there should be defined the fitness function. In this work fitness function of watermark image was defined Mean Absolute Difference (MAD) of an image. Fitness function is shown below:

$$f = \frac{1}{\sum_{x=0}^{3}\sum_{y=0}^{3}|I'(x,y)-I(x,y)|} \qquad (5.1)$$

3. Watermarking Robustness Evaluation Based on Perceptual Quality via Genetic Algorithm.

In this paper a novel benchmarking tool to evaluate the robustness of any digital image watermarking system based on GA is proposed. PSNR metric is handled, PSNR is optimized by finding the minimal degradation of image that is toleranced to be in a marked image. Given a set of different attacks, GA accomplish the optimization of the parameters in order to obtain an unmarked image with perceptual degradation as low as possible. Block diagram of implemented framework in this work is shown in Figure 5.1.

4. Adaptive digital watermarking of images using Genetic Algorithm [43].

Adaptive watermark strength optimization in Discrete Cosine Transform (DCT) domain method is proposed. Watermark strength is selected through GA intelligently. GA helps to choose the perceptibility of image that is less perceivable to Human Visual System (HVS). Proposed method makes the watermarked media robust against attacks

like low-pass filter, high-pass filter, median filters, shifting and cropping the marked image.

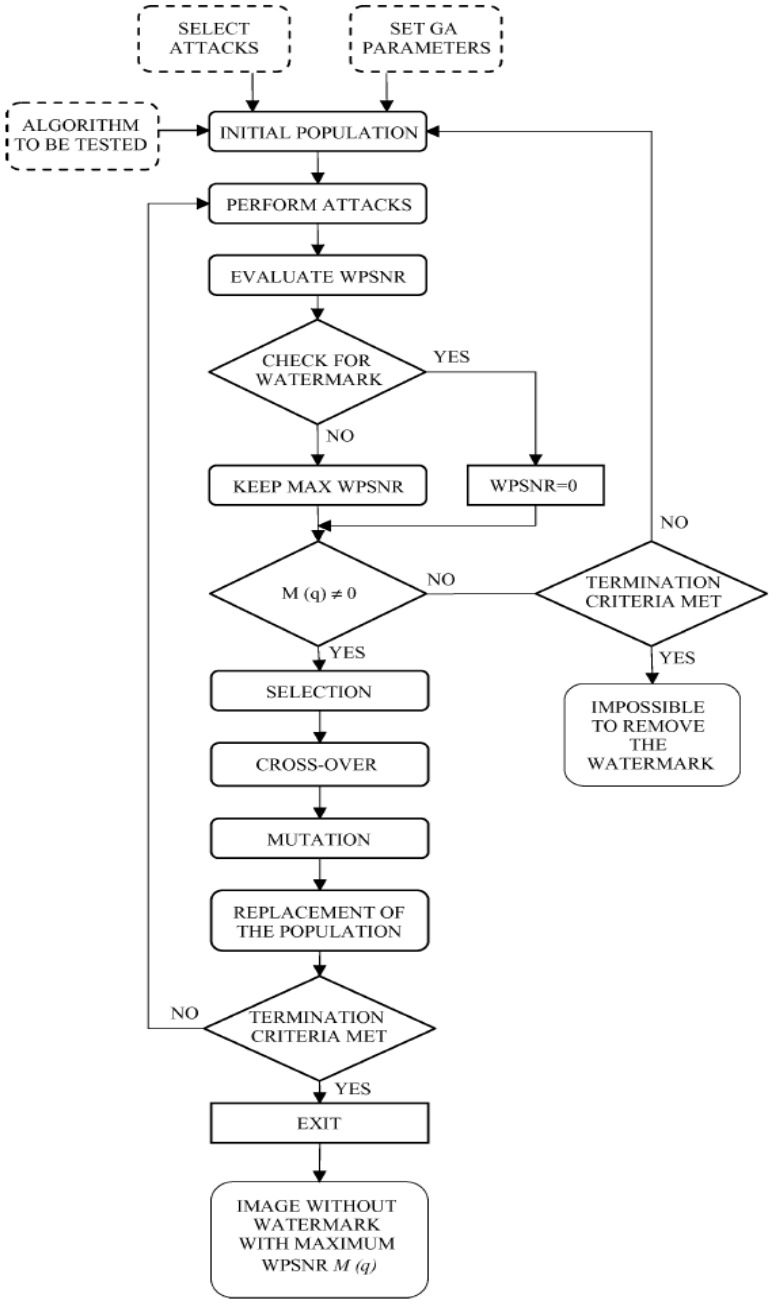


Figure 5.1 Block Diagram of the implemented framework in [42].

5. A Study on Digital Image and Video Watermarking Schemes using Neural Networks [44].

Pao-Ta Y. proposed a novel digital watermarking technique [45] based on neural networks for color images. Proposed method hides an invisible watermark into a color image and then uses a neural network to learn the relationship between the embedded watermark and watermarked image. This knowledge is used as a digital signature in the extraction process, thus there proposed a semi-blind watermarking scheme. Several embedding techniques are adopted to improve the performance.

6. The Robust Digital Image Watermarking Scheme with Back Propagation Neural Network in DWT domain [46].

In this paper proposed a blind robust digital image watermarking approach based on back propagation neural network in DWT domain. The back propagation neural network is trained in a such way that it reaches highest accuracy. BPNN is used in embedding and extracting the watermark. Pseudo-Code of this proposed work is given below [46]:

Step 1. Read the contour image of size NxN.

Step 2. Resize the color image to 256x256 pixels and use it as a cover image.

Step 3. Select the blue plane to embed the watermark.

Step 4. The frequency subcomponents {HH_1, HL_1, LH_1, {HH_2, HL_2, LH_2}, { HH_3, HL_3 LH_3}, { HH_4, HL_4, LH_4}}} are obtained by computing the fourth level DWT of the resized color image.

Step 5. Read the bitmap of size 64x64 as the watermark.

Step 6. Select the beginning position of watermark using the secret key.

Step 7. Initialize the weight vectors, fix the epochs, set the initial learning rate.

Step 8. Quantize the DWT coefficient $T_{(j+key)}$ by Q as the input to the RBFN.

Step 9. Embed the watermark using the following equation

$$T'_{(j+key)} = BPNN\ (round\ ((T_{(j+key)} / Q) + x_j \quad ... (5)$$

Where x_j is the random watermark sequence.

Step 10. Find the difference between input values and trained values. The resultant values are accepted as watermark.

Step 11. Perform IDWT on each coefficient to get the watermarked image.

7. *Image authentication algorithm with recovery capabilities based on neural networks in the DCT domain [47].*

In this paper image authentication algorithm in DCT domain based on NN is proposed. Watermark consists of the average value of each 8 × 8 block of the image. Watermark was embedded into middle frequencies coefficients of the DCT transform of an image. Additionally a NN is trained in order to use it in extraction of watermark. This proposed method becomes robust to JPEG compression. Figure 5.3 shows the flowchart of the proposed image watermarking algorithm.

