IMPROVING SECURITY FOR VIDEO WATERMARKING

By

Milan Gupta

A thesis submitted to the Auckland University of Technology in fulfilment of the requirements for the degree of Master of Philosophy (MPhil)

November 2020

Acronyms Used in This Thesis

BCH - Bose–Chaudhuri–Hocquenghem

CDT- Component Division Technique

DCT - Discrete Cosine Transform

DFT - Discrete Fourier Transform

DST - Discrete Sine Transform

DWT - Discrete Wavelet Transform

ECC - Error Correction Codes

HEVC - High-Efficiency Video Coding

HVS - Human Visual System

HVSCAP - Human Visual System with better embedding capacity

HVSVIS - Human Visual System with high visual quality

JVT - Joint Video Team

LSB - Least Significant bit

MD5 - Message-Digest Algorithm Five

MPEG - Moving Picture Expert Group

MSE - Mean Squared Error

NC - Normalized Correlation

PSNR - Peak Signal to Noise Ratio

RSA - Rivest–Shamir–Adleman

SSIM - Structural Similarity Index Measure

SVD - Singular Value Decomposition

TTP- Trusted Third Party

VCEG - Video Coding Expert Group

VLC - Variable Length Code

Abstract

A digital watermark, embedded in an image or a video frame, is additional or less visible data inserted into the original image, video, or audio in the style of a text, logo, audio, etc. In order to create it either easy or laborious to reconstruct the watermark, the embedded data is often extra or less clear. Comparative video watermarking is a highly innovative tool designed to unravel the issue of digital video manipulation and sharing. It's the process of incorporating copyright information into video watermarking.

In this thesis, we take use of singular value decomposition (SVD) and discrete wavelet transform (DWT) to embed the algorithmic rule for video watermarking, so we take advantage of Inverse DWT (IDWT) to extract the video watermarking. The approach of a digital signature is also utilized to increase privacy and authenticity.

For the watermarking, we embed an image watermark to implement video watermarking. After tampered with various attacks, the performance of this new enhanced algorithm is evaluated through MSE, PSNR, Entropy, SSIM, etc.

Keywords: Watermarking, DWT, SVD, encryption, MD5, wavelets, PSNR, entropy.

Table of Contents

List of Figures

List of Tables

Attestation of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgments), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

Signature: Date: 30 November 2020

Acknowledgment

This research work was completed as part of the Master of Computer and Information Sciences (MCIS) courses at the School of Engineering, Computer & Mathematical Sciences (SCMS) in the Faculty of Design and Creative Technologies (DCT) at the Auckland University of Technology (AUT) in New Zealand. My deepest thanks are to my supervisor Dr. Wei Qi Yan who has provided me with much appreciated technological guidance and support. I believe that I could not achieve my Master's degree without his invaluable help and supervision.

On a personal note, I would like to express my gratitude and love to my parents, wife, and son for their continuous support, understanding, and encouragement during my entire time of academic study in Auckland.

Finally, I would like to offer my blessings and regards to all those who have supported me in various ways to complete this thesis.

Milan Gupta

Auckland, New Zealand

November 2020

Chapter 1
Introduction

This chapter starts with the background and motivation of the research, which covers a brief description of watermarking importance. The scope of the thesis includes various characteristics, classifications, basic requirements, and applications of digital watermarking. The later section of this chapter highlights the challenges and major trends of video watermarking. The last section explains the structure and contribution of this thesis.

1.1 Background

Watermarking has appeared firstly in Italy in 1282, which began by applying a thin wire into the paper mould and adding a transparent label inside the paper (making the paper visible or to be treated as a trademark). The purpose and significance of the earliest watermarks are unsure. They were used for appropriate functions, such as the identification of moulds on which sheets of paper were prepared or the acknowledgment of the papermaker as trademarks. They may have portrayed mystical signs, or they may have simply acted as an honour. The watermark on paper became practical in Europe and America in the eighteenth century. They were used as trademarks, to record and show the originality of the date when the document was manufactured. The word “watermark” started to be used at that time to recognize the anti-fraud measures on cash and other documents.

At the end of the eighteenth century, the word “watermark” was first used. In 1779, Mathison commenced the first banknote forgery. Counterfeiting has caused developments in skills in watermarking. An Englishman, William Congreve, developed a technique for creating coloured watermarks by injecting dyed material during papermaking into the centre of the paper.

One more Englishman, William Henry Smith, invented fresh practical experience. The fine wire patterns used to create earlier marks are replaced by a kind of shallow relief sculpture, pressed into the design of the paper. The resulting variation created beautiful watermarks with different shades of grey on the surface of the pattern. This is the fundamental technique on the $20 paper note used today for the face of President Jackson. The word watermark, which means watermark in English, may have been taken from the German term wassermarke. A reference to the influence of watermark on the paper is possibly the meaning of the word watermark. The imperceptible messages about the objects in which they are embedded are an instance of watermarking in early history.

In the area of music, another instance of watermarking is. A U.S. patent (1961) describes a new copyright prevention innovation. By injecting an identification code into the music by applying a narrow notch philter based at 1 kHz, the watermark was introduced. The loss of energy at this frequency revealed either a dot or a dash for a decryption code. The Morse code was used on the recognition signal. This technology is close to the latest digital methods used. Until it was recognized as a means of copyright protection, digital watermarking evolved gradually.

A machine-detectable pattern that could be put on several documents for anti-counterfeiting purposes was identified in 1979. Nine years later, a method for embedding an identification code into an audio signal was identified by researchers. Researchers first employed the term digital watermark in 1988. The notion of digital watermarking gained widespread acceptance in the early 1990s. The first Information Hiding Workshop (IHW), which included digital watermarking as one of its key topics, was held in 1996.

In 1999, more conferences were dedicated primarily to the protection and watermarking of multimedia materials. Many organizations started to consider watermarking technologies during this time for use in different values. The Technical Working Group on Copy Security (CPTWG) tested watermarking systems for DVD video security. The Stable Digital Music Initiative (SDMI) has also implemented the security of music and sound systems.

The International Organization for Standardization (ISO) has developed advanced MPEG standards. Several businesses, including sounds, images, and videos, were interested in watermark technology and intellectual property rights. Dig marc, for example, used the watermark embedding and detection technology with Adobe's Photoshop in the field of image watermarking. Watermarked items became widely available in the late 1990s.

1.2 Motivations

The pervasive existence of digital network networks means that it is easy to copy and distribute digital documents to large numbers of people without any expense. Digital audio, image, and video files are downloaded by people and they can share them with friends and exploit or alter their original content. There is an immediate need to protect the ownership of those media because of this. There is a broad range of innovations that will protect against unauthorized copying. To solve this issue, digital watermarking algorithms were developed. To prove the identity of the owner and avoid copyright infringement, watermarking algorithms insert digital signatures or digital data. Copyright security services are provided to their clients by many commercial companies around the world.

The watermark is visible where it is easily seen by the owner and observer or invisible where such decoding algorithms can be identified by the originator. The watermark needs to be durable for this application so that it cannot be broken by digital media alteration. The algorithm needs to be blind, another prerequisite for watermarking for copyright protection. The host media is not needed to remove the watermarking information for blind techniques. Security is an important issue that requires only the owner to change the watermark. The number of special sessions held at recent conferences and the efforts made on related European projects such as Certimark and Encrypt is a good indication of the increasing interest in this topic. Whereas watermarking robustness has usually been associated with the possibility of decoding error or resistance to removal of watermarks, the definition of watermarking protection is still fuzzy.

Recent work has accepted that security attacks have a wider reach than robustness attacks, as the former is concerned not only with the simple impairment of communication mechanism but also with the achievement of rights given by the system's hidden parameters. Watermarking helps to recognize the actual possessor of digital information. It is one of the potential strategies for securing digital information.

The threats that a watermarking system must face dependence on the application considering where it is being employed. For example, there are some metadata applications where the sole purpose of the watermark embedding is to provide the asset in consideration an “added value” so that they are usually not susceptible to attack; this function is often shared by the other applications, such as linking content to a database or web or electronic controlling devices (such as personal video recorders or toys), when they are linked to a web or database.

The applications like medical image watermarking, legal document authentication, data tracking, or fingerprinting, on the other hand, could face a highly hostile environment where the most disruptive attack is not even that aimed at the removal of embedded watermarks. Indeed, for the applications which are connected to the legal climate, accepting a forged content as legal could be more dangerous than rejecting a valid one, or reading a watermark instead of deleting it. The watermarking safety issue has given rise to these kinds of considerations in recent years. So, the purpose of this research project is to come up with an approach that overcomes the limitations of the existing watermarking process by providing more secure and robust ways of video watermarking.

1.3 Importance of Watermarking

A major rise in the uploading of digital media files has been caused by the availability of personal computers and convenient access to the internet. Pictures, songs, videos, and other documents can be these digital files. In 1993, with the launch of the first commonly used web browser, the internet became user-friendly. The internet is an outstanding digital media delivery mechanism because it is affordable and helps people and organizations to download and distribute easily. Therefore, these files and documents have become very general to copy and alter. For a myriad of years, the unauthorized copying of certain forms of media has been a matter of concern. As a consequence, an immediate solution is needed for copyright confirmation and protection.

Digital watermarking is an effective approach for protecting intellectual property and copyrights by shielding multimedia data such as photographs, videos, or audio files from information such as signatures, logos, or manuscripts. However, a high risk of piracy is also seen by copyright owners (especially large Hollywood studios and music labels). Using analogue devices has faced a lower risk in the past than using digital media; copying an analogue file contributes to consistency degradation. However, songs and movies can be generated without any quality degradation using digital media recording, because the data is a stream of 0's and 1's.

By using the digital devices and linking them to the internet, individuals capture and upload copyright-protected material without returning or paying for their efforts to the owners of legal content. Legitimate owners of the property have begun to search for a competent method to defend their rights. Perhaps the most familiar form of preserving digital information is cryptography.

Cryptography provides a small security measure; once the decrypted material enters the consumer, there will be no further security. Therefore, further content protection is required, even after it is decrypted. The watermarking is a popular technology that is used to comply with the creator's copyright rights. The knowledge is hidden inside the content in digital watermarking. Digital watermarking can withstand various types of attacks, including compression, conversion from digital- to analogue, and changes in file format.

To survive all these processes, a watermark can be built. For several applications for copy prevention and copyright protection, watermarking has been well-thought-out. The watermark can be used in copy deterrence to warn hardware or software devices that copying should be limited. The watermark may be used in copyright protection applications to recognize the copyright holder and ensure sufficient payment of the royalties. Although copyright security and copy prevention have been major drivers of watermarking field research, there is a range of earlier applications for which watermarking has been used. It includes broadening, monitoring, monitoring activities, and confirmation. Medical photographs, satellite images, and photos taken by mobile phone cameras include other applications that include still picture watermarking.

Usually, one hidden key is used in the watermarking process. The essential element of informing the user that the material is legitimate or not by identifying the watermark is this hidden key. Insertion or embedding is called the positioning of watermarking within the device. The method by which the watermark is extracted is called detection or extraction. The use of a watermark is also a solution for copyright security and authentication of ownership; the digital data becomes more stable and is safe from infringement. There are various types of techniques for watermarking available. Each of them offers various characteristics and functions that can be used for various purposes.

1.4 Scope

Digital watermarking is characterized as the action by which a message, text, signature, or logo is concealed in an image, video file, audio file, or other media work. For quite a long time, these activities have existed. The field of digital watermarking is comparatively young and gained attention in the latter half of the 1990s as a research subject.

Digital watermarking may be noticeable, such as the pictures on money notes are printed, or invisible, for which the media covers the watermark. Examples include fabrics, product packaging, and clothing labels that can be watermarked by using special invisible inks and dyes, or as electronic signals. Watermarking is extended to physical items. Popular types of signals that can be watermarked include examples of electronic representations of audio, video, and images. The dissertation focuses on invisible watermarks using electronic signals in this study. The job of the watermark consists of an initial un-watermarked media, called the host or cover media (also known as the media representing or transmitting) and secret material (the watermark).

Digital watermarking is characterized as the process by which a message is imperceptibly embedded in the host by suitable means. It is possible to characterize a watermarking device as a structure that has two parts: embedding component and detector component. Two inputs are taken from the embedding portion. One is the message that one wants to encode as a watermark, and the other one is the work of the cover or host that one wants to embed the mark into. The job with the watermark is transmitted. By using the detector, which is used to decide whether or not the watermark exists, the embedded message can be retrieved. Digital watermarking, including identification of the copyright owner and defence, is used to give ownership protections.

1.4.1 Digital Watermarking

By comparing it to a traditional paper watermark, a digital watermark is best described to provide proof of authenticity; traditional watermarks are applied to all types of media. They are imperceptible, not even when the document for inspection is held up to alight. Similarly, in a way that can be seen by a device but is imperceptible to the human eye, digital watermarks are applied to digital images. A digital watermark includes a memo that provides information about the image-maker or distributor.

To mitigate copyright infringement, a digital watermark is used to transmit copyright information about an image. In an image-editing program or our Internet or Windows Explorer reader, a human being opens a digitally watermarked image to receive notification through a copyright symbol ((c)) that the image contains copyright and ownership information.

Digital watermark may include a link to the copyright holder or image point to complete contact information, making it easy for the observer to approve the image, license another like it, or task fresh work. To our human visual system, digital watermarks are undetectable, but provide images with a vigorous, determined identity. The digital watermark energy inside the picture varies to help conceal the digital watermark so that it remains imperceptible in both flat and detailed areas. The digital watermark is vigorous, with many traditional image edits and transformations of file formats.

Digital watermark is a sequence of bits that define the copyright and authenticate data inserted into digital audio, video, or photograph. The purpose of the watermark technique is to incorporate the secret information into the original message, which is resilient against attacks, seamlessly concealed within.

Even after its transmission, digital watermarking is an effective way to protect the copyright of multimedia data. Watermarking refers to the method by which a secret structure, called watermark, is introduced into multimedia data containing either the knowledge of the owner or the receiver of the original data object.

The three most important properties that need to be fulfilled for digital watermarking are robustness, invisibility, and protection. According to the method of concealing watermark bits in the host frame, frame watermarking approaches are divided into two major categories. The two groups are domain technique and spatial domain technique of transformation. Watermark embedding and identification were carried out in the spatial domain by directly measuring the pixel intensity values of the video frame. Transform domain techniques, on the other hand, change the host video's spatial pixel values according to a pre-determined transform and are having more robustness as compared to the spatial domain. Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT) are the most commonly used transformation domain techniques.

1.4.2 Characteristics of Digital Watermarks

The characteristics of digital watermarking are explained:

- **Robustness:** The watermark must withstand image modifications common to conventional image processing applications and, to name a few, image compression. This means that even after basic signal processing operations such as geometric image operations and noise filtering have been applied, the watermark should still be retrievable.

- **Undeletable:** The watermark, without degrading the original image, should be difficult to erase by an unauthorized user. So, being undeletable is an important characteristic of the watermark.

- **Imperceptible:** The watermark should be visually invisible in such a way that it does not affect the experience of viewing the image.

- **Unambiguous:** Unambiguity is another important characteristic of a watermark. The recovery of the watermark has to identify the owner of the watermarked image.

1.4.3 Classification of Digital Watermarking

- **Text Watermarking**

The insertion data can be embedded in text watermarking in the form of text such as the college name or any other text.

- **Image Watermarking**

The insertion information can be in the form of an image in image watermarking as any image can be embedded in data.

- **Audio Watermarking**

Audio signal of a composition recording, an auditory book, or a viable audio watermark is slightly adjusted in a definite way. This variation is so small that an auditory difference cannot be detected by the human ear. The audio watermarking technology thus offers the possibility of producing copies of a recording that are interpreted by listeners as identical to the original, but which, based on embedded details, may differ from each other.

- **Video Watermarking**

Video watermarking is also achieved by applying still image technologies to each movie frame or using dedicated methods that take advantage of the video sequence's inherent features. This adds a watermark to monitor video applications in the video stream. It is the photo watermarking extension. Real-time extraction and robustness for compression are required.

Video watermarking in the area of multimedia is a young and rapidly developing field. Subsequent variables have helped to create interest in this area. Culture is corrupted by the immense privacy of digital data, as it has become increasingly easy to copy digital media. This is an age in which the battle against "violations of intellectual property rights" has to take place. Due to malicious attacks, copyright rights must not be undermined. At this stage, the misuse of digital data needs to be secret. With the advancement of multimedia systems, the need for safe communication and digital data transfer has theoretically increased.

In image transfers, data integrity is not safe. Digital watermarking is the primary method used for the defence of intellectual property rights and copyright enforcement. Data related to copyright can be presented in the form of audio, text, image, or video. Watermarking may be either invisible or visible. Invisible watermarking means that when the watermark signal is shown, the presence of the watermark is scarcely discernible. Watermark embedding results in minimal distortion in the watermarked signal's audible or visible components. If even after applying common watermarking attacks, the watermark cannot be extracted easily from the watermarked signal, it is referred to as robust embedding.

For identification, copyright, and annotation, video watermarking embeds data into the video. A variety of methods of video watermarking have been proposed. In order to embed robust watermark and preserve the fidelity of original video, conventional encryption algorithms exploit various methods to provide access to encrypted digital data to authorized users only. However, once this data is decrypted, nobody has a way to prevent its unlawful copying and dissemination. For videos, several algorithms are extended for the development of watermarks on images. There is a large amount of redundant data between the frames. The movement and motionless areas should have a strong balance between them. Real-time and streaming video technologies must be a strong concern.

1.4.4 Types of Digital Image Watermarking

- **Visible watermarking**

A transparent translucent image that is overlaid on the primary image is a transparent watermark. Visible watermarks alter the signal altogether in such a way that the watermarked signal is completely different from the actual signal, such as applying an image to another image as a watermark. The association's seal or emblem enables the primary picture to be displayed, but it simply results in the properties of the owning company at rest. An example of visible watermarking is shown in Figure 1.1.

The watermark does not completely hide the critical picture, but it recognizes the supplier and prohibits the picture from being used without adding the marking. If the object of representative asset rights is to be accomplished, it is necessary to overlay the watermark in such a manner that does not make it easy to take out.

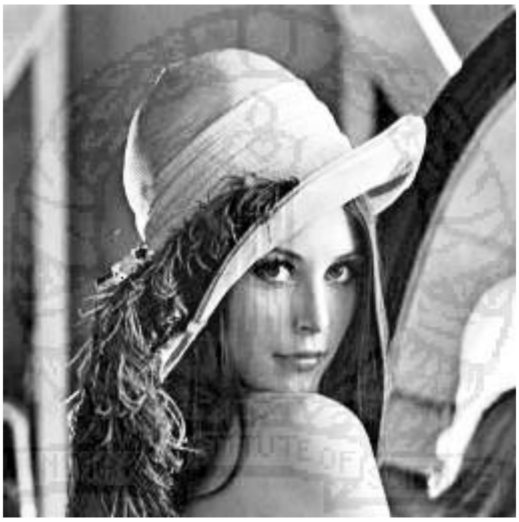


Figure 1.1: An example of visible watermarking

A clear semi-transparent text or image overlaid on the real image is a clear watermark. It allows the true image to be displayed, but by labelling the image as the property of its owner, it offers exclusive rights protection at rest. Visible watermarks next to the transformation of images are more vigorous. They are also preferable in the digital format for the physically strong exclusive defence of intellectual property rights.

- **Invisible Watermarking**

An invisible watermark is an overlaid image that cannot be seen but can algorithmically be identified. They do not convert the signal to a perceptually broad scope, i.e., the output indication has only minor variations. An invisible watermark is when only the least important bits are applied to an image by changing certain bits. Two very different forms of invisible watermarks, unlike applications of this knowledge:

  - Pertaining to prove an image's realism, a watermark that is lost when the image is digitally manipulated can be useful. The image has not been “doctored” if the watermark is still undamaged. If the watermark was harmed, then the image was manipulated. Such devices, such as digital images as evidence in court, may be critical.
  - An invisible watermark that under any image manipulation is very resistant to destruction may be useful in verifying ownership of an image suspected of misuse. The source of the image will suggest digital identification of the watermark.

Figure 1.2: An example of invisible watermarking

An example of invisible watermarking is shown in Figure 1.2. An unseen watermark is an embedded image that cannot be detected by the eyes of humans. To recognize the right shoulder, only electronic devices (or advanced software) can retrieve the secret information. To prove its validity, invisible watermarks are used to stain specialized digital content (text, photographs, or even audio content).

1.4.5 Essential Constituent of Video Watermarking

Digital watermarking is defined by features, including the efficiency of embedding, fidelity, the payload of data, blind or informed detection, robustness, protection, cipher and watermark keys, unambiguous sensitivity, false-positive rate, modification and multiple watermarks, resistance to manipulation, unobtrusiveness, cost, ready detection, and scalability. The correlative significance of all properties depends on the application requirement and the position that the watermark would play. In most practical applications, some of them are popular. The general specifications are mentioned and briefly discussed in this section. The research focuses on the watermarking of the image and video.

- **Fidelity**

What criteria does an ideal watermarking scheme have? Fidelity will be the first condition. When the cover picture gets distorted to the point of becoming irrelevant, or even extremely irritating, a watermarking device is of no interest to anyone. Ideally, except on the highest quality equipment, the watermarked image should be perceptually invisible. While visible watermarks appear to be more durable, it is ideal for the embedded label to be undetectable to the human ear or eye for general purpose applications. Invisibility is the degree to which when a user views the watermarked material, an embedded watermark remains unnoticeable. Researchers have so far attempted to conceal the watermark in such a way that it is not visible. This condition, however, clashes with the other criteria, such as robustness and tamper resistance.

- **Robustness**

An ideal watermark should also be fully distortion resistance, highly durable, either during regular usage, i.e., accidental attack, or intentional attempts to remove or disable the present watermark, i.e., malicious or deliberate attack. Unintentional attacks include transformations that, during normal use, are typically applied to images, such as resizing, enhancing contrast, cropping, etc.

Robustness means resistance to removal by signal processing of an embedded watermark. Using audio, pictures, and video signals in the digital form usually includes several kinds of distortions, such as lossy compression, or filtering, resizing, improving contrast, cropping, rotating, and so on, in the image case. For watermarking to be beneficial, even after such distortions have occurred, the mark should be observable. It is a belief that robustness against signal distortion is best achieved by putting the watermark in perceptually relevant sections of the signal. This all depends upon the lossy compression algorithm behaviour that operates without affecting the quality of the audio, video, or compressed image, by discarding perceptually insignificant data. Image compression is an especially interesting type of unintentional attack.

A final note is that either complete fragility or resistance to attack may involve robustness. It may be the case that if any tapering is present, few watermarking systems may enable the watermark to kill the original item. Watermarks concealed among perceptually insignificant data are therefore likely not to survive compression. The resistance to geometric manipulations such as translation, resizing, rotation and cropping is still an open problem in the case of image watermarking, but such operations are very common and a solution must be sought before watermarking techniques are effectively applied to the defence of image copyright. The majority of video watermarking systems are based on image watermarking techniques.

- **Use of Keys**

It is an interesting characteristic of an ideal watermarking scheme. Use of keys is introduced to make sure that the solution is not made useless as the algorithm is known to all. It may also be an aim for the scheme to use an Asymmetric Key System (AKS), such as in cryptographic private/public key systems. The private key schemes in watermarking are fairly simple to implement while asymmetric key pairs are usually not.

The risk involved is that embedded watermarking systems might have found their respective private key, ruining the security of the entire system. This was precisely the case when a secret key of DVD decoder's single implementation was left unencrypted, undermining the entire system of DVD copy protection.

- **Blind Detection**

The ability to identify the watermark without referencing the original text refers to blind detection. It is a particularly important necessity of video watermarking because of having uncompressed video files with enormous size and the complexity of indexing them while searching for a particular frame.

