CHAPTER I

INTRODUCTION

Now-a-Days due to the advancements taking place in communication technologies and abundant availability of internet, digital data can be transmitted at a faster rate with good quality. Hence protection of digital multimedia data such as movies, songs, pictures and photographs during storage, transmission, and processing has become a big challenge for the researchers. Digital watermarking **[Eleftherios K. Chrysochos, 2009]** paves the solution for this problem. It is a method of inserting digital information known as watermark into cover image results in watermarked image. During extraction, the inserted data can be extracted from the reconstructed image, which can be used for protecting digital content copyright and also ensures resistance against attacks. The watermark should be invisible, robust to geometric distortions and pixel modifications. Imperceptibility is an important characteristic of the watermarking process i.e. measure of visual similarity among the reconstructed and cover images. The process of watermarking can be also considered as the addition of noise into an image.

1.1.Watermarking Backgrounds

Keeping the digital data security in view few methods are developed for providing protection.

A. Encryption

The preliminary method used for data protection is “encryption”. It is a technique converts data into a scrambled unrecognizable code which can be communicated over a public /private network. It provides security for the data only between the sender and the receiver during the transmission. The disadvantage of this scheme is it fails to protect the data after reception and subsequent decryption. Hence unauthorized replication and subsequent transmission of data cannot be prevented.

B. Cryptography

Cryptography, the term *crypto means* secret and graphy means writing, it is the study of science to encrypt and decrypt data with the help of mathematics. It allows bidirectional communication between two people with each other securely and others will not be able to follow. A message, in the form of a plaintext is encrypted in such a way that information is hided and called ciphertext. The reverse process of obtaining original-text from the ciphertext is known as decryption.

C. Steganography

Steganography is a security scheme used to communicate secret information by embedding messages into an appropriate multi-media carrier such as audio, image and video. Only sender and receiver are aware about the presence of secret information. The aim of this method is to contain the hidden messages hence avoids suspicion and others attention. These schemes also allow secret point-to-point communication but they are prone to various attacks and less robust.

D. Watermarking

Digital watermarking [**[Y.Chang et al., 2012], [D.Sharma et al., 2015]]** is emerged to overcome the limitations of encryption schme used in cryptography and steganography techniques to embed the secret data. Compared to encryption, the watermark is embedded in its original form and doesn't prevent the users from watching, listening, viewing, or manipulating the content. Watermarking methods will establish the protection of the data from the un-authorized usage. In general, additional information is inserted as watermark into the original multi-media directly is valuable and useful.

1.2. Watermarking Method

Nowadays, role of internet was enhanced in the transmission of digital data. The use of internet during the transmission is to make the different problems by un-authorized use and change of the content. Multi-media offer several advantages especially such as high fidelity, simple to modify and more quality over analog media. Hence digital-media contents (audio, pictures, and video files) can be modified easily.

The ease of duplication and distribution of digital information needs effective copyright protection and to deal with the data integrity issues and to verify the accuracy, validity of the content authentication techniques are required. During the transmission over the internet security need to be ensured can be realized using watermarking.

Watermarking is a method of embedding additional information (in general treated as copyright) such as text, image, video, and audio known as watermark in to the contents of the digital multi-media data known as cover data. During the extraction, watermark can be extracted from watermarked image. Available software and hardware devices like camera, camcorder, printers, scanners and voice recorders are able to provide the faster communication are generated new challenges and opportunities to enable innovation in this area.

In case of invisible watermarking, watermark is not visual to view but some electronic-devices can retrieve the inserted information present in it is used to detect the owner. The watermark needs reliable detection and also robust against transformation due to image compression and cropping etc. Though stenography and watermarking both uses embedding data, steganography is used for communication between one point to the other point and also less robust to the attacks or data changes undergoes during transmission and storage. Where as watermarking is more robust against attacks. The working scheme of watermarking technique is same as the principle of the steganography. This process consists of two blocks such as embedding and extraction. The process can also provide with a key for further increase of security. The watermark embedding and extraction block diagrams are shown in as Figure 1.1-1.2 respectively.

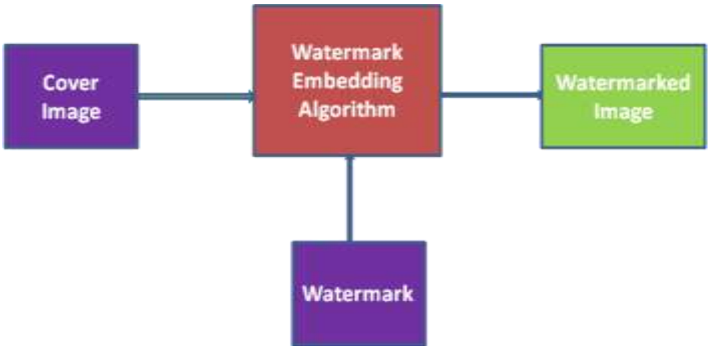


Figure 1.1 Watermark Embedding

For embedding, watermark and cover images are the inputs and watermarked image is the output. Watermark embedding is performed using Arnold transform.

