Design of Robust and Secure Video Watermarking Algorithm

Thesis
Submitted for the award of
Degree of Doctor of Philosophy
Computer Science
By
Praful Saxena

Enrollment No: MUIT0117038004

Under the Supervision of
Dr. Santosh Kumar
Associate Professor
&
Dr. Himanshu Pandey
Assistant Professor

Under the Maharishi School of Engineering & Technology
Session 2023-2024

Maharishi University of Information Technology

Sitapur Road, P.O. Maharishi Vidya Mandir
Lucknow, 226013

Declaration by the Scholar

I hereby declare that the work presented in this thesis entitled "**Design of Robust and Secure Video Watermarking Algorithm**" in fulfillment of the requirements for the award of Degree of Doctor of Philosophy, submitted in the Maharishi School of Engineering & Technology, Maharishi University of Information Technology, Lucknow is an authentic record of my own research work carried out under the supervision of Dr. Santosh Kumar and co-supervision of Dr. Himanshu Pandey also declare that the work embodied in the present thesis-

i) is my original work and has not been copied from any journal/ thesis/ book; and

ii) has not been submitted by me for any other Degree or Diploma of any University/ Institution.

Signature of the Scholar

Maharishi University of Information Technology
Lucknow

Supervisor's Certificate

This is to certify that Mr. Praful Saxena has completed the necessary academic turn and the swirl presented by him is a faithful record is a bonafide original work under my guidance and supervision. He has worked on the topic **"Design of Robust and Secure Video Watermarking Algorithm"** under the School of School of Engineering & Technology, Maharishi University of Information Technology, Lucknow.

Dr. Santosh Kumar
(Supervisor)
Associate Professor
Department of Computer Science
Galgotias University
Greater Noida

Dr. Himanshu Pandey
(Co-Supervisor)
Assistant Professor
Faculty of Engineering & Technology
University of Lucknow
Lucknow

Date:

ACKNOWLEDGEMENTS

To commence with, I pay my obeisance to my parents and ***"Shri Khatu Shyam ji"*** for giving me the strength and patience to work through all these years and to have bestowed upon me good health, courage, inspiration and zeal.

The award of degree "Doctor of Philosophy" is one of the hardest deserving achievements which are not easily found. I will always. During the entire research work some valuable people conceived their enormous positions in my heart. In this regard, I am grateful to the University and express my deep sense of gratitude to its Hon'ble **Prof. (Dr.) Bhanu Pratap Singh** Vice-Chancellor for delivering this great opportunity to me. I also want to convey regards to the registrar **Prof(Dr.) Akhand Pratap Singh** of MUIT, who has always motivated me for this work. I would like to express my special appreciation and thanks to my supervisor Associate Professor Dr. Santosh Kumar, you have been a tremendous mentor for me. I would like to thank Dean Research **Prof(Dr.) V. K Singh** ,Assistant Professor **Dr. Vaishali Singh** and Deupty Registrar **Dr. Girish Chimval** and my friends Mr. Sandeep Sharma, Mr. Vinay Kr. Pant and Dr. Neeraj Kumar Verma ,for encouraging my research and for allowing me to grow as a research scientist. Your advice on both research as well as on my career have been priceless. I am heartily thankful to you for being a great mentor for greatly obliged cooperation, for having adequate belief in my abilities to help me incrementally in build up my understanding of the research area and for all your precious endeavors on behalf of me.

I owe a special thanks to my family, who supported me and helped me throughout my life and during this study, my wife Mrs. Arpita Srivastava , my lovely daughter, Maurvi and my son Avyan, who are the pride and joy of my life. I love you more than anything and I appreciate all your patience and support during my Ph.D. studies.

Praful Saxena

ABSTRACT

Video watermarking is a pivotal field of research in the realm of multimedia security and content protection. In this research, we present an innovative and comprehensive approach to video watermarking, leveraging multiple transformation techniques, including Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD), and the integration of motion frames. The primary focus of our study is on embedding watermarks in video content while incorporating encryption measures to enhance both robustness and security.The rapid proliferation of digital video content on the internet has given rise to concerns regarding intellectual property protection, copyright enforcement, and content authenticity. Video watermarking provides a solution by enabling the seamless embedding of hidden information (watermarks) within the video content, serving various purposes, such as ownership verification, content authentication, and tracking unauthorized distribution.Our research begins with the utilization of the Discrete Wavelet Transform (DWT) to decompose video frames into different frequency components. DWT's multi-resolution property allows for an effective localization of watermark embedding in frequency subbands, optimizing the trade-off between perceptual transparency and robustness. The watermark data is encrypted before being embedded into selected DWT coefficients, ensuring secure embedding. The DWT-based approach provides resistance to common video processing operations while minimizing perceptual distortion.We complement the DWT approach with the application of the Discrete Cosine Transform (DCT). DCT is used to modify the DCT coefficients of motion-compensated frames, further enhancing robustness against video compression and format conversion. The watermark data is encrypted before being embedded into DCT coefficients to maintain security and integrity. By combining DWT and DCT, our approach achieves a balance between robustness and perceptual transparency. In addition to the transformation techniques, we integrate Singular Value Decomposition (SVD) into our watermarking framework. SVD is employed for spatial domain watermark embedding, allowing us to exploit the singular value components of the video frames. The watermark is encrypted and embedded within the singular value matrices of the video, providing an additional layer of security and robustness against attacks.To address temporal dynamics and improve robustness against video manipulations, we introduce the concept of motion frames. Motion frames are generated by tracking the motion vectors of video frames and representing this motion information as separate frames. The watermark is embedded in the motion frames, enhancing robustness against frame interpolation and scene changes.An integral aspect of our research is the incorporation of encryption into the watermarking process. Watermark encryption ensures that the hidden information remains secure, preventing unauthorized parties from tampering with or removing the watermark. Various encryption algorithms and techniques are explored, enhancing the overall security of the video watermarking system.The proposed video watermarking scheme is evaluated through a comprehensive set of experiments, including assessments of robustness, perceptual transparency, and security. Results demonstrate the effectiveness of our approach in preserving the video's perceptual quality while offering strong resistance to a wide range of attacks, such as compression, noise addition, and format conversion.

In summary, our research presents an innovative and comprehensive video watermarking approach that leverages DWT, DCT, SVD, and motion frames, while integrating encryption to enhance security. This multi-faceted approach achieves a balance between robustness and perceptual transparency, making it a valuable tool for content protection and authentication in the digital age.

LIST OF ABBREVIATIONS

Abbreviation	**Description**
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
LSB	Least Significant Bit
NC	Normalized Correlation
PCA	Principal Component Analysis
PKC	Public Key Cryptography
PSNR	Peak signal-to-noise ratio
SSIM	Structure Similarity Index
SVD	Singular Value Decomposition

LIST OF FIGURES

Chapter 1 Page No.

Chapter 3

Chapter 4

LIST OF TABLES

CONTENTS

Content Details **Page No.**

CHAPTER 1

INTRODUCTION

1.1 INFORMATION HIDING: AN OVERVIEW

The art of hiding the information is always an important technical aspects which is used to secure the digital content during communication or data transmission. The hiding of the information is now comes under the domain of Information Security. It continuously linked with the organizational function in order to guard the data from unknown as well as to fabricate the data as and when require by an authorized individual. The essential characteristics of standard information security are the availability, integrity, authenticity and confidentiality.The transmission and circulation of digital multimedia content has become vulnerable by the ceaseless growth of Internet technology. However this progress has a dark side also i.e. it has lead to an increment in unenviable and other felonious operations.

Due to lack of security on the internet, images can be copied and distributed without owners' consent. In such a situation digital watermarking is one of the solutions for authentication, copy control and right supervision of digital media. A digital image is a category under digital media. Robustness of this process is checked thoroughly by means of extracting unique watermark flawlessly with no degradation in original image[1]. Digital Asset Management System (DAMS) handles nearly compressed and encrypted media information. It is viable to watermark those compressed-encrypted media for ownership announcement or copyright control.

1.1.1 Security related with Personal Information

Security of personal information is to protect any information generated by an individual or entity from unauthorized user. It is more than just ensuring compliance with the requirements of the Privacy Act. In case of mishandling the personal information, it may cause a reputational or financial loss to the customer. This ultimately can lead to a loss of expectation and significantly harm to the reputation of organization. The noteworthy infringe can outcome in a loss of clients or industry partners and returns.

1.1.2 Protect the Confidential Information

In today's modern environment, confidential information is especially valuable. It ensures that information is kept safe from illegal access. Military operations, for example, necessitate confidentiality; the banking sector includes credit/debit card details, trade secrets, and government records, among other things. Information security faces a severe difficulty in protecting such data. Encryption is a critical tool for maintaining information confidentiality[2]. Encryption ensures that information can only be read or published by authenticated users.

1.1.3 The Trademark Protection

A trademark is a symbol, phrase, word, or design that distinguishes one company's goods from those of its competitors. The prerequisite for designating the class of goods or services to which the mark will apply must be a clear depiction of the mark. The accompanying Fig. 1.1(www.microsoft.com), for example, indicates the trademark of Microsoft, a software development business. Each application is judged on its own merits, and no simple mechanical test is employed to assess there is or is not a risk of confusion. As a result, design techniques must be established in consideration of non-branded companies that use trademarks that are similar from those of branded companies.

Figure 1.1: Trademark of Company

1.1.4 Intellectual Property Protection

The term "intellectual property" refers to the creations of human minds that are granted exclusive rights. For a limited time, innovators, artists, and company owners are granted exclusive rights to a range of intangible goods. Patents and Copyright are the two main types for property rights. Patents are property rights granted to creators that allow the patent holder to prevent others from selling, manufacturing, or utilising the innovation. Patents are further divided into two types: utility and design patents. A utility patent protects any innovative and beneficial innovation, such as a product, machine, or manufacturing process. The invention must be original and have certain socioeconomic advantages to be eligible for this patent. A design patent provides any innovative, unique, and ornamental design for a part or component. The word "authorship protection" refers to the preserving of original works of authorship such as music, literature, multimedia documents, artistic works, and computer software. Copyright holders have sole authority to disseminate, adapt, and reproduce their work. The copyright to a work exists from the moment it is created, hence registration is not required. Copyright protection [3] entails the identification of unlawful copies of (possibly falsified) multimedia objects as well as the authentication of multimedia objects. In Figure 1.2[4], you could see some examples of copyright images. The primary design principle is to implant copyright information in the origin item, which can then be removed at any point to prove ownership. Copyright protection is crucial in information security, specifically when it comes to multimedia security. The digital video multimedia object is instantly exchanged between the two or more workstations due to the availability of high internet bandwidth. Furthermore, the introduction of digital technology can be exploited by criminal users to illegally duplicate many identical copies of the original video. These capabilities raise the issue of developing copyright security mechanisms for video multimedia items. Because of all these factors, securing multimedia items such as images, music, and video necessitates significant design work.

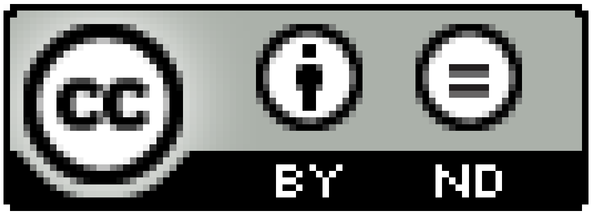

Figure 1.2: Example of Copyright Protection

1.2 Issues Related with Information Security

There are numerous reasons for securing the information, and relevant techniques must be examined and executed. Illegal gathering and use of information and information systems is one of the primary challenges. Another aspect of information security is the distribution and creation of software that disrupts the normal operation of information systems. As a result, the owner will suffer a significant financial loss. Another issue is the leakage of information across communication channels, which leads secrecy to be compromised. Moreover, unauthorized access to information in data banks and databases is a big matter of concern. One of the most significant issues is the cost of obtaining upgraded information security technologies, as technology is constantly evolving and nothing can ever be entirely secure. Even if one region is neglected, the entire system may be endangered. Another issue is that these security solutions are really quite complex, and users may not fully comprehend what they are using. If the malicious user is repeatedly entering passwords, the system's efficiency may suffer. Techniques are needed to prevent picture and video duplication, forgery, and unauthorized distribution. Placing photos or video sequences on a public network without such safeguards exposes them to theft and alteration. Many new techniques are now being introduced, and some of them may blend with current ones. Even Nonetheless, there are a number of obstacles in the way of information security.

1.3 Various Information Security Methods

Currently, a variety of strategies are deployed to remain secure. Cryptography, steganography, and digital watermarking are the three main categories of these approaches. Each approach is tailored to a unique problem. The next chapter details a basic introduction.

1.3.1 Cryptography

The most prevalent way of securing digital content is cryptography. Using an optional key at the source end, the original communication is turned into an unintelligible or encrypted version. The modified communication is known as cypher text and is sent to the intended recipient. The scrambled message is decoded at the receiver side using the same or a different but related key to restore the initial text. It supports two different types of cryptography: Asymmetric cryptosystems deploy one key (public key) for encryption and another related key for decryption, whereas symmetric cryptosystems use the same key for both encryption and decryption (private key). A digital signature system is an asymmetric cryptographic primitive, whereas symmetric cryptographic primitives comprise Electronic Code Book mode, Cipher Feedback mode, Feedback chaining cypher mode, and Counter cypher mode of operation. Each one can be used in a range of situations. Previously, cryptographic methods were used to solve multimedia and network challenges facing, ensuring that communication could be secured by encrypting the sensitive message. However, the digital content must be decrypted at some point. As a result, these solutions preserve data while transmission in an open network, but intellectual property rights are no longer protected after the data is decrypted at the destination end. The contents of the decrypted files could be misused by making multiple copies and distributing them in an unlawful manner. Encryption's protections were no longer available at this point. As a result, a variety of sophisticated concealment protocols have been proposed in order to safeguard or protect the information. The term "hiding" relates to concealing information or keeping the existence of a message hidden. In attempt to overcome these constraints, two types of techniques, steganography and digital watermarking, were introduced.

1.3.2 Steganography

Another option is to bury the secret information in a non-hazardous file. Steganography [3] is a blend of art and science used to conceal secret messages such that no one except the sender and intended receiver is aware of their existence. Instead than encrypting the message, it masks it in other seemingly innocuous things so that its existence is not disclosed. Steganography has an advantage over cryptography in that the message does not draw attention to itself. As a sense, steganography may be a viable alternative in nations where encryption is prohibited. However, because the host object must be an imitation product in order to conceal the secret information, the process of steganography can never be applied to protect the copyright of the given multimedia products.

1.3.3 Digital Watermarking

The process of digital watermarking is to hide digital mark or logo, called digital watermark, in a multimedia signal, so as to assert authenticity of owner later. A digital watermark is embedded in original media (sometimes using some key information, to be discussed later) to produce watermarked media, also called signed media, watermarked signal or signed signal. Subsequently, watermarked media is used in conjunction with original media or a Key to pull out original watermark. Process of embedding and extracting a watermark is shown in Fig. 1.3

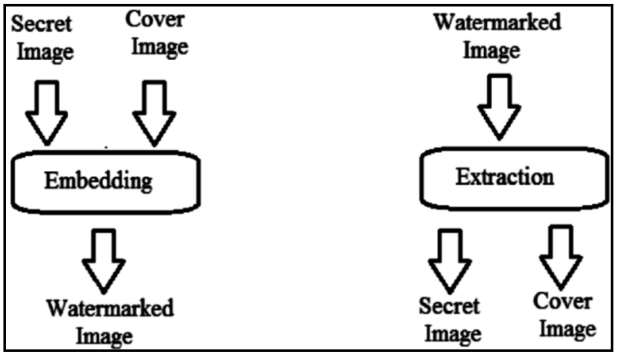

Figure 1.3: Digital Watermarking

Digital watermarking [4] is a groundbreaking technique for securing ownership of multimedia items. This method to solve embedding a watermark in the multimedia file (picture, audio, and video) in a secure, robust, and invisible manner. A watermark is a unique bit pattern included in original multimedia content that is used to verify the owner as well as the content itself. The sort of bit pattern established is determined by the application for which it was created. Copyright content, ownership information, or an authentication sequence can all be used for the watermarks. When viewed by transmitted light (or when viewed by reflected light, atop a dark background), a watermark is a distinguishing image or pattern in paper that appears as varied shades of lightness/darkness due to thickness or density changes in the paper. A watermark is a semi-transparent image or text that has been put to a sheet of paper or another image to protect the original image or make copying the item more difficult. The visibility of watermarks varies widely; while some are evident on first glance, others take further investigation. Various aids, such as watermark fluid that wets the paper without harming it, have been devised. The concept of organising and conveying anticipated work stems from the fact that encryption methods are frequently utilised to improve security in a variety of signal processing applications. Image watermarking is a cutting-edge image processing tool that addresses issues of copyright infringement and content authentication. As a result, encryption technologies are seen as the best tools for improving the application's security. The Paillier cryptosystem has additive privacy homomorphism and is quick enough for an SSP application. As a result, its been concluded that picture watermarking is appropriate. Technology is evolving rapidly these days, and it is playing an increasingly essential part in people's lives and careers. We now use the Internet and digital signals to communicate information due to the rapid development of network and digital technology. Copyright protection, source tracking, broadcast monitoring, clandestine communication, bill security, and authenticity recognition are just a few of the applications for digital watermarking. Digital watermarking is not a new technology; there are certain historical techniques and uses, but as new digital signals, applications, and attacks develop, so will comparable digital watermarking. Digital watermarks, like traditional watermarks, are only visible under particular conditions, such as after employing an algorithm, and are invisible otherwise. It's pointless to employ a digital watermark if it alters the carrier signal to the point of being noticeable. Traditional watermarks can be used on visible material (such as photographs or video), but digital watermarking uses audio, pictures, video, texts, or 3D models as the signal. At the same time, a signal may carry many watermarks. A digital watermark, unlike metadata that is added to the carrier signal, does not influence the size of the carrier signal.

Watermark Embedding Process

This section explains the algorithm that should be used to embed the watermark into the multimedia data. In general, whether the contents are original or compressed relies not only on the type of host signal, but also on whether the embedded watermark should be displayed or not. Watermark selection is obviously a key concern. It is evaluated and the results for which the system is being used. Copyright information as a watermark must be used to insert into the cover objects to protect the copyright for a specific multimedia data.

Customer information is added as a watermark if the system is developed for tracing the unauthorized user, or if the integrity of multimedia host data is of concern. The authentication information is incorporated in the host multimedia data, which is of particular interest. The embedding process is defined by a Tuple (M, W, K, M), where M represents the original multimedia data, W denotes the gathering of all bits of the watermark image, K contains the set of all keys, and WM represents the watermarked video[5]. Although in the watermarking process, the cryptography key (symmetric or public key) is optional. If it is included, however, the overall system will be more secure in preserving the hidden information.

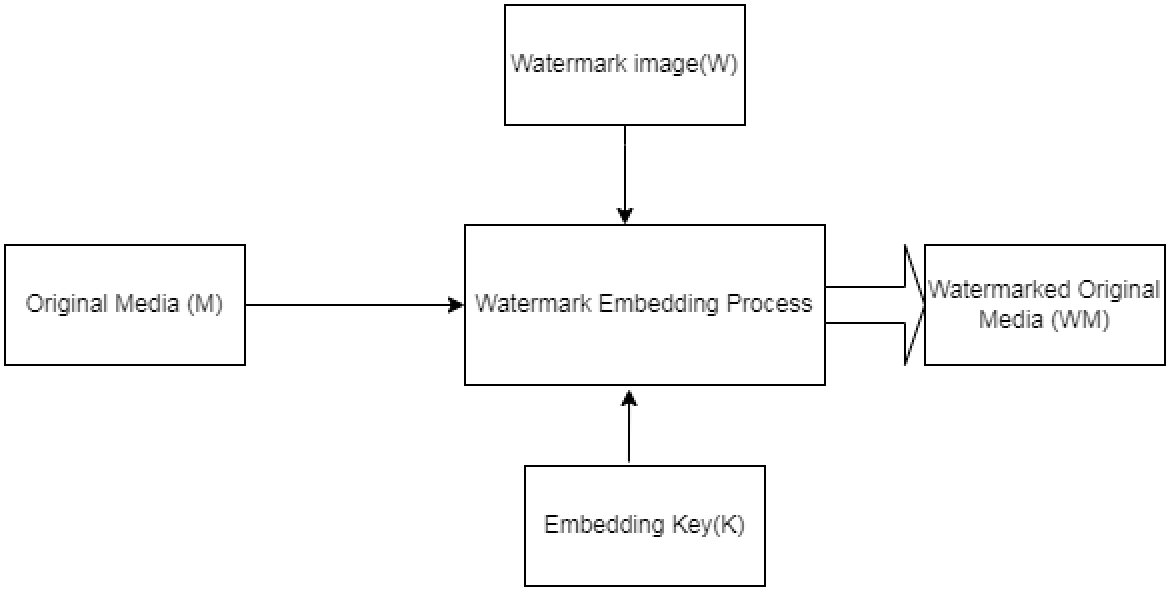

Figure 1.4 : Watermark Embedding Process

Watermark Extraction Process

The algorithm must be designed in a manner that the watermark can be extracted at any moment in order to check the effectiveness of the data or to achieve the goal for which the app was designed. As shown in Fig. 1.5, the extraction of a watermark is demonstrated by a Tuple (M, W, K, WM, EW). These settings modify depending on the type of watermarking technology. Because of several changes of watermarked information, the extracted watermark WE differs from the embedding watermark W. (MW).

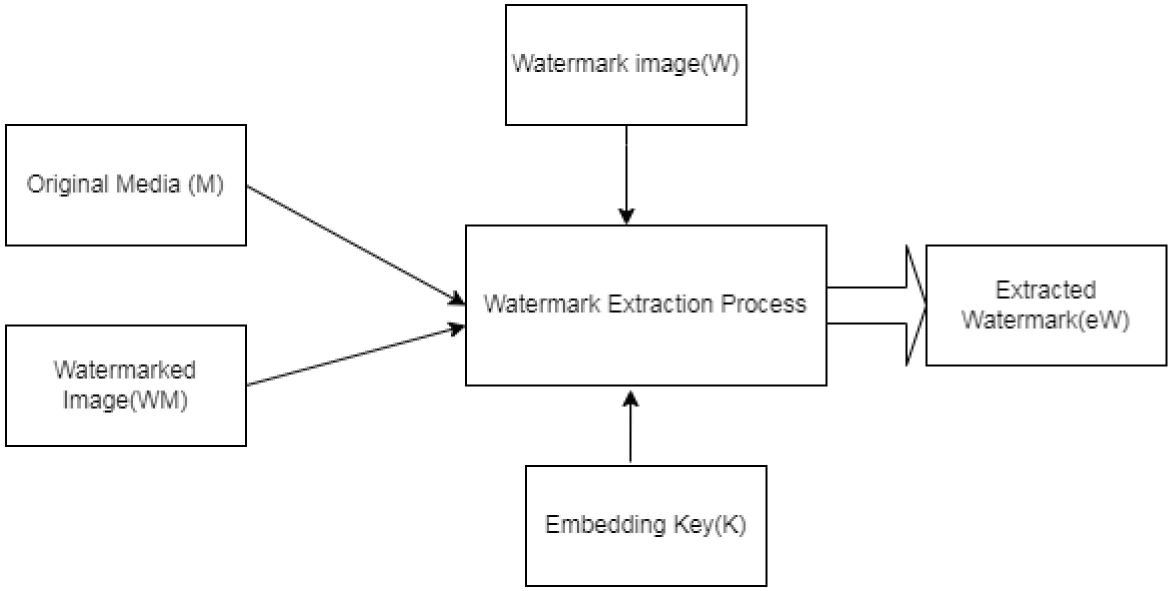

Figure 1.5: Watermark Extraction Process

Classification of Watermarking System

Depending on the user's perspective, digital watermarking methods are classified into several categories (Fig. 1.6). Watermarking methods, for example, can be categorised according on the kind of document, text, picture, audio, or video. In this thesis, we focus solely on image watermarking. Watermarking methods can also be classified depending on whether the watermarking is done in the spatial or frequency domain, and whether the watermark is visible or invisible [4]. If the encoded information can be consistently detected from the marked signal after any number of transformations, the digital watermark is said to be robust with respect to transformations. JPEG compression, rotation, cropping, additive noise, and quantization are all common image degradations. Temporal changes and MPEG compression are frequently added to this list for video content. If the watermarked content is perceptually equal to the original, unwatermarked content, the digital watermark is deemed undetectable. In general, it is simple to make either robust or invisible watermarks, but combining the two has proven to be extremely difficult. Robust undetectable watermarks have been proposed as a strategy for protecting digital property, such as in professional video content as an incorporated no-copy-allowed flag.

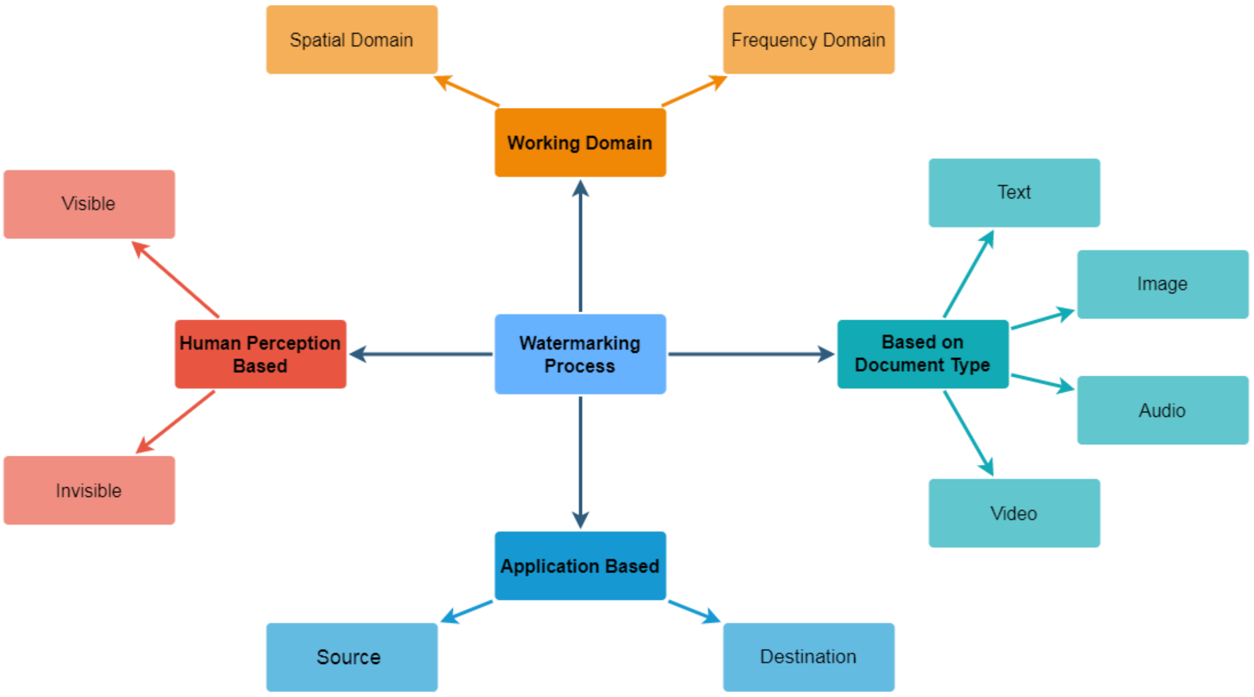

Figure 1.6: Watermarking System Classification

Two working domains are often used in image watermarking systems. Spatial Domain: based on perceptual analysis of the original image, pixels of one or more randomly selected subsets of an image are transformed. Frequency or Transform Domain: To insert the watermark information, the original image is transformed into frequency domain and some of the values of particular frequencies are changed. This method is more reliable than the spatial domain method. The second parameter is based on human perception, and there are two types of watermarking: visible and invisible. The second translucent is superimposed onto the primary material in visible watermarking and is discernible on close inspection. The watermark was masked within in the original host signal with invisible watermarking. The third criterion is dependent on the application; it is further divided into two categories: source and destination. The copyright information should be inserted as a watermark into all copies of a particular work being distributed, so according source-based watermarking. The ultimate classification is determined by the application for which it will be created. Even if the watermarked object is intentionally or unintentionally modified, the section noted that the inserted information can be retrieved at any moment to prove ownership or copyright of the concerned multimedia material. Watermarking depending on destination on the client side, in which each disseminated copy receives a unique watermark identifying the specific buyer. By collecting client information, an unauthorized user responsible for producing addition to carbon of multimedia materials and propagation in the network categorization can be easily traced in this technique.

1.4 Requirements of Digital Watermarking

There are a number of requirements that should be met by the watermarking scheme. They're all described farther down.

1.4.1 Robustness

Robustness means that the watermarking method adopted must be able to defend the watermark from many types of attacks. It's worth mentioning that these attracts can be anything from cropping, resizing, or running the image over numerous types of filters, noise, translation, and so on. It's likely that some disturbances caused by any operation will have no effect on the watermark extraction.

1.4.2 Imperceptibility

In general, it refers to the watermark's perceptual transparency. Watermarking should be done in such a way that it does not influence the image's value or the concealed message and watermark after it's been watermarked. The image alteration should not be noticeable to the human eye after that little process. The embedding of the watermark into the perceptually irrelevant region of the host signal is a simple approach to reduce distortion during the watermarking process. However, the attacker can easily update the watermark information without being discovered as a result of this.

1.4.3 Payload Capacity

Simply put, it refers to the quantity of data that can then be encoded in a host signal. The data that must be kept hidden varies in size depending on the type of application. It has a direct impact on the robustness and perceived impact. If too much data is buried in the image (more than the loading capacity), the image's quality suffers and the resolution drops dramatically. Superior capacity is usually achieved at the expense of physical strength, imperceptibility, or both. Figure 1.7[3] depicts the tradeoff between robustness, imperceptibility, and payload capacity.

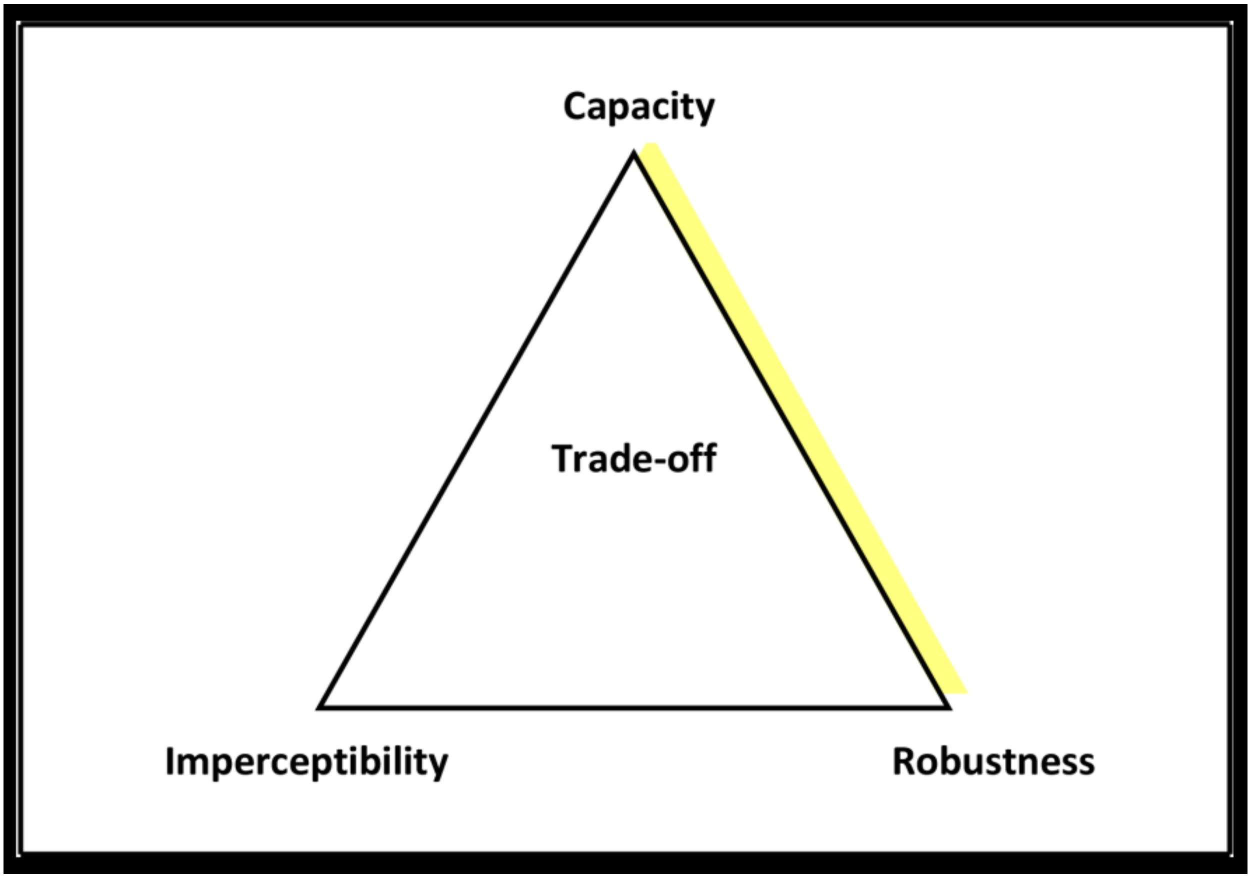

Figure 1.7: Robustness, imperceptibility, and payload capacity are all factors to consider.

