Verilog Implementation of Digital Image Watermarking

Project Report submitted in partial fulfillment of the requirements for the degree of

MASTERS of TECHNOLOGY (M. Tech.)

In

VLSI AND EMBEDDED SYSTEMS

Submitted by:

Satyan (2K15/vls/15)

Under the guidance of

Dr. S.INDU

H.O.D, Dept. of Electronics & Communications, DTU, Delhi

Department of Electronics & Communication Engineering

Delhi Technological University

(Formerly Delhi College of Engineering)

Delhi – 110042

(Session: 20015-2017)

CERTIFICATE

This is to certify that the report titled **“Verilog Implementation of Digital Image Watermarking”** is a bonafide record of Major-2 submitted by **Satyan(Roll no: 2K15/VLS/15)** as the record of the work carried out by him under my guidance. The said work has not been submitted anywhere else for the award of any other degree or diploma.

Dr. S.INDU
H.O.D. (ECE DEPTT.)
DELHI TECHNOLOGICAL UNIVERSITY

CANDIDATE'S DECLARATION

This is to certify that dissertation entitled **"Verilog Implementation of Digital Image Watermarking"** which is submitted by me in partial fulfilment of the requirement for the award of M.Tech degree in **VLSI and EMBEDDED SYSTEMS** from Delhi Technological University, Delhi, INDIA comprises only my own work and due acknowledgement has been made to all other material used.

I hereby, further declared that in case of legal dispute in relation to my M.Tech. dissertation, I will be solely responsible for the same.

Date

Satyan

Roll. No. 2K15/VLS/15

M. Tech. (VLSI)

ACKNOWLEDGEMENT

I express my deepest gratitude to my project guide DR. S.Indu (Head of Department), Department of Electronics and Communication Engineering, Delhi Technological University whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject. Her suggestions and ways of summarizing the things made me to go for independent studying and trying my best to get the maximum in my topic, this made my circle of knowledge very vast. I am highly thankful to her for guiding me in this project.

Finally, I take this opportunity to extend my deep appreciation to my family and friends, for all that they meant to me during the crucial times of the completion of my project.

Date-

Satyan

Roll No. 2K15/VLS/15

M. Tech. (VLSI)

List of Abbreviations

1D	One dimensional
2D	Two dimensional
dB	Decibel
DCT	Discrete Cosine Transform
2D-DCT	Two dimensional Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
IDWT	Inverse Discrete Wavelet Transform
LDWT	Lifting based Discrete Wavelet Transform
ECC	Error correction code
FFT	Fast Fourier Transform
FHT	Fast Hadamard Transform
FPGA	Field Programmable Gate Array
HDL	Hardware Descriptive Language
HVS	Human visual system
IDCT	Inverse Discrete Cosine Transform
IPP	Intra pixel prediction
ISO	International Organization for Standardization
JPEG	Joint photographic expert group
LSB	Least significant bit 3
MPEG	Moving picture expert group
MSE	Mean square error
PRN	pseudo-random number
PSNR	Peak signal to noise ratio
RGB	Red Green Blue
SSIM	Structural similarity index measurement
WHT	Walsh Hadamard Transform

Table of Contents

LIST OF FIGURES

ABSTRACT

The development of computer technology has brought about growth in the use of digital multimedia contents related to electronic commerce and services provided through internet. As digital media is easily regenerated and manipulated, so everyone is potentially at risk or incurring considerable financial loss. Also people are motivated to embed data or information such as owner information, company logo, date, time, brand name and even hide a secret message in the digital images to communicate secretly. Digital watermarking can prevent such a loss by providing authentication and copyright protection and plays an important role in security of important data or the content of digital media. The digital images are easily exchanged through internet and threaten to various malicious attacks so they must be protected based on copyright. Here the project represent an efficient hardware implementation of digital Watermarking which features low power consumption, simple implementation, increased processing speed, reliability and invisible image watermarking. Proposed concept would be implemented using Verilog and synthesize Into FPGA.

CHAPTER-1.

INTRODUCTION

1.1. Introduction:

People are communicating secretly for many years by using data or information hiding techniques. Information hiding techniques has already plays an important role in number of application areas.

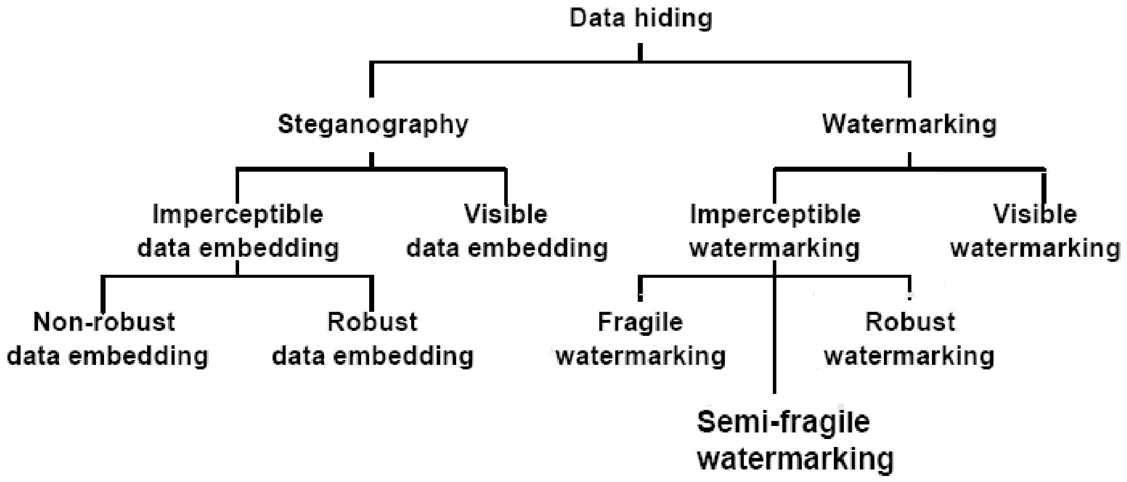


Figure 1.1 Evolution of data hiding techniques.

1.2. Steganography

Steganography is simply an art of covered or hidden writing to hide the existence of a message from an unauthorized party or for secret communication.

The main goal of steganography is to hide a message or some useful information in an audio, video, image and text(cover) data , to obtain new data which is practically indistinguishable from an original cover data in such a way that an unauthorized party cannot detect the presence of hidden information

1.3. Digital Watermarking

A digital watermark is a piece of information which may be pattern of bits, image, text file, video or other multimedia (cover) file to identify the copyright information of that file.

Watermarking is the process of embedding a watermark such as copyright information, secret message, data cover etc. Today we can easily hide information or secret messages within digital multimedia such as documents, images, audio and video etc. So, in general watermarking means hiding some useful information into multimedia content, such as an audio, video or images in such a way that it is non-perceptible when observing by humans, but it is easily detected and extracted by the owner with the help of computer or detector.
A Simple watermarking system generally consists of typical watermark embedding module and a detector that detects the watermark. The watermark embedded module inserts a pattern of bits or a piece of information within original cover image with unique watermark key.

The watermark key should be present during the process of embedding an information or data into host image with the help of which watermark can be detected and extracted from watermarked media. The watermark key basically has a one-to-one correspondence with watermark contents. The watermark key kept secret to prevent its unauthorized access and only known by authorized people which ensures that only authorized people can detect and extract the watermark to obtain the watermark and original image. Also we know that the communication channels can be noisy and very much prone to security attacks. Therefore the watermarking should be robust so that it resists both noise and security attacks.

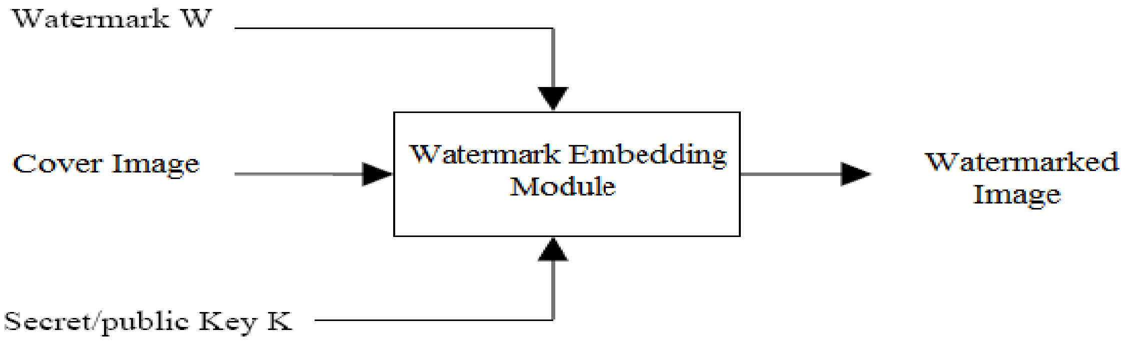


Figure.1.2 Block diagram of simple watermarking.

1.4 Properties of Digital Watermarking techniques

The given digital watermarking scheme should satisfy the following properties:

- The watermark must be invisible.
- Information or data (watermark) must not affect the quality of the cover image, audio or video etc.
- Information or data (watermark) must be easily detected and extracted.
- The watermarking technique must be robust, fragile or semi fragile.
- It must be strong enough to resist noise and standard manipulations.
- There must be no loss of any information and also compatible with the host.

1.5 TYPES OF WATERMARK

1.5.1. On the basis of human perception watermarking is divided into two parts as shown in fig.

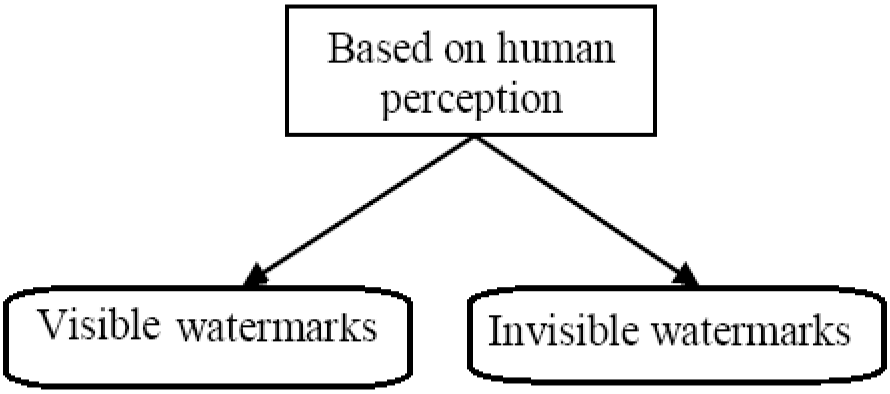
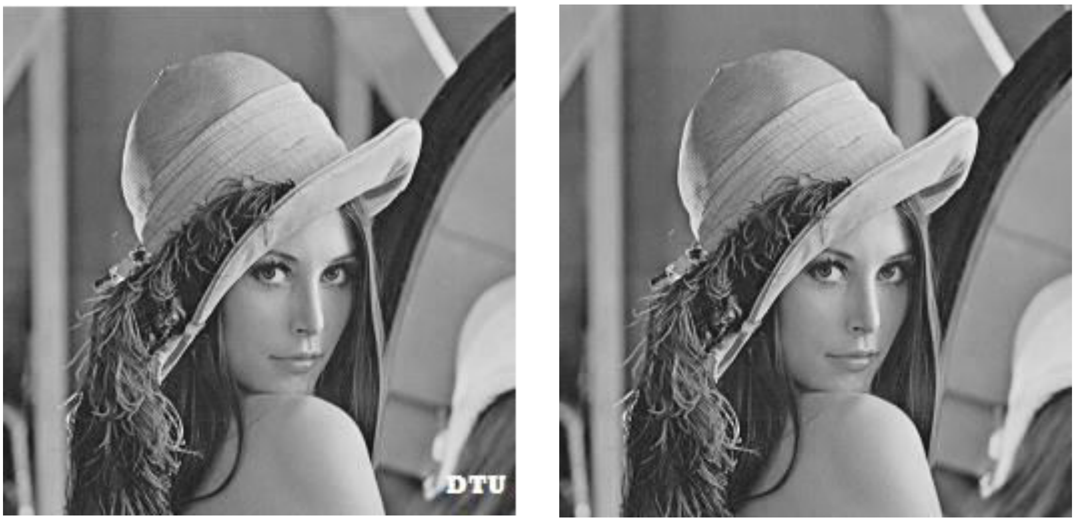


Figure 1.3. Classification based on human perception

a. **Visible watermark**: The visible watermarks such as company logo, company name, website name, owner name etc. are visible to everyone. These types of watermark easily embedded as well as easily extracted from the watermarked image. The watermarked images are not able to survive against intentional attacks, like the watermark can be removed from the watermarked image by cropping etc.

b. **Invisible watermark**: These types of watermark cannot be easily detected by viewer as the watermarked information is hidden inside the host image.

Invisible watermarking is used to hide secret information or data inside an image which cannot be detected by unauthorised user and are less prone to watermark attacks. Invisible watermarking is more robust to watermark attacks as compared to visible watermarking.



(a). Visible watermark (b) Invisible watermark

Figure 1.4. (a). Visible watermark (b) Invisible watermark

1.5.2. On the basis of watermarking application , watermarks are divided into three parts as shown in fig1.5.

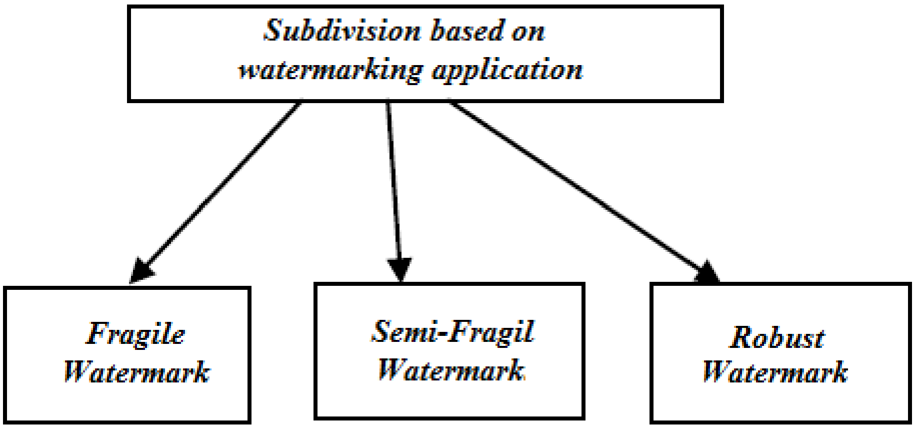


Figure 1.5. Types of watermark on the basis of application

a).**FRAGILE WATERMARKS**

Fragile watermark is highly sensitive watermark therefore it is fails to detect even small modification made on it.

b). **Semi-Fragile Watermarks:**

Semi-Fragile watermark is less sensitive as compare fragile watermark so it can tolerate modification on watermark up to some predefined threshold value. If there is no pre-defined threshold value then it is act as fragile watermark.

c). **Robust Watermarks**: These watermarks with stand against watermark attacks and able to survive against the intentional attacks. The watermarks are required to be robust watermarks for digital image or signal processing operation and malicious attacks.

1.5.3. Depending upon user's authentication, watermarks are divided into two parts as shown in fig1.6.

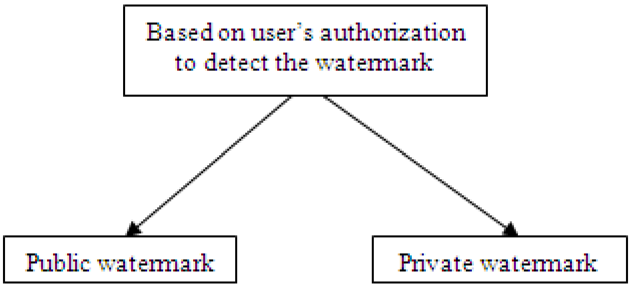


Figure. 1.6. Types of watermark on the basis of user's authorisation

Public and Private watermark:

In public watermarking all users are allowed to detect the watermark information which is embedded into an image. Therefore in public watermarking both authorized and non-authorised users can detect the embedded watermark.

