CHAPTER 1

INTRODUCTION

1.1. OVERVIEW OF THE RESEARCH TOPIC

The tremendous development in digital media, particularly in the field of compression, has allowed a widespread use of multimedia applications. It has made it possible to distribute multimedia content via the World Wide Web to a large number of people in a cost effective manner.

However, this growth has also generated new challenges for content owners with copyright and security issues. In such cases, the need to protect digital contents to ensure its integrity and authenticity has become an absolute must (Lu *et al.*, 2000a). Traditionally, encryption, steganography, cryptography techniques were used for protecting intellectual data. The past few decades have brought watermarking techniques as a solution for content protection (Lee and Jung, 2001; Barni *et al.*, 2000; Petitcolas, 1999; Eskicioglu and Delp, 2001; Fates and Petitcolas, 2000).

Watermarking is a process of embedding hidden information in a host signal. The main purpose for using watermarking techniques is for digital copyright protection, broadcast monitoring, data authentication and digital fingerprinting. Based on the digital data used for watermarking, the techniques can be categorized as, text-Based watermarking (Kim *et al.*, 2003a), image watermarking (Lu *et al.*, 2000b; Craver *et al.*, 2001; Foo *et al.*, 2001; Kaabneh and Youssef, 2001), video watermarking (Checcacci *et al.*, 2000; Lu and Liao, 2001; Hartung and Girod, 1998), audio watermarking (Sachs *et al.*, 2000; Doufexi *et al.*,2000; Buckley *et al.*, 2000; Bassali *et al.*, 2000) and 3D watermarking (Hartung and Kutter, 1999; Praun *et al.*, 1999).

Among them, image and video watermarking are two important areas that have attracted several researchers (Wang *et al.*, 2009; Mohammed and Hussein, 2009). According to Gwenael and Jean-Luc (2003), video watermarking is very different

from image watermarking, eventhough some techniques can be viewed as an extension to it.

The importance of video in the 21st century has tremendously increased as more number of videos is used during communication, entertainment and training. It is considered as an important tool that can combine all types of multimedia elements like audio, text, static and moving images. Video communication provides the advantage of being effective and has the capacity to convey a great deal of information in a time-constrained environment. Also, as a result of recent evolutions in IT technology, huge amount of high quality digital contents is also generated from High Definition Television (HDTV) broadcasting and DVD (Digital Video Disc). Advances in the network protocols and infrastructure, along with sophisticated services like high speed internet, Internet Protocol Television (IPTV), Digital Media Broadcasting (DMB) and Video On Demand (VOD) have made it possible to store, stream and share large scale of videos in an easy and cost effective manner.

However, these advancements prove to be challenging while taking the intellectual video content protection into consideration (Surekha *et al.*, 2010). This has necessitated the need for techniques that control access to video content by restricting viewing rights, reproduction rights or copying rights. Media protection or Digital Rights Management (DRM) is the set of techniques used for this purpose (Kundur *et al.*, 2004). Media protection is the management of the author's and publishers' Intellectual Property (IP) in the digital world. DRM uses four fundamental technologies, namely, encryption, steganography, cryptography and watermarking, for this purpose. Out of these techniques, digital watermarking has gained more attention while proving the integrity and authenticity of the owner (Piva *et al.*, 2002; Lin *et al.*, 2001) and is the topic of interest in this research.

The research work aims to design robust watermarking algorithms that embed invisible watermarks into compressed and uncompressed video domains. For this purpose, the present research work combines watermarking, visual cryptography and transformation techniques. This chapter aims to present the introductory materials

behind digital content protection with emphasis to the concepts of video watermarking. The research problem along with the set of research objectives is also presented.

1.2. INFORMATION SECURITY

Secret communication or secure communication is defined as a task where two entities share secret data or information and both entities do not desire or want a third party to have knowledge on the secret information. For this purpose, the person initiating the communication (source) and the person receiving the secret data at the end of communication (destination) need a manner of communication that is not susceptible to interception or eavesdropping (Agrawal and Zeng, 2005; Kurose and Ross, 2007). Secure communication allows source and destination to communicate with varying degrees of certainty that the third parties cannot intercept what was shared.

With the advancements in communication software and networks, the geographical locations and time are not considered as major issues during communications. Instead, the focus is now currently on handling the interception issues that compromise on security. Security during communication can be provided to the information or data being communicated (data hiding), to the parties involved in the communication (user hiding) or to the overall communication itself (communication hiding). In this research, data hiding methods are considered.

Figure 1.1 presents the classification of the various types of security systems available to protect digital information. The two main categories are cryptography and Steganography (art of information hiding).

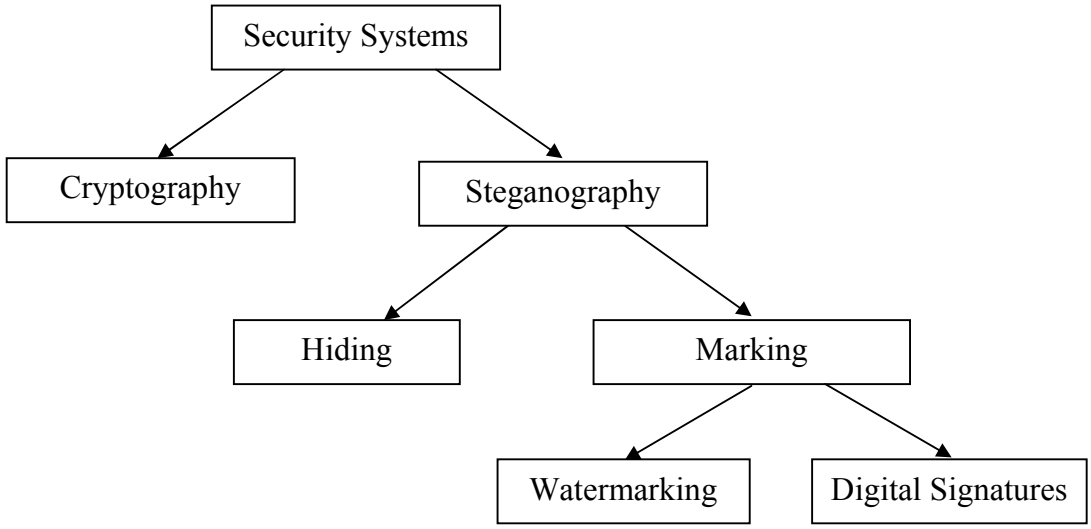


Figure 1.1 : Data or Information Hiding Tools

Cryptography can be defined as the processing of information into an unintelligible form known as encryption and is used mainly for the purpose of secure transmission. Through the use of a "key", the receiver can decode the encrypted message (the process known as decryption) to retrieve the original message. Thus, this tool of information hiding is concerned about protecting the digital contents of the message. Once decryption has been performed successfully, the data is ready to use. Cryptography "scrambles" a message so that it cannot be understood by unauthorized user. Figure 1.2 shows an example process of cryptography.