1.4.4 Reliability

It's possible that the user is aware of the proper decoding process, rendering the watermark inactive. As a result, the key used for watermarking is the more authentic technique to safeguard the watermark. Around the same time, if the user is aware of the exact procedure, finding the correct key to connect with the one used at the time of embedding should be virtually impossible. As a result, it affects the watermark's dependability or strength.

1.5 Digital Watermarking Applications

Although digital marking is offered for use in a wide range of items, the number of which is growing all the time, instead of listing them all, the most important ones are covered here.

1.5.1 Managing Copyright of Media

DRM stands for identifying, tracking, protection, investigation, and keeping track of all types of physical and intellectual asset usage [6]. Its task is to administer and enforce digital rights. The evolution of DRM has been forced by a number of circumstances that threaten virtual rights.These trends have resulted in the successful use of Digital Rights Management to manage rights to store, alter, purchase, and redistribute digital content. Digital Right Management systems can properly manage the use, access, and distribution of digital composition. Copyright principles are commonly used to protect intellectual property rights in Digital Right Management systems [7]. Watermarking is used to prevent mass illegal duplicating of this content item. When a watermark is placed in data and that data is copied or circulated, an illegal behaviour is investigated.

1.5.2 Protecting Copyright

The use of digital watermarking in copyright protection is a critical benefit. The proprietor of the composition is clearly identified using watermarking, and the proprietor's rights to distribute the content material are appropriately incorporated. As a result, a powerful watermark is embedded into the image, and it is far possible to extract the watermark in identifiable shape however after applying typical image processing/manipulation procedures to the watermarked image. Any attempt to remove the watermark may have a major visual impact on the image. As a result, alteration may be undetectable from the image's outward look. If every other strategy in the field of watermarking is utilised, such as solving a seen tag at the image revealing copyright data or a mark in the post header, then such a label is sensitive to being removed without damaging the image in any significant way. But in the other hand, a strong watermark can never be removed without drastically damaging the image's visual appearance, leading to the opinion that watermarking is a far better solution for copyright protection and owner identification than other types of approaches.

1.5.3 Authentication

In cryptography, authentication has a different meaning than it had in watermarking. It is viewed in cryptography as confirming the source of a communication or confirming someone's identity . Watermarking, as an alternative, ensures the uniqueness and reliability of an image . An image is called real if it closely resembles the original image, implying that no changes have been made. Watermarking as a method of integrity verification is far superior because, first, the watermark is embedded inside the image itself and cannot be removed without causing problems, and second, no additional space is required to store the statistics connected with the watermark. Authentication of digital photos for the purpose of proof in insurance cases could be very useful. Watermarks that are both powerful and weak can be used to authenticate the validity of a photograph.

1.5.4 Tampering Detection in Media

If a picture has been manipulated in any way, it is said to have deteriorated, and this problem is closely tied to authentication. If any erosion is found, the image is not genuine. Localization, or the precise recognition of a modified visual section, leads to further tampering inquiry. This in-depth investigation could be valuable in the fields of media and forensics, as well as in determining the gravity of meddling and the cause of deterioration [16].

1.5.5 Controlling Privacy and Annotation

Multi-bit watermarking can be used to describe the image. Facts containing imaging information pertaining to the host image and information relating to the connected patient, for example, may be cautiously incorporated into the scholarly image itself. This minimizes the need to capture both the image and its information at the same time, reducing the amount of storage space required. In the same way, similar records and images become inextricably linked. Information is saved in encrypted form rather than text form to protect the privacy of the impacted person. This capability can be be improved by using an encrypting watermark. Watermarks shouldn't have to be substantial to be utilised in software when statistics are stored in a comfortable, safe, and close setting. Reversible watermarking, also described as lossless watermarking, is ideal for such systems since it can remove the watermark from the cover image and return the true image.

1.5.6 Media Forensics

Media forensics is the study of digital facts in order to obtain recordings that are scientifically admissible as evidence in court. This is frequently accomplished through the use of digital tools. For a variety of reasons, this discipline of media forensics has grown in importance. For example, the number of cyber crimes is increasing every day, as is the amount of money lost due to frauds and piracy, necessitating the successful implementation of legislation. Transaction tracking, content recovery of valuable, and a trustworthy digital camera are examples of programmes that use media forensics . Furthermore, if compression is utilised for a very low range, tamper examination on re-sampled photos is more than productive. Semi-fragile watermarks, on the other hand, are as effective over a far wider range of compressions while also detecting and localising manipulation.

1.5.7 Software Watermarking

The topic of software safeguarding is a significant one. Software piracy refers to the illegal copying or spreading of patented software. This can be accomplished through repetition, downloading, allocating, marketing, and/or installing several copies on personal or business computers. It is estimated that 38% of the world's computer software is pirated, with losses of up to $48 billion predicted in 2007. Furthermore, piracy is present in 50% of the 108 nations analysed, with a rate of 61 percent or higher. As a result, combating software piracy and protecting software proprietary information is critical. Software watermarking techniques are used to deter software programme piracy. It entails encoding a block of personally identifiable information about a software programme, which is referred to as a software programme watermark [18]. In the current situation, the research community is becoming increasingly interested in software programme watermarking.

1.5.8 Watermarking and Cloud Security

Cloud computing has become an integral part of our daily lives, and we can't deny that just about every app on today's phones is cloud-based. Knowledge that seems to be uploaded, saved, or accessed via the cloud must be secure at all times, regardless of its static or dynamic nature. Watermarking is an authentication technology that protects data and improves cloud computing security. On-demand, pay-per-use, and economic systems IT services over the internet are supported by the cloud commercial entity version. The internet cloud is made up of virtualized data centres. To store more than one set of records on the same cloud, the cloud must be designed to be secure and private, as security breaches will result in data potentially compromised. Virtualization and supplied hardware, software, networks, and analytics sets are used to dynamically build cloud topologies. The goal is to move desktop computing to a practitioner platform based on digital server clusters located in multiple locations [20]. Digital watermarking is a means of protecting files, photos, videos, software programmes, and relational databases using digital watermarking. These methods safeguard common information devices and widely dispersed software components.

1.6 Digital Video Watermarking

In recent years, extensive study into image watermarking has been conducted. The clamour for secure multimedia streaming has grown as the popular appeal of video production and recording devices such as personal video recorders, internet audio and visual video objects tools such as YouTube, video-on-demand via set-top box devices, wireless videos, videophones, and videoconferencing has grown. Watermarking, also known as digital video watermarking, has been one of the available ways for securing a digital video asset . It can be utilised in a wide range of video applications, including copyright or content ownership protection, verification, transmission monitoring, fingerprinting, and plenty more. One of the most distinguishing features of video is the collecting of a series of still images. As a result, any picture watermarking approach can be used to videos. All of the strategies, methods, and algorithms used to incorporate motionless picture watermarks can be applied directly to genuine or compressed videos. Furthermore, video watermarking approaches must overcome additional obstacles since video watermarking solutions have consistent identifying qualities that do not present in picture or other multimedia watermarking strategies. As a result, such tactics will not yield fruitful video results. In contrast to images, there is a strong link amongst consecutive frames. This attribute makes sequence attacks more difficult because an attacker may employ techniques such as frame insertion, frame averaging, frame switching, frame substitute, and frame deletion to destroy important areas of the embedded watermark. Another feature is the video watermarking technique, which separates motion and stationary sections. For embedding, any one or the other might be utilised, but images do not have these features.

1.7 Objective of Research

The general public has been significantly transformed by the rapid growth of digital information technology. Due to the offering a broad range of multimedia technologies, digital data owners can now readily generate, manipulate, and store multimedia items. Furthermore, the rapid generation of effective internet bandwidth facilitates the transfer of multimedia documents with one machine to another in an acceptable amount of time, regardless of geographical location. However, these advantages have resulted in a slew of worrying difficulties and a slew of obstacles that must be addressed, as detailed below.

i. Because there is no discernible distinction between the genuine and copy digital multimedia video objects, unlike analogue data, an unauthorised user can generate flawless multiple copyrighted copies to fraudulently redistribute or exchange via the internet. As a result, industry businessmen may face significant financial losses. This poses the issue of devising a means for securing and protecting the copyright of the audiovisual item in question.

ii. Owing to the availability of a variety of video editing programmes like as morphing, Photoshop, and CorelDraw, video multimedia elements can be quickly manipulated without leaving any visible traces. As a result, there is still some doubt about the video's fulfilment. This poses the question of video integrity and verification.

1.8 Motivation of Research

The motivation of this study is to find a novel solution to the copyright laws for video sequences that is both resilient and unnoticeable. The main focus is on embedding a visual identity representing metadata in a video material so that the auxiliary information can be easily recovered and used to seek the copyright of the concern video. Because videos include large amounts of data, they must be compressed before being stored or transferred over the internet in order to reduce storage requirements and fulfil real-time requirements. As a result, the suggested study work not only concentrated on non-compressed domain video watermarking strategies, but also established compressed domain video watermarking approaches. Finally, the main focus is on securing video multimedia content using digital watermarking technology by examining their implementations and specifications, as there are still some problems to overcome.

1.9 Research Gap

With a qualitative research of watermarking in the uncompressed domain, the goal is to propose a novel approach in video watermarking technology. The study began with a basic understanding of information security issues and techniques for multimedia items. One of the conceivable ways for safeguarding such artifacts is the use of digital watermarking. In continuance, a thorough examination of the top of the line in uncompressed and compressed domain based digital video watermarking is conducted, with the conclusion that motion frame and encryption based approaches are better appropriate for a particular application and demand. However some of the major gap findings are as follows-

(i). Investigate the trade-off between the robustness of the watermarking algorithm and its impact on the perceptual quality of the video. Finding an optimal balance between robustness and imperceptibility is a common challenge.

(ii). Explore the development of adaptive watermarking techniques that dynamically adjust the embedding strength or strategy based on the content characteristics, ensuring optimal performance across various types of videos.

(iii). Develop techniques that adapt the watermarking process based on the motion characteristics of video frames. This can include strategies for handling fast motion, slow motion, and sudden changes in motion to improve overall performance.

(iv). Explore advanced encryption techniques to secure the embedded watermark, ensuring resistance against various attacks. Investigate how encryption impacts the computational complexity and overall efficiency of the watermarking algorithm.

1.10 Problem Statement

The design challenge is to embed copyright information in compressed or uncompressed video multimedia objects in a resilient and undetectable manner, so that when the embedded information can indeed be easily recovered by an authenticated users to verify the copyright of the concerned video multimedia object. And from the other hand, the method would be too secure for an unauthorized user to extort without considerably degrading the detection capability of watermarked video.

1.11 Organization of Thesis

Chapter 1 is related with the introductory part of Information security and its related issues. We started with the procedures for securing multimedia assets and worked our way through the many options for securing them. In addition, digital video watermarking is one of the most effective ways to protect the information encoded in the video. Even so, there are several drawbacks to this strategy, which are discussed in depth. Then we talk about why we want to do this job and what our goals are.

Chapter 2 deals with the literature study for digital video watermarking approaches was covered in this Chapter . The previous recommended systems were examined in this review section, with the video playing a prominent role as:Uncompressed video domain. Each domain is thoroughly investigated in order to identify any unsolved issues with digital watermarking.

Chapter 3 describes the methodoly used to work in the research area . This includes the various domain and approaches used to implement the proposed work.

Chapter 4 cover the algorithms proposed and implanted to design the secure watermarking methods over the video objects. This chapter covers the copyright issues can be resolved with digital video watermarking systems that take into account the source video. The strong Discrete Wavelet Transform (DWT) has been addressed in this scheme, as well as the approach that is based on it. This chapter evaluated the scheme's performance by measuring its robustness and other factors, as well as verifying the results by comparing the existing technique to the previously proposed ones. This chapter covers the outlined a video watermarking system that relied on obtaining motion frames from either the original video for watermarking. The watermarking method is strengthened by two powerful frequency transformations: Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD).

Chapter 5 states that the thesis research work was completed, and the experimental findings of the proposed methods were summarised. It also suggests the direction in which future work will be conducted.

CHAPTER 2
LITERATURE REVIEW

The literature on video watermarking produced in the previous couple of decades is covered in this review. The architecture of the host signal is used to classify the approaches and methods created for data concealing. Text, image, audio, and video are examples of host signals for multimedia objects. Many studies, comprising experimental, numerical, and analytical works, deal with the fundamentals of digital video watermarking. Others are concerned with various video watermarking applications. In a nutshell, the basic aim is to examine blind and non-blind watermarking algorithms for video streams in both compressed and uncompressed domains in order to identify the limitations and challenges of digital video watermarking.

Multimedia Multimedia-content protection, Multimedia-copy prevention, and Multimedia-copy restriction are all terms used to describe copyright protection. Multimedia Copyright protection is a pathway for preventing the regeneration of multimedia (images, video, or audio) for copyright reasons, where copyright is a legal right granted by the law to the holder or creator of creative content that allows the holder or creator of creative content to use and distribute it. There are a variety of copyright protection mechanisms that can be used to prohibit the replication of multimedia content. In today's digital and internet world, such a security measure is critical in not only preventing illicit duplication of digital media content, but also increasing the profit value for anyone who acquires an authorized version from of the content's official owner.

This chapter provides an overview of previous work in the disciplines of digital video watermarking and related fields. The ideas and procedures of digital watermarking, as well as the main assessment metrics of video watermarking, are provided in this chapter. As a literature study, various sections of this chapter examine a variety of watermarking approaches offered by diverse scholars.

2.1 Video Watermarking Review

According to previous research, video watermarking systems [7] are determined by the type of video signal, which can be compressed or uncompressed. As a result, the literature review process consists of two parts: compressed video signal and non-compressed video signal, as indicated. Each group is detailed based on two elements once more. The first factor was concerned with the sort of video signal utilized, while the second demonstrated the particular method. Every watermarking technique has advantages and disadvantages. Because video is believed to be a sequence of still photos, the same methods, systems, and algorithms that were used to insert the watermark for static uncompressed photographs were used to video as well. Video watermarking also has been done using these approaches. Similar techniques, on the other hand, are not suitable for video multimedia items because video objects include extra qualities such as redundant data, motion frames, and scene frames that are not included in images. A brief summary from each technique is given, followed by a full explanation of the functioning algorithm and any constraints that may exist. A quick summary is offered in statistical performance at the end of the section.

2.1.1 Review Based on Spatial Domain

Watermark bits are immediately inserted into the pixels of one or two essentially arbitrary parts of a frame in the spatial domain, and they are modified depending on perceptual analysis of video frames. For the insertion of the watermark object into the host signal, basic mathematical operations such as addition or replacement are performed. Least Significant Bit (LSB) and Spread Spectrum (SS) approaches are the greatest instances of video watermarking in the spatial domain. The LSB-based approach proposed a simple method for video watermarking in which the watermark bits are replaced with the least bit of each selected pixel, represented by 8 bits, of an image or video frame. Cayre et al. [8] translated the encrypted watermark into binary form, which they then inserted in the LSB position of each frame's selected pixels. The results of the experiments suggest that the watermark may be extracted satisfactorily with little computational effort. They did not, however, assess the other important characteristics, such as robustness. Another ground-breaking effort in uncompressed video watermarking is to treat the video signal as a single-dimensional signal [9]. The basic concept of spread spectrum technique for video watermarking was described by Chang et. al [10]. In opposition to transformation schemes, such a method is computationally efficient because no mathematical adjustments are used. Paul [11] described a blind video watermarking system based on the spread spectrum domain for both photos and video. The total number of pixels is represented by N, and the chip-rate used to distribute the material is indicated by R. The robustness is assessed using JPEG compression attacks, low pass filtering, rotation attacks, cropping attacks, and printing and reprovisioning assaults, according to the simulated data. There is one constraint stated by the author: if large amounts of distinct watermark copies are available to the attackers, the collusion attack may succeed in deleting them. Phin et al. [12] established a video watermarking system that takes into account the threat of frame collusion. Spatially localised and picture sensitive sub framed were presented as watermarking strategies for dealing with collusion attacks. The Type-1 collision attack and Type-2 collusion attack were both used to estimate the watermark in the experiments. The technique concluded that when only one frame is employed in the judgement process, the best estimate of the watermark may be obtained.

Galindo et al.[13] described video watermarking in the spatial domain using a visual cryptograph, and the simulation results showed that the technique is resistant to collusion. Other robustness difficulties that the approach overcomes include geometric attacks, frame swapping, frame deletion, and frame swapping. Digital video watermarking using the spread spectrum approach was also disclosed by Yang et al. [14]. Each watermark bit was modulated using a pseudo-random expansion sequence before being included in a large number of DC coefficients of a luminance DCT I-frame. Despite the fact that the watermarked video appears to be identical to the previous video, neither the sensory clarity nor the robustness were determined quantitatively (PSNR) (NC). Hameed et al. [15] illustrated a spread spectrum watermarking approach and claimed that the strategy is resistant to three types of assaults: temporal, spatial, and compression attacks. The outcomes of the investigation are divided into two categories. The first section contains the watermark extraction without any attacks, while the second section has the robustness results after implementing seven attacks. UEFISCSU, 2011 is funding this research[16]. In comparison to the transform domain, the spatial domain is simple to construct and has a low computing performance. Watermark bits are directly inserted into the host signal, which can potentially be damaged or even removed from watermarked video, making it less resistant to temporal and resynchronization attacks[17]. For example, an attacker might reorder all LSBs at arbitrary in order to entirely erase the watermark. As a result, it is a less preferred method of copyright protection for video.

2.1.2 Review based on Transform Based Methods

Cheddad et al. [18] suggested two video watermarking techniques, both of which are dependent on the Singular Value Decomposition algebraic transformation. The initial methods recommended that the watermark bit information is encoded in all three matrices of the illumination component(Y) of each frame, i.e. matrix U, S, and V. Watermark bits are included in a block of matrix U as well as in the matrix V in the second procedure. These two algorithms' abilities are compared in terms of robustness and payload. The first technique, which was based on diagonals, had better resilience findings, but the block-wise approaches had a greater data payload rate. The first algorithm's resilience is tested across four attacks. The first method is a JPEG compression attack, which yields better results when the watermark is put in the S matrix rather than the U or V matrix. When watermark is retrieved from the first algorithm in the V-matrix, the approach delivers higher robustness results from different angles versus video angular rotation kind of attack than S or U matrices. In the attached watermark video, two types of noises (Gaussian and Salt and Pepper Noise) are also introduced to test the robustness of both the watermark technique, and the V and U matrices both produce better results than the diagonal matrix S. Additional type of attack is frame dropping: while extracting the watermark in S matrix after dropping 60% of the frames, the numerical simulations generated a higher correlation value than when recovering the watermark in U and V matrices. Similarly, the robustness of both algorithms is tested against frame swapping and frame averaging, and the outcomes are nearly identical. The benefit of using the second technique is that it has a bigger payload capacity than the first approach. Because the two methods satisfy two distinct features of the watermarking system, every technique has its own set of benefits. The sole shortcoming is that none of the algorithms addressed the issue of visibility.

Walker [19] suggested an SVD-based real-time watermarking technique. The watermark was implanted by powering it to factor alpha and applying SVD on the luminance components of the video. The inverse embedding approach was used to extract the data. As the alpha factor rises, so does the performance. Six video sequences are used in this experiment. Experiments were carried out to assess the strength of the system against MPEG-4 and MPEG-2 compression attacks. The watermarked video is also subjected to other robustness difficulties such as frame resizing, rotating, and averaging attack. The disadvantages of this technique are that it is operationally expensive when compared to Fourier transform work and that it is not suitable for evolutionary algorithms because it uses a fixed size matrix. To satisfy the imperceptibility and robustness requirement, most SVD-based watermarking algorithms add the singular values of watermark information to the singular values of host signal. However, combining SVD approaches with other transformations mentioned in the same section would yield significantly different performance.

PCA is a strong tool for analyzing and recognizing data samples. Principal component analysis [20] is a computational method for transforming a large number of possibly linked smaller set of uncorrelated. Principal components are the small communities of uncorrelated variables. The principle component analysis lowers the number of dimensions in a data collection. That the very first principal component is recovered using the PCA technique, which involves creating a whole new coordinate to depict the information where its biggest energy concentration is produced, i.e. information with the highest covariance. The second principle component, as well as the third and fourth principal components and so on, can be derived using the second higher covariance. An other major benefit of PCA is that once these data values are known, the data may be compacted by reducing the number of dimensions without losing much information. Ahuja et al. [21] used principal component analysis to twist digital video watermarking. There are three colour channels in the original frame: red, green, and blue. Each of the colour band frames is then subdivided into a number of equal-sized blocks. Then, in each of the subblocks, use the PCA function to generate three PCA components: YR, YG, and YB. Finally, the watermark is inserted by selecting the perceptually relevant components from each of three components. Ultimately, the watermarked frame is created by mixing the three colour channels after using the inverse PCA. To obtain watermarked video, the process is repeated for all frames. Because the estimated variables are a concatenation of the actual variables, PCA makes it difficult to calculate the correct meaning of main component data. Another restriction is to set the ‘mean' to zero and the variance to one. If PCA is paired with another transformation scheme, such as SVD, it would almost likely provide better results than if PCA is used alone to solve watermarking techniques.

A host signal can be divided into distinct frequency bands using the Discrete Cosine Transform (DCT) [22] domain. The aggregate content of an image is represented by the very first pixel (DC coefficient) of a DCT image, while the remainder pixels are known as AC coefficients. Low frequency coefficients are AC coefficients close to the DC component, while high frequency components are the rest of the pixels. It represents a finite sequence of data points as a summation of cosine functions swinging at different frequencies. In principle, the original data is separated into 8x8 blocks of pixels, with each block receiving its own 2-D DCT operation. DCT-based watermarking was first employed for input images, but it was later expanded to video sequences. DCT-based blind digital video watermarking was proposed by Sakib et al. [23]. The Y component is taken from the randomly picked frames, and 16x16 blocks are created using the DCT. The watermarks are embedded using the DCT blocks' low pass DC coefficients. The watermark is recovered by comparing the absolute values of the low frequency DC coefficient units to the DC value of the underlying watermark. The embedding approach suggested by Sharma et al. [24] is divided into two sections. The video sequence is divided into segments and translated into the (u, v, z) domain using the spatial 2-D DCT transform in the first part. In the temporal dimension, the output is followed by a DFT transform. Watermark information is integrated in the transform coefficients in the second phase by modifying one of the arbitrarily chosen coefficient pairs. The outcomes of the experiment are divided into four categories: Case 1: Equal Watermark Energy Insertion in the Face of Various Assaults, Case 2: Abilities in the Face of Various Attacks, Case 3: Equal BER during recovery for compressed attacks, and Case 4: Capacity in the Face of Various Attacks The video watermarking predicated on DCT was described by Ibrahim et al. [25]. For the aim of embedding, three separate types are used. (a) Algorithm for integrating audio as an undetectable watermark (b) Method for integrating image as an unseen watermark are the two types. (c) Algorithm for embedding video as a watermark that is not apparent. For each of the three categories of digital video watermarking, the DCT of the watermark image is assessed and added to the DCT of the recovered component of R, G, and B separately. Adhikari [26] suggested a digital video watermarking approach based on psedo 3D DCT, which involves performing the DCT transformation twice and uncompressed quantization index modulation (QIM). Every 20 frames, a watermark is placed. They use three videos in their presentation. The goal is to simulate something. A wide range of planned and incidental attacks have been used to test the robustness. PSNR, but at the other hand, has been tested with several watermarks of various sizes. The approach of digital video watermarking predicated on DCT with and without HVS was also proposed by Lufang Taweel et al. [27]. The watermark is incorporated through into video without HVS in the first scenario, utilising the steady intensity 30 and 8 independently. Second, utilising the steady strength, the embedding positions are based on the HVS. Inter-frame assault, cut attack, generalized stabilization attack (including such noise attack, filter attack, re-sampling, etc.) and JPEG compression attack are all assessed by the technique. Rajurkar [28] proposed a digital video watermarking strategy based on the human visual system features. The watermark is perceptually added in the Discrete Cosine Transform (DCT) domain. It's also compatible with the Moving Picture Experts Group (MPEG) compression standard. The watermark is unobtrusive and unaffected by video reduction. The straightforward way to incorporate the watermark into in the host signal was proposed by Singh [29]. The spatial watermark bits are first converted to the frequency domain and used the DCT domain before being effectively appended to the coefficients of video frames. Global geometric attacks such as cropping, scaling, and rotation are used to assess the robustness. According to the research, future research will focus on improving DCT-based watermarking, which may be compared to existing systems. Furthermore, the same approach might be implemented using the Discrete Wavelet Transform (DWT), which is a reasonably advanced image processing tool with interesting characteristics. One of the most significant drawbacks of the DCT method is that it generates real values then after processing blocks of the same size. To convert real numbers to integer values, an additional quantization step is required. Another disadvantage of DCT is that the image may be warped as a result of the greater compression ratio, causing the image to look as oddly huge pixel chunks. The misleading contouring effects are another limitation. This is owing to the transform coefficients' profound quantization.

Due to its multi-resolution properties, the discrete wavelet transform (DWT) [30] is the most popular and commonly utilised transformation technique in digital image processing applications. Wavelet transforms breakdown a video frame into four non-overlapping multi-resolution sub-bands (LL, LH, HL, and HH) that may be reconstructed without mistake to recreate the original frame. The lower grade frequency DWT coefficients, also known as coarse-scale decomposition, are represented by the sub-band LL, while the middle level frequency is represented by LH and HL, high frequency is represented by HH, and the finescale of DWT coefficients is represented by LH, HL, and HH. Shanmugam [31] proposed video watermarking that was scene and video dependant. To disguise an invisible watermark, spatial masking, frequency masking, and temporal characteristics are used. The static and dynamic spatiotemporal components of the video scenes produced by the temporal wavelet transform comprise the mystery data. Currently, the video frames' wavelet coefficients are modified via a perceptually structured pseudorandom sequence. To prevent illegal removal and solve the stalemate problem, a Watermark is mathematically undetectable. The multi-resolution watermark may be recognised if the positioning of the frames in video sequences is unknown. The DWT is well suited to identifying places in the cover image at which a watermark can be efficiently placed due to its outstanding spatio-frequency localization properties. Because the considerable amount of energy is concentrated in the lower sub-bands (LLx), watermarks embedded in these sub-bands may considerably damage the image. However, it has the potential to improve robustness. The edges and roughness of the image, on the other hand, are included in the high frequency sub-bands HHx, and the human visual system is generally responsive to fluctuations in such bands. This function makes it possible to incorporate the watermark without it being visible to the naked eye. A blind video watermarking method based on DWT with larger payload capacity was described by

Kothari [31]. Geometric attacks such as shift, rotation, scaling, and cropping are used to determine the strength. Meenaksh et. al [33] developed a revolutionary idea for video watermarking in which a genetic algorithm is paired with a DWT domain. There have been included certain common attacks such as median noise signal and lossy compression, as well as video-specific techniques including frame dropping and frame averaging. Based on scene change assessment and error checking codes, Patil [34] presented a hybrid digital watermarking system. A watermark is divided into separate pieces and placed in matching frames of various scenes in the original video in a scene based watermarking method. The approach is resistant to frame averaging, dropping, swapping, and statistical analysis attacks because to this mechanism. However, the technique is vulnerable to image processing attacks. As a result, a new way to improving the performance of the watermarking system is offered. Visible audio hybrid watermarking system and hybrid model using different watermarking scene are two of these techniques. Combined video and audio watermarks were added to the video stream in the visual-audio hybrid watermarking approach. Error-correcting codes were retrieved from the watermarked video and applied to the audio stream as a watermark. It provides a stand-alone method for embedding error-correcting codes that provide additional details for watermark extraction. The technique is more robust than previous schemes that rely solely on video channels. Another strategy is divided into two categories. The first is 'various schemes for different situations,' and the second is 'different schemes for different areas of each frame,' respectively. A watermark is divided into multiple sections implanted in the appropriate frames of various scenes in the first scenario. When a watermarked video is assaulted, only one section of the watermark is affected. The downside of this approach is that the extracted watermark's accuracy is lower than that of other schemes. 'Distinct schemes for different areas of each frame' was another technique wherein four distinct watermarking strategies were performed to each frame. Each video frame is separated into four pieces, and each frame's watermark is broken into four parts as well. Finally, each component of the watermark was implanted in frames from various domains. Ahmad [35] proposed an efficient architecture for picture and video watermarking based on 2-D Scan. The purpose of this work is to protect the information of a video frames for High Definition Television broadcast monitoring (HDTV). It also has DVD protection and access control.

The watermarking approach was created to make use of a specific insertion technique to enhance video content hardware implementation. During the extraction of the watermark, the algorithm did not involve the original video.

Elashry et al. [36] suggested a 3D-DWT and Artificial Neural Network-based approach (ANN). The averaged frame of the video taken is first processed, and then the frame is sent via the wavelet domain. The low-frequency sub-band (LL) is separated into 33 non-covering blocks that have a connection between the block's centre, mean eight neighbours, and standard error. The inputs are the neighbor's mean and standard deviation, and the output is the centre of each block. The watermark is recovered using statistical parameters of coefficients in the extraction step; this approach is not completely blind, but it does require a large amount of original data to recognize the watermark sequence. Khan et al. [37] used a DWT-based blind video watermarking technique to safeguard the owner's copyright and prevent illicit duplication. Different chunks of the garbled watermark bits were suggested to be inserted into different scenes of the video by the algorithm. Frame dropping, frame, frame averaging, cropping, noise addition, median filtering, and lossy compression are all used to test the resilience. By quantizing the wavelet coefficient of the LH, HL, and HH sub-bands of the second wavelet decomposition level, Nouiua et al. [38] incorporated the watermark. Using a cryptographic key, each bit of the watermark was placed over a variety of wavelet coefficients. The watermarking algorithm's resiliency was tested against a sequence of nine different attacks using different videos. By redundantly embedding the same watermark in different frames and using an error correction code, the approach enhanced the processing bit error rate (BER). Adding Gaussian noise with a mean of 0 and a variance of 0.05, blurring with 2 x 2 pixel blocks, boosting each pixel's luminance, and Median filtering with a 3x3 pixel neighbor. The imbedded watermark is undetectable and resistant to attack, according to their findings. The suggested technique demonstrates good resistance in the face of a variety of attacks in the spatial, temporal, and compression domains. The algorithm's performance is increased by employing error-correcting codes and embedding the very same watermark many times from different frames of the movie. Purnima [39] presented a wavelet transformation-based approach. The motion part of a colour video is first detected using scene change analysis, and then the discrete wavelet transformation is applied up to the third level of decomposition, with the coefficients of HH, LH, and HH chosen. Finally, the watermark was embedded into the specified coefficients using the spread spectrum approach. The key feature of this technique is that it does not require the source video to extract the watermark. Several video-specific attacks, such as frame averaging, frame dropping, and frame swapping, as well as image processing assaults, such as filtering, insertion of impulsive noise, MPEG-2, and H.264 compression, are used to assess performance.

Kadian [40] proposed a geometrically insensitive blind watermarking technique. Under the wavelet domain, their technique explains the various components of a single watermark embedded in multiple views of a movie. To identify the watermark to the motion including coefficient, a multi-resolution motion estimate (MRME) is applied. The use of a watermark is less noticeable, according to test results. The embedding process can be broken down into three parts. The first step is to choose the embedding zones and determine the motion and detail detection techniques. The frames' middle-frequency wavelet coefficients are chosen to embed information. Described the watermark embedding strategy in the second step. The network trainer is employed in the final step of the wavelet embedding process.

The video watermarking system described by P.P [41] is composed of three specifications: visual cryptography, scene change detection, and discrete wavelet transform. The proposed scheme suggested embedding different segments of a single watermark into different scenes for generating the owner's part from the original video predicated on the frame mean and generating the identification ability to contribute based on the frame mean of the probably attacked video, i.e. their approach uses an identical sub-watermark for subsequent images in the same scene but different parts in different scenes. After being bundled, these two shares reflect copyright ownership. Eight video sequences are cascaded to conduct the experimental investigation. Each frame has a resolution of 352 × 288 pixels, and the total number of frames in the image sequences is 2400. Several video-specific attacks, such as frame averaging, frame dropping, and frame swapping, as well as image-processing techniques, such as filtering, injection of impulsive noise, compression, blurring, sharpening, scaling, and rotation, are used to assess resilience. By comparing it to the state of the art, they were able to achieve greater results. This method is effective since it identifies ownership without the use of current host video. This algorithm's security is based on a hidden failure that makes it impossible to recover the hidden identification share.

Doerr [42] investigated the digital video watermarking system in order to test the hypothesis below. The first is to approve the video by successfully extracting the watermark despite numerous image processing and video-specific attacks. The third option is to deny a video if the watermark is missing. The parameters used were to construct the hypothesis that a high resemblance indicates the presence of a watermark (H0), while a low similarity indicates the absence of a watermark (H1) (H1). Watermark detection in the context of other watermarks is a specialty. Mahesh et al.[40] used the 3-D wavelet transform to describe digital video watermarking. For robustness evaluation, an MPEG compression attack is used, and the results are compared to the state of the art.