In private watermarking only authorised users are allowed to detect the watermark information which is embedded into an image. Therefore unauthorized users are not able to detect private watermark information from watermarked image.

1.5.4. Depending upon user's authentication, watermarks are divided into two parts as shown in fig1.7.

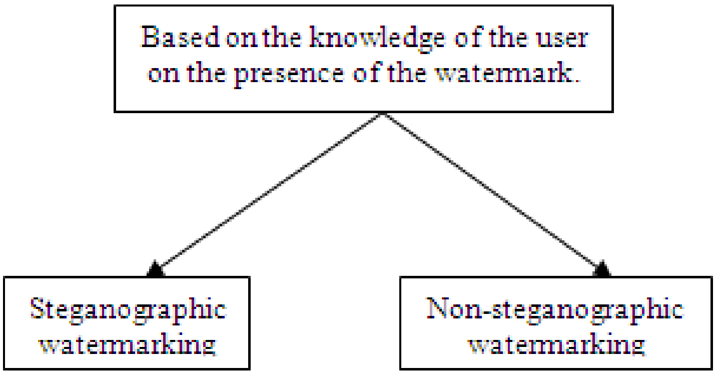

Based on the knowledge of the user on the presence of the watermark.
Steganographic watermarking
Non-steganographic watermarking

Figure 1.7 Types of watermark on the basis of knowledge of user

Steganographic & Non-steganographic Watermarking

In steganographic watermarking, an unauthorized users are not aware of existence of watermark into watermarked image as the watermark information are confidential.

In Non-steganographic watermarking both authorized as well as unauthorized user are aware of the presence of watermark which is embedded into watermarked image.

1.6. Characteristic of Digital Watermarking:

The basic requirement of digital watermarking scheme is depends on the desired applications, as the different application has different requirements. The basic characteristics of digital watermarking scheme are as follows:

- **Robustness:** It refers that the watermark inserted in digital media such as images and videos has able to survive against noise, malicious and intentional attacks. Therefore it is required that the watermark must be robust for digital image/signal processing operation. In general, it is the capability of the watermark to resist change after image processing operations such as image transformation, compression or any other modifications.

- **Imperceptibility**: It is also known as Invisibility and Fidelity. Imperceptibility refers that there is no perceptual difference between the original image and the watermarked image i.e. the desired watermarked image must looks exactly similar to the original image, and the hidden data or an information must be invisible allowing small degradation in contrast or brightness of the image.
- **Capacity**: It is also referred as "Payload" and it represents the number of bits of an image. The capacity of a digital media such as images or videos could be varying according to the application for which it is designed. Also, the capacity of the image can represents the amount of information of watermark that would be embedded into an image with necessary imperceptibility and robustness.
- **Verifiability:** The data or a piece of information which is embedded inside any digital media should be able to provide reliable and complete proof for the ownership of original data file. It is used to determine whether the object is to be protected and unauthorised access protected data, verify the authenticity, and control illegal copying of protected file or document etc.
- **Security:** It refers that only authorized person could be allowed to detect, extract and even modify the watermark or original image, which fulfil the purpose of copyright protection.

1.7. DIGITAL WATERMARKING APPLICATIONS

- **Copyright Protection**:

  In order to prevent dispute on the ownership, reliable copyright information can be embedded as a watermark into a given image which can be further extracted to identify the real owner of the image.
- **Content Authentication:**

  In this application the certain information (as watermark) is embedded in an image to detect whether the image has been modified or not, this process also used for authentication of an image or any important document.

- **Broadcast Monitoring:**

  It is especially used in the area of advertisements to ensure that the digital media is broadcasted according to the contract between the organisation or company and their clients.

- **Fingerprinting:**

  Fingerprinting is generally used to protect customers from forgery. If unknown user got a legal copy of a product and he illegally redistributed it, then fingerprinting can help to identify the duplicity.

- **Copy Control:**

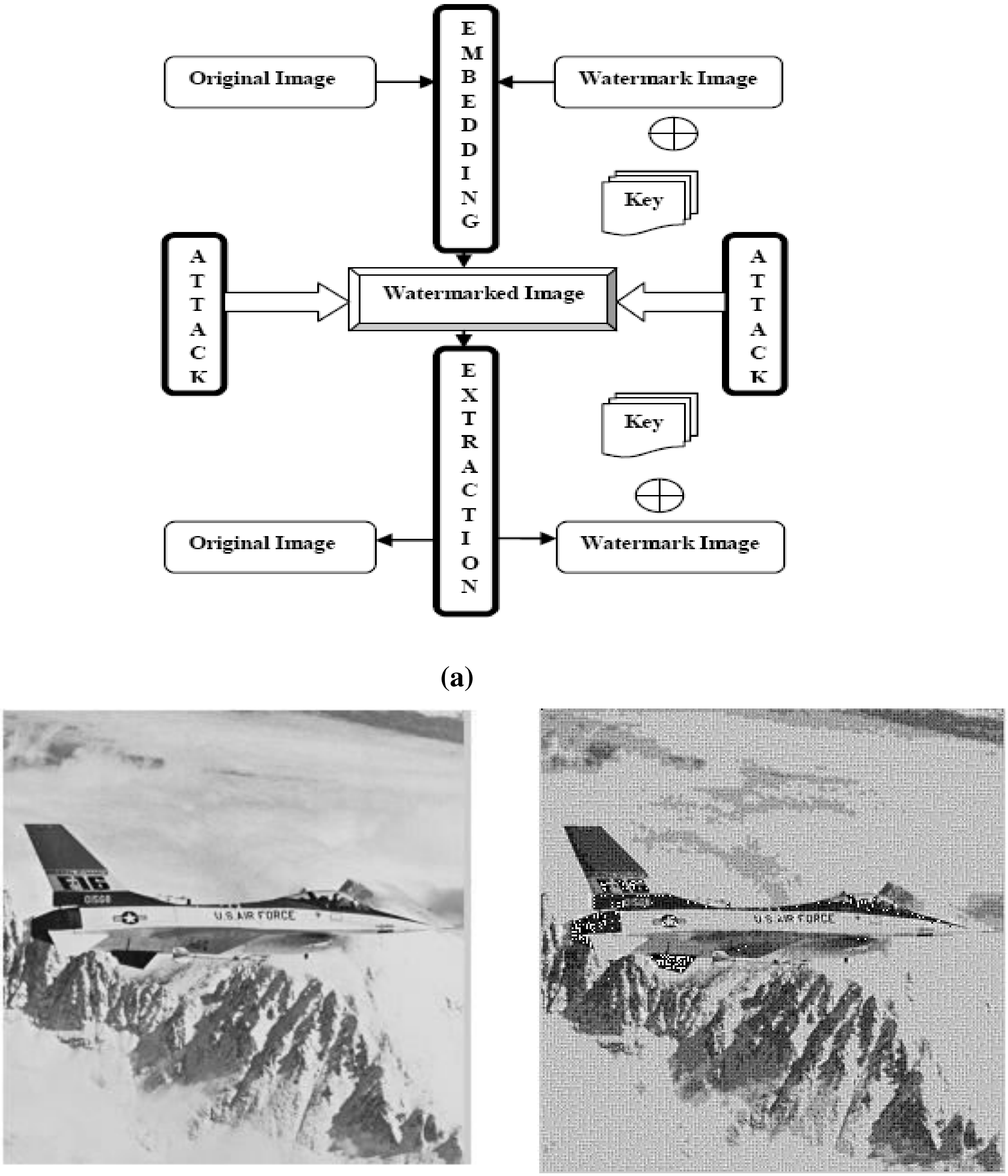
  The information that is to be watermarked into an image contains owner's information and specifies the certain number of copies. It provides tracking of legal copies for unauthorized distribution by inserting copyright information inside the original file.

- **Medical Applications:**

  To prevent the unauthorised access of electronic patient records and information from unknown users image watermarking is used. Image watermarking provides the copyright of the medical image. It can also help to secure sharing and handling of medical images.

1.8 Watermark Attacks

Change in waveform or degradation of quality of image due to noise addition and it also results in some geometric distortion like zooming, spatial transformation, rotation, cropping etc. Figure 1.8 shows the effects such attacks



(a)

(a)

(b)

Figure 1.8. (a) Block diagram representing watermarking attacks (b).Original watermark image (c). Effects of watermarking attacks on Extracted watermark

In This section, we discuss about possible attacks on watermarks. In general there are four Watermark attacks these are:

- **Simple attacks**: Simple attacks refer the change in waveform or degradation of quality of image due to noise addition. This type of watermark attacks damages the embedded watermark by modifications on an image without any effort to identify and isolate the watermark. Simple attacks consists of frequency based compression, image editing and addition of noise etc.

- **Ambiguity attacks:** This type of attacks misguide the watermark detector by generating fake watermarked data to vanish the authority of embedded watermark information by inserting multiple additional bit patterns or pixel values so that it is impossible to extract authoritative watermark.

- **Detection-disabling attacks**: These types of attacks break the correlation and make detection and extraction of the watermark from watermarked image impossible. Generally it creates some geometric distortion like zooming, spatial transformation, rotation, cropping or pixel permutation, removal or insertion. Advanced watermark detector would be used to extract the watermark from the watermarked audio, video, image etc.

- **Removal attacks:** These types of attacks analyse the embedded information or data within cover signal (i.e. watermarked data). It also estimate the inserted data or information (i.e. watermark) or the cover image and separate the watermarked data into original cover image and the watermark, and corrupt or destroy only the watermark information or data.

Note: Some watermark attacks do not belong to only one group.

1.9 **Digital Watermarking Algorithms**

The algorithms for digital watermarking are mainly divided into two broad categories that are spatial domain algorithm and transform domain algorithm as shown in figure.

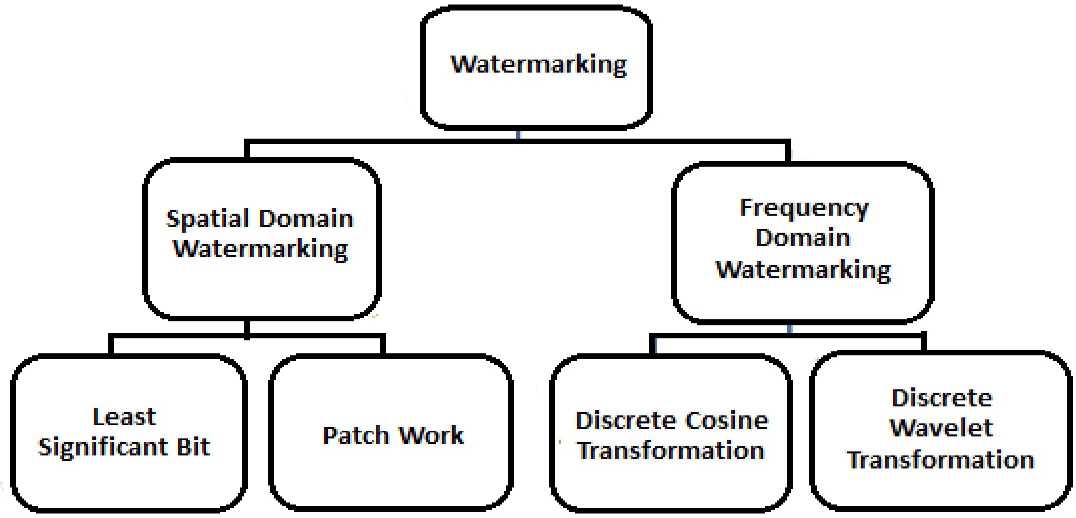

Watermarking
Spatial Domain Watermarking
Frequency Domain Watermarking
Least Significant Bit
Patch Work
Discrete Cosine Transformation
Discrete Wavelet Transformation

Figure 1.9. Classification of watermarking algorithms.

1.9.1 Spatial domain: In this domain algorithms secret data or information is directly loaded into the digital multimedia. The spatial domain algorithm further classified as follows:

a). Least significant bit algorithm: This algorithm inserts the data or an information in the form of the least significant bits which is randomly selected to ensure that the embedded data or information (i.e. watermark) is imperceptible. The main drawback of this algorithm is that it has a poor robustness against noise and the watermark information can be easily modified by filtering, image quantization and geometric distortion.

b).Patchwork algorithm: Patchwork algorithm is based on a pseudorandom, statistical model. It simply uses the statistical characteristics of pixels to insert the information or data into the brightness values of the pixels. It can resist cropping, compression coding, tone scale corrections and malicious attacks. But the amount of information which embedded is limited, in order to insert additional data or information; image can be segmented and then implement the embedding operation on each and every segment of an image.

1.9.2 Transform domain algorithm: In transform domain technique for watermarking generally, transform coefficients are modified but pixels values remains unchanged. In order to extract the watermark inverse transform is used. Transformed domain algorithms for watermarking are more robust and secure as compared to other watermarking algorithms such as spatial domain watermarking schemes because in this watermarking scheme information (i.e. watermark) can be spread out to entire image.

Some commonly used transform domain methods such as discrete cosine transform and discrete wavelet transform (DWT) etc. are discussed in chapter-2.

1.10 PERFORMANCE ANALYSIS

Performance analysis is performed to check the robustness of the various watermarking techniques. Therefore performance analysis provides assurance of improvement in a watermarking technique which is taken into account.

1.10.1. Peak Signal to Noise Ratio

It is used to measure the similarity between the cover image (i.e. original image) and watermarked image. Also it can be used to compare extracted watermark with the original watermark image. It is simply quality measure of watermarking scheme. An increase in PSNR value increases the robustness and security. For the computation of PSNR, mean Square Error (MSE) is required. Mathematically, PSNR is represented as:

$$PSNR = 10\log_{10}\left[\frac{255^2}{MSE}\right] \tag{1.1}$$

PSNR is expressed as the ratio of possible maximum power of a given signal to the power of corrupt noise. Here 255 is considered as maximum possible pixel value of the image. MSE is computed as:

$$MSE = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}[y(i,j)-y_w(i,j)]^2}{N^2} \qquad (1.2)$$

Where,

N = number of rows and columns,

$y(i,j)$= pixel value of the original image,

$y_w(i,j)$= pixel value of the watermarked image.

1.10.2 Structural Similarity (SSIM) Index

In order to predict the perceived quality of images and videos we use structural similarity (SSIM) index. It simply measures similarity between the original images and the extracted image or the original watermark image and recovered watermark image. SSIM is introduced to enhance the performance analysis methods such as PSNR and MSE.