Steganography is the practice of encoding secret information in a manner such that the very existence of the information is concealed. In the past several decades, many steganographic techniques have been documented, including the use of keywords (cleverly-chosen secret words), modulation of line or word spacing, invisible ink written between lines and microdots (Kamal, 2011). Usually the secret information is concealed by the use of an innocuous cover as to not arouse suspicion if hostile agents discover the cover.

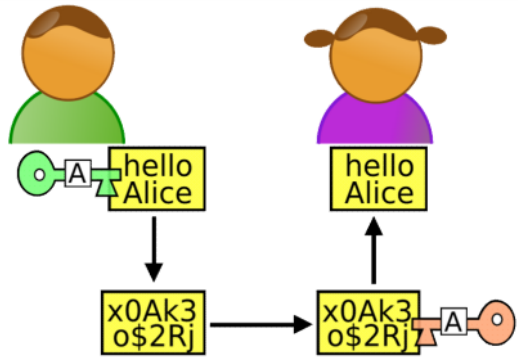


Figure 1.2 : Process of Cryptography

The primary objective of using steganography is to hide a secret message within a file with minimum distortion so that it is not noticeable to an unauthorized user. The hidden message can be later retrieved by the receiver. An example is shown in Figure 1.3.

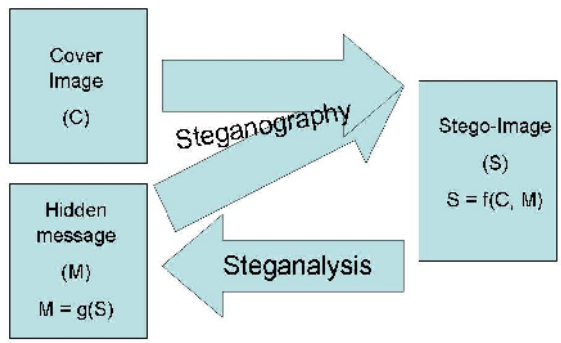


Figure 1.3 : Process of Steganography

The two general directions in which steganography can be distinguished (Cachin, 1998) are listed below.

- Protection against detection
- Protection against removal

Protection against detection is achieved using schemes that do not modify in a visible way the original unmarked object and the modifications are not visible by the humans or by the computers. Protection against removal means that the techniques should be robust to common attacks. It is impossible to remove the hidden data without degrading the object's quality and rendering it useless.

The first approach, protection against detection, involves techniques that can be used to hide information which is not detectable by a third party. The insertion and extraction of data hidden is known only to the sender and the receiver (Anderson and Petitcolas, 1998). Examples include steganography and cryptography. The second approach, protection against removal, is used for data marking and for embedding information about the author or for embedding a serial number, in other words, copyright information. Two techniques used for data marking are

(i) Digital fingerprinting

(ii) Digital watermarking.

Digital fingerprints or labels help to identify intellectual property violators. Here, the owner of the secret message embeds a serial number that uniquely identifies the user of the digital data. This acts as copyright information and makes it possible to trace any unauthorized use of the digital data. In fingerprinting applications, the information hider makes several copies of the host data available to different users. However, a different message is embedded in each copy. The message is a fingerprint or serial number, which can be used to trace any unauthorized use of the signal back to the user.

The fingerprint may contain additional user-specific information. The user should not be able to remove traces of the fingerprint without seriously degrading the signal and the fingerprint itself should be imperceptible. Developing a successful fingerprinting system is difficult, because of possible collusion between multiple users (Moulin and O'Sullivan, 2003). An example of fingerprinting process is shown in Figure 1.4.

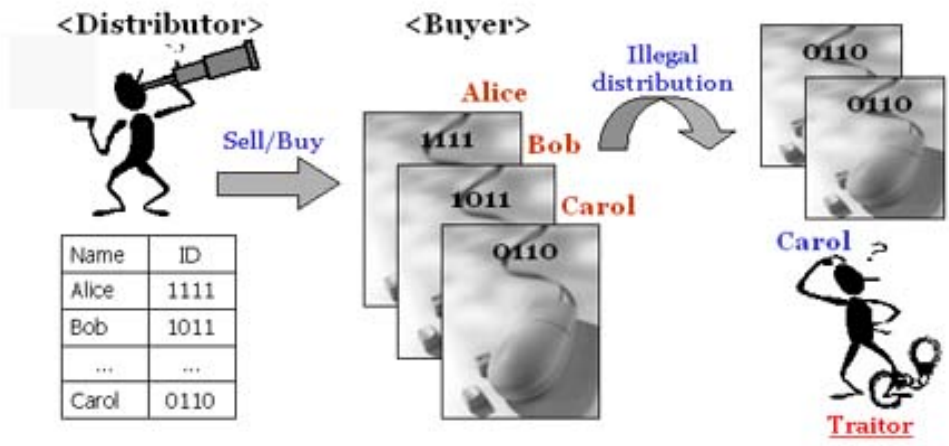


Figure 1.4 : Digital Fingerprinting

Watermarking is a field that has emerged from steganography. In steganography, secret data hidden is assumed to have no relationship with the cover medium and the requirement from such a system is that no suspicion should arise that a medium is carrying any hidden data. On the other hand, in watermarking, the secret data hidden has a relationship with the cover medium data. Data hidden is the ownership data of the cover medium and there is no issue like suspecting that a particular medium is carrying some copyright data. An example of digital watermarking is shown in Figure 1.5.

