Review Article

International Journal of Advanced Technology and Engineering Exploration, Vol 10(104)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2022.10100440

Video data security: analysis, relevance and open challenges

Purnima[1*], Rakesh Ahuja[1] and Nidhi Gautam[2]
Chitakara University Institute of Engineering and Technology, Chitkara University, Punjab, India[1]
University Institute of Applied Management Sciences, Panjab University, Chandigarh, India[2]

Received: 18-November-2022; Revised: 15-July-2023; Accepted: 16-July-2023

Abstract
With the rapid advancement of technology, ensuring authentication and security in communication over long distances has become a primary concern. The film industry is particularly vulnerable to the unauthorized distribution of digital videos, which can be easily disseminated to a global audience due to widespread internet access. Video watermarking has gained significant importance in various applications such as copyright protection, security, fingerprinting, copy control, and annotation. Watermarking, whether in the form of an image, audio, or video, is a technique used to embed additional information within a digital video signal. This embedded information is utilized for copyright owner detection. Consequently, several methods for digital video watermarking (DVW) have been developed to address this issue. Watermarking has emerged as a crucial means of verifying ownership, ensuring authenticity, and safeguarding copyrights. Researchers employ watermarking techniques to hide confidential information, which can be made either visible or obscured based on the user's requirements. This approach plays a vital role in determining the ownership of information. To ensure secure watermarking, an optimization process is often employed. This paper presents an overview of the diverse trends and techniques adopted in the field of digital watermarking. It aims to provide a comprehensive guide to research scholars interested in exploring this area of study.

Keywords
Digital video watermarking, Discrete wavelet transform, Discrete cosine transform, Robustness, Security.

1.Introduction
With the start of digitalization, huge amount of information is being transmitted over the internet every day, thereby increasing the need to secure it. Thus, in order to secure the transmission, the concept of information security has been introduced, which is a set of policies for managing the tools, processes to keep the information and its associated systems safe from the unauthentic use, leak of confidential information or alteration in the existing data. It works in two major parts i.e., system security which focuses on the legitimacy of the accurate action to be performed irrespective of the data stored as well as executed by the computer system while system assurance focuses on providing security to the information[1–3]. 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 required by an authorized individual. The essential characteristics of standard information security are the availability, integrity, authenticity and confidentiality.

*Author for correspondence

Currently, there are number of different techniques are used to secure the information. These techniques partitioned into three major categories: cryptography, steganography and digital watermarking. Each technique is designed for specific issue.

Cryptography [4] is the most common method of protecting digital contents. In this technique, the original message is converted into unintelligent form or encrypted form at the source end by using one of the different kinds of keys available. The converted message is called as cipher text transmitted to the destination. At the receiver end, the scrambled message is decrypted to get the original text by using the same or different but related key. It allows two ways of cryptography: symmetric uses the same key for encryption and decryption but asymmetric cryptosystem uses one key (public key) for encryption and another related key for decryption (private key). A digital signature scheme is a special type of asymmetric cryptographic primitive whereas electronic code book mode, cipher feedback mode, feedback chaining cipher mode and counter cipher mode of operation are symmetric cryptographic

primitives [5]. Each can be used in wide variety of applications. Another way to secure the confidential information is to hide in any non-hazardous file [6].

Steganography [7] is a combination of art and science to hide secret messages in such a way that no one, other than sender and intended receiver suspects the existence of the message. Instead of encrypting the message, it hides the clandestine message in other innocuous objects so that their very presence is not revealed. The advantage of steganography over cryptography is that the message does not attract attention to itself. Thus, steganography can be a feasible alternative in those countries where usage of encryption is illegal. However, the limitation with this technique is that the host object must be an imitation product to conceal the secret information therefore the method of steganography can never be used to protect the copyright of the supplied multimedia objects.

With the advent of technology, the security of the audio-visual aid data becomes progressively more significant. It is due to digital behaviour, that multimedia information can be repeated, changed, converted, and diffused easily. The fast data distribution over the system through images, audio, and video become the main source so as the transfer the data to others in one click. It is because of the portable nature that video and duplicity are increasing today. Even the real creator of the file may not concern about the data available on the internet formed by him/her or the creator can be unable to access his data. Thus, the current digital watermarking has been developed to resolve this issue. Watermarking is the procedure of hiding information that is known as watermarking, and mark (label) into real data. Thus, video watermarking embeds information in the video for documentation, annotation, and copyright [8]. It is a method of embedding hidden data in multimedia scheme data such as audio, textual data for identity, copyright, image and video [9].

In the era of digital media, the security of multimedia data has become a prime concern. With the rapid growth of internet-based video sharing platforms, it is essential to ensure the protection of intellectual property rights of video owners. Video watermarking has emerged as an effective solution to address the issue of copyright protection and content authentication. Video watermarking is a process of embedding an imperceptible pattern or information into a video signal, which can be used for various applications such as copyright protection, content authentication, ownership verification, tamper detection (TD), and video indexing. However, developing a robust and efficient video watermarking technique is a challenging task due to various factors such as video compression, video format conversion, geometric transformations, and various types of attacks. The motivation behind this systematic review is to provide a comprehensive analysis of the recent advances in video watermarking techniques. This review aims to identify the existing challenges, research gaps, and future research directions in this field. The objective of this review is to present a detailed analysis of the state-of-the-art video watermarking techniques, including their strengths, limitations, and applications. To achieve the objectives of this systematic review, we formulate the following research questions:

1. What are the recent advances in video watermarking techniques?
2. What are the challenges in developing an efficient and robust video watermarking technique?
3. What are the applications of video watermarking in various fields?
4. What are the future research directions in video watermarking?

To ensure the validity and reliability of the findings, a rigorous approach is used during the systematic review process. The process flow and the author's analysis are explained by the steps shown in *Figure 1*.

The past few decades, owing to the increased popularity of multimedia applications along with World Wide Web, have envisaged tremendous increase in the usage of multimedia content, especially, videos. Several innovative techniques are used both by professionals and common population to create digital videos [10]. Apart from this, there is a growing population who use videos to hide or embed details such as owner information, date, time, camera settings, event/occasion of the video, video title, secret information for value added functionalities and secret communication. Watermarks can also be used to ensure the authenticity of a digital video. There have been many watermarking schemes proposed [11, 12] each aiming to develop robust algorithms that protect digital contents and ownership. However, the continuing revolution in the communication medium is demanding and thus, it has become imperative to improve watermarking techniques that can satisfy the property of confidentiality, availability and reliability

(CAR) along with maximum transparency, capacity and robustness. Search for techniques to answer the above properties is the focus of the present research work. The main motivation is to find a technique that can simultaneously protect, preserve security without destroying or degrading the content of the video. However, existing algorithms face issues like the following:
(i) Introduction of perceptual distortions
(ii) High time complexity
(iii) Low immunity to attacks.