The DWT-based robust, scene change blind digital video watermarking was proposed by Arun [43]. The technique was constructed in such a way that many sections of a single watermark could be formed and implanted into distinct scenes of a video. Geometric assaults, median filter attacks, picture augmentation attacks, and video-specific unintentional and intentional attacks are all included in the sturdiness calculation. George et al.[44] suggested a strong blind digital video watermarking system based on DWT decomposed to four layers. The algorithm's distinctive aspect is that the watermark is a coloured video. They found that PSNR values between 31 and 44 dB correspond to acceptable perceptibility. The video watermarking approach was presented by Kundur [45], wherein the watermark is inserted in the motion areas. Watermarking is done with the HL and LH bands. The strategy was put to the test to see if it could withstand frame dropping, adaptive quantization, and frame filtering attacks.

Houmansadr [46] implemented the HVS model in the DWT domain, resulting in successful outcomes in terms of invisibility and resilience. The video watermarking based on 2 level DWT was described by Wei [47] the film provided the video sequence clip for fixing the dispute of copyright protection. Robustenss was tested with three different attacks: rotation, cropping, and Gaussian noise.

The cost of computing with DWT based video watermarking is always higher than with DCT domain based watermarking. Furthermore, processing bigger DWT kernel function or wavelet filters in video frames almost always results in blurred and noisy regions towards the borders.

Preda [48] proposed a wavelet-based blind video watermarking technique. The motion part of the colour video is recognized using scene change analysis, and the three-level 3D wavelet decomposition is used to produce the HH, LH, and HH.

Finally, they incorporate the watermark into the chosen coefficient using spread spectrum techniques. Various video-specific assaults, such as frame averaging, frame dropping, and frame switching, are used to assess performance. Some video-specific attacks are not examined in this approach. Rajab [49] presented a 3-Level DWT-based digital video watermarking approach based on comparable frame extraction. The watermark is implanted in the similar frame that is selected from each video shot once the original video is divided into video shots. The frames are subjected to a three-level DWT, with the upper sub-band being employed to hide the watermark. Perceptual invisibility is improved when the watermark is adaptively hidden in the wavelet coefficients. Simply compare the threshold value from the embedded watermark signal with the correlation values between both the watermark signal and the watermarked video to obtain the watermark on the receiver side. According to Chen [50] , video watermarking techniques based on picture interlacing minimise the original data while double the communications capacity. The watermark is embedded and extracted using a three-level discrete wavelet transform (DWT) in this method. The Arnold transform is used to encrypt or decrypt many sorts of watermarks. System resources, memory capacity, and connection bandwidth were all saved as a result of the simulation results.

2.1.3 Review based on Hybrid Approach

Although each conversion system has its own set of characteristics and is quite strong, it also has some restrictions. As a result, combining two or more transformation schemes, defined as a hybrid approach, is offered as a way to overcome the limitations and boost the watermarking system. When many transformation techniques are combined, greater results can be attained. Every transformation may result in positive qualities, however in some circumstances, the features are appropriate based on the goal. As a result, the researchers have the option of switching to a hybrid strategy[51]. Combining multiple transformation techniques delivers benefits as well as increased robustness. Below is a list of video watermarking methods that use a hybrid technique.

Singular value decomposition (SVD) and 2D principal component analysis (2DPCA) were both used by Chawla [52] to define the digital video watermarking technique. The SVD approach is used for watermarking in the spatial domain, while PCA is used in the time domain. Hou [53] offered the work to develop a blind digital video watermarking technique that is effective. The algorithm's utility is demonstrated by the use of two demanding mathematical transforms: the first is singular value decomposition (SVD), and the second is discrete wavelet transform. The following are the better results for assessing the robustness against various image-specific attacks: In comparison to the findings provided, JPEG compression, rotation, Gaussian and Salt & Pepper attacks, as well as video-specific attacks such frame dropping, frame swapping, and frame averaging were used. Liu et al. [54] proposed a binary logo hybrid video watermarking system. Each video frame is subjected to DWT, but every block of the LL and HH subband video frames is subjected to PCA. The watermark information is embedded in multiple ways using the principal components of the LL and HH blocks. The suggested method's performance is improved by merging two transformations; results reveal that now the difference between the traditional and watermarked frames is very small, and comparing the two frames is difficult[55]. Deshpandey [56] propose a blind video watermarking system based on Zernike moments and singular value decomposition (SVD). The brightness component of the original frame is sub-band decomposed using discrete wavelets transform (DWT), and the lowfrequency sections are decomposed using singular value decomposition. Finally, the secret image is hidden by changing the maximum singular value. The probable rotation attacks are compensated in detection using Zernike moments, and it is resilient against rotation attacks of any angle. Huang [57] described a geometrically insensitive video watermarking technique. Under the wavelet domain, the approach embeds different sections of a single watermark into different shots of a video. To distribute the watermark to all those coefficients that include motion, a multi resolution motion estimation (MRME) is used[58]. Furthermore, the watermark's embedding and extraction are predicated on the connection between such a coefficient and its neighboring. The watermark is less noticeable when inserted in a moving image, according to test results. The embedding procedure is divided into three stages. The motion detection algorithms are chosen in the first phase, and the watermark embedding strategy is demonstrated by utilizing only the frames' mid - frequency wavelet coefficients in the second step[59]. The final stage is to train the wavelet network that will be employed by the watermarking system. Several experiments were conducted to assess the effectiveness of the video watermarking technique. Frame shifting, cropping, scaling, rotation, and changing the aspect ratio are all examples of this. PSNR is used to determine whether visual watermarked data is of acceptable quality[60]. Rotation, resizing, and cropping attacks are all used to determine resilience. Burrus [61] uses scene change analysis to repeatedly embed the watermark into singular values of precise mathematical tensors generated from the DWT coefficient of chosen frames from each scene. In comparison to prior systems, the experimental results reveal that perceived transparency and robustness against typical attacks such as scaling, frame dropping, and frame averaging has improved.

Percival [62] presented a hybrid technique to non-blind video watermarking based on DWT and SVD. The watermark is embedded into absolute values of higher tensors generated from the DWT coefficients of picked frames of each scene.The efficiency of the proposed strategies in terms of perceived invisibility and robustness against attacks is demonstrated by experimental data on video sequences. Video watermarking using multi-resolution singular value decomposition was presented by Swanson et al. [63]. MR-SVD is used to create the geographical characteristics matrix of parameters for each frame. Furthermore, the temporal decomposition has halted this matrix. Transform the watermark bits to 1 and -1 before embedding them in the target matrix. Filtering, compression, collusion, and noise attacks are all examples of attacks that can be used to test robustness[64]. In addition, various video-specific attacks were used. A thorough approach for watermarking digital video was proposed by Yang et al. [65]. It uses a hybrid digital video watermarking approach that combines two strong transformations: the

Discrete Wavelet Transform (DWT) and Principal Component Analysis (PCA). After applying DWT to the video frames, the binary watermark is encoded in the principal components of the low frequency wavelet coefficients[66]. Filtering, contrast adjustment, noise addition, and geometric attacks are all resistant to the invisible implanted watermark. Three robust and semi-blind digital video watermarking techniques were given by Karmani [67]. These algorithms are based on hybrid transforms, which use an amalgamation of Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) techniques, as well as a combination of all three, i.e. Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD) (SVD). The original version is segmented into a number of frames in this example. On a single frame, all three hybrid transformation techniques were used, and the process was repeated for the remaining frames[68]. The effectiveness of the these algorithms was assessed using in terms of imperceptibility and toughness. CKR [69] developed a novel non-blind way for implementing temper detection and identification in order to input digital watermark in the side view, which differs from prior suggested schemes' regular procedures. The video sources of the frames are modified in the first step. Second, a grey scale picture is inserted on the luminance (Y) of YUV encoded video using the DWT-SVD method[70].

For incorporating a binary watermark into digital video frames, Amiri [71] suggested an undetectable and robust hybrid video watermarking approach. First, each video frame is subjected to DWT, and then each block of the two bands, LL and HH, is subjected to PCA. The watermark is incorporated into the LL and HH blocks' primary components. Various assaults such as Gamma Correction, automated Equalizer, contrast adjustment attack, geometric attack (Cropping, rotation), resize attack, JPEG compression attack, and MPEG compression attack are used to test the robustness of the NC[72]. Two digital video watermarking systems were described by Singh [73]. To implant the coloured watermark information, the first approach uses the LSB of the blue component of each pixel of each block derived from the Y component of each frame. The next algorithm is made up of four integrated circuits (ICs) (8:1 MUX). Intentional attacks such as frame dropping, frame averaging, and frame shifting are used to assess durability. The hybrid watermarking approach for Creative Commons Licence (CCL) applied video contents was described by Lee et al. [74]. Two watermarks are placed into the video frames: a robust and a fragile watermark. Six video clips were used to assess the scheme's effectiveness. A acceptable PSNR is obtained to test the fidelity. The robustness of the system is also successfully evaluated after four different forms of attacks are used. Finally, the experimental findings were used to compute the fragility test, which was used to determine whether the target video had been changed for geometric attacks such as cropping and scaling, as well as for frame-rate testing[75]. Rajab [76] used two powerful transformations, two level DWT and Principal Component Analysis, to implement video watermarking (PCA). The technique was tested using a variety of video sequences. Robustness is tested using Histogram equalisation, Gaussian attack, intensity adjustment attack, JPEG compression, resize, cropping, and rotation attack, however no frame specific assault is created[77].

Hussein [78] proposed a blind digital video watermarking method based on a hybrid system combining the Discrete Wavelet Transform (DWT) and the real Schur Decomposition. The resulting blocks upper triangular matrix contains a binary watermark bit, and this technique shown that the efficiency value is increased due to the Schur decomposition, and DWT takes the risks of high imperceptibility. After embedding, the watermarked video shows no signs of degradation. Furthermore, the approach is resistant to a variety of standard attacks. Blindness and payload capacity were obtained using techniques. Abdulfateh [79] described a DWT and PCA-based digital video watermarking technique. Every video frame is first subjected to a three-level DWT, after which the stochastic blocks are selected and processed using PCA. Blocks of the PCA are quantized using the Quantization Index Modulation (QIM) maximum coefficients of the subbands. To hide the watermark, several kinds of blocks are used[80]. The secret key is created when the watermark is inserted, and it is utilised to retrieve the watermark in this method. Masoumi [81] presented a hybrid solution to video watermarking that combined DWT and SVD. The experiment's findings focused on the issues of robustness and perceptibility. Using two separate grey scale pictures, logo.tif and cameraman.tif, the experiment was repeated twice. By achieving the correlation coefficient (CC) and PSNR following the initial attacks, the performance is almost good and fair. The digital video watermarking system based on DWT and SVT was proposed by Tabassum [82]. Different assaults, such as Gaussian noise, Poisson noise, Salt and pepper noise, blurring, frame averaging, and rotation attacks, are used to assess robustness. For the protection of 3D videos, Nanmaran et al. [83] presented a watermarking technique. The master share is created using this process, and it is made up of representative photos from the video. The owner shares are then formed depending on the user and master share's copyright information. Those exchanges are based on the Visual Secret Sharing method, which keeps track of users' copyright information[84]. The benefit of this technology was that it protected against deformation and was resistant to video processing attacks. Rotation and cropping attacks had no effect on this method.

For giving protection to the copy right, Nadesh et al. [85] proposed visual cryptography with scene change detection based video watermarking technology. The DWT was applied to the video source. Different elements of a certain watermark were put into scenes in different ways. The frame mean of accessible frames inside a scene was used to calculate the owner share. The recognition share was then calculated using the frame mean of the assaulted video as a starting point[86]. This approach could withstand attacks such as impulse noise, Gaussian noise injection, cropping, compression, filtering, blurring, gamma correction, and video processing. The video watermarking approach presented by Nicolas et al. [87] is based on both the spatial and frequency domains. Dual watermarks were put in the video as part of the strategy. A visible binary watermark is embedded in the spatial component of video frames, whereas another unseen binary watermark is embedded in the DCT frequency component. In this way, it accomplishes two goals: it protects both public and private watermarking in same scheme[88]. After performing several attacks such as blurring, scaling, average filtering, sharpening, and Gaussian filtering, robustness is determined. Abdallah[89] demonstrated a DWT-based SVD video watermarking approach in which the video frames are converted using the DWT utilising two-level decomposition. The frequency bands LH, HL, and HH are undergoing SVD transformation, and there is a concealed watermark in it. The suggested method is distinguished by the use of an additive method to apply a cascade of DWT-based SVDs to the frame and disguise the watermark with spatial and temporal consistency. This method improves the watermark's resistance against video processing assaults, achieves a high level of security, protects the watermark from bit errors, and provides good perceptual quality. Chaudhary [90] proposed a video security approach based on feature transforms. The side plane was used to identify the scene in the video. The SIFT characteristics were created based on the altered pixel intensity of the source video in this technique, which detected the embedding position. Scaling, temporal, and frame dropping were not an issue with this strategy.

Omidyeganeh et al.[91] suggested a digital video watermarking approach based on implementing GOP with a quantization algorithm to insert the binary watermark on the low frequency coefficients of wavelet sub-bands. The method is put to the test against a number of different types of attacks. Temporal attacks, image analysis unintended attacks, such as high contrast, geometric attacks, compression attacks, and noise insertion attacks are among the categories. Certainly, the investigator achieved better results with the hybrid approach than with the independent transformation system, but all of the above approaches fail when a real-time environment is involved, i.e. video data, whether it is a movie, a video conferencing operation, broadcast tracking, or any other video, contains large amounts of data, measured in gigabytes[92][93]. This becomes a necessary need that vast amounts of data be compressed prior before being transferred over the network. As a result, it is recommended that the watermark be embedded either during or after reduction using a reduction technology such as MPEG2, MPEG4, or any other. Finally, the investigator switched to compressed domain to address both compression and watermarking difficulties in a single approach to accommodate real-time video. Geetamma et al. [94] proposed a video watermarking method that uses a fuzzy inference system and a neural network. The payload, robustness, and imperceptibility are the major focuses of this methodology. The weighted matrix was inserted into the complete frames accessible in the video using the Bi-directional Associative Memory as a neural network. The DWT was applied to the host video, with embedding taking place in the middle band of all (Y,Cb,Cr) elements with distinct thresholds[95]. The various threshold values were generated using a fuzzy inference algorithm based on luminance, frame edge values, and texture properties. For many assaults, this approach excels in terms of resilience and imperceptibility. Das et al. [96] proposed a contourlet and SIFT transform-based dual watermarking technique. The watermarking procedure takes into account the low and high frequency bands. To avoid geometric attacks, the SIFT transform was used. The size ratio between both the histogram coefficients of the LL sub band was the first watermark. The highest energy level of the high frequency band was used for the watermark embedding process in the second step. Image segmentation and geometrical attacks were both resistant to this strategy[97]. The copyright owners are clearly driven to use video watermarking techniques to protect their rights, as seen by the negative evaluation. In comparison to the spatial domain, the transform domain is more resilient, and researchers have explored potential research avenues to boost the effectiveness of DCT, DWT, and hybrid video watermarking systems[98] . Some of the techniques in the survey used compressed video, but there is still a potential that the watermark will be lost if the compression standard is chosen incorrectly. To improve the procedure of video watermarking, more rigorous investigation and unique algorithms are required. This study focuses on non-blind watermarking approaches for uncompressed video sequences with colour watermarks, as well as extending our techniques to multiple watermarks[99].

CHAPTER 3

METHODOLOGY USED

3.1 Digital Media

Images, audio, video, time-series, conceptual patterns, and data streams are all examples of digital media . However, in this thesis, we are solely concerned with visuals.

3.1.1 Images and Video

A digital image is a matrix of intensity values represented numerically. These are made up of pixels from an image. Each pixel represents the brightness value of a single point with the coordinates (x, y). A typical depiction of a digital image is shown in Fig.3.1 . Digital equipment can be used to capture, store, and modify images. A bitmap is a rectangular array of pixels with headers that run the length of the image. Grayscale coloured and binary images are the two types of images. A grayscale bitmap would be one in which all pixels have intensity values ranging from 0-255[100]. A binary bitmap, but in the other hand, contains only two variables for all pixels: 0 and 1. A colourful picture bitmap is one in which each pixels are specified by three-byte intensity standards.

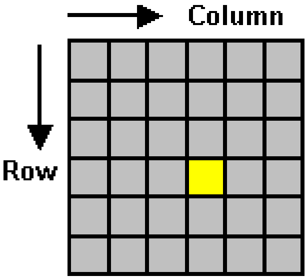

Figure 3.1: Matrix Form of an Image

A video is seen as a collection of frames. A example depiction of a movie is shown in Fig.3.2 . It comes in both uncompressed and compressed versions. Uncompressed video is untreated footage that has not been pre-processed before being stored. It is, nevertheless, of substantially higher quality than the compressed version [101]. It does, however, have storage difficulties. This is especially true for uncompressed video formats, which need a lot of RAM.

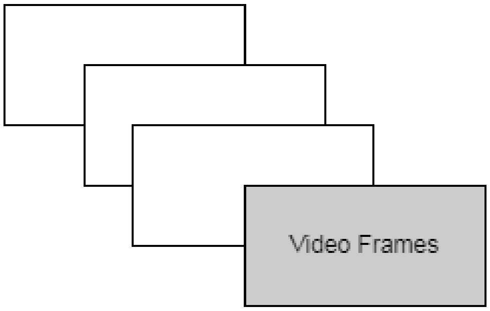

Figure 3.2: Sequence of Video

MPEG compression is commonly used for video and motion images. In an MPEG-2 video device, three forms of illustrative frames are detailed, as seen in Fig. 3.3.

Those frames are as follows-

- I-frames , those are intra image frames
- P-frame which are advanced predict frame
- B-frames, the bidirectional frames.

I	B	B	P	B	B	P	B	B	P

Figure 3.3: MPEG frames

An I-frame is one that is not connected to any other frames. P-frame is a type of prediction that leverages the prior I-frame or P-frame for mobility. B-frame delivers the highest compression quality by using prediction and subsequent I-frames or P-frames for motion correction. A block in frames can be predicted by combining a few different blocks from the previous or future grid points, or by averaged two blocks.

3.2 Discrete Wavelet Transform

Wavelet analysis is a representation of a signal on a time or space axis. Wavelet applications have been discovered in the domains of physics and mathematics, processing related with signal ,over the last few years.

Wavelets are mathematical tools that divide data into so many frequency components and investigate single constituent with a decision proportional to its scale. When matched with traditional Fourier approaches, it is more useful in analysing real-world scenarios with sharp spikes in the signals. Inside the fields of mathematics, particle physics, engineering, and seismic geology, wavelets were conceived autonomously. Wavelets attract scientists and engineers from several fields due to their transdisciplinary origins. Wavelet families were studied, as well as scale-varying essential systems, the continuous wavelet transform (CoWT), the discrete wavelet transform (DWT), the fast wavelet transform, adapted waveforms, time frequency placement, and the construction of doc wavelets[101] . Wavelets have recently emerged as a helpful and often crucial a mathematical instrument for signal analysis in the physics and engineering disciplines, thanks to recent improvements. Interactions across these fields, as well as more accurate advances over the last 10 years, have resulted in a slew of new wavelet applications, such as picture compression and current portrayals of fluid mechanics, such as turbulence. They are also used in computational imaging and have grown more important in the domain of storage and retrieval. Students will be instructed on a variety of applications utilising the Matlab wavelet package in seminars and assignments, which will cover a variety of scientific areas. Because of it has a better spatial arrangement localized and multi-resolution properties, which are akin to theoretical frameworks of the visual system in humans, DWT has been frequently used in digital picture watermarking[102]. Watermarking techniques that operate in the wavelet transform domain have received a lot of attention in the watermark research community as a result of the JPEG-2000 validation process and the move from DCT to wavelet-based image compression approaches. The advantages of employing the wavelet transform domain involve (i) the technique's intrinsic resistance toattacke related with lossy compression, and (ii) the ability to reduce calculation time by embedding watermarks inside a JPEG-2000 encoder. Some wavelet transform features are most often used in watermarking solutions. For example, quite robust watermark identification methods were developed using the wavelet transform's multi-resolution characterization of images, in which the watermark detection begins with the low-resolution sub-bands and, if that fails, moves on to the high-resolution sub-bands and supplementary coefficients it delivers[103]. Amongst some of the transforms, discrete wavelet transform (DWT) based watermarking strategies are becoming more widely known, owing to DWT's many advantages over other transforms, such as transmission with a low bit rate and in a progressive manner, product manageability, and territory (ROI) coding, which require more competent and adaptable image coding that can be used for applications for image reduction and watermarking. The DWT-based watermarking method embeds a spread spectrum watermark significantly within the DWT coefficients. DWT has proven to be effective in a variety of image processing tasks, including noise reduction, edge recognition, and compression. The signal is sent through a number of high-pass filters, also known as wavelet functions, and a series of low-pass filters, also known as scaling functions, to determine the maximum and minimum frequencies, respectively. Its significance stems from the way it connects discrete-time filters with continuous-time multiresolution. The public engagement of DWT in the conversion of a picture from the spatial and frequency domain is inspired by its computation efficiency. DWT has been used for watermarking digital photos by several researchers in the literature[104].

The actual image is segmented into four frequency sub bands called LL, HL, LH, and HH by a primary level DWT (Fig. 3.4). The lower resolution approximation factor is denoted by LL, while the horizontal, vertical, and diagonal detail components are denoted by HL, LH, and HH, accordingly. The LL band can be divided into four frequency sub-bands [5]. To obtain n-Level DWT, the procedure can be repeated many times (say, n). Watermarks are usually embedded in LL sub-bands acquired after n-degree DWT because this area denotes a high-energy zone to which the human eye is less sensitive.

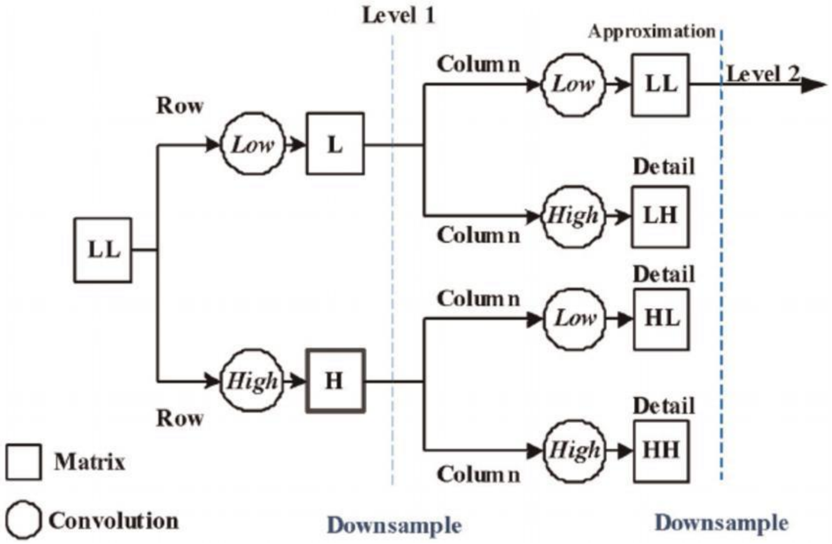

Figure 3.4: Discrete Wavelet Transform

According to studies, every one of those channels seems to have a bandwidth of about one octave. A multi-resolution deconstruction, on the other hand, divides the image in form of bands of roughly on a logarithmic scale, equivalent bandwidth[105]. As a result, it is predicted that the discrete wavelet transform will allow autonomous exploitation of the generated components with minimal observable involvement. In the three-level discrete wavelet transforms, Figure 3.5 demonstrates how the frequency bands are separated into distinct sub-bands.

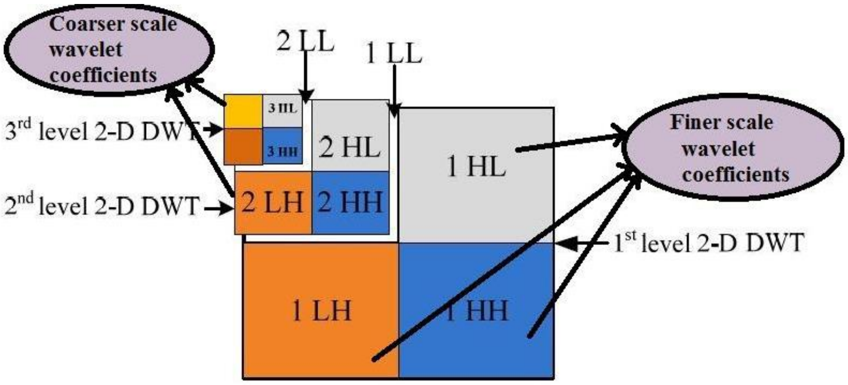

Figure 3.5: 3-Level DWT Execution

3.2.1 Applications of Wavelet Transform

Wavelets are functions that meet certain criteria; their name derives from the fact that they must Incorporate to nil, "lapping" the x-axis in front and behind.. Wavelets can help statisticians because they can effectively and cheaply transform big and noisy data sets using the Discrete Wavelet Transform and codify the wavelet coefficients. Adaptive time-frequency windows, intrinsic scalability, economical computational complexity, and flawless reproductions are all features of Discrete Wavelet Transforms. Coarse versions of images are frequently employed as a first approximation in compression algorithms in image processing and computer vision[106]. A low-pass and sub-sampled version of a signal is frequently an acceptable coarse estimate for several real-life signals in signal processing. Downloading a coarse version of an image out from World Wide Web is significantly faster than downloading the whole image, i.e. one can get the rest or further depth if the image appears to be of relevance. The wide version of a signal is better insulated versus transmission faults in communication systems than comprehensive information. Because of its excellent spatio-frequency identification qualities, the DWT is particularly suited to detecting locations in the source images in which a watermark can really be conveniently inserted. Because the majority of the energy is concentrated in the lower sub-bands (LLx), watermarks embedded in these sub-bands may considerably damage the image. Nevertheless, it has the potential to improve robustness. The high frequency subbands HHx, on the other hand, encompass the image's edges and sharpness, and the human eye is generally sensitive to alterations in such bands. This feature allows you to include the watermark even if it isn't apparent to the human eye. Several DWT-based watermarking approaches embed the watermark in the LHx and HLx frequencies subbands, where opacity is acceptable.

3.3 Singular Value Decomposition (SVD)

The SVD transformation has several applications, including the ability to approximate a matrix by one of low rank, solve linear equations, filter noise from signals, and compress image/video-frame data in digital signal processing. Singular Value Decomposition [104] is a linear algebra A rectangle matrix A can really be decomposed into the combination of the three matrices, according to this approach.: an orthogonal matrix U, a diagonal matrix S, and the inverse of an orthogonal matrix V as given in equation I.

$$\mathbf{A_{MN} = U_{MM}S_{MN}V^{T}_{NN}} \tag{I}$$

M and N represent the number of rows and columns correspondingly, in matrix A. The ortho-normal eigenvectors of AA^T are the columns of U, and the product of A and A^T is the unitary matrix 'I'. Similarly, the columns realte with the V are ortho-normal eigenvectors of A^TA, i.e. the unitary matrix 'I' is the product of A^T and A. S is known as a diagonal matrix that contains the square roots of In order of importance, eigenvalues from U or V, with the singular values on the diagonally. Each one of the matrix's singular values S_{MN} lying on the diagonal specifies the brightness of the image. A video sequence is passed through an SVD operation to obtain the three matrices U, S, and V_T in SVD-based video watermarking[105].

3.4 Discrete Cosine Transform

The Discrete Cosine Transform (DCT) is frequently used as a crucial element in video watermarking in order to embed and retrieve watermarks from video footage. DCT divides an image into different frequency ranges. Less perceptual distortion results with watermark embedding in low-frequency bands, but the watermark can be removed by straightforward signal processing attacks. Compression attacks and common image processing processes can affect high frequency components. Consequently, the middle frequency component can be the ideal option for water-mark insertion since it will strengthen the method against lossy compression. The articles that represent the study conducted by earlier researchers in each frequency domain technique are listed below. As shown in Fig. 3.6 redundancy in image pixels can be detected by applying the Discrete Cosine Transform approach, which converts spatially-oriented pixels into a frequency-domain representation[106][107].

The process of adding extra information (the watermark) to a video signal so that it is invisible to viewers but may be found or retrieved when required is known as video watermarking. With the use of DCT, video frames can be converted from the spatial to the frequency domain, allowing for the incorporation of a watermark in a way that is less obvious to humans. This is so that the watermark can be hidden by altering the DCT parameters in the high-frequency components, which normally represent subtle visual characteristics.

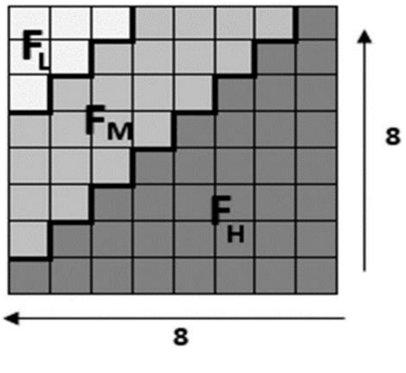

Figure 3.6: DCT Block

The goal of DCT-based video watermarking approaches is to strategically place the watermark in the DCT coefficients such that it can withstand common video processing operations such as noise addition, transcoding, and compression. Even after such actions, the watermark ought to be retrievable. Making ensuring that the embedded watermark fails to materially degrade the video's perceived quality is one of the main objectives of video watermarking[108][109]. The goal of DCT-based techniques is to reduce any visual impact by modifying coefficients in this way. The same DCT transform is used to return the watermarked video to the frequency domain when extracting the watermark from it[110][111]. Next, the suitable watermark extraction technique is applied to extract the watermark from the changed DCT coefficients. To calculate the DCT for a video frame, let us suppose that DCT is denoted by F(s, t) and a video frame is denoted by F(m, n).

$$F(s,t) = c(s)c(t)\frac{2}{\sqrt{MN}}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} F(m,n) \times \cos\,[\frac{\pi}{2M}(2m+1)s]\,\cos\,[\frac{\pi}{2N}(2n+1)t]$$

where M is the width of the frame in pixels, N is the height of the frame in pixels, and (s, t) are the DCT coefficients[112].

3.5 Basics of Encryption and Decryption

Encryption techniques are often classed based on the secure key used to encrypt/decrypt secured data. Symmetric and asymmetric encryption techniques are the two kinds .

3.5.1 Symmetric Encryption

Symmetric encryption is a sort of systematic cryptography that hides an electronic communication behind an unified encryption key. Its data processing uses a mathematical process coupled with an encryption key to render a text unintelligible. Symmetric encryption is a two-way approach since the mathematical mechanism is duplicated while decrypting a message and the secret key is the same. Symmetric encryption is sometimes owned by private encryption or secure-key encryption. To clarify, the sender or receivers agree on a secret (shared) key in this type of encryption. They next encrypt and decrypt their delivered messages using this secret key . Figure 3.7 depicts a symmetric cryptography approach. Nodes A and B must first concur on the encryption approach to be used in the encryption and decryption of transmitted data. They then choose a private key that will be used by numerous of them were in this relationship. Node A begins releasing information encrypted with both the shared secret key after the encryption configuration is complete, and node B uses the same key to unlock encrypted interactions on the receiving end.

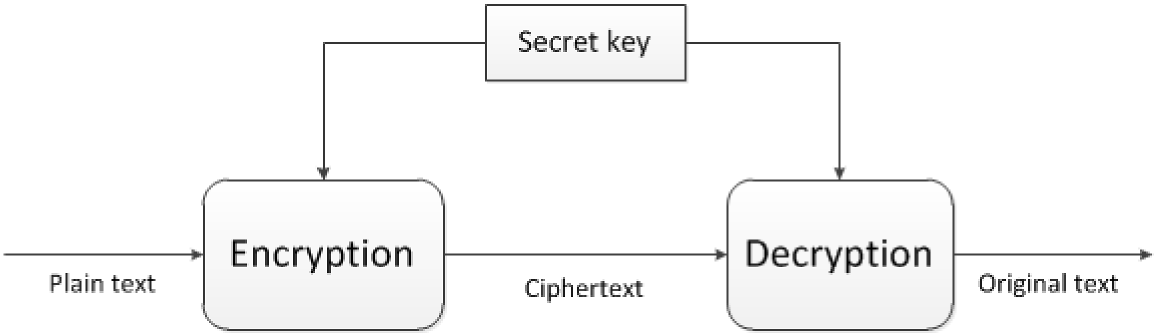

Figure 3.7: Symmetric Encryption

3.5.2 Asymmetric Encryption

Asymmetric encryption is the another face form of text conversion in which two keys are utilised, with key1 being able to encrypt and key2 being able to decrypt. It's also known as Public Key Cryptography (PKC) since customers often utilise two keys: a public key that's very well with the public and a private key that only the user understands. Figure 3.8 shows the use of two keys between nodes A and B. Node B provides its public key to node A after consenting on the type of encryption to be used inside the connection. Node A transform its messages with need of the public key it has collected. Node B then execute its private key to decrypt encrypted communications as they arrive.

