CHAPTER 1

INTRODUCTION

Since ancient times, there has been an effort to hide information within seemingly harmless information to avoid unwanted attention. The science of concealing information was later to be known as “steganography” and the current technology of “Digital Watermarking” has taken its root from it. The term “watermark” in terms of digital data was taken from the concept of watermarks used to prevent faking of currency notes.

In recent years, with the rapid and extensive growth in internet technology the distribution of works of art, including pictures, music, video and textual documents, has become easier. Digital forms of these media (still images, audio, video, text) are easily accessible. This is clearly advantageous, in that it is easier to market and sell one's works of art. However, this same property threatens copyright protection. Digital documents are easy to copy and distribute, allowing for pirating.

There are a number of methods for protecting ownership. One of these is known as digital watermarking. “Watermarking” deals with embedding information like name of the creator, status, recipient, etc. into the host data in such a way that it remains transparent or undetectable. The watermark information should be embedded in such a way that this should not be detectable and removable even after many spurious or innocuous attempts. Watermarking can be done for any form of digital data – text, image, audio, or video where copyright needs to be protected. Methods for embedding watermark information may vary between types of media, but the basis of these methods remain more or less same.

A watermark is a digital data embedded in multimedia objects such that the watermark can be detected or extracted at later times in order to make an assertion about the object. The main purpose of digital watermarking is to embed information imperceptibly and robustly in the host data. Typically the watermark contains information about the origin, ownership, destination, copy control, transaction etc. Potential applications of digital watermarking include transaction tracking, copy control, authentication, legacy system enhancement and database linking etc. With the increasing availability of digitally stored information and the development of new multimedia services, security questions are becoming even more urgent. The acceptance of new services depends on whether suitable techniques for the protection of the work providers' interests are available.

A watermark can carry any information you can imagine but the amount of the information is not unlimited. The more information a watermark carries the more vulnerable that information is. This amount is absolutely limited by the size of particular video sequence. Watermarking prefers robustness to capacity, thus a watermark typically carries tens to thousands of hidden information bits per one video frame.

1.1 Requirements of Watermarking

A digital media in its journey, from the content creator's studio to the end user, undergoes several phases of changes – analog to digital, digital to analog, transform based signal processing, coding, decoding, packetisation, fragmentation, and so on. The selected Watermarking method for embedding information has to be very effective such that the hidden information is never detectable and removable under any condition during these several cycle of changes.

Requirements for Watermarking methods can be generally classified as below:

a) Unobtrusive
b) Transparency
c) Security
d) Ease of embedding and retrieval
e) Robustness
f) Effect on bandwidth
g) Interoperability

a) Unobtrusive: the watermark should be perceptually invisible.

b) Transparency: The most fundamental requirement for any Watermarking method shall be such that it is transparent to the end user. The watermarked content should be consumable at the intended user device without giving annoyance to the user. Watermark only shows up at the watermark-detector device.

c) Security: Watermark information shall only be accessible to the authorized parties. Only authorized parties shall be able to alter the Watermark content. Encryption can be used to prevent unauthorized access of the watermarked data.

d) Ease of embedding and retrieval: Ideally, Watermarking on digital media should be possible to be performed "on the fly". The computation need for the selected algorithm should be minimum.

e) Robustness Watermarking method should be capable of extracting the watermark even after attacks: Watermarking must be robust enough to withstand all kinds for signal processing operations, "attacks" or unauthorized access. Any attempt, whether intentional or unintentional, that has a potential to alter the data content is considered as an attack. Robustness against attack is a key requirement for Watermarking and the success of this technology for copyright protection depends on this.

f) Effect on bandwidth: Watermarking should be done in such a way that it doesn't increase the bandwidth required for transmission. If Watermarking becomes a burden for the available Bandwidth, the method will be rejected.

g) Interoperability: Digitally watermarked content shall still be interoperable so that it can be seamlessly accessed through heterogeneous networks and can be played on various play-out devices that may be watermark aware or unaware.

1.2 Principles of watermarking

As an emerging technology, digital watermarking involves the ideas and theories of different subject coverage, such as signal processing, cryptography, probability theory and stochastic theory, network technology, algorithm design, and other techniques. Digital watermarking hides the copyright information into the digital data through certain algorithm. The secret information to be embedded can be some text, author‘s serial number, company logo, images with some special importance. This secret information is embedded to the digital data (images, audio, and video) to ensure the security, data authentication, identification of owner and copyright protection. The watermark can be hidden in the digital data either visibly or invisibly. For a strong watermark embedding, a good watermarking technique is needed to be applied. Watermark can be embedded either in spatial or frequency domain. Both the domains are different and have their own pros and cons and are used in different scenario.

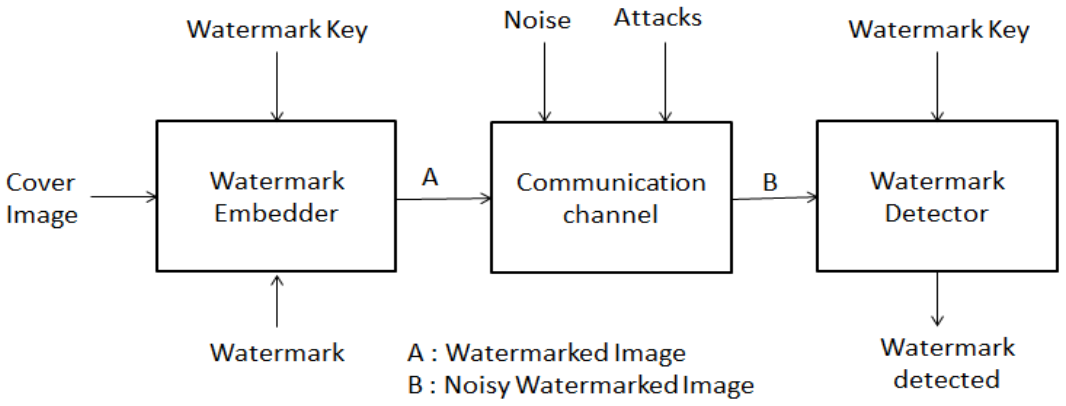


Figure 1: Digital watermarking system

1.3 Structure of a typical watermarking system:

Every watermarking system consists of at least two different units:

i. The watermark embedding unit

ii. The watermark extraction unit

Watermark Embedding process:

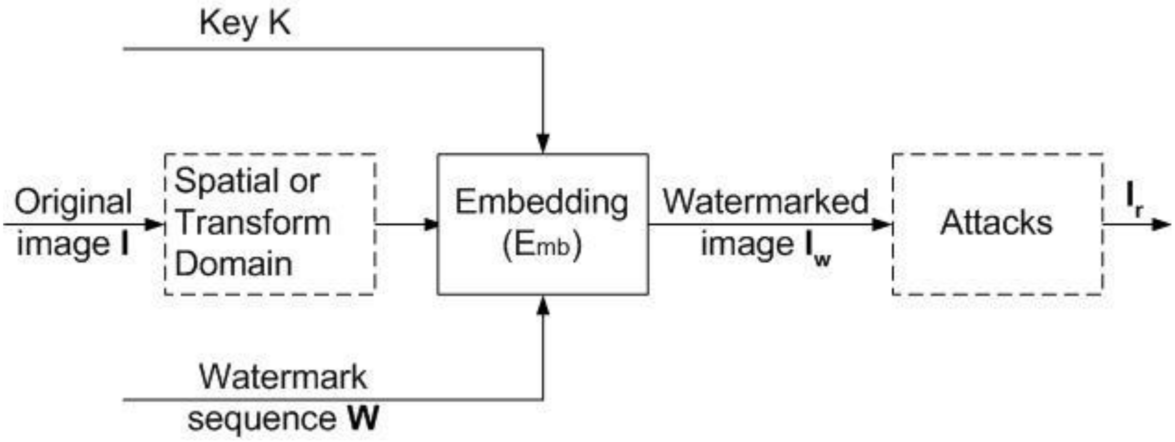


Figure 2: Watermark embedding block diagram

Watermark Extraction process

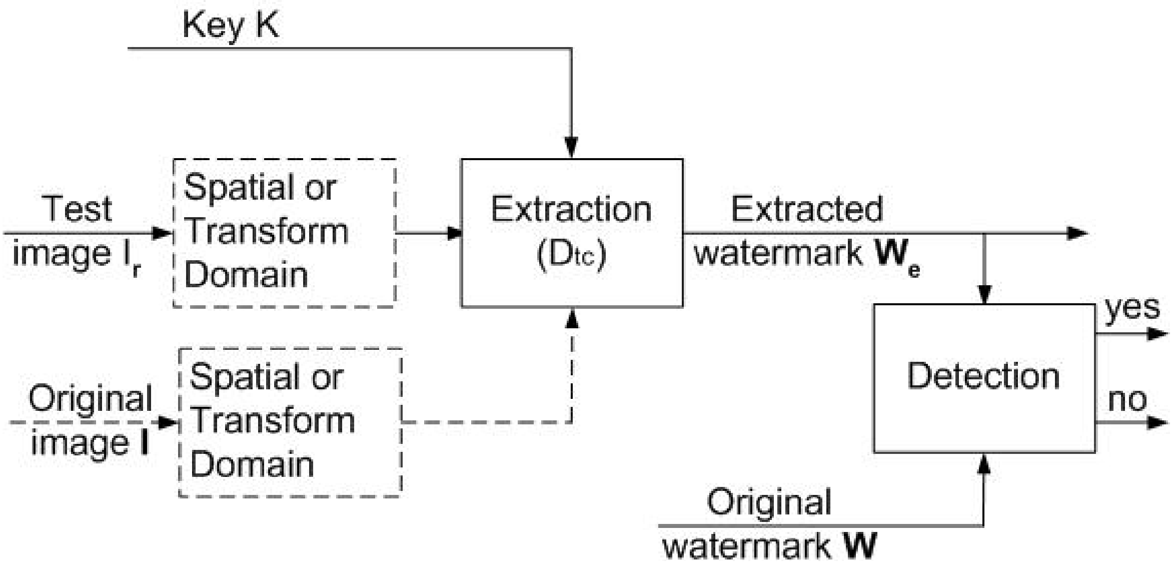


Figure 3: watermark extraction block diagram

1.4 Classifications tree for Watermarking

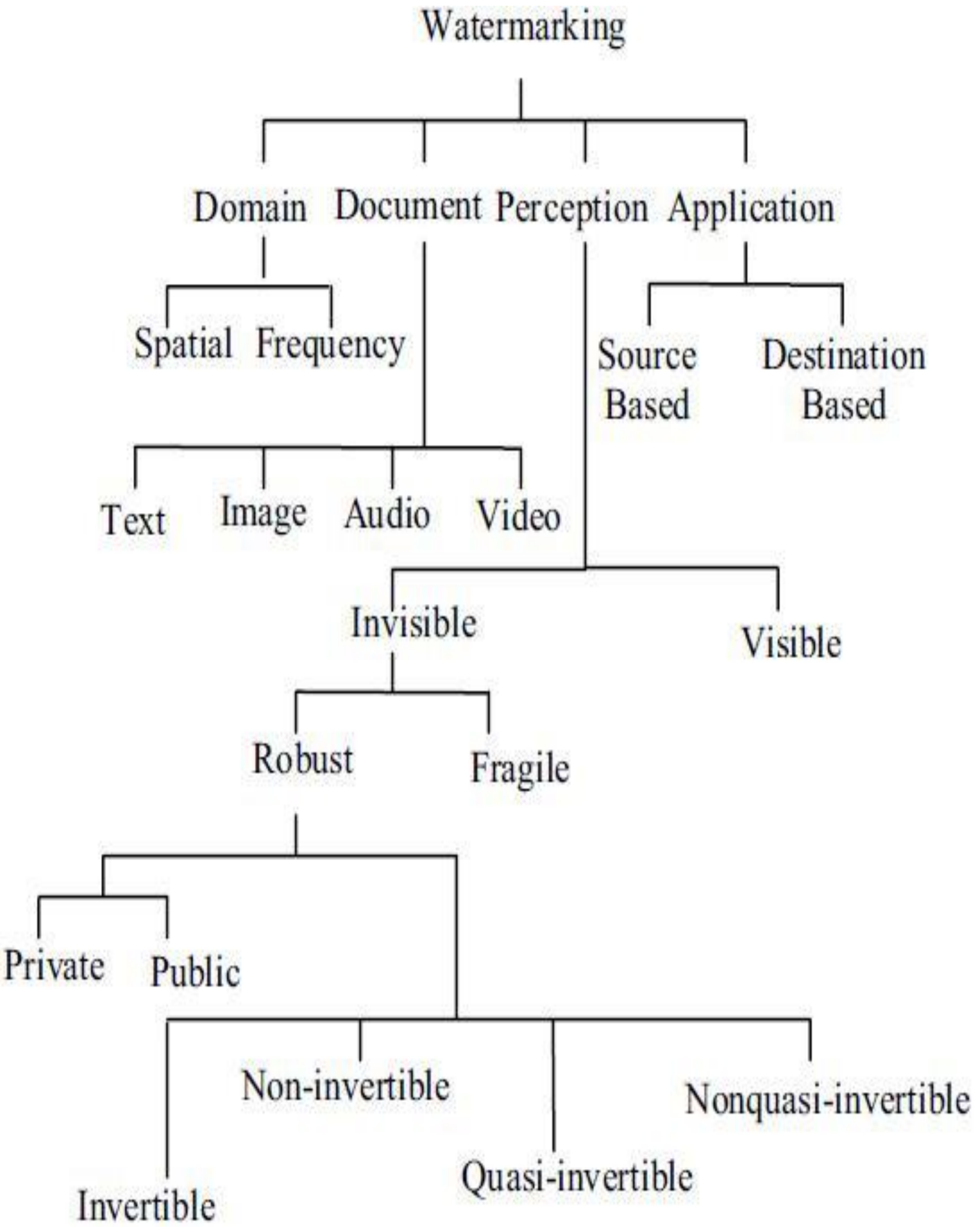


Figure 4: Classification of watermarking

1.5 TYPES OF WATERMARKING

A digital watermark is called robust with respect to transformations if the embedded information may be detected reliably from the marked signal, even if degraded by any number of transformations. Typical image degradations are JPEG compression, rotation, cropping, additive noise, and quantization. For video content, temporal modifications and MPEG compression often are added to this list. A digital watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, un-watermarked content. In general, it is easy to create robust watermark or imperceptible watermarks, but the creation of robust-and-imperceptible watermarks has proven to be quite challenging. Robust imperceptible watermarks have been proposed as tool for the protection of digital content, for example as an embedded no-copy-allowed flag in professional video content.

Digital watermarking techniques may be classified in several ways: -

1.5.1 Based on attached media/host signal:

I. Image watermarking*:* This is used to hide the special information into the image and to later detect and extract that special information for the author‘s ownership.

II. Video watermarking**:** This adds watermark in the video stream to control video applications. It is the extension of image watermarking. This method requires real time extraction and robustness for compression.

III. Audio watermarking***:*** This application area is one of the most popular and hot issue due to internet music, MP3.

IV. Text watermarking**:** This adds watermark to the PDF, DOC and other text file to prevent the changes made to text. The watermark is inserted in the font shape and the space between characters and line spaces.

V. Graphic watermarking**:** It embeds the watermark to 2D or 3D computer generated graphics to indicate the copyright.

1.5.2 Based on visibility: Watermarks can be visible or invisible-

I. **Visible watermarks**: visible watermark are designed to be easily perceived by a viewer (or listener). They clearly identify the owner of the digital data, but should not detract from the content of the data.

II. **Invisible watermarks**: invisible watermark are designed to be imperceptible under normal viewing (or listening) conditions; more of the current research focuses on this type of watermark than the visible type.

Both of these types of watermarks are useful in deterring theft, but they achieve this in different ways. Visible watermarks give an immediate indication of who the owner of the digital work is, and data watermarked with visible watermarks are not of as much usefulness to therefore not be detectable to thieves, otherwise they would try to remove it; however, they should be easily detectable by the owners.

1.5.3 **Based on robustness:** A further classification of watermarks is into fragile, semi fragile or robust.

I. A fragile watermark is embedded in digital data for the purpose of detecting any changes that have been made to the content of the data. They achieve this because they are distorted, or "broken", easily. Fragile watermarks are applicable in image authentication systems.

II. Semi-fragile watermarks detect any changes above a user-specified threshold.

III. Robust watermarks are designed to survive "moderate to severe signal processing attacks".

1.5.4 **Based on encoding format of a video**:

Since video is a collection of consecutive and equally time spaced still images then similar to image watermarking Watermarks for video can further be classified into spatial or spectrum watermarks, depending on how they are constructed:

I. Spatial watermarks are created in the spatial domain of the image, and are embedded directly into the pixels of the image. These usually produce images of high quality, but are not robust to the common image alterations.

II. Spectral (or transform-based) watermarks are incorporated into the image's transform coefficients. The inverse-transformed coefficients form the watermarked data.

III. Perceptual watermarks are invisible watermarks constructed from techniques that use models of the human visual system to adapt the strength of the watermark to the image content

IV. Blind watermarking techniques are techniques that are able to detect the watermark in a watermarked digital item without use of the original digital item.

1.6 APPLICATION OF WATERMARKING

Digital watermarks have been broadly and successfully deployed in billions of media objects across a wide range of applications. The following application areas are described in detail with information of how the technology works, case studies highlighting some of the most prevalent real world uses and links to related information that you may find useful. Digital watermarking may be used for a wide range of applications, such as

- Copyright protection
- Source tracking (different recipients get differently watermarked content)

- Broadcast monitoring (television news often contains watermarked video from international agencies)
- Content identification and management
- Content protection for audio and video content
- Forensics and piracy deterrence
- Content filtering (includes blocking and triggering of actions)
- Communication of ownership and copyrights
- Document and image security
- Authentication of content and objects (includes government IDs)
- Locating content online
- Rich media enhancement for mobile phones

Watermarks are potentially useful in many applications, including:

1.6.1 Ownership assertion: Watermarks can be used for ownership assertion. Suppose there are two persons A and B to assert ownership of a video, A can generate a watermarking signal using a secret private key, and then embed it into the original video. After then A make the watermarked video publicly available. Later, when B contends the ownership of a video derived from this public video, A can produce the unmarked original image and also demonstrate the presence of her watermark in B's video Since A's original video is unavailable to B, he cannot do the same. For such a scheme to work, the watermark has to survive video processing operations aimed at malicious removal. In addition, the watermark should be inserted in such a manner that it cannot be forged.

1.6.2 Fingerprinting: In applications where multimedia content is electronically distributed over a network, the content owner would like to discourage unauthorized duplication and distribution by embedding a distinct watermark (or a fingerprint) in each copy of the data. If, at a later point in time, unauthorized copies of the data are found, then the origin of the copy can be determined by retrieving the fingerprint. In this application the watermark needs to be invisible and must also be invulnerable to deliberate attempts to forge, remove or invalidate. Furthermore, and unlike the ownership assertion application, the watermark should be resistant to collusion. That is, a group of k users with the same video but containing different fingerprints should not be able to collude and invalidate any fingerprint or create a copy without any fingerprint.

1.6.3 Copy prevention or control: Watermarks can also be used for copy prevention and control. For example, in a closed system where the multimedia content needs special hardware for copying and/or viewing, a digital watermark can be inserted indicating the number of copies that are permitted. Every time a copy is made the watermark can be modified by the hardware and after a point the hardware would not create further copies of the data. An example of such a system is the Digital Versatile Disc (DVD). In fact, a copy protection mechanism that includes digital watermarking at its core is currently being considered for standardization and second generation DVD players may well include the ability to read watermarks and act based on their presence or absence.

Another example is in digital cinema, where information can be embedded as a watermark in every frame or a sequence of frames to help investigators locate the scene of the piracy more quickly and point out weaknesses in security in the movie's distribution. The information could include data such as the name of the theatre and the date and time of the screening. The technology would be most useful in fighting a form of piracy that's surprisingly common, i.e., when someone uses a camcorder to record the movie as it's shown in a theatre, then duplicates it onto optical disks or VHS tapes for distribution.

1.6.4 Fraud and tamper detection: When multimedia content is used for legal purposes, medical applications, news reporting, and commercial transactions, it is important to ensure that the content was originated from a specific source and that it had not been changed, manipulated or falsified. This can be achieved by embedding a watermark in the data. Subsequently when the video is checked, the watermark is extracted using a unique key associated with the source, and the integrity of the data is verified through the integrity of the extracted watermark. The watermark can also include information from the original video that can aid in undoing any modification and recovering the original. Clearly a watermark used for authentication purposes should not affect the quality of an image and should be resistant to forgeries. Robustness is not critical as removal of the watermark renders the content inauthentic and hence of no value.

1.6.5 Broadcasting Monitoring: Commercials are aired by broadcasting channels and stations. for this advertising firm purchase airtime from broadcasting channel. There are several organizations and individuals interested in broadcasting monitoring, viz. advertiser, who want to ensure if his commercial is broadcasted for all of his purchased airtime, performers, who want to ensure that they get the royalties due to them from advertising firm and owners of copyrighted works, who want to ensure that their property is not illegally re-broadcasted by pirate stations. One solution to the problem is human observers watching the broadcasting which is neither a feasible nor practically possible solution. The other solution is to match the signal with the signals present in databases to ascertain advertisers that messages are broadcasted. But matching signals from databases is very complex process and require large amount of time and money. The last solution is using watermarking techniques. It has advantage of existing within content itself, rather than exploiting a particular segment of the broadcast signal, and is therefore completely compatible with the installed base of broadcast equipment, including both digital and analog transmission.

1.7 Attacks of watermarking

A **watermarking attack** is a method where the presence of a specially crafted piece of data (e.g., a decoy file) can be detected by an attacker without knowing the encryption key.

Watermark attacks can be classified into four main groups:

a) **Simple attacks** are conceptually simple attacks that attempt to damage the embedded watermark by modifications of the whole image without any effort to identify and isolate the watermark. Examples include frequency based compression, addition of noise, cropping and correction.

b) **Detection-disabling attacks** attempt to break correlation and to make detection of the watermark impossible. Mostly, they make some geometric distortion like zooming, shift in spatial or (in case of video) temporal direction, rotation, cropping or pixel permutation, removal or insertion. The watermark in fact remains in the Cover content and can be recovered with increased intelligence of the watermark detector.

c) **Ambiguity attacks** attempt to confuse the detector by producing fake watermarked data to discredit the authority of the watermark by embedding several additional watermarks so that it is not obvious, which was the first authoritative watermark.

d) **Removal attacks** attempt to analyse or estimate (from more differently watermarked copies) the watermark, separate it out and discard only the watermark. Examples are collusion attack, de-noising or exploiting conceptual cryptographic weakness of the watermark scheme (e.g. knowledge of positions of single watermark elements).

1.8 Challenges and limitation in digital watermarking

There are various technical challenges in digital watermarking. The robustness and imperceptibility trade-off makes the watermarking quite interesting. To attain imperceptibility, the watermark should be added to the high frequency components of the original signal. On the other hand, for robustness the watermark can be added to the low frequency components only. Thus, the watermarking scheme can be successful if the low frequency components of the original signal are used as the host for watermark insertion properties of the human visual system and spread-spectrum communication, which are commonly exploited for making watermarking schemes successful.

1.8.1: Properties of visual signal: Since image and videos are visual signals, it is necessary to understand the behavior of visual signals in order to find ways to hide additional information in them. Visual signals are generally recognized as amplitude plots, intensity versus space displays of image information and intensity versus space and time displays of video scenes. These waveforms reveal a lot of information about the properties of the signals. Some of the properties of visual signals are listed:

a) **Non-stationary:** Non stationary property is common to all signals. Image and video signals contain a wealth of segments of flat or slowly changing intensity, as well as edges and textured regions. While the edges need to be preserved to maintain perceptual quality, the textured regions need to be judiciously used to store additional information

b) **Periodicity:** There exists line to line and frame to frame periodicity in image and video signals. They are not exactly periodic but there exists redundancy between frames and lines. These redundancies are exploited in any compression scheme, and need to be considered during the watermarking process.

1.8.2: **Properties of Human Visual System*:*** The success of any watermarking scheme lies in making the best use of the human visual system (HVS). Here we are discussing the various properties of the human visual system which are exploited in designing watermarking algorithms.

a) **Texture sensitivity:** The visibility of distortion depends on the background texture. The distortion visibility is low when the background has a strong texture. In a highly textured image block, energy tends to be more evenly distributed among the different DCT coefficients. In a flat-featured portion of the image the energy is concentrated in the low frequency components of the spectrum. This indicates that in strong texture regions more watermark signal can be added.

b) **Brightness sensitivity***:* The human eye is sensitive in perceiving a low intensity signal in the presence of backgrounds of different intensity. As the surrounding region intensity is increased, the relative intensity in dark areas is reduced and the sensitivity in the light areas is increased. When the mean value of the noise square is the same as that of the background, the noise square tends to be most visible against a mid-grey background. This characteristic is known as Weber‘s law. This means that the eye has high sensitivity at low intensity levels and greatly reduced sensitivity at high intensity levels.

CHAPTER 2

Techniques of video watermarking

The watermarking has been extensively studied in still images. Today many watermarking scheme are proposed for others type of digital multimedia data, the so-called new objects such as audio, video, text, hardware and 3-D meshes. This thesis is completely devoted to digital watermarking in video. Because video data is largely available on the internet and video camera are installed in public area for surveillance purpose. However popular video editing software permit to easily temper with video content and video content is no more reliable, for example in some countries, a video shot from a surveillance camera cannot be used as piece of evidence in a court room because it is not considered as trustworthy enough. In order to secure or for authentication researcher designed a methodology for verifying the originality of video content and preventing forgery.