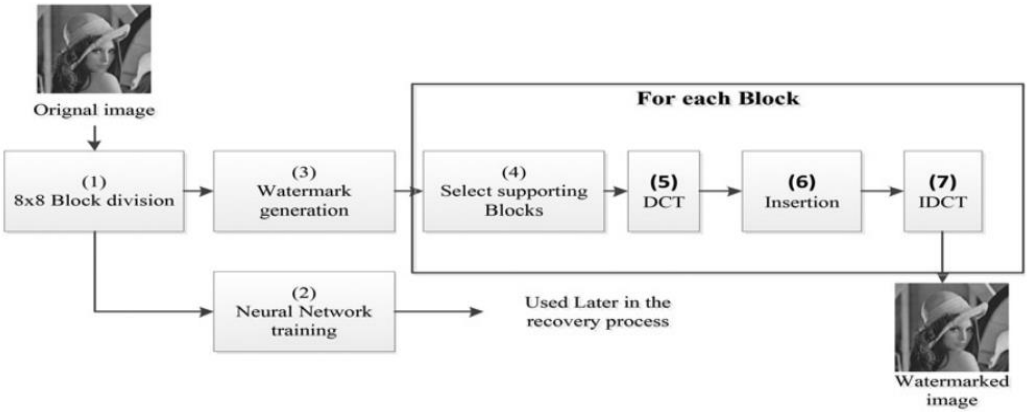


Figure 5.2 Flowchart of the proposed image watermarking algorithm in [47].

CHAPTER 6

PROPOSED WORK, EXPERIMENTAL RESULTS AND DISCUSSION

6.1. Proposed Work

In this thesis, we propose a novel method for Digital Video Watermarking using Genetic Algorithms. In Chapter 3, some digital watermarking methods are stated. It is obvious that the most straightforward and computationally the less complex one is Least Significant Bit (LSB) method. Main advantages of this method is; computational cost is low, and very imperceptible to Human Visual System (HVS). However, main drawback of LSB is; it is not robust against filtering attacks, as long as watermark is embedded into the most sensitive bit plane (LSB) of host media. We propose a novel method that may overcome this drawback as much as possible.

As stated in Chapter 4 optimization methods like Genetic Algorithm and Neural Network can be used to find the most optimum solution of a fixed problem. This searching a solution is analogious to searching a intended point in a dark space. Because of darkness, it is very challengeful to find the intended point randomly. An alternative method is to explore all the points consequently to reach that point (this point refers to the optimum point in a search space). There are search algorithms, that explores the whole space one by one: Brute Force search, linear programming, etc. This algorithms find the optimum solution exactly, but because of their computational cost, it becomes disadvantage in terms of consumed time. There available alternative algorithms that try to find the optimum point in the large search space either randomly or using historical informations in the previous states. Genetic Algorithm and Neural Network are the most widespread heuristics to reach optimum solution, where GA is inspired from genetics, and NN is inspired from neural structure of human brain.

In Chapter 5, some of the digital watermarking schemes, using either Genetic Algorithms or Neural Networks in embedding and extracting stages, are stated. It is obvious that in those studies, GA and NN were used to tune parameters according to

quality metrics of either extracted watermark or visual quality of watermarked data. PSNR and NCC values are conflicting metrics, where PSNR indicates the quality of watermarked (host signal + watermark) signal and NCC indicates the similarity between embedded and extracted watermarks. The lower Peak Signal Noise Ratio (PSNR) gives us more imporceptible watermarking scheme to Human Visual System. The higher Normalized Cross Correlation (NCC) value refers to robustness of watermarking algorithm, i.e. the embedded and extracted watermark are similar as much as possible ($0 \leq$ NCC value ≤ 1). As it is predictable, PSNR and NCC values are very crucial metrics in digital watermarking schemes.

6.2. Contributions

Contributions made in this study is listed below.

1. Achieve less computational cost – LSB watermarking. In other methods, transformed domain watermarking methods, there is computational cost due to transforming the signal from spatial domain into frequency domain. Computational costs are given in Equation 3.2.

2. Design robust and imperceptible watermarking scheme – higher PSNR value and higher NCC value. Compensation of these two performance metrics is achieved by using heuristic based search algorithm – Genetic Algorithm. It is nearly impossible to find the most optimum selection of these parameters by hands. GA provides to find the optimum parameters to be chosen while embedding. Parameter that is chosen by GA is bit plane number where to embed the watermark, rather than embedding it into Least Significant Bit (LSB). By running GA, one of the 6^{th},7^{th} or 8^{th} bit planes are selected for each frame of a video to embed the watermark in that bit plane.

3. Design Blind watermarking – using GA, this property is ensured. Because of stability of GA for a fixed search space, it becomes possible to re-find the bit planes where watermark was embedded in the extraction stage. Hereby, proposed digital video watermarking became blind digital watermarking. Blind watermarking's advantage is; no need to carry any additional data while extracting the embedded watermark from watermarked signal, which is crucial when proving ownership.

Here is a pseudo code of proposed digital video watermarking method: embedding

1. Take the video as an input
2. Parse the video into frames (still images)
3. Parse RGB frames into color channels; R-, G-, and B-channel. Select the channel which has the lowest intensity as a host data.
4. Run the Genetic Algorithm

   4.1. Randomly generate chromosomes: bit plane numbers: {6,7,8}

   4.2. Repeat {

      4.2.1. Implement GA operators: selectio, crossover, mutation.

      4.2.2. Evaluate PSNR and NCC values

      4.2.3. Evaluate fitness function for each frames of the video:

      $$f = \frac{1}{PSNR} + \frac{1}{NCC}$$

      4.2.4. Make selection among individuals according to fitness function

   } Until [end of iteration indicated by user, or do early stopping]
5. Take the optimum set of generation from GA output
6. Embed the watermark into optimum bit-planes of video frames.
7. Reconstruct a video from frames by concatenating all channels; [R; G; B] (watermarked channel and other two channels).

Genetic Algorithm parameters used in this work are given in Table 6.1

Table 6.1. GA parameters used in this study.

Number of Iterations	30
Tournament Range	5
Crossover Ratio	0.9
Mutation Ratio	0.05
Population Size	10 * N (number of frames in the video)

Here is a pseudo code of proposed digital video watermarking method: extraction

1. Take the watermarked video
2. Parse the video into frames (still images)
3. Parse RGB video frames into individual color channels. Select the channeş which has the lowest intensity. This channel is selected, because it is known that watermark was embedded into lowest instenisty color channel of the frame.
4. Run the Genetic Algorithm
   4.1. Randomly generate chromosomes: bit plane numbers: {6,7,8}
   4.2. Repeat {
      4.2.1. Implement GA operators: selectio, crossover, mutation.
      4.2.2. Evaluate PSNR and NCC values
      4.2.3. Evaluate fitness function for each frames of the video:

$$f = \frac{1}{PSNR} + \frac{1}{NCC}$$

      4.2.4. Make selection among individuals according to fitness function
   } Until [end of iteration indicated by user, or do early stopping]
5. Take the optimum set of generation from GA output
6. Extract the watermarks from bit-planes that were found in GA.
7. Now, it is possible to proof ownership, or data authentication.