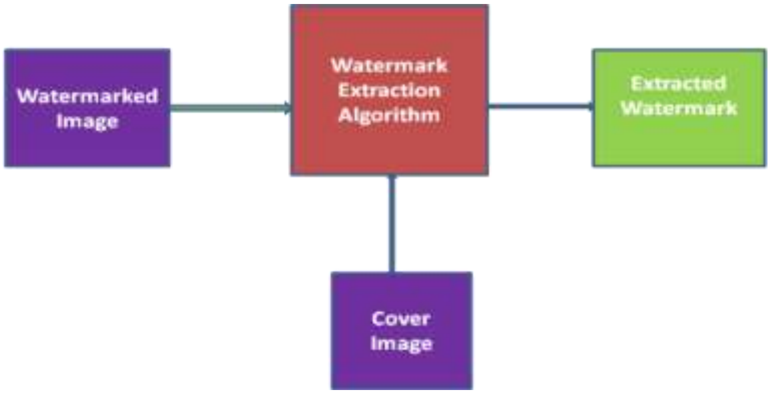


Figure 1.2 Watermark Extraction

In extraction, cover image and watermarked image are the inputs and output is the watermark. Extraction is performed using Arnold transform. In general, the overall watermarking process comprises three blocks such as watermark generation, embedding, and extraction for authentication and detection. The frame- work of watermarking is shown in Figure 1.3.

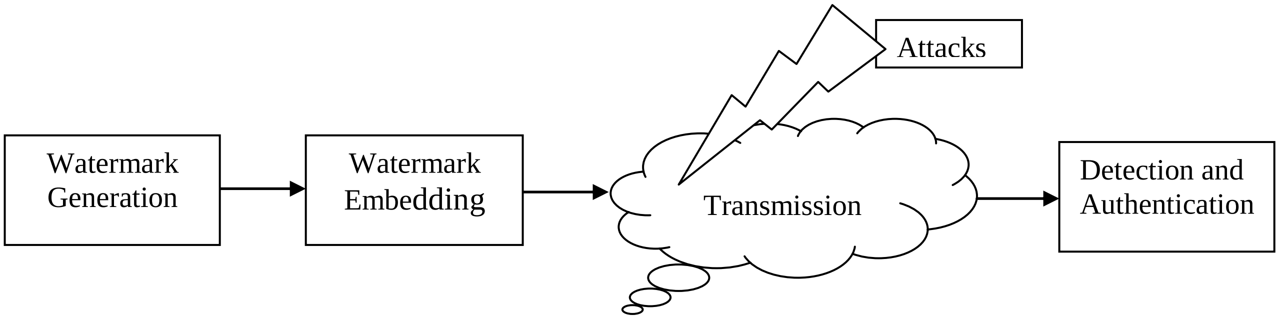


Figure 1.3 General Framework of Watermarking

Watermark is generated in such a way that its content is unique, complex and useful, difficult to disturb by the attackers. The embedding algorithm should insert the watermark in a host without disturbing the visibility of the host and at the same time difficult to locate and extract or destroy the inserted watermark for an attacker. The watermarked image at the receiver is subjected to unpredictable distortions or attacks in the communication-channel during transmission. Few of them may be un-intentional such as image compression and channel noise. The other intentional distortions are object replacement, insertion and removal etc.

Attackers would like to operate the original image I_o to remove watermark to realize their unethical intentions. The watermarked image I_{wm} is received at the receiver, which might have been tampered and therefore different from I_o. Usually, the algorithm of watermark extraction is an inverse scheme of the algorithm of embedding. There are two different types of watermark extraction methods are blind and non-blind. The cover image doesn’t need in the blind method for extraction where as it is needed in the second method called non-blind watermarking. If there are some changes happen to the transmitted image known as an attack.

1.3. Applications of Watermarking

A. Owner Identification

Identification of a owner for a particular digital video, image, song or text is an important aspect, but it is very difficult to include copyright for every item. Hence, this issue can addressed by watermarking, embedding the watermark into the image or the song itself which can be used for the owner identification in place of copy-right with each image/song.

B. Copyright Protection

Data copying can be prevented by adding a security bit to it. When the device tries to read the data the detecting circuit recognizes the security bit and stops recording the data. This would need all the copying machines need to have detection circuitry to track security bit and act-accordingly.

C. Broadcast Monitoring

Broadcast-monitoring is one of the prime applications of watermarking. Many of the advertising companies monitor their commercial paid air time of their products by using watermarking. Hence advertisements are watermarked by placing a single watermark during each video/sound-clip prior to the telecast. Monitoring schemes check for these watermarks, recognize the products based on watermark detection.

D. Finger-Print Authentication

Unauthorized copies of a document can be tracked/ detected by using fingerprint technique. Each copy of a document is watermarked with a unique code sequence. Any illegal copies of the document can be easily tracked by comparing the unique code sequence inserted into it.

E. Data Authentication

Maintenance of data truthfulness and avoidance of attacks on data can be performed by inserting watermarks in an image. Data (images) can be easily tampered even without being detected.

F. Medical Applications

Due to telemedicine, need of watermarking is very much enhanced in medicine. Addition of patient details as watermark reduces many complications while data transmission between clinical centers.