Researchers have investigated the use of watermarking in order to verify the integrity of digital video content. A basic approach consists in regularly embedding an incremental timestamp in the frames of the video [37]. As a result, frame cuts, foreign frame insertion, frame swapping, and frame rate alteration can be easily detected. This approach is very efficient for detecting temporal alteration of the video stream. However, it might fail in detecting alterations of the content itself e.g. a character is completely removed from a movie. Investigations have consequently been conducted in order to prevent modifications of the content of the video itself. One proposal [18] embeds the edge map of each frame in the video stream. During the verification process, if the video content has been modified, there will be a mismatch between the extracted edge map from the verified video and the watermarked edge map. The detector will consequently report content tampering. Another proposal exploits the idea that a movie is made up of one audio and one video stream and that both need to be protected against unauthorized tampering. The fundamental idea is then to combine video and audio watermarking [17] in order to obtain an efficient authenticating system. Features of both streams are embedded one into another. Modification from either the sound track, or the video track, is immediately spotted by the detector, since the extracted and watermarked features will differ. Embedding useful data directly into the video stream can spare much storage space.

A typical video stream is made up of two different parallel streams: the audio and video streams. Those two streams need to be synchronized during playback for pleasant viewing, which is difficult to maintain during cropping operations. Hiding the audio stream into the video one [38] will implicitly provide efficient and robust synchronization, while significantly reducing the required storage need or available bandwidth. Researchers face so many challenges in video watermarking. More and more watermarking algorithms are proposed for other multimedia data and in particular for video content. However, even if watermarking still images and video is a similar problem but it is not identical.

2.1 Aspects of video watermarking

Video sequencing is a collection of consecutive and equally time spaced still images. Apparently any image watermarking technique can be extended to watermark videos, but in reality video watermarking techniques needs to meet other challenges. Watermarked video sequences are very much susceptible to pirate attacks such as frame averaging, frame swapping, statistical analysis, digital-analog (AD/DA) conversion and lossy compressions [1]. Watermarking systems can be characterized by a number of defining properties including embedding effectiveness, fidelity, data payload, blind or informed detection, false positive rate, capacity, robustness, perceptual transparency, security, cipher and watermark keys, modification and multiple watermark, cost, tamper resistance, unobtrusiveness, ready detection, unambiguous, sensitivity, and scalability. Some of them are common to more practical applications. In this thesis, such general properties will be listed and briefly discussed and focus will put on video watermarking. These properties are discussed due to their importance in watermarking applications.

a) **Perceptual Transparency**: Invisibility is the degree at which an embedded watermark remains unnoticeable when a user views the watermarked contents. However this requirement conflicts with other requirements such as tamper resistance and robustness, especially against lossy compression algorithms. To survive the next generation of compression algorithms, it will probably be necessary for a watermark to be noticeable to a trained observer which is asked to compare the original and the marked version of the video.

b) **Robustness:** Robustness is the resilience of an embedded watermark against removal by signal processing. The use of music, images and video signals in digital form, commonly involves many types of distortions, such as lossy compression. For watermarking to be useful, the mark should be detectable even after such distortions occurred. Robustness against signal distortion is better achieved if the watermark is placed in perceptually significant parts of the signal. Due to large amounts of data and inherent redundancy between frames, video signals are highly vulnerable to pirate attacks, such as frame averaging, frame dropping, rotation, sharpening [1].

c) **Capacity**: Capacity is that amount of information that can be expressed by an embedded watermark. Depending on the application at hand, the watermarking algorithm should allow a predefined number of bits to be hidden.

2.2 Challenges in video water marking

The challenges for video Watermarking are as follows:

a) Video media is susceptible to increased attacks than any other media

b) Video content is sensitive to subjective quality and Watermarking may degrade the quality

c) Video compression algorithms are computationally intensive and hence there is less headroom for Watermarking computation

d) Video is bandwidth hungry and that is why it is mostly carried in compressed domain.

e) Therefore, Watermarking algorithm shall be adaptable for compress domain processing.

f) For low bit rate video, Watermarking poses additional challenges, as there is less room for watermark data.

g) During video transmission, frame drops are very usual. If watermark data spreads over many frames, in case of frame drops, watermark data may become irretrievable. Watermarking should be robust enough against this phenomenon.

2.3 An overview of video watermarking techniques

Many digital watermarking schemes have been proposed in the literature for still images and videos. Most of them operate on uncompressed videos, while others embed watermarks directly into compressed videos. Video watermarking applications can be grouped as security related like Copy control, fingerprinting, ownership identification, authentication, tamper resistance etc. or value added applications like legacy system enhancement, database linking, video tagging, digital video broadcast monitoring, Media Bridge etc.

Existing video watermarking techniques are divided into different categories as shown in Figure 5. They can be divided into 3 main groups based on the domain that the watermark is embedded.

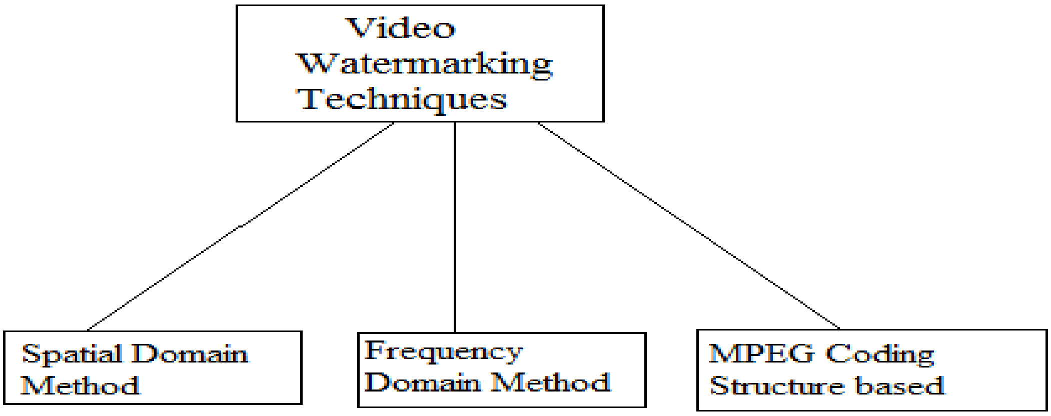


Figure: 5 classification of digital watermarking in video

2.3.1 Spatial domain watermarking:

The spatial domain watermarking techniques embed the watermark by modifying the pixel values of the host image/video directly. Low computational complexities and simplicity are the main strengths of pixel domain methods. For better performance in real time these techniques are more attractive. The main advantages of pixel based methods are that they are conceptually simple and have very low computational complexities and therefore are widely used in video watermarking where real-time performance is a primary concern. However, they also exhibit some major limitations. The need for absolute spatial synchronization leads to high susceptibility to de-synchronization attacks; lack of consideration of the temporal axis results in vulnerability to video processing and multiple frame collusion; and watermark optimization is difficult using only spatial analysis techniques.

a) **Least Significant Bit Modification:** [16]

In this technique, the Least Significant Bit of each pixel is used to embed the watermark or the copyright information. In this technique cover image is used to store the watermark, in which we can embed a smaller object multiple times. The pixels are identified where embedding will be done using a pseudo-random number generator based on a given key. LSB modification is suitable tool for steganography as it is a simple and powerful tool for it. But it cannot preserves robustness which is required in watermarking applications.

b) **Correlation-Based Techniques:**

The most straightforward way to add a watermark to an image in the spatial domain is to add a pseudo random noise pattern to the luminance values of its pixels. A Pseudo-random Noise (PN) pattern W (x, y) is added to the cover image I (x, y), according to the given below:

$$I\,w\,(x, y) = I\,(x, y) + k * W\,(x, y)$$

Where *k* denotes a gain factor and *Iw* the watermarked image. The robustness of the watermark is increased by increasing the value of k at the expense of the quality of the watermarked image. The same key is given as an input to retrieve the watermark, to the same pseudo-random noise generator algorithm, and the correlation between the noise pattern and possibly watermarked image is computed. If the correlation exceeds a certain threshold T, the watermark is detected, and a single bit is set. This method can easily be extended to a multiple-bit watermark by dividing the image into blocks and performing the above procedure independently on each block.

2.3.2 Frequency Domain Watermarking

In Most of the watermarking techniques, the watermark is embedded into the frequency domain instead of the spatial domain for the robustness of the watermarking mechanism. Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT) are the three main methods of data transformation in this domain. The main strength offered by transforming domain techniques is that they can take advantage of special properties of alternate domains to address the limitations of pixel-based methods or to support additional features. Generally, transform domain methods require higher computational time. In transform domain technique, the watermark is embedded distributive in overall domain of an original data. Here, the host video is first converted into frequency domain by transformation techniques. The transformed domain coefficients are then altered to store the watermark information. The inverse transform is finally applied in order to obtain the watermarked video.

A subsample based watermarking technique was proposed by Lu *et al*. [22], where the DCT coefficients of the sub-images were utilized to store the watermark. The method was considered complex and involved high computations, because of the complicated calculations involved in the forward and inverse transformation process. The method, however, was robust against attacks than spatial domain methods. The authors of Cheng *et al*. [23], proposed an algorithm which was based on embedding the watermark image in three times at three different frequency bands, namely, low, medium and high and the results proved that the watermark cannot be totally destroyed by either low pass, medium or high pass filter. In Chun-Shien *et al*. [32], two complementary watermarks were embedded into the host image in order to make it difficult for attackers to destroy both of them. The main benefit obtained from these techniques is that they can take advantage of properties of alternate domains to address the limitations of pixel-based methods or to support additional features. Generally, the main drawback of transform domain methods is their higher computational requirement

a) Discrete Fourier Transform

This approach first extracts the brightness of the to-be-marked frame, computing its full-frame DFT and then taking the magnitude of the coefficients. The watermark is composed of two alphanumerical strings. The DFT coefficient is altered, then IDFT. Only the first frame of each GOP is watermarked, which was composed of twelve frames, leaving the other ones uncorrupted. It is good robustness to the usual image processing. As linear/non-linear filtering, sharpening, JPEG compression and resist to geometric transformations as scaling, rotation and cropping.

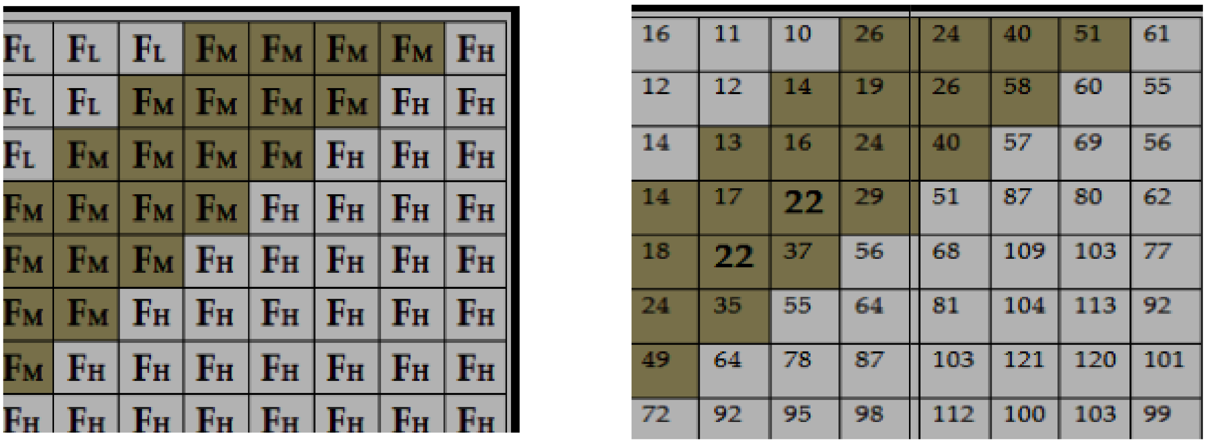
b) Discrete cosine transform

Discrete cosine transformation (DCT) transforms a signal from the spatial into the frequency domain [8] by using the cosine waveform. DCT concentrates the information energy in the bands with low frequency, and therefore shows its popularity in digital watermarking techniques. The DCT allows a frame to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of a frame. The middle frequency bands are chosen such that they have minimize to avoid the most visual important parts of the frame (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies). Two dimensional DCT of a frame with size MxN and its inverse DCT (IDCT) are defined in Equations 1 and 2, respectively.

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

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

Figure 6(a) shows the three regions in the frequency domain. FL is used to denote the lowest frequency components of the block, while FH is used to denote the higher frequency components. FM is chosen as the embedding region as to provide additional resistance to lossy compression techniques, while avoiding significant avoidance of the cover video.



FL	FL	FL	FM	FM	FM	FM	FH
FL	FL	FM	FM	FM	FM	FH	FH
FL	FM	FM	FM	FM	FH	FH	FH
FM	FM	FM	FM	FH	FH	FH	FH
FM	FM	FM	FH	FH	FH	FH	FH
FM	FM	FH	FH	FH	FH	FH	FH
FM	FH	FH	FH	FH	FH	FH	FH
FH	FH	FH	FH	FH	FH	FH	FH

(a)

16	11	10	26	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

(b)

Figure 6: Definition of DCT regions and quantization values used in JPEG compression scheme.

c) Discrete wavelet transform

The Discrete Wavelet Transform (DWT), which is based on sub band coding is found to yield a fast computation of Wavelet Transform. It is easy to implement and reduces the computation time and resources required**.** Mostly used transformation in image watermarking is DWT due to its excellence spatial localization and multi-resolution characteristic. There is various application areas in which dwt watermarking is used: owner identification, proof of ownership, transaction tracking, content authentication, copy control, device control. DWT is a mathematical tool for hierarchically decomposing an image or frame. In this, transformation is based on small waves called wavelets. Wavelet transformation provides both frequency and spatial description of an image/frame. Temporal information retained in the transformation process. DWT is the Multi-resolution decomposition of image or video frames. It splits the signal into high and low frequency parts. Higher frequency part contains information about the edge component, while the lower part again splits into the high n low frequency part. High frequency component usually used for the watermarking since the human eye is less sensitive to observe the changes in edges. In this technique video is divided into frames and dwt is applied. Dwt can be applied in different level of frequency region. In 1-level, dwt decompose the frame into four sub-bands of frequency (LL1, LH1, HL1, and HH1) as shown in figure 7 a. And for 2-level dwt we can select a sub-band from these four bands and again applying dwt technique on this divide it into four sub-bands of sub-band as LL2, LH2, LH2, HH2 as shown in figure 7 b. similarly we can further divide it into 3-level dwt and again division will be 4- level dwt. From the division at different level we can make watermarking more complex for securing our video from the different types of attacks. DWT based technique is most similar to theoretical model of HVS (human visual system) it divide the image into low frequency and high frequency component of same bandwidth. As most of the energy is concentrated in the approximate (LL) sub band having low frequency sub bands, any change in these low frequency sub bands would cause a severe degradation of image. As the human eyes are not sensitive to high frequency sub bands, the secret information is embedded in either vertical, horizontal or diagonal (LH, HL or HH respectively) sub bands.

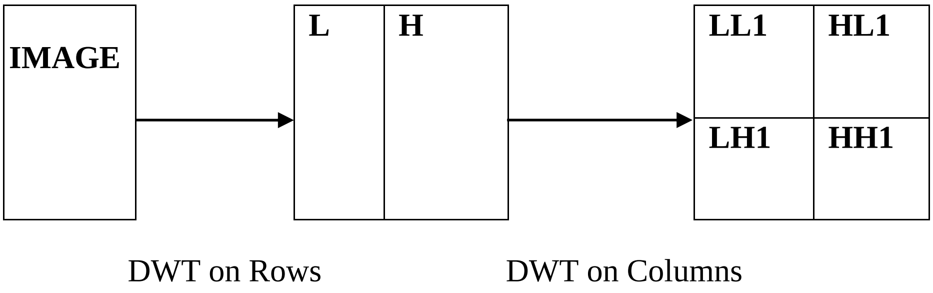


Figure 7 a: DWT decomposition of image

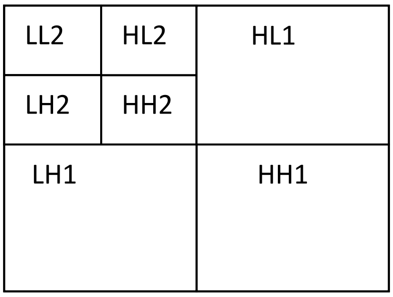


Figure 7 b: 2-Level DWT

d) Singular Value Decomposition Watermarking

The Singular Value Decomposition (SVD) is a technique that can be used in image compression techniques, but can also be applied to watermarking. The SVD is performed, after which the singular values are usually modified to embed the watermark. A pseudo-inverse SVD is then applied to obtain the original content. The SVD can be used on its own for watermarking, but is also often used in hybrid techniques which combine the SVD and the discrete cosine transform. The SVD is relatively computationally complex, but by applying it in hybrid techniques it may not be necessary to perform an SVD on the entire image, lowering the computational complexity. SVD video watermarking techniques seem to only have gained popularity after 2006, compared to other techniques that were pioneered in the late 1990s. This can possibly be attributed to the computational complexity of the SVD which may have prohibited the use in video applications when computing power was limited.

2.3.3 Compression based watermarking

In this technique, for an effective watermarking method, two fundamental requirements should be satisfied: transparency and robustness. Transparency represents the invisibility of the watermark embedded in the signal data, without degrading the perceptual quality. Robustness means that the watermark should not be removed by attacks, including signal processing, compression, re-sampling, frame dropping, frame averaging, cropping, etc. in conventional watermarking, a compressed video streams is first decomposed into the video signal and finally recompressed into standard video; a watermark signal is the embedded into the video signal and finally recompressed into the watermarked video.

This technique needs full decompressing and recompressing of the video streams which take a lot of processing time and is thus computationally intensive. To make the processing faster, it is better to watermark in the compressed domain. In compressed domain watermarking, the original compressed video is partially decoded. Then the partially decoded bit stream is modified in order to accommodate the watermark signal. Eventually, the watermarked bit stream is compressed to form watermark video.

Langelaar and Lagendilk[36], described a compressed domain watermarking technique called differential energy watermark (DEW). In their method, host video is partitioned into group of blocks, each of which is further subdivided into two sets of equal size, as determined by the watermark embedding key. By comparing the energy of the selected discrete cosine transform (DCT) coefficients within the two sets, a single bit payload is expressed. The technique is not very robust against trans-coding, particularly if the group of pictures (GOP) structure is changed.

Another compression video watermarking has been proposed by Hartung and Girod[37]. Their scheme included an approach for only compensation and watermarking; nonzero DCT - coefficient perform data rate control here. As there technique uses a single watermark signal throughout the whole video sequence, it is not robust, especially in the case of frame averaging and frame dropping. There is a number of MPEG-2 and -4-based techniques that have been proposed, including approaches based on GOP (group of pictures) modification, high frequency DCT coefficient manipulation, DCT block classification.

Vassaux *et al.*[32] proposed a video object watermarking which is based on the structure of MPEG-4. In their method, a scrambling technique that allows adapting any classical spread spectrum watermarking scheme operating in the spatial domain to the MPEG-4 requirements concerning VO manipulation was proposed. This technique could be easily added to the embedding and detection schemes without changing the watermarking algorithm. It modified some predefined pairs of quantized DCT coefficient in the luminance block of pseudo-randomly selected MBs and was based on spread-spectrum techniques. In this method, the image was first divided into equal sized blocks, where a binary sequence generated using secret key is embedded to the image. Swanson, et al. [33] presented an object-based transparent watermarking procedure for copyright protection into video sequences. To address issues associated with video motion and redundancy, individual watermarks were created for objects within the video. Each watermark was created by shaping a pseudo-random sequence according to the perceptual masking characteristics of the video. This resulted in a watermark that could adapt to each video and ensured invisibility and robustness. Furthermore, their experimental results showed that the noise like watermark was statistically undetectable to prevent unauthorized removal.

Video watermarking techniques that use MPEG-1, -2 and -4 coding structures as primitive components are primarily motivated by the goal of integrating watermarking and compression to reduce overall real-time video processing complexity. Compression in block-based schemes like MPEG-2 is achieved by using forward and bi-directional motion prediction to remove temporal redundancy, and statistical methods to remove spatial redundancy. One of the major drawbacks of schemes based on MPEG coding structures is that they can be highly susceptible to re-compression with different parameters, as well as conversion to formats other than MPEG, MPEG standard relies indeed on motion prediction and any distortion is likely to be propagated to neighbor frames. Since the accumulation of such propagating signals may result in a poor quality video, a drift compensation signal can be added if necessary. In this case, motion compensation can be seen as a constraint. However it could also be exploited so that the motion vectors of the MPEG stream carry the hidden watermark. The components of the motion vector can be quantized according to a rule which depends on the bit to be hidden. For example, the horizontal component of a motion vector can be quantized to an even value if the bit to be hidden is equal to 0 and to an odd value otherwise. All the frames of an MPEG coded video are not encoded in the same way. The intra-coded (I) frames are basically compressed with the JPEG image compression standard while the inter-coded (B and P) frames are predicted from other frames of the video.

As a result, alternative watermarking strategies can be used depending on the type of the frame to be watermarked. Embedding the watermark directly in the compressed video stream often allows real-time processing of the video. However the counterpart is that the watermark is inherently tied to a video compression standard and may not survive video format conversion.

a). Real time Watermarking [38]

Real-time can be an additional specification for video watermarking. It was not a real concern with still images. When a person wants to embed a watermark to check the presence of a watermarking an image, a few seconds is an acceptable delay. However, such a delay is unrealistic in the context of the video. Frames are indeed sent at a fairly high rate, typically 25 frames/sec., to obtain a smooth video stream. At least the embedded or the detector, and even sometimes both of them, should be able to handle such a rate. In the context of broadcast monitoring, the detector should be able to detect an embedded watermark in real-time. In a VOD environment, the video server should be able to insert the watermark identifying the customer at the same rate that the video is streamed. In order to meet the real-time requirement, the complexity of the watermarking algorithm should obviously be as low as possible. Moreover, if the watermark can be inserted directly into the compressed stream, this will prevent full decompression and recompression and consequently, it will reduce computational needs. This philosophy has led to the design of very simple watermarking schemes. Exploiting the very specific part of a video compression standard can lead to very efficient algorithms. An MPEG encoded video stream basically consists of a succession of variable length code (VLC).

A watermark can consequently be embedded in the stream by modifying those VLC code words. The MPEG standard uses indeed similar VLC code words i.e. with the same run length, the same VLC size and a quantized level difference of one. Such VLC code words can be used alternatively in order to hide a bit. Another way of a achieving real-time is to split the computations. The basic idea is to perform intensive computations once for all on the provider side and then simple client-dependent processing on request. This can be seen as some sort of preprocessing. Blind watermarking schemes, i.e. which do not consider the data to be watermarked, are the most simple but they are usually avoided in order to obtain good detection statistics. However, if some preprocessing is performed before, such a scheme may be efficient. The preprocessing step, which may consider side information and be very complex, performs some smart operations. As a result, blind watermarking can be used reliably later on client request.

b). Differential Energy Watermarks [38]

The DEW method was initially designed for still images and has been extended to video by watermarking the I-frames of an MPEG stream. It is based on selectively discarding high frequency DCT coefficients in the compressed data stream. In the embedding process The 8 x 8 pixels blocks of the video frame are first pseudo randomly shuffled. This operation forms the secret key of the algorithm and it spatially randomizes the statistics of pixel blocks i.e. it breaks the correlation between neighboring blocks. The obtained shuffled frame is then split into n 8 x 8 blocks, n is equal to 16. One bit is embedded into each one of those blocks by introducing an energy difference between the high frequency DCT-coefficients of the top half of the block (region A) and the bottom half (region B).This is the reason why this technique is called a differential energy watermark.

c). MPEG2 based watermarking

In MPEG-2 Intra coded (I-frames) frames are split into block of 8x8 pixels which are compressed using the DCT quantization, ZIG-ZAG scan, run level coding and entropy coding (VLC). Inter-coded frames (in MPEG-2 terminology: P- or B- frames) are subject to motion compensation by motion compensated prediction. The residual prediction error signal frames are split into block of 8x8 pixels which are compressed in the same way as blocks in the inter frames.

The basic idea for MPEG-2 coded video is:

(i) Generating a watermark signal for each frame of the video sequence exactly in the same manner as it done in pixel domain.

(ii) Arranging the watermark signal into a two dimensional signal having the same dimensions as the video frames.

d). MPEG-4 based watermarking

An MPEG-4 visual scene may consist of one or more video objects. Each video object is characterized by temporal and spatial information in the form of shape, motion and texture and corresponds to a 2D object in the scene. A Video Object Plane (VOP) is a time sample of video object. VOP's can be encoded independent of each other or dependent on each other by motion compensation. A VOP contains the encoded video data in form of macro blocks. A macro block contains a section of the luminance component and the spatially sub sampled chrominance components. In MPEG-4 visual standard there is support for only one chrominance format for a macro block, the 4:2:0 format. In this format, each macro block contains 4 luminance blocks, and 2 chrominance blocks. Each block contains 8x8 pixels encoded using DCT transformation.

The DCT coefficients are then adaptively quantized to low bit rates. A figure 8: is shown in which frame of MPEG-4 video steam is shown which are showing a forward prediction and backward prediction of inter and intra coded frame in watermarking.