- **Capacity and Speed**

Capacity and speed may be slightly less significant criteria for an ideal watermarking scheme. A watermarking system must allow the image to be embedded with a useful amount of information. It can vary up to different text paragraphs from a single bit. Also, the identification (or embedding) of the watermark should not be too computationally intensive in watermarking systems intended for embedded applications to avoid its usage on low-cost microcontrollers.

Capacity is the amount of information that can be conveyed by an embedded watermark. Using information-theoretical concepts, the theoretical ability of embedded watermarks was examined. The watermarking algorithm could be depending on the application at hand, allow a predetermined number of bits to be concealed. There are no general rules here, but in the case of an image, the chances of embedding at least 300-400 bits into the image should be permitted. In any event, device designers should bear in mind that it is not infinite to be able to hide the number of bits in data; but quite often it is reasonably tiny.

- **Statistical Imperceptibility**

An ideal watermarking system is having statistical imperceptibility as the last possible requirement. The algorithm for watermarking must alter the bits of the original image such that the image statistics should not be altered in any indicative fashion that is likely to reveal the existence of a watermark.

There are several different attacks to be considered and it will be helpful to incorporate countermeasures into the video streams to cope with distortions created by the processing of such videos. On a video stream, it is practically possible to do some transformation by introducing random geometric distortions for still images that get success in trapping the detector synchronization.

- **Low Error Probability**

The probability of detecting a watermark when, in fact, one does not exist, i.e., false-positive, and of not detecting a watermark, i.e., false-negative, must be very low except in the absence of signal distortions or attacks. Typically, algorithms based on statistics have no trouble fulfilling this requirement; however, if watermarking is to be legally legitimate, such skill must be demonstrated.

- **Real-time Detector Complexity**

The detection and extraction algorithms must have low complexity. These algorithms should get executed within the given real-time deadlines for consumer-oriented watermarking applications.

1.4.6 Applications of Digital Watermarking

For the last two decades, digital watermarking has been a relatively new area. It is possible to insert digital information into data and remove it later. Texts, logos, handwritten signatures, or numbers can be the watermarking details. There are many applications of digital watermarking provided as follows.

- **Copyright protection**

To define and secure copyright rights, digital watermarking can be applied. Watermarks representing metadata identifying the copyright owners can be surrounded by digital content.

- **Copy protection**

It is possible to watermark digital content to show that digital content cannot be criminally simulated. Duplication-competent devices can detect such watermarks to avoid unauthorized duplication of the material.

- **Tamper proofing**

For tamper-proofing, digital watermarks which are brittle in nature may be used. Whenever any kind of change is made to the content, digital material can be surrounded by fragile watermarks that are lost. For authenticating the material, certain watermarks can be used.

- **Broadcast monitoring**

The number of radio and television channels providing content has grown remarkably over the last few years. Exponentially, the amount of content flowing through these media vehicles continues to expand. Here, the extremely disjointed and increasingly varying market has become essential, distributors, content owners, copyright holders, etc.

- **Fingerprinting**

The features of any object that appear to differentiate it from the other small objects are fingerprints. The watermark for fingerprinting is used in copyright protection applications to trace the registered users who breach the license agreement and criminally distribute the copyrighted content. So, the data implanted in content is typically about the consumer, as the identification number of the customer.

- **Access control**

Various payments allow users to have different rights on the object (play/copy control). It is important to provide a copy and use monitoring mechanisms in a few systems to avoid unauthorized copying of the material or restrict the number of copying times. For such purposes, a robust watermark may be used.

- **Medical application**

Patient’s names may be written on X-ray records and MRI scans using visible watermarking techniques. In the care given to the patient, medicinal reports play an extremely vital role. If two patients' accounts are combined, this may lead to a tragedy.

- **Image and content authentication**

The intent of authentication is to detect modifications to the information in an image authentication application. The characteristics of the image are surrounded by variations, such as its margins, and contrasted with the current images. Cryptography, where the digital signature was previously studied in the form of message authentication, may be employed as a solution to this problem. The trustworthy digital camera is one example of digital signature technology being used for image authentication.

- **Annotation and privacy control**

A picture is possible to be annotated by using multibit watermarking. For instance, it is possible to carefully insert a patient’s records and image information relevant to any medical image into the image. This would not only decrease the storage space but also provide a close connexion between the picture and its data. By not holding confidential information as plain text in human-readable form, patient isolation is simply regulated. The watermark can be secured further through encryption. Other uses of watermarking annotation are automatic extraction of data and electronic record indexing.

- **Media forensics**

Forensic watermark applications boost the ability of any content owner to identify and respond to abuse of its property. Forensic watermarking is used to obtain proof of criminal incidents and to enforce contractual relationships between the owner of the material and the persons or organizations with which the information is exchanged.

- **Content safety for audio and video content**

Nowadays, modern digital formats are used for the rental or sale to users of commercial video and audio material like DVDs, Blue-Ray Discs, and iTunes, implement material security technologies that regulate the use of and access to the content and prohibit unauthorized copying and rearrangement of content. To obtain a decrypted copy of the material, parties attempting to designate unauthorized allocation and copying the protected commercial audio or video content must evade the security of the software.

- **Document and Image security**

Considering documents and photos produced in support of the launch of the main product, through very diverse sales and advertisement networks, commercial communication, professionals face tremendous challenges in controlling these belongings. The documents and photos are sent to the remote offices, departments, dealers, distributors, etc. and must be handled to ensure that confidentiality of data is maintained until the date of launch.

- **Improved auditing**

The digital content from the Internet continues to burgeon and find its way too many modern electronic devices and many websites around the internet-television, music, movies, etc. Digital auditing watermarking systems can validate use by all participants throughout the supply chain to enable highly accurate billing and contract compliance.

1.5 Challenges of Video Watermarking

Digital watermarking is having long centred on still photographs, but this practice disappears nowadays. Multiple watermarking algorithms are being proposed for multimedia data, and particularly for video content. However, even though it is a related issue for watermarking still images and video, it is not equivalent. New concerns and new challenges arise and need to be tackled. The three major challenges of video watermarking are explained below:

a) Various Non-Hostile Video Processing:

Digital watermarking robustness has been measured by the permanence of the embedded watermark after the attacks. To automate this method, benchmarking instruments have also been produced. The possibilities for attacking the video are multiplied in the background of the video. There are also several non-hostile video processing systems available. The non-hostile applies to the fact that even suppliers of content are likely to process their digital data a bit to leverage their resources effectively.

Photometric attack collects all attacks that change the frame's pixel values. Such improvements may be due to a wide variety of video processing processes. For example, some noise is likely to be created by the data transmission. Likewise, certain distortions in the video signal are introduced by analogue to digital and digital to analogue transformations.

To increase contrast, another common process is to conduct gamma correction. Some content owners also re-encode their digital data with a different compression ratio to minimize storage needs. The watermarking algorithm's efficiency is then likely to be altered by the induced loss of information. Similarly, users are probably moving their videos to a common format like MPEG-4, MPEG-1, or MPEG-2 from a standard video format, e.g., Uh. DivX. The watermark signals are bound to encounter some form of interference here again. To restore a low-quality video, spatial filtering is often used within each frame. There is also a need to consider inter-frame filtering, i.e., the filtering between the adjacent frames in a video. Finally, the chrominance re-sampling (e.g., 4:4:4, 4:2:2, 4:2:0) is a method that is widely used to minimize storage requirements.

- **Spatial desynchronization**

The implicit spatial synchronization between the embedder and the detector is the basis of many watermarking algorithms. A pixel is believed to be linked with a specific bit of the watermark at a given place in the frame. Non-hostile video processing, however, introduces spatial desynchronization that can bring in a severe loss of watermarking device output. For example, changes in display formats and spatial resolution.

The positional jitter occurs in a wireless environment for the video over weak analogue connexions, e.g., broadcasting. While using a handheld camera the purpose is not to remove the embedded watermark explicitly, so the distortions caused in this case can be measured as non-hostile. We can divide the handheld camera attack into two geometrical distortions of a bilinear transform.

- **Temporal desynchronization**

Likewise, the watermark signal can be influenced by temporal desynchronization. For instance, if for each frame the secret key used for embedding is different, a simple modification of the frame rate will make the detection algorithm fail. Watermarks should be built so that they withstand such an operation because changing the frame rate is very ordinary processing.

- **Video editing**

All the operations that a video editor can conduct are collected by the very last sort of non-hostile attacks. Two very popular processing methods during video editing are cut-and-splice and cut-insert-splice. Cut-insert-splice happens when in the middle of a movie, a commercial is added. The transition effects are taken, such as wipe-and-matte or fade-and-dissolve, to have a smooth transition between video scenes.

In comparison to spatial editing, this kind of editing is treated as temporal editing. In each frame of the video stream, spatial editing refers to the inclusion of visual material. For example, this involves the superimposition of video streams, such as in the Picture-in-picture technology, and graphic overlays, such as the addition of logos or subtitles. The activity is eyed by using the detector as a partial watermark is being cropped. A serious attack is likely to cause a high deterioration in the efficiency of detection.

b) Resilience Against Collusion

The collusion problem was already reported some time ago for still images. In order to generate illegal information, i.e., unwatermarked data, it refers to the collection of malicious users who combine their awareness, i.e., various watermarked data. In two different distinct cases, such collusion is successful.

- **Form I collusion**: In various copies of different data, the same watermark is inserted. From each watermarked data, the collusion will estimate the watermark and retrieve a refined watermark estimate by linear the combination e.g., an average of individual estimates. Getting a reasonable watermark estimate enables unwatermarked data to be obtained with simple subtraction of the watermarked one.
- **Form II collusion:** In various copies of the same data, different watermarks are inserted. To generate unwatermarked data, the collusion only must form a linear combination of various watermarked data, e.g., the average. Indeed, the average of distinct watermarks usually converges towards zero. In the sense of digital video, collusion is a very significant problem since there are twice as many possibilities to construct collusion as with still images. As the video is considered, it is possible to double the sources of the collusion.
- **Inter-videos collusion:** For still images, this is considered as the initial origin. To create unwatermarked video content, a group of users has a watermarked version of the video. The identical watermark gets embedded in various videos in the sense of copyright security and Form I collusion is possible. Alternatively, for everyone, the watermark would be different in a fingerprinting application, and Form II collusion can be considered. To generate unwatermarked video content, inter-video collusion requires various watermarked videos.
- **Intra-video collusion:** This is a specific source for a film or video. The video for watermarking then comes down to a series of still photos of watermarking. Sadly, this opens new possibilities for collusion.

From Form I collusion, the same watermark is placed in each frame because several images can be retrieved from the moving scenes. At the same time, if different watermarks are inserted in each frame, as they generate identical images, Form II collusion becomes a hazard in static scenes. So, the watermark can be removed from the video stream by using a watermarked video.

Real-Time Watermarking: Another specification for video watermarking could be real-time. For still pictures, it was not a legitimate concern. A few seconds is a reasonable delay when someone wants to insert a watermark or to verify the existence of a watermark in a picture. In the background of the video, however, such a delay is impractical. To achieve smooth video streaming, frames are also sent at a reasonably high rate, usually 25 frames per second. At least the embedder or the detector should be able to handle such a pace, and even sometimes both. The detector should detect the embedded watermark in real-time in the sense of broadcast monitoring.

The video server should be able to insert a watermark identifying the customer at the same rate at which the video is streamed in a VOD environment. The complexity of the watermarking algorithm should be as low as possible to satisfy the real-time requirement. Moreover, if the watermark can be embedded straight into the compressed stream, it will prevent the full decompression and recompression and consequently will reduce the computational requirements.

c) Design Issues of Video Watermarking:

The design of algorithms for video watermarking has issues that are not considered during designing algorithms for image watermarking. Unlike image watermarking, video spots a plethora of challenges to the artist. The following are the issues that must be addressed:

- Video content has a considerably high amount of data that needs to be managed effectively. This requires high computational complexity, execution, and memory or storage limitations.

- Watermark embedding takes place in several domains: spatial, frequency, and time domains. A significant attribute to be considered is the imperceptibility of the watermark. Video has a higher degree of perceptual irrelevancy and redundancy that can be utilized by both designer and attacker.

- Video, unlike images, has several standards for encryption and compression. It must be handled separately according to CODEC (e.g., H.263, MPEG2, MPEG4). The watermarking algorithm must be adapted to the video type for real-time video streaming. MPEG4 watermarking methods handle objects, for instance, while MPEG2 schemes typically work in the DCT domain.

- Popular video editing practices such as frame resizing, frame switching, frame lowering, cropping, geometric frame adjustments, frame rate changes, format transformations, and individual attacks should be preserved by Video Watermarks. Algorithms must embed a large amount of information as a watermark (like more than 60 bits per second).

- As watermarking and streaming are handled together and compatible during transmission on the Internet, the streaming problems must be carefully addressed.

1.6 Major Trends in Video Watermarking

Video watermarking is a new field of study that essentially profits from still image findings. In the scientific literature, several algorithms have been suggested and three main patterns are separated. The easiest and most straightforward solution is to view any video as a series of images and to apply an established still image watermarking method. To build new robust video watermarking algorithms, one considers and utilizes the extra temporal dimension. The last pattern considers a video stream as any data which is compressed as per the standards of video compression and is used to achieve an appropriate watermarking scheme with the features of such a standard.

Digital watermarking was thoroughly explored for still images in its very first years. Many interesting findings and algorithms were found, and the very basic issue was trying to reuse the earlier findings as new fields, such as video, were researched. As a result, the video was first regarded by the watermarking community as a concatenation of the still images and then accommodated the existent watermarking schemes to the video for the still images. When the coding culture moved from image coding to video coding, the almost same phenomenon occurred. Indeed, the first proposed video coding algorithm was Moving JPEG (M-JPEG), which compresses every frame of video using the JPEG image compression standard.

The best way to expand a watermarking method for still image is to insert the same watermark at a standard rate in the video frames. The existence of the watermark on the detector side is tested in every photo. A normal pulse in the response of the detector should be observed if the video has been watermarked. Such type of scheme has no payload, however. The detector cannot extract the provided watermark, it only indicates whether any hidden message is present or not.

On the contrary, the original data used to be much larger as compared to a single still image. High payload watermarks may be anticipated for video as one should conceal the added bits in the larger host signal. This can be achieved easily by embedding in each frame of the video an individual multi-bit watermark. One should be mindful, however, that this payload gain is balanced by the lack of robustness. Initially, Differential Energy Watermarks (DEW), a new approach was developed for still images. It was expanded to video by applying watermarking on MPEG stream I-frames. In a compressed data stream, it selectively discards the DCT coefficients of high frequency.

1.7 Thesis Structure

1.7.1 Contributions of Thesis

The basic contribution of this thesis is to utilize and apply the already existing features and technologies of image watermarking into the field of video watermarking and security.

- The watermarking process and literature review of the already existing digital watermarking techniques are explicated in Chapter 2.
- Basic requirements and different methodologies for digital watermarking are discussed in detail in Chapter 3.

- For video watermarking, the existing watermarking techniques are used with different algorithms to make videos more secure and authentic, as proposed in Chapter 3.

1.7.2 Organization of the Thesis

The detailed structure of the thesis is given below:

- Chapter 2 includes the introduction watermarking process and various techniques used for digital watermarking. As we are aware the digital image analysis is a very vast area so in this thesis we are covering and focusing on the defined scope. A comprehensive review of the literature on digital watermarking techniques and the watermarking process is outlined in this chapter.

- In Chapter 3, after the literature review in the previous chapter, we have described the methodology for video watermarking. It also explains the proposed solution and various requirements for conducting and executing this proposed solution. The algorithm with DWT and SVD using 3-level wavelets, digital signature, and various frames of video is explained. At the end of this chapter, various parameters like Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE), Entropy, and Structural Similarity Index Measure (SSIM) are discussed to evaluate the watermarking process.

- In Chapter 4, we show the results carried out from various datasets using different approaches to the watermarking process. It describes and does a comparison of results, collected against various parameters used for benchmarking and evaluation, from different approaches of the watermarking process.

- Chapter 5 is to outlines the conclusion, significance, and future work of the thesis.

Chapter 2
Literature Review

In this chapter, we expound on the literature review of the watermarking processes. In Section 2.1, we inspect the watermarking processes in detail. In Section 2.2, the research conducted on various techniques and algorithms around digital watermarking is analysed. It covers a wide area of watermarking processes based on domain, motion sensitivity, SVD, and hybrid domain. It also inspects the algorithms on video watermarking for compressed and uncompressed domains. Section 2.3 covers the literature review of various proposed/implemented approaches in brief.

2.1 Watermarking Process

Digital watermarking is a method of inserting information (i.e., watermark) into an image or other digital data that can be extracted or identified later for a variety of purposes, including for identification and authentication.

The watermark to be embedded is hidden in the cover object, it may be a picture, text, audio, or video file, and the watermark is retrieved and extracted from the picture during extraction to obtain the original image. In the field of watermarking, the general terms and meanings are:

- **Watermark:** To conceal the data that is generated. The word watermark also refers to the embedding information process, often like the actual watermark on paper. The secret message is also known as the Watermark.

- **Cover Media:** It is the media that hosts or carries the watermark. Sometimes we use the expression of host or original media.

- **Watermarked Data**: It is the medium that contains the watermark.

- **Embedding**: The process of injecting or inserting the actual watermark into the cover media. The watermark embedding is shown in Figure 2.1.

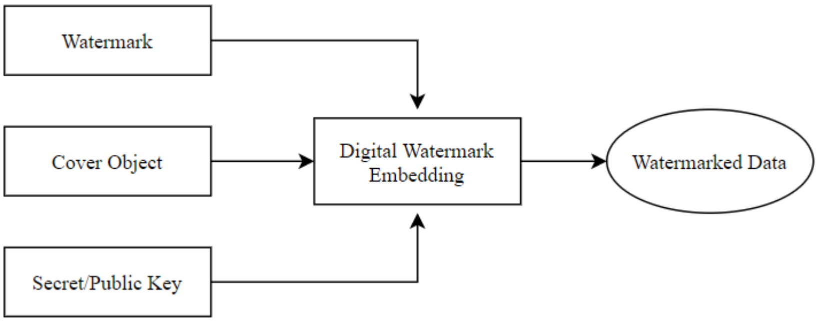


Figure 2.1: The diagram of watermark embedding

- **Detection**: The process used to identify or detect whether any watermark is present or not in the given media.

- **Extraction**: After detection, the embedded watermark used to be extracted from the watermarked data. The process of extracting the watermark is called Extraction as shown in Figure 2.2.

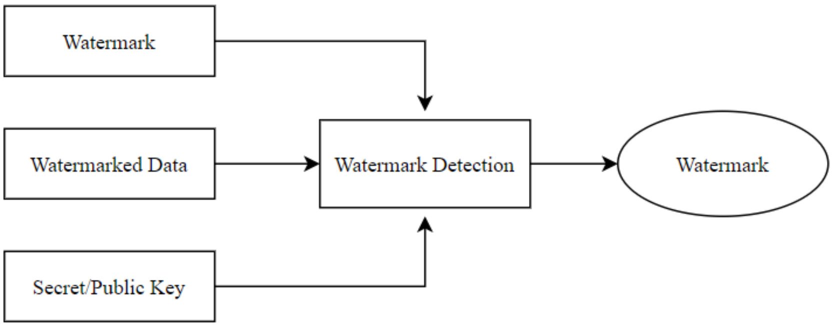


Figure 2.2: The diagram of watermark detection/extraction

- **Watermarking**: The whole scheme or process of embedding and extraction is referred to as watermarking.

- **Noise:** This is an unwanted component induced in the signal by various means. For example, through thermal processes or during transmission**.**

- **Attack:** It is the artificial process, which is used, intentionally or non-intentionally, to modify the watermarked data by altering or destroying the watermark present in it.

- **Attacked Data**: The watermarked data on which some artificial modifications are applied causing it to carry noise or errors, is termed as attacked data.

2.2 Algorithms of Digital Watermarking

2.2.1 Classification Based on Domain

Various domains are present to perform the classification of video watermarking techniques. They are spatial domains and domain transformers. Another strategy is hybrid methods that combine both the domain of space and transformation and are suggested by recent researchers.

a) Frequency Domain

The embedding of the watermark in this domain is done in the transformation domain of the initial video. For instance, the most popular domain for video watermarking is the frequency domain (DFT, DCT, DWT, etc.). The watermark is to be embedded in these transformations and distributed over the entire domain of the cover image, which is accomplished by adding a transformation to the original image. The transform domain watermark is like the spatial domain watermark, except that the values of the selected frequencies are varied instead of pixels.

The higher frequencies are lost to any compression or scaling technique applied to the host signal. Hence, for embedding, lower or mid-band frequencies are used. The watermark is spread over the complete host signal after the inverse transformation is applied, i.e., the changes that occurred due to embedding are distributed to all of the pixels in that domain. These algorithms can therefore easily sustain the cropping impacts.

- **Discrete Cosine Transform:** This was initially widely studied in the form of JPEG and MPEG by the source coding group and was later also considered for the usage of embedding a message within pictures and videos. This then expanded into the use of DCT as well for watermarking. In image coding, DCT is the most widely used transformation technique.

  There are many pixels in an image arranged in $m \times n$ blocks. The original image is firstly broken into 8×8 blocks of pixels in a DCT-based watermarking scheme. As a balance between complexity and consistency, the size of the blocks was selected. In order to obtain the DCT coefficients for each 8×8block, the two-dimensional DCT is then performed independently on each block and results in 64 DCT coefficients for each block. Middle-frequency range coefficients are chosen from the DCT coefficients and adjusted in such a way that their relative values are encoded as one or zero to insert bits of the watermark.

Due to its moderate variance property, the middle-frequency coefficients are usually chosen. This is required so that there is no perceptual manifestation of the modification of DCT coefficients. The watermarked image can be obtained by performing each block's inverse DCT.

- **Discrete Wavelet Transform:** The Discrete wavelet transform consists of the decomposition of an image by multi-scale frequency. In the case of a two-dimensional image DWT, the image is firstly broken down into four components of high, medium, and low frequencies (i.e., LL1, HL1, LH1, HH1) by horizontal and vertical sub-sampling channels using sub-band philters. To acquire the next coarser scaled wavelet coefficients, these sub-bands can be further decomposed
- **Discrete Fourier Transform:** In the signal processing area, the discrete fourier transform is widely studied and was considered in the watermarking area to offer the possibility of manipulating the host signal frequencies. To obtain the best compromise between visibility and robustness, it is often useful to select the satisfactory parts of the image to embed the watermark. In the real number arena, the two-dimensional DFT is executed, and hence the DFT of an image result in the image's magnitude and phase representation. It was thus noticed that it was possible to use phase modulation for robust watermarking.

The phase components of the DFT have a greater psychovisual effect than the components of magnitude. Therefore, a malicious attacker will cause unreasonable harm to the quality of the image by attempting to delete the watermark while the watermark is embedded in the phase components with high redundancy. This feature of the DFT coefficient guarantees the unreasonable loss of image quality caused by attacks against the watermark. For watermarking purposes, DFT proves to be helpful where phase modulation is carried out between the watermark and its cover and where the DFT is often used to break images into perceptual bands.

An algorithm for still images was proposed and then extended to still frames of raw video. Against common image processing attacks, good sustainability was achieved and experimentation with MPEG2 coding/decoding at different bit rates was carried out.

A video watermarking scheme was proposed that embeds both the watermark and a template in the video by using 3D DFT. This template has been found useful against certain attacks, such as changes in frame rates, aspect ratio modification, and frame rescaling. The video watermarking algorithms that use DCT in literature are very prominent. Since most of the video compression standards are based on DCT transformations, many digital video watermarking algorithms embed the watermark into the DCT domain, and these algorithms demonstrate good compression sustainability. In many watermarking algorithms, DCT was considered where some added watermark DCT coefficients to host video DCT coefficients and/or some algorithms modified video DCT coefficients according to watermark or HVS characteristics can be integrated into the embedding process.

b) Spatial Domain

In the spatial domain, the pixels of the frames are modified according to the watermark by simply adding or replacing bits in the selected region. The domain's characteristics are its simplicity in execution and design, less time complexity where the host video does not need to be transformed, and therefore real-time implementation is possible. A lot of watermarking techniques are proposed in spatial domains.