1.4. Watermarking Properties

Watermarking system has to satisfy some important properties like effectiveness, fidelity and robustness etc.

A. Effectiveness

It is the probability of the reconstructed image that will be correctly detected and is equal to 1 in an ideal case.

B. Image Fidelity

Watermarking scheme changes the cover image quality due to the addition of watermark which can be treated as a noise. But it should not degrade the quality much and hence less image fidelity changes are expected.

C. Robustness

It is an important aspect in watermarking. In general, watermarked image will distort during transmission over a lossy channel or due to attacks. Hence watermark will be removed or non-detectable. A robust watermark shall be able to withstand to attacks such as cropping, rotation, Gaussian-noise, scaling, and compression etc.

1.5. Watermarking - Classification

Watermarking schemes are classified into various groups based on domain, watermark type, visibility and extraction mechanism **[S.Voloshynovskiy et al., 2001]**. Classification of watermarking schemes is shown in Figure 1.4.These schemes are categorized into spatial and frequency domains based on the domain. Reconstructed image is straightly replaced by the image elements in spatial domain. Transform domain watermarking schemes provide few transforms such as FFT, DFT, DCT, and DWT. Spatial domain methods are not robust because the pixels of the watermark embedded can easily modified. Where as in the frequency domain techniques the watermark image gets distributed over the entire image hence it is robust to attacks and hence secure.

Watermarking techniques are categorized into text, video and audio depends up on the type of the multimedia information used. In our thesis we focused on invisible watermarking technique where the watermark is invisible to user and more secure than the visible watermarking technique. Invisible watermarks can be fragile or robust. In robust algorithm, watermark is not distorted due to attacks such as filtering, compressions, noise and cropping.

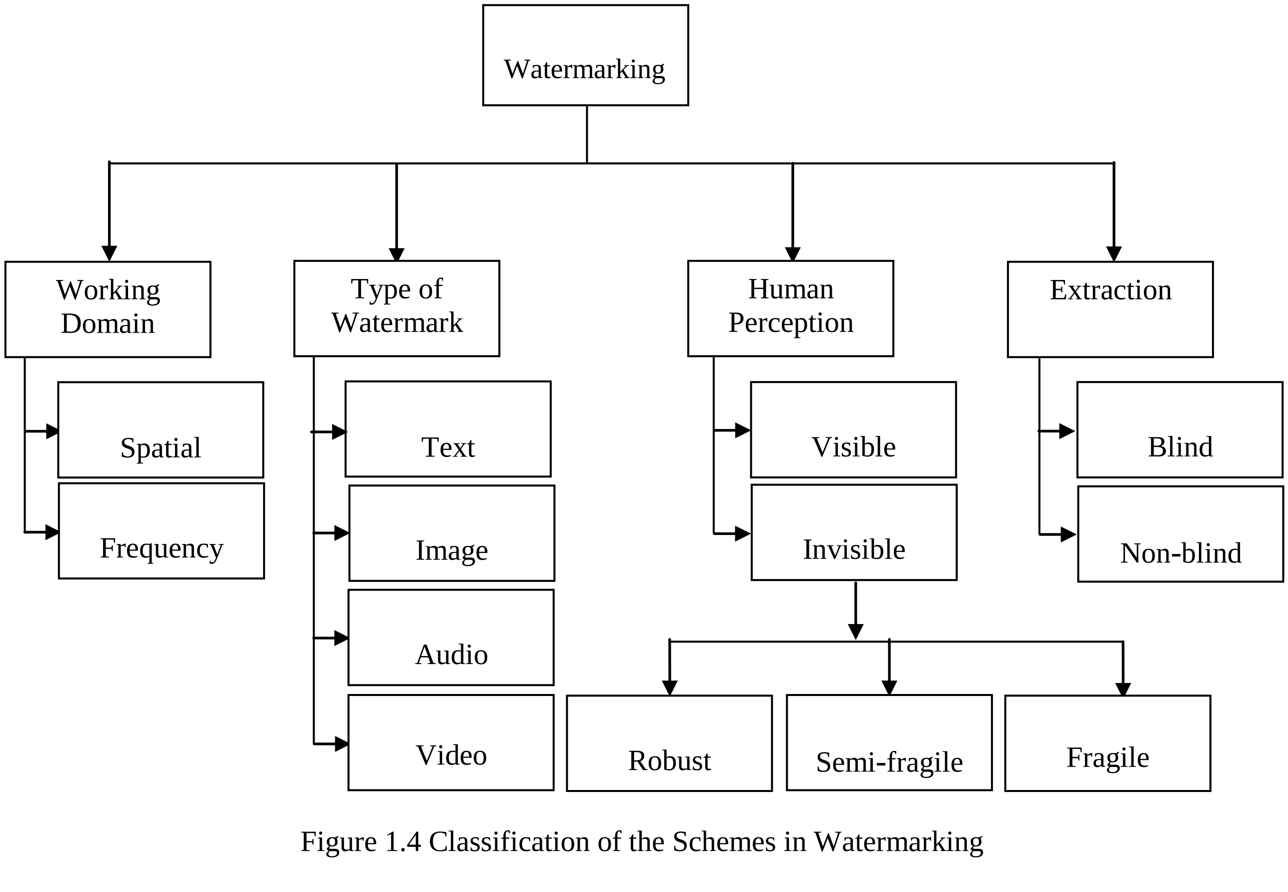


Figure 1.4 Classification of the Schemes in Watermarking

Watermarking techniques can be classified into two types such as visible and invisible watermarking depends up on the perceptibility.