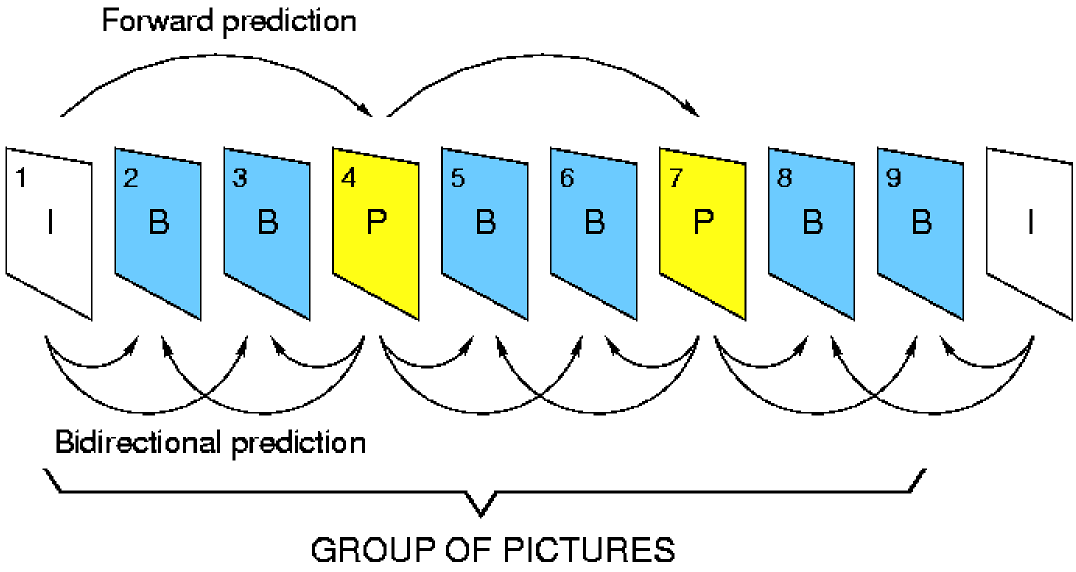


Figure 8: MPEG GOP structure

2.4 Attacks on watermarked video

There are various possible malicious intentional or unintentional attacks that a watermarked object is likely to subject to. The availability of wide range of image processing softwares made it possible to perform attacks on the robustness of the watermarking systems. The aim of these attacks is prevent the watermark from performing its intended purpose. A brief introduction to various types of watermarking attacks is as follow.

i. **Removal Attack:** Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal.

ii. **Interference attack:** Interference attacks are those which add additional noise to the watermarked object. Lossy compression, quantization, collusion, de-noising, re-modulation, averaging, and noise storm are some examples of this category of attacks.

iii. **Geometric attack:** All manipulations that affect the geometry of the image such as flipping, rotation, cropping, etc. should be detectable. A cropping attack from the right-hand side and the bottom of the image is an example of this attack.

iv. **Low pass filtering attack:** A low pass filtering is done over the watermarked image and it results in a difference map composed of noise.

v. **Forgery attack:** The forgery attacks that result in object insertion and deletion, scene background changes are all tantamount to substitution.

vi. **Security Attack:** In particular, if the watermarking algorithm is known, an attacker can further try to perform modifications to render the watermark invalid or to estimate and modify the watermark. In this case, we talk about an attack on security. The watermarking algorithm is considered secure if the embedded information cannot be destroyed, detected or forged.

vii. **Protocol Attack:** The protocol attacks do neither aim at destroying the embedded information nor at disabling the detection of the embedded information (deactivation of the watermark). Rather than that, they take advantage of semantic deficits of the watermark‘s implementation. Consequently, a robust watermark must not be invertible or to be copied. A copy attack, for example, would aim at copying a watermark from one media into another without knowledge of the secret key.

viii. **Cryptographic attacks:** Cryptographic attacks deal with the cracking of the security. For example, finding the secret watermarking key using exhaustive brute force method is a cryptographic attack. Another example of this type of attack is the oracle attack. In the oracle attack, a non-watermarked object is created when a public watermark detector device is available. These attacks are similar to the attacks used in cryptography.

ix. **Active Attacks:** Here, the hacker tries deliberately to remove the watermark or simply make it undetectable. This is a big issue in copyright protection, fingerprinting or copy control for example.

x. **Passive Attacks:** In this case, the attacker is not trying to remove the watermark but simply attempting to determine if a given mark is present or not. Cox et al (2002) suggest that, protection against passive attacks is of the utmost importance in covert communications where the simple knowledge of the presence of watermark is often more than one want to grant.

xi. **Collusion Attacks:** In collusive attacks, the goal of the hacker is the same as for the active attacks but the method is slightly different. In order to remove the watermark, the hacker uses several copies of the same data, containing each different watermark, to construct a new copy without any watermark. This is a problem in fingerprinting applications (*e.g.* in the film industry) but is not the widely spread because the attacker must have access to multiple copies of the same data and that the number needed can be pretty important.

xii. **Image Degradation:** These type of attacks damage robust watermarks by removing parts of the image. The parts that are replaced may carry watermark information. Examples of these operations are partial cropping, row removal and column removal. Insertion of Gaussian noise also comes under this category, in which the image is degraded by adding noise controlled by its mean and its variance.

xiii. **Image Enhancement:** These attacks are convolution operations that desynchronize the watermark information in an image. These attacks include histogram equalization, sharpening, smoothing, median filtering and contrast enhancement.

xiv. **Image Compression:** In order to reduce the storage space and cut the cost of bandwidth required for transmitting images, images are generally compressed with JPEG and JPEG2000 compression techniques. And video is compressed with MPEG scheme. These lossy compression methods are more harmful as compared to lossless compression methods. Lossless compression methods can recover the watermark information with inverse operation. However lossy compression techniques produce irreversible changes to the images. Therefore probability of recovering watermarked information is always very low.

xv. **Image Transformations:** These types of attacks are also called synchronization attacks or geometrical attacks. The Geometrical attacks include rotation, scaling and translation also called RST attacks. Some researchers focus on RST robustness while designing the robust watermarking systems, because it is fundamental problem. Besides RST transforms, image transformations also include other transforms such as aspect ratio change, shearing, rejection and projection.

xvi. **Attacks at other levels**: There are a number of attacks that are directed to the way the watermark is manipulated. For instance, it is possible to circumvent copy control mechanisms discussed below by super scrambling data so that the watermark is lost or to deceive web crawlers searching for certain watermarks by creating a presentation layer that alters the way data are ordered. The latter is sometimes called ‘mosaic attack’

CHAPTER 3

LITERATURE SURVEY

Various video watermarking algorithm, which includes spatial domain and transform domain algorithms are reviewed here. Variety of schemes have been employed yet now which include Least Significant Bit modification, correlation based approach, transform based approaches like discrete Fourier transform, discrete wavelet transform, discrete cosine transform, singular value decomposition, and combination of two transforms such as discrete wavelet transform with discrete cosine transform and discrete wavelet transform with singular value decomposition, and combination of three also. So many techniques have been developed in digital video watermarking. In this dissertation we are taking last ten year research paper and giving brief review of all the techniques used in past for video watermarking.

In 2000 'Masatama Ejima and Akio Miazaki [29]' proposed A wavelet based watermarking for digital images and digital video. In this he proposed a method of digital watermark for still images by using wavelet packets, and examines the robustness of the watermarking method against several image processing. This method can be easily applied to the watermark for video because in this method, embedded data are detected without the original image. So he extended the wavelet-based watermarking method to the case of watermark for video. In his method, an image is first decomposed by the wavelet transform, and then the coarsest scale component is decomposed into sub-band signals by the wavelet packets. Watermark is embedded into the sub-band signals with larger energy, and is extracted without the original image or the information of location in which data are hidden. Next, he apply this method to the watermark for still images, and examine its robustness to image processing and transformation. Further, he develop the watermark for video based on this method, and numerical experiments show that the watermark is extracted from watermarked video compressed with MPEG.

In 2001 'V Capellini et al [30]' Proposed Robust frame-based watermarking for digital video. In this paper a watermarking algorithm originally conceived for still images applications, has been extended to raw video, treating it as a set of still frames. A good robustness against common image processing and geometric manipulations has been achieved moreover experiments with MPEG2 coding/decoding at different bit rates have been carried out giving positive results. The approach proposed in this paper is to apply a tested and well-performing watermarking technique originally devised for still images, to raw video; to this end the whole non-coded sequence is considered as a collection of single frames

In 2002 'shao yafei, Zhang li, Wu Guowei [31]' has done some work as "Research of watermarking in digital video broadcasting" in this they proposed a MPEG based watermarking scheme, in which watermark is embedded by modulation of certain DCT coefficient. The threshold of the detector is dynamically adjusted along the time-axis to fit the frame characteristics. The proposed method is of low complexity and is easy to be implemented in the consumer electronics devices. It can be applied in the copy control and user tracing scenarios. A low complexity watermarking algorithm for digital video broadcasting is proposed. The watermark is embedded in the MPEG2 bit stream domain; the embedding location and strength are selected according to the human visual system (HVS): in the detection stage, a dynamic threshold selection is introduced to keep the same false positive probability along the time axis and under variable attacks. In his experiment they used the CCIR601 video sequences with frame size 720*480, 4:2:0. First of all, the raw video is compressed to 8Mbits MPEG2 stream with studio quality, then watermark is embedded into the compressed stream. They choose 2 mid to high frequency positions among each DCT block as the embedding candidates. These positions are selected randomly among a certain range in each block to keep security. Statistically, in the experiment there are about 5%-10% coefficients in these positions are changed to embed watermark. The watermarked stream is of no visual distortions after decoding. In the watermark detection, the output of the correlation detector is **1,** which is much greater than the threshold, for example, for the first I frame, the threshold is 0.203.the proposed algorithm is robust to MPEG2 re-encoding and easy to be implemented in DVB terminal devices, thus can be used in copy control and user tracing scenarios.

In 2002: another technique which is based on compressed video watermarking scheme for self authentication proposed by' 'Daniel Cross, Bijan G Mobasseri'. In this the proposed algorithm is as, I-frames watermark the entire length of the following GOP (group of pictures). The algorithm first computes the payload capacity of each GOP by identifying the population of eligible VLCs capable of carrying the watermarks. The candidate I-frame is then compressed to this target bit rate and the bits are reordered based on a GOP-unique key. The scrambled bits then sequentially watermark the GOP. Detection follows an inverse process. Watermarked video is resistant to tampering at the GOP level by observing the key sequencing needed for watermark extraction. Missing GOPs cause jumps in the required keys which can then be connected to the number of affected GOPs. Corruption or frame-level tampering inside a GOP can also be spotted using a similar approach.

The algorithm parses the entire target video once to record the number of IC-VLCs in the intra-coded blocks of every I**,** P, and B frame. These numbers are then combined to determine the total capacity of each individual GOP. The watermark-carrying capacity dictates the total number of bits from each I-frame that may contribute to the watermark mask. The algorithm then parses the target a second time, generating a watermark mask from the I-frame in a particular GOP. This mask will be used to watermark intra-coded blocks of the I**,** P, and B frames in the following GOP**.** Once a watermark mask is generated, it is scrambled according to a fixed algorithm and a key. The key is calculated using a standard key-generation algorithm seeded by the user-defined password. The key-generation algorithm re-calculates a new key for every watermark mask. After each watermark mask is scrambled, it is inserted (one bit at a time) into the parity bits of the Lc-VLCs of the GOP directly following the GOP containing the current I-frame. This process is continued until the final GOP is watermarked. The current method does not watermark the first GOP. Since any bit that is to be used as a watermark must not be modified after it has been used, each I-frame may only watermark the frames in the GOP which directly follows the current GOP. This process is continued until the final GOP is watermarked.

The capacity of the target varies depending on video content. In fact, the watermark-carrying capacity can even vary greatly from GOP to GOP. The product of the insertion process is a watermarked target ready for authentication. Proposed algorithm produces a self watermarked video and does it entirely in the compressed bit stream of MPEG-2. As a post-compression watermark, the algorithm is naturally not affected by compression. Embedding and recovery does not require expensive transforms and partial or full decompression. However, re-encoding and rate control would seriously affect survivability. The embedded watermark may be used for authentication of video and protection against tampering. The embedded watermark, having been derived from the content, cannot be pirated and used elsewhere. The GOP specific keys used for watermark embedding allows for the identification of missing, removed or altered GOPs by monitoring the keys needed for authentication. It is therefore, very difficult to edit out GOPs or import GOPs into a video to either mislead the, or conceal and destroy the evidence. Watermark embedding and authentication is integrated into the standard MPEG-2 decoder software.

In 2002, 'Ambalanath shan and Ezzatalah solari'[10] proposed a new technique based on "Real time digital video watermarking" in this paper he proposed a real time watermarking in which he uses the 'Hadamard' transform as the spreading transform for the key hence very fast coding and decoding of the imperceptible watermark is realized. This in turn, can serve to verify the source of a digital frame in real-time

In the same year another technique based on "watermarking of streaming video for Fingerprinting application" proposed by 'Fengming Huang et al.[11]' in this technique they proposed a real-time watermarking paradigm for finger-printing streaming videos over the Internet or a private video-on-demand network. His paradigm is based on a 3-tier architecture which runs a proxy server in between the video server and the client's video player. The proxy server intercepts the client's request and the video data transmitted by the server, embeds a watermark into the video data based on the client transaction information, and re-encapsulate the video data within the transport packets. Based on this paradigm, they developed a prototype capable of finger-printing MPEG4 streaming videos using standard video streaming protocols such as RTSPRTCPRTP. Pertinent design implementation issues and results of this work will be discussed. In this paper, they discussed a real-time fingerprinting technique for streaming video. By combining real-time watermarking process together with proxy-server structure, we can achieve real-time streaming video watermarking, easy installation, easy updating and storage space saving.

In 2004 'Chun Shien Lu et al'[11] proposed a "Resistance to content-dependent video watermarking to watermark estimation attacks" In his paper he focused on exploring the robustness against the watermark estimation attacks (WEAs).That are clever at disclosing hidden information for unauthorized purposes without sacrificing media's quality. In WEAs, the collusion attack naturally occurs in video watermarking while the copy attack adapts to any media watermarking. In view of this, the aim of this study is to deal with the WEAs by means of a video frame-dependent watermark (VFDW). We begin by gaining insight into the WEAs, leading to formal definitions of "optimal watermark prediction" and "perfect cover data recovery." Subject to these definitions, the video-frame hash is addressed as a constituent component of the VFDW for anti-estimation of hidden watermarks. Both mathematical analyses and experiment results consistently verify the anti-disclosure capability of the video content-dependent watermarking scheme.

His approach is the first work that takes resistance to both the collusion and copy attacks into consideration. In this paper, the video frame-dependent watermark (VFDW), which is a mixture of a frame hash and a hidden message, has been explored to withstand watermark estimation attacks (WEAs). Notably, they have pointed out that both accurate estimation of a watermark's sign and complete subtraction of a watermark's energy constitute the sufficient and necessary conditions for achieving complete watermark removal. The characteristics of the VFDW have been analyzed to justify its resistance to WEAs. Overall, the experimental results have confirmed his mathematical analyses about WEAs and VFDW. They are the first to employ the content-dependent video watermark in resisting the collusion and copy attacks, simultaneously. The proposed media hash at its current status is sensitive to geometric distortions and could potentially affect the resistance of the VFDW to them. In his future work, he will continue to study in geometrical invariance of media hash.

In 2004: another technique is proposed by 'sha wang et al [41], on "video quality measurement using digital watermarking" This paper presents an objective MPEG-2 video quality measurement method based on fragile digital image watermarking. Based on the DCT-based watermarking scheme, this paper presents a fragile digital video watermarking scheme that can work as an automatic quality monitoring system. We embed watermark in the DCT domain of l-frames of original video, and the DCT blocks for embedding are carefully selected so that the degradation of the watermark can reflect the degradation of the video quality. The contrast sensitivity value is taken into account to weighting the quality measurement according to the human vision system. The evaluations demonstrate that the effectiveness of the proposed scheme against MPEG2 compression and noise pollution.

In 2005: 'Shri aria and kaoru Arakawa [40]' proposed a "digital watermarking for color video using a non linear filter using dection process" This method is based on 'Haitsma and Zhao's methods' which embed watermark signals into the luminance mean series, but newly introduce a nonlinear digital filter, named as a component separating filter (*CS* filter), in the detecting process. The *CS* filter can effectively extract the small amplitude watermark signals on the mean series without being affected by the abrupt shot change. Moreover, it is shown that higher performance is realized by embedding into the color difference signal instead of the luminance. Computer simulations verify its high performance compared with conventional methods.

In 2006: 'Isao Echizen et al [42], proposed a "improved video verification method using digital watermarking", The proposed verification method distinguishes attacks against video content from regular modifications by extracting time codes embedded in consecutive frames of the content and then checking their continuity. A prototype implementation showed that the method is more effective than conventional ones and that it can be used by a variety of applications using video content. Evaluation using a prototype showed that the proposed method is more effective than conventional ones. It can detect and identify attacks on video content, even if the content has suffered multiple types of attacks. It is thus usable by various types of applications using video content as evidence.

In the same year 'Isao Echizen et al, proposed another technique "integrity verification system for video content by using digital watermarking" The proposed verification system distinguishes attacks against video content from regular modifications by extracting time codes and header hash values embedded in the content itself and comparing them with the actual ones, making it well suited for content storage services. Evaluation showed that the system is more effective than a current one using the digital signature scheme and that it can be used by a variety of applications using stored video content. Evaluation showed that the proposed system is more effective than a current one using the digital signature scheme and that it can be used by a variety of applications using video content.

In 2006: 'Yuk Ying Chung, Fang Fei Xu [44]' proposed "A Secure Digital Watermarking Scheme for MPEG-2 video Copyright Protection" In this paper a new hybrid approach of digital video watermarking scheme with an **E**rror **C**orrecting **C**ode (**ECC**) is proposed. This watermarking scheme maximizes the watermark payload while minimizing the perceptual degradation of video quality caused by the embedded watermark by means of an appropriate choice of embedding position. Two hybrid error correcting codes, BCH (31,8) and Turbo (3,1) with repetition code were implemented and compared. We found that the hybrid approach of BCH (31,8) with repetition code achieved higher error correcting capability than Turbo (3,1) with repetition code under the simulated noise tests.

In this paper a new hybrid approach of digital video watermarking scheme based on error correcting code for MPEG2 video was proposed and implemented. The proposed watermark scheme was developed under the triple contradictory constraints of imperceptibility, robustness and capacity. As to the watermark embedding capacity, since one watermark bit can be embedded in the LSB of the DC coefficient of one 8×8 DCT coefficient block, the maximum number of bits that can be embedded in one I-frame is exactly the same as the number of 8×8 blocks. Given a video sequence with standard image size 352×288, more than two thousand watermark bits can be embedded in just one I-frame. Therefore the proposed watermarking scheme can support large watermark payload.

In this paper He combined the watermarking scheme with different error correcting coding schemes to improve the performance in terms of watermark robustness. The hybrid approach of two error correcting codes: BCH (31,8) and Turbo (3,1) with repetition code were implemented with digital watermark technique. The effectiveness of these error correcting codes in protecting watermark were investigated. He has implemented seven cases of simulated noise to test this proposed hybrid approach of video watermarking system. To compare the error correcting capacity of these error correcting codes, the watermark correcting rate (WCR) of each error correcting code was measured under different bit error rate (BER). From the experimental results in section 5, we can see that the BCH (31, 8) has the highest error correcting capacity. When the BER is around 15%, the WCR after BCH decoding still remains above 95% and can extract the watermark information with almost perfect accuracy.

In 2007: ‘Stefano Chessa et al, proposed “Mobile Application Security for Video Streaming Authentication and Data Integrity Combining Digital Signature and Watermarking Techniques” In satellite link peculiar characteristic like no packet reordering and low bit error rate these characteristics combined with watermarking techniques to propose a novel authentication algorithm for multicast video streaming. This algorithm combines a single digital signature with a hash chain pre-computed on the transmitter side; the hash chain is embedded in the video stream by means of a watermarking technique. proposal shows several interesting features: Authentication is enforced, as well as integrity of the received multicast stream; received blocks can be authenticated on the fly; no storage is required on the receiver side, except for the amount of memory needed to store a single hash; overhead computations required on the receiver sum up to single hash per block, while a digital signature verification is amortized over the whole received stream. Finally, note that the bandwidth overhead introduced is negligible, since the applied watermarking technique introduces virtually no modifications (at least, not recognizable by humans) on the original video stream pictures.

In 2008: ‘Mohammad Afizi and Mohammad shukran’ proposed a paper for “developing an effective watermarking algorithm for video retrieval” In this paper, a novel approach of video watermarking technique for video retrieval system has been proposed and developed. The hidden information is inserted by altering the transform coefficients. some image manipulations and attacks such as basic testing, visual quality testing, watermark sequence, double watermark insertion and collusion tests were performed on watermarked video sequences. The proposed approach has passed all these attack tests without any problem, despite using very small watermark (amplitude of 100, which was used for these tests, means that the transform coefficients are only increased or decreased by 10% on average). Since these tests can be the representative for most image manipulations and attacks, this shows that the watermark generated by the proposed algorithm is robust and efficient for video retrieval system.

In 2008: 'Po-Chyi Su1, Ching-Yu Wu2, Yen-Chin Chen', proposed a technique for traffic surveillance "A Digital Video Watermarking Scheme for Annotating Traffic Surveillance Videos" A new application of exploiting digital watermarking techniques for annotating traffic surveillance videos is presented in this paper. The information of each vehicle collected from other sensors/sources will be embedded into the corresponding pixels in the recorded video to facilitate data management. The traffic scene captured by a video camera will be analyzed first and the individual vehicles are extracted and tracked by using Kalman filtering for effective watermarking.

The scheme is integrated with H.264/AVC, which is assumed to be adopted by the visual surveillance system, to achieve an efficient implementation. The issues of payload, effective embedding/detection and rate/distortion are taken into account to fulfill the requirements of such an application. The experimental results demonstrate the feasibility of this potential system. This scheme is designed under H.264/AVC [3], given the assumption that the traffic surveillance system adopts it to facilitate video transmission and storage in advanced ITS. H.264/AVC is the state-of-the-art video compression standard. Like the previous video standards, H.264/AVC is based on the motion compensated, DCT-like transform coding methodologies. Each video frame is composed of macro-blocks, which are blocks of 16 × 16 luma samples with the corresponding chroma samples. The macro-blocks may be intra- or inter-coded. In inter-coding, they are further divided into sub-macro block partitions of several different sizes for effective motion estimation.

In intra-coding, the spatial prediction based on neighboring decoded pixels in the same slice will be applied. The residual data will be divided into 4×4 sub-blocks and processed by a spatial transform, which is an approximate DCT and can be implemented with integer operations and a few additions/shifts. The point by point multiplication in the transform step will be combined with the quantization step by simple shifting operations to speed up the execution.

The many coding tools in H.264/AVC make the codec suitable to various applications. Since the digital watermarking techniques share certain similarity with the coding procedure, designing a digital watermarking scheme under the framework of H.264/AVC may achieve a great deal of efficiency. The robustness of digital watermark in a specific standard for annotation purposes may not be required. The payload should be high to carry the appropriate amount of information. The efficient execution is important since the coding process of H.264/AVC is already computationally expensive so the digital watermarking procedure should not bring in further heavy burden. Furthermore, the target bit-rate and video quality should be well preserved to fulfill the requirements of the applications.

In 2008: A technique based on "Hybrid DWT-SVD video watermarking" is proposed by 'Lama Rajab, Tahani Al Khatib, and Ali-Al HAj**'[6],** In this paper, They propose an effective, robust, and imperceptible video watermarking algorithm. The effectiveness of algorithm is brought by virtue of applying a cascade of two powerful mathematical transforms; the discrete wavelets transform (DWT) and the singular value decomposition (SVD). Reported experimental results demonstrate the effectiveness of the proposed algorithm. The DWT and SVD are different transform domain techniques and thus provide different levels of robustness against the same attack. More robustness is expected by combining benefits of the two transforms.

In this paper, they propose a hybrid algorithm in which the watermark bits are not embedded directly on the wavelet coefficients, but rather on the elements of singular values of the matrices ***S*** of the frame's DWT sub-bands. They are showing that by embedding watermark bits on the elements of the singular values of matrices ***S*** which have an imperceptible and robust watermarking**.**

In 2008: Hoseok Dol, Dooseop Choit, Hyuk Choi2, Taejeong Kim' gives a histogram based technique for camcorder as “Digital Video Watermarking Based on Histogram and Temporal Modulation and Robust to Camcorder Recording” This paper presents a blind digital video watermarking scheme which is especially robust to camcorder recording attacks and also to a variety of common video processing and geometric distortions. Using the fact that nearby frames of a video sequence are quite similar, the method embeds the watermark by temporal modulation of the frames. The watermark pattern used in modulation is generated based on the pixel-value histogram, which makes extraction free from geometric synchronization. To make it imperceptible, the watermark is adjusted according roughly to the human visual system (HVS). The experimental results demonstrate the robustness of the proposed method to camcorder recording attacks also involving geometric distortions and other video processing attacks such as MPEGs and other compression. The experimental results show that the proposed video watermarking scheme is quite robust to all attacks.

In 2008: ‘Quan Liu, Hong Liu’ proposed a new algorithm “A novel real time digital watermarking algorithm” This paper proposed a novel video watermarking scheme based on MPEG-4 compression standard. For the Intra frames (I-frames), He used a gray image as watermark. The most major difference between the traditional method and the novel scheme is that it need not embed the watermark image into the original public image. Instead, extracting the feature of the I-frames, thus we can gain an ownership map according to the feature of the I-frames and the watermark image. When piracy happens, the copyright owner can reveal his right via the ownership mapping and the feature of the suspected image to extracting the watermarking. For the Inter frames (P-frames), He Choose a partial motion vectors to embed the watermark.

According to the experimental results, the proposed methods are efficient, real-time, blind and robust. The main challenge in designing digital video watermarking schemes is to balance transparency, and robustness, which are conflicting parameters. ‘Jordan’ proposed a watermarking algorithm for MPEG-4 code video stream. He modified the motion vectors to embed watermark. ‘Zhang’ presented a revision algorithm to ‘Jordan’. He chose the higher-amplitude and little-phase macro-blocks to embed watermark in motion vectors. The authors of proposed a MPEG-2 compression watermarking scheme, but watermark information is just a two value images.