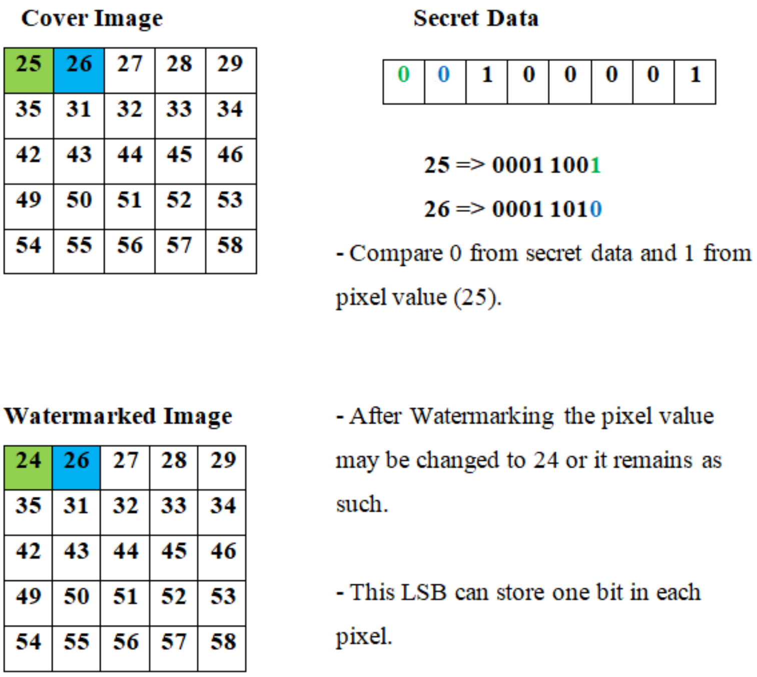
Wu et al. proposed an embedding technique to achieve perceptual invisibility by considering the difference between two adjacent pixels and by quantizing it as per the watermark bit. The system has proposed a blind extraction method that uses a combined spread spectrum and QIM to compare the spatial and transform domain video watermarking techniques. It has been observed experimentally that the spatial domain method described above has suffered from a brightening attack. A spread spectrum watermarking that has a high resistance to narrow-band interference and eavesdropping was suggested by Hartung and Girod.

Just Another Watermarking System (JAWS), is a 2D spread spectrum model was proposed by Kalker. JAWS is a scheme that makes use of shift-invariance to achieve high payload and detection reliability. This technique, however, is not resistant to attacks from rotation and scaling. Most of the spatial domain techniques are not resistant to simple cropping of images, i.e., image cropping easily removes the watermark.

- **Least Significant Bit (LSB)**: For invisible digital watermarking, there are many algorithms available. Least Significant Bit (LSB) insertion is the simplest and the most straightforward form of watermark embedding algorithm, in which the least significant bit of each 8-bit pixel is overwritten by a bit from the watermark. In this technique, by having the exceptional high channel capacity to use the complete cover image for transmission, a small object can be embedded several times. In digital images, the information can be embedded directly into each bit of image information or we can calculate the busier areas of the image to conceal these messages in less recognizable parts of the image. There were two techniques to conceal the data in the spatial domain of images and were based on the Least Significant Bit modifications of the pixel value.

  Despite its simplicity, replacing the LSB brings a lot of disadvantages. Although it may endure changes such as adding noise, cropping, the watermark is likely to be crushed by lossy compression. Purely setting the LSB bits for each pixel to one would be a better attack, completely defeating the watermark with a slight impact on the cover object. Moreover, the embedded watermark can be simply modified by a middle party once the algorithm is exposed.

  Using a pseudo-random number generator to determine the pixels to be used for embedding based on a given “seed” or key would be perfect for the essential LSB substitution. By using the LSB method, the LSB of any monochrome or colour image is able to get manipulated in a way that is imperceptible to human eye. The embedded message is decoded and, to recover the original information, it can be removed from the modified image.



Cover Image

25	26	27	28	29
35	31	32	33	34
42	43	44	45	46
49	50	51	52	53
54	55	56	57	58

Secret Data

0	0	1	0	0	0	0	1

25 => 0001 1001

26 => 0001 1010

- Compare 0 from secret data and 1 from pixel value (25).

Watermarked Image

24	26	27	28	29
35	31	32	33	34
42	43	44	45	46
49	50	51	52	53
54	55	56	57	58

- After Watermarking the pixel value may be changed to 24 or it remains as such.

- This LSB can store one bit in each pixel.

Figure 2.3: An example of LSB

An algorithm with LSB was proposed by Kurah and McHughes to which was known as image downgrading. An example of LSB is shown in Figure 2.3, the LSB insertion is an example of less perceptible or less predictable. This portion explains how an 8-bit grayscale image works and the possible effects to modify an image. The basic principle of embedding is relatively effective and simple. In case we were to use an 8-bit grayscale bitmap image, we would have to read the files and then add data to each 8-bit pixel, the least significant bits of each pixel. Each pixel in a grayscale image is shown by 1 byte consisting of 8 bits. Between the black, which is 0 to the white, which is 255, it can be 256 grey colours. Of all these bytes, the encoding principle uses the Least Significant Bit, the bit on the far-right portion.

If information is encoded to just the last two significant bits (which are the first and second LSB) of each colour component it is most likely not going to be detectable; the human retina becomes the limiting factor in viewing pictures. For the sake of this example, only the least significant bit of each pixel will be used for embedding information. If the pixel value is 25 which is the value 00011001 in binary and the watermark bit is 1, the value of the pixel will be 00011000 in binary which is 24 in decimal. The properties of Least-Significant-Bit (LSB):

- Implementation is easy.
- It is quite simple to understand.
- It results in stego-images that have concealed data that appears to be having a high level of visual fidelity.

- **Patchwork-based schemes**: The patchwork-based technique offered by Bender is another well-known spatial domain-based scheme. They identified two systems of watermarking. Second, the statistical method-based patchwork. This selects pairs of image points randomly and raises the brightness by one unit at one point while decreases the brightness of another point accordingly.

  The second approach is called texture block coding, where a random texture pattern region contained in the image is copied to the same textured area of the image. To recuperate each texture region, autocorrelation is then used. With this system, the most important issue is that it is only suitable for images that have wide areas of arbitrary texture. You can't use this scheme on photos of text.

- **Watermarking based on Correlation**: To apply a pseudorandom noise pattern to the luminance values of their pixels is the easiest way to add a watermark to an image in the spatial domain. Based on this theory, many approaches are present.

- **CDMA-based image watermarking scheme**: We may use the CDMA spread-spectrum systems to distribute all bits randomly in the original image instead of deciding the values of the watermark from “lines” in the spatial domain, thus increasing ability and enhancing cropping conflicts. Rather than a 2D image, the watermark is first formatted as a long string. Using a self-sufficient seed, a PN sequence is generated for each watermark value. Such seeds could either be stored or generated by PN techniques themselves. The watermark represents the summary of all these PN sequences; it is scaled and added to the cover image.

c) Spectrum Domain

For both the spatial domain and the frequency domain, this approach may be used. The advantage of using the spread spectrum approach is that one can retrieve the watermark without having the original unmarked picture.

2.2.2 Classification Based on Motion Sensitivity

To distinguish the video from an image, multiple variables must be taken into consideration. In the design of a video watermarking algorithm, several peculiarities help. Initial algorithms were an extension of the image watermarking that robustly embedded the watermark using frame-by-frame analysis. Video watermarking algorithms have, however, shifted to Group Of Pictures (GOP) and scene-based algorithms for the following reasons. Certain aspects are:

- In the video, the content viewed is dynamic. Human consideration cannot be concentrated simultaneously on each part of the video being played. Generally, the front object attracts, and increased focus is on the foreground as compared to the background.
- Use of the same watermark in every frame may have difficulty while maintaining perceptual and statistical invisibility. Nevertheless, applying unique watermarks in every frame also having an invisibility problem where little or no motion is present in the video. Statistically, these regions can be averaged and compared to separate the watermark.
- There are more possible attacks as compared to still images e.g., both hostile and non-hostile processing where frame dropping, frame averaging, frame rate changes, frame swapping, lossy compression, transcoding, video editing, re-sampling, etc. must be considered.
- As the host video has a lot of embedding capacity so increased information can be embedded into it with less compromise on its quality. Hence, analysis of a scene is done to select the moving objects or scenes where the HVS is less delicate to achieve perceptual invisibility. Another way, the motionless area of the video is removed by common compression algorithms to obtain the higher compression rates; therefore, watermark embedding is done in the motion area to counter various attacks.

2.2.3 Hybrid Domain Watermarking Algorithms

It is possible to differentiate hybrid domain image watermarking from hybrid domain video watermarking algorithms. In order to develop a hybrid domain video watermarking algorithm for better robustness and performance, the combination of video and audio can be considered. An algorithm is proposed for audio-video watermarking where the error correction code is created from the watermark and embedded in the audio-video channel.

This provides capabilities for error detection and error correction. Video synchronization is also provided by these hybrid techniques, which improves safety against cropping and rotation attacks. Qiu et al. suggested using, in addition to authentication, a combination of DCT transform and motion vectors to give copyright protection. However, to achieve better performance, the complexity of hybrid domain techniques is enhanced.

2.2.4 SVD-Based Watermarking Algorithms

SVD is a special matrix transformation that can convert a matrix into two orthogonal matrices and a single-value diagonal matrix. The singular value of images has adequate stability from the perspective of image processing, and it incorporates the intrinsic features of images instead of the visual characteristics. In the field of robust video watermarking, these features of SVD make it widely used, and the watermark information is always injected in the matrix of singular values to obtain strong imperceptibility. In robust video watermarking, it is typically adopted together with DWT.

A fast algorithm, gradient magnitude similarity deviation (GMSD) was used earlier to identify the shot limits of the video sequence, and later it is possible to extract representative key-frames. SVD and DWT are combined to inject the watermark information into the extracted key-frames once the watermark information is encrypted by new chaotic encryption. A blind video watermarking algorithm, based on a hybrid SVD / DWT method, was also proposed by Adul and Mwangi.DWT is implemented to the G components of the selected frames, and later SVD is implemented on the retrieved diagonal detail coefficients to embed the watermark information into the singular values matrices.

Earlier, four forms of embedding methods were presented and compared to achieve high robustness with a low payload. The fourth technique, which incorporates the identification of scene shift and the approach to the spread spectrum, integrates only one watermark into the entire frame, achieving the lowest payload yet high robustness. By scene shift identification based on the histogram difference method combined with the Fibonacci series, Sathya and Ramakrishnan extracted the mainframes. Fibonacci-Lucas scrambled the watermark before integration to enhance the algorithm's security.

The encrypted watermark is partitioned into blocks and inserted based on the DWT and SVD into the selected keyframes. The coloured watermark picture was decomposed into various 24-bit planes by Agilandeeswari and Ganesan and scrambled by using Arnold transform before the embedding. Contourlet Transform (CT) is used with video frames chosen by scene shift detection to capture smooth contours, and DWT is used to achieve better sub-bands of multiresolution. Then, the SVD is implemented to pick the DWT sub-bands for embedding the watermark. The selection of the main frames was made possible by chaotic maps. On the selected video frames, DWT is performed and SVD is applied on the transformed frames and the watermark image.

To accomplish the watermark embedding, the two singular value matrices obtained are inserted. All the video frames are taken as input processing objects for the algorithm already proposed by Shanmugam and Chokkalingam. DWT is applied to video frame luminance elements, and 2-level DWT is applied to sub-bands of the LH. Using its high stability, SVD is applied on the retrieved HL2 sub-bands, and then watermark embedding is realized. Not only doing hybrid SVD-DWT algorithms have greater relevance to human experience, but they also minimize the data factor, which means the benefits of SVD and DWT is be combined. However, the use of SVD in the embedding process of the watermark image can lead to false-positive detection problems.

2.2.5 Video Watermarking Algorithm in Uncompressed Domain

The watermarking algorithms from this category embed the watermark directly into the raw or original uncompressed video sequences before any compression was applied to it. The video sequence is encoded for transmission or storage after the watermark is embedded. The advantage of designing these methods is quite simple, but the downside is that it may not continue at the same bit rate as the original video data stream, and even after compression, the algorithm must maintain the watermark.

The algorithms were designed for watermarking in the spatial domain, based on synchronization between the extracting module and the embedding module. At a specific location, a spatial domain technique modifies a pixel as per the associated watermark bit. However, the pixel location may vary due to spatial desynchronization caused by different video processing, resulting in low performance of the watermarking scheme. Changing the spatial resolution, aspect ratio as per movie standards, etc. are the common video processing. Due to the jitter, the pixel position can also vary when a video is broadcast in wireless environments. Changing the frame rate, which causes temporal desynchronization, is another important aspect of video processing. If a different secret key is used for each frame, temporal desynchronization could be caused by the change in frame rate. Therefore, most of the uncompressed domain video watermarking algorithms are designed for transform domains instead of spatial domains. Therefore, the transformation domain is selected in a way that spatial or temporal desynchronization is less affected.

2.2.6 Robust Watermarking Algorithms on Compressed Videos

The size of video data on the Internet is enormous, so it is generally stored and distributed in compressed form. To embed and extract a watermark that is not worthy for compressed images, the traditional watermarking algorithm is based on the original file, must fully decode the file. Some compressed domain-based video watermarking algorithms have emerged as needed by the successive proclamation of international video coding standards.

In compressed videos, they embed watermark content, so watermark embedding procedures must be coupled with the corresponding standards for video coding. There is a focus on the implementation of rigorous video watermarking algorithms which is based on three coding standards, including the Moving Picture Expert Group (MPEG), H.264/Advanced Video Encoding (H.264 / AVC), and H.265/High-Performance Video Encoding (H.265 /

HEVC)MPEG-based watermarking algorithms. In 1988, an expert group, MPEG is set up jointly by the International Electro technical Commission (IEC) and the International Standardization Organization (ISO) to establish standards for the encoding, decoding, and synchronization of audio and TV image files.

MPEG series standards are the standards developed by this expert community, and different variants of the standards illustrate various uses and visual qualities, which have played a pioneering role in encouraging the advancement of multimedia communication. At first, standards for MPEG-2 and MPEG-4 are adopted, and based on them some algorithms for video watermarking are be summarised.MPEG-2 is a lossy compression format organized and formulated by MPEG in 1994 for video and audio. It is a compression system for the standard digital television and the high-definition television under different applications and codes between 3 Mbit/s and 100Mbit/s. In the compressed domain, many video watermarking algorithms need only partial decoding during the watermark embedding process to decrease the computational complexity.

In the compressed domain, the AMPEG-2 video watermarking algorithm, established on shadow-frame generation combined with DCT transformation was proposed by Wang and Pearmainto resist scaling attacks. Only the partial decoding of MPEG-2 video and the conversion between block DCT and full DCT are needed in the watermark embedding step, and the bit error rate can be reduced in the watermark extraction process using turbo codes. Li et al. proposed a video watermarking algorithm using the DC coefficients and was based on a detailed review of video encoding formats under the MPEG-2 standard.

This algorithm also does not require decoding all the video data, and after the inverse quantization process, it does the inverse DCT. In the luminance variable, the watermark information is injected into the very last DC coefficient of the last macro block for each slice, which can overcome the blocking artefacts. The watermark image was partitioned into eight binary images in a previous paper, and each image was inserted into various video sequence scenes. By integrating a visual mask established on local image attributes, a suitable set of DCT coefficients, partially decoded from the compressed videos is defined.

By changing these selected DCT coefficients, the watermark is embedded, which enhances the picture fidelity. A watermark framework was built from the architecture level combined with data compression in another paper, which has a configurable frequency and spatial domain embedding and a very large-scale integrated (VLSI) circuit architecture. A different video watermarking method, based on the empirical principal component analysis (PCA) decoding, was proposed in yet another previous paper.

Depending on the energy of the high-frequency sub-bands and the visual saliency, the sensitivity of embedding factors is calculated. Decoding is carried out by comparing elements of the first main component created by the empirical PCA, and the watermark is adaptively embedded in the LL sub-bands. The MPEG-4 is a multimedia communication format developed by MPEG in 1998 with a broad range of data rates. Its code rate ranges from 5 kbit/s to 5 Mbit/s, to support a variety of multimedia applications. By adding the already defined relationships between the pairs of quantized DCT coefficients that were in the luminance blocks of pseudo-randomly selected macroblocks, Barniet et al. inserted the watermark into video items.

In intra and inter MBs, watermarks are similarly embedded, and the masking technique is often used in the watermarked video object planes (VOPs) to reduce the visual objects. The fine granularity scalability (FGS) has been applied to video codec for watermarking based on MPEG-4, which injects watermarks during the process of encoding. The algorithm can remove the propagation of errors caused by the watermark in normal video and can use the propagation of errors caused by the modification of the watermark to protect video content.

The embedding intensity of the watermark was modified as per the local image properties, and then, by adjusting DCT coefficients, the spatial spread spectrum watermark was embedded directly into the MPEG-4bit source. The identification of scene change was introduced in another paper to select the key-frames in a compressed domain, and according to the extraction of feature points the local areas of selected key-frames were selected. The watermark embedding method is done adaptively based on Watson's perceptual model. Two Watermark embedding schemes were proposed by Gujjunoori and Amberker: The Human Visual System for High Visual Quality (HVSVIS) and the Human Visual System for Improved Embedding Capability (HVSCAP). The method HVSVIS integrates watermark data into high visual quality mid-frequency DCT coefficients, and the HVSCAP achieves the higher embedding ability by retaining better visual quality.

2.3 Reviews

In 2018, Chaudhary implemented digital video watermarking in MATLAB software by using wavelet transformation. The work on the project relies mainly on two points of view. The primary point of view describes the different watermarking techniques and illustrates the comparative description of each technique's superiority over the other. It is seen that the frequency domain is an additional suitable domain for watermarking schemes as it produces robust results compared to various domains such as special domains.

Individual watermarking algorithms were introduced by Nouioua and Shahidin 2018, to support SVD and MR-SVD in Fast Motion Frames. One of the algorithms based on wavelets, SVD, and CZ-Transform and split the frames of the cover video into red, green, and blue (RGB) bands. While most of the prevailing watermarking systems have added the watermark in each video frame, which takes enormous time and also has a noticeable impact on the quality of the video, the projected methodology selects only the fast motion frames in each shot to host the watermark.

The completely distinct technique of video watermarking has been developed by Solanki in 2018. Even if we pay zero cost, digital documents are very easy to copy by any individual. Users mostly download and share multimedia information such as images, audio, and video. For this reason, there is a great chance of digital information being repeated. There is therefore a wish to prohibit the copyright of such digital media documents. The correct solution to the current drawback is digital watermarking.

A unique video watermarking method has been introduced (Nidhi Chawla, 2018) with the use of DWT and PCA. The video water marking (VWM) theme associated with DWT and PCA is used in this paper. In the planned algorithmic rule, DWT and PCA area units are used to reinforce the embedding and decrypting technique of watermarking. The same year, Sawant has implemented Video Authentication in the digital watermarking system using Haar wavelet Transformation and LSB formula. This formula helps to remove random noise by inserting embedding data to prevent noise and attacks in the least significant part of the cover image. The results show that the planned method provides outstanding hidden invisibility, reasonable security, and well-hidden attacks.

Video encryption techniques, fixed in a compressed or uncompressed area, fall into two main categories. The first retains security and speed for encryption, and the latter retains encryption capacity. The video needs to be completely uncompressed into consecutive frames for uncompressed techniques.

Multiple studies have propped the use of Hamming code to analyse and implement cryptography to enhance security and secrecy. To make the message secure, the private message is written by entering the Hamming code (7, 4) before the login procedure. The result of the targeted message is added randomly to the unused message using the XOR function. We can access the cover video clips after steps that make sure the message is safe enough.

A human visualization system made it more attractive to analyse the results, and the use of the block-based techniques formed better results than frame-based. The Hamming and Bose-Chaudhuri-Hocquenghem (BCH) codes were used to encrypt the information, the secret message is edited. First, to distinguish interesting places from moving things, the MOT-based algorithm is used for videos. The experimental results then show that the proposed algorithm not only improves input and visibility but also improves security and stability by entering a hidden message code and dealing with different attacks.

Steganography is a technique used to conceal unknown data within cover media. It is the practice of a file being concealed within a file. Such files are suitable for encryption. Various methods of steganography were discussed by Arya in 2018, which not only conceal the message after the image but also provide protection. Data can typically be applied to audio, video, and image files in the form of text, audio, video, and image steganography. Hiding secret information is known as image steganography in the image file and as video steganography in the video file.

Steganography is a technique to embedding secret data into unsuspected objects, robust Steganography algorithm to conceal secret messages in moving videos. The video is used for data transmission as it can hold a large volume of data. The 2D-DCT of the video is taken and the secret message is embedded by checking the DCT coefficients of the video frame.

A steganography algorithm based on histograms is used to reduce the faded pixels in each frame thereby increasing and enhancing the embedding efficiency (Kelash, 2013). The quality of the stego-video is maintained as well as the secret message is made more secure. This method is more simple, easy, and authenticated as compared to other techniques. In 2014, Mostafa presented a review of various video steganography techniques. Special attention and care were paid to applications related to video Steganography using disparate cover types. Depending upon domain such as spatial domain techniques, transform domain techniques a category was made for embedding.

A comparison between the cryptography technique and the Steganography approach was proposed for concealing the secret data (Devi, 2014). From this analysis inference made is that cryptography does nothing to conceal the presence of the message to itself but just random the secret data, while Steganography emerges as an art of hiding information in such a way that its presence is unnoticed.

A new way of hiding and securing the information is explained, by Hwan and Yin in 2015, which was based on image steganography. Low processing and memory capacity IP cameras are used because IoT devices are used to provide security. The least significant bit technique is being adjusted due to the limitations of smart devices, particularly lower memory and computational power. Data tracking for earwigs and intruders will be laborious with the use of steganography and it is easy in the case of encryption because the data format in cryptography is changed. With this method, changes in the least significant bit did not result in any real degradation of quality through human perception and along with statistical analysis. For providing security and secrecy LSB insertion technique is used and suggested that cryptography should be used along with steganography to enhance security and secrecy.

A high payload video steganography algorithm was proposed by Mustafa and Elleithy in 2015 that was used in the DWT domain and based on BCH codes. The video is split into frames in this Steganography algorithm and then fragments each frame into three components Y, U, and V. The secret data is first encoded using BCH codes before the data embedding process to increase and enhance the algorithm's security and efficiency. 2D-DWT was subsequently applied to each component, but components of mesial and high frequencies (HL, LH, and HH) are used for secret information embedding.

Also, at the time of embedding and extraction, this algorithm uses two keys, which improved and boosted the system's effectiveness. This algorithm is resistant to the median attack on filtering. Linear block codes can be introduced to increase security and efficiency, and other techniques can be implemented in the frequency domain to improve or upgrade the video quality.

In the same year, Kumar worked towards steganography, and the exact video that was provided by the user is extracted after steganography of the image on video, and the difference between the input video and the output video is very small. The CDT and LSB methods are helpful, but the process has some limitations. The main limitation is that the number of frames should be greater than 255 because there is a maximum of 255 pixels in an image and we will get a maximum of 255 image matrix after applying Component Division Technique (CDT). This means that it will provide a single image with a maximum of 255 frames. For the Steganography process of an image on video by CDT, it requires the condition number of video frames>=number of Image frames. Because of the colour map and the unique matrix, we can get the exact RGB image after decoding the image. There will be zero difference between the output RGB image and the input RGB image.