6.3. Experimental Results.

In experimental work, blind, robust and imperceptible watermarking scheme is implemented. Experimental results are shown below in tables.

- Watermarks used in experiments are shown in Figure 6.1.

(a) Gaziantep University Logo

(b) Zeugma

Figure 6.1 Watermarks used in experiments

- In experiments three videos were used that are taken from source files of MATLAB:

Video 1: handshake.avi

Video 2: ShakyCar.avi

Video 3: Shuttle.avi

Video 4: xylophone.mpg

- Applied noises and filtering attacks:
    1. Median filtering [3,3],
    2. Median filtering [5,5],
    3. Averaging Filter (hsize=3),
    4. Gaussian LowPass Filtering (hsize=3,sigma=0.5),
    5. Gaussian LowPass Filtering (hsize=3,sigma=0.1),
    6. Gaussian LowPass Filtering (hsize=5,sigma=0.5),
    7. Circular Averaging Filter (r=3),
    8. Salt and Pepper Noise,

Different filters and noises applied into watermarked video frames and measured the PSNR and NCC values which indicate the imperceptibility and robustness of the proposed method, respectively.

PSNR and NCC values of attacked videos are given in Table 6.2.

In Figure 6.2, Watermarked Frames, Attacked Frames and Extracted Watermarks, Gaziantep University Logo and Zeugma, for each Bit Plane are shown after Median Filtering [5,5] in Video # 3. 8^{th} Bit plane Watermarking is equivalent with standart LSB Watermarking. Extracted watermarks differ from each other in terms of visual quality such that extracted watermark from 6th Bit plane watermarking is visually better than 7^{th} and 8^{th} bit plane watermarking. But there is a trade-off between visual

quality of extracted watermark and visual quality of watermarked frame. It is clear that in 6th bit plane watermarking visual quality of watermarked frame is not good enough. In this case the most optimum bit plane to embed the watermark from both quality metrics is 7th bit plane watermarking; so that both watermarked frame and extracted watermarks are visually better than others(6th and 8th bit plane watermarking).

Table 6.2 Average of PSNR values of watermarked frames &

Average of NCC values of extracted watermark and original watermark

(Watermark1 – Gaziantep University Logo)

		Video # 1	Video # 2	Video # 3	Video # 4
Median Filtering [3,3]	Average PSNR (dB)	45.16	26.81	44.78	46.23
	Average NCC	0.95	0.92	0.95	0.90
Median Filtering [5,5]	Average PSNR (dB)	40.00	26.09	26.07	44.60
	Average NCC	0.91	0.83	0.92	0.80
Averaging Filter (hsize=3)	Average PSNR (dB)	26.61	32.90	26.07	51.14
	Average NCC	0.30	0.20	0.44	0.19
Gaussian LowPass Filtering (hsize=3,sigma=0.5)	Average PSNR (dB)	26.09	26.09	45.40	26.09
	Average NCC	0.65	0.56	0.81	0.57
Gaussian LowPass Filtering (hsize=3,sigma=0.1)	Average PSNR (dB)	51.13	51.14	51.14	51.14
	Average NCC	1.00	1.00	1.00	1.00

Gaussian LowPass Filtering (hsize=5,sigma=0.5)	Average PSNR (dB)	26.09	26.09	45.60	26.09
	Average NCC	0.65	0.55	0.81	0.57
Circular averaging filter (r=3)	Average PSNR (dB)	26.61	26.09	26.07	26.09
	Average NCC	0.30	0.16	0.35	0.07
Salt and Pepper Noise	Average PSNR (dB)	51.05	50.59	50.47	50.15
	Average NCC	0.94	0.95	0.94	0.94

(Watermark2 - Zeugma).

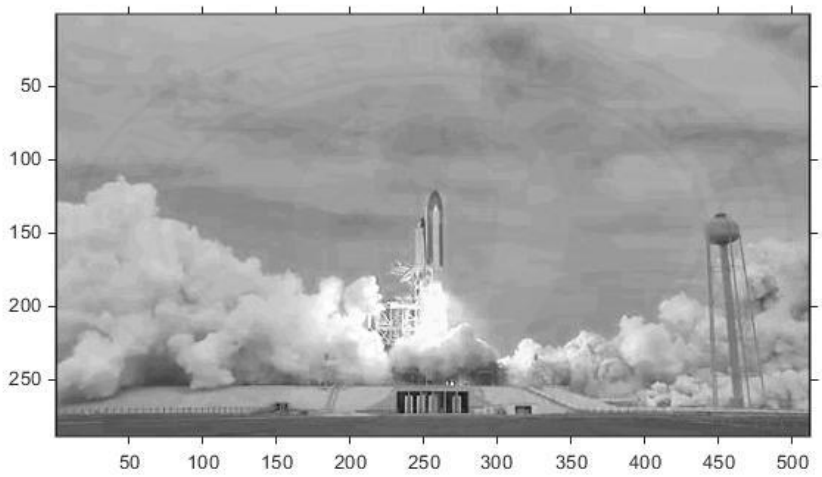
		Video # 1	Video # 2	Video # 3	Video # 4
Median Filtering [3,3]	Average PSNR (dB)	32.39	40.10	44.03	50.65
	Average NCC	0.82	0.82	0.84	0.82
Median Filtering [5,5]	Average PSNR (dB)	27.33	26.33	27.21	49.33
	Average NCC	0.76	0.75	0.77	0.74
Averaging Filter (hsize=3)	Average PSNR (dB)	26.15	34.45	25.90	51.16
	Average NCC	0.31	0.19	0.40	0.18
	Average PSNR (dB)	26.15	26.10	46.97	25.87

Gaussian LowPass Filtering (hsize=3,sigma=0.5)	Average NCC	0.67	0.57	0.81	0.58
Gaussian LowPass Filtering (hsize=3,sigma=0.1)	Average PSNR (dB)	51.09	51.14	51.17	51.16
	Average NCC	1.00	1.00	1.00	1.00
Gaussian LowPass Filtering (hsize=5,sigma=0.5)	Average PSNR (dB)	26.15	26.10	46.69	26.13
	Average NCC	0.67	0.57	0.80	0.59
Circular averaging filter (r=3)	Average PSNR (dB)	26.15	25.70	26.12	26.13
	Average NCC	0.26	0.15	0.31	0.07
Salt and Pepper Noise	Average PSNR (dB)	51.05	50.73	51.12	50.98
	Average NCC	0.95	0.95	0.95	0.95