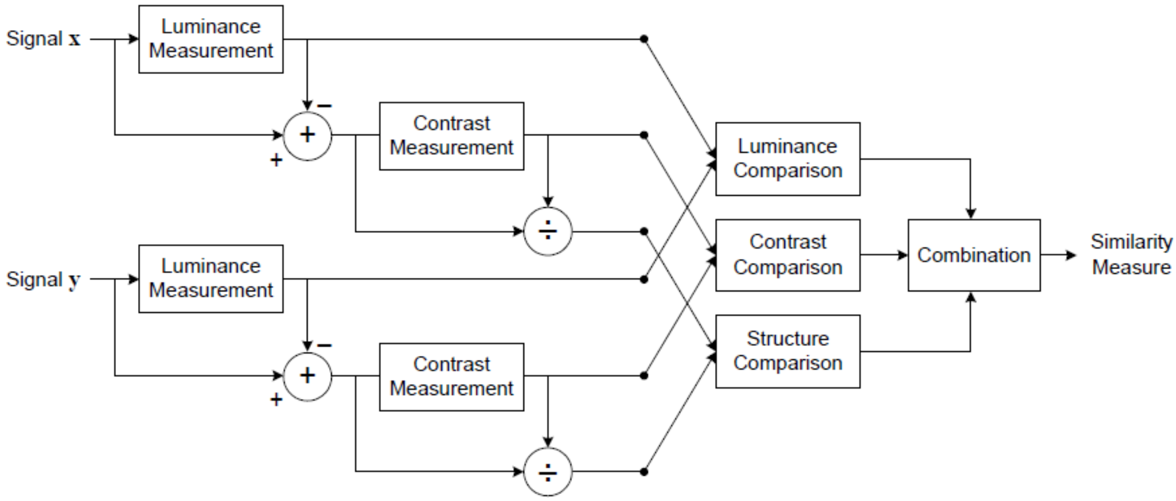


Figure.1.10: Structural Similarity Index (SSIM) measuring system

To compute the mean structural similarity index initially the original image and distorted images are splits into blocks of size 8 x 8 after that the blocks are converted into vectors.

In next step it computes mean, standard deviations and covariance values from the image by using the following mathematical tools given as:

$$\mu_x = \frac{1}{T}\sum_{i=1}^{T} x_i \tag{1.3}$$

$$\mu_y = \frac{1}{T}\sum_{i=1}^{T} y_i \tag{1.4}$$

$$\sigma_x^2 = \frac{1}{T-1}\sum_{i=1}^{T} (x_i - \bar{x})^2 \tag{1.5}$$

$$\sigma_y^2 = \frac{1}{T-1}\sum_{i=1}^{T} (y_i - \bar{y})^2 \tag{1.6}$$

$$\sigma_{xy}^2 = \frac{1}{T-1}\sum_{i=1}^{T} (x_i - \bar{x}) \cdot (y_i - \bar{y}) \tag{1.7}$$

Eq. (1.1) and (1.2) represents the mean values, (1.3) and (1.4) represents the standard deviation values and (1.5) represents the covariance value of x and y.

After computing these values as shown in above equations it analyses contrast, brightness and structural comparisons based on statistical values.
The SSIM between image x and y is calculated by equation (1.6).

$$SSIM = \frac{(2\mu_x\mu_y + c_1)\cdot(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)\cdot(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{1.8}$$

Where c_1 and c_2 are constants.

1.10.3 Execution Time

Execution time plays an important role to compute the working and performance analysis of the watermarking technique in terms of timing constraints. Execution time is used measure the time required in watermark embedding process and watermark extraction process. CPU cycles are used to measure of execution time. It can be represented as:

Start_Time = CPU_time
Execution_Time = CPU_time – Start_Time

1.10.4 Bit Correct Ratio

The Bit Correct Ratio (BCR) is the fraction of number of bits extracted correctly to the total number of embedded bits. After every attack the BCR of the extracted watermark is computed. It can be represented as:

$$BCR = \frac{100\sum_{n-1}^{L}}{L}\begin{cases} 1, & W'_n - W_n \\ 0, & W'_n \neq W_n \end{cases} \qquad (1.9)$$

Where,

L= Watermark length,

W_n = nth bit of the original watermark and

W'_n = nth bit of the recovered watermark.

1.10.5 Similarity Ratio

Similarity Ratio (SR) is simply a comparison between extracted watermarks with the original watermark. It can be represented as:

$$SR = \frac{S}{S+D} \qquad (1.11)$$

Where

S = number of matching pixels value and

D = number of different pixel values.

CHAPTER-2.

DISCRETE WAVELET TRANSFORM

CHAPTER – 2.

2.1. Survey of Wavelet transform:

From many years researchers are focusing to improve digital watermarking in wavelet domain because watermarks in this DWT domain are highly robust.

Wavelets are a simply mathematical function that satisfies a zero mean and are used to analyse signals or functions and also to represents various signals.

Definition

Let us consider the wavelet function and scaling function is given as Haar, and their basis are known. Then we are able to approximate a discrete signal in $\{f[n] \mid \sum^{\infty}_{n=-\infty} \mid f[n] \mid^2 < \infty\}$ by

$$f[n] = \frac{1}{\sqrt{M}} \sum_k W_\phi[j_0,k]\phi_{j_0,k}[n] + \frac{1}{\sqrt{M}} \sum_{n=0}^{\infty} \sum_k W_\phi[j_0,k]\phi_{j_0,k}[n] \tag{2.1}$$

Where, $f[n]$, $\phi_{j_0,k}[n]$ and $\psi_{j,k}[n]$ are the discrete functions defined in interval [0;M - 1],i.e. for M points. As the two sets $\{\phi_{j_0,k}[n]\}_{k \in Z}$ and $\{\psi_{j,k}[n]\}_{(j,k) \in Z^2}$, providing $j_0 \geq j$,are orthogonal to each other. The inner product to obtain the wavelet coefficients are as

$$W_\phi[j_0,k] = \frac{1}{\sqrt{M}} \sum_n f[n] \cdot \phi_{j_0,k}[n] \tag{2.2}$$

$$W_\psi[j,k] = \frac{1}{\sqrt{M}} \sum_n f[n] \cdot \psi_{j,k}[n] \quad , \; j_0 \geq j \tag{2.3}$$

Where,

$W_\phi[j_0,k]$ are called approximation coefficients while $W_\psi[j,k]$ are called detailed coefficients.

2.2. 2D Wavelet Transform

Let us take case of 2D Fourier transform, the basis are modified into

$$\exp(j(\omega_1 t_1 + \omega_2 t_2) \qquad (2.4)$$

Instead of $\exp(j\omega t)$. These transformed coefficient will become the scaling and wavelet function are functions of two variable and denoted by $\phi(x, y)$ and $\psi(x, y)$.
The scaled and translated basis functions are given as

$$\phi_{j,m,n}(x, y) = 2^{j/2}\phi(2^j x - m, 2^j y - n) \qquad (2.5)$$

$$\psi^i_{j,m,n}(x, y) = 2^{j/2}\psi^i(2^j x - m, 2^j y - n), \quad i = \{H, V, D\} \qquad (2.6)$$

These three wavelet functions are, $\psi^H(x, y)$, $\psi^V(x, y)$ and $\psi^D(x, y)$. Basically, the scaling function is the 2D low frequency components of the previous scaling function. Therefore, there are one 2D scaling function and three 2D wavelet functions which can be written as.

$$\phi(x, y) = \phi(x) \cdot \phi(y) \qquad (2.7)$$

$$\psi^H(x, y) = \psi(x) \cdot \phi(y), \qquad (2.8)$$

$$\psi^V(x, y) = \phi(x) \cdot \psi(y), \qquad (2.9)$$

$$\psi^D(x, y) = \psi(x) \cdot \psi(y), \qquad (2.10)$$

These functions as separable functions, therefore it is easy to analyse these 2D functions. The analysis and synthesis equations as in case of 1D wavelet inner products are modified as

$$W_\phi[j_0, m, n] = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x, y) \cdot \phi_{j_0,m,n}(x, y), \qquad (2.11)$$

$$W_{\psi}^{i}[j,m,n]=\frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\cdot\phi_{j,m,n}^{i}(x,y),\ i=\{H,V,D\} \tag{2.12}$$

$$f(x,y)=\frac{1}{\sqrt{MN}}\sum_{m}\sum_{n}W_{\phi}(j_{0},m,n)\cdot\phi_{j,m,n}^{i}(x,y)+\frac{1}{\sqrt{MN}}\sum_{i=H,V,D}\sum_{j=j_{0}}^{\infty}\sum_{m}\sum_{n}W_{\psi}^{i}(j,m,n)\cdot\phi_{j,m,n}^{i}(x,y)$$

(2.13)

2.3. Decomposition Process

Let us consider an square image of size P by P.

An image is filtered by high-pass and low-pass filters along the rows and the results obtained after filtering are down sampled by 2. These two signals corresponding to high pass frequency and low-pass frequency, each are of size P by P/2. Both of these two sub-signals are again filtered by high-pass and low-pass filters along the columns and the resulted sub-signals are again down-sampled by two. One decomposition step of the 2-D image is shown in figure:

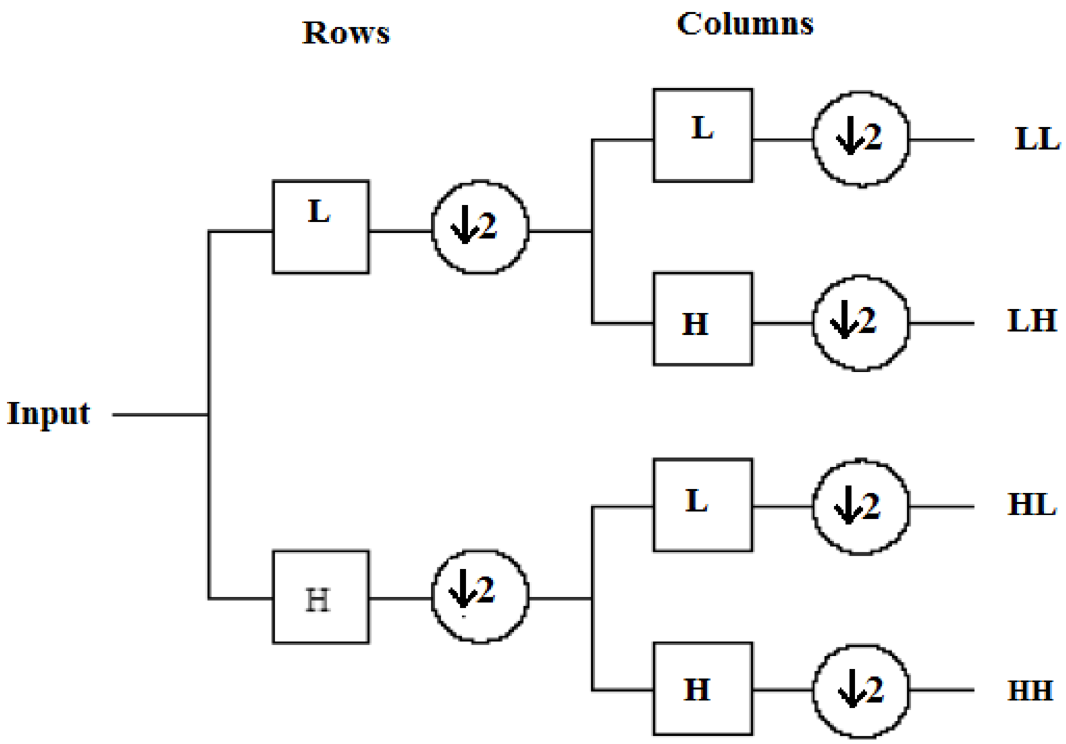


Figure2.1. Decomposition step of the 2D grey scale image

This is how in DWT an image is divided into four sub-bands each represent sub-image of size P/2 by P/2 containing information of different frequency components.

Figure 2.2, represents the one step decomposition of a 2-D image into four sub-bands.

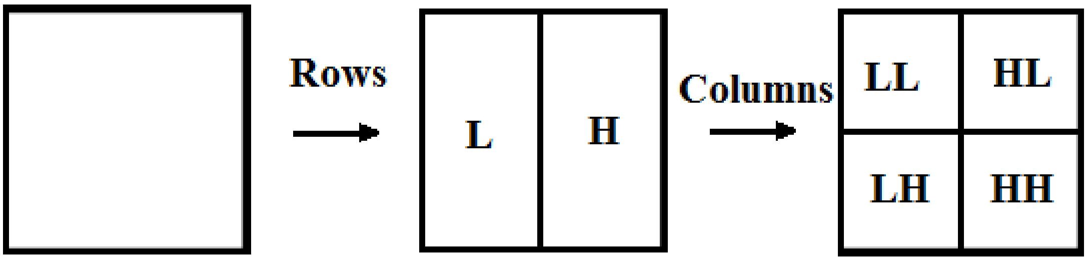


Figure 2.2 Decomposition of 2D image into four sub-bands.

The LL portion, shown in above figure is results after the low-pass filtering along both the rows and columns and it provides a rough description of an image. Therefore, LL sub-band is also known as approximation sub-band which represent coarse scale also known as approximation sub-band whereas the HH sub-band obtained by high-pass filtering first along rows and then along columns, and consists the fine(high-frequency) scale components along its diagonals. The LH (and HL) sub-bands are obtained due to low-pass filtering along rows (or column) and high-pass filtering along column (or row). LH consists of vertical information and corresponds to horizontal edges. HL consists of horizontal information corresponds to vertical edges. Sub-bands LH, HL and HH are fine scale and referred the detail sub-bands, because they integrate the high-frequency information detail of the approximation image.

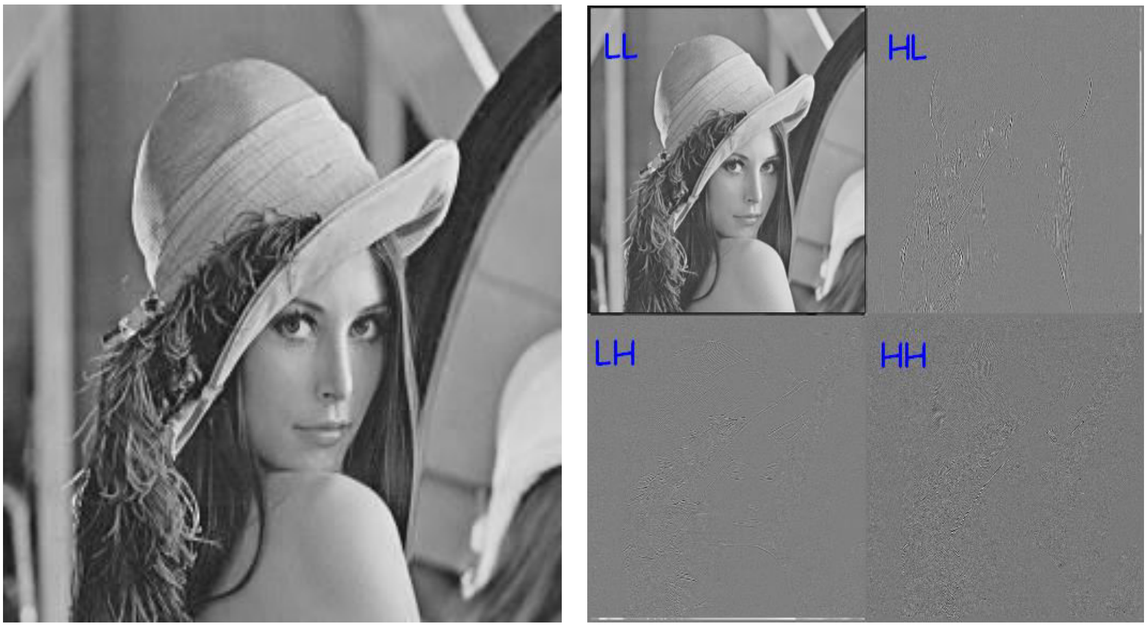


Figure 2.3. One step wavelet decomposition of Lena image.

In Discrete wavelet transform any image can decompose multiple times. Decomposition can be done continuously until the given image has been entirely decomposed into sub-bands. But if we want to perform compress back an image after decomposition and watermarking applications, then only five decomposition steps are computed.

The two common ways for decomposition in wavelet transform. These are:

a.) Pyramidal decomposition
b.) Packet decomposition

2.3.1. Pyramidal Decomposition

This decomposition mechanism is one of the most common decomposition methods. In pyramidal decomposition method we can apply further decompositions only in LL sub-band. Figure represents a typical diagram of three continuous decomposition steps. At each and every level the detail sub-bands are obtained and the further decomposition can be only done in an approximation sub-band.