The classical approach of the visible watermarking is shown in Figure 1.5a. The characters

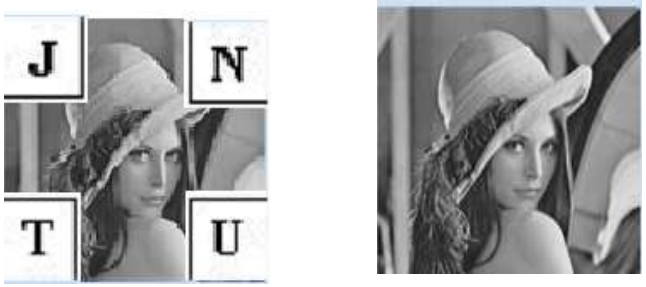


Figure 1.5 (a) Visible Watermark (b) Invisible Watermark

"J, N, T, U" is visible in that the sender wants others to know. In invisible watermarking, the cover and reconstructed images are not differentiable in Figure 1.5b. This watermark is not identified with a human eye.

1.6. Transform Domain Methods

In general transforms like SVD, DCT, DWT, CT etc. are applied on cover image and watermark is inserted into the transformed coefficients. Now-a-days hybrid transforms i.e. combination of two or three transforms such as DCT-SVD, DWT-SVD, DWT-DCT, CT-SVD, CT-DCT, and DWT-DCT-SVD are preferred to enhance robustness. The transforms DCT, DWT, SVD and CT are explained below:

1.6.1. Discrete Cosine Transform (DCT)

It's a real part of DFT in which the cosine components have been present sine terms are eliminated. The image is decomposed into small squares of size 8 x 8 pixels as shown in Figure 1.6 and transform is computed for each. For example, an image is decomposed into the square window with size of N x N dimensions, the mathematical expression for the representation of DCT, the representation of forward transform is as follows

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (1.1)$$

for $u = 0, 1, 2, \ldots, N-1$ and $v = 0, 1, 2, \ldots, N-1$

$$\alpha(u) = \sqrt{\frac{I}{N}} \quad for\ u = 0 \quad and \quad \alpha(u) = \sqrt{\frac{2}{N}} \quad for\ u = 1, 2, \ldots\ldots, N-1$$

$$\alpha(v) = \sqrt{\frac{I}{N}} \quad for\ v = 0\ and \quad \alpha(v) = \sqrt{\frac{2}{N}} \quad for\ v = 1, 2, \ldots\ldots, N-1$$

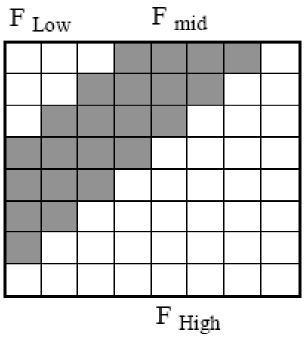


Figure 1.6 DCT Coefficients of 8X8 Block

The inverse transform can be expressed as

$$f(x,\ y) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} \alpha(u)\alpha(v)C(u,v)\, cos\left[\frac{(2x+1)u\pi}{2N}\right] cos\left[\frac{(2y+1)v\pi}{2N}\right] \qquad (1.2)$$

for x = 0, 1, 2,…, N−1 and y = 0, 1, 2,…, N −1.

1.6.2. Discrete Wavelet Transform (DWT)

In 2-D Wavelet Transforms, three 2D wavelet $\Psi^H(m,\ n)$, $\Psi^V(m,\ n)$, $\Psi^D(m,\ n)$ and 2-D scaling function $\mu(m, n)$ are considered for product of a 1-D corresponding wavelet Ψ and scaling function μ.

$$\mu(m,\ n) = \mu(m)\mu(n) \qquad (1.3)$$

$$\Psi^H(m,\ n) = \Psi(m)\mu(n) \qquad (1.4)$$

$$\Psi^V(m,\ n) = \mu(n)\,\Psi(m) \qquad (1.5)$$

$$\Psi^D(m,\ n) = \Psi(m)\,\Psi(n) \qquad (1.6)$$

Ψ^Hrespond to changes along horizontal edges as columns , Ψ^Vcorrespond to changes along vertical edges as rows, and Ψ^D measures changes along diagonalsThe filter bank in single-scale can be iterate by applying an approximate output to input of other to generate an arbitrary scale domain as shown in Figure 1.7.

Image *f* (*m*, *n*) is used as the first scale input and outputs are four quarter-size sub-images denoted as W_ϕ, W_ψ^H, W_ψ^V, and W_ψ^D.