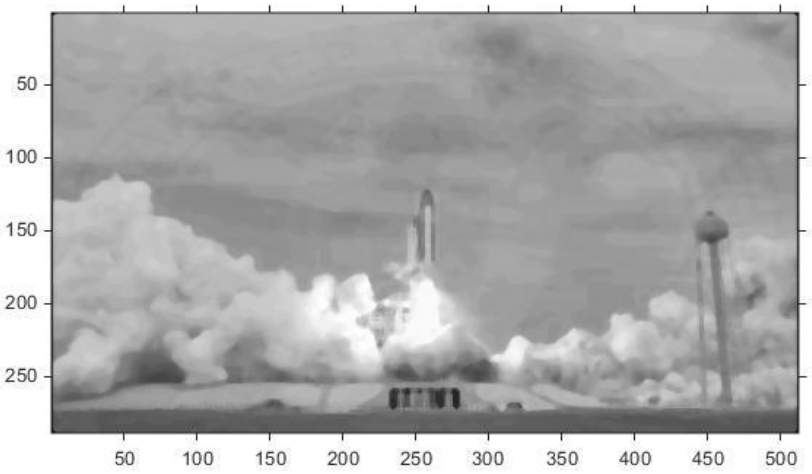
Using above mentioned parameters of GA, blind digital video watermarking is implemented. GA has to find the same bit plane numbers for watermarking scheme being blind. Accuracies of GA of finding the true bit planes, which were taken from ground truth data, by varying the iteration numbers are given in Table 6.3. Numbers in the paranthesis in the first column indicates the total number of frames of video. Numbers in the second, third, fourth and fifth columns indicates the number of frames that GA found the true bit plane to embed the watermarked using ground truth datas. Values in the paranthesis indicate the accuracy of GA to find the same bit plane numbers with respect to iteration numbers.

Table 6.3 Performance of GA according to iteration numbers; N=Number_Of_Frames.

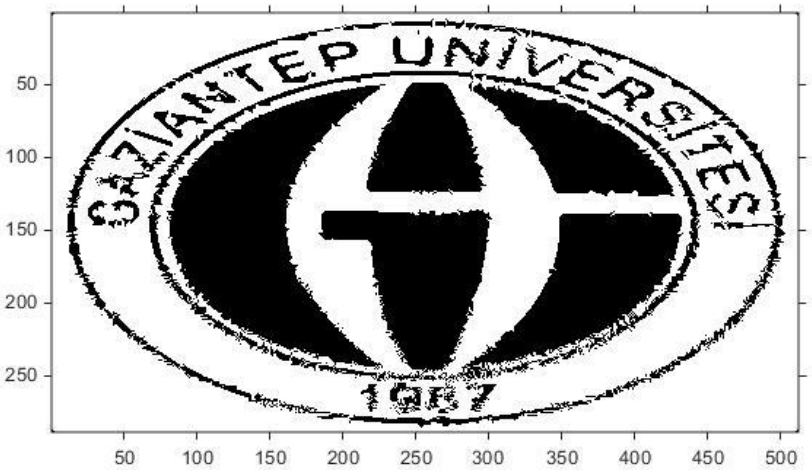
Iteration Numbers	10	30	N/2	N
	Performances of Genetic Algorithm			
Video # 1 **(145)**	92 (63.45%)	131 (90.34%)	**145 (100%)**	**145 (100%)**
Video # 2 **(132)**	87 (65.91%)	120 (90.91 %)	**132 (100%)**	**132 (100%)**
Video # 3 **(121)**	82 (67.77%)	107 (88.43%)	**120 (99.17%)**	**121 (100%)**
Video # 4 **(100)**	73 (73%)	94 (94%)	**98 (98%)**	**100 (100%)**



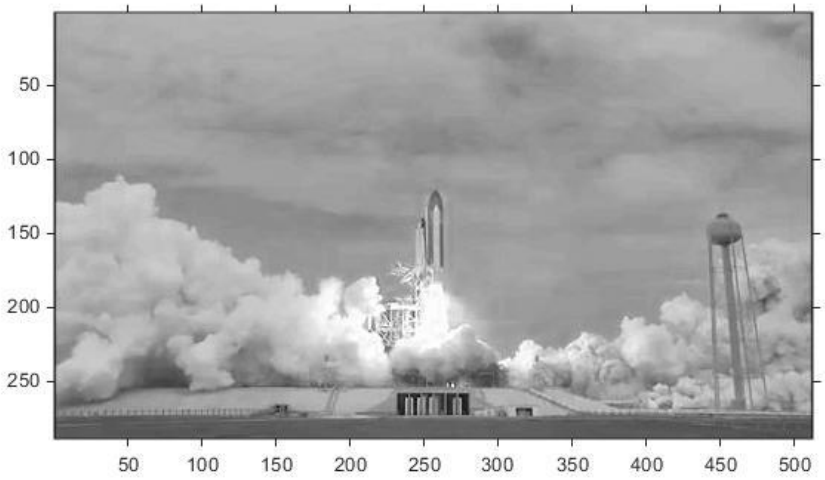
(a) Watermarked Frame (6th Bit plane)



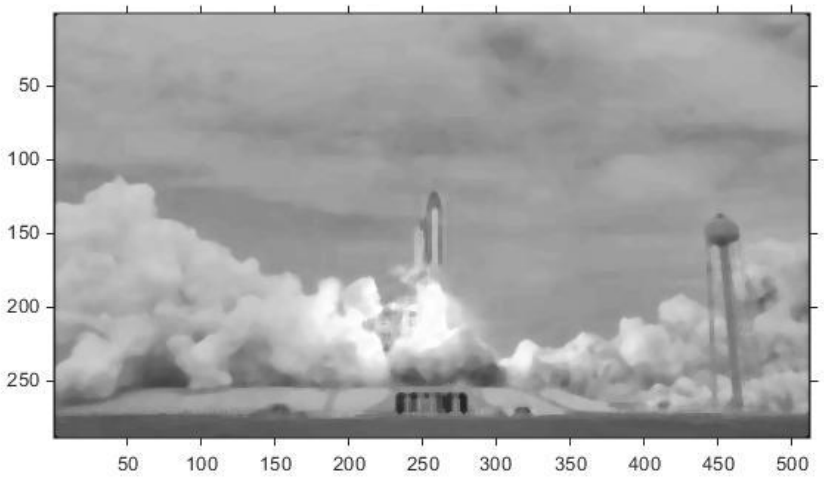
(b) Attacked Frame (6th Bit plane)



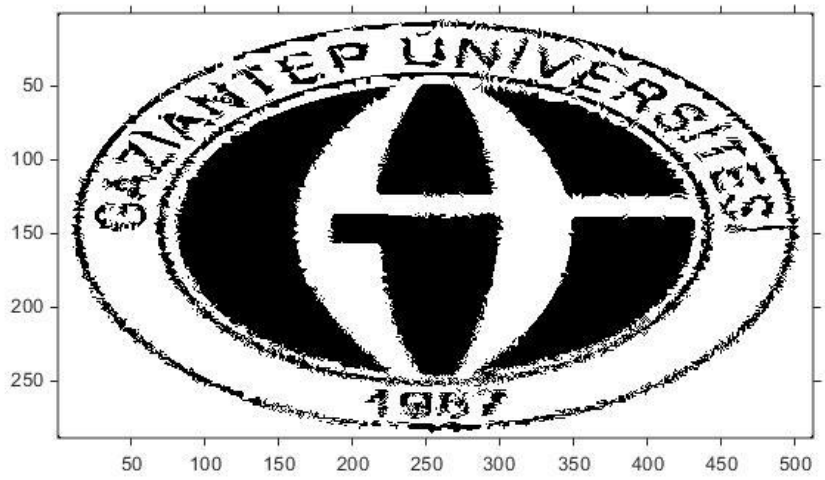
(c) Extracted Watermark (6th Bit plane)