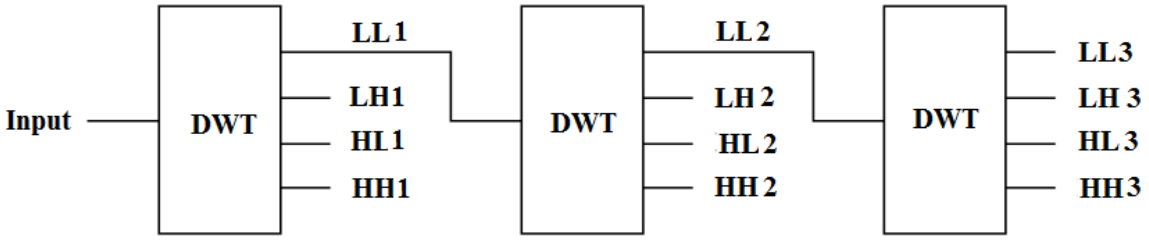


Figure 2.4. Three stage decomposition of 2D image.

Figure 2.4 represents the pyramidal structure which is obtained from this three stage decomposition. Initially there is one approximation sub-band and there are total nine detail sub-bands of an image as shown in figure 2.5. After M decompositions we have a total of sub-bands is equal to 3*M+1.

$$D(M)=3*M+1$$

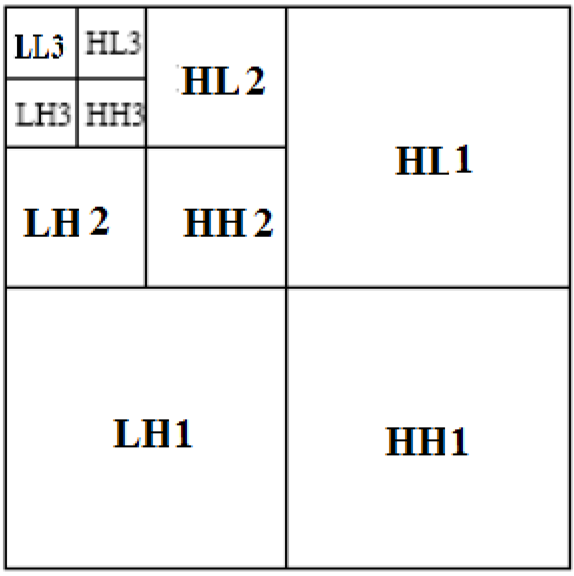


Figure 2.5 Pyramid decomposition after three decomposition steps.

Figure 2.6 represents typical three stage decomposition process in “Lena" image up to three pyramidal decomposition steps is shown.

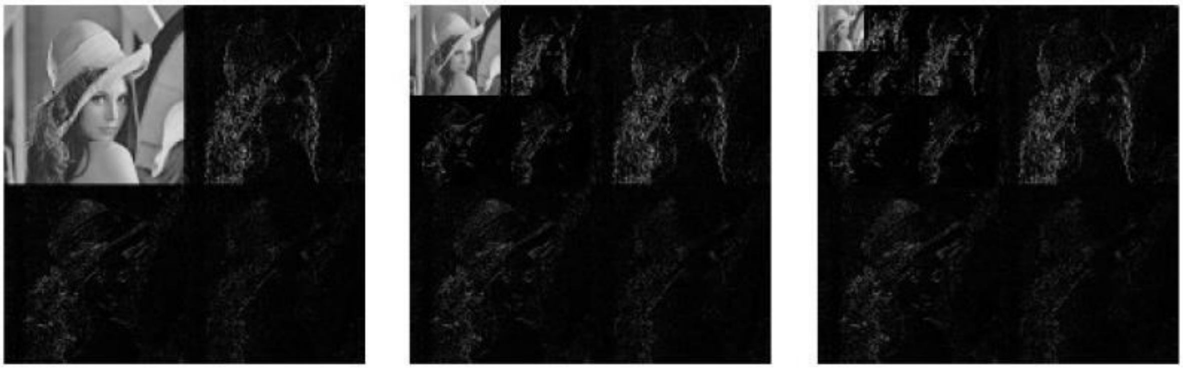


Figure 2.6 “Lena" image up to three pyramidal decomposition steps.

2.3.2. Wavelet Packet Decomposition

In wavelet packet decomposition there is no limit on number of decomposition to the approximation sub band and also it is possible perform wavelet decomposition in all sub bands to all levels.

Figure show the typical diagram for a complete two level decomposition by using wavelet packet decomposition.

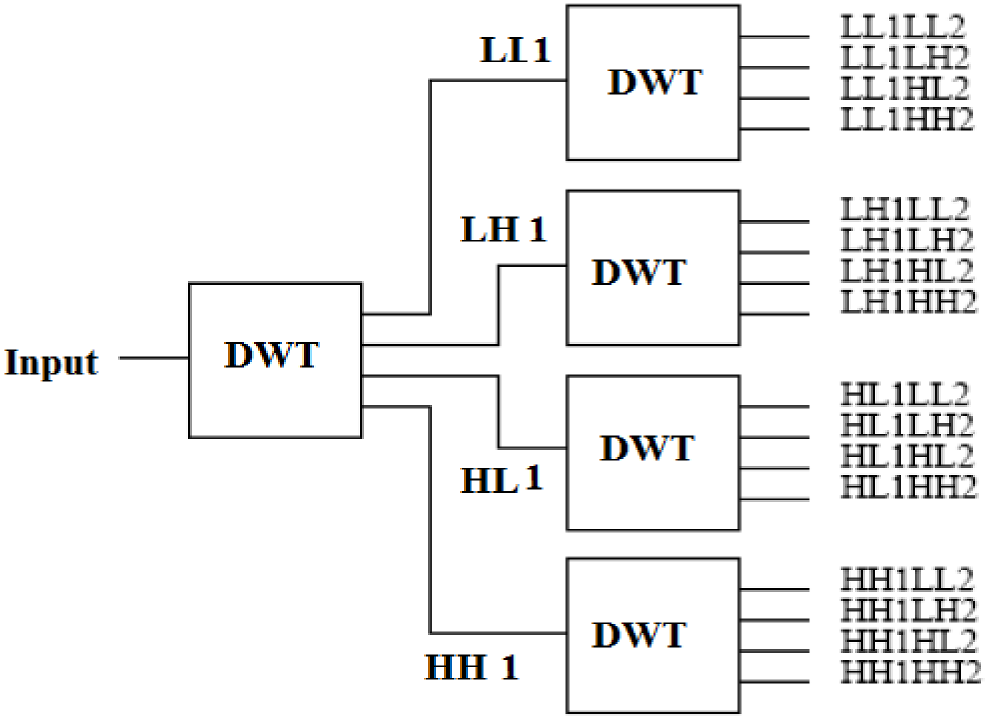


Figure 2.7. Simple wavelet packet decomposition.

Figure 2.7. Shows the resulting sub-band structure which represents the simple decomposition step from the basic building block. All sub-bands (i.e. LL, LH, HL and HL) on one level are taken as input to the filter banks for the inverse transformation and sub-band on the higher level is obtained. The same process is repeated certain number of times until the original image is regenerated.

LL1LL2	LL1HL2	HL1LL2	HL1HL2
LL1LH2	LL1HH2	HL1LH2	HL1HH2
LH1LL2	LH1HL2	HH1LL2	HH1HL2
LH1LH2	LH1HH2	HH1LH2	HH1HH2

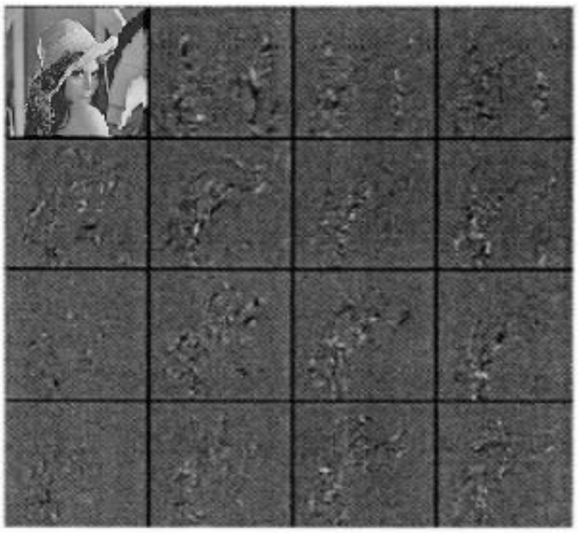


Figure 2.8. Structure of the sub-bands after two level packet decomposition.

2.4. Composition Process:

The converse of decomposition process is shown in figure 2.9. The component information belongs to all four sub-bands (i.e. LL, LH, HL & HH) of an images are up-sampled by 2 after that they are filtered with their corresponding inverse filters along the columns. The two results which belong to same domain are combined together and then again up-sampled and filtered through their corresponding filters that perform inverse function. The result of the last step is added together and we have the original image again.

It is observed that there is no information loss decomposition of an image and also when they composed again to form an image.

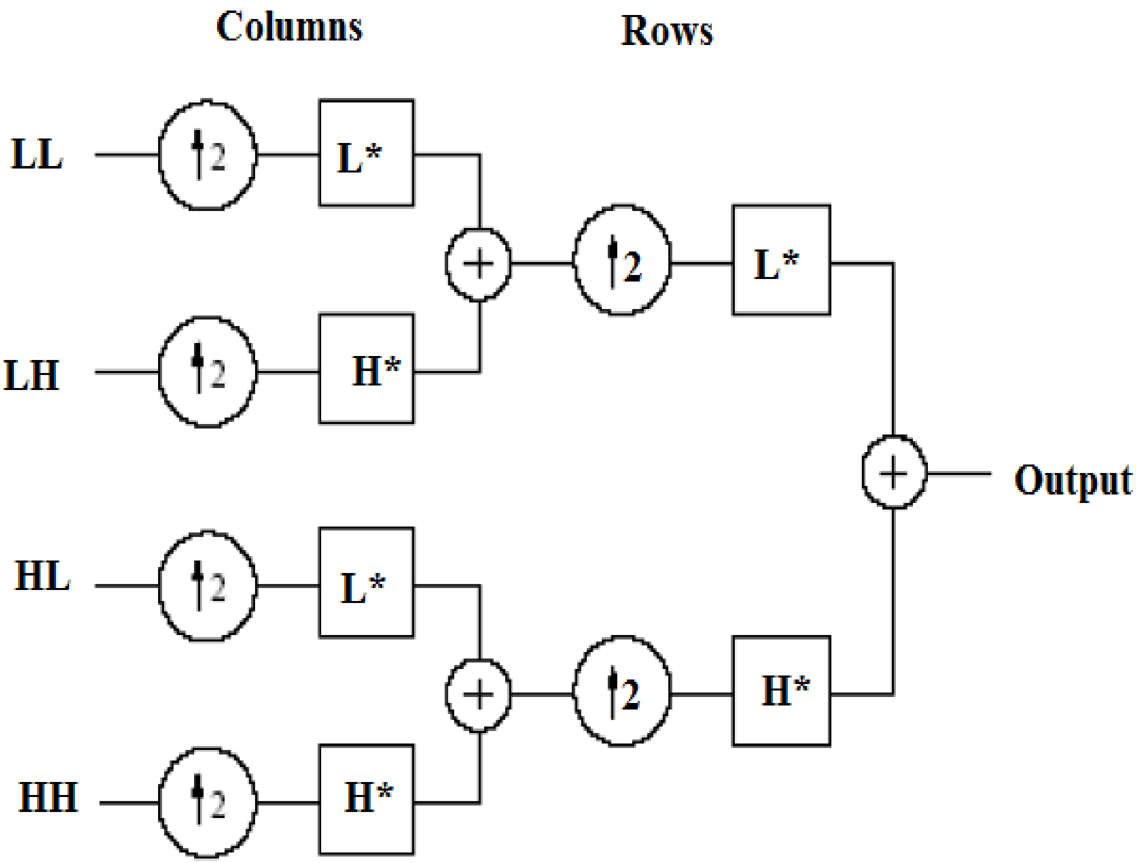


Figure 2.9. Composition of sub-bands using one step composition.

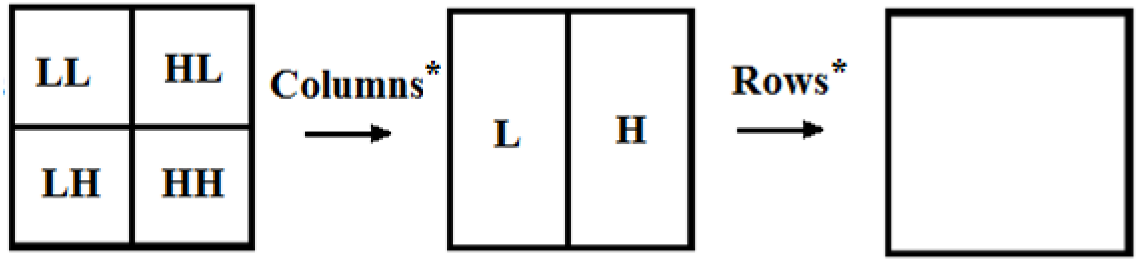
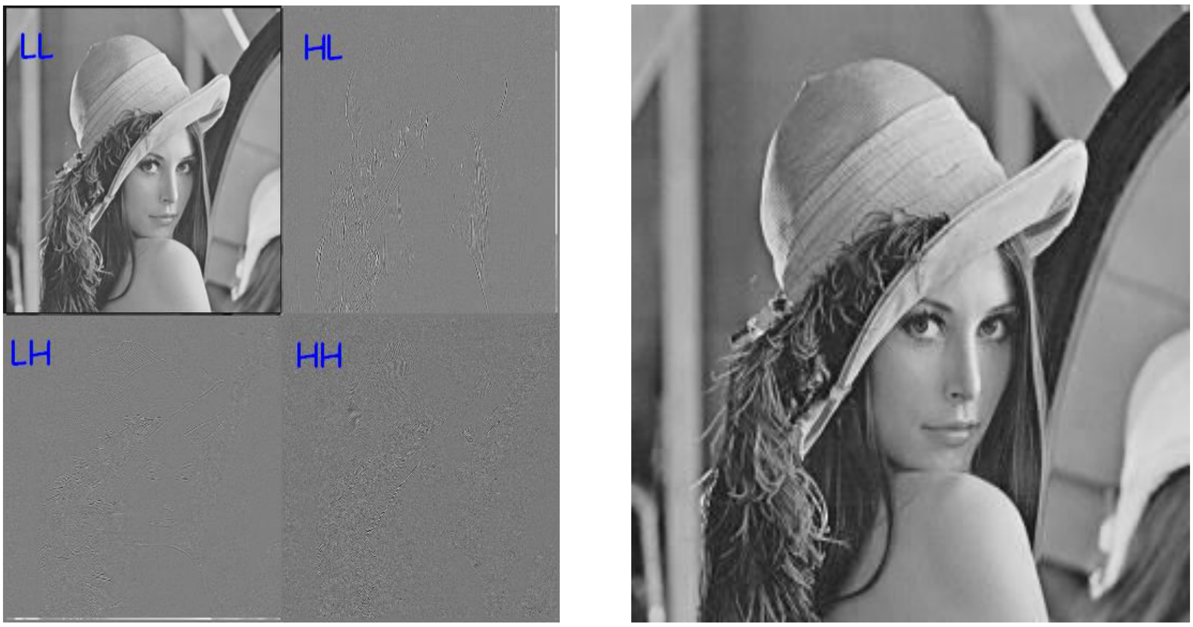


Figure 2.10. Block diagram representing one step composition.

It is observed that there is no information loss decomposition of an image and also when they composed again to form an image.