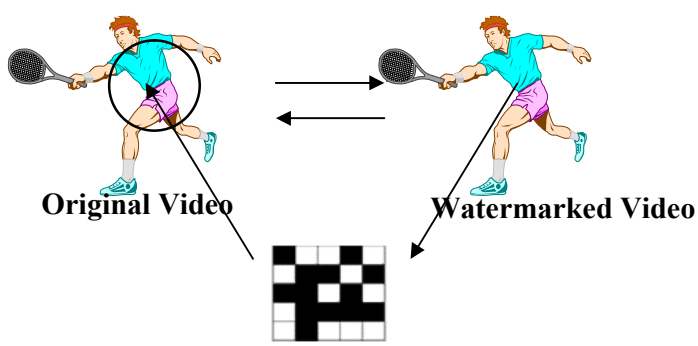


Figure 1.5 : Digital Watermarking

As the purpose of steganography is to have a covert communication between two parties, that is, existence of the communication is unknown to a possible attacker and a successful attack shall detect the existence of this communication.

Watermarking, on the contrary, as opposed to steganography, requires a system to be robust against all possible attacks.

1.3. DIGITAL WATERMARKING

Digital watermarking has been proposed as a technology to ensure copyright protection by embedding an imperceptible, yet detectable signal in digital multimedia content such as images or video (Cox *et al.*, 2007; Barni and Bartolini, 2004; Yu *et al.*, 2001). The embedded signal can be used to identify the legitimate owner holding the copyright of the content. The digital watermarking algorithm is composed of three parts (Zhang, 2009). A general watermark lifecycle phases is shown in Figure 1.6.

(i) Watermark embedding algorithm.

(ii) Watermark extraction algorithm.

(iii) Watermark detection algorithm.

A ‘digital watermark’ refers to the information to be embedded and the signal where the watermark is to be embedded is called the ‘host signal’. During the embedding process, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. This signal is then transmitted or stored. If a person makes a modification, then the digital content is said to be attacked.

A watermark attack is an attack on digital data where the presence of a specially crafted piece of data can be detected by an attacker without knowing the encryption key. Special attention has to be paid to this kind of attacks as they can help to develop better watermarking techniques and defined better benchmarks.

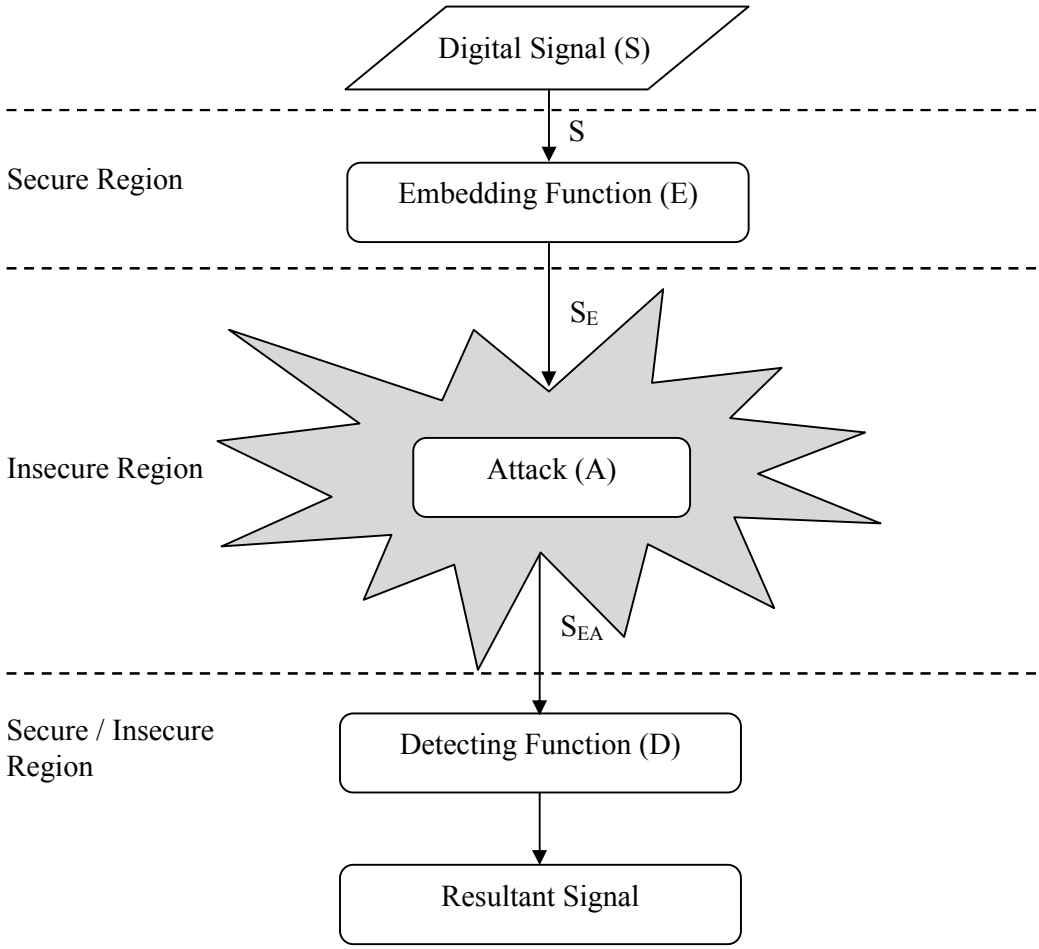


Figure 1.6 : Watermark Lifecycle Phases

Detection (often called extraction) is an algorithm which is applied to the attacked signal for hacking or destroying the watermark from it. The watermark can be extracted, if the watermark is still present in the signal and was unmodified during extraction. When a watermarking algorithm is robust, then the extraction algorithm should be able to correctly produce the watermark, even if the modifications were strong. In fragile watermarking, the extraction algorithm should fail if any change is made to the signal.

Any watermarking technique has to be evaluated to judge its performance. Three factors must be considered while evaluating a video watermarking algorithm.

- Capacity, i.e. the amount of information that can be put into the watermark and recovered without errors.

- Robustness, i.e. the resistance of the watermark to alterations of the original content such as filtering, compression or cropping.
- Visibility, i.e. how easily the watermark can be discerned by the user.