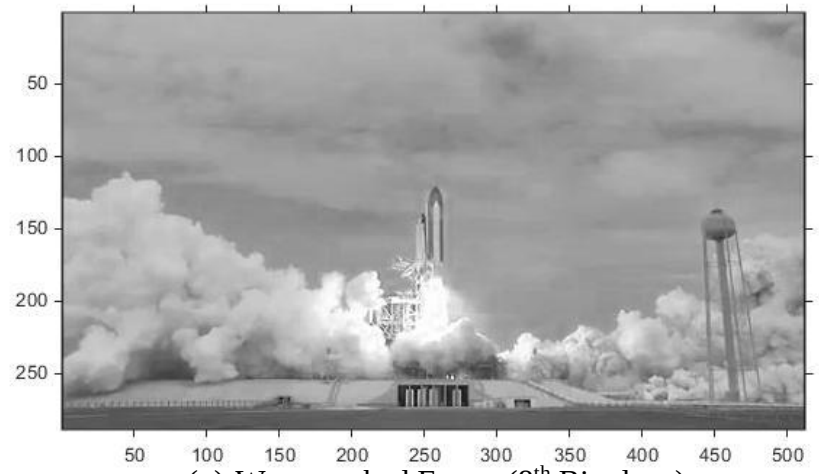
(d) Watermarked Frame (7th Bit plane)



(e) Attacked Frame (7th Bit plane)

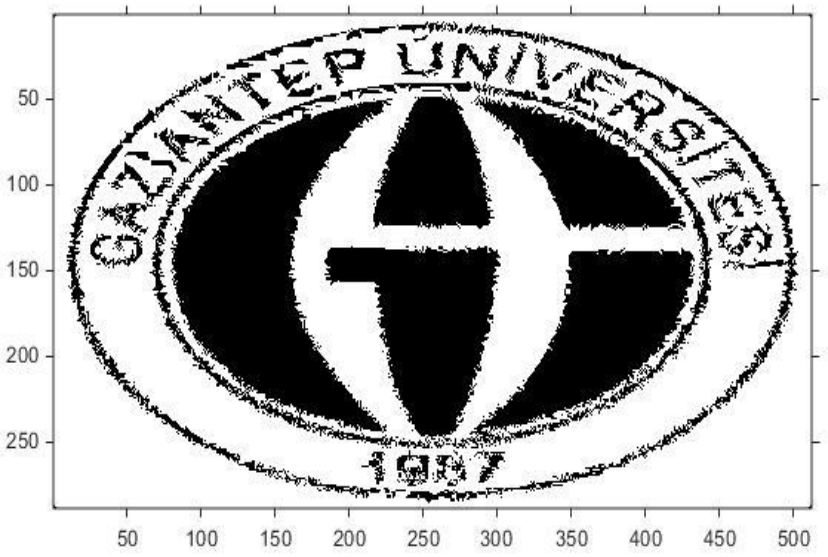


(f) Extracted Watermark (7th Bit plane)



(g) Watermarked Frame (8th Bit plane)

(h) Attacked Frame (8th Bit plane)



(i) Extracted Watermark (8th Bit plane)

Figure 6.2. Watermarked Frames, Attacked Frames and Extracted Watermarks for each Bit Plane Watermarking.

6.4. Comparison

In this subsection, we make comparisons between proposed watermarked scheme and standart LSB watermarking scheme. Our contribution was to implement more robust watermarking scheme against attacks, while keeping the straightforward implementing advantage. In Figure 6.3, it is shown that visual quality of extracted watermark using proposed watermarking scheme is better than that extracted watermark using standart LSB watermarking. Besides, there is no visual difference between watermarked frames of proposed and LSB watermarking schemes. This refers that there is no significant, almost any, visual quality difference between those of two watermarking schemes. But it is obvious that NCC values of extracted watermarks are quite different, this refers to quality of extracted watermark using proposed watermarking is better in terms of quality than those watermark that was extracted using LSB watermarking. This improvement was provided by selecting the most optimum bit plane in order to embed the watermark inside intelligently. Genetic Algorithm provides us to select the most optimum bit in terms of fitness function, that contains quality of both watermarked frame and extracted watermark. To overcome invisibility issue is provided by embedding the binary watermark into one of channels of RGB video. Channels were selected according to channel intensity. Watermark was embedded into the channel that has the lowest intensity among the frame. In Table 6.4, NCC values are given for the following configuration:

- Video # 1,
- Watermark = “Zeugma.jpg”
- Attack = Gaussian Low Pass Filter (hsize=3, sigma=0.5)

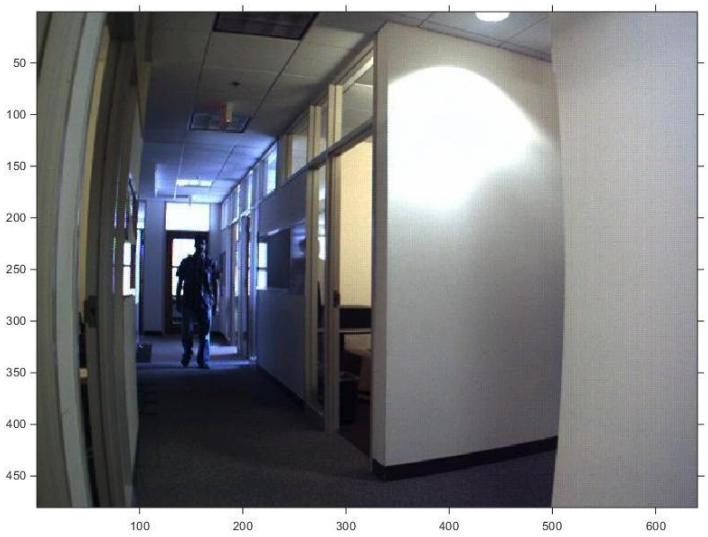
NCC values are “1” for both Watermarking schemes when there is no any noise as expected.

Table 6.4 Comparison between standard LSB watermarking and Proposed LSB Watermarking.