This paper, propose a novel MPEG-4 based watermarking algorithm. This algorithm is real-time, blind and robust. It presents a novel watermarking scheme for I-frames. The watermarking image is a gray image. Dislike the traditional algorithm; it is needless to embed the watermark image into the original image. Instead, we build an ownership map according to the I-frames feature and watermark image. When piracy happens, the copyright owner can reveal his right via the ownership mapping and the feature of the suspected image to extracting the watermarking. For the Inter-frames (P- and B-frames), they choose partial motion vectors to embed watermark. This proposed scheme is greatly effective and robust against frame deleting, frame inserting and frame recombining etc. video attacks.

In 2009: ‘Sadik A.M. Al-Taweel and Putra Sumari [45]’ presents his paper in ‘sixth international conference on computer graphics, imaging and visualization’ named as “Digital video watermarking in the discrete wavelet transform domain” In this paper they present a method for a robust watermarking insertion in a video frame. The proposed method works on the uncompressed video based on the spread spectrum communication. The researchers applied the technique in the discrete wavelet transform domain (DWT). The results showed that the watermark has high perceptual invisibility and robust against JPEG compression, geometric distortions such as Downscaling, Cropping, and Rotation, as well as noising.

The watermark was successfully extracted from the video after various attacks. In this algorithm we improve the watermarking technique which was designed by ‘Hartung and Girod’. In their work, they presented an algorithm for embedding the digital watermarks into compressed and uncompressed video sequences. The basic principle is borrowed from the spread spectrum communications. In the spread spectrum communication, a narrow band signal is transmitted over a much larger bandwidth such that the signal energy that present in any single frequency is undetectable. Similarly, the watermark bits are spread by a large factor called chip-rate so that it is imperceptible.

Watermarking Embedding process: The host video frame is transformed into one level DWT decomposition by using the Haar filter. The lowest frequency sub-band coefficients (LL) are selected for embedding. Wi (spread spectrum watermark) is added to the digital video signal Vi, to produce the watermarked video signal, Vi′

$$Vi' = Vi + Wi$$

Watermarked video frame is produced after applying IDWT to the embedded as shown in figure (9)

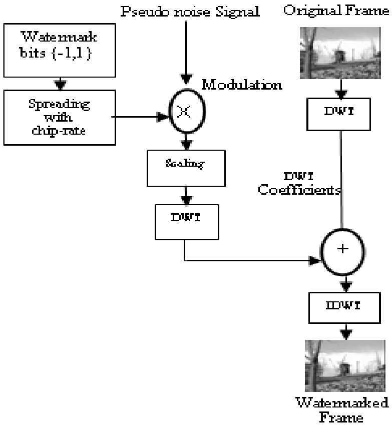


Figure 9: Watermark embedding process in DWT domain

Watermark Extracting process: The watermark is extracted without using the original, un-watermarked signal, by using demodulation where the filtered watermarked video signal is multiplied by the same pseudo noise signal Pi that was used for embedding. This is followed by summation of window of length with the chip rate, yielding the sum Sj for the Jth information bit. The recovery of the watermark bits is more robust, if the original, un-watermarked signal is available. The signal can be subtracted from the watermarked video signal before demodulation instead of the filtering operation because the subtraction removes the interference between the video signal and the embedded watermark.

Experimental result: To evaluate the algorithm, the video clips with 352×240 are used and they are spread with chip-rate = 8. Then they use the PSNR (peak signal to noise ratio) to estimate the performance of the invisibility and the detection ratio of the watermarks to estimate the performance of robustness. Result shows that the watermarked frame with PSNR=40.17 dB, original frame, and watermark frame cropped which show only the centre of watermarked frame. Scaling shows the 50% scaled down watermarked frame. Rotation attack show rotated by some angle watermarked frame. Correlation and compression attack applied and show the good results in watermarked frame, A 3 ×3 averaging filter with coefficients of 1/9 is used in the LPF. The LPF attack causes the decoded watermark to be noisy with the correlation of 0.616. Although the correlation is relatively small, the detection score remains acceptable.

In 2009： **‘**Tamás TOKÁR, Tomáš KANÓCZ, Dušan LEVICKÝ [46]’ proposed a method on “Digital watermarking of uncompressed video in spatial domain’ proposed algorithms of digital watermarking in the context of the video are robust against unintentional attacks, but many of them do not protect enough against malicious attacks. This paper presents a new video watermarking system with improved robustness, which is based on spread spectrum technique. Which verify the enhanced robustness of proposed system against malicious and non-malicious attacks. Some watermarking schemes extract the watermark from arbitrary watermarked frame whereby they need corresponding frame from the original video.

The extraction process of the proposed approach can be performed without knowledge of the original video, which further increases robustness against intentional attacks causing de-synchronization. The presented scheme also resists against frame averaging attack because same watermarks in different frames amplify each other during averaging; Watermark embedding process: The embedding process is performed in spatial domain by modification of frame pixels. The same algorithm is applied for each frame separately whereby all frames are labeled with the same watermark. In the experiments video with frame resolution 320×240 and a binary logo as watermark with size 32×24 were used. Note that video with grayscale frame is represented in true color mode i.e. all color planes (R-red, G-green, B-blue) of the frame are identical. In this paper a new video-watermarking scheme based on spread spectrum technique was proposed. As experimental results show the proposed algorithm is highly robust against various types of attacks.

The main advantage of the system is that watermark extraction process does not require knowledge of the original unmarked video. Due to this fact the system is also robust against malicious attacks that cause de-synchronization of the watermark detector. The disadvantages of the proposed approach are relatively high computational complexity and the need of uncompressed (or decompressed) video for watermark embedding. For these reasons the proposed system is not suitable for applications (e.g. broadcast monitoring) where watermark embedding or extraction must be performed in real time. However some other applications such as copyright protection, fingerprinting or copy control do not require real-time watermarking. The proposed scheme is appropriate for labeling of stored videos such as DVD films or TV movies that are not encoded and broadcasted in real time. The watermark detection and extraction processes are performed in relatively short time because their algorithm does not process whole watermarked video, but only one or several watermarked frames. In future work some modifications of the proposed algorithm are needed, which make it less computationally expensive. S copyright protection, fingerprinting or copy-control do not require real-time watermarking.

The proposed scheme is appropriate for labeling of stored videos such as DVD films or TV movies that are not encoded and broadcasted in real time. The watermark detection and extraction processes are performed in relatively short time because their algorithm does not process whole watermarked video, but only one or several watermarked frames. In future work some modifications of the proposed algorithm are needed, which make it less computationally expensive.

In 2009: 'Hanaa A. Abdallah, Mohiy M. hadhoud , and Abdalhameed A. Shaalan [4]' proposed "SVD-based watermarking scheme in complex wavelet domain for color video"
In this paper, they propose an SVD-based watermarking scheme in complex wavelet domain for color video. Video watermarking is well known as the process of embedding copyright information in video bit streams. It has been proposed in recent years to solve the problem of illegal manipulation and distribution of digital video.

In this study, an effective, robust and imperceptible video watermarking algorithm is proposed. This algorithm was based on a cascade of two powerful mathematical transforms; the 2-level Dual Tree Complex Wavelet Transform (DT-CWT) and Singular Value Decomposition (SVD). This hybrid technique shows high level of security and different levels of robustness against attacks. The proposed algorithm was tested for imperceptibility and robustness and excellent results were obtained. They compared the result with his first proposed algorithm DWT-SVD based scheme and showed that it is considerably more robust and effective. The proposed DT-CWT –SVD watermarking algorithms consist of two procedures, the first embeds the watermark into the original video clip, while the other extracts it form the watermarked version of the clip.
Watermark embedding procedure is as:-

(i) They applied 1-level DT-CWT to the watermark image W.

(ii) Apply SVD to each obtained high pass sub-band.

(iii) Divide the video clip into two video scenes.

(iv) Process the frame of each video scene using DT-CWT and SVD.

(v) Convert every video format from RGB to YUV color format.

(vi) Compute the 2-level DT-DWT for the Y (luminance) matrix in each frame. This operation generate high six sub-band.

(v) Apply SVD to each high pass sub-band.

(vi) According to the rule, modify the singular value in each high-pass sub band of the 2-level decomposition with those of the watermark.

(vii) Obtain the 6-subbands of modified DT-CWT coefficients.

(viii) Finally apply the inverse DT-CWT using the modified DT-CWT coefficients. This operation produced the final watermarked video frames.

(ix) Convert the video frame from YUV to RGB color matrix. Then reconstruct the frames into final watermarked video scene. Then reconstruct watermarked scenes to get the final watermarked video clip.

Watermark Extraction procedure is as:-

(i) Divide the watermarked video clip into two watermarked scene.

(ii) Process the watermarked frames of each watermarked video scene.

(iii) Convert the video frames from RGB to YUV.

(iv) Compute the 2-Level DT-CWT for the frames.

(v) Apply SVD to each high-pass sub band.

(vi) Extract the singular value of each high-pass sub band.

(vii) Construct the DT-CWT coefficients of the six high pass sub-bands by computing the singular vectors.

(viii) Finally apply the inverse DT-CWT to each set to construct the visual watermarks. And then repeat the same procedure for second video scene also.

Experimental results demonstrated the blindness and robustness of his proposed method as it successfully extracted the watermark from each frame without using the original video. The extracted watermark was exactly the same as the embedded original watermark. Comparing to the DWT-SVD this technique gives the best results.

In 2010: 'Liu Guang-qi, Zheng Xiao-shi, Zhao Yan-ling, Li Na [47]' proposed "A Robust Digital Video Watermark Algorithm Based on DCT Domain" in 20IO International Conference on Computer Application and System Modeling (ICCASM 2010), In this paper, a highly robust digital video watermarking technique is given. First of all, the watermark information is encrypted by Arnold transform. Then it is embedded in DCT domain by high-frequency coefficients correlation algorithm in RGB frames of source video file. The field tests indicate that the video file with the watermark information is transparent, and strong anti-aggressive. In the embedding process they applied Arnold transform on watermark image which is to be embedded in original video. First original video is converted from YUV frame to into RGB frame. Then 2-Level DCT is applied in R, G and B frame individually. With the scaling factor watermarks image is embedded. On these R, G, B frame. Then for reordering the video frame IDCT is applied and then it will convert in in YUV color matrix from the RGB matrix. And for extraction process watermark video file is converted from YUV color space into RGB space. then applied 2-D DCT on these frames. After applying Arnold transform following with the correlation coefficient calculation watermark image is extracted. The algorithm can go against many kinds of attacks, such as adding random noise, Gaussian noise Salt-Pepper noise, wavelet compression and sharpening. Theoretical analysis and experimental results show that the algorithm enhances the security of watermark and has very strong robustness and transparency.

In 2010: 'Tian Hu and Ji wei' Proposed "A digital video watermarking scheme based on 1-D DWT" Using the stability of the low-frequency components in 1D-DWT(1-dimension discrete wavelet transform), a blind video watermarking scheme is proposed in the paper. The watermark is embedded in the blocked low-frequency image by adjusting the average pixel value of each block. The experimental results demonstrate that the watermarking method has strong robustness against some common attacks, such as compression of MPEG-2, noise attack, frame exchanging. The scheme is less complex and has smaller calculation deal, so it can meet the real-time requirement. A method of embedding watermark based on 1D-DWT (1-dimension discrete wavelet transform) in a raw video is proposed in this paper. Firstly, 1D-DWT to the luminance of two consecutive frames and then can obtain a low frequency image, which is the same size as the raw frame. Then the low-frequency image is partitioned into equal-sized sub-images. Then they calculated the average pixel value of each block and then the watermark, which is usually a binary image, is embedded in these blocks according to the interval where the average pixel value of each and then the watermark. When blind detecting watermark, the low-frequency image is also partitioned and the average pixel value is computed to judge the watermark. This scheme is robust against many common attacks such as MPEG-2, noise attack, frame exchanging and so on. Embedding of watermark is as, In order to enhance the robustness of the watermarking, the watermark is embedded in low frequency image which results from temporal decomposition of the luminance of the original video frames by 1-D discrete wavelet transform. The scheme greatly reduces the complexity of the watermark embedding and extracting, and can meet the real-time requirement.
The procedure of embedding watermark is described as follows:

(i) The luminance of the former two frames, is extracted from the original video sequence, and transformed by 1-D discrete wavelet transform. Then a low-frequency image and a high-frequency image are obtained

(ii) The low-frequency image is blocked by a -by- a. And the average pixel value of each block is calculated, denoted by:

$$K = \{k\,(i, j),\, i = 1, 2,...,M;\, j = 1, 2,..., N\},\, 0 \le k(i, j) \le 255$$

The value of integer a is determined by the size of the video frame and watermark, usually $3 \le a \le 16$.

(iii) The pixel value from 0 to 255 is divided into n (the smallest positive integer that is not less than 255/ L) intervals by the quantization step L , and each interval corresponds to 0 or 1 alternate, shown in Fig.1. Then k (i, j) belongs to which interval is determined, and a matrix C is created that records the corresponding 0 or 1, described as:

$$C = \{c\,(i, j),\ i = 1, 2,...,M;\ j = 1, 2,..., N\},\ c\,(i, j) \in \{0,1\}.$$

(iv) Then comparing the $ws\ (i, j)$ and $c\ (i, j)$, if $ws\ (i, j) = c\ (i, j)$, the average pixel value $k(i, j)$ is adjusted to the centre value of the corresponding interval, otherwise $k(i, j)$ is adjusted to the centre value of the next interval.

(v) Blocks are transformed by inverse 1D-DWT, getting the watermarked frame.

(vi) In order to realize the real-time requirement, the watermark is embedded once in every 10 frames.

Blind detecting video watermark: as the average pixel value of the low-frequency image is adjusted to embed the watermark, we can judge the watermark information by computing the average pixel value.

Procedure for detecting the watermark is as;

1. The luminance of the former two frames is extracted from the video to be detected and is transformed by 1-D DWT. And a low-frequency image is obtained.

2. The low-frequency image is blocked by a -by- a . And the average pixel value of each block is computed, described as:

   $$K' = \{k'(i, j),\ i = 1, 2,...,M;\ j = 1, 2, ..., N\},\ 0 \le k'(i, j) \le 255.$$

3. That each average pixel value belongs to which interval is determined by the quantization step L. Then we record corresponding 0 or 1 in a matrix, denoted by $e\ W'$

4. At last, we can get the watermark We by anti scrambling the We' , described as:

   $$We=\{We(i,j),\ i=1,2,.....M;\ j=1,2,.....N\};\quad We(i,j) \in (0,1)$$

5. The correlation between *We* and the original watermark *We*' Is computed.

Using the stability of low-frequency components in 1-D DWT domain, the watermarking scheme is proposed in the paper that the watermark is embedded in the blocks according to adjust the average pixel value of each block. The experimental results demonstrate that the watermarking scheme is robust against multiple attacks. Because the algorithm is less complex and the watermark can be blind detected, the method provides a practicable scheme for the real-time control of video.

In 2010: 'M. Omidyeganeh et al' proposed "Robust Digital Video Watermarking in an Orthogonal Parametric Space" This paper presents an event based scheme for uncompressed video watermarking. The video signal is assumed to be a sequence of overlapping visual components – called events. Authors address this overlapping structure of video contents and present an event based approach through employing a block based Temporal Decomposition (TD) scheme. The TD describes a set of spectral parameters of the video as a linear combination of a set of temporally overlapping compact event functions. They have applied the decomposition results to digital video watermarking. To construct the matrix of parameters in the TD, multi-resolution Singular Value Decomposition (MR-SVD) is utilized and singular values of a set of MR-SVD coefficients are selected as the extracted spatial features of each frame of the video signal, and then the feature matrix is decomposed based on the TD method. The watermark is embedded in the TD target vectors which are the orthogonalized parameters representing the video events.

Experimental results show that this scheme is robust against collusion attack, frame swapping, frame dropping, uniform noise attack, median filtering attack, and the MJPEG (Motion JPEG), the MPEG-1, and the MPEG-2 compressions attacks. This method is basically different that embeds the watermark in an orthogonal matrix extracted from a set of successive frames through a de-correlation process accomplished by the TD in the selected parametric space. The TD was first introduced in 1983 and has been used successfully to resolve overlapping nature of the phonetic evolution of speech signals. It seeks for local correlations in the spectral feature space, within overlapping segments of the signal, to locate individual events. They decompose the visual events by searching for local correlations in feature space that is generally based on the video frame contents. The spatial features used are extracted from the MR-SVD coefficients of each frame. They believe this work to be the first analytical approach to the problem of data embedding in video signal.

In 2010: 'Hongaang Zhang et al' Proposed "A NEW COMBINATION FEATURE OF S-LBP AND MAIN COLOR DESCRIPTOR FOR VIDEO FRAME RETRIEVAL**"** In this paper, authors draw a Local Binary Pattern (LBP) and main color descriptor into content-based video indexing and retrieval. LBP is a powerful texture descriptor for its tolerance against illumination changes and its computational simplicity. Main color descriptor is used for representing main color distribution of the image. they propose a simplified LBP (S-LBP) operator as the texture descriptor. In most cases, texture distributions that ignore the actual positions or spatial arrangement in the image are not sufficient for representing an image. Therefore, we use zigzag based Run-length coding principle to produce S-LBP patterns histogram. Then we apply the combination of S-LBP feature and main color descriptor to represent an image in video retrieval. This paper mainly proposed a simplified LBP operator based on zigzag run-length structure. Then they combine the S-LBP and main color descriptor to produce features for representing a frame or an image in the video frame indexing and retrieval systems. The experiment that to find which video a given query frame comes from demonstrates our methods performs effective. For a large database, the proposed methods can be a solution in terms of memory management and time complexity since the computation of features is simple and efficient.

In 2010: 'Manabu Hirakawa, Junichi Iijima' propsed "Application of Digital Watermark Technology for Movie Data in Streaming Distribution Service" author investigate digital watermarking as a method for protecting for video content in this research, and consider the related technologies and methods for implementing the watermarking. In order to compare digital watermarking technology with existing technology, they have divided the characteristics of digital watermarking technology into three elements. And discuss new concepts regarding each element and clarify its characteristics. Authors make a proposal for the copyright protection of digital content, and also propose how copyright protection can be applied in the service field. To facilitate meaningful comparison between existing technologies, in this research paper author categorize the necessary requirements for digital watermarking technology into three elements: quality, strength, and data volume.

Retention of Image Quality (Quality Axis): Because digital watermarking embeds information into the image data itself, the watermarked image differs from the original. As a result, a trade-off relationship is created between image quality and the accuracy of detecting the digital watermarking. When difference between the original image and watermarked image is small, the watermarked image is similar to original image and thus considered to be high quality. A level of image quality such that human senses cannot detect any deterioration is required, and the strength and information volume of the digital watermarking must both be maintained, as will be explained later. Therefore, the available space to use processing technology on the image is extremely limited.

Strength and Confidentiality (Strength Axis): The digital watermarking information must not be lost when the image is processed, such as in DA/AD conversions including editing, alteration, and printing. The objective is to maintain the integrity of the watermark, especially against deliberate and malicious alterations. Accordingly, the embedded information must be decipherable only when the detection algorithm is used, or when someone granted those rights attempts to do so.

Data Volume to be Manage (Data Volume Axis): The volume of data to be embedded when using digital watermarking technology depends on the intended use, and the range is limited. The volume of data to be embedded will be great when the copyright information itself is embedded with the digital watermark. However, a method that uses a separate information management system and only embeds ID information into the image can reduce the volume of data to be embedded. Through these approaches, the volume of data to be embedded can be adjusted by selecting the management method. Considering the existing problems with respect to the three elements of digital watermarking, namely, image quality, digital watermark strength, and volume of embedded data, they developed a new method that is expected to improve each element.

Authors discuss improvements to the frame unit into which the digital watermarking information is inserted. Recently, with the Internet becoming universally available and with the advancement of digitization, it has become simple for websites to handle videos. This has led to the existence of a multitude of websites that post movies and video data. Compression and format conversion of video data is necessary to handle movies. However, in order to reduce the file size, these methods delete frames that do not differ from the preceding or following frame, or extract only those frames with a large change to reconstruct the image data. Therefore, even if information is inserted into every frame, the embedded information may be lost when the video data is reconstructed, and existing methods are inefficient in terms of processing load. To avoid this problem, an improved method takes a certain number of frames and consider them as a one set. This new method requires reduced processing load and increases image quality, in comparison with conventional methods. The new method takes several frames as a single unit in order to insert the digital watermarking information. Consequently, the processing load from embedding the information is light and the method is efficient. From the perspective of image quality, in comparison with the existing method of Inserting digital watermarking information into every frame. This new method of performing image processing on a group of several frames results in a higher quality image. When compared with the original image without a digital watermark, the number of frames on which image processing is performed is less than when compared to the existing method. The principle objective for using digital watermarking technology is extended beyond copyright protection, and taken a step further to consider mobile services. Traditionally, digital watermarking technology has been considered to be a security technology for protecting copyright. If this is interpreted as defense, the special characteristic of this research paper is that applied digital watermarking technology to the mobile service field as a security technology for offense.

In 2010 IEEE international symposium on multimedia ‘Aditya Vashistha, Rajarathnam Nallusamy, and Sanjoy Paul’ proposed a novel technique on watermarking which is “NoMark: A Novel Method for Copyright Protection of Digital Videos Without embedding data” In this paper, author present the No-Mark Method, a robust, reliable, and efficient scheme for copyright protection of digital video content without embedding any data in to it.

This method is based on visual cryptography and can be used to watermark individual scenes in a video and hence protects not only the copyright of complete video but also of each individual scene in the video. The method is robust against video fragmentation attack, unauthorized insertion of scenes from a protected video into another video and various other video watermarking attacks. There is no involvement of any notary agency to establish copyright ownership of a digital video. this paper present a method for watermarking video content using *(2, 2)* visual secret sharing scheme in which first visual cryptographic share is created using a secret key, watermark pattern and averaged scene image of the video to be protected during the No-Mark protection process. Second share is created using the same secret key and averaged scene image of the video to be verified during the No-Mark verification process. Watermark pattern is constructed by overlapping these two shares during the verification process. This retrieved and the original watermark patterns will be same only if the averaged scene images and the secret key used in verification process are same as those used in the protection process. This principle is used to establish copyright protection over all or selected scenes in a video.

In 2011: ‘Lufang Liao et al’[50] in the International Conference on Internet Computing and Information Services proposed “A New Digital Video Watermark Algorithm Based on the HVS” in his paper they proposed The algorithm applied to video watermark based on HVS which is rare recently, but adaptively selecting the embedding position and the embedding strength according to the host (such as videos, images etc.) is necessary, which can make robustness and invisibility best balanced. This Paper gives a new algorithm about digital video watermarking based on HVS, which makes digital video watermark greatly improved. In his experiment they select a video named 1. Avi (the number of frames is 352), experimental platform is vc6.0, the size of the watermark is 20 x 20. Firstly, they embed the watermark into the video without HVS, using the stable strength 30 and 8 separately (where 30 is the maximum of the strength set, 8 is the minimum), then they embed the watermark based on the HVS. The strengths

a= {12, 10，8, 18，13，11，30，25, 15}.

Then select some frames embedded the watermark randomly to calculate the value of PSNR. Then some has been done on this watermarked video such as Gaussian noise. They randomly select the 8 frames to extract the watermark. General stability attack(such as noise attack ,filter attack, re-sampling etc.), jpeg compression attack. After these attacks, we can clearly extract the watermark. But this algorithm can’t effectively resistant geometric attacks (such as rotation), besides they need to find out methods about how to adaptively selecting the embedding position to improve this algorithm.

In 2011: 'Jinbao Song, Jinliang Wan and Xin Xin' proposed "An Internet TV Monitoring System Using Digital Watermarking Technology" this technique is proposed to introduce the real-time video digital watermarking technology into the monitoring of the Internet TV which is out of International broadcast and TV system, building an effective monitoring system to resist the spread of illegal and pirate information. The monitoring system is expected to be of powerful operability, Scientificity, Strictness, Normality and Procedural. The system will fill in the domestic blank and to guarantee the culture security, contribute to the sound development of the culture industry. The main technology used in Internet TV Monitoring System is Digital Video Watermarking technology. From the references of this paper it can be seen that patents and products of digital watermarking technology have been obtained in the video real-time monitoring. On the whole, applying the digital watermarking technology into Internet TV monitoring system is technically feasible.

The main problem that TV program monitoring faces with is the effective monitoring of TV content legitimacy (whether passing examination and approval) and security (whether be tampered with). It is to ensure the legitimacy and security of broadcasting only by the TV program broadcast process uninterrupted real-time monitoring. And now simply relying on manual monitoring or sampling inspection is time-consuming, laborious and fails to effectively monitoring. Meanwhile, the existing regulatory system is not suitable for real-time monitoring of TV-on-demand, which is mainly adopted by the Internet TV. In addition, the monitoring of Internet illegal information now is basically only for monitoring the text messages. For the Internet TV that is the application of sounds, pictures and video, there is a great limitation in the existing monitoring equipments.

This paper proposed pay more attention to the science, normalization, rigor and procedural, which will solve the above problems. Internet TV monitoring system is a supplement and promotion for the current broadcast regulatory system, and it doesn't increase the regulatory cost over the existing regulatory system, which will not increase the national financial expenditure. Compared with the existing regulatory system, Internet TV monitoring system mainly increase television monitoring equipment --- digital watermarking monitors and program approval equipment---digital video program watermarking embedded system, and the full cost of the equipment is complete by monitored side and intermediary party. As the Internet TV monitoring system automation, Networking, Intelligence level is high it will save more man power than the existing regulatory system, and is more appropriate for management and costing savings. It can be seen from the references of this paper [20] that the proposed Internet TV monitoring system is well compatible with the existing policies and systems, it is also easy to docking with the current management system, and it can help for implementing national policies, laws and regulations in radio and television. as a concluded remarks this paper introduces a way of building a perfect system of auditing program before broadcasting and monitoring program after broadcasting by using digital watermarking technology, which can ensure that the content is safe from very beginning. And this technology can also provide strong technical support for promoting the healthily and orderly development of Internet TV.