(a) (b)

Figure 2.11. (a) Four sub-band representation of Lena image

(b) Reproduction of Lena image by using one step composition.

2.5. LIFTING SCHEME FOR DISCRETE WAVELET TRANSFORM

The Lifting-based DWT factorizes any wavelet transform of signal into a series of elementary convolution operators which is known as lifting steps. Lifting scheme reduces the number of arithmetic operations around a factor two and it leads a speed-up and a fewer computation compared to the classical DWT which is convolution-based method.

It is also known as integer based wavelet transform which is used to simplify the treatment of signal boundaries.

The lifting-based DWT has many advantages over other transform techniques including complete parallel operations, “in-place” computations of the wavelet transform, integer-to-integer transform, symmetric forward transform and inverse transform, etc.

Lifting based dwt schemes generally consists of three basic operation stages:

Splitting: where the signal splitting into polyphase components i.e. even and odd pixels

$$x_e = (x_{2k})_{k\epsilon Z} \qquad \text{and} \qquad x_o = (x_{2k+1})_{k\epsilon Z}$$

Where x_e and x_o are closely correlated .

Predicting: Here even samples are added with factor, known as prediction factor, which is derived from odd and even pixels to obtain their low frequency values.

Updating : The values of detailed coefficients gets computed by the product of predict step and the update factors, and then the output results are subtracted to the even samples to obtain high frequency values

Merging/Combining : It is similar to the operation performed in the reverse process of DWT which merge all the LL,LH,HL and HH sub-bands to reconstruct the original image.

In this procedure values of image pixels are split into even samples and odd samples then to obtain high frequency values even samples are subtracted from odd samples low frequency values is equal to sum of even and high/2 samples. This procedure is repeated again for two phases. The first phase is known as Column Filter that means performing the discrete wavelet transform operations on columns to obtain Low and High frequency values. In second phase, which is also known as Row filter we apply DWT operations on rows in order to obtain the LL, LH, HL, and HH.

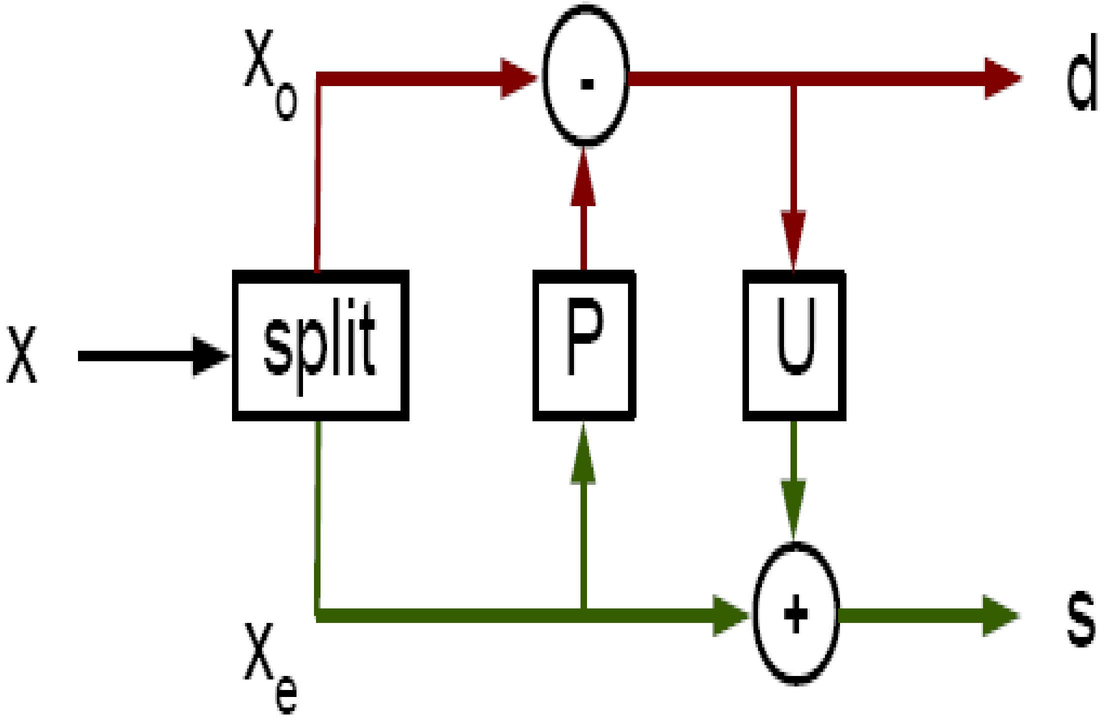


Figure 2.12. Lifting Discrete Wavelet Transform

The Inverse lifting wavelet transform(ILWT) follows the same process, as in inverse discrete wavelet transform, in reverse manner so that it reconstruct original cover image from their LL, LH, HL, and HH sub-bands values. ILWT is simply a process of generating image pixel values from frequency domain.

In this project we take two level transformations in lifting scheme for discrete wavelet transform in Verilog HDL to convert pixel values of cover image into frequency domain by using Haar transformation as used in simple DWT.

2.6. Wavelet Domain Advantages

1. Compression of video and Image into their standards such as MPEG4 and JPEG-2000 are based on wavelets. So it is possible to compress high data such as video and images.

2. Wavelet transform based video and image watermarking techniques have multi-resolution hierarchical characteristics. Therefore an image can be shown at various resolution, and it can be also sequentially processed from low resolution to high resolution.

3. It is a more robust watermarking technique used in digital image processing.

4. The high frequency sub-bands in the discrete wavelet transform consists the textures and edges information of the image which is not perceived by the human eye.

5. DWT theory is capable of explaining aspects of data that whether the signal analysis techniques miss the aspects like trends, discontinuities in higher order derivatives and decorrelation, and breakdown points.

CHAPTER-3

Implementation of image watermarking

CHAPTER-3

3.1. Algorithm for image watermarking.

Input:

Cover Image – It is a given original image which is to be watermarked.

Watermark Image – It is another image or binary pattern act as watermark.

Key – numeric key (say k) embedded with watermark and further used at the time of extraction of watermark image.

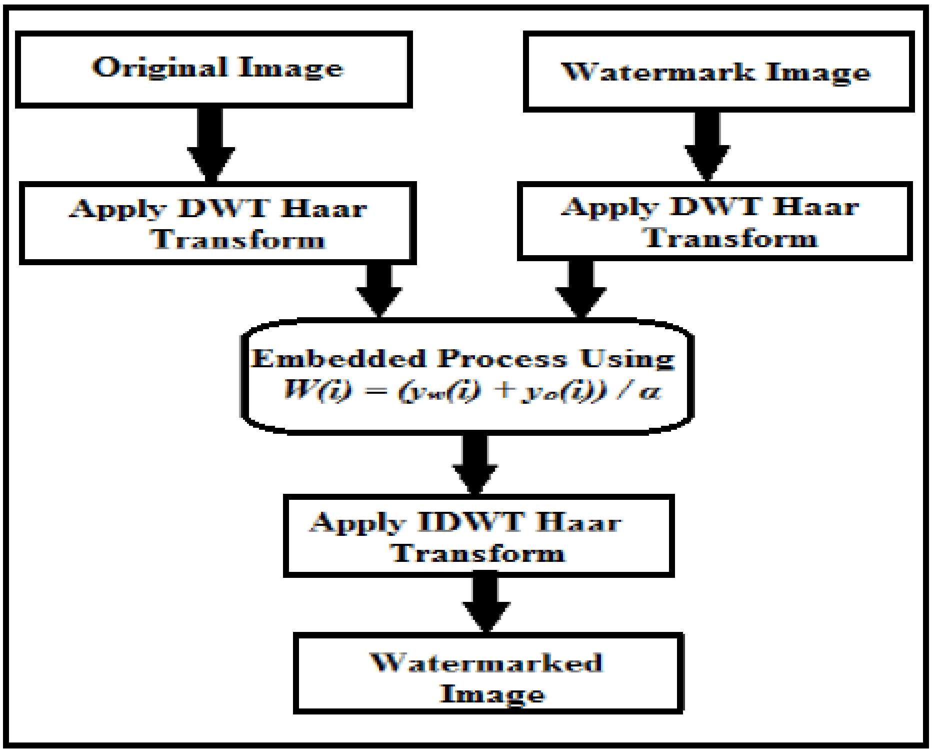


Figure 3.1. Block Diagram of Watermark embedding algorithm

A) Embedding Process:

- Get Img as Input Image(i.e. cover image).
- Get wm or Img2 as Watermark image
- Img2 to One-D bit format
- Initialization of blocksize for discrete wavelet transform referred as bsize and also initialize the Frequency threshold called freq.
- For i=1 to sizeof(wm_image)
- Apply DWT decomposition is performed on the Cover (original image) Image at level one by using one step decomposition. This decomposition results in four sub-bands CA,CH,CV and CD) in which approximation, horizontal, vertical and diagonal coefficients respectively are stored.
- Now take to next block
- If (wm_image(i)=0)
- Arrange all the Diagonal Coefficients in Ascending order
- Else
- Arrange all the Diagonal Coefficients in Descending order
- Apply Frequency Analysis on the block and hide the data or information at extract coefficient position
- Perform Inverse discrete wavelet transform(IDWT) over the image
- Obtain the Watermarked Image
- End

B) Extraction Process

- Get dwimg represents Watermark Image
- Obtain siz represents message size
- Initialize blk representing dWT Block size
- For i=1 to siz
- One step Decomposition on the image using DWT for the specific-block at position (x,y) and also extract all DWT coefficients
- Take next block
- Compare all DWT Diagonal Coefficient elements and set higher values to 1 and lower values to 0
- Msg= Message U Extract (DWT_Coefficient_Value, high, low)
- Return Msg
- End

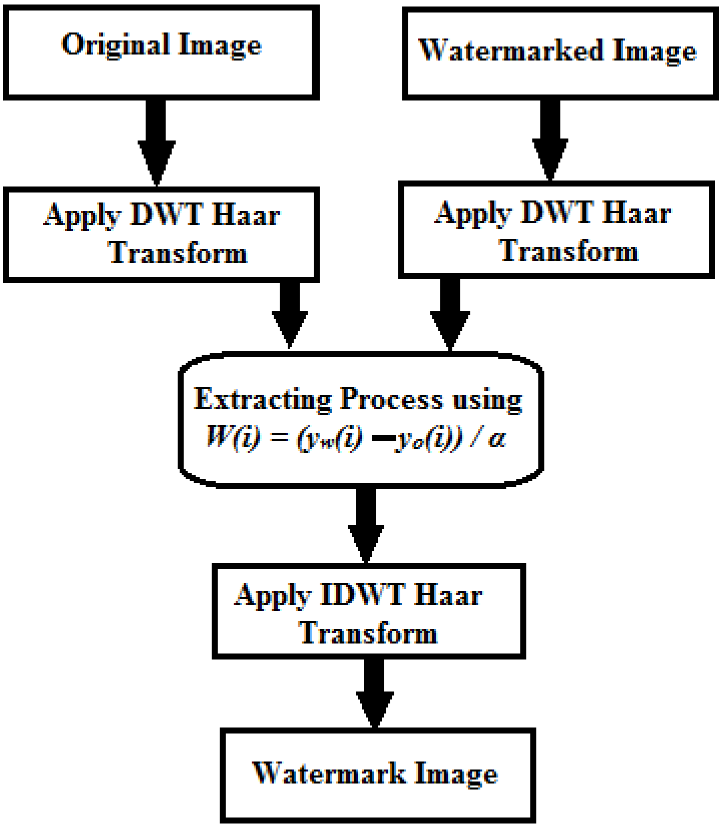


Figure 3.2. Block Diagram of extraction of Watermark from watermarked image.

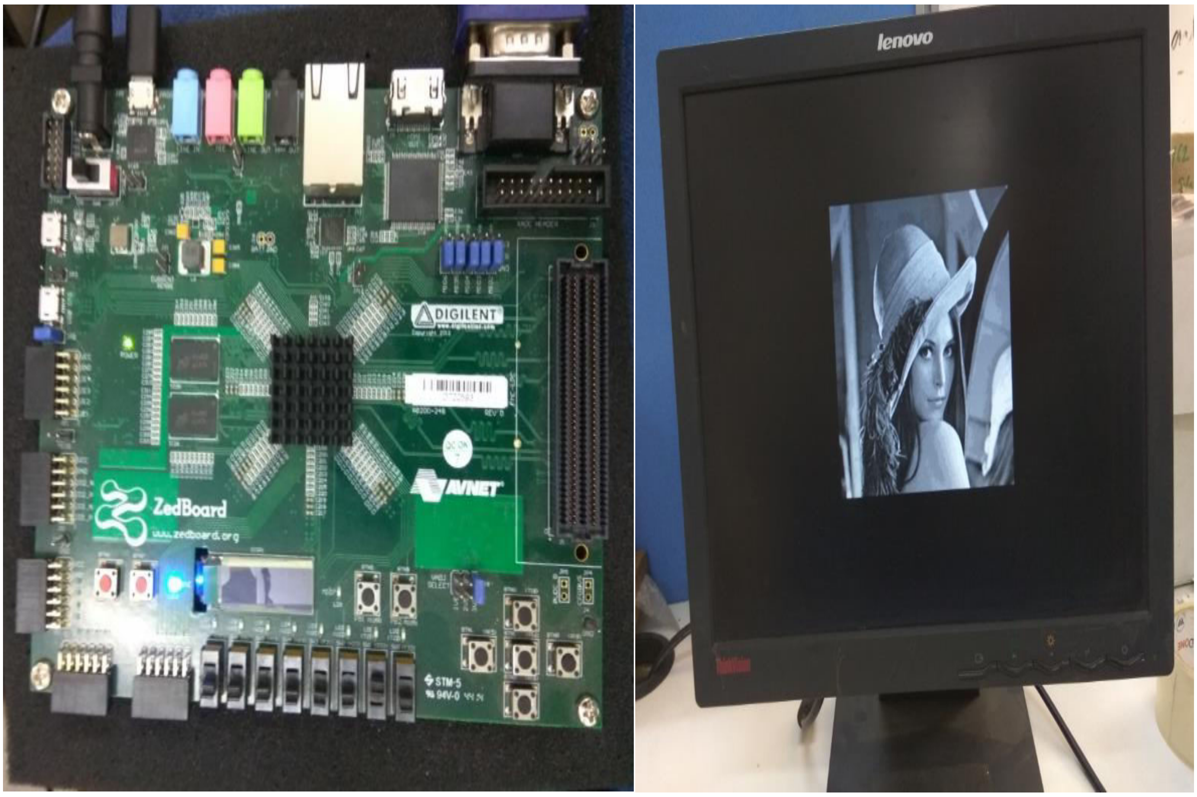
3.2 Simulation

Verilog, hardware descriptive language, is used to describe the complete hardware architecture of the watermarking system within the MPEG encoder system. Each module which is used in the design was simulated separately using VIVADO (HDL software used to simulate all digital design systems) and they passed the simulation individually.

3.2.1 FPGA Prototyping

The Verilog HDL represents the entire description of the system was compiled, synthesized and simulate into ZedBoard that includes **Xilinx Vivado® Design Edition license voucher**. and the synthesis report was analysed in Vivado 2014.2 EDA tool.

For hardware implementation here we use ZedBoard™ which is a basic development board for the Xilinx Zynq-7000 All Programmable SoC. The hardware i.e. Zedboard is shown in figure given below:



(a) (b)

Figure 3.3. (a) Image of Zedboard hardware. (b)Display watermarked image.

3.2.2 Block Memory Generator

Block memory generator provides creation of resource and power optimized block of memories for required application implemented in Xilinx FPGAs. Vivado ISE Design Suite CORE Generator enables the users to create optimized block memory functions to meet requirement of variety of application.