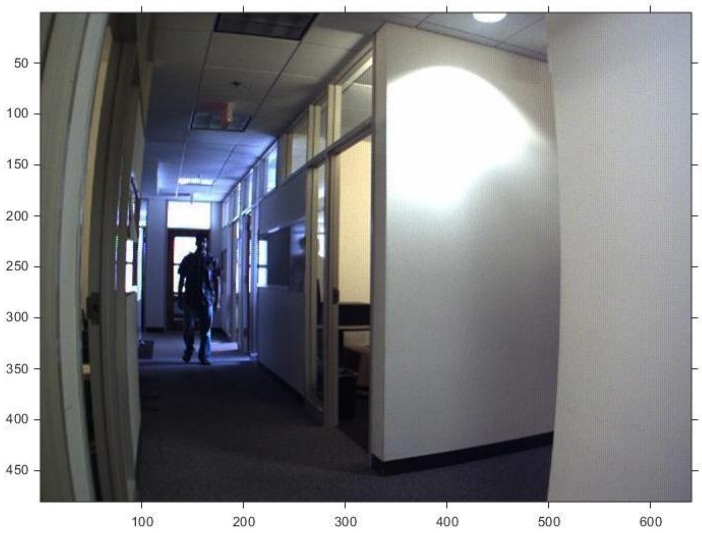
		LSB Watermarking	**Proposed Watermarking**
NCC	Gaussian LPF (hsize=3, sigma=0.5)	0.5826	0.67
	Median [5,5]	0.7438	0.7609
	Without Noise	1.00	1.00

(a) Watermarked Frame without noise (Proposed Watermarking)

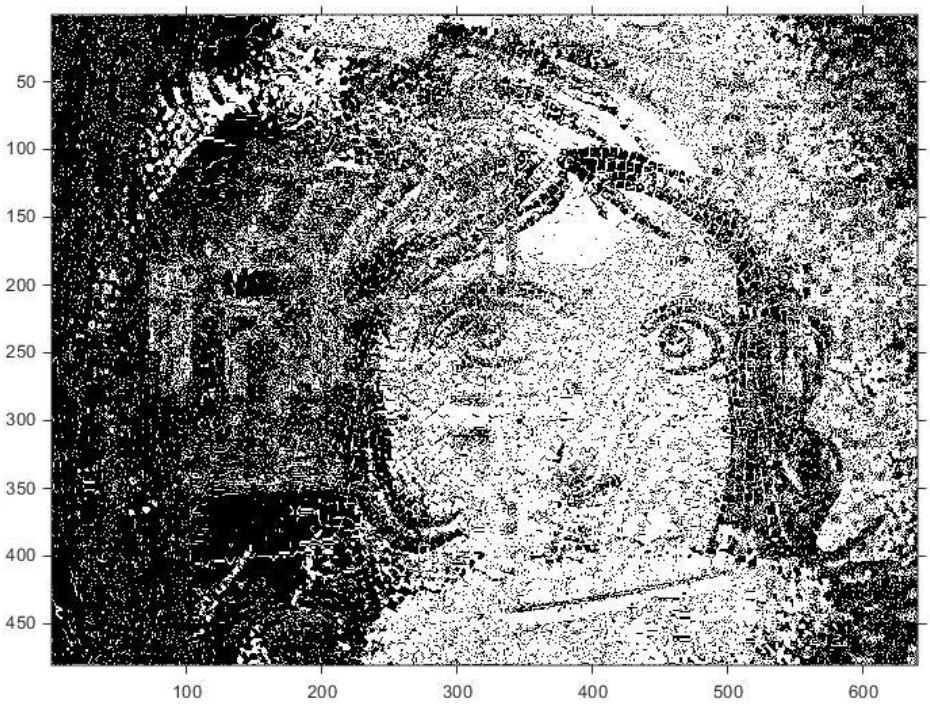
(b) Watermarked Frame without noise (LSB Watermarking)



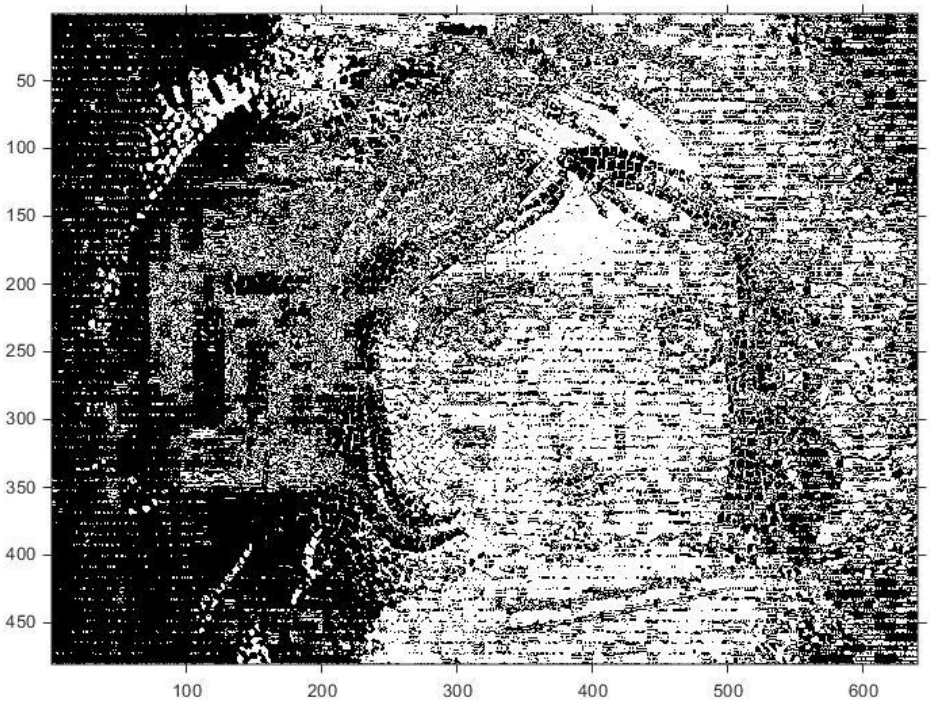
(c) Watermarked Frame with noise, Gaussian Filter. (Proposed Watermarking)



(d) Watermarked Frame with noise, Gaussian Filter. (LSB Watermarking)



(e) Extracted Watermark (Proposed Watermarking)



(f) Extracted Watermark (LSB Watermarking)

Figure 6.3 Comparison between standart LSB Watermarking and Proposed Watermarking Schemes, and resultant figures.

6.5. Exploiting Audio Attribute of the Video

Since videos are consist of not only visual frames, it also includes audio attribute. This attribute can be exploited when implementing a digital video watermarking. You will appreciate that, when we hear a loud sounds, we can not pay attention to the visual objects around us. For example, the most traffic accidents occur because of listening a music loudly. This was the inspiration for us to exploit the audio attribute of the video when embedding a watermark into the video. This was done in this manner;

- first, audio signal of the video was read from the video file,
- secondly, signals corresponding to a fixed frame that have highest amplitude were determined,
- then, earlier decided bit planes (output of Genetic Algorithm) were changed to previous bit planes (8th bit plane changed to 7th bit plane, etc) that corresponds to the frames that have high amplitude audio signal and assigned new set of bit planes.
- Watermark was embedded into the newly assigned bit planes rather than the set of old bit planes, output of the Genetic Algorithm.

NCC values of these two different set of bit planes are given below in Table 6.5. In Figure 6.4, audio signal of the Video # 4 is shown in time domain. Video # 4 was used in the following results (Because it has an audio signal in the video).

Table 6.5 NCC values of two approaches;

Bit planes decided by GA, and Bit Planes selected by additional decision using amplitudes of an audio attribute of the video.