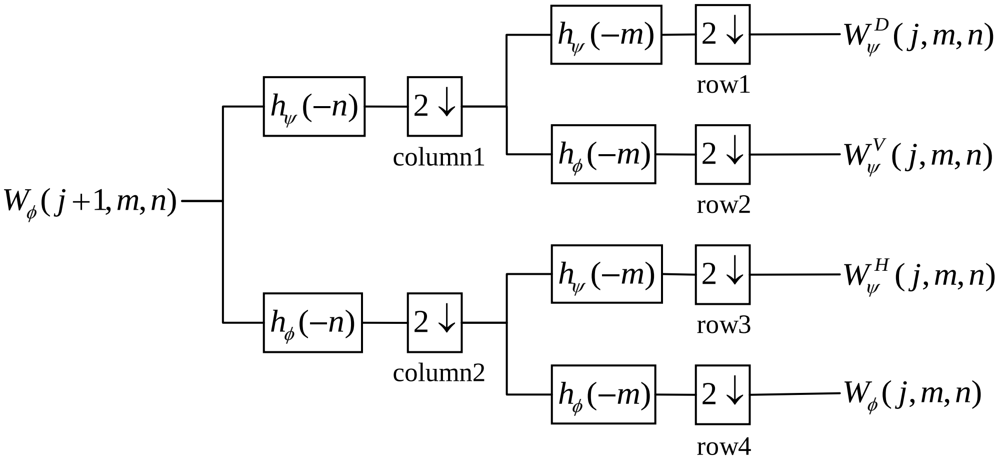


Figure 1.7 Analysis of Filter-Bank in 2D FWT

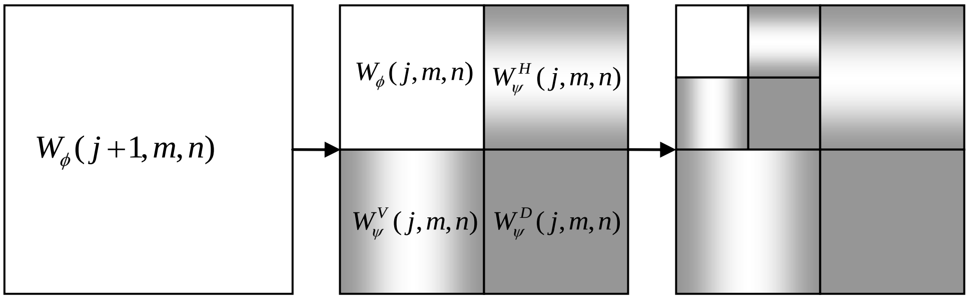


Figure 1.8 Two-scale 2D Decomposition

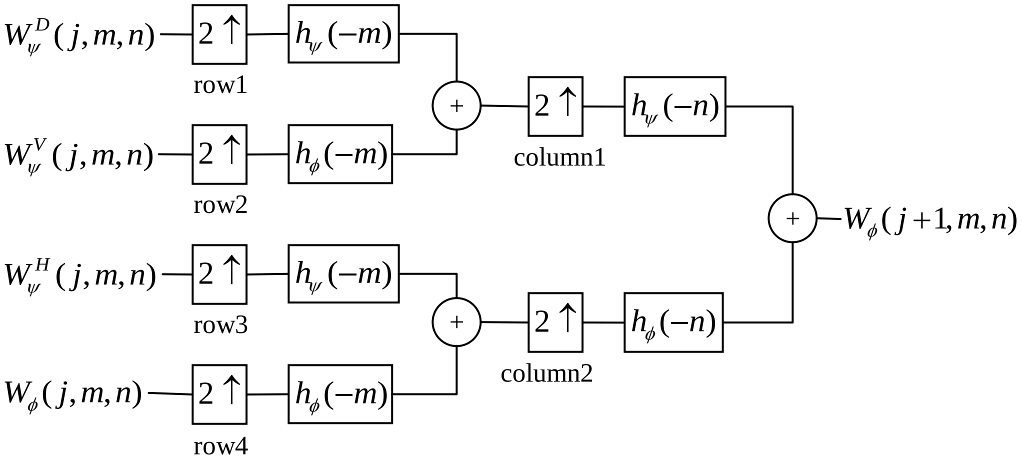


Figure 1.9 Synthesis of Filter-Bank in 2D FWT

The sub-images are following at middle and two iterations of filtering scheme generate two-scale decomposition at the right of Figure 1.8. This synthesis filter-bank is shown in Figure 1.9 that describes the inverse process. The mathematical expressions are used for the representation of DWT in 2-D as approximate and detailed coefficients.