Generation of block memory

Convert image.bmp into text file using MATLAB

- Create image.coe file
- .coe (co-efficient) file is a text file with expension ".coe". It is used to store small chunks of data into BRAM in case of digital signal and image processing filter coefficients.

- .coe binary format:

  MEMORY_INITIALIZATION_RADIX=2

  MEMORY_INITIALIZATION_VECTOR

  0100,0110,1100…..

- .coe hex format:

  MEMORY_INITIALIZATION_RADIX=16

  MEMORY_INITIALIZATION_VECTOR

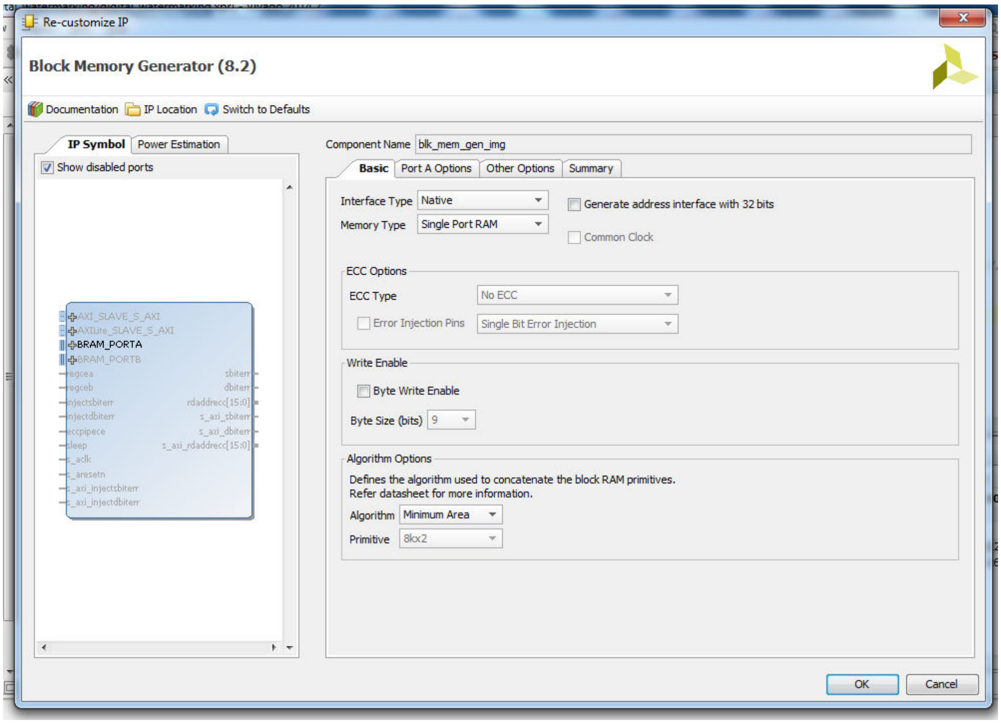
  29,A5,E3,….

Uploading of .coe file by following

Step.1- Click on add new source in selected project in vivado simulation software and select "IP Core Generator & architecture".

Step.2- Now follow "memory & storage elements", then click on RAM & ROMs->Block memory generator.

Step.3- Select "single port Ram" and click on next.



Re-customize IP

Block Memory Generator (8.2)

☑ Show disabled ports

Component Name: blk_mem_gen_img

Interface Type: Native

Memory Type: Single Port RAM

□ Generate address interface with 32 bits

□ Common Clock

ECC Options

ECC Type: No ECC

□ Error Injection Pins: Single Bit Error Injection

Write Enable

□ Byte Write Enable

Byte Size (bits): 9

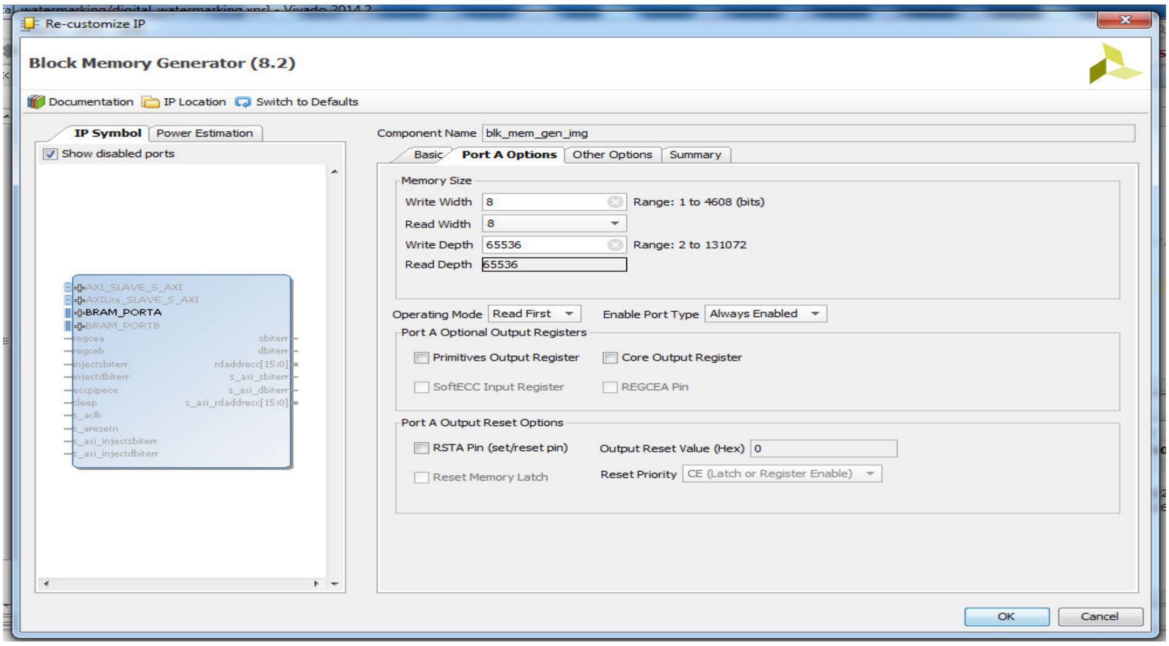
Algorithm Options

Defines the algorithm used to concatenate the block RAM primitives.
Refer datasheet for more information.

Algorithm: Minimum Area

Primitive: 8kx2

Step.4-Now enter the Data width and memory depth and go to Next.



Re-customize IP

Block Memory Generator (8.2)

Component Name blk_mem_gen_img

Memory Size

Write Width 8 Range: 1 to 4608 (bits)

Read Width 8

Write Depth 65536 Range: 2 to 131072

Read Depth 65536

Operating Mode Read First

Enable Port Type Always Enabled

Port A Optional Output Registers

□ Primitives Output Register □ Core Output Register

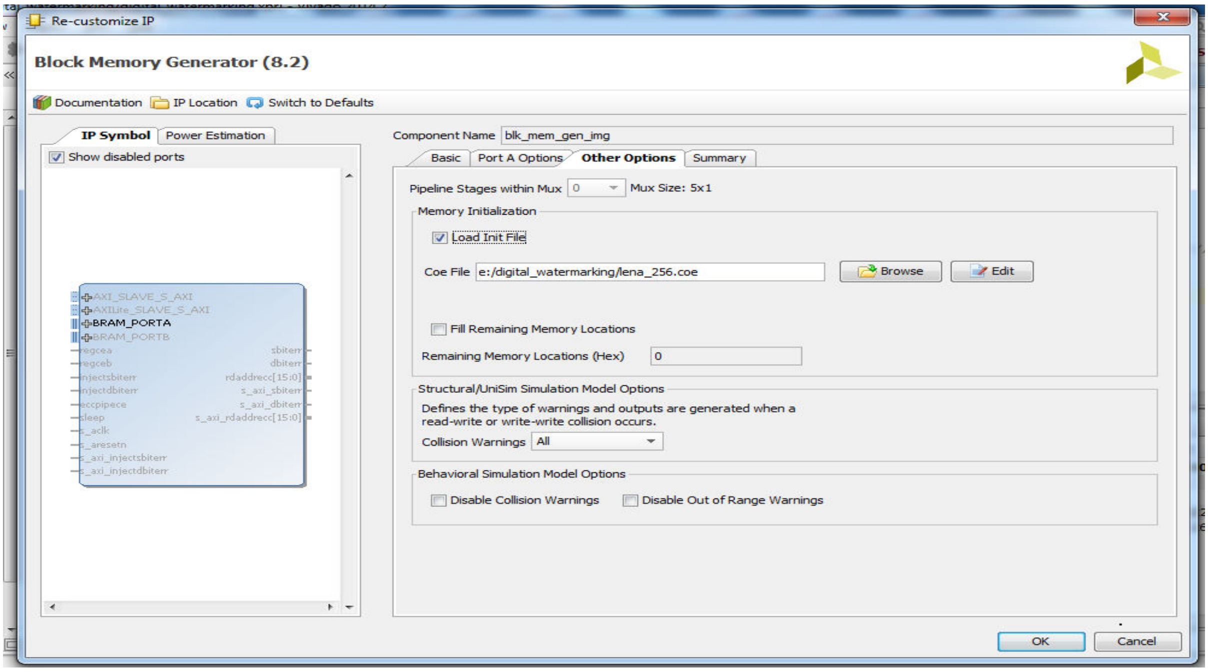
□ SoftECC Input Register □ REGCEA Pin

Port A Output Reset Options

□ RSTA Pin (set/reset pin) Output Reset Value (Hex) 0

□ Reset Memory Latch Reset Priority CE (Latch or Register Enable)

Step.5- Click on “load init file” and browse .coe file, it also show the data in memory by using “show” icon.



Re-customize IP

Block Memory Generator (8.2)

Component Name blk_mem_gen_img

Pipeline Stages within Mux 0 Mux Size: 5x1

Memory Initialization

☑ Load Init File

Coe File e:/digital_watermarking/lena_256.coe

□ Fill Remaining Memory Locations

Remaining Memory Locations (Hex) 0

Structural/UniSim Simulation Model Options

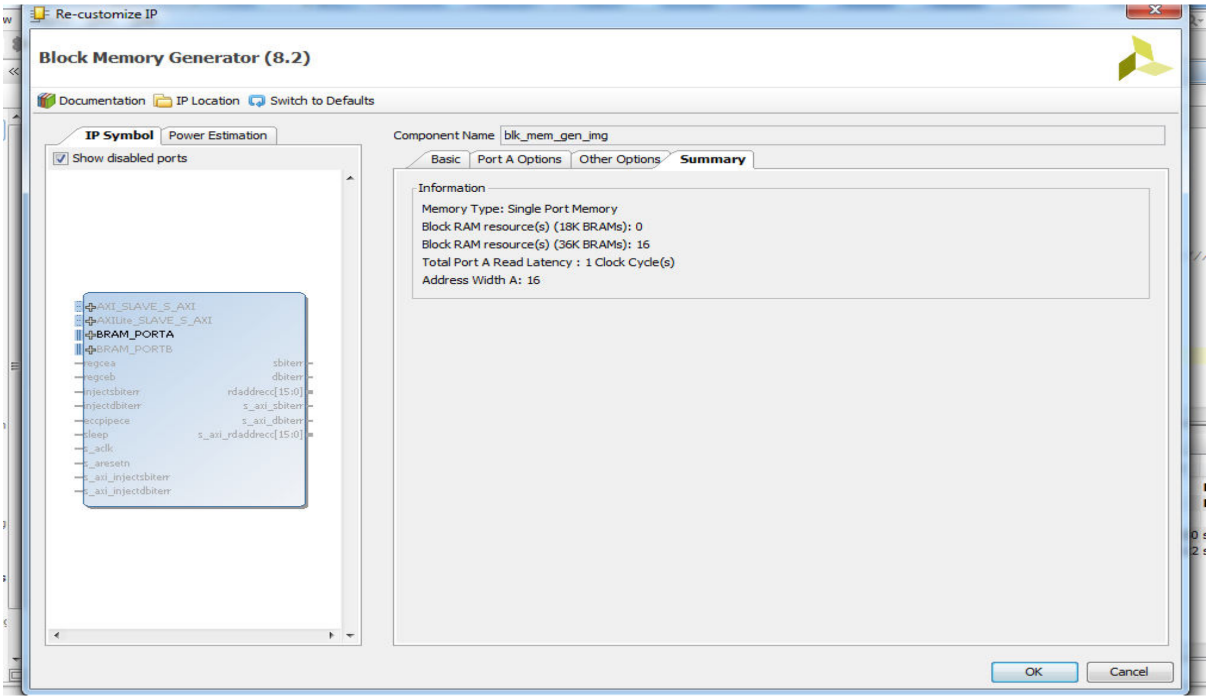
Defines the type of warnings and outputs are generated when a read-write or write-write collision occurs.

Collision Warnings All

Behavioral Simulation Model Options

□ Disable Collision Warnings □ Disable Out of Range Warnings

Step.6- Now click on “Ok” to obtain a memory IP-Core.



Block Memory Generator (8.2)

☑ Show disabled ports

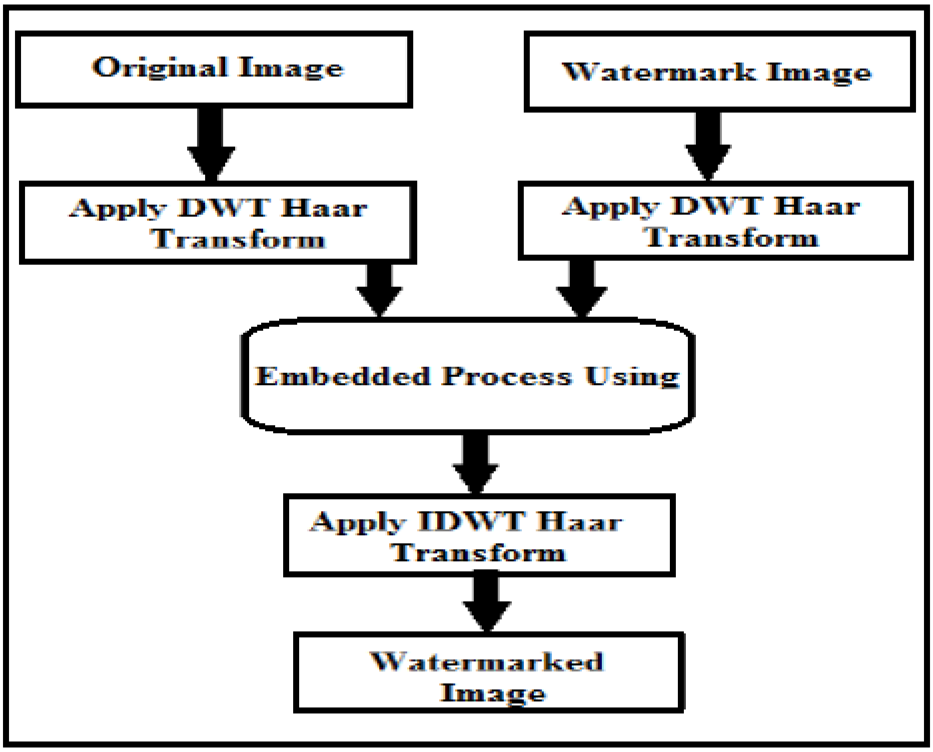
Component Name: blk_mem_gen_img

Information

Memory Type: Single Port Memory
Block RAM resource(s) (18K BRAMs): 0
Block RAM resource(s) (36K BRAMs): 16
Total Port A Read Latency : 1 Clock Cycle(s)
Address Width A: 16

3.3. Verilog HDL Implementation

Data transfer between the different operative parts are done by using pipeline fundamental. The structure of the watermark embedding algorithm is shown below in Fig. 3.1.