In 2011: 'Hitesh Panchal et al' proposed a paper on **"**Digital Watermarking on Extracted Key Frames from Uncompressed Color Video using 4-Level DWT" This paper propose a digital watermarking scheme on extracted key frames from uncompressed color video with another color watermark video using DWT. So, more information is embedded into original video while reducing the computation time and complexity compared to other schemes. This scheme is robust against attacks of frame dropping, frame averaging, noise addition and statistical analysis. Experimental results are shown to verify effectiveness and imperceptibility. An original uncompressed color video and color watermark video are taken as an input and converted into frames. By using a key frame extraction algorithm based on X2 histogram matching method, key frames of an original uncompressed video are selected to be watermarked; and this will decrease computation time and complexity of the algorithm. Then, key frames of original video and watermark video are decomposes into three different RGB components and a 4-level discrete wavelet transformation (DWT) is applied on them to obtain thirteen sub-bands in the frequency domain [5]. This allows us to embed watermarks in those regions where Human Visual System is known to be less sensitive to, such as the high resolution detail bands (LH, HL, HH). Embedding watermarks in these regions increase the robustness & imperceptibility at little to no additional impact on image quality. and can also embed the binary secret key along with watermark frame. So, watermark can be recovered from the watermarked video only using this secret key.

The embedding algorithm embeds the watermark frame and secret key into sub-bands (LH, HL) of key frame. The watermarked component is achieved by applying inverse discrete wavelet transform (IDWT) to the wavelet coefficients. The RGB color components are then concatenated together for each watermarked frame. Saving the whole frame in a new video file is the final step. Peak signal to noise ratio (PSNR) is calculated to evaluate the video quality and imperceptibility Watermark detection process is an inverse procedure of the watermark embedding process. The extraction process requires the threshold value used for detecting key frames from the watermarked video. Decompose RGB components of key frames and apply 4 – level DWT to each RGB components. Watermark frames are extracted after confirmation of secret key, apply 4 – level IDWT (inverse discrete wavelet transform) and combine all watermark frames to get watermark video. The proposed algorithm extracts the watermark directly from the decoded video without any access to the original video (blind mode).

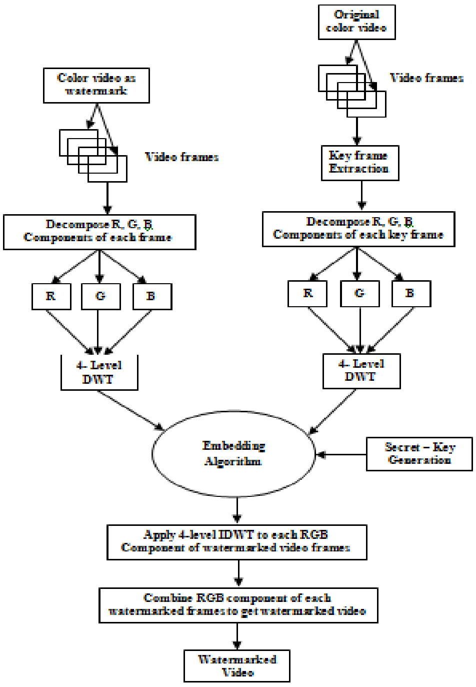

Original color video
Video frames
Color video as watermark
Video frames
Key frame Extraction
Decompose R, G, B, Components of each frame
Decompose R, G, B, Components of each key frame
R
G
B
R
G
B
4- Level DWT
4- Level DWT
Embedding Algorithm
Secret – Key Generation
Apply 4-level IDWT to each RGB Component of watermarked video frames
Combine RGB component of each watermarked frames to get watermarked video
Watermarked Video

Figure 10: Embedding process for 4-Level DWT

1. WATERMARK EMBEDDING: After, extracting key frames from the original color video, only key frames are watermarked with the watermark video. Here, computation time is reduced sufficiently because watermark is not embedded into each frame as in other watermarking scheme. This is principal advantage of this scheme. The following points summarize watermark embedding process.

    a. Each key frame resulted from the key frame extraction algorithm is decomposed into three color components (R, G, B).

    b. Apply 4 - Level DWT to RGB components. The watermark is embedded into HL and LH bands (mid frequency bands). So convert each pixel value of key frame into binary (8-bit).

    c. The watermark color video is converted into binary color video (so each pixel value will be either ‘0’ or ‘1’). The pixel values of binary watermark color video is stored into an array W(i, j). The generated secret key is appended into this array.

    d. Apply the watermark in one of the four least significant bit of pixel value. Can use 6th bit of every 8-bit pixel. If 6th bit is equal to ‘1’ then WK (i, j, k) is equal to ‘1’ else WK (i, j, k) is equalto 0’. WK (i, j, k) is the array to store the information for the original video extraction from the watermarked video. (i, j) is the pixel position of particular band and k is the frame number.

    e. Now start embedding the watermark from HL4 (4th level mid frequency band) and then if W (i, j) = 1 then 6th bit of 8-bit pixel is equal to ‘1’ and else ‘0’. This process is repeated for frequency bands LH4, HL3, LH3, HL2, LH2, HL1, LH1.

    f. Store resultant watermarked video frame data into array wk (i, j, k).

    g. Apply 4- Level IDWT to each component of watermarked video frame.

    h. Combine RGB component of each watermarked frames to get final watermarked video.

2. WATERMARK EXTRACTION: The watermark video (frames) can be recovered (extracted) from the watermarked video for the proof of authenticity without any access to the original video. This procedure is summarized below.

    a. Load watermarked video, convert into frames.

    b. Extract key frames with the threshold value used in watermark embedding.

    c. Decompose RGB components and apply 4 level DWT.

    d. Convert each pixel value of mid frequency bands (LH, HL) into binary.

    e. Compare the secret key for the confirmation.

f. Check if 6th bit of pixel value is ‘1’ then WR(i, j) =1, where WR is the recovered watermark and secret key matrix. If 6th bit of pixel value is ‘0’ then WR (i, j) = 0.

g. Decompose watermark data and secret key from the matrix WR.

h. Repeat this procedure for all three RGB components of watermarked images.

i. Apply 4 – level IDWT to RGB components of each frame. Combine all these components to get watermark frame.

j. Convert watermark frames into video.

As a conclusion author, Here showing that the algorithm is proposed for Digital watermarking on extracted key frames of uncompressed color video with color watermark video using DWT. Key frames are extracted from the original color video with the help of x2 Test histogram matching difference between consecutive frames with appropriately decided threshold. Converted binary watermark color video frames are embedded into key frames of original video. The 4-Level DWT transformation has been used for embedding watermarks into its mid frequency bands. Because only key frames are watermarked, the computation time is reduced sufficiently. Proposed scheme is robust against attacks like frame dropping, frame averaging and other statistical analysis. This work can be extended for compressed and uncompressed video with large set of frames as either in color or binary watermark to hide in to the compressed video information of the same. It is possible to have analysis of either side with all the effects with short and long period of videos.

In 2011: ‘Dong Zhong’ [51] gives a technique in ‘2011 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference’ Based on “The Study of Digital Video Watermarking Algorithm Based on the Protection of Multimedia Courseware” This paper proposes an improved digital video watermarking algorithm based on the protection of multimedia courseware according to the analyzing the traditional method of multimedia courseware copyright protection. In this paper, the streaming video watermarking embedding scheme of protecting multimedia courseware copyright has been designed by using the algorithm, meanwhile, the algorithm has been studied, the study shows that the algorithm can improve the effect of the video copyright protection greatly. According to the characteristics of multimedia courseware streaming video, this paper puts forward the postposition watermarking embedding scheme about the copyright protection, this algorithm is directly embedding watermarking to the MPEG compression encoding and it doesn't pass the process of encoding and decoding video images. The algorithm hasn't effect on the quality of video images, so it can guarantee the quality of video images effectively. The watermark algorithm embedding video based on DCT can approve the copyright of multimedia courseware. The advantage of the scheme is that it has no necessary for the process of fully decoding and the influence of the video signal encoding is lesser, improving the efficiency of watermark embedding and extracting. this paper proposes an improved video watermark algorithm based on DCT coefficient according to the method of the current copyright protection for streaming video: DCT coefficients watermarking is a kind of watermarking based on MPEG4 compression, it can change the I frame DCT coefficients in the process of compressing streaming video. It can complete the watermarking embedding in the process of decoding for encoding data, and the process of watermarking extracted is happened in compressed domain. I frame is the reference frame of B frame and P frame, if I frame DCT coefficients has been modified directly, it may cause distortion accumulation, it makes the image distortion recovering from B frame and P frame. Therefore the watermarking algorithm based on DCT coefficients can reduce distortion by adopting motion compensation measures to guarantee video quality. As a conclusion remarks in this paper the streaming video watermarking embedding scheme of protecting multimedia courseware copyright has been designed by using the algorithm, meanwhile the algorithm has been studied, the study shows that the algorithm can improve the effect of the video copyright protection greatly.

In 2011: ‘Xing Chang, Weilin Wang, Jianyu Zhao [52], Li Zhang’ in 2011 Seventh International Conference on Natural Computation, propose “A Survey of Digital Video Watermarking” , The digital watermarking for video is an effective method to protect the video copyright. Based on the previous video watermarking techniques, this paper summarizes their theories, features, model and classic algorithms and then discusses the algorithms' advantages and disadvantages. Finally, the key techniques and the development tendency of the video watermarking are discussed. In this paper the author compare various techniques of watermarking in different approach with the development of video compression standards, video watermarking technology develops from the first generation to second generation. The algorithms, which have nothing to do with the video content, are the first generation of video watermark technology. Those, which base on the video content, belong to the second generation of video watermarking technology. Mostly first-generation watermarking scheme, which extends the watermark energy to all the pixels in the frame, focuses on the discussion of computation and watermark strength, regardless of content. While the second generation of video watermarking scheme pays more attention to the combination of the watermark and the synchronization of the watermark. Above all, watermarking scheme based on video content or video object attributes is a major development direction of video watermarking.

In 2011: ‘Tomáš KANÓCZ, Peter GOC - MATIS, Patrik GALLO*, Dušan* LEVICKÝ [53]’ proposed a “Real-time digital watermarking based on SVD” This paper deals with real time video watermarking using Singular value decomposition (SVD). The last part of the paper describes experiments conducted on the proposed watermark embedding method. The goal of these experiments was to test the robustness of the method presented in the paper against several watermarking attacks. In the proposed watermarking scheme Block of watermark embedding performs: video content loading, SVD, watermark insertion and inverse SVD. Inputs of this block are original video and embedded watermark. In this, six video sequences with different dynamic properties were used in experiments (Dynamic, Mezzo Dynamic and Lightly Dynamic). Resolution of all video sequences is 576x240 pixels. Videos are cut into 10 seconds long sequences and the frame rate is 25 fps. Video sequences are uncompressed and they are in true color mode. The video frames where converted to YCbCr model from RGB. Only the luma component was modified in order to avoid information loss from chroma sub sampling. The watermark is embedded into previously selected frames to decrease computation time.

The process of watermark embedding can be described by the following equation:

$$S_w = S_{original} + \propto S_{vodz}$$

where S_w and $S_{original}$ are diagonal matrix coefficients of marked and original luma elements. $\propto$ is the power factor of the embedded watermark. Increased $\propto$ results in increased robustness, but lowers perceptual transparency. After modifying diagonal matrix coefficients by the embedding process an inverse SVD is applied.

This can be described by the following equation:

$$Y_w = U.\, S_w + V'$$

where *Yw* is a luminance matrix modified by watermark embedding, *Sw* is marked diagonal matrix and *U*, *V'* are unitary matrices of the original video. In the end of the watermark embedding process the marked frame is converted from YCbCr to RGB.
In extraction process the process of watermark extraction can be described by the following equation:

$$S_{ext} = S_w - S_{original}$$

where S_w and $S_{original}$ are diagonal matrix coefficients of marked and original luma elements. S_{ext} is diagonal matrix of the extracted watermark. The last step is inverse SVD which's result is the extracted watermark. It can be described by the following equation:

$$W_{ext} = U_w.\, S_{ext}.V'_w$$

Where U_w *and* V'_w are unitary matrices of the original watermark, which represent horizontal and vertical frame edges and the geometry of the real watermark depends on them. S_{ext} is a diagonal matrix. This matrix is the result of subtracting the diagonal matrix of the marked and original video frame. The final watermark is the average of all the extracted watermarks. The quality of the extracted watermark after the attacks was judged by objective aspects, which were Mean Square Error (MSE), Peak Signal/Noise Ratio (PSNR) and also Bit Match (BM). The influence of the embedding process was measured is compared .When the power of watermark constant factor is increased the PSNR is decrease. The constant factor is linked with robustness.

In 2012: 'Jianfei Li,Aina Sui [54], '2012 Fifth International Joint Conference on Computational Sciences and Optimization' "A Digital Video Watermarking Algorithm Based on DCT Domain" In order to solve the conflict with robustness and invisibility of video watermark, the algorithms proposed in this paper select certain blocks according to the texture. By using the binary image to deal with logistic chaotic map and error correction coding as watermarked data can improve the robustness and security. The low frequency signals of the selected blocks are modified such that their Discrete Cosine Transform (DCT) fulfills a constraint imposed by the watermark code. Experiment results show that this algorithm provides a larger embedding capacity and has a certain robustness and invisibility. The basic idea of this paper is to embed the watermark information into the lower-frequency coefficients of DCT coefficients. The main characteristic is that the 8 * 8 blocks, in which they embed the watermark information, have to satisfy the following two conditions: The first condition is to calculate a relatively small interval of DC coefficient according to each video image's biggest DC coefficient and the smallest DC coefficient firstly, only when the DC coefficient of current block are between the intervals, do it to meet the first condition. The second condition is to calculate the number of non-zero coefficient after they are quantified in order to show every block's texture complexity, only when the texture complexity meets certain conditions, we can embed watermark information into the current block.

Watermark Processing: They make the binary image's data that is encrypted with Logistic chaotic map and the correction coding as watermark information. Its every bit of data is expressed as W, and the value of W is 0 or 1.

Calculate Characteristics of DCT coefficients: For one image information of the video they make 8 * 8 Discrete Cosine Transform for its luminance components, and isolate the high-frequency coefficients and the low frequency coefficients. The coefficients of the block's top left corner are the lower-frequency coefficients whose amplitude is bigger, and others are the high-frequency coefficient whose amplitude is smaller. Then we statistics out the biggest DC coefficient and the smallest DC coefficient of the whole picture frame's luminance component.

Select the Embedding Blocks and Embed Watermark: Through the above calculated results from the minimum and maximum of DC coefficient, authors calculate a smaller interval of DC coefficient among larger DC coefficient and small DC coefficient; meanwhile they also calculate the texture complexity of each 8*8 block. they embed watermark information into the block, whose DC coefficient is on the above smaller interval and texture complexity meets certain conditions. For every qualified 8 *8 block, our experiments is to change the value of each block's DCT coefficients according to the Digital bits of w (n) (n = 0, 1, 2, 3)，the specific method is as follows: the positions that is 4, 11, 18 and 25(the four lower frequency positions) in 8*8 DCT coefficient block, their DCT coefficients is divided by the quantization step Q, and then rounding as H, Then if the result of H mod 2 is equal to the corresponding w (I), we set the DCT coefficient value to H, otherwise set the corresponding DCT coefficient to H+Q. repeat the process until all the watermark information is embedded into the video sequence.

Inverse discrete cosine transform: Finally we do Inverse Discrete Cosine Transform for the video sequence, in which we have embedded the watermark information. The basic process of extracting watermark information is an inverse process of embedding watermark information. We can extract all the embedded data by calculating the value of DCT coefficients after quantification in each block, which also meets the above two conditions, and to get the meaningful watermark information after decrypting

Experiments show that this algorithm owns greater capacity, and has certain robustness in allowing range of video watermark's invisibility. Of course, there are still many unresolved issues, such as how to prevent lower quality after compressing, how to resist random attacks in real time request, and how to resist the frame attack. These are all the challenges to meet in the watermarking technology. We will give further research in these fields in the future.

In 2012: 'Satyendra N. Biswas et al' proposed [55]"MPEG-2 Digital Video Watermarking Technique" The method proposed herein embeds several binary images decomposed from a single watermarked image into different scenes in a video sequence. The spatial spread spectrum watermark is embedded directly into the compressed bit streams by modifying the discrete cosine transform coefficients. In order to embed the watermark with minimum loss in image fidelity, a visual mask based on local image characteristics is incorporated. Simulation experiments demonstrate that the developed technique yields effective and robust protection against conventional spatial strikes, *viz*. scaling and frame averaging besides temporal attacks. In this paper, a gray scale image is used as watermark signal. The gray scale image is first converted into multiple bit plane images and then DCT is applied to all of them. These multiple sets of DCT coefficients are embedded in the original video bit stream. Only single set of these DCT coefficients corresponding to a single bit plane image has been used for embedding in all of the video frames of a single scene. When a scene change occurs, another set of coefficients corresponding to another bit plane image is employed. So, all the frames in a scene contain the same watermark information and different scenes of a video embed different watermark information. Checcacci *et al.* [11] concluded that watermarking to each and every frame in the video using a single image leads to problems in maintaining statistical and perceptual invisibility. To overcome this problem, a set of bit plane images is used instead in the method proposed herein. This strategy gives a boost against frame dropping as well as frame averaging. For efficient processing, the compressed video bit stream is first partially decomposed into DCT coefficients and other related information like that of header and shape, motion vectors, synchronization and so on. The rest of the information remains unchanged for later use. The characteristics of the image are analyzed based on the decomposed information in order to find the scene change as well as to select the appropriate DCT coefficients. For controlling the data rate, not all but only the selected DCT coefficients are modified. The selected DCT coefficients are embedded with the DCT coefficients of the watermark signal. Then, the modified DCT coefficients and all the unchanged information (side information and unchanged DCT coefficients) are used to reconstruct the final watermarked video bit stream.

Watermark Processing: A 256 gray image of size *M*x*N* is used as watermark signal so that each pixel of the gray image needed to be represented by 8 bits. As shown in Figure 3, the image is first decomposed into 8 bit planes or binary images. Then, each binary image is used as an independent watermark image signal. Before embedding the watermark into the host signal, DCT is applied to the binary watermark images. The different sets of transformed watermark signals are then embedded into different scenes and all the frames in a specific scene are used as a single set of watermark signals so that the proposed scheme can resist several conventional attacks.

Watermark Embedding: The video bit streams are partially parsed and watermarked according to the information of a specific scene and image characteristics. Then, the watermarked bit streams are reconstructed and framing information is added. Finally, the watermarked video is stored or delivered to the mainstream video network for further use. In this each GOP contains an I-frame followed by a series of P-frames and B-frames. MPEG-2 does not insist on a regular GOP structure. For example, a P-frame following a shot change may be badly predicted since the reference picture for prediction is completely different from the frame being predicted. Thus, it may be beneficial to code it as an I-frame instead.

Watermark Extraction: This is a blind detection of embedded watermark, as it does not need the original video stream. The suspected video stream is processed in order to detect the watermark signal. Video stream is first analyzed for scene change detection. Since a spatial watermark is used, watermark detection is performed on the luminance component after decompressing the video bit stream. First, resolving of the scale and orientation synchronizes the detector and then, the watermark message is read and decoded. The DCT coefficients of the bit plane watermark signal are recovered from the embedded host signals. Inverse discrete cosine transform (IDCT) is applied and then a binary bit plane image is obtained using a threshold value. The threshold value is estimated from the entropy computation. Because an identical watermark is used for all of the frames within a scene, so multiple copies of each bit plane watermark need to be obtained. Hence, each bit plane watermark signal is estimated by averaging the watermarks extracted from different frames in a specific scene. All the bit plane watermarks are recovered from successive scenes of a video clip. Then, the watermark image is constructed from all the recovered bit plane images.

Experimental results demonstrate that the proposed technique is very robust against several attacks such as collusion, frame dropping, blurring, temporal shifts and many other spatiotemporal manipulations. Robustness of the scheme can be further improved by combining with audio watermarks. When security becomes more important, all of I, P and even B frames could be watermarked in uncompressed domain with a higher computational time. The developed technique can be readily extended to do so with minor modifications.

In 2012: 'V Senthil and S. Kannan[56]' in International Conference on Innovation, Management and Technology Research (ICIMTR2012), Malacca, Malaysia, "Digital Watermarking in Video Broadcasting Using a Random Walk Method: Towards Proprietorship" in this paper, an attempt has been made to address the issue of proprietorship using the concept of random walk. While transmitting videos, it is natural that the videos are prone to various types of attacks. It may also be possible to extract watermarks at the competitors end. In this paper, a methodology is proposed in which the watermark is embedded in the video and moved according to random walk. With a random walk of digital watermark embedded into the broadcasted video it is almost impossible to capture/repeat the locus of the random walk of digital watermark. Since the locus of random walk of watermark is not known until the broadcast is being made and even during the broadcast the walk (i.e., moving of the watermark image) is completely random. The locus can-not be guessed at the owners end, even. Translated into practical terms, there can-not be any security breach between the host organization and competitors. This paper may not solve all the security issues, but nevertheless it is a feasible and useful step towards complete security, especially ownership. Standard wavelet transforms have been used in this research paper. In the proposed watermarking system the original video is first converted into frames and these frames are converted into YCbCr color component, the Discrete Wavelet Transform is applied to the Y component of the frame. The random walk procedure is applied to this transformed Y component to select the suitable coefficients for embedding. The α value is considered here as embedding strength to multiply it with the secret logo image and finally inverse Discrete Wavelet Transform is applied and all these frames are grouped to form the watermarked video. The methodology has been analyzed for robustness against various attacks to prove the authenticity. The embedding scheme uses the Daubechies wavelets by modifying the third level approximate sub-band of the DWT coefficients and the extraction scheme detects the hidden watermark in an effective way. Our watermark is also survived with the acceptable standard values such as Peak Signal to Noise Ratio (PSNR), Structured Similarity Index Measure (SSIM), Normalized Cross Correlation (NCC) and others as maintaining the visual quality. Our experience is that the proposed method providing reasonable robustness against various attacks such as frame dropping, color format change, stirmark and others and also preserving perceptual considerations of Human Visual System. As future research direction, it will be useful to consider different compression types such as H.261, H.263 and H.264 and to check the robustness against more number of video processing and other attacks.

In 2012: International Conference on Computer Science and Electronics Engineering 'Min Liu' has done some research on the "Study of Digital Video watermarking" The evaluation of watermarking system includes subjective evaluation standard and objective evaluation standard. Subjective test, because different people different experience, the test results of watermark image difference will be very big, test and evaluation result is not very effective, so in the actual test, often using the quantitative analysis method. An objective test, common standards include:

The watermark information: when using the same kind of watermarking algorithm, the embedded water the more printing, the watermarking robustness is better.

The watermark embedding strength: the embedded watermark strength, the better robustness of watermarking is better, but will not increase the watermark visibility.

The host information and characteristic signal: the greater the host signal information, the more obvious characteristics, watermarking system robustness is stronger.

In order to prevent the attack by exhaustively decipher method, this needs are large enough to the key space (key information value of the maximum range) and so should be introduced to the principle of cryptography watermarking system. To sum up, a fair objective watermark performance evaluation system, even if the input data different test set, get test results should be also similar. In order to calculate the statistics the effectiveness of the result, in the testing process should be adopted the key information and not the watermark.

In 2012: International Conference on Communication Systems and Network Technologies, 'Ashish M. Kothari and Ved Vyas Dwivedi' proposed "Transform Domain Video Watermarking: Design, Implementation and performance analysis" in this paper, author emphasized on the transform domain method for the digital watermarking of video for embedding invisible watermarks behind the video. It is used for the copyright protection as well as proof of ownership. In this paper we have specifically used the characteristics of 2-D Discrete wavelet Transform and discrete cosine transform for the watermarking. In this work they first extracted the frames from the video and then used Frequency domain characteristics of the frames for watermarking. They calculated different parameters for the sake of comparison between the two methods.

Embedding Algorithm is as follow:

1. The Video is converted into the number of frames.

2. The frame is divided into blocks and two dimensional DCT is applied to the first block.

3. If the message bit is a '1' then it is checked whether (5, 2) is less then (4, 3) or not and if it is not the two blocks are swapped so as to make (5, 2) < (4, 3).

4. If the message bit is a '0' then it is checked whether (5, 2) is greater then (4, 3) or not and if it is not the two blocks are swapped so as to make (5,2) > (4, 3).

5. If the coefficients are modified such that (5,2) – (4,3) > k. Here k is a constant and it is used to improve the robustness of the watermark.

6. Move to next block and repeat the procedure.

7. Perform Inverse DCT to have the final watermarked Frame.

8. Next frame is taken and step 3 to step 6 are repeated until the last frame comes.

9. All the watermarked frames are combined to make the watermarked video.

Extraction process is as: The stepwise execution of the extraction process for the watermark recovery from the video is shown below.

1. The Video is converted into the number of frames.

2. The frame is divided into blocks and two dimensional DCT is applied to the first block.

3. If (5,2) > (4,3) then the message bit is 1.

4. If (5,2) < (4,3) then the message bit is 0.

5. Move to next block and repeat the procedure.

6. Next frame is taken and step 2 to step 5 are repeated until the last frame comes.

In 2012: 'Tamanna Tabassum, S.M. Mohidul Islam' proposed "A Digital Video Watermarking Technique Based on Identical Frame Extraction in 3-Level DWT" In the proposed method, first the host video is divided into video shots. Then from each video shot one video frame called identical frame is selected for watermark embedding. Each identical frame is decomposed into 3-level DWT, then select the higher sub-band coefficients to embed the watermark and the watermark are adaptively embedded to these coefficients and thus guarantee the perceptual invisibility of the watermark. For watermark detection, the correlation between the watermark signal and the watermarked video is compared with a threshold value obtained from embedded watermark signal. The experimental results demonstrate that the watermarking method has strong robustness against some common attacks such as cropping, Gaussian noise adding, Salt & pepper noise adding, frame dropping and frame adding.