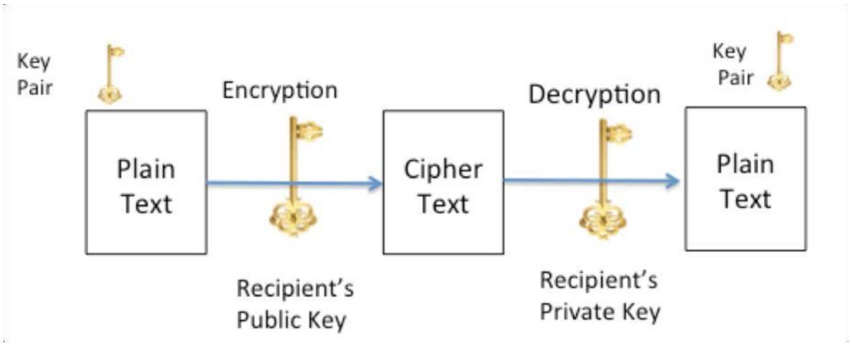

Figure 3.8: Asymmetric Encryption

This feature solves the difficulty of managing private keys in symmetric encryption. Nevertheless, because of this feature, public key encryption is mathematically more vulnerable to assaults. Moreover, while asymmetric encryption algorithms demand more computer processing capability, they are nearly 1000 times slower than symmetric ones. A hybrid strategy is widely employed to reap the benefits of each methodology. Asymmetric encryption is used to exchange private keys in this manner, followed by symmetric encryption to transport records among sender and receiver .

3.6 Motion Frame Extraction

For copyright protection, existing video watermarking solutions use scene change detection technologies. These strategies compelled the watermark to be included in both motion and non-motion video frames. However, there are a number of drawbacks to this method. One of it's problems is that intentional temporal synchronization attacks might cause the watermark to degrade or disappear[113][114]. As a result, the proposed solution solely used the watermarking method in motion frames to solve this problem. Certainly, the approach is useful for recovering the integrity of an extracted watermark while reducing the watermarked video's substantial video appearance.

CHAPTER 4
PROPOSED ALGORITHM & RESULT ANALYSIS

This chapter begins with a survey of existing video watermarking technologies. Experimental research frameworks, visible approaches, spatial domain methods, and transform domain methodologies are among the topics covered. This chapter explains the experimental framework used to implement the algorithms, as well as the dataset that was employed. The results of implemented algorithms are also compared using graphical representations. Before explaining the suggested algorithm and the research need, a sufficient history of previous techniques is provided. The suggested video watermarking algorithm has also been explained, as this thesis is about the integration video watermarking. At the end of this chapter, the fundamentals of a camcorder tracking system are explained.

4.1 Method Based on Multiple Frequency Band and SVD

The scheme demonstrated a multi-resolution wavelet decomposition-based digital video watermarking technology. To improve the overall security of the watermarking system, the technology safeguards copyright information by embedding a bit map picture as a watermark in two different locations. This method adds copyright information to the wavelet domain's individual bands. The goal of inserting the same watermark in two separate locations is to make the watermarking system more robust. The resulting watermarking method can be utilized for private watermarking programs that demand access to the original video in order to extract the watermark. The watermark is undetectable and impervious to a range of attacks, according to test results.

Although a spatial domain is limited to a few pixels for watermarking applications, the transform domain leverages all pixels, increasing the total watermarking system's robustness. The Discrete Fourier Transform (DFT) [111], Discrete Wavelet Transform

(DWT), or Handamard Transform Technique (HTT) are used in transform domain approaches. Watermarking systems based on wavelets have gained considerable acceptance in signal processing and image reduction. The wavelet domain is preferred for watermarking due to its superior HVS modelling, computational efficiency, superior space-frequency localisation, and multi-resolution capabilities. It also offers the ability to evaluate signals in both the frequency and temporal domains at the same time. There are numerous sub-bands to choose from when embedding a watermark through using coefficient of wavelet domain. Because the qualities of the various sub-bands varies, the choice of which basis to incorporate the watermark is important. The Haar wavelet has been shown to be suitable for watermarking multimedia artefacts . If F(m,n) does not describe a digital frame with dimensions of 2M x 2N, boundary prolongation should be utilised to ensure that the picture is divisible by 2 as required by the Haar wavelet transform. Based on the weight of approximating (LL), horizontal axis specific weights (HL), vertical direction (LH), and weight on the diagonal direction, one-level decomposition on the video frame yields four different resolutions (HH). It has been discovered that the LL sub-wavelet band's coefficients have the most texture and energy, indicating that enough space may be gained for watermark embedding.

4.1.1 Design of Proposed Scheme

The watermarking method is generally implemented using a blend of DWT and SVD. In some techniques, DWT single level decomposition is employed, whereas in others, DWT double level decomposition is used. Although employing a single level decomposition of DWT to implement a watermark is not a robust method, it does achieve human perceptibility. However, when employing the double level decomposition of DWT to build a watermark, the human perceptibility is poor, but the robustness is obtained. We used both solitary and double level DWT decomposition in the suggested watermarking method. For watermark embedding, this approach considers both high and low resolutions. The watermark is divided into two subbands, one at the single level (HH) and the other at the second level. On a higher subset, SVD is used single-level DWT decomposition band (HH). Before embedding a watermark picture into digital material, SVD is applied to it. The proposed approach is found to be resistant against attacks on watermarked video in this work. The pixels of video are utilised as an input, and a watermark is injected into them DWT and SVD approaches are used to create frames. The watermarking model's overall structure is depicted in Fig. 4.1

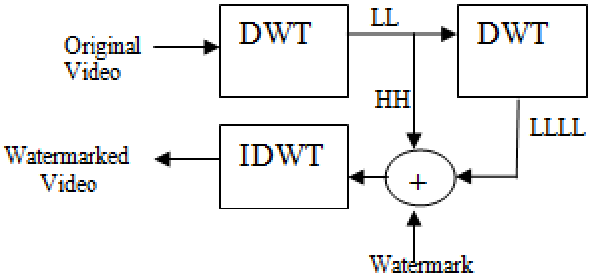

Fig. 4.1 Model based on DWT

4.1.2 Watermark Embedding Process

Step 1. The video is initially separated into frames. After that, the RGB frames are transformed into YUV components.

Step 2. On this frame, select the brightness component of Y and perform the single level DWT. This will result in four sub bands of multiple resolution (LL, HL,LH,HH). Apply the DWT to a lower frequency sub band LL again, and you'll get four sub bands of various resolution (LLLL, LLHL, LLLH, LLHH).

Step 3. Applying SVD to the higher-resolution subband HH yields three matrices: U, V, and S.

$$SVD(HH)=U_{HH}S_{HH}V_{HH} \qquad (1)$$

Step 4. Again apply SVD is applied to the watermark W, it produces three U, V, and S.

$$SVD(W)=U_{W}S_{W}V_{W} \qquad (2)$$

Step 5. Both the HH and LLLL subbands are used for embedding. First, embed the SW in the HH band by modifying the HH band's SHH using the equation below.

$$S'_{HH}= S_{HH} + \alpha 1 S_{W} \qquad (3)$$

Step 6. Apply the following equation to embed the watermark(W) into the LLLL sub band.

$$YL'=YL +\alpha 2W \qquad (4)$$

to keep the perceptibility and robustness balance, 1 and 2 are employed.

Step 7. The inverse SVD is then performed on the HH band, followed by the inverse DWT on the HH and LLLL sub bands. The watermarked frame will be created as a result of this. Combine all of the watermarked frames to make a single movie file.

4.1.3 Watermark Extraction Process

Watermark extraction from watermarked video is the converse of the technique. The procedure of watermark extraction is implemented in following steps-

Step 1. Watermarked video is split into frames, with the RGB frames being transformed into YUV components.

Step 2. Choose the Y component and execute the DWT transformation to it. As a result, there will be four subbands with different resolutions. When DWT is applied to an LL sub band, the resulting sub bands are LLLL,LLHL,LLLH,LLHH.

Step 3. From LLLL band the watermark is extracted from YL as

$$W=(YL'-YL)/ \alpha 2 \qquad \textit{(5)}$$

Step 4. SVD is applied on HH band and then extract the watermark as

$$S_{W=} (S'_{HH}- S_{HH})/ \alpha 1 \qquad (6)$$

4.1.4 Experimental Results & Analysis

The proposed method's performance was evaluated using video sequences from the Hindi film 'Hum Aapke Hai Kaun.' The clip has 36 frames with a resolution of 352 x 240 pixels and a frame rate of 23 frames per second. The scheme assessed the graphical fidelity of watermarked video as well as its resistance to various types of attacks. Figures 4.2a and 4.2b show the original video frame as well as the accompanying watermarked frame, respectively. Because both frames appear to be visually similar, imperceptibility is clearly maintained. Figure 4.3 depicts the original watermark, while Figures 4.3a and 4.3b depict the extracted watermarks from of the LLLL and HH bands, respectively, when no attack is applied. The accurate extraction is indicated by the NC values of the watermark with in two bands, which are 1 and 0.9958, respectively.

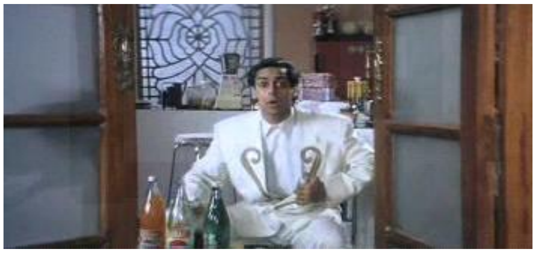

Figure.4.2a Original Frame of Video

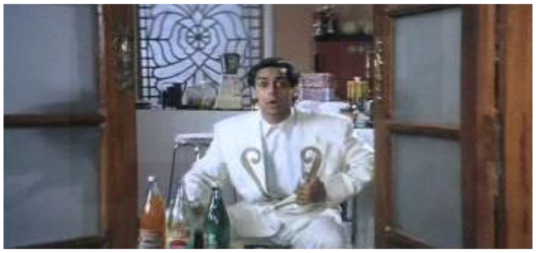

Figure. 4.2b Watermarked Frame

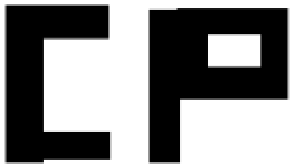

Figure.4.3 Actual Watermark

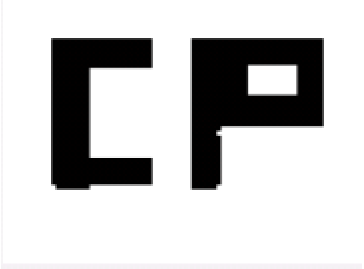

Figure.4.3a Extracted Watermark(HH)

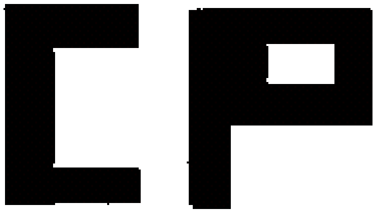

Figure.4.3b Extracted Watermark(LLLL)

4.1.5 Evaluation of Robustness

Different attacks were carried out on the watermarked frames. To assess the issue of robustness, the experimental outcomes are examined. On watermarked video, two geometric assaults were used: rotation and cropping, and a signal to noise' (SNR) attack.

4.1.5.1 Evaluation after Geometric Attack

Geometric assaults refer to tampering with the embedded watermark's coordinates. The embedded watermark might well be corrupted or even erased by malicious users as a result of such attacks. As a result, video watermarking techniques have always required that the watermark be extracted effectively, and this is an issue that should never be overlooked. As indicated in Table 3.1, the suggested approach rotates every watermarked frame anticlockwise from 0.1° to 0.5°. When watermarks are derived from second level (LLLL) decomposed of lower energy sub-bands, the suggested watermarking scheme may resist up to 0.3° of rotation, but the same watermark cannot be extracted successfully through high energy sub-bands (HH) as shown in Table 4.1.

Table4.1 Rotation Attack and Robustness Analysis

Rotation	1°	2°	3°	4°	5°
NC(LLLL)	0.8605	0.7911	0.7019	0.4512	0.2841
NC(HH)	0.3905	0.2414	0.2284	0.2054	0.1714

4.1.5.2 Evaluation after Cropping Attack

The watermark was retrieved after the first 12 columns of the embedded watermark video frames were deleted. As shown in Figure 4.5a and 4.5b , the correlation calculated values from low energy second level (LLLL) and first level (HH) decompositions of DWT are 0.7814 and 0.373063, respectively. It means that watermarks can be extracted successfully from bottom level sub-bands and not from top level sub-bands. The signal's highest information is found in the lower energy sub-band (LL), whereas the margins or boundary information is found in the high energy bands (HH). Edges, by definition, take up less space than the rest of the data, and any modifications in this area jeopardise the host material's originality. As a result, the method is vulnerable to rotation and cropping attacks using high-energy sub-bands.

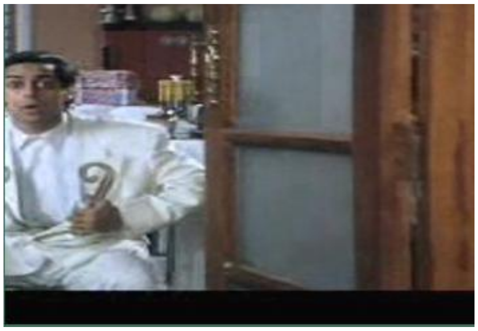

Figure.4.4 Attacked Watermarked Video

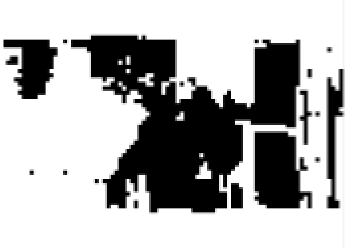

Figure.4.5a Extracted Watermark

NC(LLLL)=0.7814

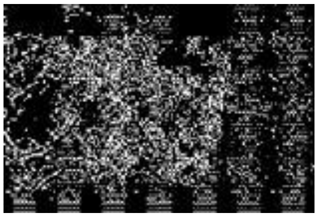

Figure.4.5b Extracted Watermark

NC(HH)=0.37461

4.1.5.3 Evaluation after SNR Attack

The second attack is the Signal to Noise (SNR) attack, in which the strength of each watermarked frame is increased by lowering the noise level, and the results are examined for extracting the watermark. According to the experimental results, as the SNR of the AWGN channel is improved, or the noise intensity is lowered, the content of the watermarked video frames in the receiver side gradually improves, and thus the quality of the recovered watermark drastically improves. The watermark could be recovered accurately with an SNR of 35 dB and an NC value nearly equal to 1.

Figure.4.6 Attacked Watermarked Video

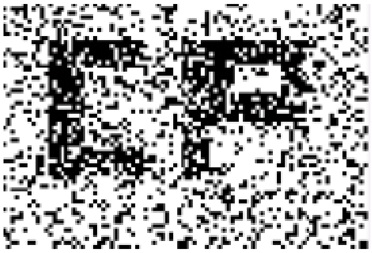

Figure.4.7a Extracted Watermark

NC(LLLL)=0.8411

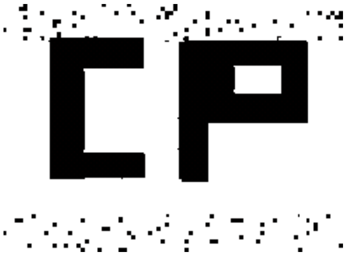

Figure.4.7b Extracted Watermark

NC(HH)=0.9824

The watermark is inserted in two different sub-bands in the video watermarking scheme: second level deconstruction of lower energy sub-band (LLLL) and single level deconstruction of higher energy sub-band (LLLL) (HH). The watermark is effectively recovered from both sites without any attack, according to experimental results. It is also concluded that when the watermark is introduced at a lower level energy sub-band, it is more resistant to geometric attacks such as rotation and cropping than when it is inserted at a higher level energy sub-band. Because of the high energy band, which includes the textual and edge regions, there is less area for extra information like as noise or a watermark to be included. A minor disruption could cause the entire watermark to be corrupted. Experiments have shown that before implementing attacks, we were almost effective in extracting the watermark. The performance is better for one type of attack, such as SNR, than for another, such as rotation and cropping. In future study, an efficient and resilient technique that uses a selection of frames rather than the complete frame can be used.

4.2 Robust video watermarking algorithm based on motion frames and encryption

The resilient, hybrid, and non-blind digital video watermarking technique based on the multi wavelet decomposition and singular value decomposition is presented in this research work. Watermark is embedded into singular values generated from discrete cosine transformed matrix generated from two level discrete wavelet segmentation of luminance component out of each motion frame of video sequence at the heart of the proposed system. The original video and watermark must be proofed during the watermark extraction process in order to resolve the copyright issue. As a result, the resulting video watermarking system can be used for private watermarking programs that demand the original video and watermark to provide ownership protection. Following a thorough examination of video watermark technologies, it was discovered that the majority of existing methods are incapable of withstanding all purposeful and inadvertent attacks, as well as combining two or more attacks for various videos. The advantage of this technique is that the watermark's security is ensured by only inserting the watermark in motion-based frames derived from the source video. Another distinction is that the higher perceptibility attained demonstrates that there is no discernible difference between both the watermarked and original frames. Furthermore, the robustness of the system is evaluated by a variety of unintended and planned attacks. The experimental findings reveal that the suggested method delivers multimedia content in a reliable, undetectable, and secure manner. In general, existing video watermarking systems make use of all subsequent frames detected by scene change detection. The watermark is inserted in both motion and static video frames using scene change methods. This method has several limitations, particularly whenever the watermark is inserted in static frames.

4.2.1 Design of Proposed Scheme

By recognizing the motion component of the video, the proposed algorithm presented a unique way for video watermarking. Two major issues with scene-based video watermarking are addressed by this technique. In general, compression standards methods keep the action element of the video while eliminating the static segment. As a result, the suggested technique can withstand lossy compressions. Second, putting a watermark in the motion zones makes it difficult for the viewer to see it because of the human visual system.

4.2.2 Process of Watermark Encryption

The rationale behind watermark encryption is to safeguard embedded video content. Encryption will take place during embedding, and decryption will take place during watermark extraction. For this, a secret key is created.The advantage of an encryption method is that no user can logically decipher the cypher image. Once the watermark has been decrypted using the secret key, it can be read. The author's suggested appropriate algorithm is determined to be an effective method for encrypting the watermark.First, we choose the key that will be used to jumble the watermark, which is K={16,1,14,3,12,5,10,7,8,9,6,11,4,13,2,15}. To scramble the watermark, a combination of even and odd digits is called a key.

The watermark's dimensions will match those of the video object. The watermark is divided and then reorganised in accordance with the value K that was determined. This procedure leads to the watermark's encryption process. The original watermark is displayed in Figure 4.8, and some of the jumbled watermark is displayed in Figure 4.9.

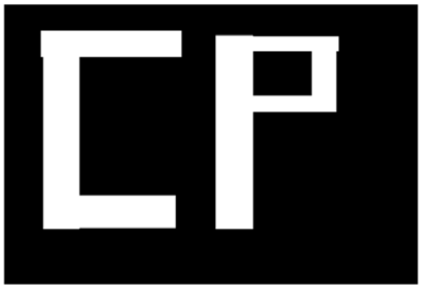

Figure.4.8: Original Watermark

For example, if No.ofMotionedFrames is 14 and No.ofKeyElements is 16, the number of partitioned pictures of a scrambled watermark object defined by the aforesaid method is 4. The scrambled image is divided into four parts (Part 1, Part 2, Part 3, and Part 4) for use in various motion frames.

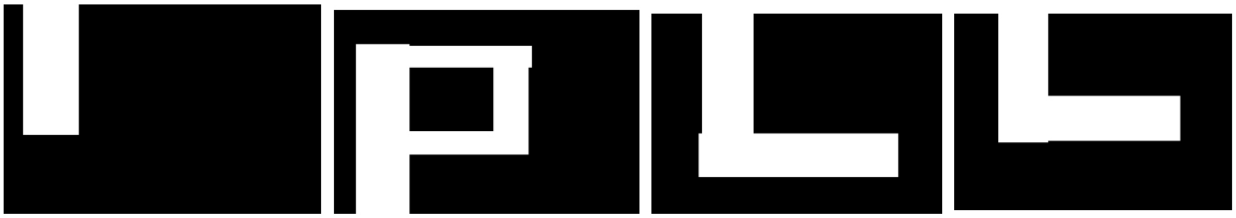

Figure.4.9 Four Parts of Scrabmled Image

4.2.3 Process of Motion Frames Extraction

After the scrambling of watermark the next step is to extract the motion frames from original video object . The motionless area of the video object is not robust and it is a comparatively easy task to exploit on the motionless frames based watermarking method. The histogram or red component of each frame is utilized to extract the frame which will be considered as motion frame. After the execution of proposed scheme 14 frames are detected as a motion frames from the coastguard video object . The threshold value is set upto 5000 to extract the frames. The proposed scheme embed the scrambled watermark into the frame which results that few frames are get watermarked instead of all. It is also observed that quality of watermarked video also maintained .

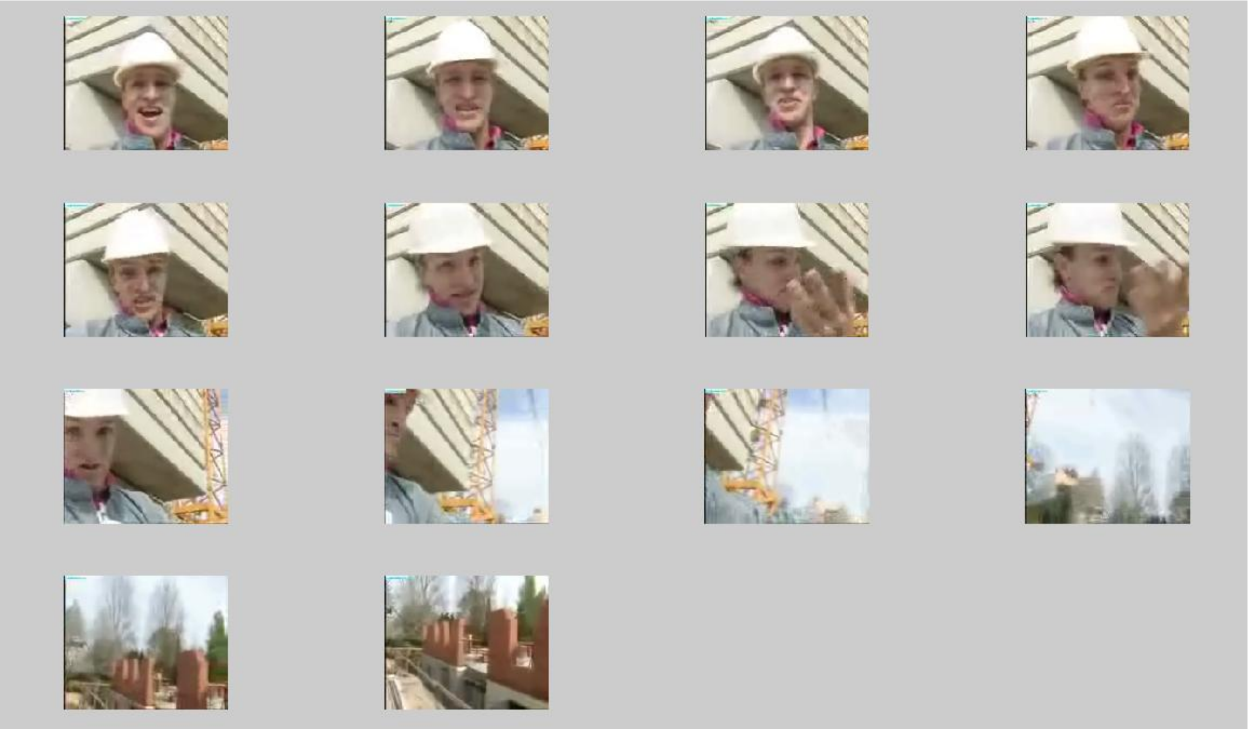

Figure.4.10 Extracted Motion Frames from *Foreman.avi*

4.2.4 Process of Watermark Embedding

The encrypted portion of the watermark is embedded into the motion frame in order to implement the algorithm for embedding the scrambled watermark.Should the chosen frame not be a motion frame, then there won't be any embedding operation carried out. Only motion frames are used in the embedding procedure. Repeat the encrypted watermark sequence starting from step one if the number of retrieved motion frames exceeds the number of encrypted watermark segments. Convert the motion frame into different brightness components now. Following the conversion, four subbands—LL, LH, HL, and HH—are produced by discrete wavelet transformation up to 2-Level. The watermark is inserted using the HH band. Use the SVD method on this band to create a matrix of three components, then insert the watermark using the diagonal matrix. The diagonal matrix is utilised for watermarking, and the SVD technique is also applied. The embedding of watermark is executed by following equation-

$$SVD_{WD} = SVD_{Y} + \alpha SVD_{W} \qquad (7)$$

SVDY is the diagonal matrix of Y component after the apply SVD operation on it. SVDw represents the diagonal matrix of scrambled watermark.The value of α will be 0.01. After performing the watermarking operation the resultant diagonal matrix is SVDWD which is watermarked frame. After the insertion of watermark on all frames the watermarked video is generated which leads the final watermarked video. Figure 5 shows the flowchart of the proposed method for watermark embedding.

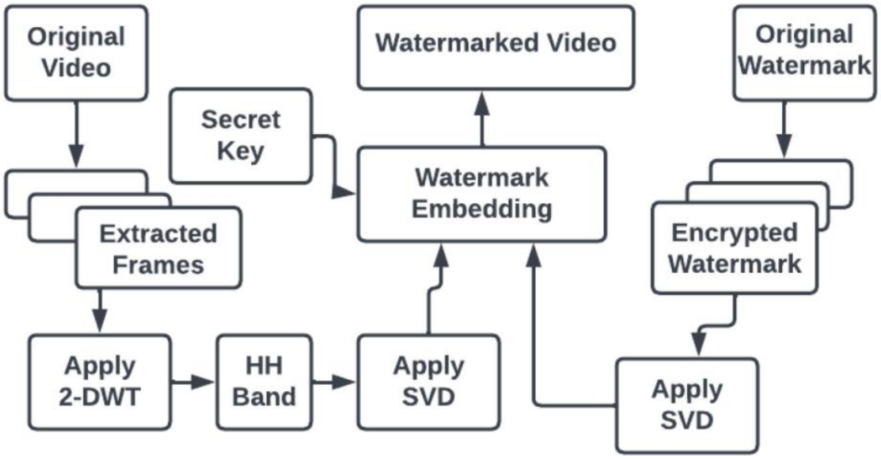

Figure.4.11 Watermark Embedding Flow Chart

4.2.5 Process of Watermark Extraction

When we wish to remove the watermark that has been introduced into a motion frame, we must use the extraction technique. In order to do this, take the next RGB frame out of the watermarked video and determine whether it is a motion frame. It needs to have a watermark if it's a motion frame. Utilise the method that divides an RGB frame into its three constituent parts, Y, Cb, and Cr. Apply the DWT for level 2 now, and choose the HH band. To determine the diagonal matrix, which contains singular values, apply the SVD method. The singular values of watermark is generated by given mathematical formula-

$$S_{w'} = (S_o - S_w)/\alpha \qquad (8)$$

In this case, Sw and So stand for the unique values of the frame that was taken from the watermarked and original source videos. To obtain every watermark, repeat this method. After that, the final watermark will be formed.

The singular values of the source motion video frame and the watermarked video frame are S_o and S_w, respectively. Repeat this method to obtain all of the watermarks, and then generate the final watermark. The approximated watermark can be created in the following way:

$$\text{Watermark= UW x SW' xVW} \quad (9)$$

The watermark's orthogonal matrix is made up of UW and VW. These numbers are known as the original watermark values.We run the embedding algorithm on two videos. The original video and the watermarked version are shown in Figures 4.11a and 4.11b. The results of the embedding operation on a different video are shown in Figures 4.12a and 4.12b.

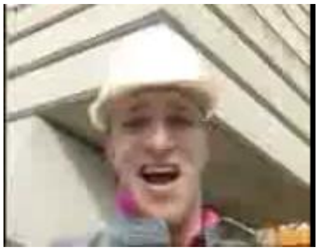

Figure. 4.11a Original Frame

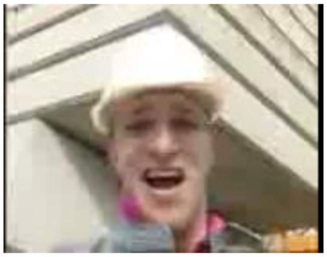

Figure. 4.11b Watermarked Frame

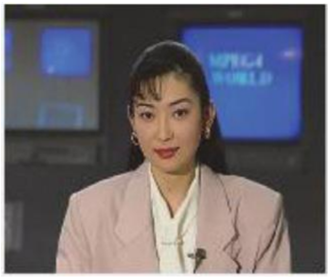

Figure. 4.12a Original Frame

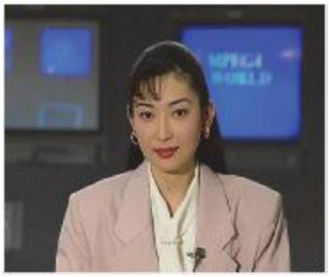

Figure. 4.12b Watermarked Frame

4.2.6 Performance Evaluation of Proposed Method

Two important aspects need to be verified when the watermark is extracted: the algorithm's resilience and perceptibility.A variety of attacks are used on watermarked video for result processing, and after that, the extraction procedure is put into action. The PSNR is a tool for perceptibility measurement. PSNR is measured in dB. The endurance of the proposed watermarking technique is evaluated by examining its aspects. To remove the watermark that was added to the actual video object, a number of attacks are carried out on the watermarked video. The suggested is determined to be resilient to the above-described attacks. The evaluation is carried by analyzing the original watermark and driven out watermark by observing NC. The table shown below is the level of sturdiness of proposed algorithm. The proposed algorithm is applied on two videos foreman.avi and akiyo.avi. The applied attacks mentioned above measure the robustness of the algorithm.

The suggested scheme's robustness was tested through a series of tests. To do this, various attacks are performed on the watermarked video in order to extract the attacked watermarked video file, which is then utilized to retrieve the watermark. Some of the attacks are focused on exploiting video's inherent qualities. One of video's characteristics is its temporal feature, which is represented by a series with still images known as video frames. An attacker may not change the graphical fidelity of watermarked video by changing the sequence of some of the nearby frames, but he or she may damage the embedded signal. Another feature of video is that it contains a high level of redundancy between frames.

Table 4.2: Proposed Algorithm Robustness Results (Foreman.avi)

S.No	Attack Performed	NC	PSNR
1	Speckle Noise	0.881	40.2414
2	Frame Deletion(around 10%)	0.908	38.1008
3	Rotation(15 Degree)	0.893	47.0024
4	Gaussian Low Pass Filter	0.811	42.2003
5	Cropping	0.898	37.8870
6	Salt and Pepper	0.882	41.2404

Table 4.3: Proposed Algorithm Robustness Results (akiyo.avi)

S.No	Attack Performed	NC	PSNR
1	Speckle Noise	0.902	39.0047
2	Frame Deletion(around 10%)	0.911	38.0021
3	Rotation(15 Degree)	0.901	41.2414
4	Gaussian Low Pass Filter	0.806	43.5724
5	Cropping	0.885	40.0122
6	Salt and Pepper	0.917	41.2141

4.2.6.1 Performance Evaluation after Rotation Attack

Each watermarked frame is rotated anticlockwise from 0.1° to 0.6° in the proposed design. By recovering 74% of the watermark, it is determined that the suggested watermarking approach can resist up to 0.3° of rotation of the whole watermarked video frames. By establishing a PSNR of more than 30 dB, the perceptibility of watermarked video can be maintained up to 0.5°. The scheme is ideal for these two crucial parameters up to 0.3° in order to preserve the balance among perceptibility and robustness.