A design method was utilized for video steganalysis, targeting pixel domain steganography based on HEVC video frames (Tasdemir, 2015). A high correlation among neighbouring pixels is displayed both in the temporal and spatial domains. The results attained display that the filters employed can capture both temporal and spatial distortions introduced by the steganography techniques. To increase accuracy version 3 of HEVC can be used. LSB method is discussed in an extensive sense, displaying its efficiency to embed information in the images and then its retrieval. In forthcoming data can be encrypted with a security key to boosting the level of security and other techniques like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT)can be used to increase and enhance the robustness and efficiency of the system.

Various steganographic techniques have been overviewed (Pal, 2016) and the main types and classifications of steganography were planned during that time. We analytically evaluate various planned approaches that show that the image's image quality is disgraced when hidden data grows to a certain limit using LSB-based techniques. Amongst them, techniques are fixed by concerning the assessment of the analytical properties of noise or perceptible analysis that can be spotted or display a hint of image modification. Depending on the previous mask, in 2016, Mustafa implemented the data hiding process by hiding a secret message from the DCT and DWT coefficients in all movement areas of this video. The art of secrecy and digital data communication has been taken care of by the technological development of both digital content and communication.

Based on skin-tone detection, the steganography technique was introduced (Kudel, 2016) with wavelet transform, which is one of the newest methods to hide the data into a skin image or video, which is not that serious to the Human Visual System (HVS).

For this approach biometric features like skin-tone are very important. This process embeds the secret data in specified regions rather than embedding it anywhere in the image. First, take the input image and then detect the skin-tone on the colour model of Hue, saturation, value (HSV).

Second, mask images that have been converted to the frequency domain. By using Haar-discrete wavelet transform (DWT), this is accomplished and leads to the four sub-bands. The sub-band LL (Low-Low band) is used to process the data. Haar transforms uses distinct levels of DWT, and it calculates the payload (count of bits to be embedded). Secret data embedding is carried out by tracing skin pixels in one of the given high-frequency sub-bands. First of all, crop the image, then performed all embedding process steps. Cropping results provide more security as compared to without cropping because this cropped region works as a key during decoding.

A safe steganographic video algorithm (Mustafa, 2016) based on the standard block policy was proposed. Nineteen blocked video sequences are used as a private message as cover data and a binary image objective. Using the private key to improve system safety, pixels for both cover videos and private messaging are periodically updated. We can access the cover video clips after steps that make sure the message is safe enough. Furthermore, access to each sector is periodically selected and will vary in some cases to improve the stability of the steganography strategy.

In 2017, Cem explained steganography as a method of concealing information from illegal parties within a messenger file so that it is small. Many techniques are planned to be integrated to collect a new colour image steganography method to obtain greater efficiency, secure expanded payload capacity, detachment integrity check, and cryptography security at the same time. Different formats were supported as per the proposed work. For further process, it is permanently added to encrypted header information and then fixed into the cover image. The Fisher-Yates Shuffle algorithm is used to select the next pixel location, fix the encrypted data and header information process while the Histogram-enhanced LSB and Chi-square analyses are conducted for security analysis.

In all steganography video modes, the ability to conceal and stabilize against attacks are three essential needs to be taken into consideration.

Based on the Multiple Object Tracking (MOT) algorithm and Error Correction Codes (ECC), it reflects the powerful and secure algorithm of the Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) algorithm.

An algorithm was proposed for Pixel Mapping Method (Bhattacharya and Sanyal, 2012) to conceal data, and providing high embedding capacity and imperceptible stego-image for the human vision of the secret message. The algorithm gave no degradation in the visual quality of the video and good results with high embedding capacity. Prabakaran proposed another algorithm to provide high data embedding capacity and to enhance data security and integrity. Moreover, stego-images are not perceived by intruders and show robust results. In forthcoming other wavelet-based techniques can be used for enhanced and secure results.

A study is done by Raja, to achieve secure stego-image and robustness. The combination of LSB algorithms with DCT transformation has been used. Also, compression techniques using quantization and run-length coding are executed on raw images. The LSB technique provides maximum payload which is embedded into the cover image to achieve the Stego-object. Run-length coding and quantization enhance the security of the system.

The secret images/data (i.e., cover image) can be extracted without any distortion to the carrier image (Jothy et.al, 2016). As the secret data is embedded inside the images of the carrier using IWT, the presence of the data is hidden. Fewer distortion results in a higher PSNR value. In comparison to the other methods, this technique offers the high quality of the stego-image with high PSNR values. Besides, this technique can make it easier to transmit the information to the recipient independently and more securely.

Steganography algorithms based on the spatial domain and transform domain are most used by the present Steganography tools. For data hiding applications, LSB Steganography in spatial and transform domain. A new algorithm for colour image Steganography method which executes the S-Tools and F5 in many aspects was introduced. This algorithm enhances the system performance and can retrieve the secret data even after the presence of the noise. The approximate embedding capacity is intensified to a great extent. It opened the scope to implement the 3-3-2 approach along with encryption. The PSNR value is taken as a performance measure to evaluate the quality of video distortions. In forthcoming, a more secure Steganography algorithm and more appropriate can be carried out by encrypting the secret message before embedding it in the moving videos.

Chapter 3
Methodology

The issues and shortcomings of previous work are resolved by proposing some improvements and a combination of existing approaches. In Section 3.1, we explain the different methods that are used to improvise the watermarking process. The hardware and software requirements to carry out this solution are mentioned in Section 3.2. We have explained the proposed solution along with details around our algorithm and ways to enhance the privacy of video watermarking in Section 3.3 and Section 3.4, respectively. Finally, Section 3.5explains various parameters that are used as benchmarks to evaluate the effectiveness and performance of the proposed solution.

3.1 Methods

There is a myriad of methods that could have been used to propose and implement a new approach. The basic methods that are going well with our proposed approach and methodology are explained.

3.1.1 Singular Value Decomposition Watermarking

The singular value decomposition (SVD) is a technique that is used for image compression techniques and applied to watermarking as well. The SVD is performed, and then the singular values are usually altered to inject the watermark. Then, a pseudo-inverse SVD is applied to retrieve the original content. The SVD is used on its own for the watermarking but it is often used in the hybrid techniques which incorporate both discrete cosine transform and SVD. Comparatively, the SVD is computationally complex, but after applying it in the hybrid techniques it may not be required to perform SVD on the complete image which lowers the computational complexity.

3.1.2 Discrete Wavelet Transform Watermarking

In this watermarking scheme, the watermark is partitioned into various parts and embedded in the respective frames of various scenes in the video. As an identical or same watermark is used for each motionless scene and the independent watermarks are used for consecutive different scenes, the proposed method is sturdy against the attack like frame dropping, swapping, averaging, and lossy compression. The video is partitioned into different scenes and by scene change detection each frame is converted into a wavelet domain before the actual watermark is embedded. This watermark is required to be pre-processed, being cropped into various parts.

This watermark scheme is based on four levels of discrete wavelet transform (DWT). Discrete wavelet transform with 3-level decomposition is shown in Figure 3.1. All frames in the video are normalized to 256×256 pixel size. Normalization will be performed in both the insertion and detection phase; this can make the watermark to be robust to the resizing of the video frame.

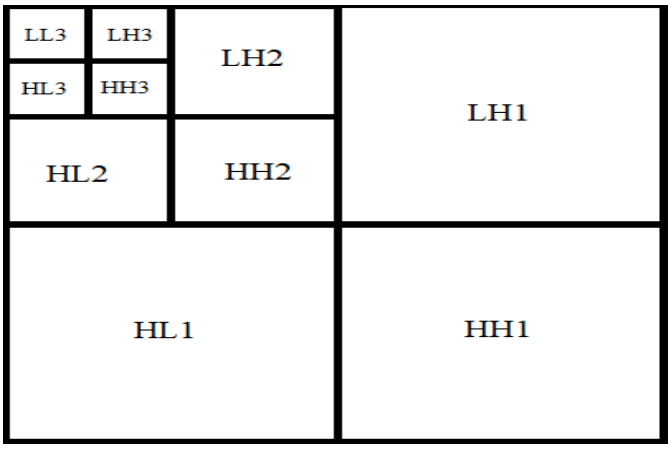


Figure 3.1: Discrete wavelet transform (DWT) with 3-level decomposition

The scheme is robust against format conversions because the watermark is inserted before compression. Otherwise, the drawback of the techniques is that, since the code is directly embedded into the compressed stream such as MPEG-4, the copyright information is lost if the video file is converted to a different compression standard, such as MPEG-2.

The steganography technique is characterized mainly by imperceptibility and capacity. Imperceptibility means the embedded data must be perceptually invisible to the observer.

The performance of the proposed technique is evaluated using different video streams (by dividing them into various frames) and secret messages images. The perceptual imperceptibility of the embedded data is indicated by comparing the original video with its stego-video. When we hide a secret image in the video there will be no loss in quality of video and even none can guess the presence of data within a video.

3.1.3 Cryptography

Cryptography is a way of protecting information and performing secure communication by using codes. It means keeping the communications private and providing a better mechanism of information security by using encryption and decryption techniques. Encryption means converting the plain message into a cipher message that has no meaning to anyone until one has the secret key to decrypt the cipher text. Decryption is the reverse process of encryption i.e., converting a cipher message into a useful plain message. This is achieved by using a secret decryption key.

The types of cryptography are shown in Figure 3.2. Cryptography has been achieved by using any of the following three ways: Symmetric Key (SKC), asymmetric Key (AKC) – using public-private keys, Hash functions (one-way cryptography).

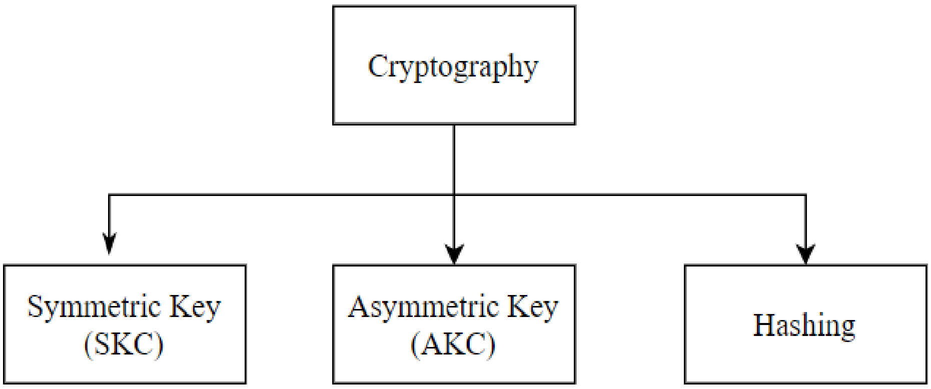


Figure 3.2: The types of cryptography

3.1.4 Hashing

Hashing means using an algorithm or function, called the Hash function, to generate a unique value for the data on which it is being applied. Hashing is used to provide privacy, security, and authentication in a much better way than encryption. The use of hashing in an image also referred to as Perceptual hashing, is a way of generating a hash value according to the visual contents of the applied image. There are several hashing algorithms with different techniques like Message Digest (MD5), Secure Hash Algorithm (SHA), and Whirlpool, etc. MD5 is the most commonly used hashing algorithm.

3.1.5 Digital Signature with Watermarking

A digital signature is a kind of cryptography. The basic process of the digital signature is quite similar to the handwritten signature, it is just like any signature on paper and it is having a digital certificate that is used to verify the identity. The signature confirms that information is originated from the party having a respective signature on it.

In digital signature, we generate the hash value from the original message, generate the digital signature on this with the sender's private key, and encrypt this data with the receiver's public key. The proposed scheme of digital signature is shown in Figure 3.3. On the receiver's end data is decrypted with the receiver's private key (as it was encrypted using the receiver's public key). Now, the digital signature (generated by using the sender's private key) will be verified by using the sender's public key at the receiver, confirms that it has been sent by the intended sender only with no intruder involved. Now, the hash is calculated on received data at the receiver's side and compared against what was sent with the message. If both hash matches, then all good otherwise it indicates something fishy is involved in the data transfer.

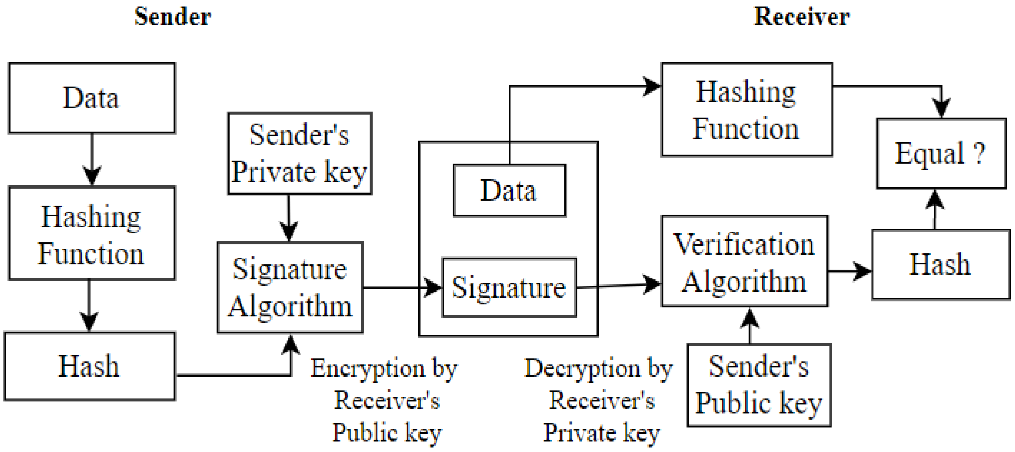


Figure 3.3: The proposed scheme of digital signature

Image Authentication

We will use the methods of digital signature and hashing for image/frame authentication. As an improvised approach, we will propose another scheme, capable of image authentication using hashing and digital signature. In the experiment, the signature will be extracted from the original image and will be embedded as a watermark into the image. On the receiver's side, the signature and watermark are extracted from the modified image. Now, we can verify the various blocks of the image. The image is authentic if the watermark and signature of corresponding blocks are the same. But any difference in the signature and the watermark indicates that the area/block has been modified and the image is not authentic.

3.2 Requirements

3.2.1 Database Requirements

The videos/images are processed, evaluated, and stored in the form of datasets at various steps of the watermarking process. The database is required to store these dataset values of images and videos.

- Database for watermark insertion.
- Database for watermark detection.

3.2.2 Software and Hardware Requirements

To perform the operations and to calculate the results with proposed approaches different software and hardware requirements need to be met. The proposed system has the following software and hardware requirements to proceed with thesis work:

- **HARDWARE**
    - Window hard disk-100GB
    - Window RAM -4GB
    - Tests were run on a Pentium i3 processor of 1.7 GHz

- **SOFTWARE**
    - Platform- windows XP/7/8/10
    - Language-MATLAB 0.7

MATLAB is a software platform that provides high-performance during technical computing, which integrates visualization, computation, and programming environment. Furthermore, MATLAB provides a modern environment of programming language: it uses built-in debugging and editing tools, supports object-oriented programming, and sophisticated data structures. Due to these factors, MATLAB becomes an excellent tool for research and teaching.

MATLAB has various advantages as compared to other conventional computer languages to solve technical problems. It is an interactive system that uses an array as a basic data element that does not require any dimensioning. The software has been available commercially since 1984 and is accepted as a standard tool in most industries and universities worldwide.

In order to enable a wide range of computations, it has powerful built-in routines. It also has graphics commands that are easy to use which makes the results visualization available immediately. Some specific applications are combined into packages and referred to as toolboxes. There are some toolboxes for symbolic computation, signal processing, control theory, optimization, simulation, and many other fields of engineering and applied science.

3.3 Proposed Solution

In this thesis, we have proposed a hybrid approach for video watermarking which is used by combining both discrete wavelet transform (DWT) and singular value decomposition (SVD) for watermarking. Moreover, a 3-level discrete wavelet transform is applied in this research work for better results. Furthermore, Daubechie’s wavelets are applied to an image to improve performance parameters like PSNR and MSE. Finally, the watermarked images are combined to generate the video producing a watermarked video. The proposed approach can be enhanced by using digital signature watermarking and hashing which is explained later as an extension/enhancement of this approach.

3.3.1 Introduction

We have come up with another solution to embed watermarks in videos. The basic approach of the proposed solution is described below:

- Divide the video into frames and choose a few frames that are compatible with the watermark size.
- Perform the 3-level discrete wavelet transformation (DWT), SVD, and different operations on the chosen frames.
- Apply SVD on the watermark, and then these frames are embedded into the initial frames.
- Nonetheless, apply SVD to the compressed watermarked frame followed by 3-level IDWT to the generated uncompressed watermark frames.

- Recombine all the watermarked frames to make a video and compare each original video with a watermarked video.
- Apply multiple types of attacks on the watermarked frames within the video. Calculate the MSE, PSNR, Entropy, and SSIM for embedding and extracting methods before and after applying the attacks.

3.3.2 Proposed Watermark Embedding and Extraction

The basic algorithm used for embedding and extraction of the watermarks in different frames of video is mentioned below:

Step 1: Take the video as input.

Step 2: Divide the video into various frames.

Step 3: On each frame, apply the video compression by using a 3-level discrete wavelet transform and SVD.

Step 4: Add the watermark information to each of the compressed frames by using the least significant bits algorithm.

Step5: Apply the SVD and 3-level IDWT to each of the watermarked compressed frames. This is called the process of decompression.

Step 6: Finally, reconstruct the watermarked frames and obtain the watermarked video.

Step 7: Similarly, apply the video compression by using 3-level discrete wavelet transform and SVD on each frame of watermarked video.

Step 8: Extract the embedded watermark from each frame and reconstruct the complete watermark image.

Step 9: Evaluate the performance of the watermarking process (embedding and extraction) using parameters like PSNR, MSE, Entropy, and SSIM.

The scheme of watermark embedding and extraction is shown in Figure 3.4.

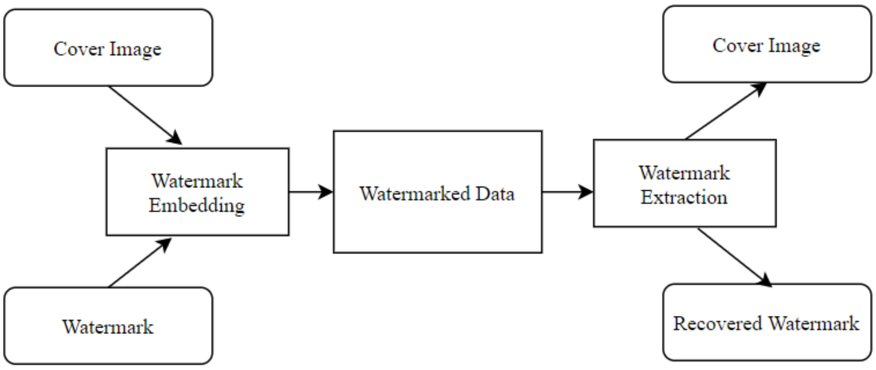


Figure 3.4: Watermark embedding and extraction

3.3.3 Proposed Algorithm (3-Level DWT-SVD Watermarking)

The algorithm steps used in the 3-level DWT-SVD watermarking process to embed and extract the watermark are given below:

The steps for watermark embedding:

Step 1: Decompose the watermark video into *m* different watermark images.

$$W = W_1, W_2, W_3, ..., W_m \tag{3.1}$$

Step 2: Apply Singular Value Decomposition for each of the watermark images.

$$[U_w(j), S_w(j), V_w(j)] = svd(W(j)) \tag{3.2}$$

where $j = 1,2,3,\ldots,m$

Step 3: Divide the host video into scenes and frames.

Step 4: Apply 3-level DWT on each frame of the j^{th} scene to retrieve the *LL3*(*j*) sub-band coefficients.

Step 5: Apply the SVD for each compressed frame of the j^{th} scene.

$$[U_i(j), S_i(j), V_i(j)] = svd(LL3_i(j)) \tag{3.3}$$

where *i* is frame in j^{th} scene

Step 6: Add watermark information into each compressed frame of the j^{th} scene by using the LSB algorithm.

$$D_i(j) = S_i(j) + K \bullet S_w(j) \tag{3.4}$$

where *K* is watermark strength

Step 7: Compute watermarked LL_3' sub-band coefficients and apply 3-level Inverse DWT to get WM components.

$$LL_{3i}'(j) = U_i(j)\bullet D_i(j)\bullet V_i(j) \quad (3.5)$$

Step 8: Finally, reconstruct all watermarked frames and retrieve the watermarked video.

The steps for watermark extraction:

Step 1: Apply 3-level DWT on each frame of the j^{th} scene of watermarked video to retrieve$LL3'(j)$ sub-band coefficients.

Step 2: Apply SVD for each compressed frame of the j^{th} scene of the watermarked video.

$$[U_i'(j), S_i'(j), V\mathrm{i}'(j)] = svd(LL_{3i}'(j)) \quad (3.6)$$

where i is frame sequence in j^{th} scene

Step 3: Extract the watermark image w'(j) for the j^{th} scene.

$$W'(j) = U_w'(j)\cdot S_w'(j)\cdot V_w'(j) \quad (3.7)$$

where $S_{\mathrm{w}}'(j) = (S_{\mathrm{i}}'(j) - S_i(j))/K$.

Step 4: Finally, reconstruct a single watermark from extracted watermark images.

$$W' = W'_1 + W'_2 + W'_3 + \cdots + W'_m \quad (3.8)$$

3.3.4 Flowchart

The flowchart for digital watermarking is generated by following the algorithm steps mentioned in the previous section. The flowchart of the digital watermarking system is given in Figure 3.5.

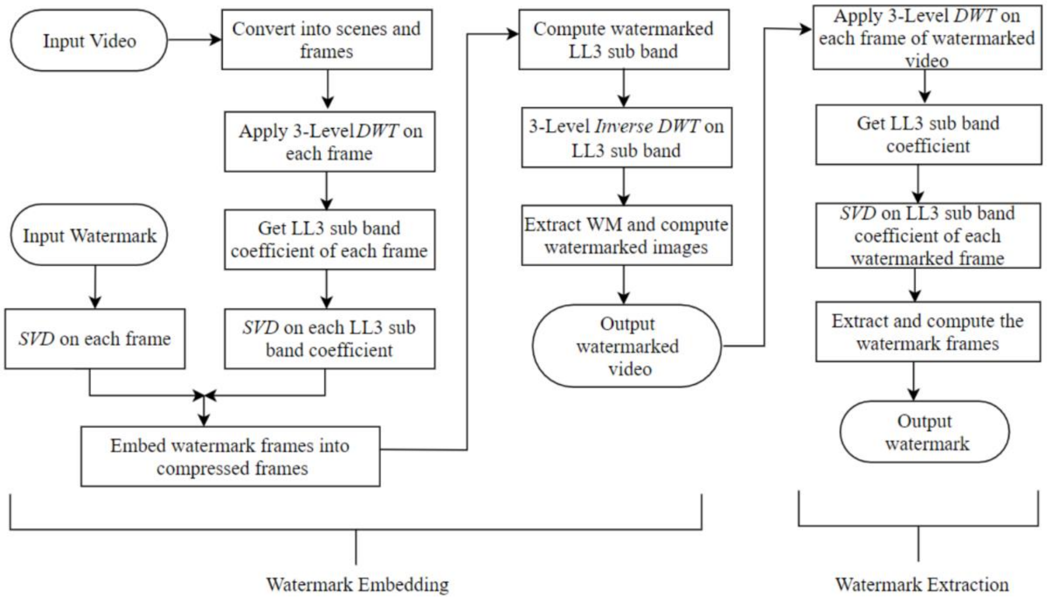

Input Video
Convert into scenes and frames
Apply 3-Level *DWT* on each frame
Get LL3 sub band coefficient of each frame
SVD on each LL3 sub band coefficient
Input Watermark
SVD on each frame
Embed watermark frames into compressed frames
Compute watermarked LL3 sub band
3-Level *Inverse DWT* on LL3 sub band
Extract WM and compute watermarked images
Output watermarked video
Apply 3-Level *DWT* on each frame of watermarked video
Get LL3 sub band coefficient
SVD on LL3 sub band coefficient of each watermarked frame
Extract and compute the watermark frames
Output watermark
Watermark Embedding
Watermark Extraction

Figure 3.5: The flowchart of the proposed watermarking scheme (3-level DWT-SVD)

3.4 Enhancing Privacy with Digital Signature

The algorithm, proposed in Section 3.3.3, is able to be extended further to improve privacy, security, and authentication in the field of video watermarking. As we know, a digital signature guarantees that the contents of a transit message will not be altered, and the message is originated via the intended sender only.