Proposed digital video watermarking technique based on 3-level DWT. At first the formation of 3-Level DWT are presented. Then the proposed watermark embedding process, including identical frame extraction technique. Discrete wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image. DWT is the multi-resolution description of an image. The decoding can be processed sequentially from a low resolution to the higher resolution. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL sub-band of the previous level is used as the input. To perform second level decomposition, the DWT is applied to LL1 band which decomposes the LL1 band into the four sub-bands LL2, LH2, HL2, and HH2. To perform third level decomposition, the DWT is applied to LL2 band which decompose this band into the four sub-bands: LL3, LH3, HL3, HH3.The proposed system will separate the video into video shots. Each video shot has one or more video frames that are almost identical. In order to determine whether two video frames are identical we compare the two image pixels.

Moreover we also consider on global characteristics of the frames, which is intensity histogram.

According to video standard, the intensity for a RGB frame can be calculated as;

$$I = 0:299R + 0:587G + 0:114B$$

where R, G and B are Red, Green and Blue values of the pixels. Generally, the human visual system is least sensitive to the range of high frequency. Among three channels of the RGB image, the blue channel has characteristic of the highest frequency range. So, for the high performance the blue channel is transformed into DWT and the watermark is embedded from HL3 sub-band of the blue channel of the host video frame. If the HL3 sub-band is fill-up then the remaining watermark signal is embedded in LH3 sub-band. again, if the LH3 sub-band is over then HH3. If HH3 is over then the next upper level is used that is HL2, LH2, HH2 is used. In this way all the watermark is embedded into the video frame (see Figure 11).This process has the benefit of larger watermark can be embedded into the video. As we are placing the watermark into the high frequency part of the blue channel, so the greater invisibility of the watermark in the watermarked video frame is achieved.

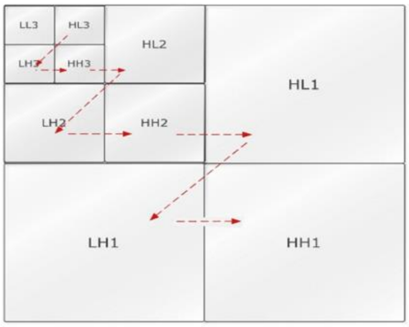


Figure 11: Watermark embedding order in 3-level DWT sub-bands. The dotted arrow line indicating the order

For the detection process without the original video, authorized detection of the hidden information can be easily accomplished by using the watermarked video and watermark signal. The detector detect whether the watermark is present or not in the watermarked video. Similar to the embedding process, before detecting the watermark the system need to extract the video shots and then select the appropriate frame from each video shot. Then 3-level DWT is performed on the blue channel of selected frame. Finally compute the average threshold value and watermark is extracted. The result of this technique show little bit complexity in watermark embedding process. though the system has some limitation but show better results in various attacks.

In 2013: ‘G prabakaran, R. Bhavani, M. Ramesh’ proposed[53] “A robust QR code video watermarking scheme in SVD and DWT composite domain” In this paper propose a video watermarking with text data by using the Quick Response (QR) Code technique. The QR Code is prepared to be watermarked via a robust video watermarking scheme based on the singular value decomposition (SVD) and Discrete Wavelet Transform (DWT).

In addition to that logo or watermark gives the authorized ownership of video document.SVD is an attractive algebraic transformer watermarking applications. SVD is applied to the cover I-frame. The extracted diagonal value is fused with logo or watermark. DWT is applied on SVD cover image and QR code image. The inverse transform on watermarked image and add the frame into video this watermarked (include logo and QR code image) the video file sends to authorized customers. In the reverse process check the logo and QR code for authorized ownership. These experimental results can achieved, acceptable imperceptibility and certain robustness in video. In this technique a QR code is used which is a quick response (QR) code. it is a two dimensional barcode invented by the Japanese corporation Denso Wave. Information is encoded in both the vertical and horizontal direction, thus holding up to several hundred times more data than a traditional bar code (figure a). QR Codes holds a considerably greater volume of information than a 1D Barcode (figure b). QR Code can encode in many types of characters such as numeric, alphabetic character, Kanji, Kana, Hiragana, symbols, binary, and control codes.

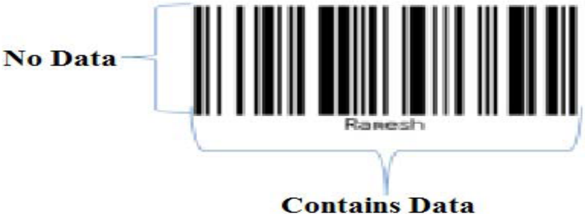


Figure 12 a: 1 D bar code

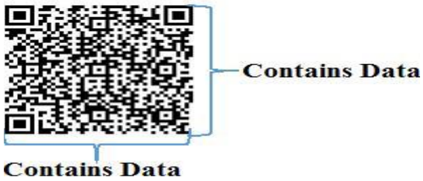


Figure12 b: QR bar code

Watermark an invisible signature embedded in an image to show authenticity or proof of ownership. Discourage unauthorized copying and distribution of images over the internet.
Author proposed embedding technique as shown in the figure 13;

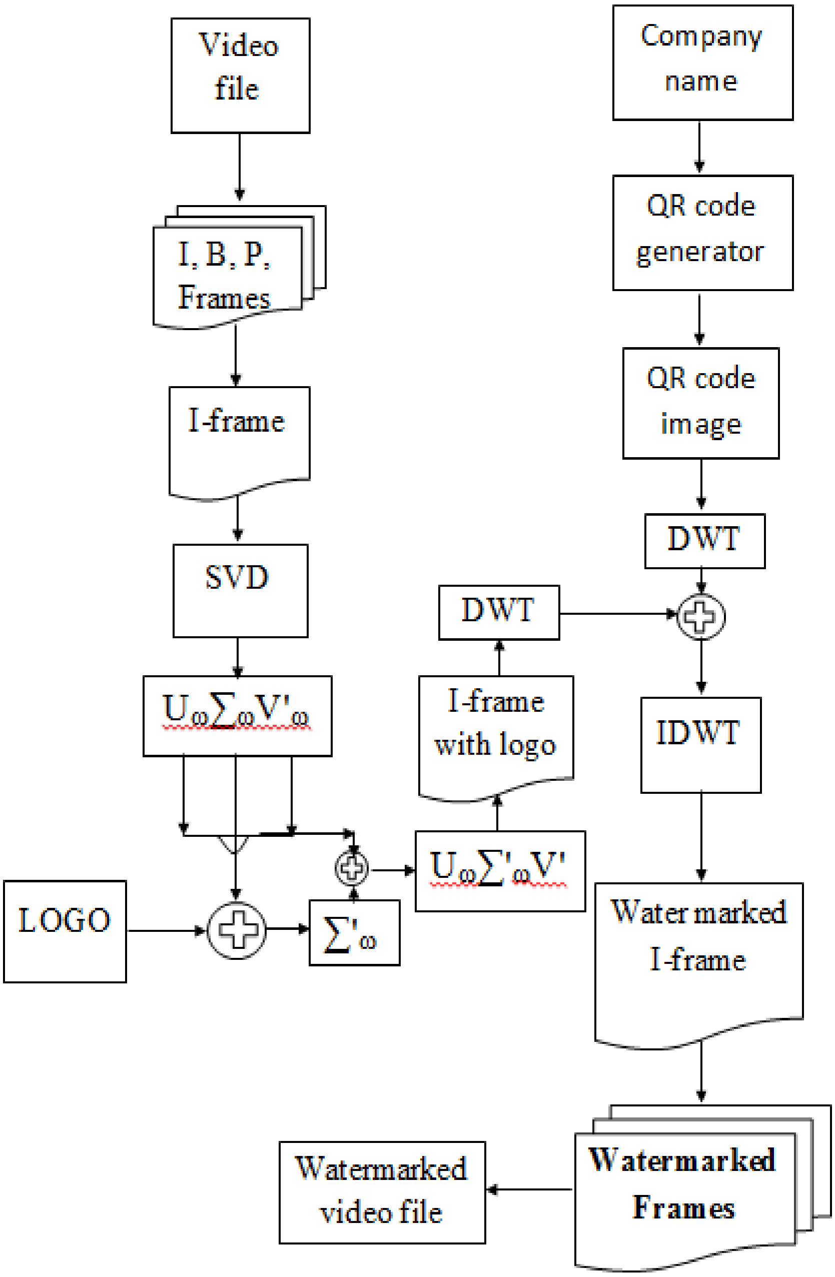


Figure 13: shows the proposed embedding process

Algorithm for embedding process:

Step 1: Read the video file and extract RGB P-frame, B-frame, and I-frame.

Step 2: Read the I-frame image as a cover image.

Step 3: Generate a QR code image with company name.

Step 4: Apply SVD to I frame and get three singular coefficients as u,Σ,v'

Step 5: Add logo with components of an SVD image to get an SVD cover image

Step 6: Apply DWT on both SVD cover image and QR code image to get combined image.

Step 7: Take the inverse DWT on the combined image to get Watermarked I frame.

Step 8: Finally watermarked I frame image to get the watermarked video.

Algorithm for extraction process: In extracting process, SVD is applied to watermarked image and recover the logo. Apply DWT on original video file and watermarked I-frame extract wavelet co-efficient fusion process on the wavelet co-efficient, take the IDWT to obtain the QR code image. Finally extract the verification text. Extraction block diagram is shown in figure 14.

Step 1: Read the watermarked video files and extract Watermarked I frame.

Step 2: Read the original video file and extract original Video I frame.

Step 3: Apply DWT on both videos I frame.

Step 4**:** Subtract watermarked video I frame coefficient with original video I frame coefficient and take Inverse DWT to get a QR code image.

Step 5: By using QR code reader extract company name From QR code image.

Step 6: Apply SVD on watermarked I frame to recover the logo by using the singular value component.

Evaluation of various attacks shows that this method is convenient, feasible and practically used for providing copyright protection. Experimental results show that our method can achieve acceptable certain robustness to video processing.

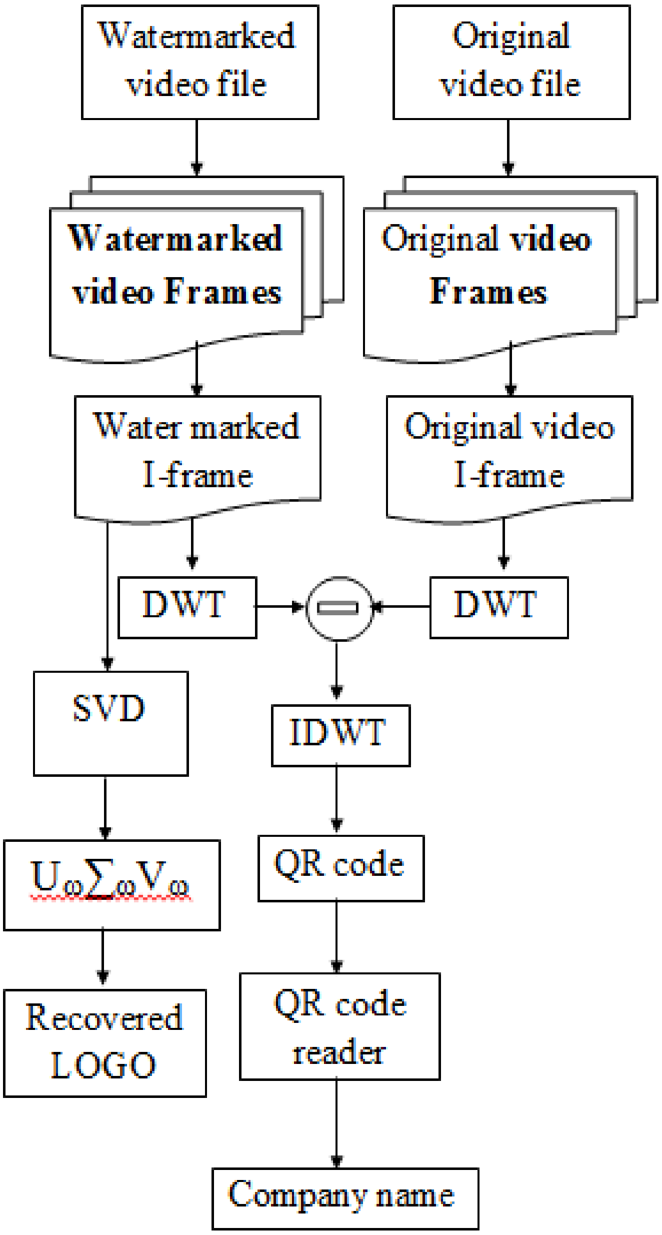


Figure 14: Block diagram for extraction process

CHAPTER 4

THEORY OF DWT and SVD

Here we describe the theory of our proposed work. Proposed work for this thesis is ‘Digital watermarking in video’ is based on the hybrid technique of DWT-SVD. Before proposing the algorithm here we describing the theory of discrete wavelet transform and singular value decomposition.

4.1 Introduction of Fourier transform: The Fourier transform is an useful tool to analyze the frequency components of the signal. However, if we take the Fourier transform over the whole time axis, we cannot tell at what instant a particular frequency rises. Short-time Fourier transform (STFT) uses a sliding window to find spectrogram, which gives the information of both time and frequency. But still another problem exists: The length of window limits the resolution in frequency. Wavelet transform seems to be a solution to the problem above. Wavelet transforms are based on small wavelets with limited duration. The translated-version wavelets locate where we concern. whereas the scaled-version wavelets allow us to analyze the signal in different scale. A wave is an oscillating function of time or space and is periodic. In contrast, wavelets are localized waves. They have their energy concentrated in time or space and are suited to analysis of transient signals. While Fourier Transform and STFT use waves to analyze signals, the Wavelet transforms uses wavelet of finite energy.

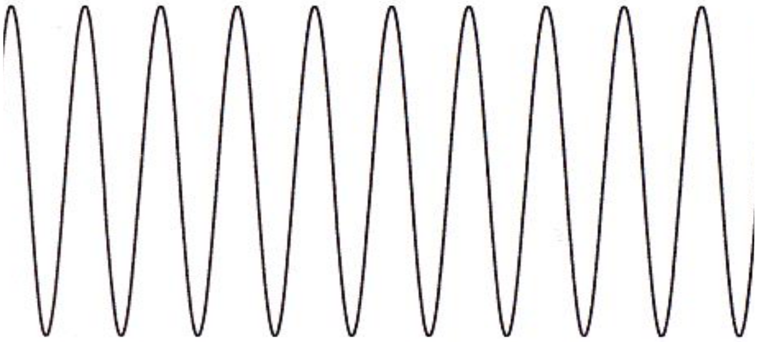


Figure 15 a: A wave

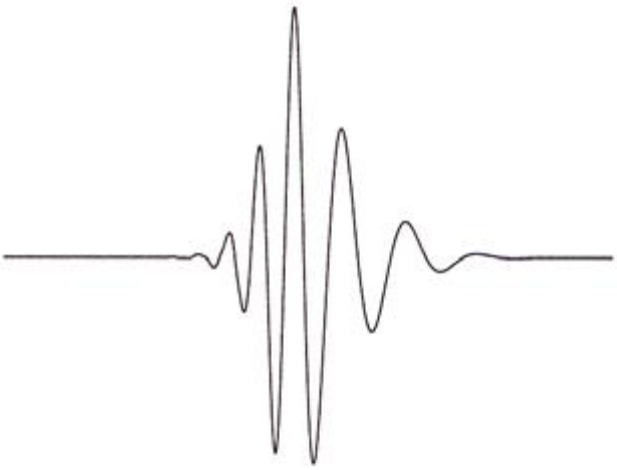


Figure 15 b: A wavelet

The wavelet analysis is done similar to the STFT analysis. The signal to be analized is multiplied with a wavelet function just as it is multiplied with a window function in STFT, and then the transform is computed for each segment generated. However, unlike STFT, in Wavelet Transform, the width of the wavelet function changes with each spectral component. The Wavelet Transform, at high frequencies, gives good time resolution and poor frequency resolution, while at low frequency the Wavelet Transform gives good frequency resolution and poor time resolution.

4.2 History of wavelet [11]: The first literature that relates to the wavelet transform is Haar wavelet. It was proposed by the mathematician Alfrd Haar in 1909. However, the concept of the wavelet did not exist at that time. Until 1981, the concept was proposed by the geophysicist Jean Morlet. Afterward, Morlet and the physicist Alex Grossman invented the term wavelet in 1984. Before 1985, Haar wavelet was the only orthogonal wavelet people know. A lot of researchers even thought that there was no orthogonal wavelet except Haar wavelet. Fortunately, the mathematician Yves Meyer constructed the second orthogonal wavelet called Meyer wavelet in 1985. As more and more scholars joined in this field, the 1st international conference was held in France in 1987 In 1988, Stephane Mallat and Meyer proposed the concept of multi-resolution. In the same year, Ingrid Daubechies found a systematical method to construct the compact support orthogonal wavelet. In 1989, Mallat proposed the fast wavelet transform. With the appearance of this fast algorithm, the wavelet transform had numerous applications in the signal processing field. Summarize the history. We have the following table:

- 1910, Haar families.
- 1981, Morlet, wavelet concept.
- 1984, Morlet and Grossman, "wavelet".
- 1985, Meyer, "orthogonal wavelet".
- 1987, International conference in France.
- 1988, Mallat and Meyer, multi-resolution.
- 1988, Daubechies, compact support orthogonal wavelet.
- 1989, Mallat, fast wavelet transform.

4.3 Scaling in DWT: The Wavelet Series is just a sampled version of CWT and its computation may consume significant amount of time and resources, depending on the resolution required. The Discrete Wavelet Transform (DWT), which is based on sub-band coading is found to yield a fast computation of Wavelet Transform. It is easy to implement and reduces the computation time and resources required. In CWT, the signals are analyzed using a set of basis functions which relate to each other by simple scaling and translation. In the case of DWT, a time-scale representation of the digital signal is obtained using digital filtering techniques. The signal to be analyzed is passed through filters with different cutoff frequencies at different scales.

4.4 DWT and Filter banks

4.4.1 Multi-resolution analysis and filter bank: Filters are one of the most widely used signal processing functions. Wavelets can be realized by iteration of filters with rescaling. The resolution of the signal, which is a measure of the amount of detail information in the signal, is determined by the filtering operations, and the scale is determined by up-sampling and down-sampling (sub-sampling) operations. The DWT is computed by successive low-pass and high-pass filtering of the discrete time-domain signal as shown in figure 4.4.1 this is called the Mallat algorithm or Mallat-tree decomposition. Its significance is in the manner it connects the continuous-time multi-resolution to discrete-time filters. In the figure, the signal is denoted by the sequence x[n], where n is an integer. The low pass filter is denoted by G_0 while the high pass filter is denoted by H_0.

At each level, the high pass filter produces detailed information d[n], while the low pass filter associated with scaling function produces coarse approximations, a[n]. At each decomposition level, the half band filters produce signals spanning only half the frequency band. This doubles the frequency resolution as the uncertainity in frequency is reduced by half. In accordance with Nyquist's rule if the original signal has a highest frequency of ω, which requires a sampling frequency of 2ω radians, then it now has a highest frequency of ω/2 radians. It can now be sampled at a frequency of ω radians thus discarding half the samples with no loss of information. This decimation by 2 halves the time resolution as the entire signal is now represented by only half the number of samples. Thus, while the half band low pass filtering removes half of the frequencies and thus halves the resolution, the decimation by 2 doubles the scale.

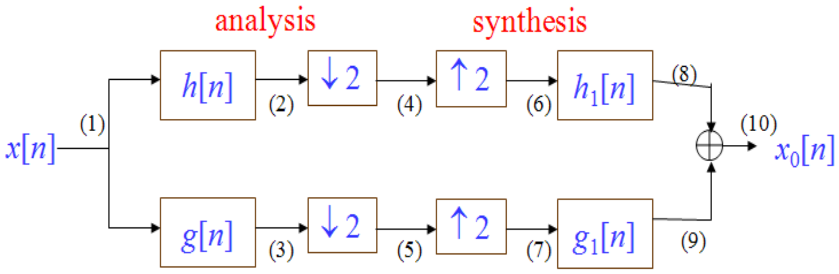


Figure 16: Analysis and synthesis in discrete wavelet transform

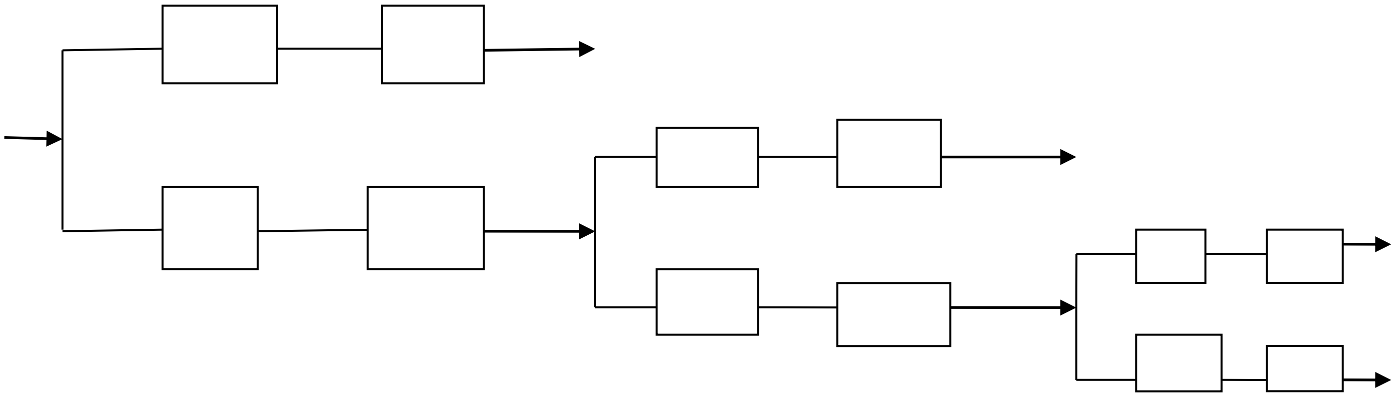


Figure 17: Three level wavelet decomposition tree.

With this approach, the time resolution becomes arbitrarily good at high frequencies, while the frequency resolution becomes arbitrarily good at low frequencies. The time-frequency plane is resolved. The filtering and decimation process is continued until the desired level is reached. The maximum number of levels depends on the length of the signal. The DWT of the original signal is then obtained by concatenating all the coefficients, a[n] and d[n], starting from the last level of decomposition. Figure 17 shows the reconstruction of the original signal from the wavelet coefficients. B. The approximation and detail coefficients at every level are up-sampled by two, passed through the low pass and high pass synthesis filters and then added. This process is continued through the same number of levels as in the decomposition process to obtain the original signal. The Mallat algorithm works equally well if the analysis filters, G_0 and H_0, are exchanged with the synthesis filters, G_1 and H_1.

4.4.2 Condition for perfect reconstruction: In most Wavelet Transform applications, it is required that the original signal be synthesized from the wavelet coefficients. To achieve perfect reconstruction the analysis and synthesis filters have to satisfy certain conditions. Let $G_0(z)$ and $G_1(z)$ be the low pass analysis and synthesis filters, respectively and $H_0(z)$ and $H_1(z)$ the high pass analysis and synthesis filters respectively. Then the filters have to satisfy the following two conditions as

$$G_0(-z)\,G_1(z) + H_0(-z).\,H_1(z) = 0 \quad 2.2$$

$$G_0(z)\,G_1(z) + H_0(z).\,H_1(z) = 2z^{-d}$$

The first condition implies that the reconstruction is aliasing-free and the second condition implies that the amplitude distortion has amplitude of one. It can be observed that the perfect reconstruction condition does not change if we switch the analysis and synthesis filters.

There are a number of filters which satisfy these conditions. But not all of them give accurate Wavelet Transforms, especially when the filter coefficients are quantized. The accuracy of the Wavelet Transform can be determined after reconstruction by calculating the Signal to Noise Ratio (SNR) of the signal. Some applications like pattern recognition do not need reconstruction, and in such applications, the above conditions need not apply.

4.5 Classification of wavelet: We can classify wavelets into two classes:

a) Orthogonal

b) Bi-orthogonal.

Based on the application, either of them can be used.

(a) Features of orthogonal wavelet filter banks

The coefficients of orthogonal filters are real numbers. The filters are of the same length and are not symmetric. The low pass filter, G_0 and the high pass filter, H_0 are related to each other by

$$H_0(z) = z^{-N} G_0(-z^{-1}) \quad 2.4$$

The two filters are alternated flip of each other. The alternating flip automatically gives double-shift orthogonally between the low-pass and high-pass filters. i.e., the scalar product of the filters, for a shift by two is zero.

i.e., $\Sigma G[k]\, H[k-2l] = 0$, where $k,l \in Z$

Filters that satisfy equation 2.4 are known as Conjugate Mirror Filters (CMF). Perfect reconstruction is possible with alternating flip. Also, for perfect reconstruction, the synthesis filters are identical to the analysis filters except for a time reversal. Orthogonal filters offer a high number of vanishing moments. This property is useful in many signal and image processing applications. They have regular structure which leads to easy implementation and scalable architecture.