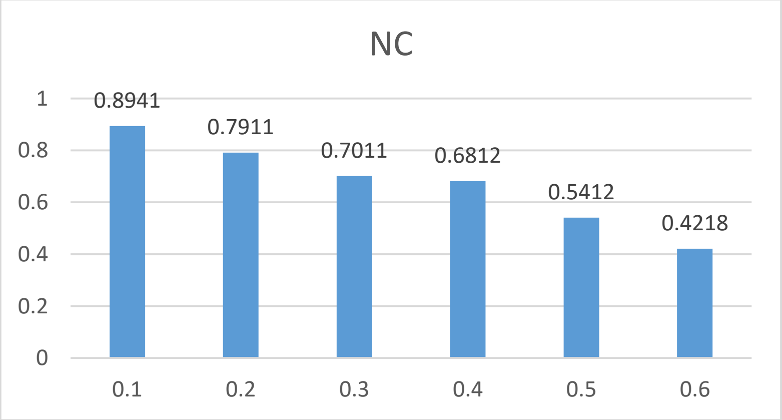

Figure.4.12 Robustness against Rotation Attack

4.2.6.2 Performance Evaluation after Cropping Attack

Cropping the number of columns from 60 to 140 by replacing zeros in such columns from watermarked video frames in a very way that the width of the frames is not affected is another component of the experiment. It's for the sake of keeping the perceptibility of watermarked footage and calculating the PSNR quickly. Measures of satisfactory characteristics are acquired. As demonstrated in Figure. 4.13, up to 65 columns of watermarked frames can be cropped. In terms of robustness, the watermark is extracted successfully (85 percent) when cropping is approximately 140 columns, as illustrated in Figure. 4.13

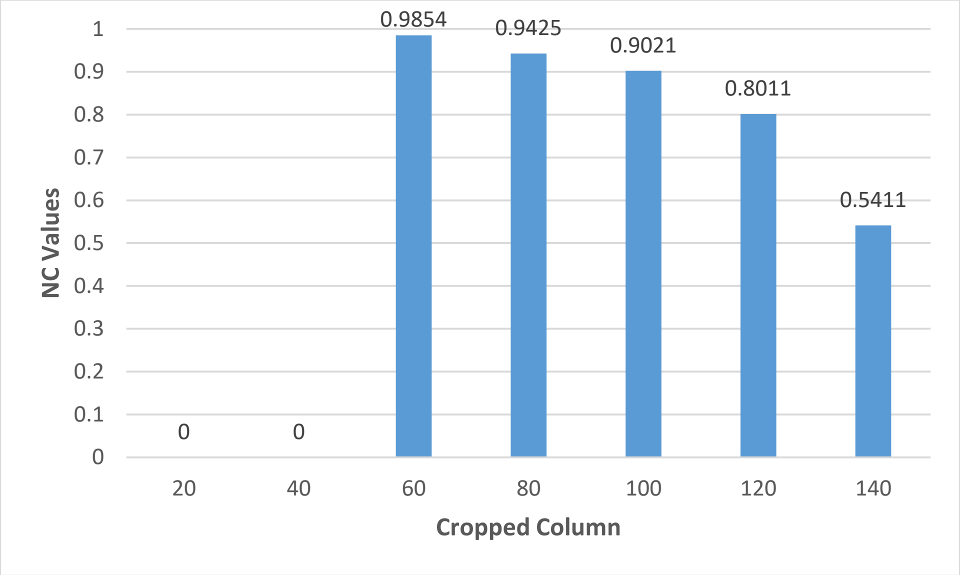

Figure. 4.13 Robustness against Cropping Attack

4.2.6.3 Performance Evaluation after Noise & Filtering Attack

Another technique to test the resilience of the embedded watermark is to add noise to the watermarked video. To distort and degrade the footage, four distinct types of noise were added: Speckle, Poisson, Gaussian, and Salt & Pepper. As a result, one of the negative consequences is that extracting the watermark information becomes difficult. At a 0.1 interval, the intensities of Speckle, Gaussian, and Salt & Pepper are altered from 0.002 to 0.006. The watermarked system can endure speckle noise attacks of up to 0.003 intensity and salt and pepper noise attacks of up to.005, however the results for Gaussian noise attacks are not satisfactory because the distortions level is too high to maintain robustness.

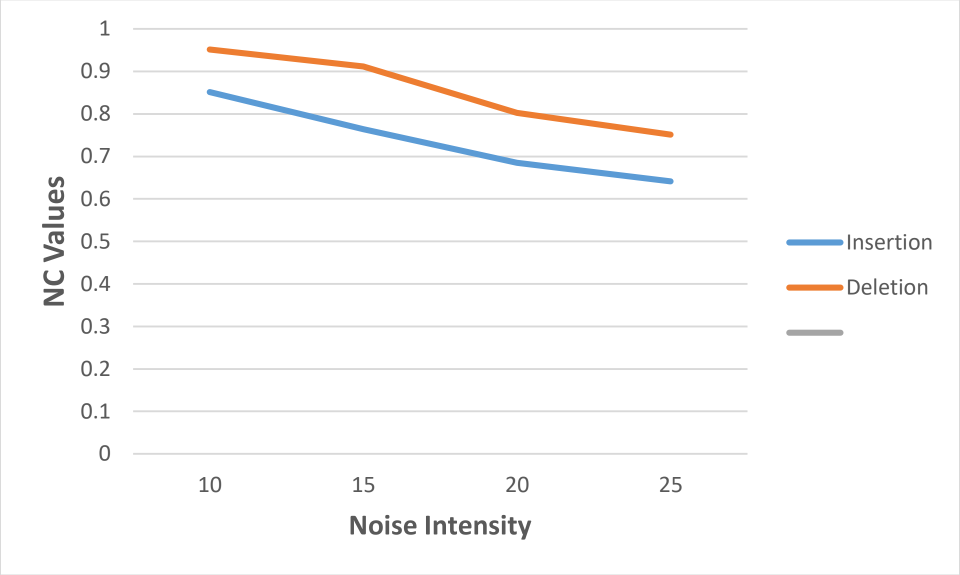

Figure. 4.14 Robustness against Noise Intensity Attack

4.2.6.4 Performance Evaluation after Frame Dropping & Insertion Attack

The presence of redundancy in video frames is one of its characteristics. A malevolent user can utilise this feature to choose frames from various parts of a watermarked video and drop them in such a way that the chosen video frames are permanently removed from the watermarked video. In this case, an attacker ensures that the perceptibility of watermarked video is not considerably harmed. To achieve this, 10 to 50 frames from the watermarked video are removed. Some motion frames, such as the 32nd and 16th from the Foreman, are dropped during the dropping process. The proposed technique, as shown in Figures 4.15, conveys fine robustness while providing adequate perceptibility while sacrificing over 30 frames (10%).Inserting frames from other videos is a typical sort of unintended attack in video watermarking systems. In most circumstances, commercial breaks must be inserted at various points throughout the video's playback. Inserting frames from other videos into the watermarked video can be done in two ways. In the first case, the commercial video clip is inserted, but the number of frames inhabited by the supplemental video clip is replaced by the original video frames in order to maintain the video's length, while in the second case, the chosen video clip is inserted into the watermarked video without regard for the video's length. A significant amount of watermarked video data is lost in both circumstances. Nonetheless, an attacker must ensure that the perceptibility of watermarked video is not significantly harmed.

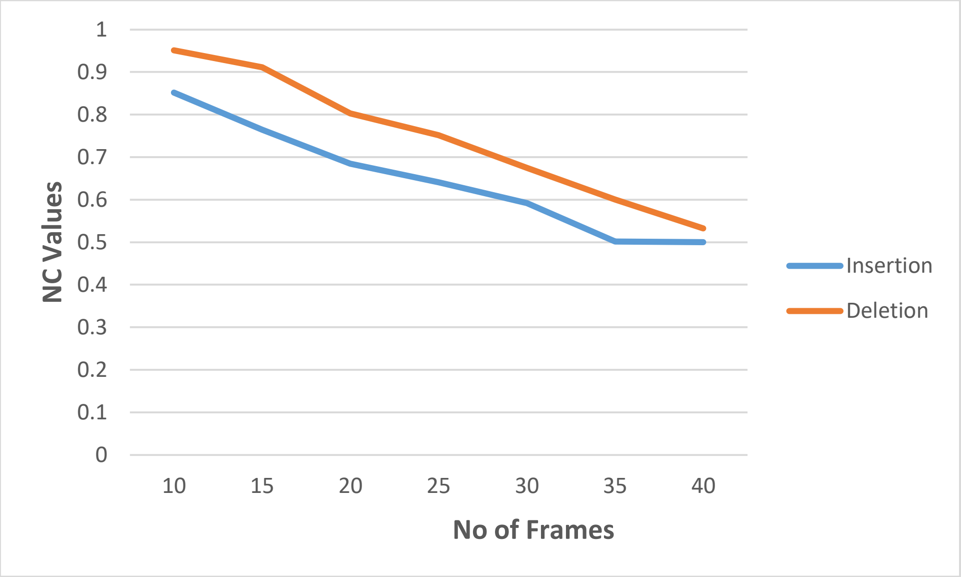

Figure. 4.15 Robustness against Frame Dropping & Insertion Attack

This project offered a way for safeguarding the copyrighted information embedded in the host video through video watermarking. The selection of motion frames for embedding purposes utilizing a hybrid transform domain technique is the method's main inspiration. The watermark is contained in the two-dimensional wavelets of the HH frequency sub-band, and the luminance component of motion frames is transformed using two more powerful transformations, DWT and SVD. This scheme's unique feature is that it achieves high robustness by covering a wide range of intentional and unintentional signal processing and video-specific attacks such as frame dropping, frame averaging, frame swapping, frame inserting, median filtering, and combining different types of attacks. Because the original watermark and original video are required for watermark retrieval, the generated watermarking algorithm is utilized for private watermarking.

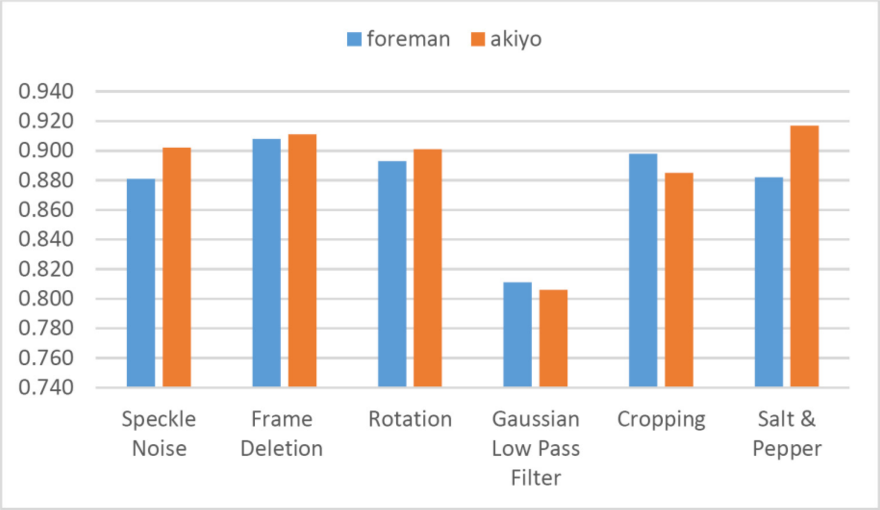

Figure. 4.16 Result Comparison(NC Values) on foreman and akiyo video

According to the post-extraction technique, the extracted watermark has strong NC and PSNR values that withstand a variety of attacks.The NC and PSNR values in Tables 1 and 2 demonstrate how resilient the suggested approach is to various attacks. A comparison of the two video objects when the suggested procedure is applied is shown in Figure 4.16 .

4.3 Robust Video Watermarking Algorithm based on DCT-SVD approach and Encryption

First, the motion frames from the host video are extracted. The define process from the previous section can be used to complete the extraction. Watermark extraction, watermark embedding, and watermark encryption make up the three sections of the suggested technique.

4.3.1.Watermark Encryption

Getting in the binary image as a collection of pixel values is the first stage. A pixel's value can only be either 0 or 1. The binary string that makes up the secret key will be utilised to establish the sequence in which the pixels are switched. The image's pixel indices must then be randomly permuted in the following phase. The sequence in which the pixels are swapped will be decided by this permutation. In this stage, a beginning position in the permutation is determined using the secret key. A value within 0 and the permutation's length should be the beginning point. Change the pixels at each pair of indices that have the same XOR value as the key as you work your way through the permutation from the beginning.

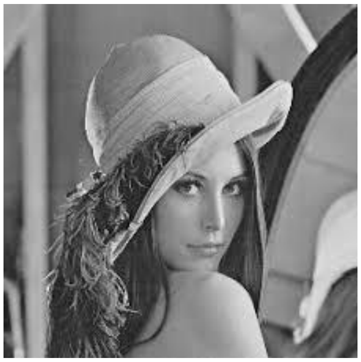

Figure. 4.17 Original Watermark

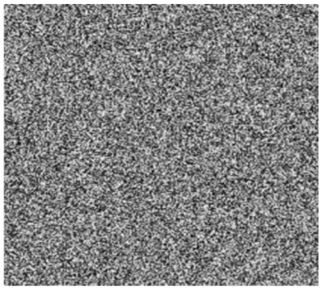

Figure. 4.17 Encrypted Watermark

4.3.2 Motion Frame Extraction

The scene change detector can be used to locate and eliminate relevant frames of the host video object. This is achieved by taking advantage of a correlation between the frames of the video. The process can be used in many ways, depending on how much fine-tuning is required for the results. A histogram, binary search, and linear interpolation are just a few of the methods available for filtering comparable frames from the movie. Scenes with similar values are gathered into a single bin using a histogram technique, and an effort is made to identify the limit range for the highest number of components. This tactic is based on the idea of measuring the signal's dispersion throughout the whole spectrum and using the data for analysis. The difference in the histogram heights for the same bins serves as the statistical measure in this case. In the first step, similar frames are removed using a filtering method that removes identical frames. To get rid of duplicate frames, the filtering process uses the histogram, binary search, and linear interpolation. This approach is known as the HiBisLI technique. Sorting arrays serves as the foundation for the binary search method, which computes the approximate value. The linear interpolation method can be used to estimate any function with two values. You can use either of these methods to take out similar frames from the cover video, retaining only the frames that are unique.

Using histograms to extract motion frames from a video entails detecting motion by analysing the variations in pixel brightness between successive video frames. The general procedures for extracting motion frames from histograms are as follows: To read the video's frames, use a video reader. To lower the algorithm's computing complexity, convert each frame to grayscale. Using a histogram function, determine each frame's histogram. The distribution of pixel intensities in the grayscale image should be represented by the histogram. To find variations in the brightness of the pixels, compute the disparity between the histograms of successive frames. To find frames whose pixel intensity changes are greater than a predetermined threshold, threshold the difference in the histograms. The quantity of motion needed to be detected can be used to determine this threshold. As the motion frames, extract the frames where the histogram difference is greater than the threshold.

The Proposed method is implemented using MATLAB and the sample video of “foreman.avi” is used . After the implementation there were total 300 frames out of which 114 are motion frames . In Fig. 4 some of the sample motion frames are shown .

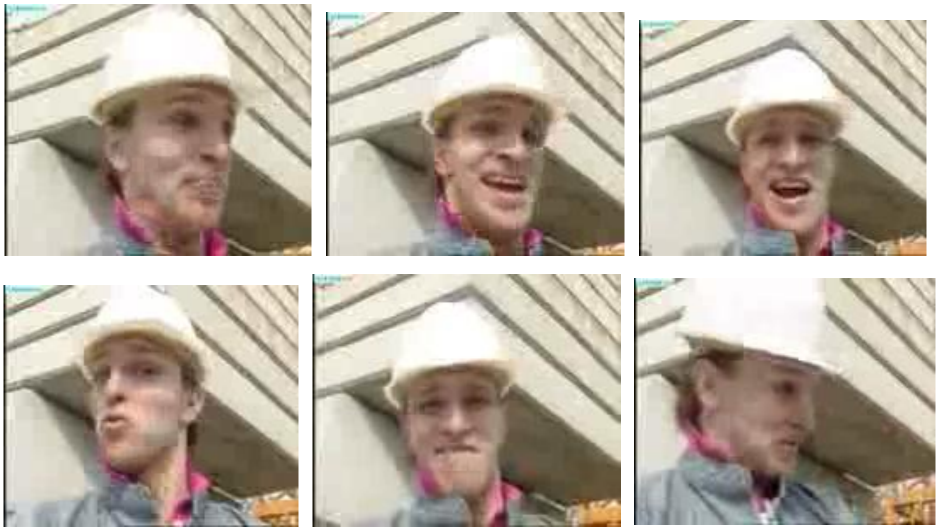

Figure. 4.18 Extracted Motion frames

4.3.3 Watermark Embedding

The process of Encryption is done in following steps-

Step1. To determine which frames in the host video the watermark should be put in, extract the motion frames.

Step 2. DCT is applied on the frame with the aim of splitting the frame into 8X8 pixel block.

Step 3. Apply SVD on the blocks placed prior to DCT to obtain the orthogonal and singular matrix of the frame .

$$I=U\times S \times V \tag{9}$$

Step 4. Now apply the SVD method on the watermark image to be embedded . This will results orthogonal and singular matrix of the watermark .

$$W= U_W \times S_W \times V_W \tag{10}$$

Step 5. Now to exchange the singular matrix S with the matrix S_W

$$I_{wat}=U^T \times S_W \times V^T$$

Step 6. Apply Inverse SVD to I_{wat}

Step 7. Apply the Inverse DCT and this will result the watermarked frame.

Step 8. Repeat the process on selected frames so that the complete video will be watermarked .

Figure. 4.19 Original Video Before Embedding

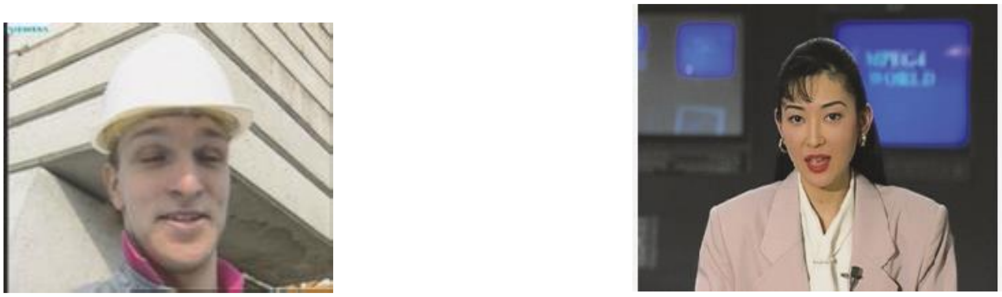

Figure. 4.20 Watermarked Video After Embedding

4.3.4 Watermark Extraction

The process of Watermark Extraction is done in following steps-

Step 1. Extract the motion frames from the watermarked host video .

Step 2. Apply DCT process on the watermarked frame . Divide the image into 8 x 8 block.

Step 3. Apply the SVD process on the watermarked frame to obtain the singular values S_{ew} of it.

Step 4. Apply the SVD process to get all three values , Sw and Vw .

$$W= UW \times SW \times VW \qquad (11)$$

Step 5. Apply SVD on the original watermark image to get the orthogonal and singular matrix .

$$I_W= U_{ew}\times S_{ew} \times V_{ew} \qquad (12)$$

Step 6. Apply Inverse SVD to the , VW from the original watermark and Sew from the watermarked image which will result the final extracted watermark image.

Step 7. In a similar way the watermark can be extracted from other different motion frames.

4.3.5 Performance Evaluation of Proposed Algorithm

The original watermark is shown in Fig.4.22 and the watermarked video is shown in Fig. 4.21. The Watermarked video is shown in Fig.22.

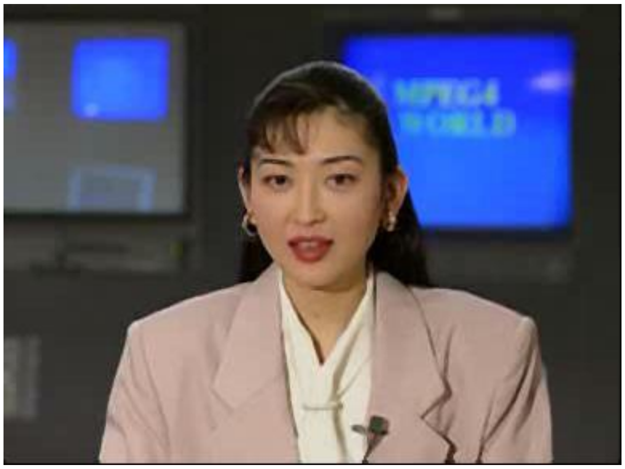

Figure. 4.21. Original video Frame(Akiyo.avi)

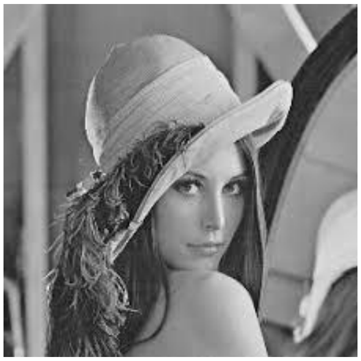

Figure. 4.21. Original Watermark

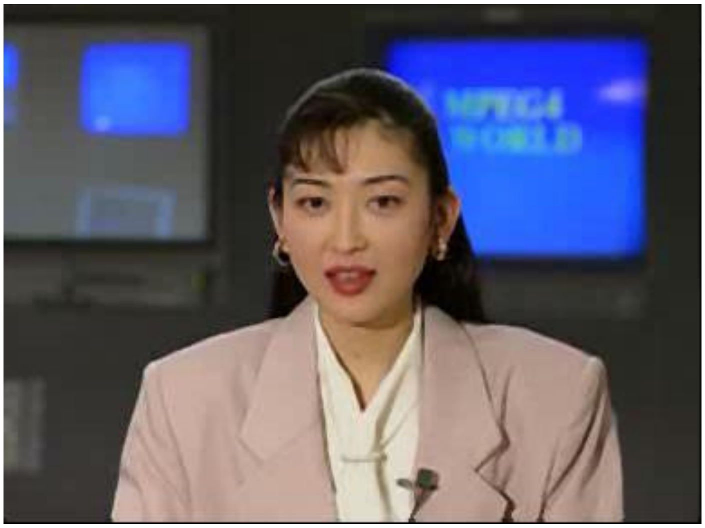

Figure.4.22 Watermarked Video Frame

The suggested algorithm's robustness is covered in this section.Using a variety of attacks on a movie that has a watermark and then extracting the watermark is one way to test the algorithm's robustness. The degree to which the recovered watermark and the original watermark resemble each other demonstrates how resilient the suggested approach is to different types of attacks. Two metrics, known as the Normalised Correlation (NC) and the Structural Similarity Index (SSIM), are frequently used to assess similarity. SSIM is a commonly used tool for comparing two photos' similarity.

The watermarking method's robustness is determined by the NC parameter. Robustness studies apply a variety of watermarking attacks, including geometric assaults, noise addition, filtering, JPEG compression, and several typical attack types, to the watermarked video. Filtering attacks can be classified into three categories: mean, median, and Gaussian Low Pass Filter (LPF). The geometric attacks that are employed are cropping, rotation, and flipping. A subset of the attacks mentioned above are chosen in order to determine how resistant the suggested approach is. The outcomes of SSIM and NC against the carried out assaults on the watermarked films are displayed in Tables 4.4 and Table 4.5.

Table 4.4: Robustness Analysis after attacks (Foreman.avi)

S.No	Attack Performed	SSIM	NC
1	Speckle Noise	0.9912	0.851
2	Frame Deletion(around 10%)	0.8891	0.878
3	Rotation(15 Degree)	0.9001	0.993
4	Gaussian Low Pass Filter	0.9087	0.812
5	Cropping	0.8879	0.898
6	Salt and Pepper	0.8874	0.882
7.	JPEG Compression	0.8003	0.863

Table 4.5: Robustness Analysis after attacks(akiyo.avi)

S.No	Attack Performed	SSIM	NC
1	Speckle Noise	0.8702	0.902
2	Frame Deletion(around 10%)	0.9018	0.807
3	Rotation(15 Degree)	0.8957	0.893
4	Gaussian Low Pass Filter	0.9007	0.957
5	Cropping	0.8977	0.943
6	Salt and Pepper	0.9112	0.921
7.	JPEG Compression	0.8801	0.872

The suggested reliable method for watermarking videos that embeds a watermark into video frames using the Singular Value Decomposition (SVD) and Discrete Cosine Transform (DCT). The experimental results demonstrate that the proposed method offers better robustness against various attacks such as compression, noise addition, and filtering, while still preserving good perceptual quality of the watermarked video. The suggested method uses encryption to make the watermark more robust towards malicious attacks. The watermarked video retains a high degree of structural similarity with the original video, as indicated by the maximum value of the SSIM (Structural Similarity Index) of 0.99. Comparing PSNR values of five images in research, especially in image processing or compression studies, is crucial. PSNR provides a quantitative measure for evaluating image quality after reconstruction or processing. Analyzing PSNR across multiple images helps assess the effectiveness of different methods or algorithms applied to these images. A higher PSNR signifies better fidelity, indicating images closer to their originals. This comparison enables researchers to pinpoint superior techniques, understanding strengths and weaknesses to make informed choices for specific applications. Table 4.6 shows the comparison of proposed methods with some existing methods.

Table 4.6: PSNR/NC based comparison of proposed and existing methods

S.No	Attack Performed	[35] PSNR	[85] PSNR	[33] NC	[32] PSNR	Pro.-1 PSNR	Pro.-2 NC
1	**Speckle Noise**	32	12	0.92	28.83	39.0047	0.902
2	**Frame Deletion(around 10%)**	-	-	-	-	38.0021	0.807
3	**Rotation(15 Degree)**	37	-	0.65	26.91	41.2414	0.893
4	**Gaussian Low Pass Filter**	-	12	0.88	28.84	43.5724	0.957
5	**Cropping**	22	11	-	28.86	40.0122	0.943
6	**Salt and Pepper**	38	-	-	28.86	41.2141	0.921
7.	**JPEG Compression**	-	-	-	28.94	-	0.872

CHAPTER 5
CONCLUSION & FUTURE WORK

5.1 Conclusion

The subject of multimedia security in formation and delivery is the focus of this thesis. The implications of this thesis and their impact on numerous variables linked to security when distributing multimedia content are discussed in this concluding chapter, with a special emphasis on piracy detection using an exclusive experimental setting. The chapter concludes with a few possibilities for expanding the scope and application of the work provided in this thesis. Because of the rapid advancement of technology and the growing demand for multimedia services, it is now feasible to easily distribute these videos, which is a significant benefit of the current communication medium. Because copying and freely modifying digital data is common during correspondence, protecting media content is a difficult undertaking.

SVD provides robustness to common signal processing operations. By embedding watermarks in the singular values, the watermark becomes less susceptible to common video processing operations, such as compression, filtering, or resizing, ensuring robustness against unintentional distortions. SVD allows for modifying the singular values in a way that their statistical properties remain consistent with the original matrix. This helps in maintaining the perceptual quality of the video and ensures that the watermark is transparent to viewers. Embedding the watermark in the SVD domain can enhance the security of the watermarking system. By using the singular values, which represent the intrinsic characteristics of the video frames, the watermark can be hidden more effectively, making it harder for unauthorized users to detect or remove. SVD provides a natural way to select the appropriate singular values for watermark embedding, allowing for selective embedding in regions with less impact on the perceptual quality. This selective approach enhances robustness and minimizes the visual impact of the watermark on the video.

A multi-faceted approach in implementing video watermarking using a combination of three-time Discrete Wavelet Transform (DWT) aims to strike a balance between robustness and perceptual transparency. DWT decomposes the video frames into multiple frequency bands, providing flexibility in choosing where to embed the watermark. By focusing on specific frequency components, the watermark can be inserted in regions that are less perceptually sensitive, minimizing the impact on visual quality.

The multi-faceted approach allows for selective embedding, meaning that watermark information can be inserted in specific frequency and temporal components based on their perceptual impact. This adaptability enables the system to adjust the embedding strategy, balancing robustness and transparency according to the characteristics of the video content. The use of three-time DWT involves decomposing each frame into three temporal levels (LL, LH, HL, and HH), allowing for the embedding of watermark information not only in the spatial domain but also across different temporal scales. This temporal embedding provides robustness against frame-wise manipulations, such as frame deletion or insertion.

The approach takes into account the characteristics of the Human Visual System (HVS) to identify regions where the watermark is less likely to be perceptually noticeable. This consideration is essential for achieving transparency while maintaining the desired level of robustness against attacks.

Digital watermarking is one of the most effective ways to protect multimedia material against copyright infringement. The four alternative approaches to video watermarking algorithms with colour watermarks for copyright protection of digital video were created in this research. The video watermarking approach that is based on discrete wavelet transform technology were first investigated in the uncompressed domain. The wavelet coefficients were used to insert the identical watermark at two separate sub-bands at the same time. The goal of creating the resulting watermarking design model is to use it in personal watermarking applications in which the original video must be deemed available for watermark extraction with the owner.

The first solution proposes wavelet-based video watermarking with a colour watermark image to improve security and simplify the process. In place to evade the embedding time delay, a selective frame embedding-based technique is used. The concatenated colour watermark is hidden in the selected frames after they have undergone two level decomposition. The original video in this method was uncompressed brief video sequences, and the findings reveal that the watermarked video quality is good and that estimating the original and embedded video is challenging. Our non-blind watermarking methodology clearly registered average NC values of 0.8541, which is higher than prior methods. The proposed approach demonstrates invisibility in the face of noise and geometrical challenges.

Another video watermarking approach relies on motion frames and employs the DWT, and SVD transform domains. The suggested method solves the drawbacks of scene change detection-based methods. The scheme's superiority is that it strengthens the overall watermarking process by just examining motion frames, as opposed to an all-frames method. Another distinction is that the higher perceptibility attained demonstrates that there is no noticeable difference between both the watermarked and original frames. Furthermore, outstanding resilience results are obtained by employing a succession of unintended and intentional attacks in two modes.

5.2 Future Scope of the Work

This thesis examines the research work on video watermarking. However, in future development, the following task could be pursued to secure digital video copyright.

- Integrating motion frame based and visual cryptography techniques into the watermarking process improves the security of the process and increases its robustness against collusion attacks. When such research is combined with the findings of this thesis, a complete solution to digital right management for copyright protection of video multimedia products can be provided.
- Using the MPEG-2 compression standard, more improvements can be made by producing distinct pieces of encrypted watermarks to be put in discontinuous frames of video. This method improves the overall security of real-time video watermarking systems.
- Any video watermarking scheme's resilience should be able to survive further attacks such as ambiguity, collusion, and joint attacks, and work can also be extended to increase the capacity of watermark bits utilized for embedding.

References

[1] A. A. Alwan, M. A. Shahidan, N. N. A. Sjarif, M. M. Hashim, and M. S. M. Rahim, "A review and open issues of diverse text watermarking techniques in spatial domain," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 17, 2018.

[2] B. Pinkas, "Cryptographic techniques for privacy-preserving data mining," *ACM SIGKDD Explor. Newsl.*, vol. 4, no. 2, 2002, doi: 10.1145/772862.772865.

[3] H. A. Abdullah, "Hybrid method for video watermarking & encryption," in *Proceedings of the 2012 International Conference on Image Processing, Computer Vision, and Pattern Recognition, IPCV 2012*, 2012, vol. 1.

[4] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "Image steganography techniques: an overview," *Int. J. Comput. Sci. Secur.*, vol. 6, no. 3, 2012.

[5] I. J. Cox and M. L. Miller, "Preprocessing media to facilitate later insertion of a watermark," in *International Conference on Digital Signal Processing, DSP*, 2002, vol. 1, doi: 10.1109/ICDSP.2002.1027817.

[6] N. Leelavathy, E. V Prasad, and S. S. Kumar, "Video Watermarking Techniques: A Review," *Int. J. Comput. Appl.*, vol. 104, no. 7, 2014, doi: 10.5120/18215-9199.

[7] H. Tao, L. Chongmin, J. M. Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: A review," *J. Appl. Res. Technol.*, vol. 12, no. 1, 2014, doi: 10.1016/S1665-6423(14)71612-8.

[8] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," *IEEE Transactions on Signal Processing*, vol. 53, no. 10 II. 2005, doi: 10.1109/TSP.2005.855418.

[9] R. Naskar and R. S. Chakraborty, "Reversible Digital Watermarking: Theory and Practices," *Synth. Lect. Inf. Secur. Privacy, Trust*, vol. 5, no. 1, 2014, doi: 10.2200/s00567ed1v01y201401spt010.

[10] X. Chang, W. Wang, J. Zhao, and L. Zhang, "A survey of digital video watermarking," in *Proceedings - 2011 7th International Conference on Natural Computation, ICNC 2011*,

2011, vol. 1, doi: 10.1109/ICNC.2011.6022111.

[11] R. T. Paul, "Review of Robust Video Watermarking Techniques," *IJCA Spec. Issue Comput. Sci. - New Dimens. Perspect.*, vol. 3, no. 1, 2011.

[12] C. C. Phin, N. H. A. Rahman, and N. C. Pa, "A digital image watermarking system: An application of dual layer watermarking technique," *Int. J. Informatics Vis.*, vol. 1, no. 4–2, 2017, doi: 10.30630/joiv.1.4-2.78.

[13] D. Galindo, S. Martin, P. Morillo, and J. L. Villar, "A practical public key cryptosystem from Paillier and Rabin schemes," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 2567, 2003, doi: 10.1007/3-540-36288-6_21.

[14] Y. Yang, Y. Zhao, J. Zhang, J. Huang, and Y. Gao, "Recent Development of Theory and Application on Homomorphic Encryption," *Dianzi Yu Xinxi Xuebao/Journal Electron. Inf. Technol.*, vol. 43, no. 2, 2021, doi: 10.11999/JEIT191019.

[15] K. Hameed, A. Mumtaz, and S. a. M. Gilani, "Digital Image Watermarking in the Wavelet Transform Domain," *World Acad. Sci. Eng. Technol.*, vol. 2, 2008.

[16] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, 1998, doi: 10.1109/49.668979.

[17] J. Raju, "A study of joint lossless compression and encryption scheme," 2017, doi: 10.1109/ICCPCT.2017.8074366.

[18] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3. 2010, doi: 10.1016/j.sigpro.2009.08.010.

[19] J. S. Walker and T. Q. Nguyen, "Adaptive scanning methods for wavelet difference reduction in lossy image compression," in *IEEE International Conference on Image Processing*, 2000, vol. 3, doi: 10.1109/icip.2000.899325.