The design was realized in Verilog using VIVADO simulation software. A 2D-DWT is implemented on the input pixels first. These pixel values generated using MATLAB by converting original image and watermark image file into text file. These text file which contains all the pixel information or values taken as intermediate values and are stored in a BRAM by using Block Memory Generator. These inputs are stored into different std_logic register. After this 2D wavelet transform(DWT2) using haar transformation in which first transfer all pixel values from memory to img register then generate high pass coefficients and low pass coefficients by using multiplier, adder, buffer and shift registers in which the pixel values of cover image and watermark image are multiplied by some constant value and then combined in an adder as we want to perform one step decomposition to generate LL, HL, LH and HH sub bands for both original image and watermark image. Figure shows following procedure

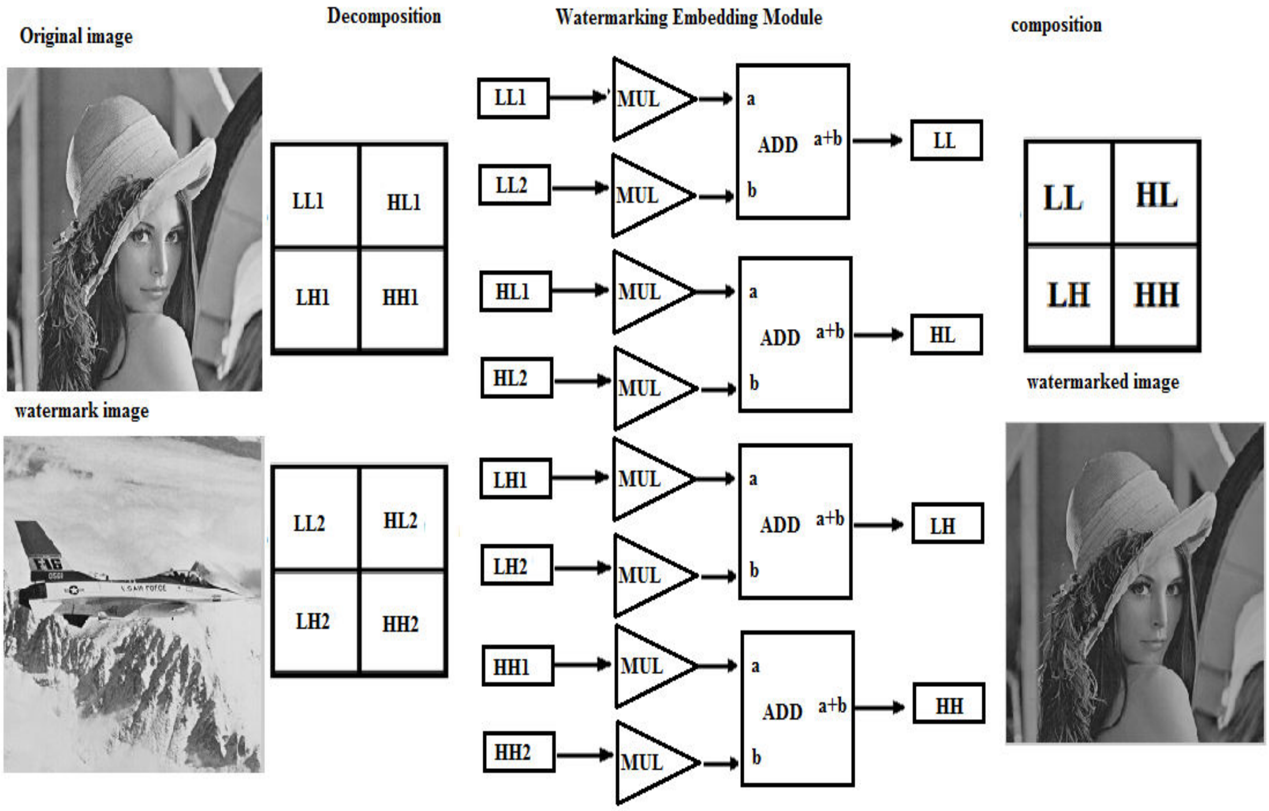
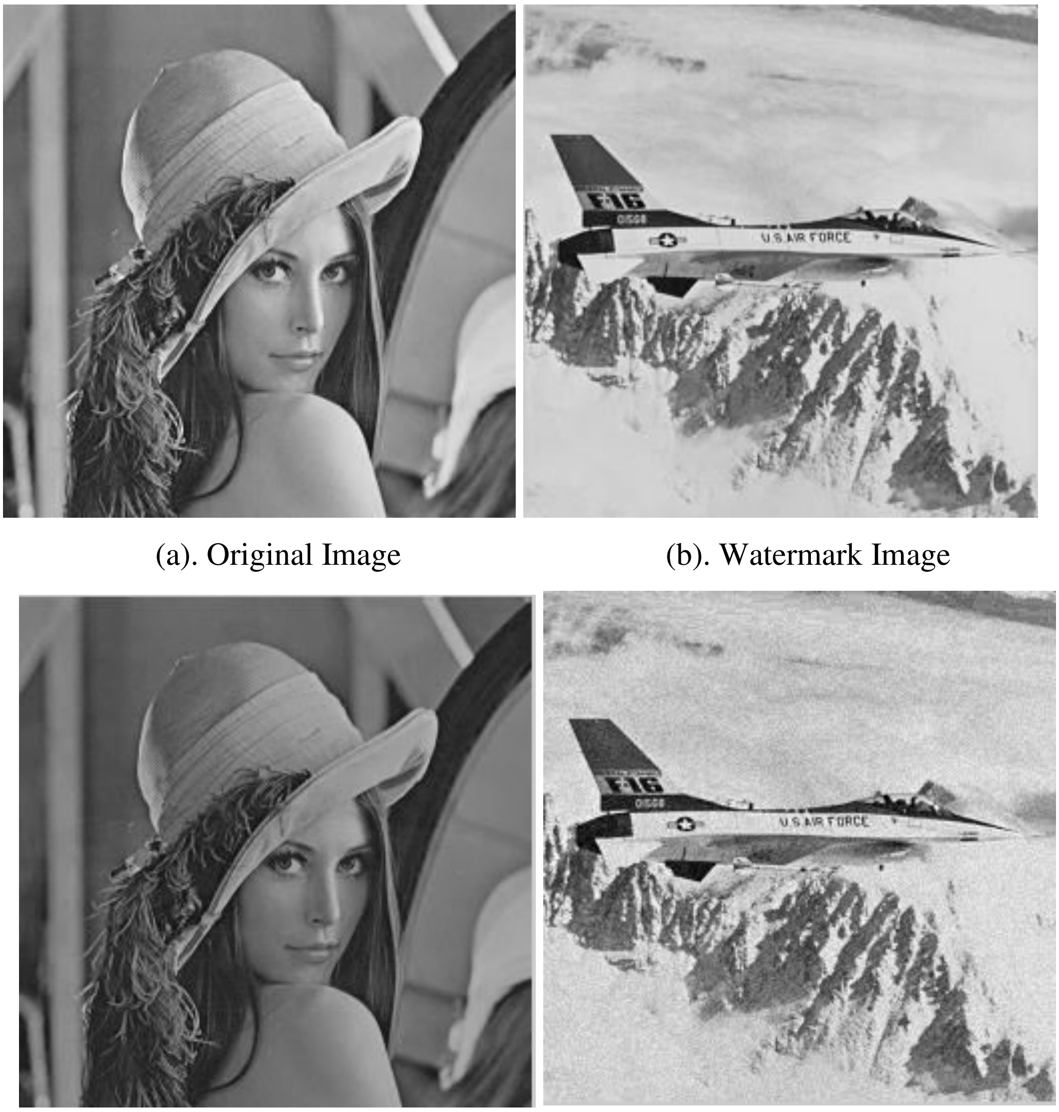


Figure 3.4. Procedure for watermarking

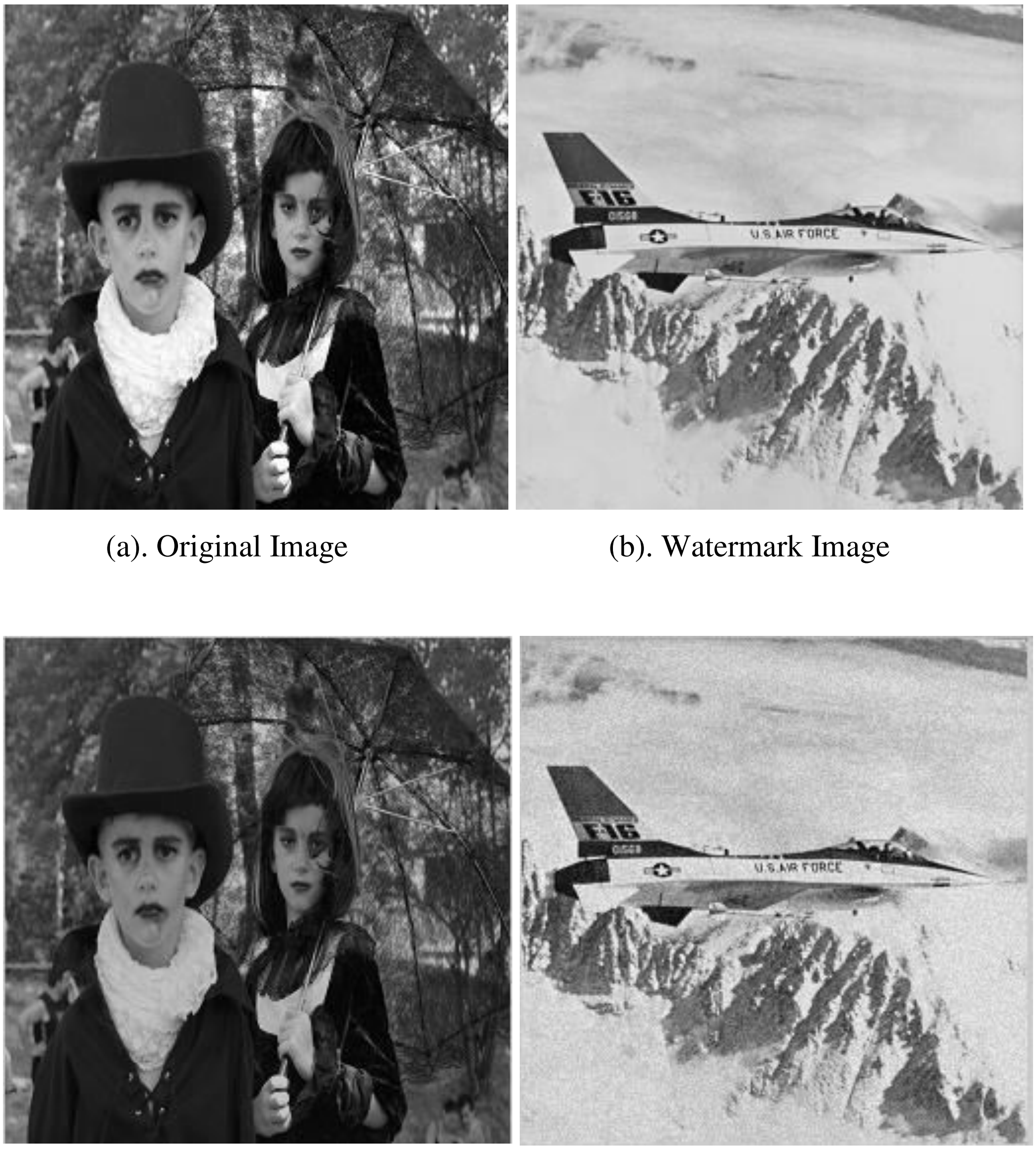
Another check register is used which indicates the completion of watermarking operation. Similarly extraction of watermark from the watermarked image is performed by taking watermarked image and the original image and just perform the compliment calculations on the sub-band values of LL, HL, LH and HH of the watermarked image and the original image with the help of adder/subtractor and the multiplier.



(a). Original Image (b). Watermark Image

(c).Watermarked image (d). Extracted Watermark

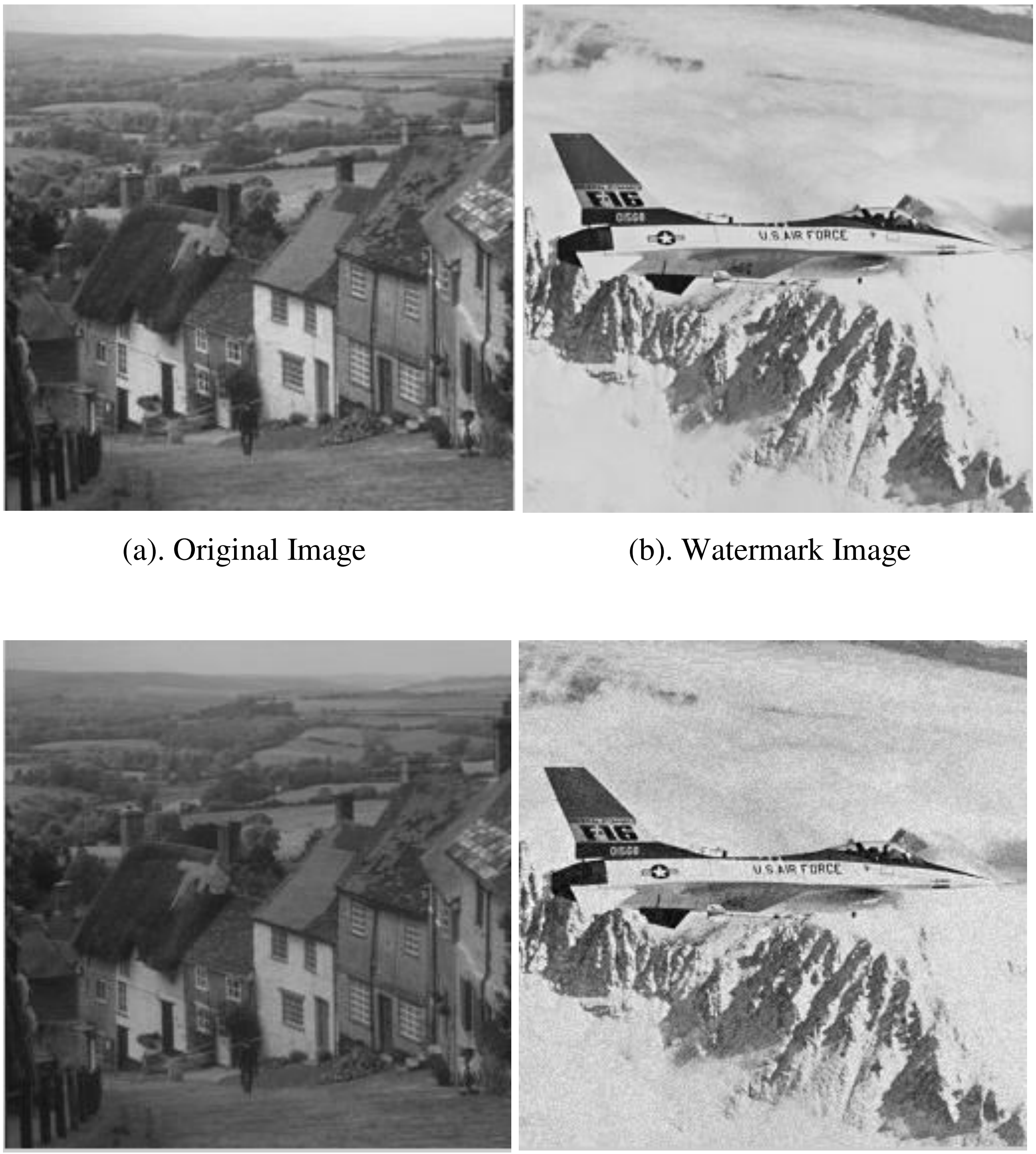
Figure 3.5 Image watermarking on “Lena.bmp”