So, considering the high degree of privacy, security, and authenticity mechanism provided by digital signature we have used digital signature along with hashing algorithms to generate the watermarks. Now, this digitally signed watermark is used for video/image watermarking as already mentioned in the proposed algorithm to verify the authenticity and ownership of any video/image.

3.4.1 Proposed Algorithm (3-Level DWT-SVD using Digital Signature)

Now, the algorithm proposed in Section 3.3.3 is combined with hashing and digital signature during watermark embedding and extraction. We have used the hash function on the cover image/frame to generate the message digest. The RSA encryption scheme (with sender’s private key) is applied to the message digest to generate the digitally signed watermark which is embedded in the cover image/frame to generate the watermarked video/image. Now, we have extracted the digitally signed watermark from the watermarked video/image and its hash value (message digest) is generated by applying the RSA decryption scheme (with sender's public key) on it.

Finally, the hash value of the cover image/frame is compared with the hash value of the digitally signed watermark to confirm the authenticity and security of watermarked video/image. The steps for respective algorithms are explained below:

The steps of video watermarking with digital signature:

Step 1: Divide the host video into scenes and frames.

Step 2: Apply the hash function (MD-5) on each cover image (or frame) to generate the message digest (D_i).

Step 3: Apply encryption scheme (RSA) with sender's private key on this message digest (D_i) to generate the digital signature (S_i).

Step 4: This digital signature (S_i) is used as Watermark (W_i) and will be embedded in different images/frames, from where it is generated.

Step 5: Now, use the watermarking embedding steps for each frame/image as described in section 3.3.3.

Step 6: Finally, the watermarked video is reconstructed along with the different digital signatures.

The steps of video watermark extraction with digital signature:

Step1: Follow the watermarking extraction steps for each frame/image as described in section 3.3.3. It will provide the extracted watermark (W'_I i.e., i^{th} digital signature (S'_i) embedded as a watermark) with each frame/image.

Step 2: Now, apply the decryption scheme (RSA) with the sender's public key on this digital signature (S'_i) and retrieve the message digest (D'_i).

Step 3: Similarly, retrieve the message digest (D_i) by applying the hash function (MD-5) on the cover image (or frame).

Step 4: Finally, compare the two message digests (i.e., D'_i and D_i) to verify the authenticity, integrity, and ownership of the respective image/frame or video.

3.4.2 Flowchart

The flowchart of the digital watermarking scheme with a digital signature approach is generated by following the algorithm steps mentioned in section 3.4.1. The flow diagram of the proposed watermarking scheme using a digital signature (for watermark embedding) is given in Figure 3.6.

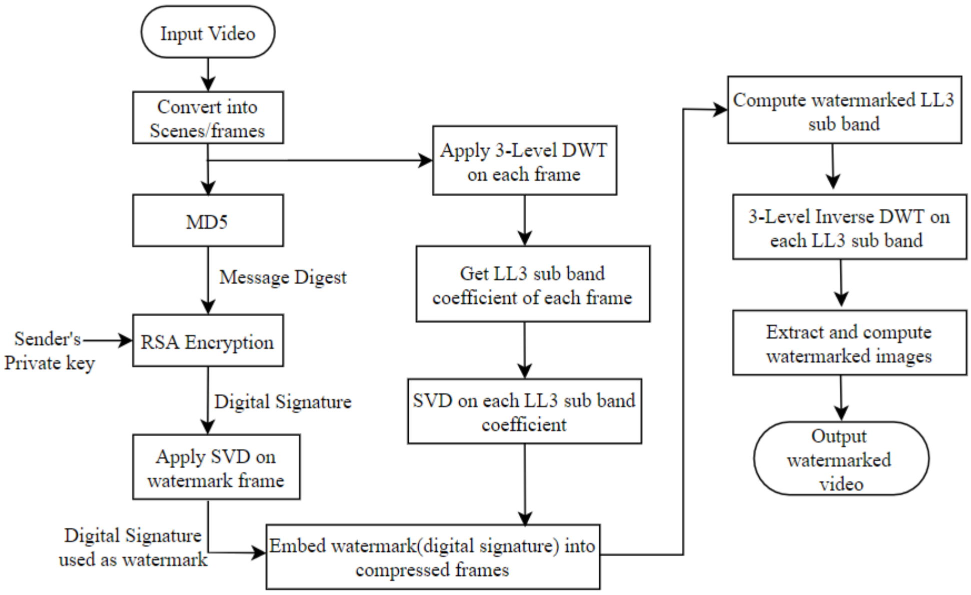

Input Video
Convert into Scenes/frames
MD5
Message Digest
Sender's Private key
RSA Encryption
Digital Signature
Apply SVD on watermark frame
Digital Signature used as watermark
Apply 3-Level DWT on each frame
Get LL3 sub band coefficient of each frame
SVD on each LL3 sub band coefficient
Embed watermark(digital signature) into compressed frames
Compute watermarked LL3 sub band
3-Level Inverse DWT on each LL3 sub band
Extract and compute watermarked images
Output watermarked video

Figure 3.6: The flowchart of the proposed watermarking scheme with digital signature (3-level DWT-SVD using digital signature)

Similarly, the flowchart of the watermark extraction scheme using the digital signature to verify the authenticity and authorization of the video is shown in Figure 3.7.

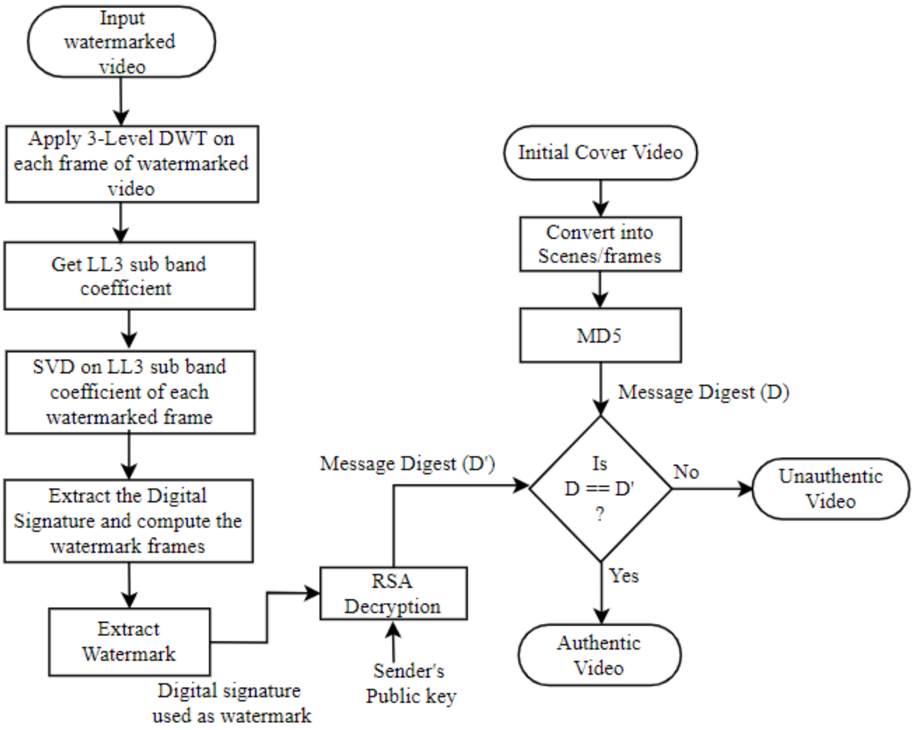

Input watermarked video
Apply 3-Level DWT on each frame of watermarked video
Get LL3 sub band coefficient
SVD on LL3 sub band coefficient of each watermarked frame
Extract the Digital Signature and compute the watermark frames
Extract Watermark
Digital signature used as watermark
RSA Decryption
Sender's Public key
Message Digest (D')
Initial Cover Video
Convert into Scenes/frames
MD5
Message Digest (D)
Is D == D' ?
No
Yes
Unauthentic Video
Authentic Video

Figure 3.7: The flowchart of the proposed watermark extraction scheme with digital signature (3-level DWT-SVD using digital signature)

3.5 Benchmarking/Evaluation

Benchmarking is used to evaluate the image quality and highlight their weaknesses or strength. They are also used to measure how efficiently various watermarking algorithms are performed so that proper comparisons between these methods are possible. Image quality metrics are the figures of merit used to evaluate imaging systems. The image quality metrics can be largely classified into two categories: objective and subjective.

Subjective image quality is a method to evaluate images by a viewer and it vigorously examines the fidelity and at the same time considers an image.

In objective measures of image quality metrics, various statistical indices are examined to indicate the reconstructed image quality. The image quality metrics give some measure of the closeness between the two digital images by making use of differences in the statistical distribution of the pixel values. The main error metrics used to compare the compression are Peak Signal to Noise Ratio

(PSNR) and Mean Square Error (MSE). We have used the below parameters to evaluate the effectiveness of the proposed algorithms.

3.5.1 Mean Square Error

The MSE is a measurement of the error with respect to the centre of the image values, i.e., the mean of the pixel values of the image, and by averaging the sum of the squares of the error between the two images. The MSE is defined as eq.(3.9).

$$MSE = \frac{1}{m*n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - I'(i,j)]^2 \qquad (3.9)$$

where *MSE* is the mean squared error, *I* is the original Image and *I'* is the watermarked image, *m* is the number of rows of pixels and ***i*** is the index of that row, *n* is the number of columns of pixels and ***j*** is the index of that column. A lower value of the *MSE* indicates a lesser error is present in the reconstructed image.

3.5.2 Peak Signal to Noise Ratio

The PSNR is used to estimate the quality of the reconstructed image in comparison to the original image. This is a standard way to measure image fidelity. Here, the original image is referred to as 'signal' and the error in the altered image as 'noise'. PSNR is the single number value, measured in decibels (dB) which is used to measure and reflect the reconstructed image quality. The PSNR is defined as

$$PSNR = 10.log_{10}\left(\frac{{MAX_I}^2}{MSE}\right)$$

$$= 20.log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

$$= 20.log_{10}(MAX_I) - 10.log_{10}(MSE)(3.10)$$

where MAX_I is the maximum pixel value in the image. These pixels are having a representation of 8 bits per sample that is 255.

3.5.3 Entropy

Entropy is a concept that was originally developed from the study of the physics of heat engines. It is a measure that describes the quantity of disorder in a system. Another way of expressing entropy is to consider the various states in which a system can adapt. Hence a low entropy system signifies a small number of such states, while a high entropy system will have many states. It is a statistical measure of randomness that can be used to characterize the texture of the image which is given as input. Entropy is calculated as eq. (3.11).

$$H = -\sum_{i=1}^{n} P_{\mathrm{i}} * \log_2 P_i \qquad (3.11)$$

where H is the entropy, P_i is the probability of the occurrence of symbol i, and n is the greyscale level of an input image (0-255).

Entropy is one of the various statistical means used to measure the texture content of a video frame or an image. The texture of an image gives measures of features such as coarseness, regularity, and smoothness. Generally, the human eye is insensitive to the high entropy areas. Hence, if a watermark is embedded in the high entropy areas of a video frame or an image then a high level of imperceptibility can be obtained.

3.5.4 Mean

Mean is the average value of all numbers provided in a system. In the watermarking process, we calculate the mean of the image/frame by calculating the average colour value of all pixels in an image to identify the share/basic colour of the image. Mean is used to get an idea around what colour pixels should be used to summarize the colour of the complete image.

$$m = \frac{\sum_{i=1}^{n} x_i}{n} \qquad (3.12)$$

where m is the mean value, x_i is the value of one pixel, n is the number of pixels.

3.5.5 Variance

Variance is a mathematical calculation to identify how each number in a set is different from the mean value of the set. In watermarking, it is used to identify the spread between various pixels of an image with the mean value of that mage. It is calculated by adding the squares of the differences of each pixel value for the mean and dividing it by the total number of pixels. The mathematical equation is given as

$$\sigma^2 = \frac{\sum_{i=1}^{N}(x_i - \bar{x})^2}{N-1} \tag{3.13}$$

where σ^2 is the variance, x_i is the value of one pixel, $\bar{x}$ is the mean value of all pixels, and N is the number of pixels.

3.5.6 Structural Similarity Index Measure (SSIM)

The Structural Similarity Index Measure (SSIM) is an alternative visual quality metric that is used to measure the similarity between two videos. It is a full reference metric. The weakness of PSNR and MSE metrics is that sometimes they do not represent the several distortions perceived by the human visual system.

A new metrics SSIM is introduced that has greater similarity with the human vision system. SSIM is more effective at estimating the perceptual quality of images than the PSNR and MSE as it considers image degradation as a perceived change in structural information. Structural information is the idea that the pixels have strong interdependencies especially when they are spatially close. These dependencies carry important information about the structure of the objects in the visual scene. The similarity measure using SSIM is already proven very robust and versatile in various environments. The diagram of the SSIM system is shown in Figure 3.8.

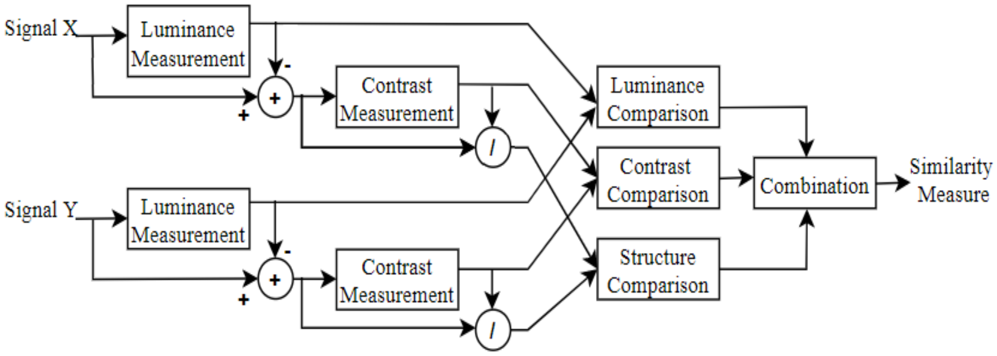


Figure 3.8: SSIM system

The SSIM result varies from -1.0 to 1.0, where -1.0 represents very noticeable distortion and 1.0 stands for perfect quality. The SSIM is given as

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c1)(2\sigma_{xy} + c2)}{(\mu_x^2 + \mu_y^2 + c1)(\sigma_x^2 + \sigma_y^2 + c2)} \tag{3.14}$$

where $\mu_x$is the average of x,$\mu_y$is the average of y, $\sigma_x^2$is the variance of x,$\sigma_y^2$is the variance of y, $\sigma_{xy}$is the covariance of x and y, and c_1,c_2 are constant variables to stabilize the division. The SSIM uses luminance, contrast, and structure comparison functions to estimate the perceived quality of an image.

- *Luminance Comparison (LC):* The luminance comparison is carried between the original image and the degraded image by using the equation (3.15)

$$LC = \frac{2\mu_x\mu_y}{\mu_x^2 + \mu_y^2} \tag{3.15}$$

where $\mu_x = \bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \,, \mu_y = \bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$.

- *Contrast Comparison (CC):* The contrast comparison between the original image and the degraded image is calculated by using the equation (3.16)

$$CC = \frac{2\sigma_x\sigma_y}{\sigma_x^2 + \sigma_y^2} \tag{3.16}$$

where $\sigma_x^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x-\bar{x})^2$, $\sigma_y^2 = \frac{1}{N-1}\sum_{i=1}^{N}(y-\bar{y})^2$.

- *Structure Comparison (SC):* The structural comparison for the original and the degraded image is done by using equation (3.17)

$$SC = \frac{\sigma_{xy}}{\sigma_x \sigma_y} \tag{3.17}$$

where $\sigma_x = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu_x)^2}$, $\sigma_y = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(y_i - \mu_y\right)^2}$,

$\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(x - \overline{x})(y - \overline{y})$, N as the size of the image(s), x_i and y_i as the intensity of the original and the degraded image, and $\bar{x}$ and $\bar{y}$ as the mean intensity of respective images, we can combine all these three comparisons to calculate SSIM as

$$SSIM(x, y) = LC \cdot CC \cdot SC \tag{3.18}$$

$$SSIM(x, y) = \frac{2\mu_x\mu_y}{\mu_x^2+\mu_y^2} . \frac{2\sigma_x\sigma_y}{\sigma_x^2+\sigma_y^2} . \frac{\sigma_{xy}}{\sigma_x\sigma_y} \tag{3.19}$$

This is as same as what we have seen earlier with c_1 and c_2 are 0.

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c1)(2\sigma_{xy} + c2)}{(\mu_x^2+\mu_y^2 + c1)(\sigma_x^2+\sigma_y^2 + c2)} \tag{3.20}$$

Chapter 4
Results and Discussion

The purpose of this chapter is to provide and evaluate various results that are generated by applying the proposed approach in the previous chapter. In Section 4.1, the basic dataset was used for generating the results. In this section, different results with multiple watermarks are generated and evaluated based on various benchmarking parameters. Section 4.2 covers the results around complete videos so that the proposed solution can be used for video watermarking. In Section 4.3, the performance and effectiveness of the proposed approach/solution are evaluated by applying different attacks on data and generating the results. Finally, in Section 4.4 we compare the performance of various approaches with different datasets.

4.1 Results with Sample Dataset (Images)

The proposed approach (3-level DWT-SVD)is applied to various images and videos to test and verify the outcomes of it. We have used various images and videos to generate the standard datasets for the provided approach. The videos are divided into different frames to leverage and enrich the sample dataset. Several images/frames are used in the watermarking process while using the proposed watermarking approach. Figure 4.1 shows the important images from the sample dataset.

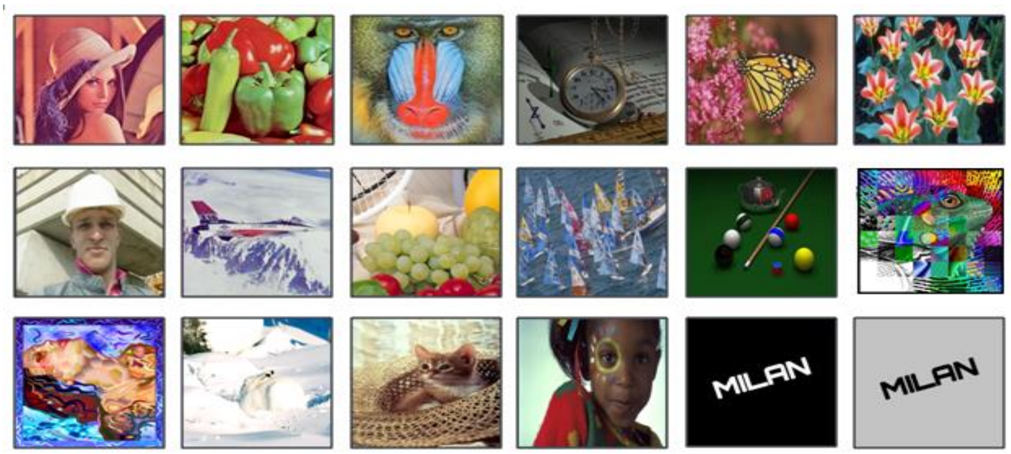


Figure 4.1 Sample images and video frames from datasets

Apart from these images, we are having a number of videos in this dataset like Foreman, Beach, Multiple Scene Type, Different Times of Day, Plants and Butterfly, and General Traffic videos. We have applied the proposed watermarking approach to multiple images/frames, to generate the respected watermarked images, extracted watermarks. The SSIM images are also generated to measure the effectiveness of the watermarked image and extracted watermark i.e., to evaluate the performance of the proposed watermarking approach with these sample images/frames. During the watermarking process, different types of images are generated for each image being watermarked.

Cover Image: Cover images can be taken by extracting frames from the mp4 video. This cover image is used to hide a secret message or an invisible watermark. Figure 4.2 (a) shows the sample images used as Cover images.

Secret Message: A watermark image is a secret message that is superimposed on the cover image with high transparency**.** Figure 4.2 (b) shows the Initial Watermark images for Watermark_1.

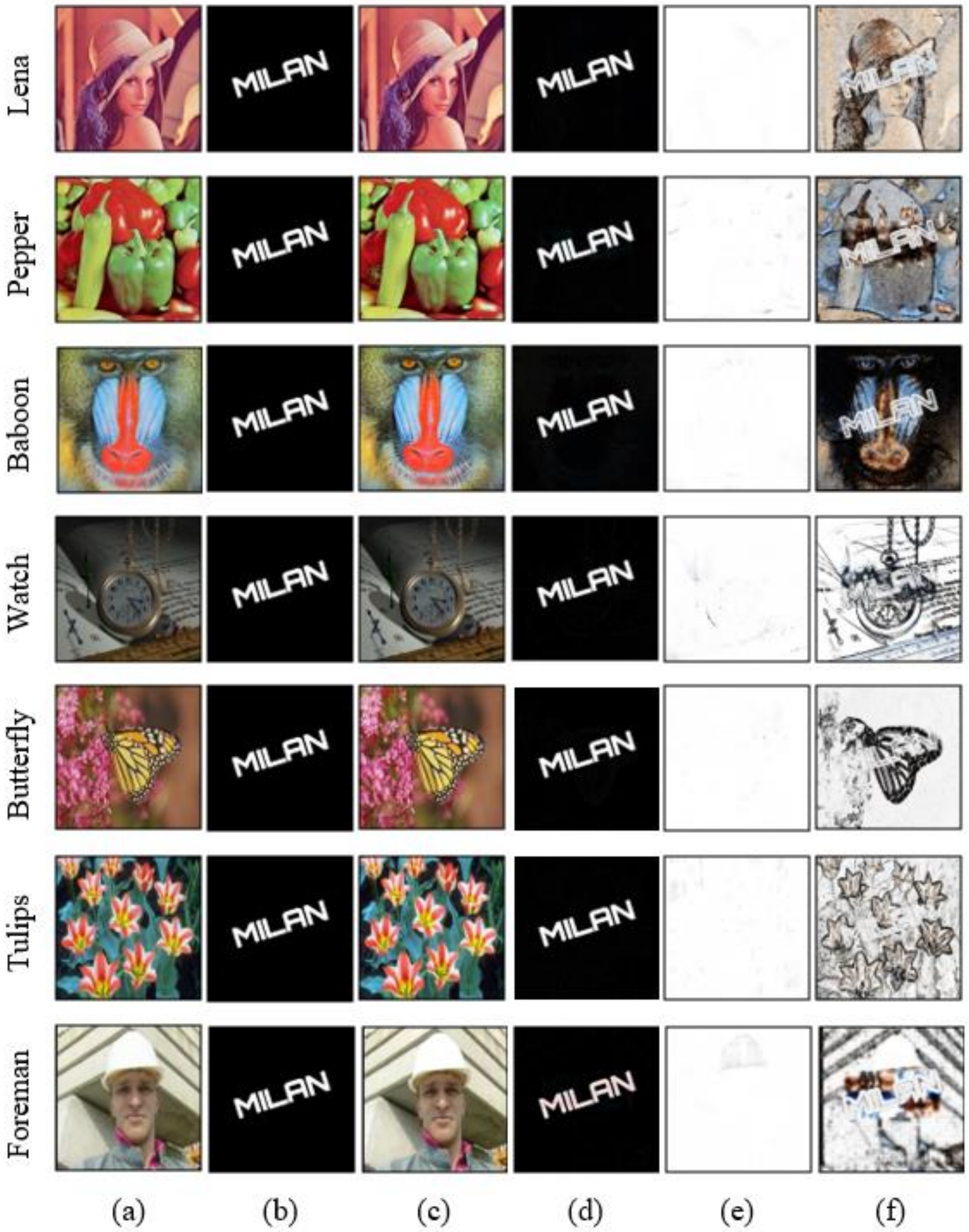


Figure 4.2 Watermarking images (a) cover images (b) watermark image_1 (c) watermarked images (d) extracted watermarks (e) SSIM for cover images / watermarked images (f) SSIM for extracted watermark

Watermarked Image: A watermarked image contains a secret message embedded in the original image**.** Figure 4.2 (c) is having the Watermarked images generated with corresponding Cover images and Watermark_1.