The forward 2-D wavelet transform as follows for approximate coefficients

$$w_{\emptyset}\ (k_0, u, v) = \frac{1}{\sqrt{MN}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} f\ (m, n)\ \emptyset_{k_0,i,j}\ (u,\ v) \tag{1.7}$$

Where *u = 0, 1, 2,……., M-1* and *v = 0, 1, 2,……., N-1.*

Forward 2-D wavelet transform of is as follows for detailed coefficients

$$\mathrm{w}_{\varphi}^{\mathrm{i}}\ (\mathrm{k}_0, \mathrm{u}, \mathrm{v}) = \frac{1}{\sqrt{MN}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} f\ (m, n) \quad \varphi^{i}{}_{k_0,u,v}(u, v) \tag{1.8}$$

Where *u = 0, 1, 2,…….M-1* and *v = 0, 1, 2,…….N-1.*

Inverse DWT can be expressed as follows

$$f\ (m, n) = \frac{1}{\sqrt{MN}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} w_{\emptyset}\ (k_0, u, v)\ \emptyset_{k_0,u,v}\ (m, n) + \frac{1}{\sqrt{MN}} \sum_{d=H,V,D} \sum_{a=k_0}^{\infty} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} w_{\varphi}^{i}\ (k_0, u, v) \quad \varphi^{i}{}_{k_0,u,v}(u, v)$$

where *m = 0, 1, 2,…….M-1* and *n = 0, 1, 2,…….N-1.* (1.9)

A 2-D transform can be computed by using 1-D to all rows of input and next all columns repeatedly. Four transform coefficient sets (LL, HL, LH, and HH) are generated by applying single-level 2-D wavelet to an image as shown in Figure 1.10.In which, A filter (either a LPF or HPF) is applying to the rows and columns denoted as the first and second letters respectively.

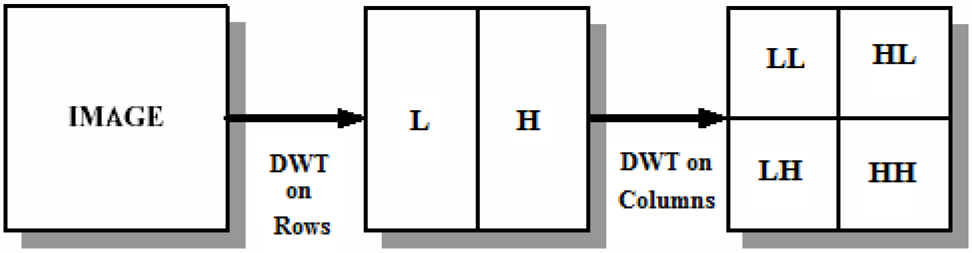


Figure 1.10 Decomposition of the Single-Level 2D- DWT of an Image

An image is partitioned in to two parts low-and-high frequencies. The high-frequencies are largely located at the edge of an image. The portions of the low frequency components are decomposed in to two square windows of low and high frequencies. The image has been completely decomposed into appropriate sub bands in the continued watermarking process, which is in Figure 1.11.

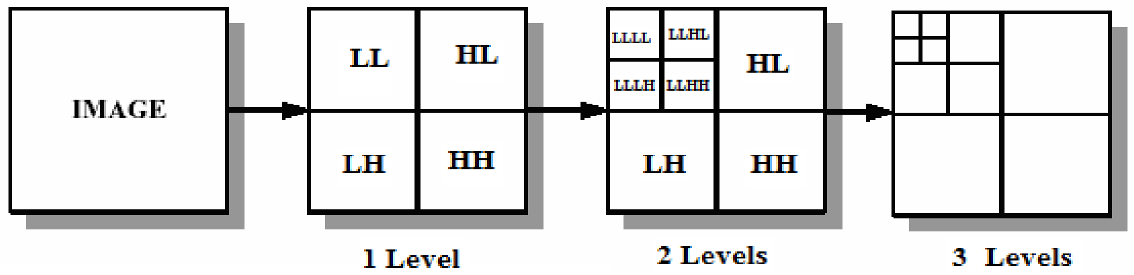


Figure 1.11 Level Decomposition of an Image

A data structure is generated by the wavelet called scale-space representation. In which low and high frequency signals are precisely located in frequency and pixel domains respectively. The increase in frequency causes to increase in the spatial resolution, but the frequency in DCT domain is independent of the frequency resolution. The sharp edges are localized in spatial region, which consist of high frequency content significantly, can be seen in the detail sub-bands of an image and form the contours.

1.6.3 Singular Value Decomposition (SVD)

It is a kind of a non-negative real-matrix provided for matrix- diagonalization. The image is represented with an orthogonal transforms. Assume S be an image with size of P×Q. The matrix of SVD (S) can be expressed as

$$\mathrm{S}= M\ R\ N^{T} \qquad (1.10)$$

$$S = [m1 \quad m2 \quad \ldots \quad \ldots \quad m\mathrm{P}]\begin{bmatrix} \sigma 1 & & & \\ & \ddots & & \\ & & \ddots & \\ & & & \sigma Q \\ & & & & 0 \end{bmatrix}\begin{bmatrix} n1 \\ n2 \\ \vdots \\ \vdots \\ nP \end{bmatrix} \qquad (1.11)$$

$$S = \sigma_1 m_1 n^T{}_1 + \sigma_2 m_2 n^T{}_2 + \ldots + \sigma_q m_q n^T{}_q \qquad (1.12)$$

Where q shows rank of matrix R, M and N are unitary orthogonal-matrices, it represents details of the geometry in the cover image. *R is* a diagonal matrix with $P\times P$ *size.* Each pixel in R is a descending order of non-negative values. An image can be viewed as a sum of N Eigen values. σ_i indicates the value of singular corresponding Eigen image, which shows the brightness of energy.