		First set of Bit Planes	**Second set of Bit Planes**
NCC	Gaussian LPF (hsize=3, sigma=0.5)	0.58	0.60
	Median [5,5]	0.74	0.7498
	Without Noise	1.00	1.00

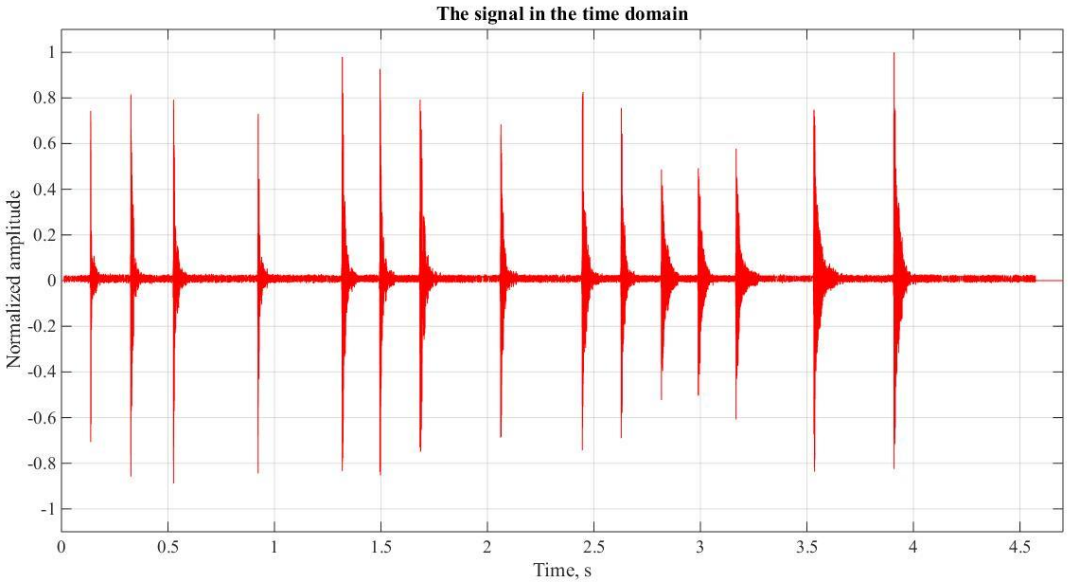


Figure 6.4 The audio signal of the Video # 4 in the time domain.

6.6. Discussion

Experiments suggest that usage of GA ensure the design of blind LSB watermarking. And it is obvious from experimental results that small number of iterations may be enough to find the optimum bit plane number, but these iteration numbers can vary according to number of frames in the video.

This thesis states that the most straightforward digital watermarking method LSB may be preferrable to embed the watermark into digital videos. The main disadvantage of LSB watermarking was its weakness against filtering attacks and noises. Reason of this weakness is; the watermark is embedded into the most sensitive bit plane, actually it provides maximum imperceptibility. But sometimes, embedding the watermark into the second least significant bit, 7^{th} bit plane, may provide full imperceptibility, while being more robust to attacks and noises compared to embedding the watermark into LSB. From this point of view, a new approach for Digital Video Watermarking is proposed, that embeds the watermark into 6^{th}, 7^{th} or 8^{th} bit by looking to its sufficient imperceptibility and providing high robustness. At this point, GA is used to make decisions, where to embed the watermark to achieve higher robustness while preserving the imperceptibility of watermarked video.

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1. Conclusion

In the Master Degree duration, I have learn how to perform inividual research by exploring the proposed papers and conference reports. By reading papers, it maked sense that watermarking schemes can be designed by optimization methods while there are some trade-offs between watermarking parameters. Then, started to research the optimizatiom methods like Genetic Algorithm and Neural Networks.

Genetic Algorithm is very nice option to search an optimum point in a large search space, if there are constraints in time to perform brute-force search. GA acts randomly, but it is also based on historical informations, and tries to find the optimum solution to a specific task.

On the other hand, Neural Network is also one of optimization method, that learns the nature of the search space, and tries to predict the optimum solution to the problem. NN learns the weights (connections between neurons among layers) from the ground truth data.

Selection between these two optimization methods can be done according to number of features of the task. In this thesis, we used two performance metrics, PSNR and NCC metrics, and results show that usage of GA is more suitable than the usage of NN.

7.2. Future Work

Nowadays, NN much more developed, and became useful in artificial intelligence and machine learning problems. One of the successful application area of NN is scene understanding, and interpretation of the scene such what does exist in the image, and extracting semantic content of the image. In this kind of applications Recurrent Neural

Networks and Convolutional Neural Network are used. Convolutional Neural Network are used widely in the area of image and video recognition, and natural language processing. Recurrent Neural Networks is used at handwriting recognition or speech recognition.

In the future, I am planning to learn these RNNs and CNNs, and implement some projects about these NN.

In the last month, Google released a framework on Neural Network named TensorFlow. TensorFlow is the Open Source Software Library for Machine Intelligence. Thousands of Google Engineers have been working on this framework, and released the TensorFlow in December, 2015.

I am going to investigate the tutorials and implement the projects in the TensorFlow. I am believe that next decades will be Artificial Intelligence revolution. So, I am wanting to follow up the new releases in this area.

REFERENCES

[1] K.Sathisyasekar, S.Karthick Swathy Krishna K S. (2014). A Research Review On Different Data Hiding Techniques, *International Journal Of Engineering And Computer Science ISSN:2319-7242,* **3**, 3655–3659.

[2] Ramandip singh, Sukhmeet kaur. (2015). Review Paper On Various Data Hiding Techniques, *International Journal of Engineering And Computer Science ISSN:2319-7242*, **4**, 13760–13764.

[3] Richa Gupta, Sunny Gupta, Anuradha Singhal. (2014). Importance and Techniques Of Information Hiding: A Review, *International Journal Of Computer Trends And Technology (IJCTT),* **9**, 260–265.

[4] Gopika V Mane, G.G. Chiddarwar. (2013). Review Paper on Video Watermarking Techniques, *International Journal of Scientific and Research Publications,* **3**, 1–5.

[5] Mohan Durvey, Devshri Satyarthi. (2014). A Review Paper on Digital Watermarking, *International Journal of Emerging Trends and Technology in Computer Science (IJETTCS),* **3**, 99–105.

[6] Vinita Gupta, Mr. Atul Barve. (2014). A Review on Image Watermarking and Its Techiques, *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE),* **4**, 91–97.

[7] Alka N. Potkar, Saniya M. Ansari. (2014). Review on Digital Video Watermarking Techniques, *International Journal of Computer Applications (IJCA),* **106**, 7–12.

[8] Józef Lubacz, Wojciech Mazurczyk, and Krzystof Szczypiorski. (2014). Principles and Overview Network Steganography, *IEEE Communication Magazine*, 225–229.

[9] Jasleen Kour, Deepankar Verma. (2014). Steganography Techniques – A Review Paper, *International Journal of Emerging Research in Management & Technology,* **3**, 132–135.

[10] Lisa M. Marvel, Charles G. Boncelet and Charles T.Retter. (1999). Spread Spectrum Image Steganography, *IEEE Transactions on Image Processing*, **8**, 1075–1083.

[11] Nitin Jirwan, Ajay Singh, Sandip Vijay. (2013). Review and Analysis of Cryptography Techniques, *International Journal of Scientific & Engineering Research,* **4**, 1–6.