[20] A. Kipnis and E. Hibshoosh, "Efficient Methods for Practical Fully Homomorphic Symmetric-key Encrypton, Randomization and Verification.," *IACR Cryptol. ePrint Arch.*, 2012.

[21] S. B. Rakesh Ahuja, “All Aspects of Digital Video Watermarking Under an Umbrella,” *Int. J. Image, Graph. Signal Process.*, vol. 7, no. 12, p. 54, 2015.

[22] L. Zhi, Z. Xinglei, L. Yong, and S. Qibin, “Constructing secure content-dependent watermarking scheme using homomorphic encryption,” 2007, doi: 10.1109/icme.2007.4284728.

[23] M. N. Sakib, S. Das Gupta, and S. N. Biswas, “A Robust dwt-based compressed domain video watermarking technique,” *Int. J. Image Graph.*, vol. 20, no. 1, 2020, doi: 10.1142/S0219467820500047.

[24] B. Sharma, P. Sharma, and V. Kulshreshtha, “Study of wavelets using chaotic map on DWT based blind video watermarking,” *Int. J. Adv. Technol. Eng. Explor.*, vol. 4, no. 37, 2017, doi: 10.19101/ijatee.2017.437006.

[25] M. M. Ibrahim, N. S. Abdel Kader, and M. Zorkany, “Video multiple watermarking technique based on image interlacing using dwt,” *Sci. World J.*, vol. 2014, 2014, doi: 10.1155/2014/634828.

[26] A. Adhikari and M. Sing, “A Hybrid Video Watermarking Technique based on DWT, SVD and SCHUR Decomposition,” *Int. J. Comput. Appl.*, vol. 179, no. 9, 2018, doi: 10.5120/ijca2018916079.

[27] S. A. M. Al-Taweel and P. Sumari, “Robust video watermarking based on 3D-DWT domain,” 2009, doi: 10.1109/TENCON.2009.5395859.

[28] K. A. Rajurkar and P. S. K. Nanda, “A Hybrid DWT, PCA and SVD based Digital video watermarking Scheme-A Review,” *IJARCCE*, 2015, doi: 10.17148/ijarcce.2015.4321.

[29] G. Singh and N. Goel, “Entropy based image watermarking using discrete wavelet transform and singular value decomposition,” 2016.

[30] F. Alenizi, F. Kurdahi, A. Eltawil, and A. Aljumah, “DWT-based watermarking technique for video authentication,” in *Proceedings of the IEEE International Conference on Electronics, Circuits, and Systems*, 2016, vol. 2016-March, doi:

10.1109/ICECS.2015.7440244.

[31] M. Shanmugam and A. Chokkalingam, “Performance analysis of 2 level DWT-SVD based non blind and blind video watermarking using range conversion method,” *Microsyst. Technol.*, vol. 24, no. 12, 2018, doi: 10.1007/s00542-018-3870-x.

[32] A. M. Kothari, V. Dwivedi, and R. M. Thanki, “Singular Value Decomposition (SVD)-Based video watermarking,” in *Signals and Communication Technology*, 2019.

[33] K. Meenakshi, K. Swaraja, and P. Kora, “A robust DCT-SVD based video watermarking using zigzag scanning,” in *Advances in Intelligent Systems and Computing*, 2019, vol. 900, doi: 10.1007/978-981-13-3600-3_45.

[34] N. Patil and V. R. Udupi, “Development of reversible video watermarking algorithm based on hybrid DWT-SVD,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 4S2, 2019.

[35] I. Ahmad and S. Shin, “A novel hybrid image encryption–compression scheme by combining chaos theory and number theory,” *Signal Process. Image Commun.*, vol. 98, 2021, doi: 10.1016/j.image.2021.116418.

[36] I. F. Elashry *et al.*, “Efficient chaotic-based image cryptosystem with different modes of operation,” *Multimed. Tools Appl.*, vol. 79, no. 29–30, 2020, doi: 10.1007/s11042-019-08322-5.

[37] F. A. Khan, A. Bouridane, S. Boussakta, R. Jiang, and S. Almaadeed, “Secure facial recognition in the encrypted domain using a local ternary pattern approach,” *J. Inf. Secur. Appl.*, vol. 59, 2021, doi: 10.1016/j.jisa.2021.102810.

[38] I. Nouioua, N. Amardjia, and S. Belilita, “A Novel Blind and Robust Video Watermarking Technique in Fast Motion Frames Based on SVD and MR-SVD,” *Secur. Commun. Networks*, vol. 2018, 2018, doi: 10.1155/2018/6712065.

[39] Purnima and R. Ahuja, “Design of digital video watermarking technique based on motion frames,” *J. Comput. Theor. Nanosci.*, vol. 16, no. 10, 2019, doi: 10.1166/jctn.2019.8521.

[40] P. Kadian, S. M. Arora, and N. Arora, “Robust Digital Watermarking Techniques for Copyright Protection of Digital Data: A Survey,” *Wireless Personal Communications*, vol.

118, no. 4. 2021, doi: 10.1007/s11277-021-08177-w.

[41] P. P., “DIGITAL VIDEO WATERMARKING USING MODIFIED LSB AND DCT TECHNIQUE,” *Int. J. Res. Eng. Technol.*, vol. 03, no. 04, 2014, doi: 10.15623/ijret.2014.0304112.

[42] G. Doërr and J. L. Dugelay, “A guide tour of video watermarking,” in *Signal Processing: Image Communication*, 2003, vol. 18, no. 4, doi: 10.1016/S0923-5965(02)00144-3.

[43] T. Sathies Kumar and C. Arun, “A review of robust video watermarking technique,” *Journal of Advanced Research in Dynamical and Control Systems*, vol. 2017, no. Special Issue 2. 2017.

[44] M. George, J. Y. Chouinard, and N. Georganas, “Digital watermarking of images and video using direct sequence spread spectrum techniques,” in *Canadian Conference on Electrical and Computer Engineering*, 1999, vol. 1, doi: 10.1109/ccece.1999.807181.

[45] K. Su, D. Kundur, and D. Hatzinakos, “<title>Novel approach to collusion-resistant video watermarking</title>,” in *Security and Watermarking of Multimedia Contents IV*, 2002, vol. 4675, doi: 10.1117/12.465307.

[46] A. Houmansadr and S. Ghaemmaghami, “A novel video watermarking method using visual cryptography,” 2006, doi: 10.1109/iceis.2006.1703171.

[47] L. Wei, “A improved video watermarking scheme based on spread-spectrum technique,” in *2010 International Conference on Networking and Digital Society, ICNDS 2010*, 2010, vol. 1, doi: 10.1109/ICNDS.2010.5479254.

[48] R. O. Preda and N. Vizireanu, “New robust watermarking scheme for video copyright protection in the spatial domain,” *UPB Sci. Bull. Ser. C Electr. Eng.*, vol. 73, no. 1, 2011.

[49] L. Rajab, T. Al-Khatib, and A. Al-Haj, “Video watermarking algorithms using the SVD transform,” *Eur. J. Sci. Res.*, vol. 30, no. 3, 2009.

[50] L. Chen and J. Zhao, “Adaptive digital watermarking using RDWT and SVD,” 2015, doi: 10.1109/HAVE.2015.7359451.

[51] Lindsay, “A tutorial on Principal Components Analysis,” *Commun. Stat. - Theory*

Methods, vol. 17, no. 9, 2002.

[52] N. Chawla and V. Singh, “A novel video watermarking scheme based on DWT and PCA,” *Int. J. Eng. Adv. Technol.*, vol. 7, no. 5, 2018.

[53] H. S. Hou, “A fast recursive algorithm for computing the discrete cosine transform,” *IEEE Trans. Acoust.*, vol. 35, no. 10, 1987, doi: 10.1109/TASSP.1987.1165060.

[54] L. S. Liu, R. H. Li, and Q. Gao, “A robust video watermarking scheme based on DCT,” 2005, doi: 10.1109/icmlc.2005.1527856.

[55] A. Koz and A. A. Alatan, “Oblivious spatio-temporal watermarking of digital video by exploiting the human visual system,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 3, 2008, doi: 10.1109/TCSVT.2008.918446.

[56] N. Deshpande, A. Rajurkar, and R. Manthalkar, “Robust DCT based video watermarking algorithms for assorted watermarks,” in *ICSPS 2010 - Proceedings of the 2010 2nd International Conference on Signal Processing Systems*, 2010, vol. 1, doi: 10.1109/ICSPS.2010.5555632.

[57] H. Y. Huang, C. H. Yang, and W. H. Hsu, “A video watermarking technique based on pseudo-3-D DCT and quantization index modulation,” *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 4, 2010, doi: 10.1109/TIFS.2010.2080675.

[58] A. Joshi, V. Mishra, and R. Patrikar, “Real time implementation of integer DCT based video watermarking architecture,” *Int. Arab J. Inf. Technol.*, vol. 12, no. 6A, 2015.

[59] S. W. Kim, S. Suthaharan, H. K. Lee, and K. R. Rao, “Perceptually tuned robust watermarking scheme for digital video using motion entropy masking,” 1999, doi: 10.1109/icce.1999.785187.

[60] S. A. M. Al-Taweel, P. Sumari, S. A. K. Alomari, and A. J. A. Husain, “Digital video watermarking in the discrete cosine transform domain,” *J. Comput. Sci.*, vol. 5, no. 8, 2009, doi: 10.3844/jcssp.2009.536.543.

[61] C. S. Burrus, R. A. Gopinath, and H. Guo, *Introduction to Wavelets and Wavelet Transforms: A Primer*. 1998.

[62] D. B. Percival and D. Mondal, “A Wavelet Variance Primer,” in *Handbook of Statistics*, vol. 30, 2012.

[63] M. D. Swanson, B. Zhu, and A. H. Tewfik, “Multiresolution scene-based video watermarking using perceptual models,” *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, 1998, doi: 10.1109/49.668976.

[64] C. V. Serdean, M. A. Ambroze, M. Tomlinson, and J. G. Wade, “Adding robustness to geometrical attacks to a wavelet based, blind video watermarking system,” in *Proceedings - 2002 IEEE International Conference on Multimedia and Expo, ICME 2002*, 2002, vol. 1, doi: 10.1109/ICME.2002.1035842.

[65] G. Yang, X. Sun, and X. Wang, “A genetic algorithm based video watermarking in the DWT domain,” in *2006 International Conference on Computational Intelligence and Security, ICCIAS 2006*, 2006, vol. 2, doi: 10.1109/ICCIAS.2006.295247.

[66] P. W. Chan, M. R. Lyu, and R. T. Chin, “A novel scheme for hybrid digital video watermarking: Approach, evaluation and experimentation,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 15, no. 12, 2005, doi: 10.1109/TCSVT.2005.856932.

[67] S. Karmani, R. Djemal, and R. Tourki, “Efficient hardware architecture of 2D-scan-based wavelet watermarking for image and video,” *Comput. Stand. Interfaces*, vol. 31, no. 4, 2009, doi: 10.1016/j.csi.2008.09.015.

[68] X. Li and R. Wang, “A Video Watermarking Scheme Based on 3D-DWT and Neural Network,” 2008, doi: 10.1109/ism.workshops.2007.29.

[69] C. K.R and R. K., “DWT Based Blind Digital Video Watermarking Scheme for Video Authentication,” *Int. J. Comput. Appl.*, vol. 4, no. 10, 2010, doi: 10.5120/863-1213.

[70] X. Y. Wang, L. Li, H. F. Li, P. P. Niu, S. M. Wang, and H. Y. Yang, “A Blind Watermark Decoder in DT CWT Domain using Multivariate Bessel K Form Distribution,” *Jisuanji Xuebao/Chinese J. Comput.*, vol. 42, no. 5, 2019, doi: 10.11897/SP.J.1016.2019.01112.

[71] M. Masoumi and S. Amiri, “A blind scene-based watermarking for video copyright protection,” *AEU - Int. J. Electron. Commun.*, vol. 67, no. 6, 2013, doi: 10.1016/j.aeue.2012.11.009.

[72] M. El'Arbi, M. Koubaa, M. Charfeddine, and C. Ben Amar, "A dynamic video watermarking algorithm in fast motion areas in the wavelet domain," *Multimed. Tools Appl.*, vol. 55, no. 3, 2011, doi: 10.1007/s11042-010-0580-5.

[73] T. R. Singh, K. M. Singh, and S. Roy, "Video watermarking scheme based on visual cryptography and scene change detection," *AEU - Int. J. Electron. Commun.*, vol. 67, no. 8, 2013, doi: 10.1016/j.aeue.2013.01.008.

[74] Y. Y. Lee, H. S. Jung, and S. U. Lee, "Multi-bit video watermarking based on 3D DFT using perceptual models," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 2939, 2004, doi: 10.1007/978-3-540-24624-4_23.

[75] L. Agilandeeswari and K. Ganesan, "A robust color video watermarking scheme based on hybrid embedding techniques," *Multimed. Tools Appl.*, vol. 75, no. 14, 2016, doi: 10.1007/s11042-015-2789-9.

[76] L. Rajab, T. Al-Khatib, and A. Al-Haj, "A Blind DWT-SCHUR Based Digital Video Watermarking Technique," *J. Softw. Eng. Appl.*, vol. 08, no. 04, 2015, doi: 10.4236/jsea.2015.84023.

[77] R. N. P. Hitesh Patel, Jignesh Patoliya, Pradip Panchal, "Digital Robust Video Watermarking Using 4-level DWT," *Int. J. Adv. Eng. Technol.*, vol. 11, no. 2, p. 101, 2010.

[78] J. Hussein and A. Mohammed, "Robust Video Watermarking using Multi-Band Wavelet Transform," *J. Comput. Sci.*, vol. 6, no. 1, 2009.

[79] A. A. Abdulfetah, X. Sun, and H. Yang, "Robust adaptive video watermarking scheme using visual models in DWT domain," *Inf. Technol. J.*, vol. 9, no. 7, 2010, doi: 10.3923/itj.2010.1409.1414.

[80] H. A. S. S. Bedi, Rakesh Ahuja, "Copyright Protection Using Video Watermarking Based on Wavelet Transformation in Multiband," *Int. J. Comput. Appl.*, vol. 66, no. 8, p. 5, 2013.

[81] M. Masoumi, "A Blind Video Watermarking Scheme Based on 3D Discrete Wavelet Transform," *Int. J. Innov. Manag. Technol.*, vol. 3, no. 4, 2012, doi: 10.7763/ijimt.2012.v3.281.

[82] T. Tabassum and S. M. M. Islam, “A digital video watermarking technique based on identical frame extraction in 3-Level DWT,” 2012, doi: 10.1109/ICCITechn.2012.6509780.

[83] R. Nanmaran *et al.*, “Wavelet transform based multiple image watermarking technique,” in *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 993, no. 1, doi: 10.1088/1757-899X/993/1/012167.

[84] J. Kaufman and M. Celenk, “Digital video watermarking using singular value decomposition and 2D principal component analysis,” 2006, doi: 10.1109/ICIP.2006.312982.

[85] R. K. Nadesh, R. Srinivasa Perumal, K. Arivuselvan, and K. Aishwarya, “A Hybrid Approach for Video Watermarking Using DWT and SVD,” 2019, doi: 10.1109/i-PACT44901.2019.8960038.

[86] S. A. Patil, “Digital Video Watermarking Using Dwt And Pca,” *IOSR J. Eng.*, vol. 3, no. 11, 2013, doi: 10.9790/3021-031144549.

[87] G. J. Xu and R. D. Wang, “A blind video watermarking algorithm resisting to rotation attack,” 2009, doi: 10.1109/ICCCS.2009.34.

[88] M. El’Arbi, C. Ben Amar, and H. Nicolas, “Video watermarking based on neural networks,” in *2006 IEEE International Conference on Multimedia and Expo, ICME 2006 - Proceedings*, 2006, vol. 2006, doi: 10.1109/ICME.2006.262846.

[89] E. E. Abdallah, A. Ben Hamza, and P. Bhattacharya, “Video watermarking using wavelet transform and tensor algebra,” *Signal, Image Video Process.*, vol. 4, no. 2, 2010, doi: 10.1007/s11760-009-0114-7.

[90] D. Chaudhary and P. Sharma, “Digital Video Watermarking Scheme using wavelets with MATLAB,” *Int. J. Comput. Appl.*, vol. 180, no. 14, 2018, doi: 10.5120/ijca2018916272.

[91] M. Omidyeganeh, H. Khalilian, S. Ghaemmaghami, and S. Shirmohammadi, “Robust digital video watermarking in an orthogonal parametric space,” 2010, doi: 10.1109/TENCON.2010.5686643.

[92] T. Shankar and G. Yamuna, “A robust video watermarking scheme using sparse principal component analysis and wavelet transform,” in *International Journal of Computational Science and Engineering*, 2017, vol. 15, no. 3–4, doi: 10.1504/IJCSE.2017.087409.

[93] S. Murty.P, K. Venkatesh, and R. Kumar. P, “A Semi-Blind Reference Video Watermarking using Hybrid Transforms for Copyright Protection,” *Int. J. Comput. Appl.*, vol. 51, no. 9, 2012, doi: 10.5120/8067-1460.

[94] T. Geetamma and J. Beatrice Seventline, “A novelblind audio and video watermarking,” *Int. J. Appl. Eng. Res.*, vol. 10, no. 17, 2015.

[95] H. M. E. Salwa A.K Mostafa, A. S. Tolba , F. M. Abdelkader, “Video Watermarking Scheme Based on Principal Component Analysis and Wavelet Transform,” *Int. J. Comput. Sci. Netw. Secur.*, vol. 9, no. 8, p. 45, 2009.

[96] S. Das, P. Bandyopadhyay, M. Banerjee, and A. Chaudhuri, “Uncompressed video authentication through a chip based watermarking scheme,” 2011, doi: 10.1109/EAIT.2011.49.

[97] H. D. Kim, T. W. Oh, J. W. Lee, and H. K. Lee, “A hybrid watermarking scheme for CCL-applied video contents,” 2011, doi: 10.1109/EuVIP.2011.6045512.

[98] N. I. Yassin, N. M. Salem, and M. I. E. Adawy, “Entropy based video watermarking scheme using wavelet transform and Principle Component Analysis,” 2012, doi: 10.1109/ICEngTechnol.2012.6396128.

[99] T. A.-K. & A. A.-H. Lama Rajab, “A Blind DWTSCHUR Based Digital Video Watermarking Technique,” *J. Softw. Eng. Appl.*, vol. 8, no. 4, p. 224, 2015.

[100] N. I. Yassin, N. M. Salem, and M. I. El Adawy, “QIM blind video watermarking scheme based on Wavelet transform and principal component analysis,” *Alexandria Eng. J.*, vol. 53, no. 4, 2014, doi: 10.1016/j.aej.2014.07.008.

[101] H. Agarwal, R. Ahuja, and S. S. Bedi, “Highly Robust and Imperceptible Luminance Based Hybrid Digital Video Watermarking Scheme for Ownership Protection,” *Int. J. Image, Graph. Signal Process.*, vol. 4, no. 11, 2012, doi: 10.5815/ijigsp.2012.11.07.

[102] D. K. Thind and S. Jindal, “A semi blind DWT-SVD video watermarking,” in *Procedia Computer Science*, 2015, vol. 46, doi: 10.1016/j.procs.2015.02.104.

[103] X. Liu, R. Zhao, F. Li, S. Liao, Y. Ding, and B. Zou, “Novel robust zero-watermarking scheme for digital rights management of 3D videos,” *Signal Process. Image Commun.*, vol. 54, 2017, doi: 10.1016/j.image.2017.03.002.

[104] T. R. Singh, K. M. Singh, and S. Roy, “Robust video watermarking scheme based on visual cryptography,” 2012, doi: 10.1109/WICT.2012.6409198.

[105] N. Deshpande, A. Rajurkar, and R. R. Mathalkar, “Robust Dual Watermarking Scheme for Video Derived from Strategy Fusion,” *Int. J. Image, Graph. Signal Process.*, vol. 6, no. 5, 2014, doi: 10.5815/ijigsp.2014.05.03.

[106] O. S. Faragallah, “Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain,” *AEU - Int. J. Electron. Commun.*, vol. 67, no. 3, 2013, doi: 10.1016/j.aeue.2012.07.010.

[107] N. Sahu and A. Sur, “SIFT based video watermarking resistant to temporal scaling,” *J. Vis. Commun. Image Represent.*, vol. 45, 2017, doi: 10.1016/j.jvcir.2017.02.013.

[108] J. Li, P. Zhong, Y. Zhu, and C. Guo, “Robust wavelet-based watermarking scheme for video copyright protection,” 2014, doi: 10.1109/CISP.2014.7003762.

[109] I. A. Ansari, M. Pant, and C. W. Ahn, “Robust and false positive free watermarking in IWT domain using SVD and ABC,” *Eng. Appl. Artif. Intell.*, vol. 49, 2016, doi: 10.1016/j.engappai.2015.12.004.

[110] Z. Li, S. Q. Chen, and X. Y. Cheng, “Dual Video Watermarking Algorithm Based on SIFT and HVS in the Contourlet Domain,” *IEEE Access,* vol. 7, 2019, doi: 10.1109/ACCESS.2019.2899378.

[111] P. I. Solachidis V, “Circularly Symmetric Watermark Embedding in 2D DFT Domain,” in *IEEE Trans Image Process*, 2001, p. 1741.

[112] M. J. Tsai, K. Y. Yu, and Y. Z. Chen, “Joint wavelet and spatial transformation for digital watermarking,” *IEEE Trans. Consum. Electron.*, vol. 46, no. 1, 2000, doi:

10.1109/30.826405.

[113] V. Santhi and P. Arulmozhivarman, “Hadamard transform based adaptive visible/invisible watermarking scheme for digital images,” *J. Inf. Secur. Appl.*, vol. 18, no. 4, 2013, doi: 10.1016/j.istr.2013.01.001.

[114] J. Liu, D. Huang, and J. Hu, “Orthogonal wavelet bases for digital watermarking,” *Dianzi Yu Xinxi Xuebao/Journal Electron. Inf. Technol.*, vol. 25, no. 4, 2003.

Curriculum Vitae

Praful Saxena

Adarsh Colony , Civil Lines , Rampur(U.P)-244901
Mob- 7906885774 email- shyam.praful@gmail.com

OBJECTIVE

To obtain a position as an elementary faculty that will utilize my dedication to student's educational needs and development. To encourage creativity and higher-order thinking in a way that increases student performance .

PROFESSIONAL QUALIFICATION

- **Ph.D(Pursuing)** from Maharishi University of Information Technology Lucknow.
- **M.Tech (Computer Engineering)** from Shobhit University Meerut(U.P) with 8.14 CGPA.
- **B.E(CSE)** from Dr. B R Ambedkar University Agra(U.P) with 70%.

TEACHING EXPERIENCE (TOTAL 20 YRS)

- Working as an **Assistant Professor** at **"Moradabad Institute of Technology, Moradabad"** from August 2023 to till date.
- Worked with **iNurture Education Solutions Pvt Ltd Bengaluru** as a **Senior Faculty – IT(Information Security)** From Aug-2016 to May-2023.
- Worked as an **Assistant Professor** at **"Rakshpal Bahadur College of Engg. & Technology Bareilly"** from Aug-2015. To July 2016.
- Worked as an **Assistant Professor** at **"Krishna Institute of Management & Technology Moradabad"** form July 2009 to July-2015.
- Worked as a **Lecturer** at **"Moradabad Institute of Technology Moradabad"** from Aug 2004 to Aug 2009.
- Worked as a **Lecturer** at "**Bhagwant Institute of Technology Muzaffarnagar**" from Aug 2003 to Aug 2004.

TECHNICAL CERTIFICATION

- Qualified Microsoft Certification (MTA 98-367) in **"Security Fundamentals"** .
- Qualified NPTEL certification course in **"Information Security-IV"** conducted by IIT Chennai.
- Qualified NPTEL certification course in **"Ethical Hacking "** conducted by IIT Chennai .
- Qualified NPTEL certification course in **"Cryptography & Network Security"** conducted by IIT Chennai.
- Qualified Certification in **"E-Content Development Course "** from International Institute of Organized Research(I2OR) .

RESEARCH PUBLICATIONS

International Conferences

- A. Ahad, M. S. Khan and P. Saxena, *"Analysis of Keylogging spyware for information theft,"* 2023 1st International Conference on Intelligent Computing and Research Trends (ICRT), Roorkee, India, 2023, pp. 1-4, doi: 10.1109/ICRT57042.2023.10146672.
- P. Saxena and S. Kumar, *"SCD based Video Watermarking by Using Wavelet Transform and SVD,"* 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), Sonepat, India, 2021, pp. 288-291, doi: 10.1109/CCICT53244.2021.00060.
- P.Saxena and S. Kumar, *" Video Watermarking Technique based on Motion Frame by using Encryption Method, "* 2021 International Conference on Emerging Trends in Mathematical Sciences & Computing (IEMSC) ,Kolkata,India .
- N. K. Verma, S. Kumar, M. Kumar and P. Saxena, "An Alternate Approach to Improve Access Time for Defining Frequent Item Set Through 'A-Apriori' in Textual Data Set," 2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, India, 2020, pp. 1-6, doi: 10.1109/ICRAIE51050.2020.9358344.
- P.Saxena, H.John and S. Rastogi (2013) "DWT-DCT-SVD based semi –blind reference image watermarking scheme using Trignometric function" at ICEMT 2013 Sri Lanka .
- P.Saxena, S.Garg and A. Srivastava(2012) " DWT-SVD Semi Blind Image Watermarking Using High Frequency Band" published At ICCSIT-2012 PSRC Singapore.
- P.Saxena(2012) " A Nascent Approach for Symmetric Key Encryption Using Double DES" At ICCA-12 Pondicherry (India).

International Journals

- Saxena, Praful & Kumar, Santosh(2023) Robust video watermarking algorithm based on motion frames and encryption, Journal of Discrete Mathematical Sciences and Cryptography, 26:5, 1327–1339, DOI: 10.47974/JDMSC-1748
- P. . Saxena and S. . Kumar, "Robust Video Watermarking Algorithm based on DCT-SVD approach and Encryption ", IJRITCC, vol. 11, no. 5, pp. 85–91, May 2023.
- Saxena. P , Kumar .S (2021)."Hybrid Approach based Video Watermarking Technique by using scene detection" .IJRCTCSIT July '21, Vol. VII Issue I.
- Saxena. P , Kumar .S (2019). Robust Video Watermarking scheme based on DWT and SVD approach using Multiple frequency bands .Parishodh Journal Sep '19, Vol. VIII Issue IX.
- Saxena. P., Sharma. S. K., and Verma. N. K (2017). An Analysis of Energy Efficiency and Traffic Using Cloud Computing in Portable Devices., i-manager's Journal on Cloud Computing, 4(1), Jan-Jun'17, 1-7.
- Saxena. P, and Sharma. S. K (2017).Analysis of Network Traffic by using Packet Sniffing Tool:Wireshark ., IJARIIT ,Vol.3 Issue 6.
- A.Srivastava and P.Saxena "DWT-DCT-SVD based semi blind Image Watermarking using middle frequency band", IOSR-JCE Vol. 12 Issue 2 P.No. 63-66.
- P.Saxena, H.John and S. Rastogi (2013) "DWT-DCT-SVD based semi –blind reference image watermarking scheme using Trignometric function" at IJCCIT 2014 Sri Lanka Vol.2 Issue 2.
- P.Saxena and I.Saxena(2013) "A Robust Semi-Blind Image Watermarking Technique" at IOSR-JCE 2013 Vol.10 Issue 10 (e-ISSN: 2278-0661, p- ISSN: 2278-8727)
- P.Saxena(2014) "DWT-SVD based image watermarking: a semi blind approach" at IGJER Vol.9 Issue 2 .

PG PROJECT GUIDED

- M.Tech Thesis is Guided on the topic of "Robust Image Watermarking based onDWT & SVD" . Scholar from " Teerthankar Mahaveer University Moradabad"
- M.Tech Thesis is Guided on the topic of " DWT-SVD Semi Blind Image Watermarking Using High Frequency Band" . Scholar from Banasthali Vidyapeeth , Jaipur,Rajasthan (INDIA).
- M.Tech Thesis is Guided on the topic of "Image Watermarking for Copy-Right Protection "Scholar from Sri Venketeshwar University Moradabad.

RESPONSIBILITIES AT INSTITUTE LEVEL

- Serves as a Head of Department(CSE).
- An active member of Institute's **Proctor Board** and **Anti Ragging Squad**.
- Convener of CS&IT Student Society.
- Convener of Institute's Annual Functions
- Time Table committee Incharge.
- Active Participation in Students training for different company's interview.

FACULTY DEVELOPMENT PROGRAM

- FDP(5 days) attended on the Topic "**Cyber Security & Cyber Forensics** " conducted by **MVSR Engineering College , Hyderabad**
- FDP(5 days) attended on the Topic "**Cyber Security** " conducted by **ATAL Academy AICTE New Delhi(SMVEC ,Puducherry)**
- FDP(5 days) attended on the Topic "**Cyber Security** " conducted by **ATAL Academy AICTE New Delhi(Osmania University Hyderabad)**
- FDP(5 days) attended on the Topic "**Cyber Security and Forensics**" conducted by **ATAL Academy AICTE New Delhi(Gautam Budh University Noida)**
- FDP(5 days) attended on the Topic "**Cyber Security**" conducted by **ATAL Academy AICTE New Delhi(Dr Hari Singh Gaur University).**
- FDP(5 days) attended on the Topic "**Cyber Security**" conducted by **ATAL Academy AICTE New Delhi.**
- FDP(One Week) attended on the Topic "**Emerging Trends ,Issues and Challenges in Next Generation Technology "** conducted by **Rama University ,Kanpur**
- FDP(One Week) attended on the Topic "**Application of Different Tools and Techniques for Academic ,Research Writing and Reporting**" conducted by **R.R Institute of Modern Technology Lucknow.**
- FDP(One Week) attended on the Topic "**R Programming**" conducted by **Indo Global Group of Colleges ,Chandigarh.**
- FDP(Two Weeks) attended on the Topic "**Managing Online classes and Co-creating MOOCS "** conducted by **Ramanujan College ,University of Delhi**
- FDP attended on the Topic "**Network Simulation and Data Security "** conducted by CCSIT , **Teerthankar Mahaveer University , Moradabad**.
- FDP attended on the Topic "**Introduction to Data Science using Python & R-Tool "** conducted by CCSIT , **Teerthankar Mahaveer University , Moradabad** in collaboration with iNurture Education Solutions Pvt Ltd Bengaluru .
- FDP attended on the Topic "**Pattern Recognition and Image Analysis "** at conducted by **IIT Roorkee.**

OTHER ACHEIVEMENTS

- Serves for **DOEACC Society** as a “**Examination Observer- 2021** ” for the conduction of online exams in Rampur City(UP).
- Serves for **DOEACC Society** as a “**Examination Superintendent-2016** ” for the conduction of online exams in Rampur City(UP).
- Serves for **Sam Higginbottomas University Allahabad** as a “**Examination Observer-2015**”for the conduction on theory exams in Rampur City(UP).
- Active Session Chair at IEEE Conference held at TMU Moradabad

COMPUTER SKILLS

Web VAPT:	Burpsuit Tool
Network VAPT:	Nessus Tool, Nexpose Tool
Simulation:	Packet Tracer,MATLAB
Language:	C,C++
Platforms:	Win 7 ,Win 8 ,Win 10
Database	ORACLE 10,MySQL
Hardware:	System Hardware & Maintenance
Linux Based:	Kali Linux
Network Sniffing:	Wireshark, Cain & Abel,NMAP
Web Technologies:	HTML,CSS

BASIC EDUCATION

- Intermediate- U.P. Board with 68%(1998)
- High School -U.P. Board with 64%(1996)

SKILLS

Interpersonal Skills

- Team Spirit.
- Flexible Nature.
- Positive Attitude.
- Target specific approach and conviction towards work.

Professional Skills

- Quick learner with problem solving skills and Punctuality.
- Effective communication and ability to sense students needs.

PERSONAL DETAILS

Father’s Name	:	Shri Shailendra Kumar Saxena
Date of Birth	:	10 Jan 1981
Marital Status	:	Married
Spouse Name	:	Arpita Srivastava
Nationality	:	Indian
Languages	:	English & Hindi

Praful Saxena

List of Publications in Journal(Scopus Indexed)

1. Saxena, P. ., & Kumar, S. . (2023). Robust Video Watermarking Algorithm based on DCT-SVD approach and Encryption . International Journal on Recent and Innovation Trends in Computing and Communication, 11(5), 85–91. https://doi.org/10.17762/ijritcc.v11i5.6581

2. Saxena, Praful & Kumar, Santosh(2023) Robust video watermarking algorithm based on motion frames and encryption, Journal of Discrete Mathematical Sciences and Cryptography, 26:5, 1327–1339, DOI: 10.47974/JDMSC-1748

List of Publications in Conference

1. P. Saxena and S. Kumar, "SCD based Video Watermarking by Using Wavelet Transform and SVD," 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), Sonepat, India, 2021, pp. 288-291, doi: 10.1109/CCICT53244.2021.00060.