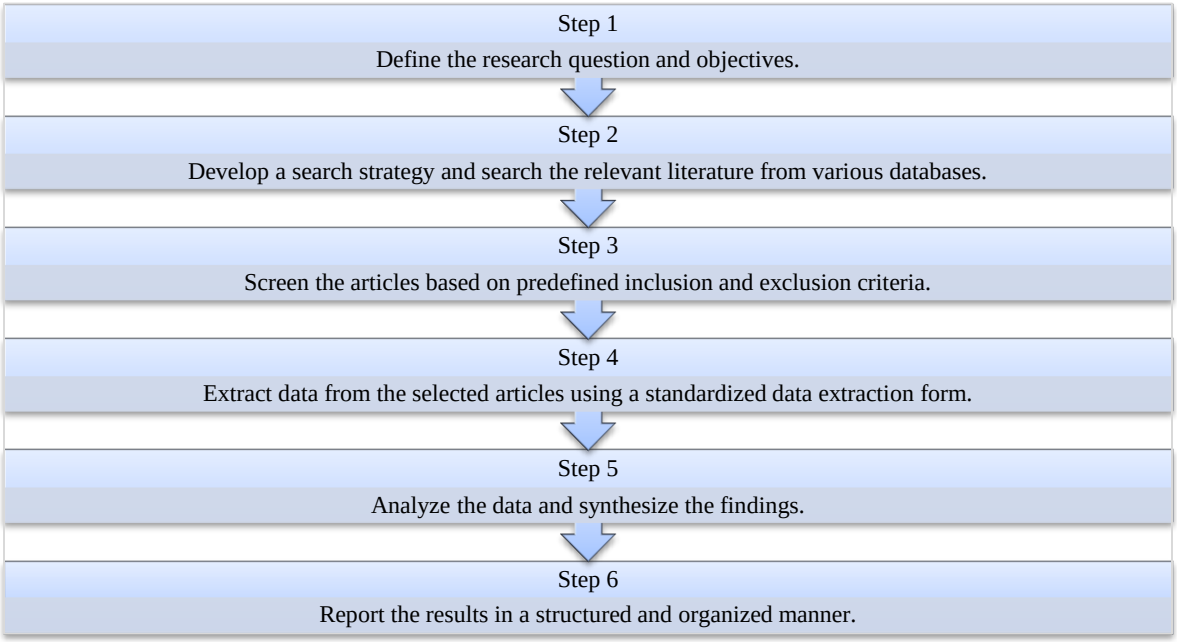

Figure 1 Steps to show the process flow

Thus, advanced schemes that can solve the above problems are to be designed to achieve more comprehensive and sustained, privacy control and TD. Further, presently the speed of the embedding and extraction procedures is high and depends on each watermark. Many algorithms for developing watermarks on images are extended for videos [13]. But some points need to be considered during the extensions

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

The contribution of this systematic review in the field of video watermarking is given as follows:

1. A comprehensive survey of recent advances in video watermarking techniques.
2. A critical analysis of the existing challenges and limitations in video watermarking.
3. A discussion of the potential applications of video watermarking in various domains.
4. Identification of research gaps and future research directions in video watermarking.

This systematic review aims to provide a comprehensive analysis of video watermarking techniques, challenges, and future research directions. The findings of this review will be useful for researchers, practitioners, and policymakers working in the field of digital media security.

2.Background

2.1Video watermarking model

Video watermarking is a technique to embed and retrieve data into and from the digital video data. This approach is a solution to the issue of safeguarding rights ownership [14, 15]. However, the growing popularity of video-based applications like a private video recorder, and internet media, has increased the need for safe communication of videos.

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the times new roman or the symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.

Some features of digital video watermarking (DVM) are described below [16]:

- High correlation between consecutive video frames. If autonomous watermarks are embedded in every frame, then risk may accomplish video frame averaging to eliminate the essential parts of the embedded watermarking.
- The real time operations and minimum complexity are required by copyright protection and broadcast monitoring.
- Watermark video sequences are more vulnerable to video threats like averaging and interchanging of video frames, numerical study, digital and analog conversion and loss compression.

Most of the digital image watermarking algorithms has been extended for video watermarking. Some of the key points which should be kept in mind while using such algorithms are given as-

- Initially, the video is converted into frames. Most of these frames have redundant data.
- As the video frames have both motionless and motion regions, there is requirement to create equilibrium between such regions.
- Real time streaming of video objects and applications related to the area should be kept in mind while implementation.

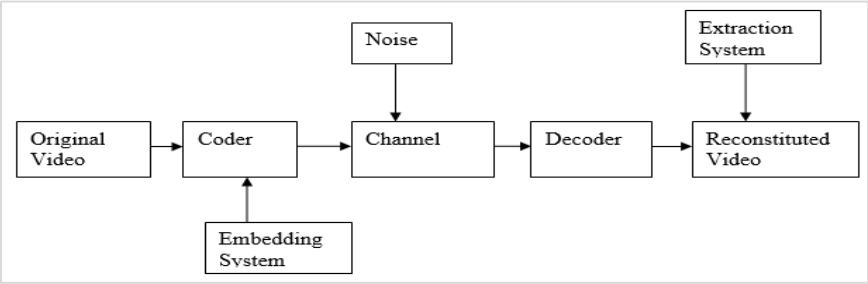

Figure 2 Steps to implement Video Watermarking

The process of DVW consists of two major steps which are named as embedding system and extraction system as shown in the *Figure 2*.The methods related to image and video watermarking are dissimilar, and the implementation of video watermarking involves more issues. For instance, the chances of video objects to possess similar frames are very high due to which the signals are highly exposed to video-specific attacks which includes all the frame related operations [17]. Thus, it is a method to embed and retrieve data into and from the digital video data. As per the various insertion methods of watermarking, the algorithms of implementing the said technique can be categorized into three different types which are described in the following sub-sections as shown in *Figure 3*. The DVW algorithms using the given techniques possess several benefits as well as drawbacks [18].

1) Non-compressed domain video watermarking

In these algorithms, the binary text/image is inserted in the actual video object [19]. The said technique also possesses some flaws like elevated bit rate (BR) of the video object while streaming the same. They have various pros like-

- The execution of the algorithm is comparatively easy.
- Numerous image watermarking methods can be used in the implementation of the algorithm.
- No explicit video compression standards are required.

With the advantages, this scheme also possesses several disadvantages which are given as-

- The watermark extraction process is quite complex as absolute decoding need to be done.
- With the help of compression standard, the watermark can be easily extracted.
- The video after implementing compression is to be decoded and then encoded as the insertion completes.

2) Encoding phase watermarking of video object

In this phase, the watermark is embedded in the object, and after the implementation both the

components acquire alike properties. The various video compression standards for high definition (HD) videos are moving picture experts group-2(MPEG-2), moving picture experts group-4 (MPEG-4), and H.264 [20, 21]. The various benefits of this scheme are-

- The embedding process in estimated coefficients is efficient and uncomplicated.
- In such algorithms, the watermark insertion and removal can be implanted in real time by making the altering the encoder.

The scheme has number of drawbacks also which are explained briefly as

- Capacity of the watermark to be inserted in the video is influenced by various coding limits.
- Here, some watermarking algorithms are restricted to an extent due to the modification of encoder and decoder while implementation [22].

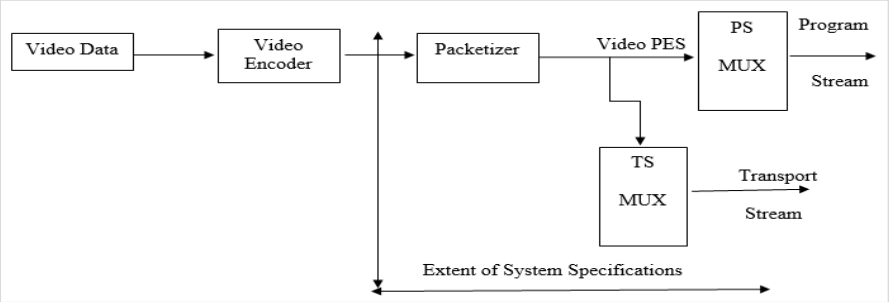

Figure 3 Model for MPEG-2 system

3) Watermarking after compression

In this specific area, the content (binary text/image) is to be embedded in the data directly. The major advantage of this method is to maintain the visual quality of the object, at the same time keeping its complexity at the low level and further encoding and re-encoding of the bit stream is not required [22].