In which, each singular value shows that the perception of the layer of an image, hence the specifying couple of singular vectors indicates that an image- geometry. This transform is applying to complete cover image and vary all singular values to insert watermark in a common approach of SVD-based watermarking. A main property of this scheme is to change very little in all the modified singular values of each attack. The singular values of watermark are inserted in an original object as the expansion of this property.

1.6.4. Contourlet Transform (CT)

It is a novel multi-scale and geometrical transform. It can acquire efficiently the edge information of all directional representation of images **[Do and Vettori et al., 2013]**. The proposed contour-let is to overcome the limitation dealing with curved parts.

This transform consist two important blocks such as Laplacian Pyramid (LP) and Directional Filter-Bank (DFB). Pyramid block is built by using a twin filters known as analysis- and -synthesis filters. This window produces a low frequency sub-band image at each level and it is decomposed an image in to octave radial-like frequency bands to acquire point-discontinuities and the difference between prediction and original to form a band-pass image (BPI) in its result. These BPIs are forwarded from the pyramidal partition to the filter-bank.

In the filter bank, a directional decomposition is accomplished and two-channel quincunx filter- bank (QFB) is used for partition of each BPI in to horizontal and vertical directions, acquiring directional-data. It divides each detail-band in to several directions, it is evaluated in terms of a power of 2, to join all these discontinuities for the formation a linear- structure Figure 1.12.

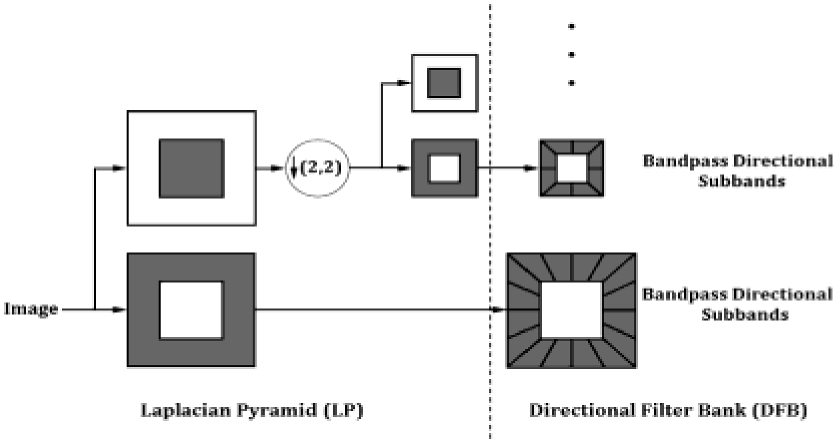

(2,2)
Bandpass Directional Subbands
Image
Bandpass Directional Subbands
Laplacian Pyramid (LP)
Directional Filter Bank (DFB)

Figure 1.12 LP and DFB parts of the CT

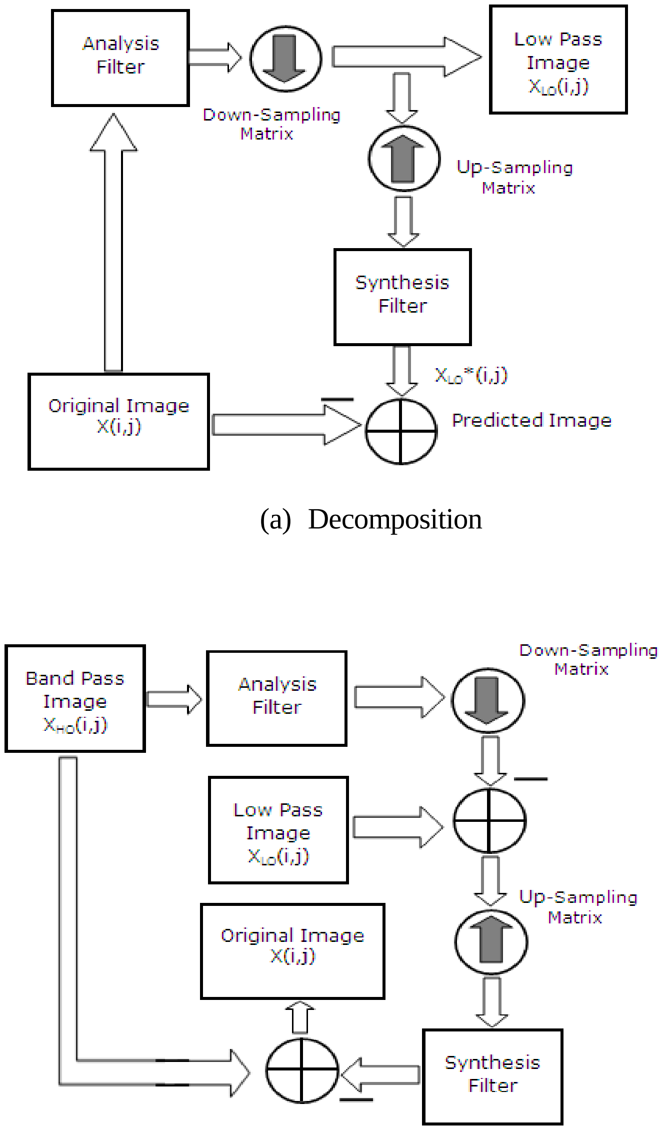
The CT makes better than the popular DWT due to inherent properties of directionality and anisotropy, LP and DFB are combined together is called the pyramidal- directional filter-bank (PDFB). In which, for ladder structure the pyramidal filters and directional filters are considered. Hence, The DFB decomposition has been taken to be four from course to finer scale at each pyramidal level specifically.