(b) Features of bi-orthogonal wavelet filter banks

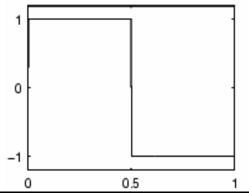
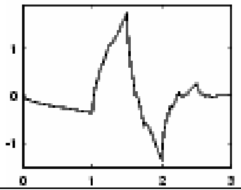
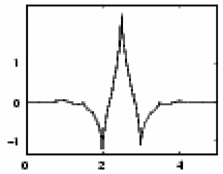
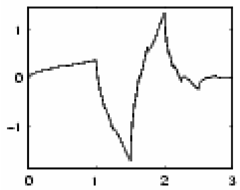
In the case of the bi-orthogonal wavelet filters, the low pass and the high pass filters do not have the same length. The low pass filter is always symmetric, while the high pass filter could be either symmetric or anti-symmetric. The coefficients of the filters are either real numbers or integers. For perfect reconstruction, bi-orthogonal filter bank has all odd length or all even length filters. The two analysis filters can be symmetric with odd length or one symmetric and the other anti-symmetric with even length. Also, the two sets of analysis and synthesis filters must be dual. The linear phase bi-orthogonal filters are the most popular filters for data compression applications.

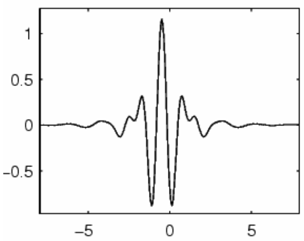
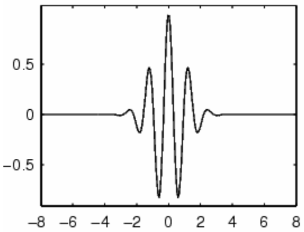
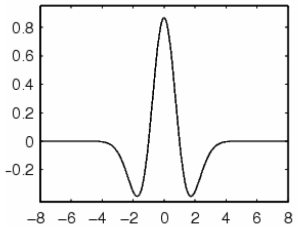
4.6 Wavelet families:

There are a number of basis functions that can be used as the mother wavelet for Wavelet Transformation. Since the mother wavelet produces all wavelet functions used in the transformation through translation and scaling, it determines the characteristics of the resulting Wavelet Transform. Therefore, the details of the particular application should be taken into account and the appropriate mother wavelet should be chosen in order to use the Wavelet Transform effectively.

Haar wavelet is one of the oldest and simplest wavelet. Therefore, any discussion of wavelets starts with the Haar wavelet. Daubechies wavelets are the most popular wavelets. They represent the foundations of wavelet signal processing and are used in numerous applications. These are also called Maxflat wavelets as their frequency responses have maximum flatness at frequencies 0 and π. This is a very desirable property in some applications. The Haar, Daubechies, Symlets and Coiflets are compactly supported orthogonal wavelets. These wavelets along with Meyer wavelets are capable of perfect reconstruction. The Meyer, Morlet and Mexican Hat wavelets are symmetric in shape. The wavelets are chosen based on their shape and their ability to analyse the signal in a particular application.

Table1. Wavelet families and its result

S. No.	Wavelet families	Wavelet result
1	HAAR	
2	DAUBECHIES4	
3	COIFLETS1	
4	SYMLETS2	

5	MEYER	
6	MORLET	
7	MEXICAN	

4.7 Applications of Wavelet

There is a wide range of applications for Wavelet Transforms. They are applied in different fields ranging from signal processing to biometrics, and the list is still growing. One of the prominent applications is in the FBI fingerprint compression standard. Wavelet Transforms are used to compress the fingerprint pictures for storage in their data bank. The previously chosen Discrete Cosine Transform (DCT) did not perform well at high compression ratios. It produced severe blocking effects which made it impossible to follow the ridge lines in the fingerprints after reconstruction. This did not happen with Wavelet Transform due to its property of retaining the details present in the data.

In DWT, the most prominent information in the signal appears in high amplitudes and the less prominent information appears in very low amplitudes. Data compression can be achieved by discarding these low amplitudes. The wavelet transforms enables high compression ratios with good quality of reconstruction. At present, the application of wavelets for image compression is one the hottest areas of research. Recently, the Wavelet Transforms have been chosen for the JPEG 2000 compression standard.

For most compression applications, processing involves quantization and entropy coding to yield a compressed image. During this process, all the wavelet coefficients that are below a chosen threshold are discarded. These discarded coefficients are replaced with zeros during reconstruction at the other end. To reconstruct the signal, the entropy coding is decoded, then quantized and then finally Inverse Wavelet Transformed.

Wavelets also find application in speech compression, which reduces transmission time in mobile applications. They are used in de-noising, edge detection, feature extraction, speech recognition, echo cancellation and others. They are very promising for real time audio and video compression applications. Wavelets also have numerous applications in digital communications. Orthogonal Frequency Division Multiplexing (OFDM) is one of them. Wavelets are used in biomedical imaging. For example, the ECG signals, measured from the heart, are analyzed using wavelets or compressed for storage. The popularity of Wavelet Transform is growing because of its ability to reduce distortion in the reconstructed signal while retaining all the significant features present in the signal.

4.8 Singular value decomposition (SVD) [12]

A singular value and corresponding singular vectors of a rectangular matrix A are, respectively, a scalar σ and a pair of vectors u and v that satisfy

$$Av = \sigma u$$

$$A'u = \sigma v.$$

With the singular values on the diagonal of a diagonal matrix Σ and the corresponding singular vectors forming the columns of two orthogonal matrices U and V,
We have

$$AV = U\Sigma$$

$$A'U = V\Sigma.$$

Since *U* and *V* are orthogonal, this becomes the singular value decomposition

$$A = U\Sigma V'.$$

The full singular value decomposition of an *m*-by-*n* matrix involves an *m*-by-*m* *U*, an *m*-by-*n* *Σ*, and an *n*-by-*n* *V*. In other words, *U* and *V* are both square and *Σ* is the same size as *A*. If *A* has many more rows than columns, the resulting *U* can be quite large, but most of its columns are multiplied by zeros in *Σ*. In this situation, the *economy* sized decomposition saves both time and storage by producing an *m*-by-*n* *U*, an *n*-by-*n* *Σ* and the same *V*. The eigen value decomposition is the appropriate tool for analyzing a matrix when it represents a mapping from a vector space into itself, as it does for an ordinary differential equation. On the other hand, the singular value decomposition is the appropriate tool for analyzing a mapping from one vector space into another vector space, possibly with a different dimension. Most systems of simultaneous linear equations fall into this second category. If *A* is square, symmetric, and positive definite, then its eigen value and singular value decompositions are the same. But as 'A' departs from symmetry and positive definiteness, the difference between the two decompositions increases. In particular, the singular value decomposition of a real matrix is always real, but the eigen value decomposition of a real, non-symmetric matrix might be complex.

Singular Value Decomposition (SVD) is an orthogonal process, which leads to matrix decomposition of matrix *A* to its left and right singular matrices *U* and *V* and to the diagonal matrix S. following equation describes relation among these matrices

$$A=U.S.V'$$

Where *U* is a orthogonal matrix of m x n, $U\ U'=Im$

And *S* is n x n diagonal matrix, and *V* is a n x n ortho-normal matrix $VV'=In$

The diagonal Element of *S* are called the singular value. *I* will refer to the singular value wi as the singular value of the ith columns of *U* and *V*. The singular value decomposition exists always and is unique up to 1) Same permutations in columns of *U*, *W* and *V*) Linear combinations of columns of *U* and *V* with equal singular values.

Multiplication of *U, S* and *V'* (*V'* is transposition of matrix *V*) gives us:

$$A_{mxn} = U_{mxn}\, S_{mxm} V'_{nxn} = \sum_{i=1}^{\min(m,n)} \sigma_i \,.\, u_i \,.\, v'_i$$

Where σ_i={R+ }, i=1... min (m, n) are singular values (diagonal elements of matrix *S*), which are arranged in descending order. u_i are left singular vectors (columns of matrix *U*), and *vi* are right singular vectors (rows of matrix *V*). U and V are unitary matrices, which means

$$U\,U' = I_{mxn}\;;\quad V\,V' = I_{mxn}$$

Increasing the singular values (*SV*) of matrix *S* increases the luminance of the image and vice versa. This means that matrix *S* is linked with luminance of the image, and matrices *U* and *V* are linked with horizontal and vertical image edges. An interesting property of SVD is its invariance against geometric transformations, for example rotation and image scaling.

CHAPTER 5

PROPOSED WORK on “DUAL BAND WATERMARKING USING DWT-SVD

The fast growth of internet and application using digital multimedia technologies has put the accent on the need to provide copyright protection to multimedia data. A digital watermark can be described as a visible or preferably invisible identification code that is permanently embedded in the data. So it can remain present within the cover media after any decoding process. Digital watermarking techniques have been developed to protect the copyright of multimedia objects such as text, image, audio, video, etc. In this dissertation we are proposing a DWT-SVD based digital watermarking technique in video for the copyright protection.

5.1 DWT based watermarking

Niu *et al*. [47] uses the 3D DWT and the gray level digital watermark image. This method performs the 3D DWT as the unit of 64 frames and embeds the watermark made by the multi-resolution hierarchical structure and the hamming code. This method use the error correction coding to correct error bits, the side information is large. Therefore, to embed bit planes of the gray watermark and error correction bits, this method have need of the complex structure. The bit error of the most significant pixel also affects the extracted gray watermark image. They proposed the effective video watermarking algorithm using the 3D DWT and two spread spectrum sequences. Two visible binary watermark images are preprocessed using the mixing and the permutation. After the video sequence divides into video shots, they perform the 3D DWT about video shots respectively. After selecting sub-bands of embedding the watermark considering the robustness and the invisibility, He embed the watermark with two spread spectrum sequences define as the temporal user key. In the process of the watermark extraction, the watermark is finally extracted by comparing the similarity between two spread spectrum sequences and the extracted watermark set. Although He use the visible binary water- mark images, the use of two spread spectrum sequences has the effect to embed the different watermark into each video frames, is robust against the noise, and increase the precision of the watermark extracting. The proposed algorithm produces the watermarked frames that are not different to the original frames subjectively and is robust enough against the attacks of the low pass filtering, the frame dropping and the MPEG coding, etc.

In watermark preprocessing step, He Embed two binary watermark images into the middle frequency range in the wavelet transform domain. Before embedding step He mixed two watermark images into two 2-D pseudorandom permutation about the watermarked images. In his technique He employed the 3D DWT. The 3D DWT is computed by applying the separate 1D transforms along the temporal axis of video frames transformed by the 2D DWT video watermarking scheme of directly extension of image watermarking by taking each frame as an individual still image. Since this method has two disadvantages. First, the pirate easily extracts the watermark by statistical comparing or averaging of the successive video frames. Second, if different watermarks are embedded into each frame, the watermark amount is large. To overcome the pirate attacks on the watermark and the disadvantage as remarked above, we use the 3D DWT that decomposes frames along not only the spatial axis but also the temporal axis. In video watermarking, first, to divide the video sequence into video shots, He use spatial different metric (SDM) to use the dissimilarity between the adjoining frame pair, this method is that the efficiency is low but the algorithm is simple. And then, the spatial 2D DWT is performed and the temporal 1D DWT is performed about selected video shots respectively. In the 3D DWT coefficients, He embed two preprocessed watermark images into the HL sub-band and the LH sub-band of three level about the spatial axis and low pass frames about the temporal axis. He except for the LL sub-band of three level to satisfy the invisibility and high pass frames consisted of the dynamic components to satisfy the robustness. In this method to check the robustness, He used the various attacks like the spatial low pass filtering (LPF), the frame averaging, the frame dropping, and the MPEG coding. To test the frame dropping and the interpolation dropped the odd index frames. The missing frames were replaced with the average of the two neighborhood frames. The NC of two watermarks is 0.819 and 0.793 respectively. To test the MPEG coding, a watermarked video frames coded at 1.5 Mbps is used The NC of two watermarks is 0.844 and 0.846 respectively. The extracted watermark images have a quality as good as claim the copyright and ownership of the digital media.

Discrete wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image [45]. DWT is the multi-resolution description of an image. The decoding can be processed sequentially from a low resolution to the higher resolution. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL sub-band of the previous level is used as the input. To perform second level decomposition, the DWT is applied to LL1 band which decomposes the LL1 band into the four sub-bands LL2, LH2, HL2, and HH2. To perform third level decomposition, the DWT is applied to LL2 band which decompose this band into the four sub-bands: LL3, LH3, HL3, HH3.

Amir zamanidoost et al [23]. gives a blind video watermarking algorithm based on 3D wavelet transform and Human Visual System (HVS) model is proposed. The proposed method is based on extracting temporal characteristics of video signal and using it to adjust spatial features of each frame. These frames are designed based on HVS model embed the message. Then the message will be extracted from video watermarked through blind way. Experimental results verifies the robustness of this method against frame swapping, frame dropping, frame averaging and MJPEG and MPEG2 compression.

Frequency domain watermarking schemes are relatively more robust than the spatial domain watermarking schemes, particularly in loss compression, noise addition, pixel removal, rescaling, rotation and sharing [].color video and color watermark video are taken as an input and converted into frames. By using a key frame extraction algorithm based on X2 histogram matching method, key frames of an original uncompressed video are selected to be watermarked; and this will decrease computation time and complexity of the algorithm. Then, key frames of original video and watermark video are decomposes into three different RGB components and a 4-level discrete wavelet transformation (DWT) is applied on them to obtain thirteen sub-bands in the frequency domain. This allows us to embed watermarks in those regions where Human Visual System is known to be less sensitive to, such as the high resolution detail bands (LH, HL, HH). Embedding watermarks in these regions increase the robustness & imperceptibility at little to no additional impact on image quality. the embedding algorithm embeds the watermark frame and secret key into sub-bands (LH, HL) of key frame. The watermarked component is achieved by applying inverse discrete wavelet transform (IDWT) to the wavelet coefficients. The RGB color components are then concatenated together for each watermarked frame. Saving the whole frame in a new video file is the final step. Peak signal to noise ratio (PSNR) is calculated to evaluate the video quality and imperceptibility. Watermark detection process is an inverse procedure of the watermark embedding process. The extraction process requires the threshold value used for detecting key frames from the watermarked video. Decompose RGB components of key frames and apply 4 – level DWT to each RGB components. Watermark frames are extracted after confirmation of secret key, apply 4 – level IDWT (inverse discrete wavelet transform) and combine all watermark frames to get watermark video. The proposed algorithm extracts the watermark directly from the decoded video without any access to the original video (blind mode).

5.2 SVD Based Watermarking

Recently, some watermarking schemes based on Singular Value Decomposition (SVD) [4] have been developed and applied with success to protect digital images. The SVD of an N x N matrix A is defined by the operation as

$$A=USV'$$

Where *U* and *V* are unitary matrix and *S* is a diagonal matrix. The diagonal entries of *S* are called singular values of A and are assumed to be arranged in decreasing order, the column of the U matrix are called the left singular vectors while the columns of the V matrix are called the right singular vectors of A. each singular value specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image layer. The SVD is a numerical technique used to diagonalize matrices in numerical analysis. The main properties of SVD from the viewpoint of image processing application is: The SV's of an image have very good stability, i.e. when a small perturbation is added to an image its SVs do not change significantly and SVs represent intrinsic algebraic image properties. Interesting property of SVD is its invariance against geometric transformation, for example rotation and image scaling. SVD based watermarking in complex domain has been proposed by 'Hanaa A Abdullah et al [4]' The algorithm was based on a cascade of two powerful mathematical transforms; the 2 level Dual Tree Complex Wavelet Transform (DT-CWT) and Singular Value Decomposition (SVD). This hybrid technique shows high level of security and different levels of robustness against attacks.

In Real time video watermarking based on SVD [53], watermark is embedded using six video sequences with different dynamic properties (Dynamic, Mezzo Dynamic, Lightly dynamic). Resolution of all video sequence is 576x240 pixels. Videos are cut into 10 second long sequences and the frame rate is 25 fps. Video sequences are uncompressed and they are in true colour mode. The embedded watermark is a binary image. The size of the watermark is modified to the spatial resolution of the original video. The video frame is converted into YCbCr model from RGB. Only the luminance component is modified in order to avoid information loss from chroma sub sampling. The watermark is embedded into previously selected frames to decrease computation time. After modifying diagonal matrix coefficients by the embedding process an inverse SVD is applied. This SVD based method is robust against unintended attacks like lossy compression. And also robust against specific intended attacks on the video frame like frame averaging, frame resizing and frame rotation. Robustness of this watermark video can also increased by incrementing the scaling factor.

5.3 DWT-SVD based watermarking

A two-dimensional DWT transforms a frame from the spatial domain to the frequency domain by passing it through a series of low-pass filters and high-pass filters. Outputs of the filters correspond to multi-resolution sub-bands each possessing unique characteristics making it suitable for specific digital processing applications. The sub-band with the lowest frequency components is referred to as the approximation sub-band and it contains most of the energy of the input frame. Due to its excellent Spatio-frequency localization properties, DWT can identify areas within a given frame in which a 'watermark' can be imperceptibly embedded. In particular, this property allows to exploit the Human Visual System (HVS) masking effect: if a DWT coefficient is modified, only the region corresponding to that coefficient will be modified [6].

The DWT and SVD are different transform domain techniques and thus provide different levels of robustness against the same attack. More robustness is expected by combining benefits of the two transforms. Lama Rajab et al [6], gives a technique ‘Hybrid DWT-SVD video watermarking’ In his technique he proposed a watermark embedding procedure in which video clip is converted into frames ‘F’, convert each frame ‘F’ from RGB to YUV color space. Then compute the 2-level dwt for the Y (luminance) matrix of each frame ‘F’ this operation generate seven dwt sub-bands. {LL1, LL2, HL2, LH2, LH1, HH1}, as shown in figure 7 b. Each sub-band is a matrix of dwt coefficients at a specific resolution.

In next step He applied the SVD operator on the HL2 sub-band. The operator decomposes the sub-band’s coefficient matrix into three independent matrices as U_{HL2}, S_{HL2}, V_{HL2} , In next step he rescale the watermark image so that its size of the S_{HL2} matrix which will be used for embedding. In next step he embed the watermark W into S_{HL2} by substituting the watermark bit W_i with the LSB (least significant bit) bit of S_{HL2}(i,i).

In the next step apply the inverse SVD operator on the modified SHL2’ matrix to get the modified coefficient matrix HL2’, the inverse operation SVD operation produces the modified coefficient matrix HL2’ then applied inverse DWT on the modified coefficients matrix HL2’. This finally produces the final watermarked video frame F’ then convert the video frame from YUV to RGB. And cascade the watermarked to get the final watermarked video clip. And for the watermark extraction process convert the video frames F’ from RGB to YUV color matrix, compute its 2-Level DWT for the Y matrix of the frame. Then it decomposes in seven sub-bands as {wLL1, wLL2, wHL2, wLH2, wHH2, wLH1, wHH1}, apply the SVD operator on the wHL2 sub band. The SVD operator decomposes into three sub-band’s matrices as U_{wHL2}, S_{wHL2}, V_{wHL2}. Extract the embedded watermark from the diagonal entries of SwHL2. And in last step construct the watermark W by cascading all watermark bits Wi. then after embedding and extraction process they evaluated performance of algorithm against three video specific attacks frame dropping, frame averaging, and frame swapping.

Charles Way Hun Fung and Walter Godoy Jr[6]. Propose a technique in third international conference on computational intelligence, modeling & simulation based on “A New Approach of DWT-SVD Video Watermarking [3]” in this paper a different method to embed the watermark in videos that insert information in the side view, unlike the regular approaches that insert on the frames. In this method embedded the watermark changing the video references of the frames with dimension equivalent on the number of frames like width and the same height than the original video. After this process the DWT-SVD watermarking is used to insert a grayscale image on the luminance (Y) of YUV converted video. The results show the success to make an imperceptible watermarking and robust against several attacks like noise addition, frame attacks, and MPEG compression.

In this dissertation we are proposing a technique on video watermarking using 2D DWT and 2-level SVD technique. In this we are taking a video which is decomposed into number of frames and embedding a watermark image on each frame. First we converted the video sequence into frames and convert these frames from RGB to GRAY level and then resize these frames as 256x256. 1-Level 2-D DWT is applied on each frame. DWT decomposes each frame into low frequency, mid frequency and in high frequency (LL, LH, HL, HH) band then we applied SVD on HL and LH sub-band called it dual band. SVD converts it into three matrices as *U1S1V1’* of both in HL and LH Sub-band. we are embedding watermark on S matrices after converting it into Gray scale from RGB with some scaling factor. Divide the watermark image half of size with respect to host frames and apply half of watermark image in HL sub-band and other half in LH sub-band After that we again applied SVD on this watermarked frames which further convert this single matrix into three matrices as *U2S2V2’* now multiply S2 matrix with U1 and V1 matrix component of HL and LH band to make it inverse SVD. For getting watermarked video apply IDWT on this inverse SVD result and rearrange the frames in video. This approach gives a more secure watermarked video. Watermarking extraction process is applied on watermarked video to prove the authenticity. To demonstrate the authenticity of this watermarked video we applied some attacks such as Gaussian filtering, median filtering, frame rotation, contrast adjustment and sharpness attack which show its PSNR and NCC value in comparison with the original video.

The proposed video watermarking algorithm consists of two procedure in first procedure we embed the watermark in video. And in second procedure we extracts the watermark symbol from watermarked video, here we are proposing watermark embedding algorithm and watermark extraction algorithm in two section as follow:

5.4 **Watermark Embedding Process:**

Step 1. Take the original video and convert it into frames F.

Step 2. Convert the frames from RGB to Gray as m1

Step 3. Resize the m1 into m2 as 256x256.

Step 4. Take a watermark image (wm) of size 128x128

Step 5. Divide this watermark image into half of the size with the Host frames as 128 x 128

Step 6. Watermark image is divided into two columns as 1 to 64 is wm1 and 65 to 128 is wm2

Step 7. Apply DWT on (m2) each and every frame F of the original video. this operation generate four sub-bands in every frame as {LL, LH, HL, HH}. Each sub-band is a matrix of DWT coefficients.

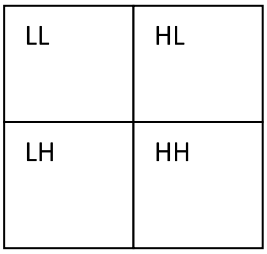


Figure 18: 1-Level 2D DWT

Step 8. Apply SVD operator on LH and on HL sub-bands. The SVD operator decompose each sub-band coefficient matrices into three independent matrices as follow

$$\text{HL}=U_{hl}.S_{hl}.V_{hl} \qquad (1)$$

$$\text{LH}=U_{lh}.S_{lh}.V_{lh} \qquad (2)$$

Step 9. Embed the watermark image (wm2) in S matrix with some scaling factor ‘c’ both in HL and LH band. The given equation is as

$$A_{hl}=S_{hl}+\text{C}*\text{wm1} \qquad (3)$$

$$A_{lh}=S_{lh}+\text{C}*\text{wm2} \qquad (4)$$

where C is a scaling factor.

Step 10. Apply SVD on Ahl and Alh which decompose this matrix into three sub matrices as

$$A_{chl} = U_{chl}\,.S_{chl}.V_{chl} \qquad (5)$$

$$A_{clh} = U_{clh}\,.S_{clh}.V_{clh} \qquad (6)$$

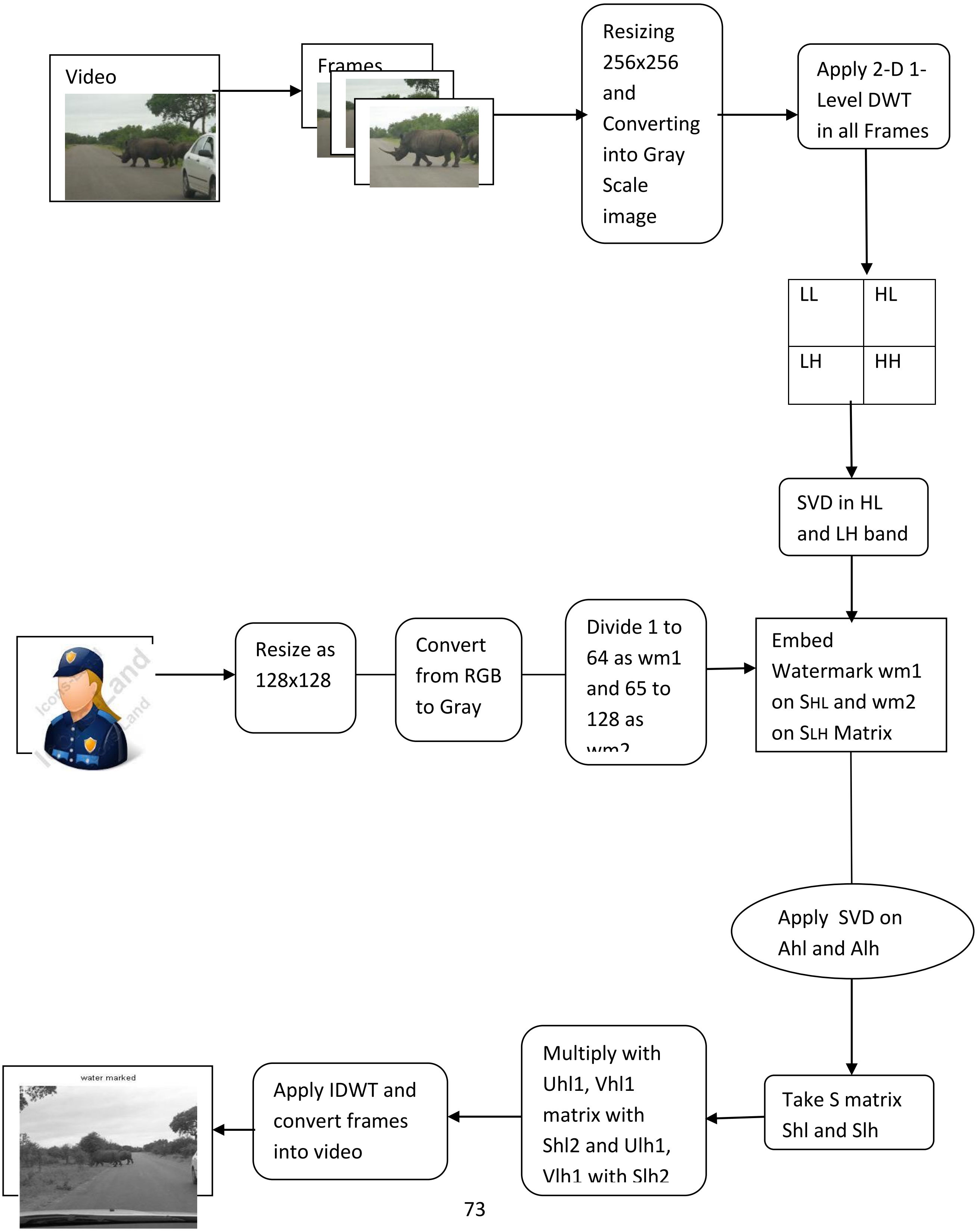
Step 11. Take these S matrices S and S and multiplied them with the U and V matrices which is generated from the first level SVD component.

$$A_{dlh} = U_{lh}\,.S_{clh}.V_{lh} \qquad (7)$$

$$A_{dhl} = U_{hl}\,.S_{chl}.V_{hl} \qquad (8)$$

Step 12. Apply inverse discrete wavelet transform and rearrange these coefficients to create the watermarked Video (Aw).