Thus, every algorithm consists of some positive as well as some negative points. In realistic areas of relevance, the above mentioned schemes are used depending upon the requirement and the type of watermark to be put into the host object.

2.2Aspects of watermarking

The chief aspects of watermarking technique are discussed in *Table 1*[23]. Some of these features are of great significance for basic watermarking scheme. The term robustness defines the strength of the watermark like a delicate watermark is not that sturdy and hence reduces the robustness against several processing methods. It is not possible to change or eliminate the watermark. When a watermark is used for other applications, it is required that the watermark remained in host information, even if the host data quality is reduced practically or non-practically. The parameter is computed by the normalized correlation coefficient (NCC) given by Equation 1.

$$NCC=\frac{\sum i \sum j . W_{ij} * W'_{ij}}{\sqrt{\sum i \sum j (W_{ij})^2} \sqrt{\sum i \sum j (W'_{ij})^2}} \quad (1)$$

Imperceptibility helps in insertion without affecting the quality of the video frame. Watermarking algorithms may embed the watermark so that it may not affect the fundamental host data quality. The Watermarking embedding process is imperceptible; if human beings cannot differentiate the actual data from inserted watermark data [24]. The tool used for the measurement of the said aspect is peak-to-signal-noise-ratio (PSNR) given by Equation 2 and 3.

$$PSNR= 20 \log_{10} \left(\frac{\text{maxx}}{\sqrt{mean\ square\ error(MSE)}}\right) \quad (2)$$

$$MSE= \frac{1}{P \times Q} \sum_{x=1}^{P} \sum_{y=1}^{Q} ||AF - WF'|| \quad (3)$$

max_x= maximum of WF (x, y) where i ranges from 1 to P and j ranges from 1 to Q respectively. Here, mean square error (MSE) is the error between actual frame (AF) and the watermarked frame (WF'). The result of PSNR value is calculated in db.

The important attribute of video watermarking is to implement security and to add additional security algorithm to make the scheme more secure. Finally, the capacity of the object to embed the watermark, as the size of the same can affect the quality of the object which is a most important issue [25]. Some more relevant areas of applications related to the general features of watermarking are briefly depicted in the tabular form.

Table 1 Associating characteristics with significance

S. No.	Attribute	Analysis	Significant Areas
1	Robustness	- Associated with extraction of watermark -Oppose attacks & other manipulations	Forensics practices, Copyright protection
2	Detectability	-Related to efficient insertion method -Maintains the visual quality of object	Digital Records, Owner Identification
3	Security	-Allied to secure the host object - Using some security algorithm to keep the host safe	Copying, Piracy, For Armed Forces
4	Capacity	-Associated with the size of the object to be inserted - Embedding of many objects can be done - Check the appropriate size to maintain the quality	Broadcast Monitoring, Video Authentication
5	Expenditure	-Total Expenses involved in the execution of the complete system	Law enforcement, Defence, Journalism
6	Reliability	-To check the overall result to be dependable	Almost all the application areas

2.3 Relevance of digital video watermarking (DVM)

Fingerprinting

It has been researched that unlawful dissemination of video content after copying video content through a camcorder from drama theatre is the main issue [26]. Video content creators used this method to trace the origin of unlawful duplicates [27]. Following this method, a specific watermark image has to be put in all the copies given to all the clients where the video is to be shown. It may comprise the client's detection or the information about the cinema theatre, so that if the copyrights are violated, then the one who created the video content may condemn the client or the theatre crew who allowed the felonious act of copying.

Copy regulation

Watermarking is utilized to regulate arithmetical replay and recording sensors, for example, digital video disc (DVD), for avoiding illegal copying and playing. If the sensor identifies the watermark content while creating the duplicates, the illicit act of copying can be avoided. Thus, the utilization of video content is increased, which may be used to manage the online streaming and it may be exploited to regulate online streaming by storing watermarking filters at system hop.

Broadcast monitoring

The content of the video is disseminated over the television (TV) networks and if the content has broadcasted as a contract. It may be authenticated using active or passive monitoring. The existing and actual videos are compared previously, and a maximum number of data storage is needed, if the security technique of watermarking may impart the vigorous surveillance in an imperceptible and sturdy way [28].

Video authentication

The authentication of the content can be checked by embedded watermarking in the host. The application areas like video surveillance and medical imaging in which the protection of the content from substitutes is necessary [29]. A delicate watermarking helps to identify tampering and avoids data where the segments of data have been changed.

Copyright protection

A copyright vendor (owner) may embed watermarking comprising the copyright data in the host video if decoded; it may be utilized as evidence of the rights. Hence, as the purpose of videos was to delay the rights of the video content by eliminating the watermark, it must be robust to different threats in real-time applications [30, 31].

2.4 Watermarking attacks

In watermarking, there are some popular attacks pertaining to the video object [32] like averaging, swapping, addition, dropping of frames and other geometric attacks etc. Additionally, there are several purposive or deliberate attacks and inadvertent attacks, which are further categorized as shown in the *Figure 4.*

2.5 Video watermarking schemes

There are several schemes assist in the implementation of video watermarking. They are classified based on diverse parameters. These methods have been surveyed in survey for the different types of videos and images. Watermarking is done on compressed as well as non-compressed videos [33]. The existing watermarking methods are shown in *Figure 5.*