These factors are interdependent and thus, increasing the capacity will decrease the robustness and/or increase the visibility. Thus, it is important to consider all these three factors during evaluation or comparison of watermarking algorithms.

1.4. TAXONOMY OF WATERMARKING TECHNIQUES

This section provides a brief discussion on the categorization of digital watermarking algorithms. The digital watermarking algorithms can be categorized in different manner (Lee and Jung, 2001; Yusof and Khalifa, 2007). The various techniques are summarized in Figure 1.7.

1.4.1. Types of Data Embedded

First, watermark techniques can be divided into four groups according to the type of data to be watermarked (Figure 1.8).

- **Text watermarking -** Text watermarking aims at embedding additional information in the text itself with the goals of (i) concealed communication and hidden information transport of content and authorship authentication and (ii) finally of enriching the text with metadata.
- **Image watermarking –** Image watermarking aims at embedding secret information into a digital image with the goals of robustness for copyright and authentication.

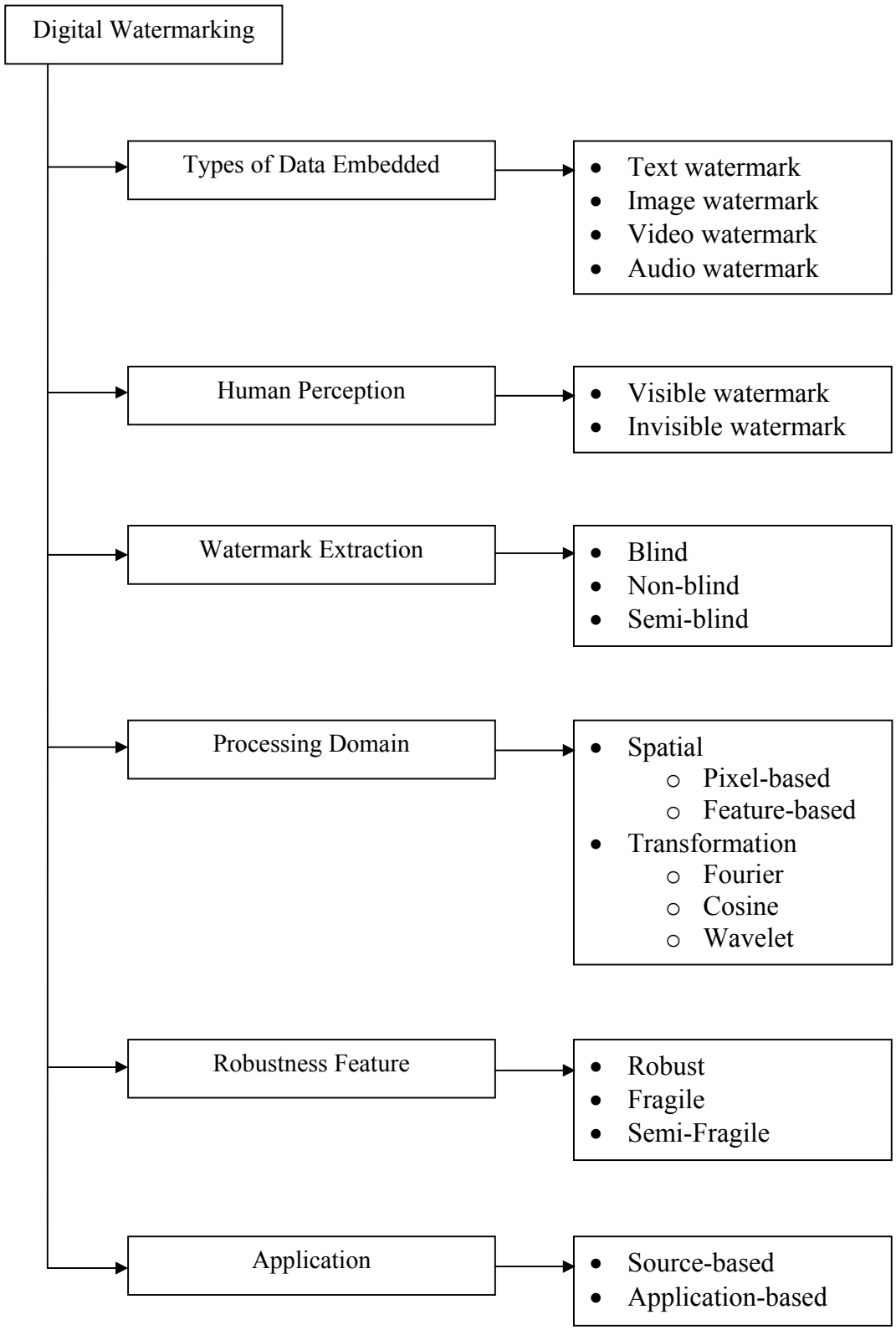
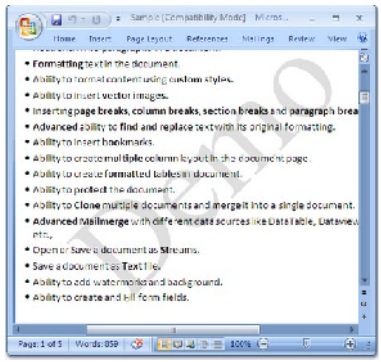


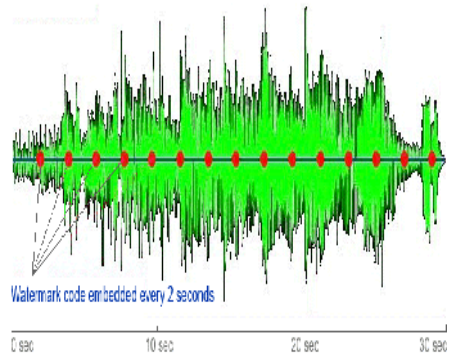
Figure 1.7 : Watermarking Techniques



(a) Text Watermark

(b) Image Watermark

(c) Video Watermark



(d) Audio Watermark

Figure 1.8 : Types of Data Embedded

- **Video watermarking –** Video watermarking involves embedding information of into digital video frames. . Digital video is a stream of frames and are generally a collection of images and sounds. Most of the presented techniques on images and audio can therefore be applied to video files too (Stanislaw and Slawomir, 2007). Ideally, a user viewing the video cannot perceive a difference between the original, watermarked video and unwatermarked video. However, a watermark extraction application can read the watermark and obtain the embedded information.