WATERMARK EMBEDDING PROCESS:


Video
Frames
Resizing 256x256 and Converting into Gray Scale image
Apply 2-D 1-Level DWT in all Frames
LL
HL
LH
HH
SVD in HL and LH band
Resize as 128x128
Convert from RGB to Gray
Divide 1 to 64 as wm1 and 65 to 128 as wm2
Embed Watermark wm1 on SHL and wm2 on SLH Matrix
Apply SVD on Ahl and Alh
Take S matrix Shl and Slh
Multiply with Uhl1, Vhl1 matrix with Shl2 and Ulh1, Vlh1 with Slh2
Apply IDWT and convert frames into video
water marked

5.5 WATERMARK EXTRACTION ALGORITHM:

Step 1. Rearrange the wm1 and wm2 for watermark symbol and resize it as 128x128.

Step 2. Resize the watermarked video as 256x256.

Step 3. Apply DWT on watermarked video (Aw), which decomposed it into four sub-bands as {WLL, WLH, WHL, WHH}

Step 4. Apply SVD in WLH and in WHL sub-bands. Which decompose it into three matrices as USV, equation is

$$D_{HL} = U_{WHL} . S_{WHL} . V_{WHL} \qquad (9)$$

$$D_{LH} = U_{WLH} . S_{WLH} . V_{WLH} \qquad (10)$$

Where D_{HL} and D_{LH} are the retrieved watermark

Step 5. For rebuilding the watermark image we are using following equation

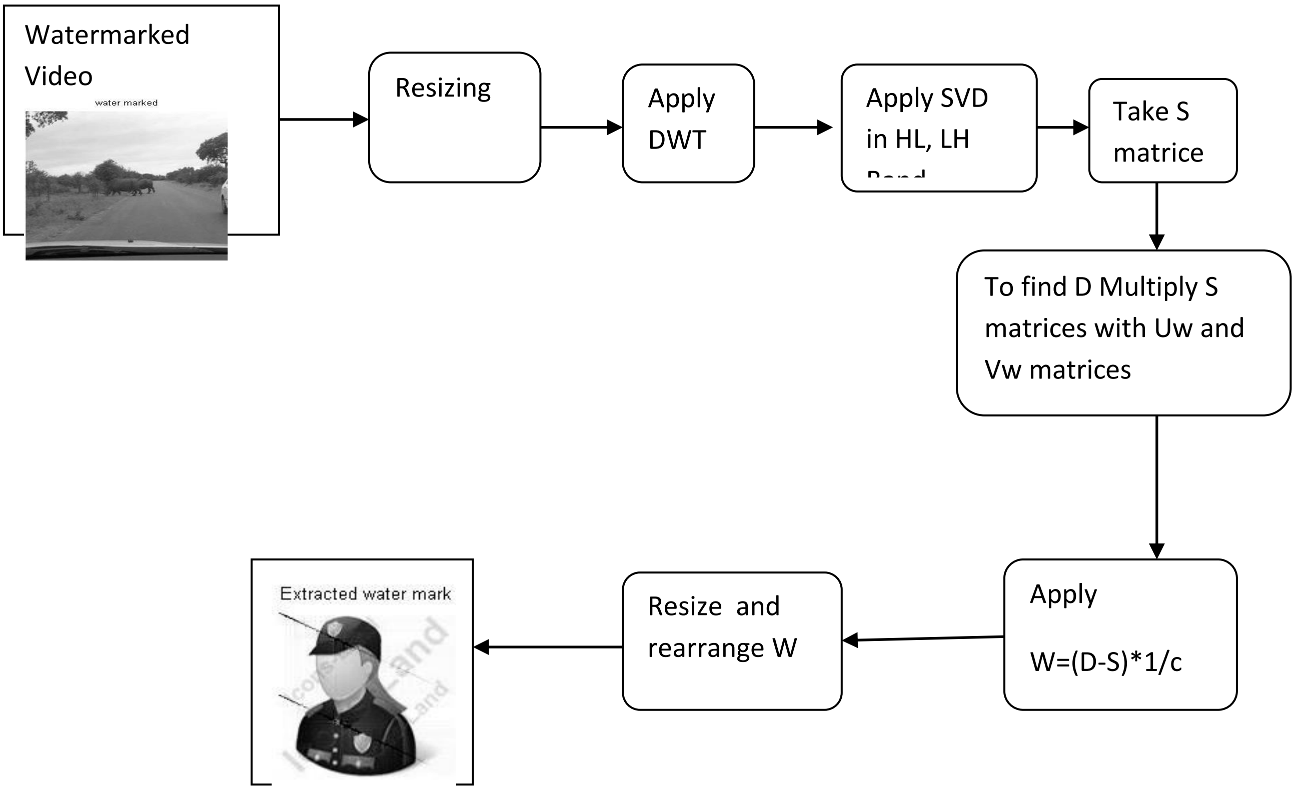
$$W1= (D_{HL} - S_{HL})*1/C \qquad (11)$$

$$W2= (D_{LH} - S_{LH})*1/C \qquad (12)$$

Step 6. Resize w1 and w2 as [64 128]

Step 7. Rearrange w1 w2 as [w1 w2]. Then we get extracted waterimage.

WATERMARKING EXTRACTION PROCESS



5.6 RESULTS AND SIMULATION

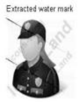
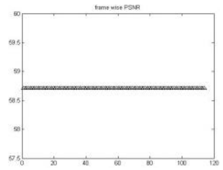
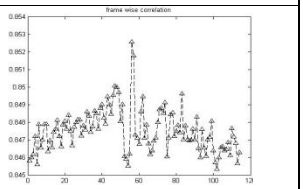
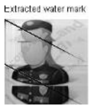
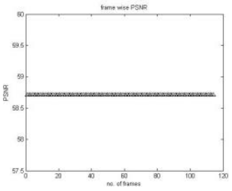
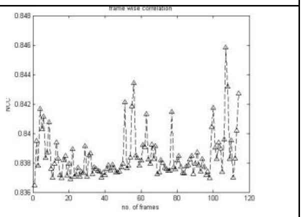
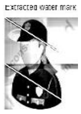
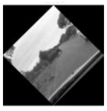
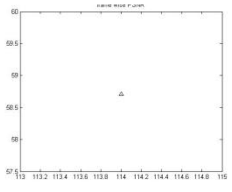
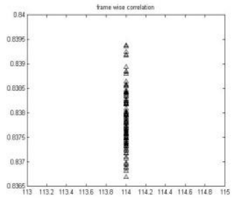
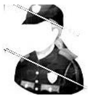
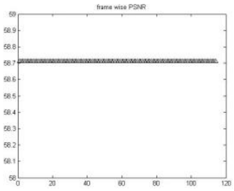
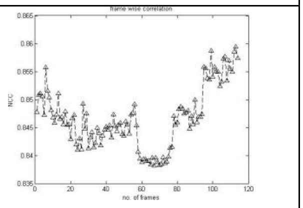
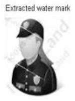
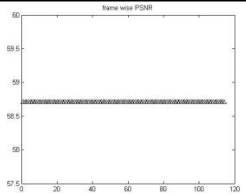
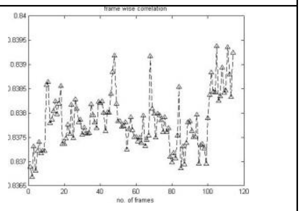
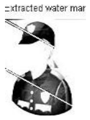
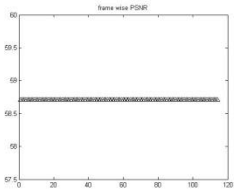
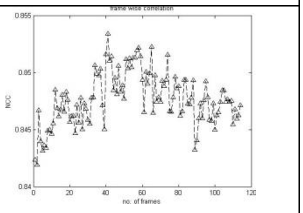
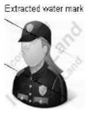
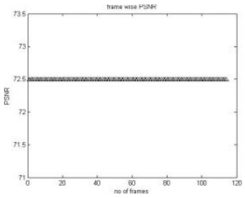
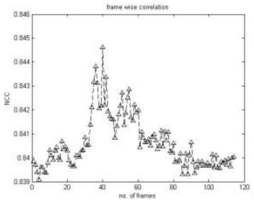
For experimental evaluation we evaluated the performance of the proposed DWT-SVD video watermarking algorithm. We illustrate the proposed method checking some features: imperceptibility and robustness against different types of attacks. Algorithm is evaluated by taking a Rhino video of size 320x240 pixels with 114 frames. For the watermark we have a color image of size 204x204 pixels value. Which resize into 128x128 pixels on each frame.

We applied some physical attacks and signal processing attacks on watermarked video and compared these result with the original watermarked video. As shown in table 3:

Table 3: watermarking results after applying attack

S. NO.	ATTACKS	MAXIMUM PSNR VALUE	MAXIMUM NCC VALUE
1.	WATERMARKED VIDEO WITHOUT ATTACK	75.2323	0.8446
2.	GAUSSIAN ATTACK	59.9781	0.8516
3.	MEDIAN FILTERING	59.9883	0.8458
4.	FRAME ROTATION	59.9781	0.8511
5.	HISTOGRAM EQUALIZATION	59.9781	0.8595
6.	CONTRAST ADJUSTMENT	59.9781	0.8394
7.	SHARPNESS	59.9781	0.8535

Table 3: Extracted watermark and its PSNR, NCC Value after applying attacks

S.No.	Watermarking attacks	Original watermark	Extracted watermark	Watermarked video	PSNR	NCC
1.	Gaussian attack					
2.	Median filtering					
3.	Frame rotation					
4.	Histogram equalization					
5.	Contrast adjustment					
6.	Sharpness					
7.	Without attack					

A. Imperceptibility

Imperceptibility means that the perceived quality of the host image should not be distorted by the presence of watermark. In this experiment we tested the watermarked video and compare it with the original video analyzing frame-by-frame, and checking the PSNR values for each frame that result a mean value: 75.23. At this PSNR value no quality degradation in the watermarked video was perceived.

$$PSNR = 10\log_{10}\frac{\max size(host\ image)^2}{\sum i \sum j\, I(i,j) \times I_w\ (i,j)}$$

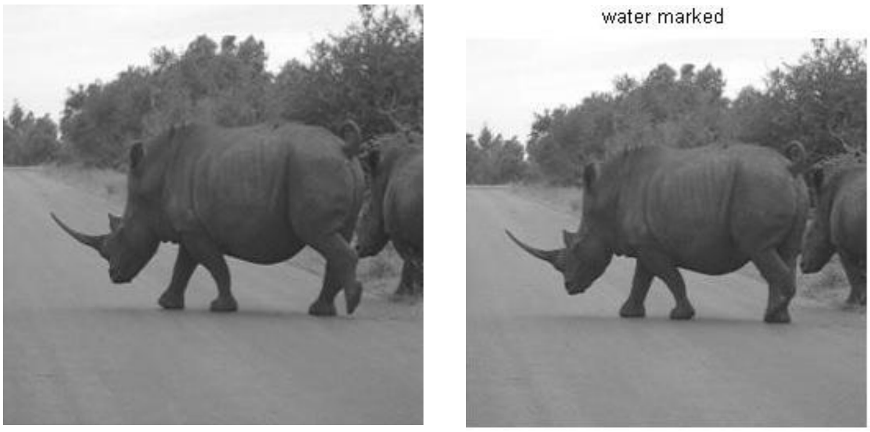


Figure 21: comparison between the original frame and watermarked frame

B. Robustness against attacks

Robustness is a measure of the immunity of the watermark against attempts to remove it or degrade it by different types of digital signal processing attacks. In video watermarking robustness is usually measured against two types of attacks; standard attack and frame attacks. Standards attacks include compression, rotation, Gaussian noise, salt & pepper noise and many others. For both type of attacks we measured the similarity between the original and extracted watermarks using the correlation factors which may vary between 0 to 1. In table 2:

we measure the some standard image oriented attacks along with the PSNR value and normalize cross correlation (NCC) value.

$$NCC(w, w') = \frac{\sum i \sum j \; w(i,j) \times w'(i,j)}{\sqrt{(\sum i \sum j \; w(i,j)^2) \times (\sum i \sum j \, w'(i,j)^2)}}$$

C. Video Angular Rotation

The watermarked video frames for the three scenes were rotated with different angles. As shown in table 3: the correlation values generally indicate robustness of the first algorithm against the video frames rotation. Here we applied 45 degree rotation in the watermarked frame.

D. Gaussian noise

Common additive noise were added with varying intensities to the watermarked video frames for the all the frames. Gaussian noise is tested as shown in table 2: results generally indicate robustness of the algorithm against addition of Gaussian noise.

After applying these attacks we evaluate the performance of the watermarked video frames such as MSE (mean square error), BER (bit error rate), PSNR (peak signal to noise ratio), NCC(normalize cross correlation).

The mean square error is defined as average squared difference between a reference frame and a distorted frame it is calculated by the formula given below

$$MSE = \frac{1}{XY}\left[\sum_{i=1}^{X}\sum_{j=1}^{Y}(w(i,j) - w(i,j)^2\right]$$

X and Y are height and width respectively of the image w (i,j) is the pixel value of host frame w’(i,j) is the pixel value of embed image.

E. SNR (Signal to Noise ratio)

SNR is used to measures the sensitivity of the imaging. It measures the signal strength relative to the background noise. It is calculated by the formula given below:

$$SNR = 10 \; \log_{10}\left(\frac{P_{signal}}{P_{noise}}\right)$$

F. The PSNR (peak signal to noise ratio)

PSNR is used to determine the degradation in the embedded image with respect to the host image. It is calculated by the formula as

$$PSNR = 10 \log10 (L*L/MSE)$$

L is the peak signal value of the cover image which is equal to 255 for 8 bit images.

G. BER (bit error ratio)

BER is the ratio that describes how many bits received in error over the number of the total bits received. It is calculated by comparing bit values of embed and cover image.

$$BER = P/ (H*W)$$

H and W are height and width of the watermarked image. P is the count number initialized to zero and it increments by one if there is any bit difference between cover and embed image.

6. Conclusion

Nowadays piracy and proofing ownership is a very challenging problem in multimedia industry. Digital watermarking is good technique for proofing the ownership and authenticity.

In this dissertation work we give brief review of previous research paper work on watermarking in video. And also gives brief introduction on watermarking in multimedia files.

In our thesis work we are proposing a new video watermarking techniques based on DWT-SVD that uses a 2D 1-Level DWT and 2-Level SVD technique which can be used for authenticity and proof of ownership in multimedia industry.

Experimental results show that this algorithm is more robust with signal processing attacks and physical attacks. The value of PSNR and NCC is measured for all the attack. which shows that this technique gives better result as compare to previous proposed techniques on DWT-SVD. The watermark image can be recover or extract with the higher values of correlation when the watermarked video is attacked with the noise addition, frame rotation, sharpness attack and histogram equalization, contrast adjustment, median filtering.

The possible application of this proposed scheme is proof of ownership, fingerprinting, to preventing video piracy and fraudulent in video.

In our future work we will apply 2-level DWT on host video frames. After that we will apply DCT in LH band, FFT in HH band and SVD in LL band for colour video. And will try watermarked video should also be in true colour form.

Bibliography

[1] Tian Hu, Ji Wei, "A digital video watermarking based on 1D-DWT, 978-1-4244-5316-0/10, 2010 IEEE

[2] Xiang chang, weilin wang, jianyu zhao, li zhang, "A survey of digital video watermarking" 2011 seventh international conference on natural computation. IEEE

[3] Charles way Hun Fung, Walter Godoy jr, "A New approach of dwt-svd video watermarking scheme using the side view" 978-1-4577-1180-0/11 2011 IEEE

[4] Hanaa A Abdallah, Mohiy M. Hadhoud, and Abdalhameed A Shaalan, "svd-based watermarking scheme in complex wavelet domain for color video" 978-1-4244-5844-8/09, 2009 IEEE

[5] K. Su, D. Kundur and D. Hatzinakos, "A novel approach to collusion-resistant video watermarking", Proceedings of the SPIE, vol. 4675, pp. 491-502.

[6] Lama Rajab, Tahani al Khatib and Ali Al-Haj, "Hybrid dwt-svd video watermarking" 978-1-4244-3397-1/08, 2008 IEEE.

[7] Barun Pandhwal, D.S Chaudhry, "An overview of digital watermarking techniques" IJCSE: 2231-2307 vol 3, issue 1 march 2013

[8] R. B. Wolfgang, C. I. Podilchuk and E. J. Delp, "Perceptual watermarks for digital images and video", Proceedings of the IEEE, vol. 87, pp. 1108-1126, (1999).

[9] M. M. Reid, R. J. Millar and N. D. Black, "Second-generation image coding: An overview", ACM Computing Surveys, vol. 29, pp. 3-29

[10] F. Deguillaume, G. Csurka, J. Ruanaidh, and T. Pun, "Robust 3D DFT video watermarking," *Proceedings Electronic Imaging' 99: Security and Watermarking of Multimedia Contents*, Vol. 3657, San Jose, CA, Jan. 1999.

[11] Chun lin liu, " A tutorial of the wavelet transform", Feb 2010

[12] Javier R movellan, "Tutorial on singular value decomposition"

[13] Gopika V mane, G. G. Chiddarwar, "review paper on video watermarking techniques", International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 1 ISSN 2250-3153

[14] J. Dittmann, M. Steinebach, I. Rimac, S. Fisher, R. Steinmetz, Combined audio and video watermarking: embedding content information in multimedia data, in: Proceedings of SPIE 3971, Security and Watermarking of Multimedia Content II, 2000, pp. 176–185.

[15] J. Dittmann, A. Steinmetz, R. Steinmetz, Content-based digital signature for motion pictures authentication and content fragile watermarking, in: Proceedings of the IEEE International Conference on Multimedia Computing and Systems, Vol. 2, 1999, pp. 209–213.

[16] Tamanna Tabassum, S.M Mohidul Islam, "A digital video watermarking technique based on identical frame extraction in 3-level dwt"

[17] G prabakaran, R. Bhavani, M. Ramesh, "A robust QR code video watermarking scheme based on svd and dwt composit domain" PRIME feb 2013, IEEE

[18] Ashish M kothari, ved vyas tyagi, "Transform domain video watermarking: design implementation performance analysis" 2012 international conference on communication system and network technologies,IEEE

[19] Min Liu, "study of digital video watermarking" 2012 international conference on computer science and electronics engineering" IEEE

[20] N R bamane, S.B Patil,"comparison & performance analysis of different digital watermarking techniques" International Journal of Scientific & Engineering Research Volume 4, Issue 1, January-2013 1 ISSN 2229-5518

[21] Verma, B., Jain, S., Agarwal, D.P. and Phadikar, A. (2006) A New color image watermarking scheme, Infocomp, Journal of computer science, vol. 5,N.2, Pp. 37 42.

[22] Lu, W., Lu, H. and Chung, F.L. (2006) Robust digital image watermarking based on subsampling, Applied Mathematics and Computation, vol. 181, Pp. 886-89

[23] Cheng, L.M., Cheng, L.L., Chan, C.K. and Ng,K.W. (2004) Digital watermarking based on frequency random position insertion, Control, Automation, Robotics and Vision Conference, vol. 2, Pp. 977-982.

[24] B. Mobasseri, M. Sieffert, R. Simard, Content authentication and tamper detection in digital video, in: Proceedings of the IEEE International Conference on Image Processing, Vol. 1, 2000, pp. 458–461.

[25] D. Mukherjee, J. Chae, S. Mitra, A source and channel coding approach to data hiding with applications to hiding speech in video, in: Proceedings of the IEEE International Conference on Image Processing, Vol. 1, 1998, pp. 348–352

[26] Manpreet kaur, Sonia Jindal, Sunny behal, ―A Study of Digital image watermarking‖, Volume2, Issue 2, Feb 2012.

[27] Chris Shoemaker, "Hidden Bits: A Survey of Techniques for Digital Watermarking", Independent Study, 2002.

[28] Amir Zamanidoost et. Al. "A Novel 3D Wavelet based method for blind digital

video watermarking" IEEE ISIA 2010, penang Malysia

[29] Masataka Ejima and Akio miyazaki, "a wavelet based watermarking for digital images and video" 0-7803-6297/00, 2000 IEEE

[30] V.Capellini and M barni, "Robust frame based watermarking for digital video" 1529.4188/01,2001 IEEE.

[31] Shao yafei, zhang li, wu guowei, " research of watermarking in digital video broadcasting"ICSP 2002, IEEE

[32] Chun-Shien, L., Shih-Kun, H., Chwen-Jye, S. and Mark, L.H. (2000) Cocktail watermarking for digital image protection," IEEE Transactions on Multimedia,vol. 2, pp. 209-224

[33] Vassaux, B., Nguyen, P., Baudry, S., Bas, P. and Chassery, J. (2002) Scrambling technique for video object watermarking resisting to mpeg-4, Proceedings Video/Image Processing and Multimedia Communications 4th EURASIP-IEEE Region 8 International Symposium on VIPromCom, pp. 239-244

[34] Rakesh Kumar, Savita Chaudhary, "video watermarking using wavelet transform", international journal of computer trends and technology-volume 4, 5 may 2013

[35] Satyendra N. Biswas, et al, "MPEG-2 Digital video watermarking technique", 978-1-4577-1772-7 2012 IEEE

[36] Hartung and Girod, "watermarking of uncompressed and compressed video", signal processing, vol-66, pp 283-301, 1998

[37] G.Langelaar and R Lagendijk, "optimal differential energy watermarking of DCT encoded images and video", IEEE transaction on image processing, vol. 10, pp, 148-158, 2001

[38] Gwenael Doerr, Jean Luc Dugelay, " A guide tour of video watermarking".,signal processing, image communication (18) 2003, pp 263-282

[39] Prabhisek singh, R S Chadha, "A survey of digital watermarking techniques applications and attacks" International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013

[40] Shin aria and kaoru arakawa, "digital watermarking for color video using a non linear filter in dection process" 0-7803-8639-6/04, IEEE

[41] Sha whang et al, "video quality measurement using digital watermarking" 0-7803-8817-8/04, 2004 IEEE

[42] Isao Echizen et al, "improved video verification method using digital watermarking" IIHMSP-06,2006 IEEE

[43] Isaon Echizen et al, “Integrity verification system for video contant by using digital watermarking” 2006 IEEE

[44] Yuk Ying Chung, Fang fei Xu, “A secure digital watermarking scheme for MPEG2 video copyright protection, Proceedings of the IEEE International Conference on Video and Signal Based Surveillance (AVSS'06) 0-7695-2688-8/06 © 2006 IEEE

[45] Sadik A.M. Al taweel, Putra sumari, “Digital video watermarking in the Discrete wavelet transform domain” 2009 sixth international conference on computer graphics, imaging and visualization. IEEE

[46] Tamas Tokar et al, “digital watermarking of uncompressed video in spatial domain”2009 IEEE

[47] Liu Guang qi, Zheng xiao shi, zhao yan ling, Li na, “A robust digital video watermark Algorithm based on DCT domain” ICCASM 2010 IEEE

[48] Xin Lu, Shuaihua Dang, “A new animation image colour texture feature extraction method” 2010 IEEE

[49] Aditya Vashishtha,rajarathnam nallusamy, and sanjoy paul, “NomarK: A novel method for copyright protection of digital videos without embedding data” 2010 IEEE symposium on multimedia

[50] Lufang liao et al, “A new digital video watermark algorithm based on the HVS” 2011 international conference on internet computing and information services IEEE

[51] Dong Zhong, “ the study of digital video watermarking algorithm based on the protection of multimedia courseware”, 2011 IEEE

[52] Xing Chang, weilin weng et al, “ A survey of digital video watermarking” 2011 seventh international conference on natural computation IEEE

[53] Tomas kanocz et al, “Real time digital video watermarking based on SVD”, 2011 IEEE

[54] Jianfi li, aina sui, “A digital video watermarking algorithm based on DCT domain” 2012 fifth international conference on computational sciences and optimization IEEE

[55] Satyendra N biswas et al, “ MPEG-2 Digital video watermarking technique” 2012 IEEE

[57] G prabakaran, R bhavani,M ramesh, “Arobust QR code video watermarking scheme based on SVD and DWT composite domain”, International conference on PRIME feb 2013 IEEE.