Reprints of published papers related to thesis

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6581
***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 14 April 2023*

Robust Video Watermarking Algorithm based on DCT-SVD approach and Encryption

Praful Saxena[1], Santosh Kumar[2]
[1]Research Scholar , Computer Science & Engineering
Maharishi University of Information Technology
Lucknow, India
shyam.praful@gmail.com
[2]School of Computing & Engineering
Galgotias University
Greater Noida, India
Sant7783@hotmail.com

Abstract— Sharing of digital media content over the internet is increasing everyday .Digital watermarking is a technique used to protect the intellectual property rights of multimedia content owners. In this paper, we propose a robust video watermarking scheme that utilizes Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) for embedding a watermark into video frames. The proposed method uses encryption to make the watermark more robust against malicious attacks. The encryption key is used to modify the watermark before it is embedded in the video frames. The modified watermark is then embedded in the DCT and SVD coefficients of the video frames. The experimental results show that the proposed method provides better robustness against various attacks such as compression, noise addition, and filtering, while maintaining good perceptual quality of the watermarked video. The proposed method also shows better resistance against geometric attacks such as cropping, rotation, and scaling. Overall, the proposed method provides an effective solution for protecting the intellectual property rights of multimedia content owners in video distribution and transmission scenarios.

Keywords- Watermarking,Discrete Cosine Transform, Singular Valur Decomposition, Encryption.

I. INTRODUCTION

Due to extensive use of multimedia and the Internet, digital content, particularly digital photographs, digital videos has drawn a lot of attention. The Internet and media technologies make it exceedingly simple, inexpensive, and expedient to change, replace, regenerate, and distribute digital images. Data authentication safeguards the integrity of the multimedia component by ensuring its accuracy and consistency. One type of authentication method that has drawn scholars to this area of study is digital image watermarking. This approach creates the watermarked image by embedding a watermark (ownership information) into the host image. Later, the system takes the created watermarked image and extracts the watermark image from it. Digital watermarking is a process of embedding an imperceptible pattern of digital data within a multimedia file, such as an image, video, or audio clip. This pattern serves as a digital signature that can be used to authenticate the content's origin, track its usage, or protect it against unauthorized duplication. The watermark is typically added by altering the least significant bits of the file's pixels or samples, so that the visual or auditory quality of the content is not affected. The watermark may contain information such as the creator's name, copyright notice, or a unique identifier that can be used to link the content to a specific owner or distributor[1].

Digital watermarking has a wide range of applications, including content protection, copyright management, forensic analysis, and multimedia authentication. For example, watermarking can be used to prevent piracy by making it easier to detect and track illegal copies of a file. It can also be used to trace the source of leaked or stolen content, or to prove ownership in case of disputes[2]. However, digital watermarking also raises concerns about privacy, security, and fair use. Critics argue that watermarking can be used to invade users' privacy by tracking their consumption habits or to limit their rights to use or share the content. Therefore, the design and implementation of digital watermarking systems require careful consideration of ethical, legal, and technical issues[3]. A digital image watermarking system has four design features: imperceptibility, resilience, capacity, and security. Nevertheless, these needs cannot be met at the same time due to their limitations and incompatibilities. The application often determines how imperceptibility, robustness, and capacity are balanced. Also, it was found in the literature that spatial domain approaches are less reliable than transform domain methods. Spatial domain techniques directly use the pixel values in the image. So, by modifying these pixel values, the watermark can be integrated into the host image[4]. These spatial domain approaches are only appropriate for images with no noise. Cropping attacks can omit the watermark image, which is a significant disadvantage of spatial domain watermarking[5].

II. METHODOLOGY USED

In this research work the focused areas are Discrete Cosine Transform, Singular Value Decomposition , Motion frame selection and Encryption method for Watermark.

A. Discrete Cosine Transform

The Discrete Cosine Transform (DCT) is a mathematical tool that is commonly used in digital image and video processing, including in digital watermarking. DCT is a technique that converts a spatial signal into its frequency domain representation[6]. It does this by representing the image as a sum of sinusoidal functions of different frequencies and amplitudes, with each sinusoidal function representing a specific frequency component of the image. In watermarking, the DCT can be used to embed the watermark within the image or video by modifying the high-frequency components of the image or video[7]. High-frequency components are typically areas of an image where there is rapid change, such as edges or textures, and they are less sensitive to human perception than low-frequency components, which contain smoother variations in the image. The watermark can be added to the high-frequency coefficients of the DCT by modifying the values of the coefficients in a way that is imperceptible to human vision or hearing. The modification process is carefully designed to minimize the impact on the original image quality, and the changes are usually distributed across several DCT coefficients to make the watermark more robust against common image processing operations, such as cropping or compression. When the watermarked image is received, the DCT coefficients are extracted, and the watermark can be detected by applying a watermark extraction algorithm that looks for the specific pattern or signal that was embedded in the DCT coefficients[8]. Overall, the DCT plays an important role in watermarking by providing a way to embed the watermark into an image or video in a way that is robust, imperceptible, and reversible. Equation 1 shows the DCT coefficient for 8 X 8 blocks size of divided image .

$$F(u,v) = \frac{1}{4}C(u)C(v)\sum\nolimits_{i=0}^{7}\sum\nolimits_{j=0}^{7} f(i,j) \cos\left(\frac{(2i+1)u\pi}{16}\right)\cos\left(\frac{(2j+1)v\pi}{16}\right) \quad (1)$$

Where F(u,v) is the DCT coefficient of the image.

B. Singular Value Decomposition

The Singular Value Decomposition (SVD) is another mathematical tool that is commonly used in digital watermarking, especially in watermarking of audio signals. SVD is a matrix decomposition technique that decomposes a matrix into three matrices that represent its singular values, left singular vectors, and right singular vectors. In watermarking, SVD can be used to embed the watermark within the audio signal by modifying the singular values of the audio signal's SVD[9]. The singular values represent the amount of energy in the audio signal's frequency components, and modifying them can alter the audio signal's energy distribution in the frequency domain. The watermark can be added to the audio signal's SVD by modifying the singular values in a way that is imperceptible to human hearing.

The modification process is carefully designed to minimize the impact on the original audio quality, and the changes are usually distributed across several singular values to make the watermark more robust against common audio processing operations, such as filtering or compression. When the watermarked signal is received, the SVD is computed, and the watermark can be detected by applying a watermark extraction algorithm that looks for the specific pattern or signal that was embedded in the singular values[10].

Overall, SVD plays an important role in watermarking of digital signals by providing a way to embed the watermark into the audio signal in a way that is robust, imperceptible, and reversible. Suppose there is an image of size M×N that will be watermarked. The image can be presented in a nonzero matrix and made into Equation 2.

$$A = USV^T \quad (2)$$

Where A is denoting as a matrix of image ,S in singular matrix and U and V are the orthogonal matrix .

C. Motion Frame Selection

The host video object's related frames can be found and removed using the scene change detector's functionality. By exploiting a correlation between the video's frames, this is accomplished. Depending on the need for the results to be refined, the procedure can be used up to various degrees. There are many ways to filter similar frames from the video, including linear interpolation, binary search, and histogram. Using a histogram approach, scenes with comparable values are collected in one bin, and an attempt is made to determine the cut-off range for the greatest number of elements[11].

The idea behind this strategy is to measure the signal's distribution across the entire spectrum and use this information for analysis. In this instance, the statistical measure is the difference between the heights of the histograms for the same bins. At the initial stage, a filtering technique that eliminates identical frames is utilized to eliminate comparable frames.

***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 14 April 2023*

The histogram, binary search, and linear interpolation are all used as part of the filtering procedure to remove duplicate frames. The HiBisLI method is the name of this method. The approximate value is calculated using the binary search approach, which is based on sorting arrays. Any function with two values can be approximated using the linear interpolation approach. Either of these techniques can be used to remove comparable frames from the cover video, leaving just the frames that are different from one another.

Extracting motion frames from a video using histograms involves using the changes in pixel intensities between consecutive frames of the video to detect motion. Here are the general steps to extract motion frames using histograms: Use a video reader to read the frames of the video. Convert each frame to grayscale to reduce the computational complexity of the algorithm. Compute the histogram of each frame using a histogram function. The histogram should capture the distribution of pixel intensities in the grayscale image. Compute the difference between the histograms of consecutive frames to detect changes in pixel intensities. Threshold the difference in histograms to identify frames where the changes in pixel intensities are above a certain threshold. This threshold can be set based on the amount of motion required to be detected. Extract the frames where the difference in histograms is above the threshold as the motion frames.

III. LITERATURE REVIEW

The performance of the transform domain algorithms is superior to the spatial domain methods. Maintaining a trade-off between the design needs at the same time is crucial. The right domain to retain this trade-off by integrating two or more transform domain algorithms is the hybrid domain approaches. The DWT-based technique is effective in both the temporal and frequency domains, yet DWT occasionally produces subpar results. A hybrid method based on lifting wavelet transform (LWT), DCT, and SVD is developed to get over the conventional restrictions of the wavelet-based watermarking algorithm. The Canny edge detector is now utilized to choose the ideal place for putting the binary watermark. Multiple scaling factor (MSF) has been employed during watermark embedding to preserve the trade-off between imperceptibility and resilience, and particle swarm optimization (PSO) has been used to achieve optimum MSF. However, the technique is not resistant to hybrid, resynchronization, and print/scan attacks. The method doesn't take the watermark image's security into account. Moreover, it is not calculated how many watermarks can be included. DCT is a popular technique used in image and video compression, and it has also been used in video watermarking. DCT-based watermarking works by embedding the watermark in the DCT coefficients of the video frames. The watermark is embedded in the high-frequency coefficients of the DCT matrix because they are less visible to the human eye[12]. The watermark is also spread across multiple frames of the video to increase its robustness.

Several studies have explored the effectiveness of DCT-based video watermarking techniques. The proposed DCT-based video watermarking technique that uses a non-blind method to embed the watermark. The technique was found to be robust against common video processing attacks such as frame averaging, frame dropping, and frame flipping[13]. The authors proposed a DCT-based video watermarking technique that uses a singular value decomposition (SVD) pre-processing step to enhance the robustness of the watermark. The results showed that the technique was robust against a variety of attacks, including noise addition, compression, and geometric transformations[14].

Several studies have explored the effectiveness of SVD-based video watermarking techniques. The proposed an SVD-based video watermarking technique that uses a chaotic map to enhance the security of the watermark. The results showed that the technique was robust against a variety of attacks, including cropping, filtering, and compression[15]. The proposed an SVD-based video watermarking technique that uses a non-negative matrix factorization (NMF) pre-processing step to enhance the robustness of the watermark. The results showed that the technique was robust against a variety of attacks, including geometric transformations, filtering, and compression. In the case of content authentication, the high frequency components (HH) of IDWT are employed to embed the logo information as a delicate watermark onto the host image. Imperceptibility, robustness, and capacity are three competing and constrained objectives, and an optimization process called artificial bee colony (ABC) is utilized to achieve the best possible balance between them. Another method applies different DWT levels to the cover (or host) image before merging DCT and DWT. Here, a spread transform quadrature index modulation (QIM) technique is utilized to insert the watermark. It uses an orthogonal matching pursuit compression reconstruction approach to boost the watermarking system's efficiency[16]. The frequency domain and spatial domain are the two domains used in watermarking for the message insertion procedure. Since computation in the spatial domain is faster, simple data are frequently inserted there. The frequency domain is more assault resistant and takes longer to process than the spatial domain, which excels in speed but is not immune to attacks during picture processing[17] . One technique used in image processing for the compression of images is the discrete cosine transform (DCT). DCT's two primary advantages for compressing images and videos are as follows- Concentrate the energy of the image into a few coefficients (energy compaction). Reduce coefficient interdependence as much as possible

DOI: https://doi.org/10.17762/ijritcc.v11i5.6581
***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 14 April 2023*

IV. PROPOSED METHOD

The initial process is to extract the motion frames the host video . The extraction can be done by using the define process in the previous section . The proposed method is divided into three section watermark encryption , watermark embedding and watermark extraction.

A. Watermark Encryption

Initial step involves reading in the binary image as an array of pixel values. Each pixel can have a value of 0 or 1. The secret key is a binary string that will be used to determine the order in which pixels are swapped. Next step involves generating a random permutation of the pixel indices in the image. This permutation will be used to determine the order in which pixels are swapped. This step involves using the secret key to determine a starting position in the permutation. The starting position should be a value between 0 and the length of the permutation. Traverse the permutation from the starting position, swapping the pixels at each pair of indices with the same XOR value as the secret key. Repeat until the end of the permutation is reached. This step involves outputting the scrambled image as an array of pixel values. The scrambled image should be visually different from the original binary image, but still maintain the same overall structure. Fig. 1 shows the original watermark and Fig. 2 shows the encrypted watermarked after applying the encryption.

Figure 1. Original Watermark

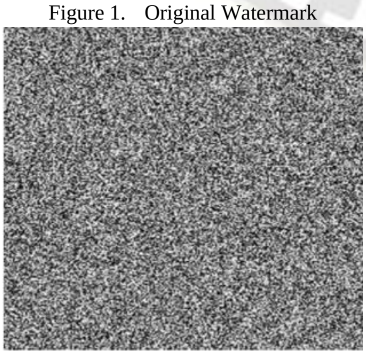

Figure 2. Encrypted Watermark

B. Watermark Embedding

- Extract the motion frames from the host video to identify the frames in which watermark is to be embedded .
- DCT is applied on the frame with the aim of splitting the frame into 8X8 pixel block.
- Apply SVD on the blocks placed prior to DCT to obtain the orthogonal and singular matrix of the frame .

$$I = U \times S \times V \qquad (3)$$

- Now apply the SVD method on the watermark image to be embedded . This will results orthogonal and singular matrix of the watermark .

$$W = U_W \times S_W \times V_W \qquad (4)$$

- Now to exchange the singular matrix S with the matrix S_W

$$I_{wat} = U \times S_W \times V^T \qquad (5)$$

- Apply Inverse SVD to I_{wat}
- Apply the Inverse DCT and this will result the watermarked frame.
- Repeat the process on selected frames so that the complete video will be watermarked .
- Fig. 3 shows the block diagram of this complete process.

C. Watermark Extraction

- Extract the motion frames from the watermarked host video .
- Apply DCT process on the watermarked frame . Divide the image into 8 x 8 block.
- Apply the SVD process on the watermarked frame to obtain the singular values S_{ew} of it.
- Apply the SVD process to get all three values U_w , S_w and V_w .

$$W = U_W \times S_W \times V_W \qquad (6)$$

- Apply SVD on the original watermark image to get the orthogonal and singular matrix .

$$I_w = U_{ew} \times S_{ew} \times V_{ew} \qquad (7)$$

- Apply Inverse SVD to the U_W , V_W from the original watermark and S_{ew} from the watermarked image which will result the final extracted watermark image.
- In a similar way the watermark can be extracted from other different motion frames .

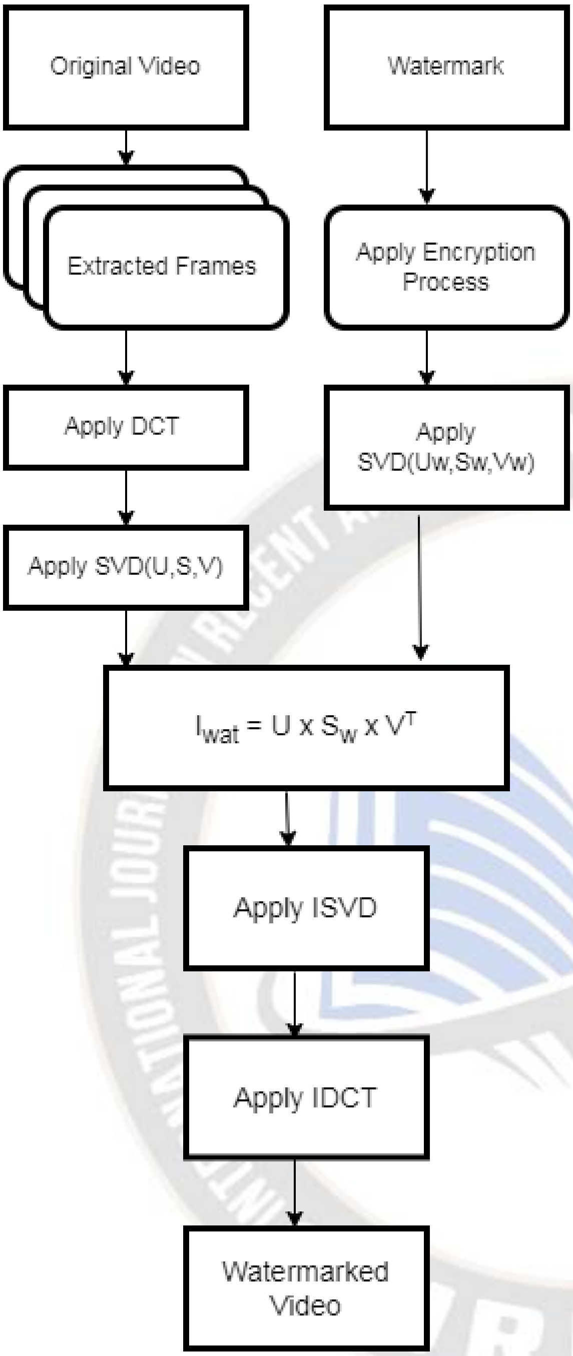

Figure 3. Watermark Embedding Process

V. RESULTS AND DISCUSSION

The proposed algorithm is implemented on two videos “foreman.avi” and “akiyo.avi” . This section contains the three parts the extraction of motion frames, Watermarked embedding process and the results discussion after performing various attacks on watermarked video.

A. *Motion Frames Extraction*

The method of extracting the motion frames from video is defined in the previous section . The proposed method is implemented using MATLAB and the sample video of “foreman.avi” is used . After the implementation there were total 300 frames out of which 114 are motion frames . In Fig. 4 some of the sample motion frames are shown .

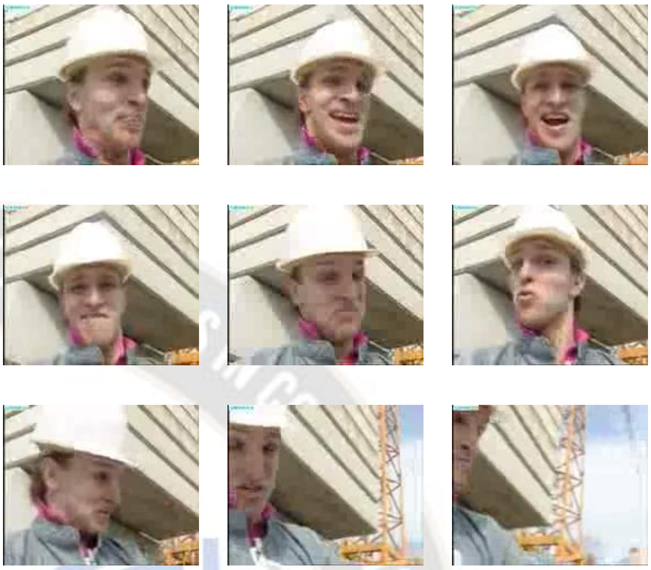

Figure 4. Extracted Motion Frames

B. *Watermark Embedding*

The method for embedding the watermark in the video is defined in the previous section . The proposed algorithm is implemented on two sample videos . Fig. 5 shows the original video and the Fig.6 shows video after embedding the watermark.

Figure 5. Original Video

Figure 6. Watermarked Video

C. *Robustness Analysis*

This section includes the robustness of proposed algorithm .The strategy to check the robustness of algorithm is to apply the various types of attacks on the watermarked video and then

***Article Received**: 14 February 2023 **Revised**: 28 March 2023 **Accepted**: 14 April 2023*

extract the watermark . The similarity between the extracted watermark and the original watermark shows how much the proposed algorithm is robust against the various attacks. To check the similarity two metrics are used commonly called Structural Similarity Index (SSIM) and Normalized Correlation(NC). SSIM is frequently used to measure the similarity between two images .NC parameter used for the robustness of Watermarking method. Several watermarking attacks, such as JPEG compression, noise addition, filtering, geometric assaults, and multiple types of common attacks are used to applied on the watermarked video as part of robustness studies. There are three different kinds of filtering attacks: mean, median, and Gaussian Low Pass Filter (LPF). Cropping, rotation, and flipping are the geometric attacks used. To calculate the robustness of the proposed algorithm some of the above stated attacks are selected . Table 1 and Table 2 shows the results of SSIM and NC against the performed attacks on the watermarked videos..

TABLE I. ROBUSTNESS ANALYSS(FOREMAN.AVI)

S.No	Attack Performed	SSIM	NC
1	Speckle Noise	0.9912	0.851
2	Frame Deletion (around 15%)	0.8891	0.878
3	Rotation(45 degree)	0.9001	0.993
4	Gaussian Low Pass Filter	0.9087	0.812
5	Cropping(left)	0.8879	0.898
6	Salt and Pepper	0.8874	0.882
7	JPEG Compression	0.8003	0.863

TABLE II. ROBUSTNESS ANALYSS(AKIYO.AVI)

S.No	Attack Performed	SSIM	NC
1	Speckle Noise	0.8702	0.902
2	Frame Deletion (around 10%)	0.9018	0.807
3	Rotation(60 degree)	0.8957	0.893
4	Gaussian Low Pass Filter	0.9007	0.957
5	Cropping(left)	0.8977	0.943
6	Salt and Pepper	0.9112	0.921
7	JPEG Compression	0.8801	0.872

VI. CONCLUSION

The paper proposes a robust video watermarking scheme that utilizes Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) for embedding a watermark into video frames. The proposed method uses encryption to make the watermark more robust against malicious attacks, and the experimental results show that the proposed method provides better robustness against various attacks such as compression, noise addition, and filtering, while maintaining good perceptual quality of the watermarked video. The maximum value of SSIM (Structural Similarity Index) is 0.99, which indicates that the watermarked video maintains a high level of structural similarity with the original video. The value of NC (Normalized Correlation) is 0.9500, which suggests that the watermark is well-correlated with the original watermark, indicating good embedding and extraction accuracy. Overall, the proposed method provides an effective solution for protecting the intellectual property rights of multimedia content owners in video distribution and transmission scenarios. However, it's important to note that the effectiveness of any watermarking scheme also depends on the specific application and the potential attacks it may face. In future the proposed method can be extended by using other methods such as DFT , Hybrid approach of DWT-DCT or FDCuT

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” *Signal Processing*, vol. 90, no. 3. 2010, doi: 10.1016/j.sigpro.2009.08.010.

[2] X. Chang, W. Wang, J. Zhao, and L. Zhang, “A survey of digital video watermarking,” in *Proceedings - 2011 7th International Conference on Natural Computation, ICNC 2011*, 2011, vol. 1, doi: 10.1109/ICNC.2011.6022111.

[3] S. K. Praful Saxena, “Hybrid Approach based Video Watermarking Technique by using Scene Detection,” *IJRTCSIT*, vol. 12, no. 1, p. 10, 2021.

[4] T. Sathies Kumar and C. Arun, “A review of robust video watermarking technique,” *Journal of Advanced Research in Dynamical and Control Systems*, vol. 2017, no. Special Issue 2. 2017.

[5] S. B. Rakesh Ahuja, “All Aspects of Digital Video Watermarking Under an Umbrella,” *Int. J. Image, Graph. Signal Process.*, vol. 7, no. 12, p. 54, 2015.

[6] F. Ernawan, D. Ariatmanto, and A. Firdaus, “An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients,” *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3067245.

[7] N. Deshpande, A. Rajurkar, and R. R. Mathalkar, “Robust Dual Watermarking Scheme for Video Derived from Strategy Fusion,” *Int. J. Image, Graph. Signal Process.*, vol. 6, no. 5, 2014, doi: 10.5815/ijigsp.2014.05.03.

[8] N. Chawla and V. Singh, “A novel video watermarking scheme based on DWT and PCA,” *Int. J. Eng. Adv. Technol.*, vol. 7, no. 5, 2018.

[9] L. Chen and J. Zhao, “Adaptive digital watermarking using RDWT and SVD,” 2015, doi: 10.1109/HAVE.2015.7359451.

[10] S. K. Praful Saxena, “Robust Video Watermarking scheme based on DWT and SVD approach using Multiple frequency bands,” *Parishodh*, vol. 8, no. 9, p. 74, 2019.

[11] L. Agilandeeswari and K. Ganesan, “A robust color video watermarking scheme based on hybrid embedding

techniques," *Multimed. Tools Appl.*, vol. 75, no. 14, 2016, doi: 10.1007/s11042-015-2789-9.

[12] A. K. Abdulrahman and S. Ozturk, "A novel hybrid DCT and DWT based robust watermarking algorithm for color images," *Multimed. Tools Appl.*, vol. 78, no. 12, 2019, doi: 10.1007/s11042-018-7085-z.

[13] Y. Yang, Y. Zhao, J. Zhang, J. Huang, and Y. Gao, "Recent Development of Theory and Application on Homomorphic Encryption," *Dianzi Yu Xinxi Xuebao/Journal Electron. Inf. Technol.*, vol. 43, no. 2, 2021, doi: 10.11999/JEIT191019.

[14] A. Kanhe and A. Gnanasekaran, "Security of electronic patient record using imperceptible DCT-SVD based audio watermarking technique," *Int. J. Electron. Telecommun.*, vol. 65, no. 1, 2019, doi: 10.24425/123560.

[15] A. A. Mohammed, B. A. Jebur, and K. M. Younus, "Hybrid DCT-SVD Based Digital Watermarking Scheme with Chaotic Encryption for Medical Images," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1152, no. 1, 2021, doi: 10.1088/1757-899x/1152/1/012025.

[16] A. Chopra, S. Gupta, and S. Dhall, "Analysis of frequency domain watermarking techniques in presence of geometric and simple attacks," *Multimed. Tools Appl.*, vol. 79, no. 1–2, 2020, doi: 10.1007/s11042-019-08087-x.

[17] S. S. Jamal, T. Shah, S. Farwa, and M. U. Khan, "A new technique of frequency domain watermarking based on a local ring," *Wirel. Networks*, vol. 25, no. 4, 2019, doi: 10.1007/s11276-017-1606-y.

Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 5, pp. 1327–1339
DOI : 10.47974/JDMSC-1748

Robust video watermarking algorithm based on motion frames and encryption

Praful Saxena *
Department of Computer Science and Engineering
Maharishi University of Information Technology
Lucknow
Uttar Pradesh
India

Santosh Kumar †
Department of Computing and Engineering
Galgotia University
Greater Noida
Uttar Pradesh
India

Abstract

Rapidly growing technologies over the internet are used to transfer digital media content at a high rate nowadays. The growth in these technologies results in the creation of identical copies of original multimedia data easily. The creation of these identical copies states the false claim of the ownership of digital media by any malicious user. The proposed method suggests protecting these types of the false claim by inserting a watermark into selected motion frames. Before embedding the watermark, it is scrambled by using an algorithm having a secret key. With help of this key, the scrambled watermark will be reconstructed whenever it is required. With the help of DWT method along with using SVD technique watermark is inserted into the selected frame from the original media. The results of the proposed algorithm show that the scheme is secure and robust against different types of attacks whether it is intentional and unintentional. The proposed scheme is found more secure for the protection of false claims of malicious users over digital media.

Subject Classification: *68U10 Computing methodologies for image processing.*

Keywords: *Ownership protection, Wavelet transform, Motion frames, SVD, Video watermarking.*

* *E-mail:* **shyam.praful@gmail.com (Corresponding Author)**
† *E-mail:* **sant.7783@hotmail.com**

1. Introduction

The higher growth in the internet bandwidth makes it easily possible to share multimedia data over various devices. This high order sharing reduces the possibility of security of digital media content. The advancement of technology related to multimedia content introduces lots of issues like ownership, authentication of content, copyright protection, and many more. Tempering with digital media is one of the major concerns related to the copyright protection of media. Proper solutions should be developed to protect the media from such unauthorized user access. The use of cryptography enables the protection of media content during transmission. The malicious user cannot access or modify the media content without knowing the encryption key. The scheme associated with the cryptographic approach encrypts the data at the authorized user end and at the end of the receiver the data will be decrypted which results in the original data. Therefore a secure and robust scheme needs to be developed to avoid illegal media reproduction and false claims of digital media content. The advent of watermarking schemes gives a feasible solution for such problems having some challenges still to be faced.

Digital Watermarking is a feasible scheme in which additional information is hidden into host media content having a relation between both of them. Digital watermarking can be applied to audio, video, and image. Watermark is used proof copyright protection by embedding the watermark into the real source video and after that extraction process is performed which results from the same watermark which was extracted. In the process of digital watermarking proper balanced tradeoff should be maintained among payload, robustness, and perceptibility. In the watermarking method, the extraction process can only be performed by an authorized user only in the case to prove copyright protection. The scheme used to embed the watermark should maintain robustness so that embedded information should not be destroyed by any malicious use [1]. In case to select the type of watermark we can consider any gray level image, name, logo any timestamp, etc. These types of watermark are frequently used in various watermark implementation techniques. In the present scenario of the market, various types of video content are available like advertisements, training videos, workshop videos, games, etc. The video objects are categorized as real source video and compressed video. During the implementation of the same, the balanced trade-off among watermarking features should be balanced. Any malicious user can try to modify the video content by performing some kind of attack. Attacks can be categorized as geometric attacks, cropping, resize, and rotation attacks[2]. Another category of attacks performed on the image is image enhancement like histogram equalization, histogram processing, noise removal, frame restoration, contrast enhancement, and many more. In the video, media attacks are intentional and unintentional specific attacks. Any malicious user can insert the video frame or some clip of video are cut down from the real source video content[3]. Such kind of attacks comes under the category of unintentional attack. The replacement of frames comes under intentional attacks. During the implementation of the watermarking scheme, the perceptibility should be maintained up to a minimum threshold value. Another consideration is to maintain the payload capacity which states that the amount of information to be embedded into the host file.

2. Methodology Used

2.1 *Discrete Wavelet Transform*

Discrete Wavelet transform is the kind of mathematical tool that is used to implement wavelet transform. It uses the discrete set of wavelet scales having some defined rules. the Wavelets are the mathematical tool that is used to change the coordinate system as per the need. The original signal is broken down into a series of wavelets by the wavelet transform, which differs from a continuous wavelet transform[4]. The construction of the wavelet can be done from a scaling function which describes the scaling properties of an object. The layer having more resolution states that it contains more information about the object like an image. The wavelet results in the natural multi-resolution image having all the important edges of the image. Its generation and calculation of DWT are well suited to the digital computer[5]. If an image is passed through the DWT function then it is a sum of the wavelets having different locations and scales. DWT represents the image into high pass and low pass coefficients. In this, the image is passed through the high and low filters. When the image is passed through the DWT then the analysis filter is used to separate the image into various frequency bands. The analysis filters separate the image into four sub-bands LL, LH, HL HH. It is also called the first level of decomposition and it also represent the finer scale coefficients. The various level of decomposition depends on the need of the application implementation. In most of the watermarking methods the decomposition is done up to 3 level. The multi resolution concept is a conceptual concept

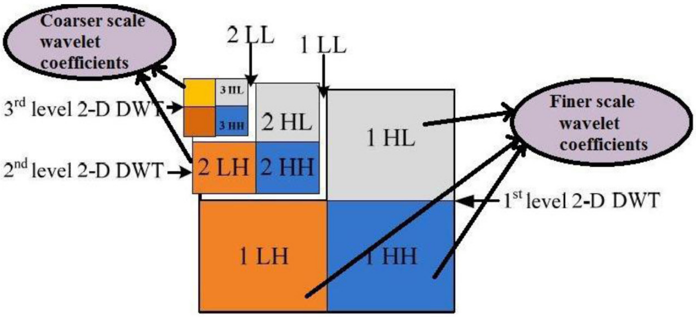

Figure 1

3Level DWT

that shows the signals that will be decomposed into fine details and finer approximations. The finer details subspaces are represented by a coarse and finer approximation. One of the major benefit for using the Discrete Wavelet Transform method is its excellent spatio-frequency localization property[6]. DWT is used by many watermarking algorithm for the copyright protection due to the imperceptibility property also[7].

2.2 *Singular Value Decomposition*

Singular value decomposition is a linear algebra mathematical tool which is used for the purpose of factorization of a real or complex matrix[8].SVD tool performs the decomposition of square matrix into ant m x n matrix with the extension polar decomposition. When SVD is applied on any m x n complex or real matrix M than it will be factorized into the form of UΣV* where U is defined as the real or complex unitary matrix of the order m x m. Σ is defined as the rectangular matrix having non negative numbers on the diagonal and its order is m x n. V is defined as the real or complex unitary matrix having order of n x n. The diagonal entries are called the singular values of matrix M[9].