In this transform, high-frequency sub-band is obtained by G-filtered low-frequency sub-band subtracting from cover image. Low-frequency coefficients are affected by changing of high-frequency coefficients due to the properties of Laplacian. It is clearly distinct from the wavelet transform. In case of wavelet, high-frequency sub-band is produced by using high-pass filtering to cover image.

Hence low-frequency coefficients are not affected by changing high-frequency coefficients due to no spreading-effect of Laplacian in the wavelet. The inserted watermark is doubted to low-pass filtering and compression attacks, which collapse the high-pass coefficients of an image.

In contrast, if watermark is inserted in to more detail sub-bands of contour-let, it is interest to be spread-out in to all sub-bands for the reconstruction of watermark. Thus watermarking technique in this transform method may be robust to spectral attacks broadly resulting from high and low frequencies image processing.

On peppers image, this transform is using two pyramidal levels and these are again partitioned in to four and eight directional sub-bands. Large and small coefficients are represented in white and black respectively. This transform arranges successive filtering for spatial as well as directional resolution.



(a) Decomposition

(b) Reconstruction

Figure 1.13 Decomposition and Reconstruction of Single Level of Pyramid.

These properties of contour-let are useful to detecting image locations, in which the watermark can freely be hidden. This research work takes the benefit of the features and inserts watermark in contour-let coefficients of an image.

The second level of ladder based filter bank structures is useful in generating sparse expansion of typical images contain smooth contours. The point-discontinuities are caring by Pyramidal filter bank (PFB) depend up on Laplacian hence joining of all the points to linear-structures is reached through DFB. PFB is the first stage of the PDFB of the contour-let, output of which is forwarded to DFB in cascade as shown in Figure 1.12.

In the pyramidal stage of an image, it is down- sampled to produce low-pass image. Hence the error in prediction is considered as the un-correlated BPI in eq1.13. as the difference of the cover and the predicted images. This can be continued by applying iteratively on $F\mathrm{L}_0(m, n)$ to get $F\mathrm{L}_1(m, n)$, $F\mathrm{L}_2(m, n)$, ... $F\mathrm{L}_N(m, n)$ as shown in Figure 1.13(a). The mathematical expressions are used to form the reconstruction from the BPI image is shown in Figure 1.13(b).

$$FH_0(m, n)= F(m, n)- F^{*}L_0(m, n) \tag{1.13}$$

Where $F(m, n)$ shows the cover image, $F\mathrm{L}_0(m, n)$ represents the low-pass image, $F^{*}L_0(m, n)$ denotespredicted image, $FH_0(m, n)$ indicates band-pass image reconstruction and N represents number of the pyramidal level. The BPI FH_0(m, n) generated through pyramidal-decomposition in next-stage is forwarded by DFB, all of them together to form PDFB of the contour.

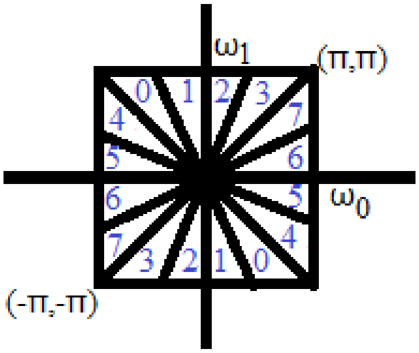


Figure 1.14 Frequency Partitioning of DFB

The directional bank is designed by arranging r-level binary-tree partition, which leads to 2^r squared windows to acquire high- frequency using QFB and fan filters with 8 Sub-bands for r = 3 as shown in Figure 1.14.

1.7. Motivation

People living in rural and remote areas are struggling with medical care, good-quality specialty medical systems and specialist physicians. Telemedicine is communicating clinical centers to hospitals.

Tele is a Greek word distance and *mederi* is a Latin word to heal. i.e. healing by wire is referred futuristic with “experimental” but today has a variety of applications in patient care and public health.

The following issues present in the medical domain motivated us to work in this research area.

i. Preserving the security and authenticity of medical images, while distributing the medical images between hospitals due to an ever-increasing demand for telemedicine.

ii. Providing imperceptibility and security for patient information due to the usage of EHR is a big challenge.

iii. While transmission protecting the medical data against various attacks such as filtering, compression, noise, and cropping is still a problem.

1.8. Thesis Organization

Chaper1 covers the introduction of watermarking. Remaining thesis was organized as follows. Chapter2 describes the literature review done while carrying out the research. Chapter3 deals with the two proposed transform based methods. Chapter4 discusses about the benchmarking of the proposed methods by applying geometrical and pixel modification attacks.Chapter5 deals with the application of algorithm to single modal medical images.Chapter6 deals with the Multi modal medical imaging applications. Chapter7 deals with Conclusions of the work.