(a). Original Image (b). Watermark Image

(c).Watermarked image (d). Extracted Watermark

Figure 3.6 Image watermarking on “kids.bmp”



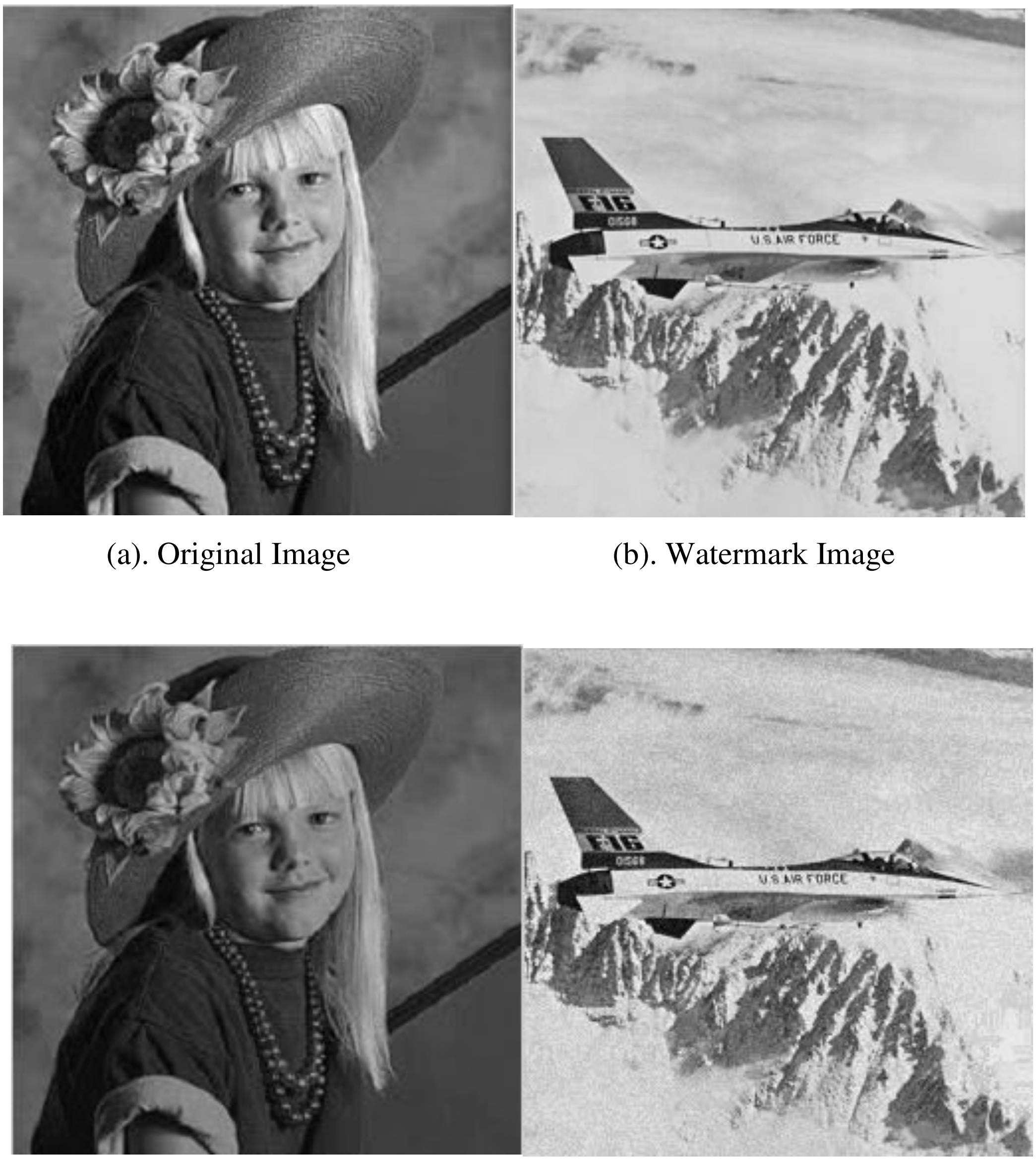
(a). Original Image

(b). Watermark Image

(c).Watermarked image

(d). Extracted Watermark

Figure 3.7 Image watermarking on “Goldhill.bmp”



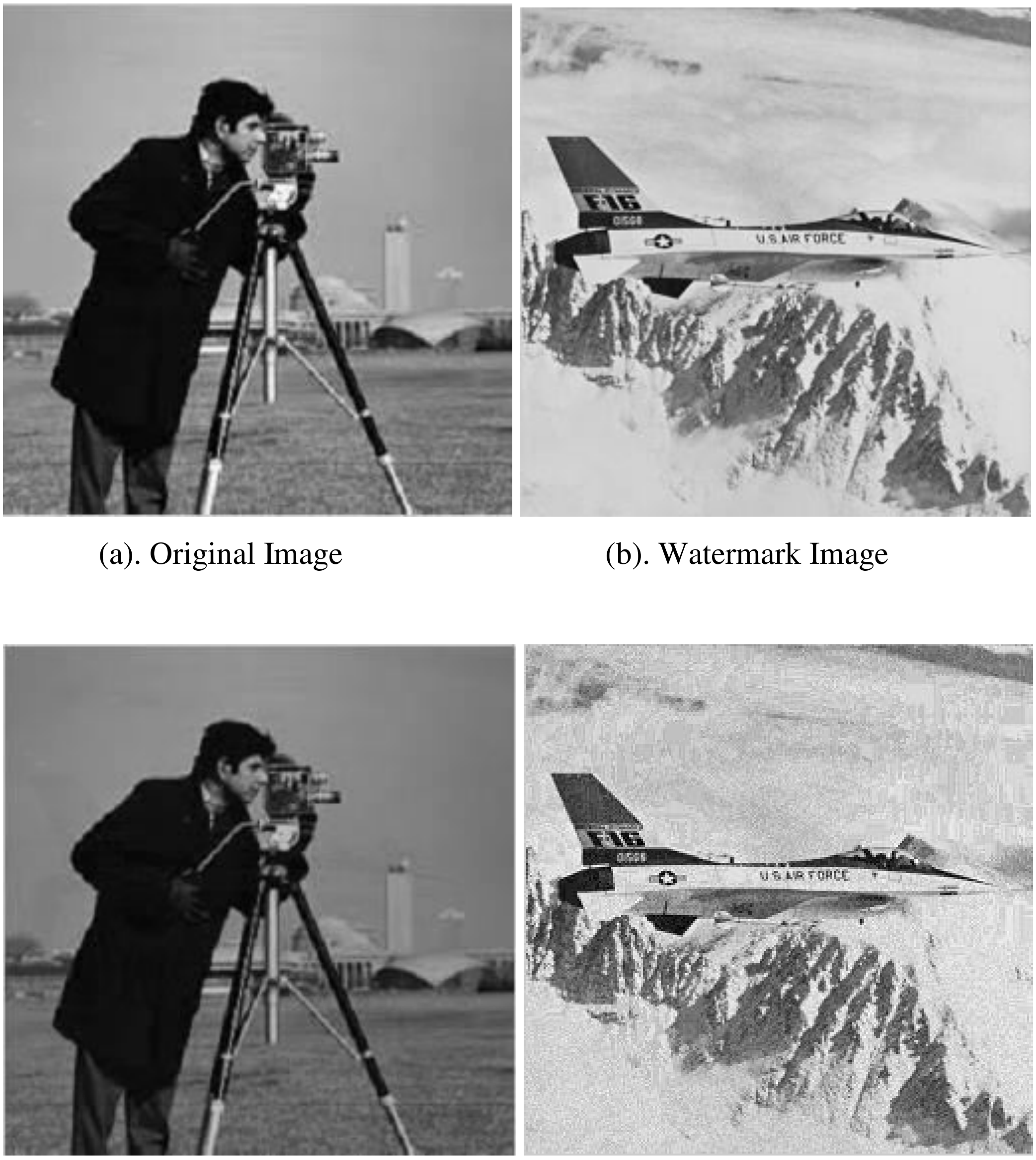
(a). Original Image

(b). Watermark Image

(c).Watermarked image

(d). Extracted Watermark

Figure 3.8 Image watermarking on “girl.bmp”



(a). Original Image (b). Watermark Image

(c).Watermarked image (d). Extracted Watermark

Figure 3.9 Image watermarking on “cameraman.bmp”

3.4. Comparison of watermarking on different images

Table 3.1. Comparison of watermarking on different images

S.NO.	COVER IMAGE /WATERMARK IMAGE	PSNR	SSIM
1.	LENA.BMP JETPLANE.BMP	18.9332 16.5825	0.9421 0.5282
2.	KIDS.BMP JETPLANE.BMP	18.1799 16.8260	0.9389 0.5186
3.	GOLDHILL.BMP JETPLANE.BMP	18.2101 16.8308	0.9229 0.5109
4.	GIRL.BMP JETPLANE.BMP	18.1628 16.8166	0.9369 0.5124
5.	CAMERAMAN.BMP JETPLANE.BMP	18.1403 16.8047	0.9354 0.5076

It is concluded that watermarking on Lena.bmp we obtain better results. The result obtain can be further optimized by taking higher values of constant coefficient considered.

Chapter 4

Conclusions and Future Scope of Work

CHAPTER-4.

4.1 Conclusions

An image contains of large amount of information or data for digital processing therefore we need fast and reliable processors. FPGAs are highly suitable for the processing of video and image applications used in broadcasting, biomedical imaging, high definition video conferencing, online security, video surveillance etc.

This thesis presents a successful Verilog implementation of invisible watermarking technique using discrete wavelet transform in which first level of decomposition and composition are applied by using Haar transform and then embeds the main watermark into the cover image. For encryption XOR operation is used.

In this HDL implementation of digital watermarking technique we took original cover image and watermark image in 256*256 Bitmap grey scale images.

4.2 **Advantages of watermarking using HDL:**

- As we are using DWT for embedding watermark in cover image which is more robust against many watermarking attacks.
- As we are implementing image watermarking in FPGA board which provides portability and availability.

- This HDL implementation can provide low power, reduce cost, and improve performance and productivity for important video and imaging applications.

4.3 Future Scope of Work

Watermarking is very popular in the field of research for copyright protection and authentication of important documents, images, audios and videos. For many years, research work in the field of data hiding is going on image watermarking implementation in an efficient manner.

The security of images are taken as major concern because it is easily available on internet, and do not provide any charges for their access, and they are required to be protected.

References

[1]. Md. Imroze Khan, S. Soni, B. Acharya, and S. Verma “IMPLEMENTATION OF DIGITAL WATERMARKING USING VHDL” Vol. 3, No. 1, January-June 2012, pp. 15-21

[2]. Frank Hartung and Friedhelm Ramme, “Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications”, *IEEE Communications Magazine*, Nov 2000, 38, No. 11. pp. 78-84.

[3]. Cayre F, Fontaine C, Furon T. “Watermarking Security: Theory and Practice”. *IEEE Transactions on Signal Processing*, 2005, 53 (10) : pp. 3976-3987.

[4]. Jiang Xuehua. "Digital Watermarking and its Application in Image Copyright Protection", 2010 International Conference on Intelligent Computation Technology and Automation,05/2010

[5]. Xiao-wei Zhang, Lin-lin Zhao, Zhi-juan Weng. “A Wavelet-Based Robust Watermarking Algorithm of High Credibility[J]”. *IEEE Trans. Proceedings of International Conference on Wavelet Analysis and Pattern Recognition*, 2009, pp. 298-302.

[6]. S. R. Subramanya and BYung. K. Yi. “Digital Rights Management”, *IEEE Potentials*, March-April 2006, 25, Issue 2, pp. 31-34.

[7]. Frank Hartung, Martin Kutter, “Multimedia Watermarking Techniques”,Proceedings of The IEEE, Vol. 87, No. 7, pp. 1085 – 1103, July 1999. pp. 1079 - 1107.

[8]. Ingemar J. Cox, J. P. Linnartz,“Some General Methods for Tampering with Watermarks” *IEEE Journal on Selected Areas in Communication*, 1998, 16(4): pp. 587-593.

[9]. R. C. Gonzalez and R. E. Woods, Digital Image Processing (2nd Edition). Prentice Hall, January 2002.

[10]. Bharatkumar Sharma. "Parallel discrete wavelet transform using the Open Computing Language: a performance and portability study", 2010 IEEE International Symposium on Parallel & Distributed Processing Workshops and Phd Forum (IPDPSW), 04/2010

[11]. C.S. Lu, H.Y.M Liao, “Multipurpose watermarking for image authentication and protection,” *IEEE Transaction on Image Processing*, vol.10, pp. 1579-1592, Oct. 2001.

[12]. Dixit, Arun, and Poonam Sharma. "A Comparative Study of Wavelet Thresholding for Image Denoising", International Journal of Image Graphics and Signal Processing, 2014.

[13]. Xiao-wei Zhang, Lin-lin Zhao, Zhi-juan Weng. “A Wavelet-Based Robust Watermarking Algorithm of High Credibility[J]”. *IEEE Trans. Proceedings of International Conference on Wavelet Analysis and Pattern Recognition*, 2009, pp. 298-302

[14]. Fleet D.J., “Embedding Invisible Information in Color Images”. *Proc. of ICIP*, 1997, (1) : pp. 532-535.

[15]. T. Dimitrios, N. Spiridon, D. Lambros. “Applying Robust Multibit Watermarks to Digital Images”. *Journal of Computational and Applied Mathematics*, 2009, 227 (2009): pp. 213-220.

[16]. Cox I.J., Killian J , Leighton T , et al. “Secure Spread Spectrum Watermarking for Images”, Audio and Video. *Proc. of IEEE ICIP,* Lausane, Switzerland, 1996, (3) : pp. 243-246.

[17]. G. Voyatzis, I. Pitas. “Protecting Digital Image Copyrights A Framework”, *IEEE Transactions on Computer Graphics and Applications*, 1999, 19(1): pp. 18-24.

[16]. Piyali Mandal, Ashish Thakral, Shekhar Verma, “Watermark Based Digital Rights Management”, *ITCC* 2005, pp. 74-78.

[17]. Digital Watermark Bender, Gruhl, Morimoto, and Lu (1996), “Techniques for Data Hiding”, *IBM Systems Journal*, 35, pp. 313-336

Thesis

[18]. Brigitte Jellinek, “Invisible Watermarking of Digital Images for Copyright Protection” submitted at University Salzburg, pp. 9 – 17, Jan 2000.

[19]. Harpuneet Kaur, “Robust Image Watermarking Technique to Increase Security and Capacity of Watermark Data”, submitted at Thapar Institute of Engineering & Technology , May 2006

[20]. Saraju Prasad Mohanty, “Watermarking of Digital Images”, Submitted at Indian Institute of Science Bangalore, pp. 1.3 – 1.6, January 1999.

Internet Links

[21] A. K. Vanwasi, “Digital Watermarking - Steering the future of security” Edition 2001, available at http://www.networkmagazineindia.com/200108/security1.htm

[22] “DIGITAL WATERMARK” available at http://www.ncd.matf.bg.ac.yu/casopis/05/Vuckovic/Vuckovic.pdf

[32] “Digital Watermarking” available at
http://en.wikipedia.org/wiki/Digital_watermarking

[33] “Fundamentals of Wavelets” available at
http://documents.wolfram.com/applications/wavelet/index2.html

[34] “MATLAB - The Language of Technical Computing” available at
http://www.mathworks.com/access/helpdesk/help/pdf_doc/matlab/getstart.pdf