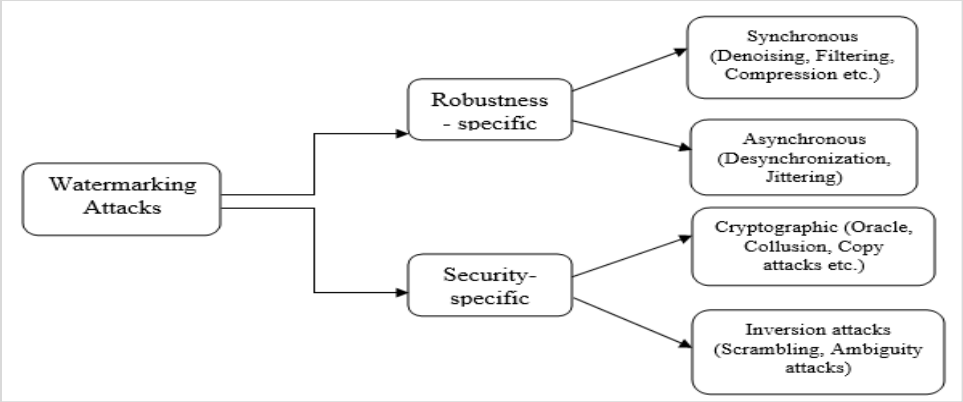

Figure 4 Classification of attacks in watermarking

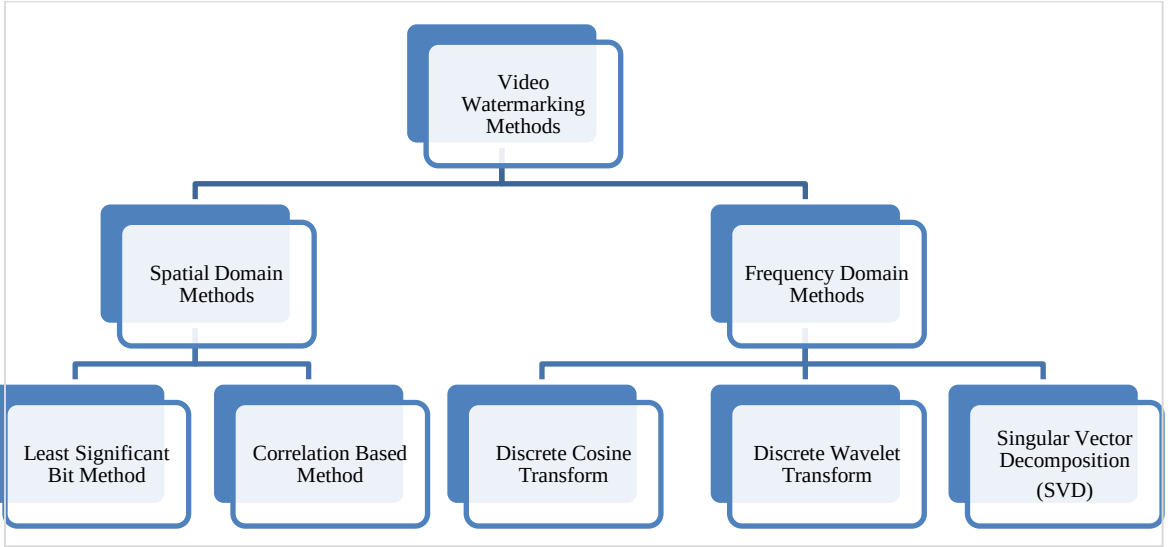

Figure 5 Video watermarking schemes

Spatial-domain watermarks

Spatial-domain techniques (pixel or coordinate domain), a text/image is inserted in the specific frame of the video object by updating the pixels of the same. They are quite simple and convenient to execute and also need fewer things resulting in involvement of less computational cost. However, they are not proved to be reliable and sturdy and can withstand several video-specific attacks.

Least significant bit (LSB) modification method

The straight-forward method of inserting a watermark is where the insertion is being done on the LSBs of the real video content. In the said approach, generally a smaller object may be embedded number of times in order to provide maximum capability of channel for transferring the information. During attacks like cropping, noise addition, lossy compression etc. even if a single watermark survives, it would be accepted and considered as success. LSB substitution is quite simple to implement but at the same time it has several limitations. In addition to this, if the process is detected, the attackers can conveniently alter the inserted object.

Correlation method

The said method involves the use of correlation properties of noise patterns in the frames of the video object. Taking an example of some noise W is inserted in the image component I as per the equivalence 1 shown here.

$$I_w(a,b)= I(a,b) + k\, W(a,b) \quad (4)$$

Where 'k' is used to represent the constant value which shows the gain, and I_w is the resultant image. According to this method, if the value of gain factor increases, then the robustness of the watermark also increases but the quality of the same decreases. During the retrieval process, the same steps need to

be followed, and the association between the added noise and the resultant image is calculated. If it comes out to be more than threshold value taken, then the detection of the watermark is done as well as only one bit is set, this procedure can be implemented on the watermark with more bits conveniently with the decomposing the frames and converting them into blocks, finally repeating the method for every block[34].

1) Transform domain watermarks

Frequency-domain techniques (transform-domain) alter the coefficients of the altered sections of the video as per insertion scheme which makes it difficult to retrieve the inserted watermark. Thus, the above said methods are more efficient in perceiving the better values for the features named strength and imperceptibility while designing such algorithms. Discrete cosine transform (DCT), discrete wavelet transform (DWT), discrete Fourier transform (DFT) and singular value decomposition (SVD) methods are the procedures of information modification where the content inserted is disseminated over the original data making it hard to remove.

i) DCT

It is the method of representing the data by summing up the cosine functions moving at different frequencies. It converts the object from its spatial-domain to the transform-domain. In this technique, an object is divided into spectral sub-bands. The results here are computed with the help of DCT coefficient, it generally comes out to be a visual object of different frequencies [35]. The frequency values displayed horizontally diverge in horizontal direction and the rest placed vertically deviate from top to bottom. The binary text/image taken as watermark is proved to be more sturdy and imperceptible if the process insertion is being done on the middle frequency band [36]. This method is analogous to DFT.

ii) DWT

This is an important technique used for watermark insertion in the process of digital watermarking. According to it, the frames of a video (image) are decomposed at multi-resolution levels. At the first level, the same is decomposed into the bands starting from low to high frequencies comprising of row frequency and column frequency [37]. This technique is believed to give better and authentic results as compared to other techniques available. The feature of multi-band decomposition of DWT makes it to produce highly accepted robustness results of the watermark with good visual quality of the object.

iii) DFT

In DFT, initially the brightness of the target frame is checked followed by taking the magnitude of the coefficients. The DFT coefficient is altered and then the inverse DFT is applied. This method results in better sturdiness as compared to other techniques while applying basic filtering, sharpening, geometric and compression attacks but the sufficient quantity of information can be inserted to the video content [38, 39].

iv) SVD

It is the method in which the frequency domain (FD) consists of optimal states. In this scheme, after extracting a frame from the original video, it treats the image in the form of a matrix divided by the technique in the 3 specific components U, S and V^T. The SVD operation of matrix A (N × N) is defined and shown by the Equation 5:

$$A = U\ S\ V^T \quad (5)$$

where U and V matrices are considered as the singular vectors of A and S matrix values placed diagonally are said to be singular values of A. Furthermore, a relationship of the basic characteristics with the above mentioned techniques and their comparison [40, 41] with each other is shown in tabular form as given as the *Table 2* shown below.

Table 2 Comparison of video watermarking schemes

S. No.	Approach	Advantage	Limitation	Usage
1.	LSB	Easiest spatial domain (SD) method and as the name suggests, lest significant bit is used to add the watermark or information in the multimedia content	This technique is least secure and involves poor strength, thus preferred for steganography application only.	It is generally not used for watermarking of a video object
2.	Correlation Based Method	Here, pseudo-random noise is added to luminance component of the pixel of the object. The computation uses the gain factor which finally maintains the quality and the	The higher value of gain factor reduces the quality of the video object whereas the smaller value of the same affects the	If the correlation coefficient is higher than the threshold, that particular feature will be selected

S. No.	Approach	Advantage	Limitation	Usage
		sturdiness of the watermark.	sturdiness of the method.	
2.	DCT	An effective and fast algorithm which can be used for computation and the output for the constants consist mainly of large number of near zero values. Another advantage being that the transformation is orthogonal; preserving the energy [42].	The input from 8 x 8 blocks are integer-valued, the output values are typically real-valued making it need a quantization step so as to make some decisions about the values in each DCT block and produce output that is integer-valued.	On the basis of PSNR, this method gives better results with bigger coefficients and compression
3.	DWT	DWT helps in capturing both frequency and location information known as temporal resolution. As data are shattered into more components, it is easier to filter in or filter out a given non-stationary waveform.	Greater complexity. More and more processing power is needed and thus more time. If the signal is stationary, the DWT might not be needed [43, 44]. In DWT, it is harder to interpret the results.	It avoids blocking of the area in the object.
4.	SVD	Abridges the data, take the noise, helps in improving the final outcome. This method works efficiently with the smaller dataset as well.	The data after applying the transformation may become little complex and thus, tricky to comprehend [45].	It uses complete component of the matrices, thus making it easier to influence and examine.
5.	Principal component analysis (PCA)	By implementing PCA on the dataset, all the principal components are devoid of any correlation with one another. Performance of the algorithm is drastically improved as PCA takes away the correlated variables.	Once PCA is implemented, original features turn into principal components, which might not be as readable and interpretable as the Original features. If the PCA is implemented on varied data, the principal components will be based towards high variance leading to false results [46, 47]. In case wrong selection of principal components is done, information loss might occur as compared to the original list of features.	It is quite useful in order to increase the calculation speed by condensing the dimension of the content.