Recovered Watermark: Extracted secret message image from a watermarked image. Figure 4.2 (d) is having the corresponding Extracted watermarks recovered from Watermarked Images.

SSIM Image: To measure the similarity between cover and watermarked image, initial and Extracted watermark, the SSIM images are used. Figure 4.2 (e) is having the SSIM image for Cover and Watermarked image while the same for Initial and Extracted watermark is shown in Figure 4.2 (f).

The mentioned images are generated with Watermark_1 by using different images/frames from the provided dataset. The generated images as output are shown in Figure 4.2.

Table 4.1: Results with watermarked images and extracted watermarks_1

Image	Parameters	MSE	PSNR	SSIM	Mean	Variance	Entropy
Lena	Watermarked Image	2.65	54.71	0.99	131.56	3.86E+03	7.81
	Extracted Watermark	3.39	53.64	0.67	14.37	2.86E+03	2.84
Pepper	Watermarked Image	1.74	56.54	0.99	114.08	4.84E+03	7.72
	Extracted Watermark	4.26	52.65	0.53	15.12	2.81E+03	3.23
Baboon	Watermarked Image	2.43	55.09	0.99	129.77	3.55E+03	7.82
	Extracted Watermark	3.85	53.09	0.22	18.29	2.83E+03	3.79
Watch	Watermarked Image	1.95	60.81	0.99	75.36	2.08E+03	7.30
	Extracted Watermark	3.83	57.89	0.78	13.90	2.85E+03	2.36
Butterfly	Watermarked Image	1.76	58.25	0.99	107.17	3.20E+03	7.64
	Extracted Watermark	2.70	56.39	0.80	14.05	2.91E+03	2.42
Tulips	Watermarked Image	1.36	59.37	0.99	104.83	5.48E+03	7.79
	Extracted Watermark	2.35	56.99	0.72	14.30	2.91E+03	2.70
Foreman	Watermarked Image	2.20	49.49	0.99	158.72	3.99E+03	7.56
	Extracted Watermark	10.82	39.09	0.75	12.95	2.95E+03	2.79

As shown in Figure 4.2, the various images are generated during the watermarking process while applying the mentioned approach (3-level DWT-SVD) to different images/frames. Now, for each of these generated images, few parameters are calculated to identify and measure the effectiveness of the applied watermarking process.

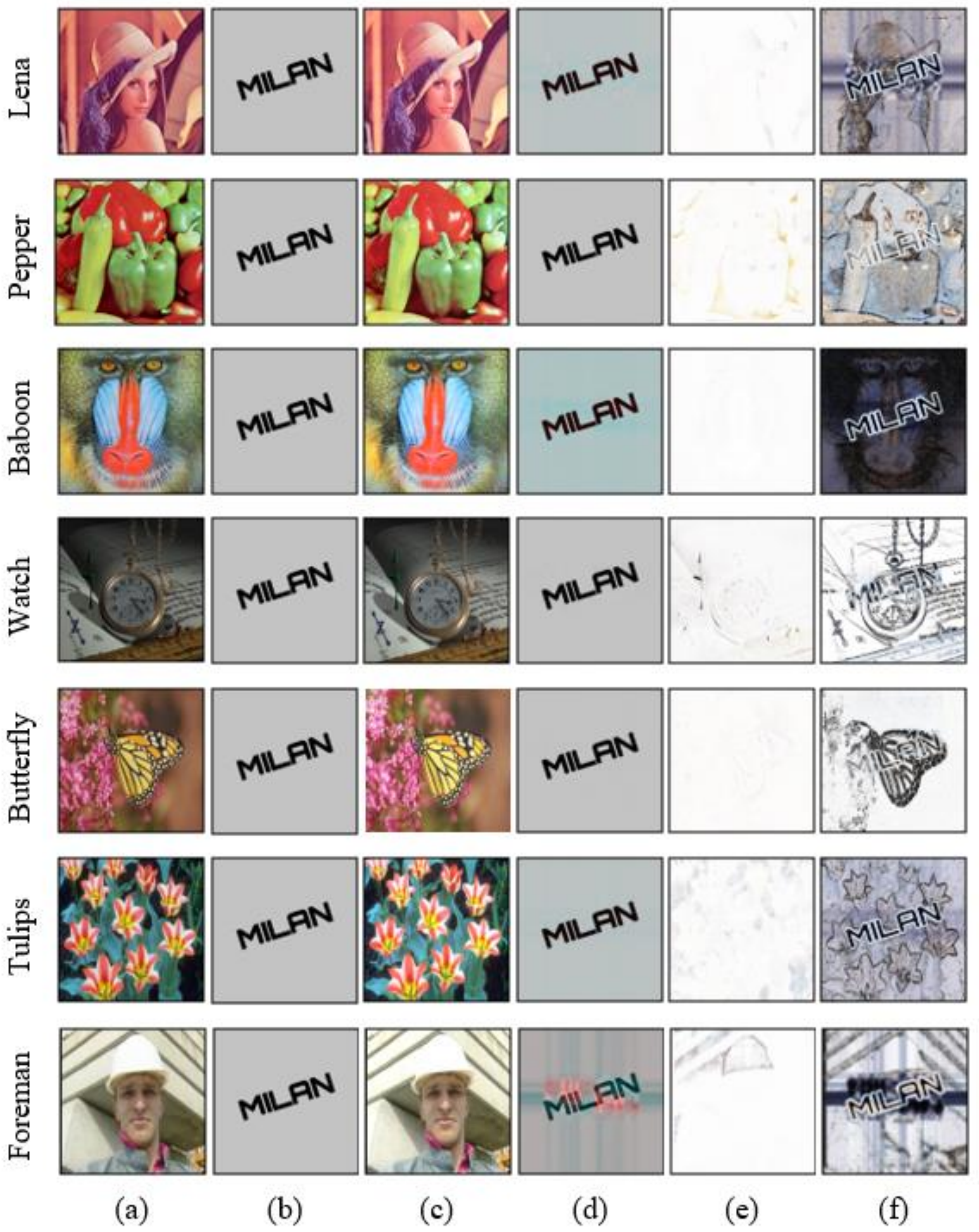


Figure 4.3 Watermarking images (a) cover images (b) watermark image_2 (c) watermarked images (d) extracted watermarks (e) SSIM for cover images / watermarked images (f) SSIM for extracted watermark

The performance of the watermark algorithm is evaluated based on various parameters like PSNR, MSE, Entropy, Mean, Variance, and SSIM. Table 4.1 shows the results for various parameters calculated for different images/ frames. The values of these parameters are calculated for the generated watermarked image and extracted watermark for each of the sample images/frames against watermark_1.

The Mean Square Error value for various images (including respective watermarked image and extracted watermark) is quite low while the respective Peak Signal to Noise Ratio is quite high. This shows the effectiveness and performance of the proposed approach with images of a given dataset against Watermark_1are good. The other performance parameters like Similarity Structure Index Measure for different images are quite high and approaching towards value 1, which indicates that the similarity of images before and after applying watermark remains intact with a given approach. Similarly, the values mentioned in Table 4.1 for Mean, Variance, and Entropy of different images signify the effectiveness and robustness of the proposed solution with a given dataset.

We have tried another watermark image (Watermark_2) on a similar set of images/frames and generated the respective watermarked images and extracted watermarks. In this way, we have tried the same approach with multiple watermarks to verify its behaviour and performance.

Thus, Figure 4.3 gives a comparative view of the same watermarking approach for a different watermark. Figure 4.3 shows the various images generated with Watermark_2 like these are generated earlier with Watermark_1.

Table 4.2 shows the parameters calculated for generated watermarked images and extracted watermark for each of the sample images/frames. These results are calculated for similar parameters of the same images/frames against Watermark_2 that were shown in Table 4.1 against Watermark_1. This provides a comparative view of both results with different watermarks.

In Table 4.2, we see that the Mean Square Error value (with watermark_2) is quite good as compare to the previous one(watermark_1), specifically for watermarked images while the same is not so good for extracted watermarks.

The peak signal to noise ratio (PSNR) is quite good which signifies the effectiveness of the proposed approach with watermark_2 as well. Similarly, the Structure Similarity Index and Entropy values are high and showing good results for all the images tried from the dataset against another watermark (Watermark_2).

Table 4.2: Results with watermarked images and extracted watermarks_2

Image	Parameters	MSE	PSNR	SSIM	Mean	Variance	Entropy
Lena	Watermarked Image	1.65	85.96	0.98	146.26	3.89E+03	7.69
	Extracted Watermark	44.31	42.49	0.59	182.32	1.56E+03	5.23
Pepper	Watermarked Image	0.72	76.95	0.97	128.75	4.97E+03	7.87
	Extracted Watermark	15.57	47.03	0.68	185.15	1.75E+03	4.82
Baboon	Watermarked Image	1.43	85.84	0.98	143.68	3.64E+03	7.61
	Extracted Watermark	98.04	38.86	0.20	178.56	1.80E+03	6.57
Watch	Watermarked Image	0.99	85.80	0.95	89.60	2.33E+03	7.40
	Extracted Watermark	10.45	53.53	0.83	184.71	1.70E+03	3.80
Butterfly	Watermarked Image	0.85	89.99	0.98	122.03	3.26E+03	7.62
	Extracted Watermark	11.04	50.28	0.83	184.72	1.71E+03	4.02
Tulips	Watermarked Image	0.75	81.12	0.96	119.13	5.63E+03	7.65
	Extracted Watermark	43.34	44.34	0.64	181.73	1.58E+03	5.01
Foreman	Watermarked Image	0.21	98.45	0.98	158.72	3.99E+03	7.18
	Extracted Watermark	13.23	37.90	0.67	185.06	1.73E+03	5.67

So, the low values of MSE and high values of PSNR, SSIM, and Entropy for the watermarked images indicate that the watermarks are embedded in the image without disturbing the overall appearance and quality of the images/frames. The same is true for the respective values obtained for the extracted watermark of each image/frame in both cases.

4.2 Evaluation with Videos

To apply the watermarking to complete video, the video is sub-divided into various frames and each frame will be treated as a single image. Various frames from the Foreman video are shown in Figure 4.4. Now, the same process of watermarking process is applied to all or selected frames of that video to apply the watermarking. Finally, all the generated watermarked frames are combined to have the watermarked video.

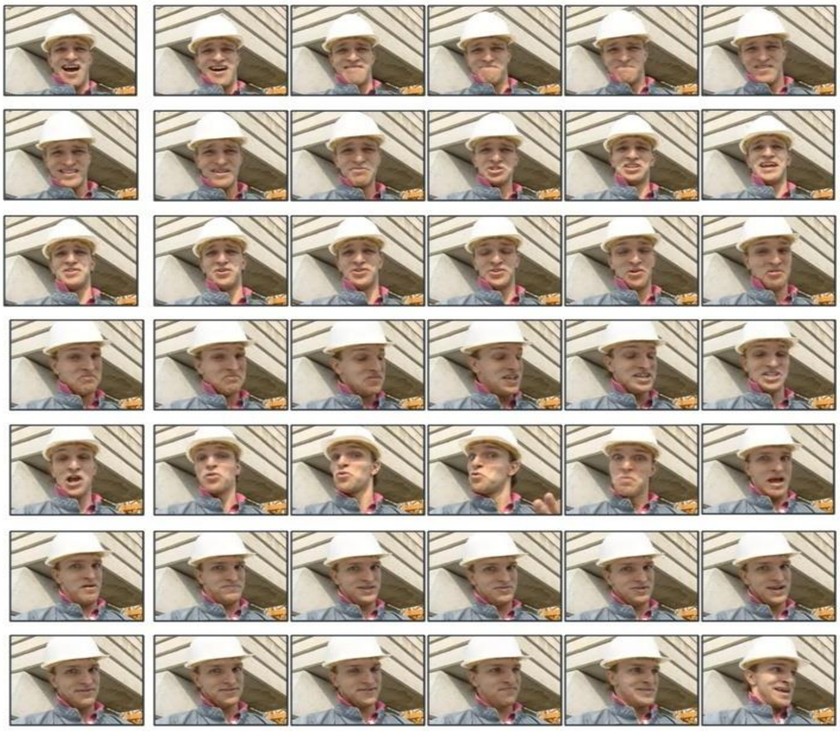


Figure 4.4 Frames dataset from a video (Foreman)

In order to calculate the effectiveness and success of the applied watermarking process, the parameters of the result are calculated against each frame of the video, as mentioned in the previous section. Finally, we have combined the parametric results of all frames/images to get the corresponding parameter result for the complete video.

Table 4.3: PSNR values for 90 watermarked frames (Video: Foreman)

Frames	**PSNRs**									
1 - 10	39.09	39.10	39.10	39.13	39.12	39.14	39.12	39.11	39.10	39.11
11 - 20	39.08	39.08	39.08	39.09	39.09	39.09	39.10	39.10	39.10	39.10
21 - 30	39.06	39.08	39.08	39.10	39.11	39.10	39.10	39.12	39.12	39.11
31 - 40	39.09	39.07	39.07	39.07	39.09	39.08	39.09	39.07	39.07	39.07
41 - 50	39.07	39.07	39.07	39.07	39.07	39.08	39.08	39.08	39.08	39.08
51 - 60	39.08	39.08	39.08	39.09	39.09	39.09	39.10	39.10	39.10	39.08
61 - 70	39.10	39.12	39.13	39.14	39.13	39.12	39.14	39.14	39.15	39.15
70 - 80	39.11	39.09	39.09	39.08	39.09	39.10	39.11	39.09	39.08	39.09
80 - 90	39.08	39.09	39.08	39.07	39.07	39.09	39.09	39.08	39.09	39.09
Average	**39.09**									

The Foreman video is partitioned into several frames and every frame is processed with the proposed watermarking process. Table 4.3 shows the PSNR values for various frames. Finally, we have calculated the average value of PSNR from all the frames to measure the PSNR value for watermarked video.

We have also measured other parameters like MSE and SSIM on the frames of video Foreman. These frames were processed with the proposed watermarking approach and respective values are shown in Table 4.4 and 4.5. Finally, we have calculated the average values of these parameters for watermarked video.

Table 4.4: MSE values for 90 watermarked frames (Video: Foreman)

Frames	**MSEs**									
1 – 10	11.11	11.12	11.12	11.16	11.14	11.16	11.14	11.13	11.12	11.13
11 - 20	11.09	11.09	11.13	11.11	11.13	11.11	11.12	11.13	11.13	11.12
21 - 30	11.14	11.14	11.16	11.14	11.13	11.12	11.12	11.13	11.13	11.13
31 - 40	11.11	11.17	11.17	11.17	11.13	11.16	11.16	11.16	11.14	11.16
41 - 50	11.09	11.13	11.14	11.15	11.18	11.15	11.18	11.2	11.18	11.19
51 - 60	11.16	11.18	11.18	11.18	11.16	11.18	11.19	11.18	11.16	11.16
61 - 70	11.15	11.14	11.13	11.13	11.13	11.14	11.15	11.15	11.16	11.16
70 - 80	11.15	11.16	11.14	11.13	11.16	11.14	11.13	11.14	11.13	11.14
80 - 90	11.12	11.12	11.12	11.12	11.12	11.12	11.14	11.16	11.16	11.16
Average	**11.14**									

Table 4.5: SSIM values for 90 watermarked frames (Video: Foreman)

Frames	**SSIMs**									
1 - 10	0.65	0.66	0.66	0.67	0.65	0.67	0.65	0.64	0.66	0.64
11 - 20	0.66	0.66	0.64	0.62	0.64	0.63	0.63	0.64	0.64	0.63
21 - 30	0.65	0.65	0.67	0.65	0.64	0.63	0.63	0.65	0.65	0.64
31 - 40	0.69	0.68	0.68	0.68	0.67	0.67	0.68	0.68	0.65	0.67
41 - 50	0.67	0.67	0.70	0.69	0.69	0.71	0.69	0.71	0.71	0.70
51 - 60	0.69	0.69	0.69	0.64	0.73	0.71	0.71	0.69	0.68	0.67
61 - 70	0.67	0.65	0.67	0.67	0.67	0.65	0.67	0.67	0.71	0.71
70 - 80	0.69	0.67	0.64	0.64	0.67	0.65	0.64	0.65	0.64	0.65
80 - 90	0.66	0.66	0.64	0.67	0.65	0.63	0.68	0.67	0.67	0.67
Average	**0.67**									

From Table 4.3, 4.4, and 4.5 we see that the average values of PSNR, MSE, and SSIM for a complete watermarked video are 39.09, 11.14, and 0.67 respectively. These values are quite good and ensuring the effectiveness of the applied approach for watermarking process.

We have applied the same approach to different videos that are present in the dataset mentioned in section 4.1. The various parameters (i.e., PSNR, MSE, and SSIM) measured for these watermarked videos are given in Table 4.6.

Table 4.6: PSNR, MSE, and SSIM values for Video Datasets

Dataset (Videos)	**PSNR**	**MSE**	**SSIM**
Beach (90 frames)	54.15	8.39	0.74
Multiple Scene Type (40 frames)	55.12	8.21	0.74
Different Times of Day (60 frames)	48.23	9.47	0.72
Plants and Butterfly (90 frames)	58.45	7.60	0.76
General Traffic (60 frames)	51.64	8.84	0.75

Each video is divided into a different number of frames, called frameset. The parameter values for each watermarked video are calculated by averaging the respective values for its frameset as we have done for the Foreman video.

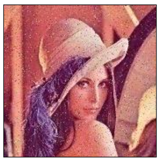
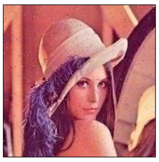
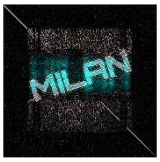
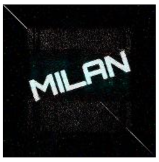
4.3 Evaluation with Attacks

In Section 4.1, we have generated watermarked images, extracted watermarks, and calculated the various parameters to measure the effectiveness of the applied process/approach. There was no modification/alteration involved in the watermarked image before extracting the watermark from it. It means, the previous results were calculated in an ideal condition, where no tempering/modification/attacks were attempted on generated watermarked.

There are several types of attacks that are implemented in a watermarked image before extracting the watermark out of it. The proposed approach is evaluated for this condition as well by applying several attacks on the watermarked image. The watermark is extracted post-attack(s) and result parameters are calculated to measure the performance of the applied process/approach as it is calculated in earlier cases.

- **Noise Attack:** Various signal processing operations to do the noise modifications/attacks (non-geometrical attacks) are implemented on the watermarked image of Lena. The attacks of Salt & Pepper (with var 0.05 and 0.01)are applied to evaluate the results of the proposed approach and it shows the respective PSNR and Normalized Correlation (NC) values for attacked watermarked image and the extracted watermark in Table 4.7 below:

Table 4.7: PSNR and NC results for Salt & Pepper attack

Attack	**Salt & Pepper (var = 0.05)**	**Salt & Pepper (var = 0.01)**
Attacked Frame	 (PSNR = 50.90)	 (PSNR = 52.23)
Extracted Watermark	 (PSNR = 48.90) (NC = 0.73)	 (PSNR = 49.44) (NC = 0.85)

The ***Gaussian*** attack with var 0.05 and 0.01 is also applied and it shows the attacked watermarked and extracted watermark along with the respective PSNR and NC values. The latter case giving better results as shown in Table 4.8.

Similarly, the *Speckle* attack is applied to the watermarked image with var 0.05 and 0.01. Table 4.9 shows the respective PSNR and NC values along with attacked watermarked and extracted watermark.

Table 4.8: PSNR and NC results for Gaussian attack

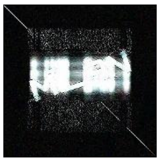
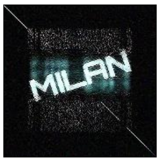
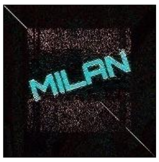
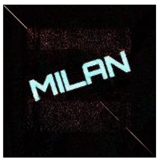
Attack	**Gaussian (var =0.05)**	**Gaussian (var =0.01)**
Attacked Frame	 (PSNR = 52.11)	 (PSNR = 53.217)
Extracted Watermark	 (PSNR = 48.92) (NC = 0.66)	 (PSNR = 52.68) (NC = 0.7)

Table 4.9: PSNR and NC results for speckle attack

Attack	**Speckle (var =0.05)**	**Speckle (var =0.01)**
Attacked Frame	 (PSNR = 48.15)	 (PSNR = 51.14)
Extracted Watermark	 (PSNR = 48.70) (NC = 0.85)	 (PSNR = 50.44) (NC = 0.91)

- **Rotate Attack:** The rotation attack is a geometric attack applied by moving/rotating the image clockwise/anti-clockwise to introduce modifications. The watermarked image of Lena is attacked with different angles and evaluated in each case. The extracted watermarks with respective PSNR and NC values are shown in Table 4.10.
- **Resize and Crop Attack:** Resize and crop attacks are also geometric attacks. The Resize attack is implemented by changing the size of the watermarked image and then restoring it to the same level. The Resize and Crop attacks were implemented on the watermarked image of Lena like other

attacks. The respective extracted watermarks and PSNR and NC values are given in Table 4.11.

Table 4.10: PSNR and NC results for rotation attack

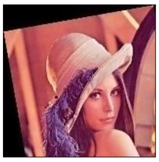
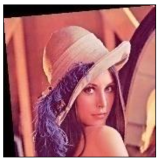
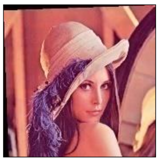
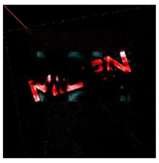
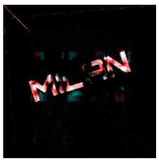
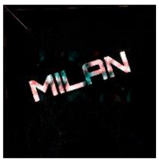
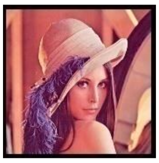
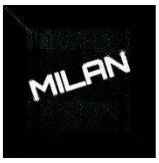
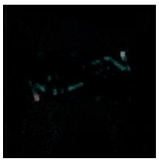
Attacks	**Rotate** **(10 degrees)**	**Rotate** **(5 degrees)**	**Rotate** **(2 degrees)**
Attacked Frame	 (PSNR = 49.34)	 (PSNR = 52.23)	 (PSNR = 53.45)
Extracted Watermark	 (PSNR = 48.11) (NC = 0.68)	 (PSNR = 48.50) (NC = 0.71)	 (PSNR = 48.72) (NC = 0.76)

Table 4.11: PSNR and NC results for resize and crop attack

Attack	**Resize** **(512 to 256 to 512)**	**Crop**
Attacked Frame	 (PSNR = 48.34)	 (PSNR = 45.33)
Extracted Watermark	 (PSNR = 51.83) (NC = 0.88)	 (PSNR = 15.58) (NC = 0.43)

The generated values of extracted watermark are very less in case of a Crop attack as compared to other attacks that are implemented on the watermarked image of Lena.

4.4 Results

The results of the proposed approach with the different datasets and attacks are shown in sections 4.1, 4.2, and Section 4.3. Now, we have used different datasets having multiple images and videos to apply to various approaches. These different datasets are verified/tested against already existing watermarking techniques (i.e., SVD, 2-DWT). The same datasets were used against our proposed approach (3-level DWT-SVD) and a combination of this approach with the digital signature (i.e., 3-level DWT-SVD using Digital Signature).