- **Audio watermarking –** Audio watermarks are special signals embedded into digital audio. Audio watermarking schemes rely on the imperfection of the human

auditory system. However, humans are more sensitive than sensory motors and therefore, good audio watermarking schemes are difficult to design.

1.4.2. Human Perception

Based on human perception, watermark algorithms are divided into two categories, namely, visible watermarking and invisible watermarking. Visible watermark is associated with perception of the human eyes so that if the watermark is embedded in the data in the way that can be seen without extraction. Examples of visible watermarks are logos used in papers and video. On the other hand, an invisible watermarking cannot be viewed by human eyes. So, it is embedded in the data without affecting the content and can be extracted only by the owner or the person who has right for that. For example images distributed over the internet and watermarked invisible for copy protection. An example is given in Figure 1.9. Dual watermark is a combination of a visible and an invisible watermark (Boland *et al.*, 1995).

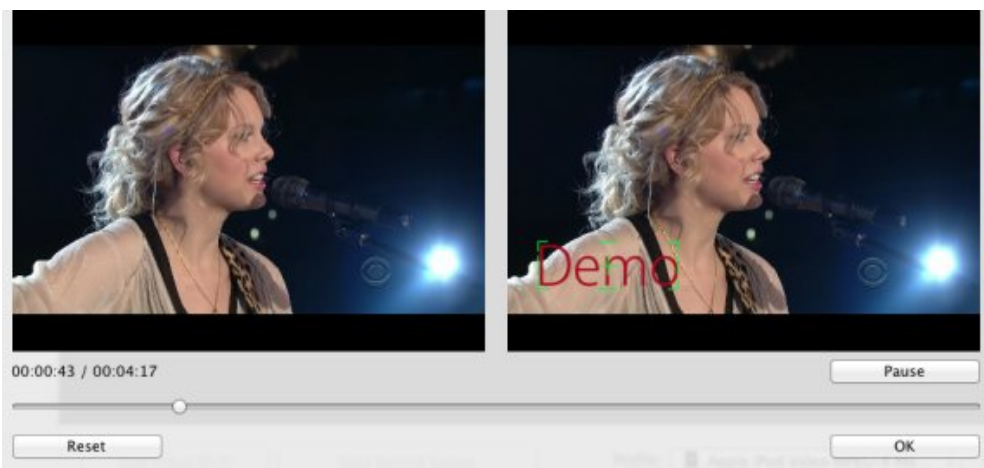


Figure 1.9 : Visible and Invisible Watermarking

1.4.3. Extraction Method

Watermark algorithms, based on the method used for watermark extraction is classified as blind, non-blind and semi-blind techniques.

- **Blind or public watermarking:** In public watermarking, there is no need for original signal during the watermark detection process. Only the secret key is

required. In public watermarking, users of the content are authorized to detect the watermark.

- **Non-blind or private watermarking:** In non-blind or private watermark, original signal is required for detection of the watermark. In private watermarking the users are not authorized to detect the watermark.

- **Semi-blind watermarking**: In semi-blind watermarking, sometimes extra information is needed to correctly detect the watermark. Certain algorithms need to access the original digital content just after adding the watermarking, which is called published watermarked signal.

1.4.4. Processing Domain

Finally, based on processing domain, two groups of watermarking techniques exist. They are spatial domain and transform domain. In the spatial domain based watermarking techniques, the pixel values are modified to embed the watermark data into the cover signal. These methods exploit the statistical properties of the image pixels during embedding and extraction processes. Techniques in spatial domain class generally share the following characteristics:

- The watermark is applied in the pixel domain.
- No transforms are applied to the host signal during watermark embedding.
- Combination with the host signal is based on simple operations, in the pixel domain.
- The watermark can be detected by correlating the expected pattern with the received signal.

The main strengths of pixel domain methods are that they are conceptually simple and have very low computational complexities. Some examples include grey scale watermarking techniques like tagging, Least Significant Bit (LSB), predictive coding techniques and texture block coding (Hartung and Kutter, 1999).

In transform domain methods, transform coefficients are modified for embedding the watermark. Transformation domain is also called as frequency domain as the values of frequency can be altered from their original values by the watermarking algorithm. The main strength offered by transform domain 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. Some examples of transform domain are Discrete Fourier Transformation (DFT), Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT).

1.4.5. Robustness Feature

Additionally, classification can be based on the robustness feature and are categorized as follows.

- **Robust watermark:** One of the properties of the digital watermarking is robustness. A watermark algorithm is robust if it can survive after common signal processing operations such as filtering and lossy compression.

- **Fragile watermark:** A fragile watermark should be able to detect after any change in signal and also possible to identify the signal before modification. This kind of watermark is used for the authenticity or verification of original content.

- **Semi-fragile watermark:** These types of watermarks are sensitive to some degree of change to a watermarked signal.

1.4.6. Application

Furthermore, from the application point of view, watermark techniques can be grouped as source-based or destination-based. In the first group, that is source-based techniques, all copies of a particular data have a unique watermark, which identifies the owner of that data, while in the destination-based, each distributed copy is embedded using a unique watermark data, which identifies a particular destination.

This study aims to design and develop invisible, robust, watermarking techniques for securing the copyright information of video files. The following section discusses digital video watermarking in detail.

1.5. DIGITAL VIDEO WATERMARKING

The term "Video" is a Latin term and means "I see" (Abdul-Ahad *et al.*, 2008). Video is basically a three-dimensional array of colour pixels. Two dimensions serve as spatial (horizontal and vertical) directions of the moving pictures and 1-d (one dimension) represents the time domain. A data frame (video frame image) is the set of all pixels that correspond to a single time moment. A frame can be considered as a still image (Hui and Yeung, 2003; Cox and Miller, 2001; Doerr and Dugelay, 2004).

Digital video watermarking is a technology to embed and retrieve information into and from digital video data. The features desired from any video watermarking scheme is that they should ensure digital ownership, have the ability to track the source of the digital video, have no visible video degradation, have quick and easy way to detect video manipulation and should have easy implementation procedure. The basic characteristics are imperceptibility, security, reliability and low complexity of watermarking algorithm.