From the results given in the *Table* 2, the best method with respect to accuracy can be identified but the results vary for all the schemes as it depends upon the various features like size, quality of the data used to

implement the technique. Currently, the most significant accuracy is given either by combination of various transform-domain methods known as hybrid approach or by individual methods depending upon the input data/ video object i.e., DCT, DWT, SVD, PCA.

The major objectives of this study are given as below-

- To present an organized review and investigation of the work done in the field of DVW.
- To show various watermarking schemes in order to insert and extract a watermark from the given video object.
- To analyze several methods available through various performance evaluators.

This paper is composed of seven different sections. Section 1 presents the introduction. In section 2, the background of the topic is given in detail. Section 3 includes discussion regarding the mapping methodology of the systematic review. In section 3, the mapping report for the systematic review is presented, which covers the mapping strategy for the complete work. In section 4, the detailed literature survey of the research work done in DVW, along with the advantages and limitations, are discussed. In section 5, the various challenges occurred while designing an algorithm is given. Discussion and analysis are covered in section 6. Finally, conclusions and future recommendations have been provided in section 7.

3.Review methodology

The methodology used in this systematic review is outlined below, including the search string, selection criteria, process flow, literature trend, publication distribution, year and publisher-wise distribution, and justification for the selection. The search strategy was designed to identify all relevant articles on video watermarking. The search string was formulated using a combination of keywords and Boolean operators. The search was conducted in the following electronic databases: IEEE Xplore, ACM Digital Library, Scopus, and Web of Science. The search string used was as follows:

(("video watermarking" OR "DVM" OR "audio-visual watermarking" OR "multimedia watermarking") AND ("robust" OR "imperceptible" OR "invisible" OR "secure" OR "reversible" OR "fragile" OR "semi-fragile" OR "tamper-proof" OR "tamper-evident" OR "blind" OR "non-blind" OR "robustness" OR "security" OR "fidelity" OR "authentication" OR "encryption"))

In this section, the mapping methodology of the systematic review is presented. The review and meta-analysis is categorized into three parts. The first part focused on publication trends, criteria of the selection of papers and the methodological scenario on DVW. The second part includes the major publishers chosen for the study. The third part gave the idea about the current scenario of DVW. The major mapping questions by recognizing the scope after comprehensive search of literature from last more than two decades are related to the enhanced safety of the inserted watermark in the video against diverse attacks like collusion, composite and ambiguity attacks as well as maintaining the quality loss of the video object, thus raising the questions about the size of watermark before initiation and to find the answer about the best hybrid approach/technique available to secure the transfer of multimedia content[48–51].

The rules followed to complete this overview are classified into two different categories.

i) Expanded study of research articles having novel techniques to embed and extract the watermark.
ii) Discussion of papers already published to check the accuracy of schemes and compare them to find the best available in this field.

3.1Inclusion and exclusion criteria for the paper selection

The parameters used for including and excluding the studies in this review are discussed in the *Table 3* given below. The trend in the number of publications and year-wise distribution of articles on video watermarking over the years is shown in the *Figure 6* below and Bubble chart representation of most cited articles from 2015-2017 is shown in the *Figure 7*. *Figure 8* shows Bubble chart representation of most cited articles from 2018-2020. *Figure 9* shows the PRISMA [52] style of representation adopted for paper selection in the study. Based on inclusion and exclusion criteria, only 117 papers were selected for the final study.

3.2Major publishers selected for the study

An extensive literature has been studied in the area of DVW. The research papers are identified from diverse platforms like Google Scholar, IEEE Xplore, ACM Library, ScienceDirect, other Journals, Conferences, Books and Blogs with the help of keywords ‘Video Watermarking’, ‘Multimedia Security’, ‘Copyright Protection’, ‘Imperceptibility’,

'Information Hiding', 'Robustness', 'Transform-domain method' [53–58].

Table 3 Parameters for study inclusion and exclusion

S. No.	Inclusion	Exclusion
1	Contemporary resources which were not dated and were in sync with the current technical advancements.	Most of the literature on the subject were old and thus did not warrant the usage for the objectives laid for the study.
2	The methods and matrices laid in the resources were contemporary leading to an insight into the study.	The other paper/literature which were excluded used methods and matrices which didn't align with objectives of my study.
3	Articles that propose new and hybrid watermarking methods to get appropriate results.	Articles that are duplicates and have overlapping content. Most of the resources excluded were associated with studied of image watermarking; thus making them redundant for usage.
4.	Articles published in reputed peer-reviewed journals, conference proceedings and books.	Articles that are not available in full text.

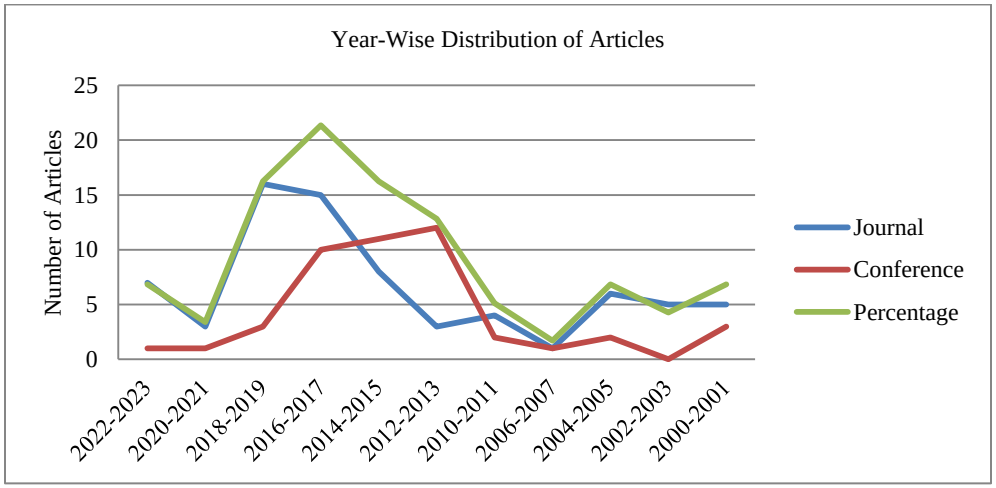

Figure 6 Graphical representation of year-wise distribution of articles

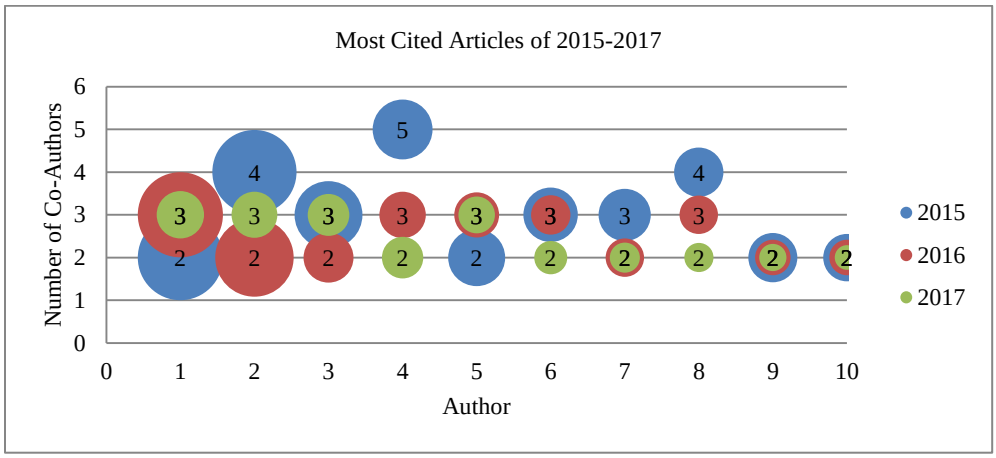

Figure 7 Bubble chart representation of most cited articles from 2015-2017

From last two decades, around 204 research papers were identified in the said area, out of which 87 papers were excluded as they were old, redundant, observed ineligible by the tools used in implementation and the techniques were mismatched with the study. 117 studies were taken into consideration containing 66 published in reputed Journals and 51 from several conference proceedings

consists of hybrid methods to get apt results and contemporary sources close to the current generation of studies. The paper distribution in terms of publishers is presented in *Table 4.*