[12] Y. Yalman, Ö. Çetin, İ. Ertürk, F. Akar. (2014). Veri Gizleme, *Beta Yayıncılık,* ISBN: 978-605-33-3063-9.

[13] Gustavus J. Simmons. (1984). The Prisoners' Problem and Subliminal Channel, *Advances in Cryptology,* 51–67.

[14] Niels Provos, Peter Honeyman. (2003). Hide and Seek: An Introduction to Steganography, *IEEE Computer Society,* 32 – 44.

[15] Schyndel R.G., Tirkel A., Osborne C.F. (1994). A Digital Watermark, *IEEE International Conference on Image Processing, ICIP*, 86 – 90.

[16] Prabhishek S., Chadha R.S. (2013). A Survey of Digital Watermarking Techniques, Applications and Attacks, *International Journal of Engineering and Innovative Technology, IJEIT,* 165 – 175.

[17] Lalit K.S., Vishal Sh. (2014). Survey of Digital Watermarking Techniques and its Applications, *International Journal of Computer Science Trends and Technology, IJCST,* 70 – 73.

[18] Khalid M., Sekharjit D., James F. (2005). Frequency Domain Watermarking: An Overview, *The International Arab Journal of Information Technology,* 33 – 47.

[19] Bhupendra R. (2013). Digital Image Watermarking Technique Using Discrete Wavelet Transform and Discrete Cosine Transform, *International Journal of Advancements in Research & Technology,* 19 – 27.

[20] Zunera J., Anwar M.M. (2009). A Review Of Digital Watermarking Techniques for Text Documents, *International Conference on Information and Multimedia Technology,* 230 – 234.

[21] Manjit T., Dr. Sandeep K.S., Meenakshi Sh. (2011). Digital Image Watermarking Technique Based on Different Attacks, *International Journal of Advanced Computer Science and Applictions, IJACSA*, 14 – 19.

[22] Preeti P., Rajeev K.S. (2014). A Survey: Digital Image Watermarking Techniques, *International Journal of Signal Processing and Pattern Recognition*, 111 – 124.

[23] Mehran A., Damon M.Ch. (2015). Digital Image Watermarking via Adaptive Logo Texturization, *IEEE Transactions on Image Processing, Vol.24,* 5060 – 5073.

[24] Maneli N., Russell M.M. (2005). Compressed-Domain Video Watermarking for H.264, *Center for Signal and Image Processing , Georgia Institute of Technology*, 1 – 4.

[25] Mauro B., Franco B., Nicola Ch. (2005). Watermarking of MPEG-4 Video Objects, *IEEE Transactions on Multimedia*, 23 – 32.

[26] Kazuto O., Go O. (2015). Watermarking for HEVC/H.265 Stream, *IEEE International Conference on Consumer Electronics*, 102 – 103.

[27] Deepa S.K., Jadhav M.M., Mahesh Kh. (2011). A Robust Watermarking Approach for raw video and it's DSP Implementation, *International Journal of Advanced Engineering Research and Studies*, 198 – 208.

[28] Komal V.G., Pallavi K.P. (2012). Overview of Audio Watermarking Techniques, *International Journal of Emerging Technology and Advanced Engineering*, 67 – 70.

[29] Jieh-Min Sh., Der-Chyuan L., Ming-Chang Ch. (2005). A semi-blind digital watermarking scheme based singular value decomposition, *Computer Standars & Interfaces*, Volume: 28, 428 – 440.

[30] Nasir I., Khelifi F., Jiang J., Ipson S. (2011). Robust Image wtermarking via geometrically invariant feature points and image normalisation, *IET Image Processing*, Volume:6, 354 – 363.

[31] Yong D. Ch., Chung H.K. (2003). Robust Image Watermarking Against Filtering Attacks, *SICE Annual Conference in Fukui*, 3017 – 3020.

[32] Ramos C.C., Reyes-Reyes R., Nakono-Miyakate M., Peres-Meana H. (2010),. A Blind Video Watermarking Scheme Robust to Frame Attacks Combined with MPEG2 Compression, *Journal of Applied Research and Technology*, 323 – 339.

[33] Ingemar J. C., Jeffrey A. B., Jessica F., Ton K. (2008). Digital Watermarking and Steganography, *Morgan Kaufmann Publishers*.

[34] M. Bahadır Ç. (2004). Design of Digital filters with Minimum Phase and Optimum Magnitude Response by Using Genetic Algorithm, Master-Degree Thesis.

[35] Mitchel M. (1999). An Introduction to Genetic Algorithms, *A Bradford Book The MIT Press*.

[36] Winter G. (1995) . Genetic Algorithms in Engineering and Computer Science.

[37] Christopher R.S., Marc T., Darrell W., Peter F.S. (2007). Foundations of Genetic Algorithms , *9th International Workshop.*

[38] McCulloch W.S., Walter P. (1943). A logical calculus of the ideas immanent in nervous activity, *The bulletin of mathematical biophysics*, 115 – 133 .

[39] Hopfield J.J. (1982). Neural Networks and physical systems with emergent collective computational abilities, *Proc. Natl. Acad. Sci, USA*, volume:79, 2554 – 2558.

[40] Ramanjaneyulu K., Rajarajeswari K. (2010). An oblivious and robust multiple image watermarking scheme using Genetic Algorithm, *The International Journal of Multimedia & its Applications*, Volume:2, 19 – 38.

[41] Yang G., Sun X., Wang X. (2006). A Genetic Algorithm based Video Watermarking in the DWT domain, *IEEE*, 1209 – 1212.

[42] Giulia B., Valentina C., Francesco G.B., Claudio F. (2009). Watermarking Robustness Evaluation Based on Perceptual Quality via Genetic Algorithms, *IEEE Transactions on Information Forensics and Security*, Volume:4, 207 – 216 .

[43] Bushra S., Muhammad I., Arfan J.M., Muhammad T., Anwar.M.M. (2010). Adaptive digital watermarking of images using Genetic Algorithm, *IEEE,* 1 – 8.

[44] Bibi I., Santhi V. (2011). A Study on Image and Video Watermarking Schemes using Neural Netwroks, *International Journal of Computer Applications,* Volume:12, 1 – 6.

[45] Pao-Ta Y., Hung-Hsu T., Jyh-Shyan L. (2001). Digital watermarking based on neural networks for color images, *Signal processing,* 663 – 671.

[46] Nallagarla R., Varadarajan S. (2012). The Robust Digital Image Watermarking Scheme with Back Propagation Neural Network in DWT domain, *International Conference on Modelling Optimization and Computing,* 3769 – 3778.

[47] Maher E., Chokri B.A. (2013). Image authentication algorithm with recovery capabilities based on neural networks in the DCT domain, *IET Image Processing,* Volume:8, 619 – 626.

[48] Abdulkhaev A., Kayhan S.K. (2015). A New Approach for Video Watermarking Using Genetic Algorithm, *Elektrik Elektronik Mühendisliği Kongresi.*

[49] Christopher M.B. (2006). Pattern Recognition and Machine Learning, *Springer.*