Video watermarking marks digital video content so that a particular copy can be traced back to the original user. It is mainly used as a preventive measure for unauthorized copying of copyrighted material. It is defined as a data hiding technique that adds unremovable data to the frames of video that is transparent to the user, in order to protect the video from illegal copying and identify manipulations.

As mentioned in Section 1.3, the general process of video watermarking consists of three main steps (Mane and Chiddarwar, 2013), namely,

(i) Embedding (original video is marked with secret data).

(ii) Broadcast (watermarked video is transmitted using a distribution channel).

(iii) Retrieval (recovery of watermark to decide on access).

In the distribution channel, removal of watermarks can occur in two manners, (i) Unintentional or (ii) Intentional. Both the attacks result in alteration or removal of watermarks and have to be avoided. The intentional removal of watermark to breach the intellectual property is termed as 'Attack'. The main goal of any video watermarking algorithm is to resist these attacks.

1.5.1. Place of Watermarking

While using watermarking to protect video content, the answer to 'when' and 'where' to embed the watermark are two crucial questions that have to be handled carefully. A watermark can be embedded into video signals either before compression process (Uncompressed video data) or after the compression process (Compressed video data) (Pröfrock *et al.*, 2006; Hartung and Girod, 1996).

In compressed domain watermarking, video is partly decoded, modified to accommodate the watermark and re-compressed to form watermarked videos. Here, the watermark embedder has no knowledge of how the video will be decompressed and therefore, cannot make informed decisions based on the compression parameters. Further, it requires the watermark to be inserted with excessive strength, which can adversely impact watermark perceptibility. These algorithms are also computationally expensive and the compression step adds additional compression noise thus degrading video quality.

With uncompressed video medium, the watermark is embedded into the raw frames of the video signal and the watermarking algorithm is not influenced by the compression algorithm and therefore is more robust. Here, both compression and watermarking algorithms seek irrelevant data for embedding and therefore has to be designed carefully. These algorithms results with more quality degradation and therefore the algorithms should try to minimize them.

In video watermarking domain, compressed domain has more acceptance over uncompressed domain processing. This is because most of the video files have high bandwidth requirement and therefore is usually stored and transmitted in compressed

form. However, watermarking for compressed video data in real time is very challenging because of computation requirements. The computation requirement is almost equal to (if not more) a decoder. Watermarking algorithms usually tend to become more and more complex as the bit rate for the output video decreases. For low-bit rate channels there is less headroom for watermark data and spreading cannot be done effectively. Hence, the algorithm chosen should be robust enough to withstand different kinds of attack.

1.5.2. Features of Video Watermarking

An ideal digital watermark should have the following important features. However, the relative importance of these properties is application dependent.

- **Transparency (invisibility):** Transparency or imperceptibility is the characteristic of hiding a watermark in a way that does not degrade the visual quality of an image. A closely related terms is fidelity. Fidelity refers to perceptual similarity between the watermarked data and the original data. The watermark should be imperceptible both statistically and perceptually. It means that no visual effect should be perceived by the end user. Further, the embedding process should not degrade the signal quality. However, in some applications a little degradation is accepted to have higher robustness or lower cost.

- **Robustness**: A watermark algorithm is called robust if it can survive against changes made by signal processing operations. In contrary, a watermark algorithm is termed as fragile if the watermark is destroyed by modifications. If the application uses a digital watermark for ownership identification, then it is desirable to have the watermark to be robust against any modifications. The main requirement here is that the watermark should not be destroyed or should not have any quality degradation in the presence of unintentional or malicious signal and geometric distortions like conversions (analog-to digital or digital-to-analog conversion), re-sampling, rotation, cropping, quantization, scaling, dithering and compression of the content. On the other hand, if the applications use digital watermarking for content authentication, then the watermark under consideration

should be fragile. In other words, the watermarks should get destroyed whenever the content is modified so as to detect any modifications made to the content.

- **Use of keys :** Another property of an ideal watermarking system is that it implement the use of keys to ensure that the approach is not rendered useless the moment that the algorithm becomes known. Asymmetric key system such as public/private key cryptographic systems can also be used for these purposes. Eventhough, both private and public keys can be used, public keys are generally more frequently used, eventhough the private key systems are simple to implement. The reason behind this is due to the chance that the private key can be discovered and thus, ruins the security of the entire system.

- **Capacity**: A watermarking system must allow for a useful amount of information to be embedded into a digital signal. The amount of information that can be embedded in a watermarked signal is called data payload. The data payload in watermarking means the number of bits encoded with the image. The payload of the embedded watermark information must be sufficient to enable the envisioned application.

- **Inseparability:** After the process of embedding the digital cover content with the watermark, separating the content from the watermark to retrieve the original content should not be possible.

- **Blind detection :** Blind detection refers to the ability to detect the watermark without access to the original document. Because of the immense size of uncompressed video files and the difficulty of indexing them to search for a specific frame, it is an especially important requirement in video watermarking.

- **Low error probability :** Even in the absence of attacks or signal distortions, the probability of failing to detect the watermark, i.e. false-negative and of detecting a watermark when, in fact, one does not exist, i.e. false-positive, must be very small. The statistically-based algorithms have no issue in satisfying this requirement, but, such ability must be demonstrated, if watermarking is to be legally credible.

- **Real-time detector complexity :** For consumer-oriented watermarking applications, it is important that the complexity of the detection and extraction algorithms be low enough to execute within the specified real-time deadlines.

- **Security**: The digital watermarking techniques should prevent unauthorized users (hackers) from detecting and modifying the watermark (attacks) embedded in the cover signal. It is the ability of the watermark to resist malicious attacks. Secret keys can be used to ensure that only authorized users are able to detect/modify the watermark.

- **Computation cost :** Computation cost is the measure of computing resources required to perform watermark embedding or detection processes. It can be measured using the processing time for a given computer configuration.

- **Complexity**: Depending on the application, the insertion is done only once and can be performed off-line. Consequently, the complexity of encoding plays less important role than the complexity of the decoding. But in real-time applications, both these procedures should be in a simple form.