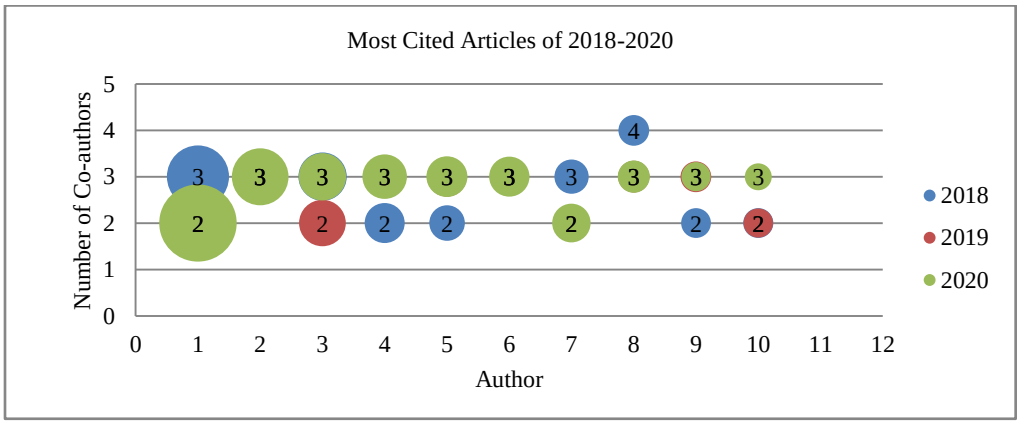

Figure 8 Bubble chart representation of most cited articles from 2018-2020

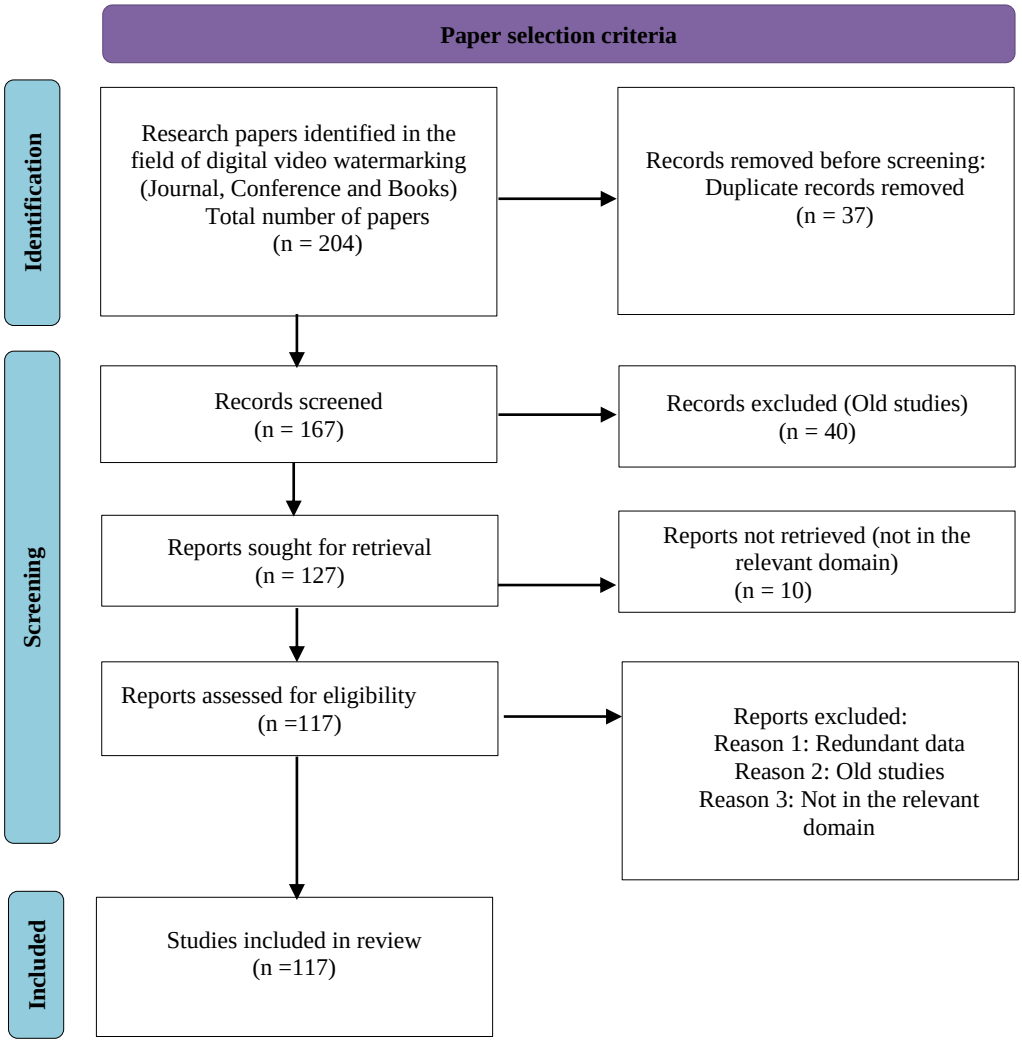

Figure 9 PRISMA style representation used for paper selection

Table 4 Distribution of papers based on different publishers

S. No.	Publication	Number of papers	Percentage
1.	IEEE Conference	32	27.35
2.	IEEE Journals	23	19.65
3.	Elsevier Conference	19	16.23
4.	Elsevier Journal	10	8.54
5.	Springer Journal	9	7.69
6.	Others (MDPI, Hindawi, etc.)	24	20.51
Total		117	100

The selected articles represent a diverse range of research in video watermarking techniques and applications. The inclusion and exclusion criteria were designed to ensure that the selected articles are relevant and of high quality. The selected articles were published in reputable journals, conference proceedings, and books, and were written by experts in the field. The review process was conducted systematically, and any disagreements were resolved through discussion and consensus. Therefore, the selected articles are considered to be representative of the current state.