Table 4.12: Results classification comparison with PSNR, MSE, and SSIM (watermarked image/video)

Dataset (Image/Video)		**Existing Approach (SVD, 2-DWT)**			**Our Approach (3-level DWT-SVD)**			**Our approach with Digital Signature (3-level DWT-SVD using Digital Signature)**		
		PSNR	MSE	SSIM	PSNR	MSE	SSIM	PSNR	MSE	SSIM
Images	Lena	40.12	44.87	0.51	42.49	44.31	0.59	42.28	44.40	0.53
	Pepper	45.57	15.91	0.59	47.03	15.57	0.68	46.97	15.79	0.62
	Baboon	35.86	98.71	0.18	38.86	98.04	0.20	39.31	97.29	0.27
	Watch	51.17	12.14	0.72	53.53	10.45	0.83	53.28	10.53	0.79
	Butterfly	47.83	12.44	0.72	50.28	11.04	0.83	50.58	10.91	0.87
	Tulips	43.74	44.17	0.61	44.34	43.34	0.64	42.62	44.97	0.59
Videos	Foreman	37.12	11.45	0.61	39.09	11.14	0.67	38.19	10.87	0.69
	Beach	52.10	9.15	0.65	54.15	8.39	0.73	52.83	8.95	0.71
	Multiple Scene Type	53.12	9.18	0.65	55.12	8.21	0.74	53.26	8.81	0.70
	Different Times of Day	45.54	8.84	0.69	48.23	9.47	0.72	43.89	9.95	0.69
	Plants and Butterfly	56.54	8.10	0.71	58.45	7.55	0.76	57.16	7.60	0.76
	General Traffic	48.15	10.07	0.66	51.64	8.84	0.75	46.37	8.53	0.72
Average		**46.41**	**23.75**	**0.61**	**48.60**	**23.03**	**0.68**	**47.23**	**23.22**	**0.66**

The average PSNR, MSE, and SSIM values for different datasets were calculated for watermarked images/videos against each of these three approaches. Table 4.12 represents the result classification of PSNR, MSE, and SSIM values for watermarked images/videos with different approaches.

The existing approach has used a 2-level DWT technique for the watermarking process while the proposed approach (3-level DWT-SVD) has used slightly different ways with 3-level DWT for various videos and its frames to perform the video watermarking. Table 4.12 shows that the results of the proposed approach (3-level DWT-SVD) are much better than the existing approach for PSNR, MSE, and SSIM values calculated for different datasets of images and videos. The overall average results of all the datasets for all three parameters with the proposed approach are better than the existing approach.

Similarly, when we have tried our approach combined with the digital signature (i.e., 3-level DWT-SVD using Digital Signature), we have calculated the average PSNR, MSE, and SSIM values for each dataset which is having mixed results as compared to the existing approach. In some cases, it has performed better than the existing approach and, in some cases, it hasn't. We have applied digital signatures to achieve more security, privacy, and authenticity which compromised a little on parameter values for few datasets depending upon the nature of videos and images present in them.

Overall, we have seen that the proposed approach (3-level DWT-SVD) has performed better for the watermarking process and when it is combined with the digital signature (i.e., 3-level DWT-SVD using Digital Signature) it has performed well by ensuring more privacy, security, and authenticity as compared to the existing approach (SVD, 2-DWT).

Chapter 5
Conclusion and Future Work

This is the last chapter of the thesis. In Section 5.1, we have explained the evaluation of the research methodology used. In Section 5.2, we have dealt with the significance of the work done in this thesis. The conclusion of the thesis is described in Section 5.3 and finally, this thesis will be closed in Section 5.4 with the vision of our future research work.

5.1 Evaluation of Research Methodology

In this thesis, we have investigated and applied a little different way of watermarking process for videos by using the Decomposition of Singular Value (SVD) and Discrete Wavelet Transform (DWT) techniques. Videos are segmented into various frames and 3-level discrete wavelet transformation is applied with SVD. We have combined this approach with hashing and digital signature techniques as well. As we know most of the previously existing approaches and ways of the watermarking process are based on images only and not using digital signatures as a watermark, we have shown how the digital signatures can be used as a watermark along with the 3-level wavelet and SVD methods. In particular, the use of hashing and digital signature as a watermark resolved the issue of achieving a high level of security, privacy, and authenticity. Therefore, the research question "is it really possible to achieve a high level of privacy, security, and authenticity with video watermarking?" has been answered up to some extent.

5.2 Significance

This thesis has contributed in a significant way by showing how we have achieved a more robust watermarking process by using SVD and 3-level of wavelets in the DWT method. Using deeper level wavelets is important to achieve robustness in video watermarking. Also, making use of hashing and the digital signature is quite impressive and significant in the video watermarking process. We have improvised this approach of video watermarking by using the digital signature itself as a watermark. This idea of using a digital signature as a watermark helps to achieve more security, authenticity, and privacy in the process while robustness is already present with different levels of wavelet approach. The two significant contributions of these proposed approaches are:

- Increased robustness with 3-level DWT techniques for video watermarking.

- A high level of security, privacy, authenticity, and ownership are achieved in video watermarking with hashing and digital signature.

5.3 Conclusion

The method of embedding copyright information into a video bit stream is well known as video watermarking. In recent years, it had been suggested that the issue of illicit exploitation and dissemination of digital video should be solved. A robust, efficient, secure, and imperceptible video watermarking algorithm for copyright protection has been proposed in this thesis.

The algorithmic solution of this thesis is based on cascading the two efficient mathematical transforms; the SVD and3-level DWT. These two different techniques of transform domain show a high degree of complementary and we could achieve different levels of robustness by their combination against the same attack. Also, the use of hashing and digital signature as a watermark took it one level further to attain security, authenticity, and privacy.

The proposed approaches are verified with different datasets and several attacks are implemented on the watermarked videos/images. The respective results are explained with various benchmarking parameters. The corresponding result comparison is also carried for different proposed and existing approaches.

5.4 Future Work

In this section, we discuss future work and the areas that are not covered in the proposed solution. There are some limitations in the given approach which provides the scope of future work as a continuation of this work. The techniques and approaches used in this solution can be improvised or extended further to achieve more robustness, speed, and to cover different types of images and videos.

The use of binary images like QR codes doesn’t go well with the provided approach. The binary images do not use the concept of RGB so the given approach can be taken as a base and modified or improvised further to incorporate watermarking for binary images as well.

The proposed approaches use3-level Discrete Wavelet Transform (DWT), Decomposition of Singular Value (SVD), and Least Significant Bit (LSB). So, there is a possibility that one can use the frequency domain techniques like Discrete Cosine Transform **(**DCS) and Discrete Fourier Transform (DFT) during the watermark embedding process.

Also, the evaluation or benchmarking of the watermarking process is done based on various parameters like PSNR, MSE, SSIM, Variance, Entropy, etc in the given solution. The same can be extended to cover the evaluation on distributions which can give more accurate/close results and provide coverage over a wide range of parameters.

References

Abdallah, H.A., Ghazy, R.A., Kasban, H., Faragallah, O.S., Shaalan, A.A., & Hadhoud,M.M.(2014). Homomorphic image watermarking with a singular value decomposition algorithm. *Information Processing and Management,*50(6), pp. 909–923

Abdulrahman, A., & Öztürk, S. (2018). A novel hybrid DCT and DWT based robust watermarking algorithm for color images. *Multimedia Tools and Applications,* 78, pp. 17027-17049.

Abinaya, A., Manisha, M., Priyanga, A., Prasanna, M., & Gunasekaran, R. (2017). Data hiding in encrypted images secured image watermarking system for image ownership.*International Journal of Computer Trends and Technology (IJCTT),*pp. 40-44

Ahuja, R., & Bedi, S.S. (2015). All aspects of digital video watermarking under an umbrella. *International Journal of Image, Graphics, and Signal Processing,* (12), pp. 54-73

Adegboye, M.A., Ajao, L.A., & Badmus, T.A. (2019). Performanceevaluation of multiple transform watermarking system for privacy protection of medical data using PSNR and NC.*Acta Electrotechnica et Informatica,* 18(4), pp. 44–51

Akter, A., Tajnina, N.E., & Ullah, M.A. (2014). Digital image watermarking based on DWT-DCT: Evaluate for a new embedding algorithm. *National Conference on Informatics, Electronics & Vision (ICIEV),* pp. 1-6

Ali, Z., Imran, M., Alsulaiman, M., Zia, T., & Shoaib, M. (2018). A zero-watermarking algorithm for privacy protection in biomedical signals. *Future Generation Computer Systems (FGCS),* 82, pp. 290-303

Alizai, Z.A., Tareen, N.F., & Jadoon, I. (2018). Improved IoT device authentication scheme using device capability and digital signatures. *International Conference on Applied and Engineering Mathematics (ICAEM),* pp. 1-5

Al-Gahtani, H.B., & Al-Daraiseh,A.A. (2015). Developing an efficient digital image watermarking for smartphones.*IEEE Applications and Networking Symposium (WSWAN)*,pp.1-6

Ananthapraba, B., & Thyagarajan, K. (2019). Medical image privacy using watermarking techniques. *International Journal of Scientific Research & Communications (IJSRC),* 5(5), pp. 235-248

Arpana, J.R., & Ayyappan, S. (2015). Image watermarking using Diffie-Hellman key exchange algorithm.*International Conference on Information and Communication Technologies (ICICT),* 46, pp. 1684-1691

Arya, R.K., Singh, S., & Saharan, R. (2015). A secure non-blind block-based digital image watermarking technique using DWT and DCT. *IEEE Advances in Computing, Communications and Informatics international Conference (ICACCI),* pp. 2042-2048

Asikuzzaman, M., & Pickering, M.R. (2018). An overview of digital video watermarking. *IEEE Transactions on Circuits and Systems for Video Technology*, 28(9), pp. 2131-2153

Asikuzzaman, M.,Alam, M.J., & Pickering, M.R. (2015). Blind and robust video watermarking scheme in the DT CWT and SVD domain.*IEEE Picture Coding Symposium (PCS),* pp. 277-281

Benoraira, A., Benmahammed, K., & Boucenna, N. (2015). Blind image watermarking technique based on differential embedding in DWT and DCT domains.*EURASIP Journal on Advances in Signal Processing*,pp. 1-11

Bamane, N., & Patil, S. (2013). Comparison & performance analysis of different digital video watermarking techniques. *International Journal of Scientific & Engineering Research,* 4(1), pp. 1-6

Bansal, M., Yan, W., Kankanhalli, M. (2003) Dynamic watermarking of images.Pacific Rim Conference on Multimedia.

Bansal, N.,Deolia, V.K., Bansal, A., & Pathak, P. (2015). Comparative analysis of LSB, DCT, and DWT for digital watermarking.*IEEE Computing for Sustainable Global Development (INDIACom)*, pp. 40-45

Bassel, A., Nordin, M.J., & Abdulkareem, M.B. (2017). An improved robust image watermarking scheme based on the singular value decomposition and genetic algorithm. *International Visual Informatics Conference (IVIC),* pp. 702-713

Bayoudh, I., Jabra, S.B., & Zagrouba, E. (2017). A robust video watermarking for real-time application. *International Conference on Advanced Concepts for Intelligent Vision Systems (ACIVS),* 77, pp. 493-504

Begum, M., & Uddin, M. (2020). Digital image watermarking techniques: A review. *Information - Open Access Journal,* 11(2), pp.110

Bhadra,J.,Banga, M.K., & Murthy, M. (2017). Securing data using elliptic curve cryptography and least significant bit steganography.*International Conference on Smart Technology for Smart Nation*,pp. 1460-1466

Bhandari, A., Bhuiyan, M., & Prasad,P.W.C.(2017). Enhancement of MD5 algorithm for secured web development.*Journal of Software,* 12(4), pp. 240-252

Bhardwaj, A., & Khuteta, A. (2017). Digital video watermarking techniques: A review. *International Journal of Engineering and Computer Science,* 4(3), pp. 21328-21332

Bouridane. A., & Ibrahim, M.K. (2013). Digital image watermarking using balanced multiwavelets. *IEEE Transactions on Signal Processing,* pp. 1519-1536

Bt, A., Zamani, M., Kohpayeh, S., & Koohpayeh, T. (2015). A survey on digital image watermarking techniques in spatial and transform domains. *International Conference on Advances in Computing, Control, and Networking - ACCN 2015,* pp. 89-93

Buhari, A.M., Ling, H.C.,Baskaran, V.M., & Wong, K. (2016). Fast watermarking scheme for real-time spatial scalable video coding. *Signal Processing: Image Communication,* 47, pp. 86–95

Cai, C.T., Feng, G., Wang, C., & Han, X. (2017). A reversible watermarking algorithm for high-efficiency video coding. *International Congress on Image and Signal Processing, BioMedical Engineering and Informatics, Shanghai, China,* pp. 1-6

Chandran, S., & Bhattacharya, K. (2015). Performance analysis of LSB, DCT, and DWT for a digital watermarking application using steganography. *IEEE Electrical, Electronics, Signals, Communication and Optimization Conference (EESCO),* pp. 1-5

Chang, P.C., Chung, K.L., Chen, J.J., Lin, C.H., & Lin, T.J. (2014). A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames. *Journal of Visual Communication and Image Representation,* 25(2), pp. 239-253

Chaudhary, D., & Sharma, P. (2018). Digital video watermarking scheme using wavelets with MATLAB. *International Journal of Computer Applications,* 180(14), pp. 30-34

Chawla, N. (2018). A novel video watermarking scheme based on DWT and PCA. *International Journal of Engineering and Advanced Technology (IJEAT),* 7(5), pp. 62-68

Chen, W., Shahid, Z., Stutz, T., Autrusseau, F., & Callet, P.L. (2014). Robust drift-free bit-rate preserving H.264 watermarking. *Multimedia Systems,* pp. 179-193

Cheng, W., & Li, Z.D. (2016). Robust watermarking algorithm of color image based on DWT-DCT and chaotic system. *IEEE International Conference on Computer Communication and the Internet,* pp. 370–373

Chidambaram, N., Reddy, K.S.H., Varma, K.V., Dheeraj, K.J.S., Reddy, A.S., & Rengarajan, A. (2020). Tamper detection of medical images using a modified hashing algorithm. *International Conference on Intelligent Computing, Information and Control Systems (ICICCS),* pp. 491-498

Chopra, A., Gupta, S., & Dhal, S. (2019). Analysis of frequency-domain watermarking techniques in presence of geometric and simple attacks. *Multimedia Tools and Applications,* 79, pp. 501-554

Dhoka, M.S., & Kadam, J. (2014). Digital watermarking for medical images using biorthogonal wavelet filters and transformed watermark embedding. *International Journal of Advanced Computer Research (IJACR),* 4 (2), pp. 705

Ding, W., Yan, W., Qi, D. (2001)Digital image scrambling. *Progress in Natural Science*, 11(6), 454-460

Ding, W., Yan, W., Qi, D. (2002) Digital image watermarking based on discrete wavelet transform. *Journal of Computer Science and Technology,* 17(2): 129-139 (2002)

Dixit, A., & Dixit, R. (2017). A review of digital image watermarking techniques. *International Journal of Image, Graphics and Signal Processing,* 9(4), pp. 56-66

Dutta, T., Gupta, H.P. (2017). An efficient framework for compressed domain watermarking in P frames of high-efficiency video coding (HEVC) - encoded video.*ACM Transactions onMultimedia Computing, Communications, and Applications,* 13, pp. 12

Dutta, T., & Gupta, H.P. (2016). A robust watermarking framework for high-efficiency video coding (HEVC) - Encoded video with blind extraction process. *Journal of Visual Communication and Image Representation (JVCIR),* 38, pp. 29-44

Elrowayati, A.A., Abdullah, M.F.L., Manaf, A.A., & Alfagi, A.S. (2016). Robust HEVC video watermarking scheme based on the repetition-BCH syndrome code. *International Journal of Software Engineering and its Applications,*10, pp. 263-270

Emad, E., Safe, A., Refaat, A., Osama, Z., Sayed,E., & Mohamed, E. (2018).A secure image steganography algorithm based on least significantbit and integer wavelettransform.*Journal of Systems Engineering and Electronics,* 29(3), pp. 639-649

Fazli,S., & Moeini, M. (2016). A robust image watermarking method based on DWT, DCT, and SVD usinga new technique for correction of main geometricattacks. *Optik,*127(2), pp. 964–972

Fallahpour, M., Shirmohammadi, S., & Ghanbari, M. (2015). A high capacity data hiding algorithm for H.264/AVC video. *Security and Communication Networks,* (8), pp. 2947–2955

Faragallah, O.S. (2013). Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain. *AEU - International Journal of Electronics and Communications,*67, pp.189-196

FathimaNasreen, K., & Chitra, P. (2016). A robust encryption and digital watermarking scheme for dicom images using quaternion and DWT-SVD. *International Conference on Green Engineering and Technologies (IC-GET),*pp. 1-6

Favorskaya, M.N., & Buryachenko, V.V. (2020). Detecting relevant regions for watermark embedding in video sequences based on deep learning. *International Conference on Intelligent Decision Technologies,*pp. 129-139

Favorskaya, M.N., & Savchina, E. (2017). Content preserving watermarking for medical images using shearlettransform and SVD. *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences (ISPRS),* pp. 101-108

Feng, L., Yan, W. (2014) Visual Cryptography for Image Processing and Security Theory, Methods, and Applications. Springer International.

Gaj, S., Kanetkar, A., Sur, A., & Bora, P.K. (2017). Drift-compensated robust watermarking algorithm for H.265/HEVC video stream. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 13, pp. 11

Gaj, S., Patel, A.S., & Sur, A. (2016). Object-based watermarking for H.264/AVC video resistant to RST attacks. *Multimedia Tools and Applications*, 75, pp. 3053-3080

Gaj, S., Rathore, A.K., Sur, A., & Bora, P.K. (2017). A robust watermarking scheme against frame blending and projection attacks. *Multimedia Tools and Applications*, 76, pp. 20755–20779

Gaj, S., Sur, A., & Bora, P.K. (2015). A robust watermarking scheme against re-compression attack for H.265/HEVC. *In Proceedings of the 5th National Conference on Computer Vision, Pattern Recognition, Image Processing, and Graphics, Patna, India*, pp. 1-4

Gaur,R.,Vig, R., & Kaur, A. (2018). An effectual hybrid approach using data encryption standard (DES) and secured hash algorithm (SHA) for image steganography.*International Journal on Recent and Innovation Trends in Computing and Communication*, 6(5), pp. 44-53

Geetamma, T., & Raju, K.P. (2013). Multiresolution scene based digital video watermarking.*International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA)*, pp. 659-666

Geiger, C. (2019). Measurement of digital watermarking for automated test system data integrity. *IEEEInternational Workshop on Metrology for AeroSpace (MetroAeroSpace)*, pp. 17-21

Ghalejughi, M., & Akhaee, M.A. (2016). Video watermarking in the DT-DWT domain using hyperbolic function. *International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*,pp. 97-100

Goel, B., & Agarwal, C. (2013). An optimized un-compressed video watermarking scheme based on SVD and DWT. *International Conference on Contemporary Computing (IC3)*, pp. 307-312

Goldwasser, S., & Micali, S. (2019). Providing sound foundations for cryptography. *ACM Books*, pp. 411–496

Gosavi, C.S., & Mali, S.N. (2014). Frame selection for video watermark embedding using scene change detection algorithm. *International Journal of Electronics Communication and Computer Engineering,* 5(4), pp.162-164

Gujjunoori, S., & Amberker, B.B. (2013). DCT based reversible data embedding for MPEG-4 video using HVS characteristics.*Journal of Information Security and Applications,* (8), pp. 157–166

Gupta, A., Verma, H.K., & Gupta, S. (2013). A hybrid framework for registration of carotid ultrasound images combining iconic and geometric features. *Medical & Biological Engineering & Computing,* 51, pp. 1043-1050

Gul, E., & Öztürk, S. (2018). A novel hash function based fragile watermarking method for image integrity. *Multimedia Tools and Applications*, pp. 1-18

Gupta, G., Gupta, V.K., & Chandra, M. (2018). An efficient video watermarking -based security model. *Microsystem Technologies,* 24, pp. 2539-2548

Gupta, Y., & Tiwari, N. (2017). A robust technique for digital watermarking using 3-DWTSVD and pattern recognition neural network. *IOSR Journal of Computer Engineering,* 19, pp. 23-29

Hakim, S., & Fouad,M.(2017). Improving data integrity in communication systems by designing a new security hash algorithm. *Journal of Information Sciences and Computing Technologies(JISCT),* 6(2), pp. 638-647

Han, L., Zhou, G.Y., Xu, L., & Fang, L. (2017). Beyond SIFT using binary features in loop closure detection.*IEEE International Conference on Intelligent Robots and Systems,* pp. 4057–4063

Han, Y., He, W., Ji, S., & Luo, Q. (2014). A digital watermarking algorithm of color image based on visual cryptography and discrete cosine transform. *IEEE P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC),* pp. 525-530

Hannoun, K., Hamiche, H., Lahdir, M., Laghrouche, M., & Kassim, S. (2018). A novel DWT domain watermarking scheme based on a discrete-time chaotic system. *InternationalFederation of Accountants (IFAC),* 51, pp. 50-55

Harahap, M.K., & Khairina, N.(2020). Dynamic steganography least significant bit with stretch on pixels neighborhood. *Journal of Information Systems Engineering and Business Intelligence,*6(2), pp. 151-158

He, Y.L., Yang, G.B., & Zhu, N.B. (2012). A real-time dual watermarking algorithm of H.264/AVC video stream for video-on-demand service. *AEU-International Journal of Electronics and Communications,*66, pp. 305-312

Himeur, Y., & Boukabou,A. (2018).A robust and secure key-frames based video watermarking system using chaotic encryption. *Multimedia Tools and Applications,*77, pp. 8603–8627

Hsu, C., & Tu, S. (2019). Digital watermarking scheme for copyright protection and tampering detection. *International Journal on Information Technologies & Security (IJITS),* 11, pp. 110-117

Husain, F. (2012). A survey of digital watermarking techniques for multimedia data. *International Journal of Electronics and Communication Engineering, 2(1),* pp. 37-43

Hussein, N.H. (2015). Digital image authentication algorithm based on fragile invisible watermark and MD-5 function in the DWT domain. *The Journal of Engineering,* 21, pp. 21-41

Ibrahim, M., Kader, N.S.A., & Zorkany,M. (2014). Video multiple watermarking technique based on image interlacing using DWT. *The Scientific World Journal,* Article ID 634828, pp. 1-12

Jacob, M., & Mitra, S. (2015). Video watermarking techniques.*International Journal of Recent Technology and Engineering (IJRTE),* 4, pp. 1-4

Jain, P., & Ghanekar, U. (2018). Robust watermarking technique for textured images. *Procedia Computer Science,* 125, pp. 179-186

Jianfeng, L., Wang, M., Junping, D., Huang, Q., Li, L., & Chang, C.C. (2015). Multiple watermark scheme based on DWT-DCT quantization for medical images. *Journal of Information Hiding and Multimedia Signal Processing,* 6(3), pp. 458-72

Jiang, B., Yang, G., & Chen, W. (2015) A cabac based HEVC video steganography algorithm without bitrate increase. *Journal of Computer Information Systems,*11(6), pp. 2121–2130

Jiang, D.Y., Li, D., & Kim, J.W. (2015). A spread spectrum zero video watermarking scheme based on dual transform domains and log-polar transformation. *International Journal of Multimedia and Ubiquitous Engineering,* 10, pp. 367–378

Joshi, A.M., Gupta, S., Girdhar, M., Agarwal, P., & Sarker, R. (2016). Combined DWT-DCT-based video watermarking algorithm using Arnold transform technique. *International Conference on Data Engineering and Communication Technology, India,* pp. 455-463

Joshi, A.M., Mishra, V., & Patrikar, R.M. (2015). Design of real-time video watermarking based on integer DCT for H.264 encoder. *International Journal of Electronics,* 102, pp.141-155