In summary, while designing a watermarking algorithm, trade-offs exist among three parameters, payload, fidelity and robustness. Data payload is the number of bits that can be embedded in the digital data, the fidelity is the degradation introduced into the signal and the robustness is the ability of the watermark to remain readable after innocent or malicious signal processing operations on the signal. These parameters are conflicting and they should be chosen to meet the requirements of the application.

When designing watermarking algorithms for video, there are additional conflicting parameters, such as the need for low complexity and constant bit rate. In some video applications, watermark embedding or detection needs to be performed in real time. Thus, video watermarking algorithms should have low complexity. Because of the large size of video files, they are usually stored and distributed in a compressed format. Video watermarking algorithms should not increase the bit rate of the compressed video.

1.5.3. Applications of Video Watermarking

Video watermarking enables two different scenarios as given below.

- **Forensic analysis :** A content provider embeds a mark in a video that identifies the consumer of that video.

- **Screening :** A content provider embeds watermark into a video that describes requirements for playback of that video.

Video watermarking is desired in various scenarios like forensic analysis, screening, Broadcast monitoring of video sequences, DVD protection and access control, Database retrieval, Robust identification of digital content. Irrespective of the application area, the main goal is for copyright protection. This section presents some applications of digital watermarking in the context of video.

- **Copy control :** Copy protection is a widely exercised application in video watermarking. In this a watermark is used to indicate whether a video content is copyrighted. This watermark can only be removed with a severe degradation of the video sequence. The work on copy protection issues in DVD is being carried out by the Copy Protection Technical Working Group (CPTWG).
- **Broadcast monitoring:** A commercial advertisement may be watermarked by putting a unique watermark in each video or sound clip prior to broadcast. Automated monitoring systems can then receive broadcasts and check for these watermarks, identifying when and where each clip appears. This proves very helpful for the advertisers as they actually pay for only the number of times the advertisement was actually relayed.
- **Fingerprinting:** A fingerprinting technique can be used to trace the source of illegal copy. Every copy available can be watermarked with a unique bit sequence. Now, if a copy is made illegally the source can be easily tracked since each original copy had a unique bit sequence embedded into it.
- **Copy protection:** To prevent the data from being copied, a watermark can be introduced in the data with a copy protect bit. When the copying device reads the data, the watermark detecting circuitry should detect the watermark and stop

recording. This would need all the copying machines to have the watermark circuitry to identify the watermark and act accordingly.

- **Video authentication:** In applications involving instance videos captured by surveillance cameras, checking the integrity of the images and the video is a major issue. Fragile, semi fragile and robust watermarking are the commonly used policies. A slight modification on the cover video destroys fragile watermarks. Semi fragile watermarking can resist content conserving operations and be sensitive to content varying transforms.
- **Copyright protection:** Copyright protection of video data is an important issue in digital video delivery networks. There are many techniques of video watermarking for copyright protection. In one of the techniques, a watermark is added to the video signal that carries information about the sender and the receiver of the delivered video.
- **Miscellaneous :** Apart from the above, video watermarking is also widely used in various other applications like, error detection, compression, advertisement, content ID and archive related applications.

The applications presented in this section are summarized in Table 1.1.

TABLE 1.1

APPLICATIONS OF VIDEO WATERMARKING

Application	Purpose of Watermarking
Copy control	Prevent unauthorized copying
Broadcast monitoring	Identify the video being broadcast and check usage
Fingerprinting	Track back a malicious user
Video authentication	Ensure that the original content has not been altered
Copy protection	Prove ownership
Enhanced video coding	Bring additional information (For example, for error correction)
Advertisement	Verify the frequency of display of an advertisement
Content ID and archive	Add meta-data (for example, owner, data) for archive

1.6. ATTACKS IN VIDEO WATERMARKING

There are many challenges in the design a video watermarking algorithm. Simple signal processing enhancement techniques, such as gamma correction, sharpening and filtering and geometric attacks, such as cropping, resampling and rotation, alter the performance of watermarking algorithms. Transcoding, which involve changing the compression ratio to adapt to the storage capacity, converting the video format and chrominance resampling, are likely to remove the watermark. Spatial desynchronization, such as changes in display formats (4/3, 16/9 and 2.11/1) and changes of resolution and temporal desynchronization such as frame rate modification may also affect watermark detection algorithms. Also, video editing, such as the addition of a commercial into the middle of a movie, a transition between scenes and superimposition, such as picture-in-picture technology, subtitles and logos, degrade the performance of watermarking algorithms.

A more serious problem with video or audio signals, which are long, is the possibility of a self-collusion attack. A collusion attack is a very powerful attack for still images. There are two types of collusion attacks. If the same watermark is embedded in different data, the watermark data can be estimated from each occurrence and the average of those estimates will be a refined estimate. If different watermarks are embedded in the same data, several users can collude by averaging their decoded signals to reduce the strength of the watermark and possibly render it unreadable.

However, with video one video sequence is enough to remove the watermark. If the same watermark is embedded in all the frames, the first type of collusion can be used to remove the watermark from different scenes. If a different watermark is embedded in each frame, the second type of collusion can be used to remove the watermark from correlated scenes. Recognizing these possibilities, the watermarks inserted in two video frames should be as similar as the two frames are. According to Hartung and Kutter (1999), Watermark attack can be classified into four main groups:

(i) **Simple attacks** : These types of attacks attempt to damage the embedded watermark by modifications of the whole frame without any effort to identify and isolate the watermark. Examples include frequency-based compression, addition of noise, cropping and correction.

(ii) **Detection-disabling attacks** : These attempt to break correlation and to make detection of the watermark impossible. Geometric distortion like zooming, shift in spatial or (in case of video) temporal direction, rotation, cropping or pixel permutation, removal or insertion are used.

(iii) **Ambiguity attacks** : In these attacks, the detector uses 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.

(iv) **Removal attacks** : The removal attacks estimates the watermark, separate it out and discard only the watermark. Examples are collusion attack, denoising or exploiting conceptual cryptographic weakness of the watermark scheme (e.g. knowledge of positions of single watermark elements).