3. Literature Review

The fast motion frame to embed the watermark into video object. Author converts the fast frame RGB to YCbCr color space and after that the frame gets transformed into 1-level decomposition of MR SVD. SVD is applied on each block approximation which provides robustness to the algorithm. The algorithm is tested against various attacks and the Watermark is extracted from the video object having a satisfied perceptibility[10]. The various applications of watermarking and its design features. Authors describes the implementation schemes which are categorized in spatial domain and frequency domain. A scheme to extract the watermark from the distorted video by using distortion model based on barrel. After applying the attacks the watermark calculated is by means of correlation and mean square error to find the accuracy of watermark signal[11]. The use of scrambled watermark for the implementation of watermarking over video object. Author uses un-encoded video to measure the security of the algorithm.Generalized Multi stage Arnold scheme is used to scramble the watermark. Scrambling the watermark improves the security feature of the algorithm. Author implements the watermarking process by selecting the U component from the YUV model. Proposed algorithm gives a good quality to the video object after embedding[12]. To avoid accidentally embedding the watermark in all the video frames, we only use the frames with big motion energy to embed it. This method works since the human visual system can't detect the details of fast moving regions. The algorithm is focused on the classification of blocks and shot segmentation. The watermark is computed as a small image that is proportional to the size of the host image. It is then embedded into the selected frames[13].

Discrete Wavelet Transform (DWT), Hessenberg Decomposition (HD), and Singular Value Decomposition (SVD) are the foundations of the watermarking method proposed in this research, which is enhanced by the Firefly Algorithm (FA). The suggested method makes the approach blind by using Hu's invariant moments, which are resistant to attacks that rotate, scale, and translate (RST) the image. The watermark is undetectable in the final watermarked image, making it appropriate for a broad range of watermarking applications. The suggested method involves applying a 2 Level DWT to a given colour image to separate it into the LL, LH, HL, and HH bands. These HH band coefficients are used as HD's input. To create the U, S, and V matrices, the output is placed through an SVD process. The Hu's unchanging values are scaled and transformed into binary strings using logarithm scaling. The binary matrix corresponding to the binary watermark is periodically XoRed with the same values to produce a new binary matrix with an identical dimension as the count of 2X2 partitions of S. Through altering the orthogonal V matrices, the watermark is embedded. The Firefly technique is used to calculate the change's size while taking robustness and imperceptibility into account as trade-off characteristics[14]. A robust image steganography method for sharing photos on social networks is presented in this paper and is based on graph signal processing. We first used quantum scrambling to obtain a scrambled version of the secret image for the embedding. The cover image and scrambled secret image were then both subjected to graph wavelet processing, which was followed by (alpha) merging on both image signals (cover image signal and scrambled image signal). The generated image was then subjected to an inverse graph wavelet modification to produce the stego image. This study used graph wavelet treatment to enhance interpixel correlation, which led to both the extracted secret image and the stego image having great visual quality[15]. The generated image is subjected to the GSP-based inverse wavelets to produce the stego image. As illustrated in the simulation results, the application of GSP in this case improves inter-pixel correlation, leading to superior visual quality stego and derived secret image[16].

4. Watermark Encryption and Frame Extraction

The logic behind the encryption of watermark is to provide the security to embedded video object. The encryption will be done during the embedding and decryption will be done during the extraction of watermark. Secret key is generated for this purpose.The benefit of encryption mechanism is that the cipher image is not logically readable by the any user. The watermark will be in a state of readable after decrypting it with the secret key. Appropriate algorithm[2] proposed by author is found a strong algorithm for encrypting the watermark.Initially we decide the key used for scrambling the watermark which will be as follows: K={1 6,1,14,3,12,5,10,7,8,9,6,11,4,13,2,15}. Key is a arrangement of even and odd numbers which will be used to scrambling the watermark. The size of the watermark will be same as of the video object. The watermark is portioned and the again rearranged as per the decided value K. This process results the encryption process of watermark. Figure 2 shows the original watermark and Figure 3 shows some parts of the scrambled watermark.

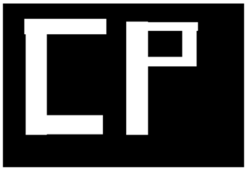

Figure 2

Original Watermark

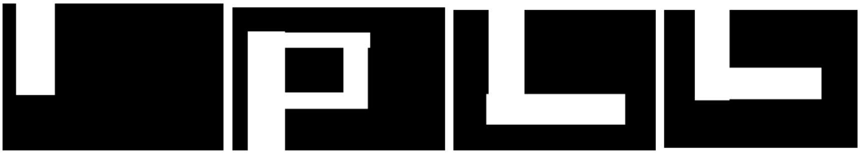

Figure 3

Scrambled Watermark

After the scrambling of watermark the next step is to extract the motion frames from real source video object. The motionless area of the video object is not robust and it is a comparatively easy task to exploit on the motionless frames based watermarking method. After execution of proposed process 14 frames are found which were based on the motion from the coastguard video object. The threshold value is set upto 5000 to extract the frames. The proposed scheme embed the scrambled watermark into the frame which results that few frames are get watermarked instead of all. It is also observed that quality of watermarked video also maintained.

Figure 4

Sample Extracted frames from Video

5. Proposed Watermarking Scheme

5.1 *Watermark Embedding*

The algorithm for inserting the scrambled watermark is implemented by embedding the encrypted part of watermark into motion frame.If the selected frame is not a motion frame than no embedding process will be

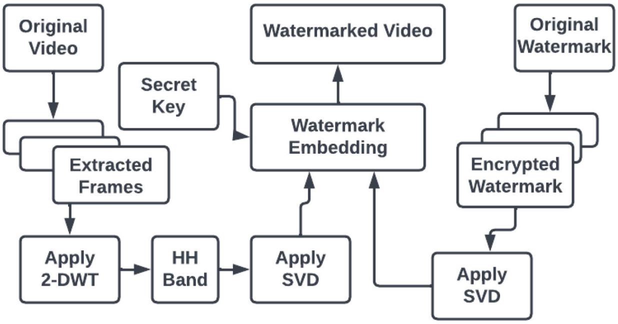

Figure 5

Watermark Embedding Flow Chart

executed. The embedding process done only on motion frames. If the count of extracted motion frames is more than the encrypted parts of watermark than repeat the sequence of encrypted watermark from one. Now transform motion frame into various luminance components. After the conversion, discrete wavelet transformation is executed up to 2-Level which results in four sub bands LL, LH, HL, HH. The HH band is used for the insertion of watermark. Apply the SVD method on this band which results the matrix of three components from which diagonal matrix is used insert the watermark. SVD method is also applied on watermark and diagonal matrix is used for watermarking purpose. The embedding of watermark is executed by following equation-

$$SVD_{WD} = SVD_{Y} + \alpha SVD_{W} \tag{1}$$

SVDY is the diagonal matrix of Y component after the apply SVD operation on it. SVDw represents the diagonal matrix of scrambled watermark.The value of α will be 0.01. After performing the watermarking operation the resultant diagonal matrix is SVDWD which is watermarked frame. After the insertion of watermark on all frames the watermarked video is generated which leads the final watermarked video. Figure 5 shows the flowchart of the proposed method for watermark embedding.

5.2 *Watermark Extraction*

The Extraction process is required when we need to extract the watermark which is inserted into motion frame. For this extract the adjacent RGB frame from the watermarked video and evaluate that if it is motion frame. If it is a motion frame than it must contain a watermark in it. Apply the process which results RGB frame into three different

Figure 6

Original Video

Figure 7

Watermarked Video

Figure 8

Original Video

Figure 9

Watermarked Video

components stated as Y, Cb and Cr. Now apply DWT of 2 level and select HH band. Apply SVD method to find the diagonal matrix which is singular values. The singular values of watermark is generated by given mathematical formula

$$S_{w'} = (S_o - S_w)/\alpha \tag{2}$$

Here Sw and So represents the singular values of the frame which is extracted from the real source video and watermarked video frame. Now repeat this process to obtain all the watermark and then the final watermark is generated. The estimated watermark can be generated as-

$$Watermark = UW * SW' *VW \tag{3}$$

UW and VW are the orthogonal matrix of watermark. These values are referred as the values of original watermark.The embedding algorithm is performed on two videos. Figure 6 and Figure 7 are the original video and watermarked video. Figure 8 and Figure 9 are the result of embedding process on another video.

6. Experimental Results

After the extraction of watermark , two major characteristics are to be checked one is robustness of algorithm and perceptibility.For the result processing various attacks are applied on watermarked video and then the extraction process is implemented. PSNR is tool used for the measurement of the perceptibility. The unit of PSNR is dB. The features of video are investigated in order to assess the suggested watermarking scheme's durability. Various attacks are executed on the watermarked video to destroy the watermark inserted in real video object. The proposed is found robust against defined attacks above. The evaluation is carried by analyzing the original watermark and driven out watermark by observing NC. The table shown below is the level of sturdiness of proposed algorithm. The proposed algorithm is applied on two videos foreman.avi and akiyo.avi. The applied attacks mentioned above measure the robustness of the algorithm.

Table 1

Proposed Algorithm Robustness Results (Foreman.avi)

S.No	Attack Performed	NC	PSNR
1.	Speckle Noise	0.881	40.2414
2.	Frame Deletion (around 10%)	0.908	38.1008
3.	Rotation	0.893	47.0024
4.	Gaussian Low Pass Filter	0.811	42.2003
5.	Cropping	0.898	37.8870
6.	Salt and Pepper	0.882	41.2404

Table 2

Proposed Algorithm Robustness Results (akiyo.avi)

S.No	Attack Performed	NC	PSNR
1.	Speckle Noise	0.902	39.0047
2.	Frame Deletion (around 15%)	0.911	38.0021
3.	Rotation	0.901	41.2414
4.	Gaussian Low Pass Filter	0.806	43.5724
5.	Cropping	0.885	40.0122
6.	Salt and Pepper	0.917	41.2141

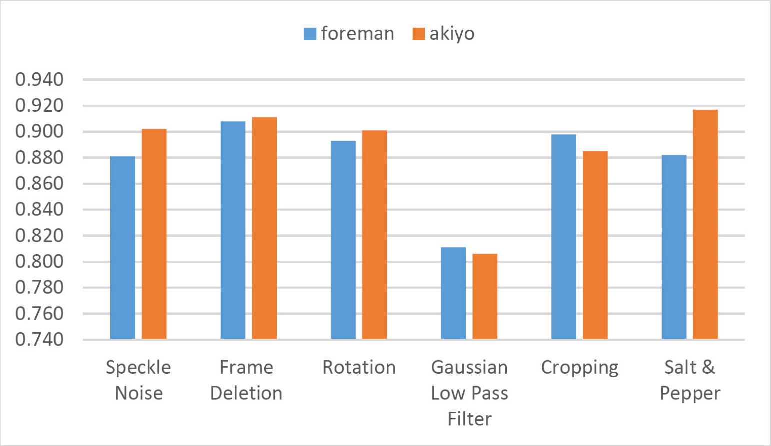

Figure 10

Result Comparison(NC Values) on foreman and akiyo video

The post extraction method shows that the extracted watermark has robust values of NC,PSNR with respect to several attacks.Table 1 and Table 2 shows the values of NC and PSNR and these values shows the robustness of the proposed method against several attacks. Figure 10 shows comparison on the two video oblects on which the proposed method id implemented.

7. Conclusion

The quality of the proposed scheme is that it manages to maintain the robust ness against attacks, video specific attacks. The security proposed in the algorithm is implemented at 2-layer security. The watermark is encrypted before the process of embedding and further it is segmented into sub images by extracting the motion frames from real source video object. Total number of frames in video object is 300 but only very few of the frames have gone through the process of embedding which improves the quality of video after embedding. After using the suggested algorithm, it was discovered that there was no similar visual gap between the watermarked and original source videos, indicating that the watermark's quality was sufficient in terms of imperceptibility. Because the real inserted watermark and real source video are provide whenever the extraction phase is executed, such resulting watermarking technique is ideal for applications which are private in nature. The greater robustness should be tested for composite assaults, collusion attacks, ambiguity attacks, algorithms should also be designed for video watermarking which are in blind category , according to future studies.In the blind video watermarking there is no requirement of real source video and original watermark for the extraction of embedded watermark.

References

[1] Q. Li and E. C. Chang, "Zero-knowledge watermark detection resistant to ambiguity attacks," in *Proceedings of the Multimedia and Security Workshop 2006, MM and Sec'06*, 2006, Vol. 2006, doi: 10.1145/1161366.1161395.

[2] R. Ahuja, Purnima, M. J. Haque, S. Tanwar, N. Gautam, and A. Rana, "Secure and Robust Watermarking Scheme based on Motion Features for Video Object," (2020), doi: 10.1109/ICRITO48877.2020.9197967.

[3] N. Chawla and V. Singh, "A novel video watermarking scheme based on DWT and PCA," *Int. J. Eng. Adv. Technol.*, Vol. 7, No. 5, (2018).

[4] L. Agilandeeswari and K. Ganesan, "A robust color video watermarking scheme based on hybrid embedding techniques," *Multimed. Tools Appl.*, Vol. 75, No. 14 (2016), doi: 10.1007/s11042-015-2789-9.

[5] Z. S. Veličković, Z. N. Milivojević, and M. Z. Veličković, "A secured digital video watermarking in chrominance channel," in *2018 23rd International Scientific-Professional Conference on Information Technology, IT 2018* (2018), vol. 2018-January, doi: 10.1109/SPIT.2018.8350858.

[6] A. A. Mohammed, D. A. Salih, A. M. Saeed, and M. Q. Kheder, "An imperceptible semi-blind image watermarking scheme in DWT-SVD domain using a zigzag embedding technique," *Multimed. Tools Appl.*, Vol. 79, No. 43-44 (2020), doi: 10.1007/s11042-020-09694-9.

[7] M. Shanmugam and A. Chokkalingam, "Performance analysis of 2 level DWT-SVD based non blind and blind video watermarking using range conversion method," *Microsyst. Technol.*, Vol. 24, No. 12 (2018), doi: 10.1007/s00542-018-3870-x.

[8] H. A. Abdallah, M. M. Hadhoud, and A. A. Shaalan, "SVD-based watermarking scheme in complex wavelet domain for color video," (2009) doi: 10.1109/ICCES.2009.5383220.

[9] G. G. & R. Kumar, "Analysis of image types, compression techniques and performance assessment metrics : A review," *J. Inf. Optim. Sci.*, Vol. 43, No. 3, p. 8 (2022).

[10] A. D. & M. N. Mohanty, "Transformation of 1-D data to 2-D image using stochastic mapping method for secured skin lesion detection," *J. Inf. Optim. Sci.*, Vol. 43, No. 8, p. 8 (2022).

[11] M. K. G. & S. R. D. Apoorva Katyayan, Ajay Khunteta, "Detection of copy-move image forgery using normalized cross correlation and fast fourier transform," *J. Stat. Manag. Syst.*, Vol. 22, No. 4, p. 10, (2019).

[12] K. Meenakshi, K. Swaraja, and P. Kora, "A robust DCT-SVD based video watermarking using zigzag scanning," in *Advances in Intelligent Systems and Computing*, Vol. 900 (2019), doi: 10.1007/978-981-13-3600-3_45.

[13] R. Naskar and R. S. Chakraborty, "Reversible Digital Watermarking: Theory and Practices," *Synth. Lect. Inf. Secur. Privacy, Trust*, Vol. 5, No. 1, (2014), doi: 10.2200/s00567ed1v01y201401spt010.

[14] M. M. Sachin Sharma, Shikha Choudhary, Vijay Kumar Sharma, Ankur Goyal, "Image Watermarking in Frequency Domain using Hu's Invariant Moments and Firefly Algorithm," *I.J. Image, Graph. Signal Process.*, Vol. 14, No. 2, pp. 1-15 (2022).

[15] V. K. Sharma, P. C. Sharma, H. Goud, and A. Singh, "Hilbert quantum image scrambling and graph signal processing-based image steganography," *Multimed. Tools Appl.*, Vol. 81, No. 13, (2022), doi: 10.1007/s11042-022-12426-w.

[16] V. K. Sharma, D. K. Srivastava, and P. Mathur, "Efficient image steganography using graph signal processing," *IET Image Process.*, Vol. 12, No. 6, (2018), doi: 10.1049/iet-ipr.2017.0965.

SCD based Video Watermarking by Using Wavelet Transform and SVD

Praful Saxena
Research Scholar
MUIT
Lucknow,India
shyam.praful@gmail.com

Dr Santosh Kumar
Associate Professor ,CSE
MUIT
Lucknow,India
sant7783@hotmail.com

***Abstract*—Embedding the Watermark in all frames of cover video is not a good practice in terms of complexity . This paper proposed the method in which the watermark will not be inserted into all frames of cover video. Due to the frequent illegal copying of digital media like image , video and audio. Watermarking method is playing an important approach for the purpose of copy right protection. This paper propose SCD method which enables to embed the watermark in selected frames of cover . Use of wavelet transform technique and singular value decomposition makes the approach robust against various attacks . The performance measurement of the algorithm shows the robustness against intentional and unintentional attacks.**

Keywords—SCD, DWT, Singular Value Decomposition ,Copyright protection ,Digital watermarking ,Multimedia security.

I. Introduction

The need of security is important for every data due to the frequently growth of internet and ease of data access due to it. As the multimedia data is easily accessible nowadays hence the ownership of data is always at risk due to illegal authorities over the internet. Digital watermarking is one of the solution of such illegal activities on digital media . With the help of digital watermarking the ownership of digital media can be proved . Digital watermarking is having a several applications like copyright protection, unique identification of the owner ,copy control ,editing of multimedia , broadcast monitoring , fraud and tamper detection and many more. Digital watermarking can be stated as imperceptible transmission of some additional data along with the existing multimedia data . This additional data is called Watermark in terms of watermarking .Watermarking is an approach to hide our data into multimedia content like image, video or audio. In digital watermarking we create a hidden channel during the transmission of multimedia data over the internet. The embedding of additional data into the cover object does not result in any visible distortions . The digital watermarking methods can be implemented as audio watermarking ,audio watermarking and video watermarking .In audio watermarking approach an unique identifier is used to embed into audio signal to proof the owner identification .One of the most reliable audio watermarking approach is Spread spectrum audio watermarking in which the transmission of narrow band signal is done over a much larger bandwidth so that the energy of the signal is undetectable in any signal frequency .Hence the watermark in audio watermarking is spread over many frequency band so that one can not detect the energy in any single band . In image watermarking approach the additional information is inserted into the cover image for the purpose of copyright protection and other proof of ownership. This additional information may the name of object owner , small image ,logo of organization or any text. In video watermarking method the additional data is embedded into video sequence so that video can be protected against the illegal copying or illegal ownership of video object . Video watermarking approach is an extension of the image watermarking approach but in video watermarking the challenges are higher than the image watermarking approach such that the large volume of data between the frames ,absence of balance between motion and motionless frames and the real time requirement during broadcasting of video . The video watermarking approach should be imperceptible and robust . Apart from robustness, reliability, imperceptibility, practicality, and video watermarking algorithms should also address issues such as localized detection, real time algorithm complexity, synchronization recovery, effects of floating-point representation, power dissipation etc. The implementation of video watermarking approach is done by two methods one is spatial domain video watermarking and frequency domain watermarking[1] . In spatial domain method the watermarking method is executed by directly modifying the pixel value of the host video. The modification of the Least Significant Bit is the most frequently used method for Watermarking .With the help this approach the small object can be inserted into the host object . The major drawback of this approach is that it can not resist against the attack which is et to pixel to pixel basis .The LSB technique was improved by using the pseudo random number generator to identify the pixel to be used to embed the watermark .The another approach of video watermarking is frequency domain in which the additional data is to be inserted into the host object by using various frequency domains. Majorly the three main methods used for data transmission are Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT).In this approach initially the host object is converted into frequency domain by using any transformation technique .After applying the embedding process into the host object , the inverse transformation is applied which results the watermarked video . In video watermarking there are two category of video used one is compressed video and another is uncompressed video[2]. If the video object is available in uncompressed format than the watermarking is implemented by using spatial and frequency

978-1-6654-2392-2/21/$31.00 ©2021 IEEE
DOI 10.1109/CICT53244.2021.00060

domain approach but the balance tradeoff watermarking features must be maintained . There are several types of attacks which are performed on the watermarked video . Image processing attacks includes geometric attack ,cropping and rotation attacks , image enhancement attacks[3] . The approach used for the implementation of video watermarking must robust against these attacks . After applying these attacks on the watermarked video the watermark should be extracted which can proof the robustness of the watermarking approach .Quality of video is also ensured during watermarking.

II. Methodology used

A. *Discrete Wavelet Transform(DWT)*

Discrete Wavelet transform is the implementation of wavelet transform which uses the discrete set of wavelet scales having some defined rules . the Wavelets are the mathematical tool which is used to change the coordinate system as per the need . Wavelet transform decomposes the original signal into set of the wavelets which is having the difference from continuous wavelet transform .The construction of the wavelet can be done from a scaling function which describes the scaling properties of an object . Wavelet has an unconditional basis as a result the size of the wavelet coefficients drop off rapidly. The wavelet expansion coefficients represent a local component thereby making it easier to interpret. Wavelets are adjustable and hence can be designed to suit the individual applications. Wavelet are the tools which can be used to decompose signals like image into hierarchy of increasing resolution on the applied object .The layer having more resolution states that it contains the more information about the object like image .The wavelet results into the natural multi resolution of image having all the important edges of the image . Its generation and calculation of DWT is well suited to the digital computer [4,5].If an image is passed through the DWT function than it as a sum of the wavelets having different location and scale. DWT basically represent the image into high pass and low pass coefficients . In this the image is passed through the high and low filters [9] . When the image is passed through the DWT than the analysis filter is used to separate the image into various frequency bands . The analysis filters separate the image into four sub bands LL,LH,HL HH. It is also called the first level of decomposition and it also represent the finer scale coefficients .This decomposition DWT can be done up to various level .2D-DWT shows that ,DWT is applied further on first level DWT and this will be applied on LL band of first level decomposition[8,9] . The various level of decomposition depends on the need of the application implementation . In most of the watermarking methods the decomposition is done up to 3 level. In wavelet transformation the multi resolution concept is designed which represents the signals, where a single event will be decomposed into finer and finer details. A signal is represented by a coarse approximation and finer details. The coarse and the detail subspaces are orthogonal to each other by applying successive approximation recursively the space of the input signal can be spanned by spaces of successive details at all resolutions .One of the major benefit for using the Discrete Wavelet Transform method is its excellent spatio-frequency localization property . DWT is used by many watermarking algorithm for the copyright protection due to the imperceptibility property also .

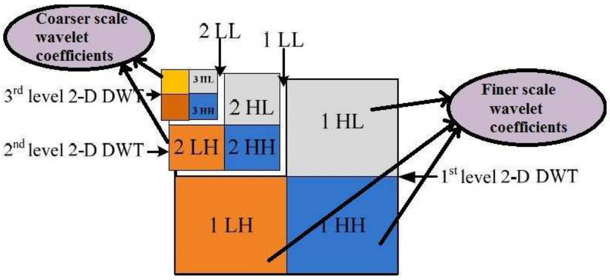

Fig . 1. Wavelet Transformation(3 Level DWT)

B. *Singular Value Decomposition(SVD)*

Singular value decomposition is a linear algebra mathematical tool which is used for the purpose of factorization of a real or complex matrix [6].SVD tool performs the decomposition of square matrix into ant m x n matrix with the extension polar decomposition . When SVD is applied on any m x n complex or real matrix M than it will be factorized into the form of UΣV* where U is defined as the real or complex unitary matrix of the order m x m. Σ is defined as the rectangular matrix having non negative numbers on the diagonal and its order is m x n. V is defined as the real or complex unitary matrix having order of n x n [7]. The diagonal entries are called the singular values of matrix M. The rank of the matrix M is equal to the non singular values . The columns of the matrix U and V are called left singular vectors and right singular vectors of matrix M respectively. SVD is having some major property for which it is considered a good for watermarking . One is the energy content of the image is located in the singular values after applying SVD . Another is the stability of the singular values which states that it does not change easily

C. *Scene Change Detection (SCD)*

The functionality of the scene change detector is to detect and remove the similar frames from a host video object. This is achieved by using a correlation between the frames of the video. The method can be applied up to various levels as per the requirement for the refinement of the results . Filtering a similar frames from the video there are various methods such as linear interpolation , binary search and histogram. Histogram approach gathers the scenes having a similar values in the same bin and then tries to find the cut-off range for the maximum number of elements . The concept in this approach is to determine the spread of the signal over the whole spectrum and to use this spread data for the analysis to find the similar frames . In this case, the difference of distance between histogram heights of the same bins is used as a statistical measure. To remove similar frames, a filtering method is used in the initial stage that filters out the same frames. To filter out the same frame, the filtering method consists of the histogram, binary search, and linear interpolation. This approach is known as HiBisLI method. Binary search approach calculates the approximate value and it is based on sorting of arrays [9].The Linear Interpolation method is used to approximate the value for any given function having two values . By using any of these methods the similar frames in the cover video can be removed and the existing frames are the frames which are not similar to each other . Distinct frames are used for the execution for video watermarking method. Embedding and extraction of watermark from these frames reduces the complexity in terms of time . These are more robust and secure against various attacks . Most of the similar frames of the video are not a part of video watermarking embedding process. It is also found that detection of similar frames by using approach of Histogram method results the more to accurate number of frames[10,11] . Binary search and linear interpolation results are also found satisfactory for the detection of similar frame in a given video .

III. PROPOSED ALGORITHM

For the implementation of proposed algorithm we need an image as watermark and the cover video. The size of the watermark image is 256 x 256 . The proposed algorithm consist of two parts watermark embedding process and watermark extraction process.

A. Watermark Embedding

Watermark embedding is done by using following steps-
(i) Convert the color watermark image into gray scale image.
(ii) Resize the watermark image into the size of 32 x 32.
(iii) After converting the cover video into frames use scene change detector algorithm to find out the frames those who are changed not similar to previous frames.
(iv) Convert the frames into RGB scale.
(v) .Now Decompose the scene changed frames by DWT tool which will give four sub bands LL,LH,HL and HH. All of the energy is contained in LL band.
(vi) Apply Level-3 DWT on LL band which will again give the four subband.
(vii) Now Apply the SVD method on Level-3 LL band and on Watermark image.
(viii) The watermark embedding is done by using following equation –

$$\boldsymbol{SVD_{WE}= SVD_V + SVD_W*\alpha}$$

Where the α=0.05, SVD_V is the value of Cover video frame and SVD_W is the value of Watermark to be inserted .
(ix) Now Apply the inverse SVD tool on the frame .
(x) Apply the inverse DWT operation of 2 Level , this will result the final Watermarked frame of cover video.

B. Watermark Extraction

Watermark extraction is the exact reverse process of Watermark Embedding. This process is used to proof the identity or copy right protection of multimedia content. For the extraction purpose we need watermarked video, cover video and the watermark to find out our embedded watermark. This extracted watermark will help to proof the identity of the owner of the multimedia content. The proposed algorithm for Watermark Extraction is as follows-

(i). Convert the embedded video into the frames.
(ii). Apply scene-change detector algorithm using a successive estimation of statistical measure.
(iii). With help of RGB-to-Gray converter, convert the frame into gray scale.
(iv). Resize the extracted frames into the size of 256x256.
(v) Apply the DWT tool on the scene changed frames which into four sub bands LL,LH,HL and HH.
(vi). Again apply DWT tool on LL band which denotes the 3-Level DWT.
(vii). Now apply SVD tool on 3-Level LL band.
(viii). For the extraction of watermark from the above step apply the equation-

$$\boldsymbol{SVD_W=(SVD_{WE}-SVD_V)/\alpha}$$

Where the α=0.05, SVD_V is the value of Cover video frame and SVD_W is the value of Watermark to be inserted and SVD_{WE} is the value of Embedded video.

IV. RESULTS AND EXPERIMENTS

The proposed algorithm is implemented in MATLAB . For the experiment purpose mp4 format video is considered and the watermark image in JPG or TIF format is considered . The size of the watermark image is 256x256.

A. Embedding Process

The process of Watermark embedding initialize with the cover video object foreman.avi which is gone through the process of SCD. The cover video "foreman.avi" is used for the embedding process.

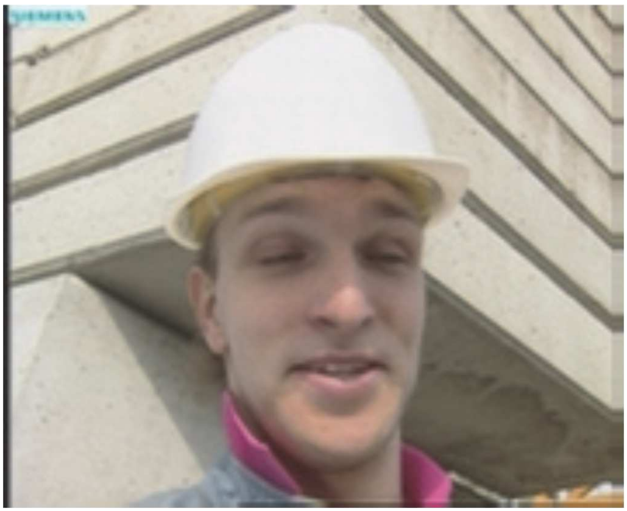

Fig.2. Cover Video

After applying SCD technique the non-similar frames are extracted

Fig.3. Sample After SCD execution of foreman.avi

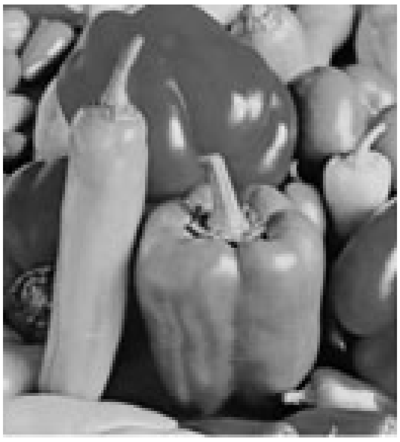

Fig.4. Original Watermark

After the completion of embedding process the cover object consist of the watermark

Fig.5 Watermarked Video

B. Performance Measure

The proposed algorithm is implemented in MATLAB . For the experiment purpose mp4 format video is considered and the watermark image in JPG or TIF format is considered . The size of the watermark image is 256x256. SCD is applied on the cover object and the results are shown in a table

TABLE I. SCD Result

Video Type	**Method Used**	**No. of Scene Detected**	**Changed Scene Detected**
Rushman.avi	Correlation	371	74

a) Performace afetr attack: For the measurement of proposed algorithm several attacks is performed on Watermarked video . The attacks can be categorized as Image processing attacks , JPEG compression attack and geometrical attacks. The performance measure of the algorithm is explored in the table.The performance is measured on the value of calculated NC values after the extraction of Watermark from the Watermarked video

TABLE II. Performance Measure after attack

S.No	**Attack Category**	**Attack**	**NC**
1	Image Processing Attack	Motion Blur	0.80021
2		Normal Blur	0.80012
3		Salt & Pepper	0.9011
4		Gaussian Noise	0.6032
5		Burring	0.9002
6		Sharpening	0.9411
7	JPEG Compression	JPEG Compression	0.9501
8	Geometrical Attack	Stretching	0.9311
9		Rotation	0.9401
10		Resizing	0.9511

V. CONCLUSION

A robust video watermarking technique is proposed which is based on 2D-disrete wavelet transform using level-3 decomposition is presented using Daubechies wavelets and Singular Value Decomposition (SVD) . Low frequency coefficients of wavelet (LL subband) are used for embedding the Watermark into cover video . This technique embeds an invisible watermark into the scene-changed video frame. The table shows the NC values of extracted watermark from the Watermarked video after applying various attacks. It is observed that NC values of the extracted watermark is at high range which shows that the proposed algorithm is robust against various attacks.

REFERENCES

[1] Ahuja Rakesh , S. S. Bedi, " Compressed Domain Based Review on Digital Video Watermarking Techniques", Information Technologyof Elixir International Journal, 2016 101, pp. 43622-43633.

[2] Ahuja , R and Bedi, SS " All aspects of digital video watermarking Under an Umbrella" , International journal of Image Graphics and Signal Processing ,2015 ,7(12), p.54.

[3] Manoj Kumar, Dolley Shukla "Review of Video Watermarking Techniques",International Journal for Innovative Research in Science and Technology, Vol 1, Issue 8, January 2015.

[4] Anand A, Singh AK "An Improved DWT-SVD domain watermarking for medical information security" .Comput Communication,2020, 152 :72 -80.

[5] Borra S, Swamy G "Sensitive digital image watermarking for copyright protection" , International Journal of Network Security 2013 15(2): 113-121

[6] D. K. Shaveta, "Attack resistant robust video watermarking using scaled wavelet transform with SVD-DCT techniques", Int. J. Modern Comput. Sci. **3** 2015.

[7] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEE Transactions on Multimedia, vol. 4, no. 1, pp. 121–128, 2002.

[8] D. K. Shaveta, "Attack resistant robust video watermarking using scaled wavelet transform with SVD-DCT techniques", Int. J. Modern Comput. Sci. 3 2015.

[9] A. Zear, A. K. Singh and P. Kumar, "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine", Multimed. Tools Appl. 2016 , 1–20.

[10] Gaobo, Y., Xingming, S. and Xiaojing, W., 2006, November. A genetic algorithm based video watermarking in the DWT domain. In 2006 International Conference on Computational Intelligence and Security (Vol. 2, pp. 1209-1212). IEEE.

[11] Leelavathy, N., Prasad, E.V. and Kumar, S.S., 2012. A scene based video watermarking in discrete multiwavelet domain. International journal of multidisciplinary sciences and engineering, 3(7).