Kang, Q., Li, K., & Chen, H. (2014). An SVD-based fragile watermarking scheme with grouped blocks.*International Conference on Information Technology and Electronic Commerce (ICITEC),* pp. 172-179

Kashyap, N. (2012). Image watermarking using a 3-level discrete wavelet transform (DWT). *I.J. Modern Education and Computer Science,* 3, pp. 50-56

Kaur, H. (2013). Study on audio and video watermarking. *International Journal of Communication Network Security,* 2(1), pp. 34-38

Kaur, K., Gupta, I., & Singh, A. (2019). Digital image watermarking using (2, 2) visual cryptography with DWT-SVD based watermarking.*Computational Intelligence in Data Mining,* pp. 77-86

Kaur, M., Jindal, S., & Behal, S. (2012). A study of digital image watermarking. *International Journal of Research in Engineering and Applied Sciences*, 2, pp. 127-134

Kaur, R., & Jindal, S. (2014). Robust digital image watermarking in high-frequency band using median filter function based on DWT- SVD.*IEEE Advanced Computing & Communication Technologies International Conference*, pp. 47-52

Kaur, R., & Jindal, S. (2013). Semi-blind image watermarking using a high-frequency band based on DWT-SVD. *In International Conference on Emerging Trends in Engineering and Technology,* pp. 19-24

Kaur, P., & Laxmi, V. (2014). An upgraded approach for robust video watermarking technique using Stephens algorithm. *International Journal of Computer Science and Mobile Computing (IJCSMC),*3(11), pp. 612–622

Kavadia, C., & Shrivastava V. (2012). A literature review on watermarking techniques. *International Journal of Scientific Engineering and Technology,* 1(4), pp. 08-11

Kekre, H.B.,Sarode, T., & Natu, S. (2015).Robust watermarking by SVD of watermark embedded in DKT-DCT and DCT wavelet column transform of host image.*IEEE Communication, Information & Computing Technology International Conference (ICCICT),*pp.1-6

Kerbiche, A., Jabra, S.B., Zagrouba, E., & Charvillat, V. (2018). A robust video watermarking based on feature regions and crowdsourcing. *Multimedia Tools and Applications,*77, pp. 26769–26791

Khairina, N., Harahap, M.K., & Lubis, J.H. (2018). The authenticity of image using hash MD5 and steganography least significant bit.*International Journal of Information System & Technology,* 2(1), pp. 1-6

Khalilian, H., & Bajic, I.V. (2013). Video watermarking with empirical PCA-based decoding. *IEEE Transactions on Image Processing,* 22, pp. 4825–4840

Khan, A., Siddiqa, A., Munib, S., & Malik, S.A. (2014). A recent survey of reversible watermarking techniques.*Information Sciences,* 279, pp. 251-272

Khan, M., Kushwaha, A., & Verma, T. (2015). A new digital image watermarking algorithm.*IEEE Industrial Instrumentation and Control International Conference,* pp. 885-890

Khan, S., Wahid, M., Khan, T., Ahmad, N., & Zafar, M.H. (2018). Column level image authentication technique using hidden digital signatures.*International Conference on Automation and Computing (ICAC),* pp. 1-6

Klim, S.M. (2017). Selected least significant bit approach for hiding information inside colorimage steganography by using magic square. *Journal of Engineering and Sustainable Development,* 21(1), pp. 74-88

Ko, C.C., Kuo, Y.L., Hsu, J.M., & Yang, B.Z. (2013). A multiresolution video watermarking scheme integrated with feature detection.*Journal of the Chinese Institute of Engineers,* 36(7), pp. 878-889

Kothari, A.M., & Dwivedi, V.V. (2012), Transform domain video watermarking: Design, implementation, and performance analysis. *International Conference on Communication Systems and Network Technologies,* pp. 133-137

Krishna, S.K., & Vinod, G.V. (2018). Performance evaluation of video watermarking. *International Journal of Engineering Sciences & Research Technology,* 7(4), pp. 279-284

Kumar, S., Yadav, A.K., Gupta, A., & Kumar, P. (2015). RGB image steganography on multiple frame video using LSB technique.*International Conference on Computer and Computational Sciences (ICCCS),* pp. 226-231

Kumar, P., & Sharma, A.K. (2019). A robust digital image watermarking technique against geometrical attacks using support vector machine and glow worm optimization. *International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI),* pp. 733-747

Kumar, S. (2015). A comparative study of transform based on secure image steganography. *International Journal of Computer and Communication Engineering,* 4(2), pp. 107-116

Kumar, S., Singh, B., & Yadav, M. (2020). A recent survey on multimedia and database watermarking. *Multimedia Tools and Applications,* pp. 1-49

Kunhu, A., Nisi, K., Sabnam, S., Majida, A., & Al-Mansoori, S. (2016). Index mapping-based hybrid DWT-DCT watermarking technique for copyright protection of videos files. *International Conference on Green Engineering and Technologies, Coimbatore, India,* pp. 1-6

Shukla, D., & Sharma, M. (2018). Robust scene-based digital video watermarking scheme using level-3 DWT: Approach, evaluation, and experimentation.*RadioElectronics and Communications Systems,* 61, pp. 1-12

Kunhu, A., Al-Ahmad, H., & Taher, F. (2017). Medical images protection and authentication using hybrid DWT-DCT and SHA256-MD5 hash functions. *IEEE International Conference on Electronics, Circuits, and Systems (ICECS),* pp. 397-400

Kunhu, A., Taher, F., & Al-Ahmad, H. (2015). A new multi watermarking algorithm for medical images using DWT and hash functions. *International Conference on Innovations in Information Technology (IIT),* pp. 230-234

Leelavathy, N., Prasad, E.V., & Kumar, S. (2012). A scene-based video watermarking in discrete multiwavelet domain. *International Journal of Multidisciplinary Sciences and Engineering,* 3(7), pp. 12-16

Li, J., Liu, H.M., Huang, J.W., & Shi, Y.Q. (2012). Reference index-based H.264 video watermarking scheme.*ACM Transactions on Multimedia Computing, Communications, and Applications,*8, pp. 33

Li, J.F., Wang, Y.B., & Dong, S.S. (2017). Video watermarking algorithm-based DC coefficient.*International Conference on Image, Vision, and Computing, Chengdu, China*, pp. 454-458

Li, H., Li, Z., Du, Z., & Wang, Q. (2016). Digital image watermarking algorithm using the intermediate frequency. *Telecommunication Computing Electronics and Control (TELKOMNIKA),* 14, pp.1424-1431

Ling, H., Feng, H., Zou, F., Yan, W., Lu, Z. (2010)A novel collusion attack strategy for digital fingerprinting International Workshop on Digital Watermarking, pp.224-238.

Li´skiewicz, M., Reischuk, R., & Wölfel, U. (2017). Security levels in steganography insecurity does not imply detectability.*Theoretical Computer Science,* pp. 1-15

Liu, Y.X., Liu, S.Y., Zhao, H.G., Liu, S., & Feng, C.A. (2017). Data hiding method for H.265 without intra-frame distortion drift.*International Conference on Intelligent Computing, Liverpool, UK,* pp. 642-650

Liu, Y.X., Liu, S.Y., Zhao, H.G., & Liu, S. A. (2018). New data hiding method for H.265/HEVC video streams without intra-frame distortion drift. *Multimedia Tools and Applications*, 14, pp. 94

Liu, J., Li, J., Chen, J., Zou, X., & Cheng, J. (2018). Medical image watermarking based on SIFT-DCT perceptual hashing. *International Confederation of Contamination Control Societies (ICCCS),* pp. 334-345

Liu, J. (2018). An image watermarking algorithm based on energy scheme in the wavelet transform domain. *IEEEInternational Conference on Image, Vision, and Computing (ICIVC),* pp. 668-672

Long, M., Peng, F., Li, H.Y. (2018). Separable reversible data hiding and encryption for HEVC video. *Journal of Real-Time Image Processing,*14, pp. 171-182

Maheshwari, J.P., Kumar, M., Mathur, G., Yadav, R., & Kakerda, R.K. (2015). Robust digital image watermarking using DCT based pyramid transform via image compression. *International Conference on Communications and Signal Processing (ICCSP),* pp. 1059-1063

Makbol, N.M., & Khoo, B.E. (2014). A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. *Digital Signal Processing,* 33, pp. 134-147

Mander,K., & Jindal, H. (2017). An improved image compression-decompression technique using block truncation and wavelets.*International Journal of Image, Graphics and Signal Processing(IJIGSP),* 9(8), pp.17-29

Mane, G. V., & Chiddarwar, G. (2013). Review paper on video watermarking techniques. *International Journal of Scientific and Research,* 3(4), pp. 1-5

Mehto, A., & Mehra, N. (2016). Adaptive lossless medical image watermarking algorithm based on DCT & DWT. *Procedia Computer Science,* 78, pp. 88-94

Mishra, A., Agarwal, C., Sharma, A., & Bedi, P. (2014) Optimized gray-scale image watermarking using DWT–SVD and firefly algorithm. *Expert System and Applications,* 41(17), pp. 7858–7867

Mishra, B., & Kashyap, R. (2016). A review paper on digital watermarking techniques & its applications. *International Journal of Science and Research (IJSR),* 5(6), pp. 1864 – 1868

Mohammadi,S.(2015). A novel video watermarking algorithm based on chaotic maps in the transform domain.*IEEE Artificial Intelligence and Signal Processing International Symposium, (AISP),* pp. 188-191

Mohammed, A.A., & Ali, N.A. (2018). Robust video watermarking scheme using high-efficiency video coding attack. *Multimedia Tools and Applications,* 77, pp. 2791-2806

Mohananthini, N., & Yamuna, G. (2015). A study of DWT-SVD based multiple watermarking scheme for medical images. *International Journal of Network Security,* 17(5), pp. 558-568

Mohanarathinam, A., Kamalraj, S., Ravi, R.V., & Manikandababu, C.S. (2020). Digital watermarking techniques for image security: A review. *Journal of Ambient Intelligence and Humanized Computing,* pp. 3221–3229

Mondal, S., Debnath, R., & Mondal, B.K. (2016). An improved color image steganography technique in spatial domain. *International Conference on Electrical and Computer Engineering (ICECE),* pp. 582–585

Mood, N., & Konkula, V. (2018). A novel image watermarking scheme based on wavelet transform and genetic algorithm. *International Journal of Intelligent Engineering and Systems,* 11, pp. 251-260

Muhammad, K., Sajjad, M., & Baik, S.W. (2016) Dual-level security based Cyclic18 steganographic methodand its application for secure transmission of keyframes during wireless capsule endoscopy. *Journal of Medical Systems,*40, pp. 114

Muhammad, N., & Bibi, N. (2015). Digital image watermarking using partial pivoting lower and uppertriangular decomposition into the wavelet domain. *IET Image Proc,* 9(9), pp. 795–803

Nair, R., Varadharajan, V., Joglekar, S., Nallusamy, R., & Paul, S. (2014). Robust transcoding resistant watermarking for H.264 standard. *Multimedia Tools and Applications,* 73, pp. 763-778

Nouioua, I. (2018). A novel blind and robust video watermarking technique in fast motion frames based on SVD and MR-SVD. *Hindawi Security and Communication Networks,* Article ID 6712065, pp. 1-16

Pan, Z.Q., Lei, J.J., Zhang, Y., Sun, X.M., & Kwong, S. (2016). Fast motion estimation based on a content property for low-complexity H.265/HEVC encoder. *IEEE Transactions on Broadcasting,* 62, pp. 675–684

Potkar, A.N., & Ansari, S.M. (2014). Review on digital video watermarking techniques. *International Journal of Computer Applications,*106(11), pp. 6-10

Powar, P.V. (2013). Implementation of a digital video watermarking scheme based on FGPA. *International Journal of Electrical, Electronics, and Computer Systems,* 1, pp. 99-104

Pradhan, A., Sekhar, K.R., & Swain, G. (2018). Digital image steganography using LSB substitution, PVD, and EMD. *Mathematical Problems in Engineering,* pp. 1-12

Prasad, K.K., & Aithal, P.S. (2018). A study on fingerprint hash code generation based on MD5 algorithm and freeman chain code.*International Journal of Computational Research and Development (IJCRD),* 3(1), pp. 13-22

Rachmawati, D., Tarigan,J.T., & Ginting, A.B.C. (2018). A comparative study of Message Digest 5(MD5) and SHA256.*Journal of Physics: Conference Series,* 78, pp. 1-6

Raj, P.A., & Umamageswari, M. (2014). Using digital signature. *International Journal of Computer Network and Security (IJCNS),* 6(1), pp. 16-21

Raju,U.S.N., Sethi, K., Choudhary, S., & Jain, P. (2015). A new hybrid watermarking technique using DCT and DWT based on scaling factor. *IEEE Futuristic Trends on Computational Analysis and Knowledge Management International Conference (ABLAZE),* pp. 232-235

Rana, R.,Thangjam, S., & Singh, S. (2018). Performance analysis of video watermarking in transform domain using differential embedding.*Information and Communication Technology for Intelligent Systems (ICTIS),*pp. 566-574

Rassem, T.H., Makbol, N.M., & Khoo, B.E. (2016). Performance evaluation of RDWT-SVD and DWT-SVD watermarking schemes. *AIP Conference Proceedings,* 1774, pp. 050021-1 - 050021-9

Reddy, V.R. (2017). An intelligent and robust digital image watermarking scheme for security enhancement. *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE),* pp. 45-54

Roy, S., & Pal, A.K. (2017). A robust blind hybrid imagewatermarking scheme in RDWT-DCT domain using Arnold scrambling.*Multimedia Tools and Applications,*76(3), pp. 3577–3616

Sahoo, B.M., Behera, J., & Rout, R.K. (2015). A robust fragile watermarking technique for digital image. *International Journal of Engineering Research and Technology (IJERT),* pp. 1-7

Sahu, H., & Patil, E. (2020). A review on digital video watermarking. *International Research Journal of Engineering and Technology (IRJET),*7, pp. 5432-5435

Saini, L.K., & Shrivastava, V. (2014). A survey of digital watermarking techniques and its applications. *International Journal of Computer Science and Telecommunications (IJCST),*2, pp. 70-73

Sang, J., Liu, Q., & Song, C.L. (2020). Robust video watermarking using a hybrid DCT-DWT approach.*Journal of Electronic Science and Technology,* pp. 1-8

Sanivarapu, P.V., & ChandraMouli, P.V.S.S.R., (2018). Adaptive, robust, and blind digital watermarking using Bhattacharyya distance and bit manipulation. *Multimedia Tools and Applications,* 77, pp. 5609-5635

Sanivarapu, P.V., & ChandraMouli, P.V.S.S.R.(2017). A robust semi-blind watermarking for color images based on multiple decompositions. *Multimedia Tools and Applications, 76,* pp. 25623-25656

Sanku, D., Kiran, S., Takore, T.T., & Kumar, P.R. (2018). Digital image watermarking in RGB host using DWT, SVD, and PSO techniques. *International Conference on Micro-Electronics, Electromagnetics and Telecommunications (ICMEET),* pp. 333-342

Saqer,W., & Barhoom,T. (2016). Steganography and hiding data with indicators based LSB using a secret key.*Engineering, Technology & Applied Science Research,* 6(3), pp. 1013-1017

Sarma, A., & Ganguly, A. (2012). An entropy-based video watermarking scheme. *International Journal of Computer Applications,* 50(7), pp. 32-35

Sawant, P.M. (2018). Digital watermarking system for video authentication. *International Journal of Advanced Research in Computer and Communication Engineering,* pp. 1-4

Sethuraman, S., & Srinivasan, S. (2016). Survey of digital video watermarking techniques and its applications. *Engineering Science,* 1(1), pp. 22-27

Shahid,M., & Kumar, P. (2018). Digital video watermarking: Issues and challenges. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),*7, pp. 440-403

Shanmugam, M., & Chokkalingam, A. (2018). Performance analysis of 2 levels DWT-SVD based non-blind and blind video watermarking using range conversion method. *Microsystem Technologies,* pp. 1-9

Sharma, V., & Kumar, S. (2013). A new approach to hide text in images using steganography. *International Journal of Advanced Computer Research,* 3(4), pp. 701-708

Shukla, K.M., & Mehta, A.K. (2015). A review on digital watermarking techniques, applications, and attacks. *International Journal of Engineering and Computer Science (IJECS),* 4(4), pp. 11237-11245

Shukla, N., & Sharma, S. (2016). A survey on video watermarking method for reliability and security in video using the least significant bit. *International Journal for Research in Applied Science & Engineering Technology (IJRASET),* 4(3), pp. 357-358

Singh, A., Jain, S., & Jain, A. (2013). A survey: Digital video watermarking. *International Journal of Scientific & Engineering Research,* 4(7), pp. 1261- 1265

Singh, N., & Bhardwaj,J. (2018). Comparative analysis for steganographic LSB variants. *International Conference on Computing, Communication and Signal Processing (ICCASP),*2(1),pp. 827-835

Singh, N., Joshi, S., & Birla, S. (2019). Suitability of singular value decomposition for image watermarking. *International Conference on Signal Processing and Integrated Networks (SPIN),* pp. 983-986

Singh, P., & Chadha, R.S. (2013). A survey of digital watermarking techniques, applications, and attacks. *International Journal of Engineering and Innovative Technology (IJEIT),* pp. 165-173

Singh, R., Nigam, S., Singh, A., & Elhoseny, M. (2020). On wavelet domain video watermarking techniques. *Intelligent Wavelet Based Techniques for Advanced Multimedia Applications,* pp. 65-76

Singh, T.R., Singh, K.M., & Roy, S. (2013). Video watermarking scheme based on visual cryptography and scene change detection. *AEU-International Journal of Electronics and Communications,* 67(8), pp. 645-651.

Sneha, C.D.R., & Shivamkutty, M. (2014). Digital watermarking of video using hybrid techniques.*IEEE Advances in Communication and Computing Technologies International Conference (ICACACT),*pp.1-5

Solanki, A., & Bakaraniya, P. (2018). Different video watermarking techniques - A review. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* 3(1), pp. 1890-1894

Sonoda, K., & Morisaki, K. (2017). Digital audio watermarking robust against locality sensitive hashing. *Advances in Intelligent Information Hiding and Multimedia Signal Processing,* pp. 115-122

Su, P.C., Kuo, T.Y., & Li, M.H. (2017). A practical design of digital watermarking for video streaming services. *Journal of Visual Communication and Image Representation,* 42, pp. 161-172

Sujatha, P., & Devi, R. (2017).A glance of digital watermarking techniques with an evaluation of Haar and Daubechies wavelet. *International Journal of Applied Engineering Research (IJAER),* 9, pp. 9652–9657

Tabassum, T., & Islam,S. M. M. (2012). A digital video watermarking technique based on identical frame extraction in 3-level DWT.*International Conference on Computer and Information Technology (ICCIT),* pp. 101-106

Takore, T.T., Kumar, P.R., & Devi, G.L. (2016). A modified blind image watermarking scheme based on DWT, DCT, and SVD domain using GA to optimize robustness. *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai,* pp. 2725-2729

Tasheva, A., Tasheva, Z., & Nakov, P. (2017). Image-based steganography using modified LSB insertion method with contrast stretching. *International Conference on Computer Systems and Technologies*, pp. 151-158

Tayan, O., Kabir, M.N., & Alginahi, Y.M. (2014). A hybrid digital signature and zero-watermarking approach for authentication and protection of sensitive electronic documents.*The Scientific World Journal,*pp. 2-14

Tayan,O.,Alginahi,Y.M., & Kabir, M.N. (2013). An adaptive zero-watermarking approach for authentication and protection of sensitive text documents.*International Conference on Advances in Computer and Information Technology (ACIT),* pp.205-208

Tiwari, D., Arya, K.V., & Saraswat, M. (2013). Digital video watermarking using scene detection. *International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA 2012),* pp. 315-323

Tsai, T.H., Wu, C.Y., & Fang, C.L. (2014). Design and implementation of joint data compression and digital watermarking system in a MPEG-2 video encoder. *Journal of Signal* Processing Systems, 74, pp. 203–220

Verma, V.S., & Jha,R.K. (2015). An overview of robust digital image watermarking.*IETE Technical Review,*pp. 479-496

Vo, C., Vo, H.P., & Nguyen, S.T. (2019). Applying watermarking in digital image copyright protection.*Researches of Engineering and Technology (RET),*pp. 1-8

Volos, C.K.,Kyprianidis, I.M., & Stouboulos, I.N. (2013). Image encryption process based on chaotic synchronization phenomena. *Signal Processing,* 93(5),pp. 1328-1340

Wahid, M., Ahmad, N., Zafar, M.H., & Khan, S. (2018). On combining MD5 for image authentication using LSB substitution in selected pixels. *International Conference on Engineering and Emerging Technologies (ICEET),* pp. 1-6

Wang, C.Y, Shan, R.Y, & Zhou, X. (2018) Anti-HEVC recompression video watermarking algorithm based on the all phase biorthogonal transform and SVD. *IETE Technical Review,* 35, pp. 1–17

Wang, X.Y., Shi, Q.L., Wang, S.M., & Yang, H.Y. (2015). A blind robust digital watermarking using invariant exponent moments. *International Journal of Electronics and Communications,* 70(4), pp. 416-426

Winderickx, J., Braeken, A., Singelée, D., Peeters, R., Vandenryt, T., Thoelen, R., & Mentens, N. (2018). Digital signatures and signcryption schemes on embedded devices: a trade-off between computation and storage. *ACM International Conference on Computing Frontiers,* pp. 342–347

Wu, Y., Zhou, Y., Noonan, J.P., & Agaianc, S. (2014). Design of image cipher using latin squares. *Information Sciences,*264, pp. 317–339

Xuemei, J., Quan, L., & Qiaoyan, W. (2013). A new video watermarking algorithm based on shot segmentationand block classification. *Multimedia Tools and Applications,* 62(3), pp. 545–560

Yan, W. (2019) Introduction to Intelligent Surveillance. Springer International.

Yan, Q., Kankanhalli, M. (2002) Erasing video logos based on image inpainting *IEEE ICME'02.*

Yan, W., Qi, D. (2001) Mapping-based watermarking of 2D engineering drawings. *International Conference on CAD/Graphics,* 464 – 469.

Yang, J., & Li, S.B. (2017). An efficient information hiding method based on motion vector space encoding for HEVC. *Multimedia Tools and Applications,* 77, pp. 11979–12001

Yang, Y., & Li, H.(2015). The application of DCT algorithm in digital watermarking by MATLAB and simulation. *International Conference on Modelling, Identification, and Control (ICMIC),* pp. 1-5

Yassin, N.I. (2012). Block-based video watermarking scheme using wavelet transform and principal component analysis. *International Journal of Computer Science Issues,* pp. 296-301

Yavuz, E., Yazıc, R., Kasapbas, M.C., & Yamac, E. (2015). A chaos-based image encryption algorithm withsimple logical functions. *Computer Electrical Engineering,* 54, pp. 471–483

Yu, X., Wang, C., & Zhou, X. (2018). A survey on robust video watermarking algorithms for copyright protection. *Applied Sciences,* 8(10), pp.1891

Zhang, W., Li, X., Zhang, Y., Zhang, R., & Zheng, L. (2017). Robust video watermarking algorithm for H.264/AVC based on the JND model. *KSII Transactions on Internet and Information Systems,* 11, pp. 2741–2761

Zhou, X, Ma, J., Du, W., & Li, Y. (2014). A dynamic multiple digital watermarking model based on temporal series. *International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC),* pp. 367–371

Zhou, X., Zhang, H., & Wang, C. (2018). A robust image watermarking technique based on DWT, APDCBT, and SVD. *Symmetry,* 10(3), pp. 77

Zhou,Y., Wang, C., & Zhou, X. (2019). An intra-drift-free robust watermarking algorithm in high-efficiency video coding compressed domain. *IEEE Access,* 7, pp. 132991-133007

Zhu, L. (2012). Electronic signature based on digital signature and digital watermarking. *International Congress on Image and Signal Processing (CISP),* pp. 1644–1647