1.7. CHALLENGES IN VIDEO WATERMARKING

While image watermarking already entered our life, video watermarking has not become common yet. This is due to the fact that the problem is complicated and usually requires stronger computation resources. It is important to note that video watermarking is even more useful than image watermarking. Illegal distribution of movies through internet is one of the biggest problems of the content owners. Another problem is broadcast hijacking, which is usually done on the TV broadcasting of video.

Video has three dimensions and thus there are additional requirements and security issues when compared with image watermarking schemes. The design and development of video watermarking techniques is considered as a challenging job because of the following reasons.

- Advancements in software and transmission technology make it difficult to design a watermarking technique that meet the three characteristics, namely, Tranparency, Capacity and Robustness.

- Due to large storage space the video requires, it is usually necessary to decode the watermark message from a small portion of the video. This means that the watermark information should be spread through the whole video. A designer should define a trade-off between payload and portion of the video required for watermark retrieval. Due to this requirement the schemes with holographic property are especially useful.

- Videos are usually distributed in compressed form. Even DVDs and Digital TV broadcasts are based on MPEG (Moving Picture Experts Group) compression. To have a real time decoder and encoder, the watermark needs to be encoded and decoded in compressed domain. In addition the video compression format may be changed by some parties (not necessary hostile ones). Thus, every scheme should be checked against various compression techniques.

- In video broadcast systems there is a limit on the bandwidth. Insertion of the watermark may increase the required bandwidth. A designer should be aware of this fact and prevent cases of breaking the upper limit of the bandwidth.

- Video media is susceptible to increased attacks than any other media. As the number of frames is high, robustness against temporal attacks is very difficult. 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.

- Selection of positions to insert watermark is very challenging because of the temporal scene changing feature of videos.

- Video content is sensitive to subjective quality and watermarking may degrade the quality.

1.8. MOTIVATION

The past few decades, owing to the increased popularity of multimedia applications along with World Wide Web, have envisaged tremendous increase in the usage of multimedia content, especially, videos. Several innovative techniques are used both by professionals and common population to create digital videos(Jensen-Link and Thompson,1995). Apart from this, there is a growing population who use videos to hide or embed details such as owner information, date, time, camera settings, event/occasion of the video, video title, secret information for value added functionalities and secret communication. Watermarks can also be used to ensure the authenticity of a digital video.

There have been many watermarking schemes proposed (Hasan *et al.*, 2012; Channalli and Jadhav, 2009), each aiming to develop robust algorithms that protect digital contents and ownership. However, the continuing revolution in the communication medium is demanding and thus, it has become imperative to improve watermarking techniques that can satisfy the property of CAR (Confidentiality, Availability and Reliability) along with maximum transparency, capacity and robustness. Search for techniques to answer the above properties is the focus of the present research work. The main motivation is to find a technique that can simultaneously protect, preserve security without destroying or degrading the content of the video. However, existing algorithms face issues like the following:

(i) introduction of perceptual distortions

(ii) high time complexity and

(iii) low immunity to attacks.

Thus, advanced schemes that can solve the above problems are to be designed to achieve more comprehensive and sustained, privacy control and tamper detection. Further, presently the speed of the embedding and extraction procedures is high and depends on each watermark. Many algorithms for developing watermarks on images are extended for videos (Despande and Rajurkar,2010). But some points need to be considered during the extensions.

- Between the frames there exists a huge amount of intrinsically redundant data.
- There must be a strong balance between the motion and the motionless regions.
- Strong concern must be put forth on real time and streaming video applications.

All these challenges and issues motivated this research work to focus on developing watermarking techniques that hide copyright information in video frames.

1.9. RESEARCH OBJECTIVES

To address the issues and challenges faced by the existing video watermarking techniques, this research work proposes techniques that can hide copyright information inside a video file. The primary objective of these techniques is as follow.

> *"To design and develop robust watermarking techniques that can be used for copyright protection of video data in both compressed and uncompressed domains"*

The secondary objectives to meet the above main goal are framed as follows.

- To use visual cryptography and nested watermarks to increase the robustness, payload and transparent characteristics of the proposed algorithms.
- To develop techniques that identifies optimized locations for embedding watermarks into video data.
- To proposed techniques that insert watermark in uncompressed (raw) and compressed video sequences based on transformation techniques.
- To develop techniques that
    - Reduce computation complexity
    - Maintain visual quality of video data
    - Resist attacks

1.10. ORGANIZATION OF THE CHAPTERS

The underlying objective of this research work is to develop video watermarking algorithms. This chapter introduced the concepts behind the research topic and presented the formulated research goals. The rest of the dissertation is organized as below.

The literature review is a critical look at the existing research significant to the work that are carried out. In case of watermarking, several researchers have addressed the problem of information hiding. A critical look at the various available literatures related to the present research work is given in **Chapter 2, Review of Literature**.

The research methodology used in the design of the proposed algorithms along with a brief description of the various techniques used by each step is presented in **Chapter 3, Methodology** along with the overall research methodology. The proposed video techniques perform watermarking in two steps. They are (i) selection of embedding frames and (ii) embedding / extraction of watermarks in videos. The watermark embedding is performed both on compressed and uncompressed videos. The techniques used for selecting the embedding frames that produce minimum video degradation are presented in **Chapter 4, Design of Frame and Region Selection Algorithms.** The embedding and extraction algorithms for uncompressed and compressed domains are respectively presented in **Chapter 5 (Design of Watermarking Techniques).**

To analyze the performance of the proposed watermarking algorithms, several experiments were conducted using different videos and copyright images. The results obtained from these experiments are presented and discussed in **Chapter 6, Results and Discussion**. The research study is concluded along with future research directions in **Chapter 7, Summary and Conclusion.** The work of several researchers are quoted and used as evidence to support the concepts explained in this dissertation. All such evidences used are listed in the reference section (Bibliography) of the dissertation.

1.11. CHAPTER SUMMARY

Since the rise of the Internet one of the most important factors of information technology and communication has been the content protection. Due to the nature of the current digital world, many techniques have become essential for the protection of digital data. Watermarking is a techniques used for such applications. This study proposes enhanced watermarking techniques for protecting video content. This chapter provided a brief introduction to the research work along with the research objectives. To achieve the objectives outlined in this chapter, a clear understanding of the existing solutions is needed and for this purpose a literature study was conducted. The result of such a study is presented in the next Chapter, Review of Literature.