3.3Current scenario and recent trends of video data security

As video watermarking being increasingly studied upon, a lot of resources are being generated. A lot of work in the field of different approaches like DCT, DWT, and SVD [59–63] etc. has been published in various reputed journals (ACM, Elsevier, and IEEE). Most of this work has been covering the non-compressed domains as stated above. The current scenario has very less resources on compressed domain, hardware video watermarking and collusion attacks, thus making these topics an imperative to work upon [64–66]. Aggregating and working on these methods is time consuming as the data needs to be collated from a lot of sources across online and offline inventory. Collusion Attacks' and Ambiguity Attacks' resources are mainly hard to find and corroborate due to very little work done on it [67–70]. Taking into account all of the above factors we can easily come to the conclusion that above stated domains need to be studied more so as to create a comprehensive and exhaustive platform. On the basis of existing literature and research, some of the recent trends in the field of video watermarking with significant potential for future development and improvement include:

1. Deep learning-based techniques: Recent research has explored the use of deep learning-based techniques for video watermarking, which have shown promising results in terms of robustness and security.
2. Blockchain-Based Watermarking: Blockchain-based watermarking techniques have been proposed as a potential solution for protecting digital media copyright. These techniques enable the creation of tamper-proof records of digital media ownership and usage.
3. Multi-Modal Watermarking: Multi-modal watermarking techniques that combine different types of watermarking methods, such as digital, visual, and audio watermarking, have been proposed to increase the robustness and security of watermarking.
4. Reversible Watermarking: Reversible watermarking techniques that enable the extraction of the original video without any loss of quality have gained attention in recent years. These techniques can be useful in applications where the video needs to be modified or compressed.
5. Adversarial Attacks: Adversarial attacks that attempt to remove or alter the watermark have become a significant challenge for video watermarking. Recent research has focused on developing more robust watermarking techniques that can withstand these attacks.

4.Review of literature

The systematic review and the study of the methods used for DVW are given in the section. The research questions like major approaches used for video watermarking, the discussion of research articles with the results and techniques are discussed here. It also provides various advantages and the challenges of the techniques used.

The systematic review conducted on video watermarking involved searching for relevant articles in various electronic databases using a well-formulated search string. The selection criteria were based on the inclusion and exclusion criteria, which ensured that the selected articles were of high quality and relevant to the topic. The review process involved screening the selected articles by two independent reviewers, and any disagreements were resolved through discussion and consensus. The

literature review on video watermarking revealed that there are various techniques and algorithms that can be used to embed watermarks in video stream (VS). These techniques can be classified into two main categories: SD and FD. In the SD, the watermark is embedded directly into the video frames, while in the FD; the watermark is embedded in the frequency coefficients of the video frames. The review also revealed that there are various applications of video watermarking, including copyright protection, authentication, TD, and content identification. The performance of video watermarking techniques can be evaluated using various metrics such as robustness, imperceptibility, capacity, and security. The evaluation of video watermarking techniques is usually done using simulation and experimental methods. The literature review also highlighted some of the challenges faced in video watermarking, including the trade-off between robustness and imperceptibility, the vulnerability of video watermarking to various attacks such as geometric distortions and compression, and the need for a robust and secure key management system. Another challenge is the need for standardization of video watermarking techniques and evaluation metrics. One of the advantages of the systematic review is that it provides a comprehensive and unbiased overview of the literature on video watermarking. The review process involves rigorous screening and evaluation of the selected articles, ensuring that only high-quality and relevant articles are included. The review also highlights the current trends and challenges in video watermarking, providing insights into areas that require further research. *Table 5* compares the spatial and FD video watermarking techniques. It shows that the FD techniques are more commonly used than the SD techniques. This is because the FD techniques are more robust to attacks such as compression and noise.

Table 5 Comparison of spatial and FD video watermarking techniques

Technique	SD	FD
DCT	X	✓
DWT	X	✓
SVD	X	✓
LSB	✓	X

4.1Approaches used for securing a video object

In 2013, Lei et al. [71] used DCT on some of the bands retrieved after executing DWT on the host. The result shows that the suggested approach performed well aligned to several attacks. Authors proposed a robust and safe watermarking scheme using the dither modulation and particle swarm optimization for the quantization of breath sounds. The techniques used are lifting wavelet transform (LWT), DCT and SVD to implement and get the best results in imperceptibility and sturdiness.

In 2014, Agrawal and Khurshid [72] proposed a research method on the DVW structure that embedded robust and unclear watermark data into VS of MPEG 4, H.264/AVC, MPEG 1, and MPEG 2 standards. The procedure of embedding was given in the form of a discrete wavelet (DW) domain. However, the things between the transparency and vigour were measured as an optimization issue that was resolved by genetic and particle swarm based on crossbreed nature-inspired optimization method. However, an acoustic signal was transformed into a 9-bit plane through bit-plane slicing and inserted into the data frames of video signals as a logo. The simulation analysis outcomes depends on the performance parameters such as PSNR and NCC confirmed that the planned technique defines consistent enhancements for different series related to current ones for geometrical threats such as rotation and cropping. The experiment result shows that the watermarking method was more robust against different threats. A video watermarking method DWT and genetic algorithm (GA) and particle swarm optimization (GA-PSO) was implemented using an audio signal watermark. Further enhancement can propose technique using hybrid technique with GA-PSO based on the image watermarking approach.

In 2015, Guo et al. [73] gave a watermarking algorithm in combination with the concept of encryption. Prior to executing watermark insertion process, Homomorphic Cryptosystem (HCS) is used to encrypt the host object.

In 2014, Asikuzzaman et al. [19] developed a novel bit-plane spliced, a twisted colour-based image embedded on the colour watermarking by utilising hybrid transformations with better imperceptibility and robustness. Various methods were used conversions with the high robustness, and data rate (n represents the number of motion frames) that were separating by 24 images in 1 sec of the video; here n was representing the complete amount of the video data frames. They sliced the color watermark picture into twenty-four segments using the bit plane slicing (BPS) method. Firstly, they were known as Arnold transformation key (ATK) for scrambling the segments to get the initial level of safety. Therefore, a

security achieved with a suitable key only may convert the receiver segments. Secondly, they embedded those twisted slices on the DWT mid-frequency factors (lower and higher band) of sequential first phase contourlet transform un-moved frames of the color videos. Thus, the unmoved data frames were recognized through histogram variation that depends on the shot boundary detection (SBD) method. After that, to improve the security level, they created an eigen vector (V) from the Red Green Blue (RGB) image watermarking using the covariance matrix (Cov) and extreme eigen value (E), and it embedded on other DWT mid-frequency coefficients. Consequently, embedding the slices (but not the entire picture) may enhance the rate of imperceptibility. The embedded mid-frequency site may resist the low, high (LH) pass filtering threats; thus, it maximizes the phase of reliability. Therefore, the planned approach was more appropriate for security. Lastly, unless the payload was confirmed, they required twenty-four un-moved data frames for inserting the watermark onto the shield-video. Thus, the remained data-frames may be used for inserting the three dimensional (3D) images. Experimental outcomes proved that the planned scheme presents a reliable performance against numerous noteworthy image processing threats, temporal and spatial threats.

In 2016, Arab et al. [74] discussed video watermarking, specifically to the audio or video interleaved (*.avi) kind of video file format. They developed 2 novel watermarking methods that offered a maximum level of softness and effective tamper detection (ETD). Individually, models were susceptible to 9 different kinds of common threats that demonstrated VW8F to be larger, mainly in terms of imperceptibility. However, it analyzed from the results that VW8F provided a better imperceptibility (PSNR value = 47.88 ~ 48 dB), and confirmed value at recognizing a wide variety of interfering related to the same methods.

In 2016, Han et al. [75] presented a novel watermarking approach that depends on the host image (HI) assessment and soft computing approach GA. Using the characteristics of the human visual system (HVS), the three-dimensional(3D) image assessment may assure the softness. It improved the inserting ability of the logo (watermark) under a similar graphic effect, which may insert more watermarks in the HI. The GA was used in the inserting procedure. It may not individually enhance the image quality, then improve the authentication and vigour of a watermarked image (WI). This approach fulfilled an optimum compromise among the robustness and picture quality. Also, the numerical results showed that the research technique was a better presentation in terms of transparency.

In 2016, Sridhar and Arun [76] authors discussed the technology of watermarking which was an efficient approach to resolve the issue of protecting multimedia data. It was the capability of covering the data into a host such that the embedded information was invisible.

In 2017, Kumar et al. [77] proposed a method, the luminance band of the chosen data frames was taken in the future, and it was gathered to different image pixel segments. Binary 3D colour watermark images were divided into different segments, concatenate the layers, and then embedded into separate flipped under wavelets. After that, release the shares into the image, and load in terms of unique luminance layers. Simulated results achieved the higher image quality parameter (PSNR) with less error rate, and the correlation coefficient of video watermarking was closest to unity.

In 2018, Shukla and Sharma [78] utilizes two algorithms, one for detecting scene boundaries using statistical estimation and another for embedding watermarks in the detected scenes using DWT with Haar wavelet decomposition by using the LH sub-band and LL sub-band of the cover video. The experimental results showed that embedding with the LL sub-band provided better visual imperceptibility as well as improved performance in terms of normalized correlation and bit error rate (BER). The scheme outperformed existing schemes in terms of robustness, imperceptibility, and computational time.

In 2017, Yoo and Kim [79] represented an event watermarking codec which was vigorous besides the re-encrypting threats for the maximum range of the videos. The codec used a separation method and text detector methods for developing event watermarking to HVS. The simulation outcomes confirmed which research method fulfils the needs of invisibility, real-time processing, and vigour against the minimum BR encrypting and video format conversion. The research method was the main benefit of flexibility, minimum computation, and simplicity, etc. Therefore, it was a valuable candidate for several new and real-time uses like audio-visual fingerprinting for device boxes, internet protocol TV, personal video recorders (PVRs), and TV cable setup

devices, etc. Results were presented in the terms of recognition rate, the BR per series beside windows media video (WMV), MPEG-4 H.264, and MPEG 2 re-encrypted videos. The logo may be removed from every data frame of the watermarked VS. This research method can improve the HVS model to minimize processing time and maximize multimedia manipulation efficiency.

In 2018, Himeur and Boukabou [80] implemented a video watermarking technique where watermark data were encoded through novel chaotic encode and embedded in the key-frames extraction from the VS. Hence, an easy and fixed frame extraction approach based on gradient degree similarity deviation (GDSD) was utilized. This method may expressively reduce the difficulty of video watermarking schemes. It includes the watermark in a shade way, novel extraction and embedded methods were designed through the quantization procedure. A binary conversion based on wavelet transformation and decomposition method was achieved to insert the watermark with minimum graphic noise. The analysis was done to identify the system shown by sequences of the experiments. Hence, the planned algorithm has improved performance than the existing approach in the form of strength and softness. Moreover, the authentication requirement of the planned method was acquired with a proposed chaotic encoded process.

In 2018, Zear et al. [81] implemented various watermarking methods based on DWT, DCT and SVD for medical uses. It identifies the confirmation resolution research approach used three-logos in terms of a medical-lump image, the specialist verification code, and analytic data of the patient as the texture logos. To enhance the vigour system shows off the 3D image watermark, back propagation neural network (BPNN) was developed to the removed image to optimize the distortion properties on the WI. Therefore, the authentication of the WI was improving through Arnold transformation (AT) existing embedding it into the cover image (CI). Also, the sign and autograph texture logos (watermarks) were encrypted by a mathematical lossless-compression method and hamming error correction code (HECC) correspondingly. The encoded and compressed text watermark was then embedded into the CI. Numerical outcomes were acquired by changing the gain factor, varied the dimension of texture logos (watermarks), and the various CI modalities. The consequences were delivered to demonstrate that the planned approach was capable to withstand various signal processing threats and offered better performance for capability, security, robustness, and imperceptibility, etc. The robustness system presentation of the technique was also associated with other methods. Lastly, the video quality of the logo image was calculated by a particular approach. It represents that the video quality of the image watermarked was suitable for analysis at various gain-factors. Thus, the research approach can search for potential use in the avoidance of patient id holdup in health care uses.

In 2018, Shukla and Sharma [82] represented a DVW scheme for copy and copyrights protection. The research approach applied to the hybridization of DWT and scene change detector (SCD). The proposed method was presented in four phases such as the initial phase was searching the data frame wherever the logo (watermark) was to be embedded. The watermark investigation was done by the three-level decomposition of low-level sub-band with a DWT that was explained in the second phase. However, the robustness and transparency were analyzed under 15 various threats in the 3rd phase. Enhancement in the transparency and robustness as compared to watermarking using similarity index (SI) in the 4th phase. The simulation result analysis showed that the research technique produces the removed image and video marked of the high quality and may endure various digital image processing, *.jpeg geometric, and compression threats. Experimental outcomes define the enhancement in the system shown as the decomposition phase maximizes from phases 1 to 3. The proportional result investigation with the prior methods defined the enhanced imperceptibility, vigour, and the optimized computation time (CT) of the research method.

In 2018, Nouioua et al. [83] developed a new and reliable DVW method depends on SVD executed in the multiple resolutions SVD field. Generally, the prior techniques were embedding the logo in all the video data frames. It was high time consumption models, and influence video HD quality. The planned approach selected single high-speed motion data frames in every slot to host the logo (watermark). Thus, the number of data frames to be managed was subsequently optimized, high quality of the videos that assured and in the meantime, HVS may not sign the changes in the high-speed motion areas. The result analysis showed that the research approach may attain better transparency while being robust against several types of threats like filtering,

distortion, compression, and frame collusion (FC). The comparative analysis with various approaches searched in the survey that offered better robustness.

In 2019, Arab et al. [84] discussed the main interesting issues of DVW methods, specifically the vigour of SD. The research methods verify the effectiveness of the TD, and then the softness of the study method can be studied by the quality parameters such as PSNR. The quality parameter was considered to define the signal-quality; if these parameters reduced the value as well. In the proposed work, few threats were applied to planned models to select the consistency of the tamper recognition and imperceptibility of the proposed model that was experimented with PSNR. This parameter was considered to recognize the signal quality; where the PSNR ratio reduces with the signal quality. It was identified that quality has a through correlation with imperceptibility. The NCC was utilized to relate the refined logo (watermark) with the actual watermark. NCC parameter may compute the removed watermark to identify the vigour. For analyzing the effectiveness of initial threats applied to the watermark video. The digital video watermark data frames were prolonged, then the Microsoft office image manager or window paint was utilized for applying threats at the end again, the data frames were merged and then the effected video was checked for identifying the tamper. It evaluated the performance metrics such as PSNR and NCC.

In 2015, Singh et al. [85] studied the digital data over the internet was un-secure and several methods developed for security purposes. Stenography, Cryptography and watermarking were the methods that secure the information over the internet. The analysis of digital watermarking was done with the various methods and comparative analysis with several parameters. Video Watermarking was using for several motives such as image authentication (IA), security, copyright, and various purposes. Several methods such as transformations and encoding were also included in watermarking for giving reliable outcomes. The planned model defined the method of digital watermarking, and represented the robustness, and secure 3D image watermarking through coefficient differencing, and chaotic encryption (CE).

In 2020, Mohanarathinam et al. [86] analyzed the DVW methods with advantages and disadvantages. The DVW arrangements with the embedding of secure information into real data. DVW methods were categorizing into three major classes, and depending on the field, kind of the document such as texture, image, video, music, and human perception (HP), etc. The performance metrics like PSNR, MSE, and BER. They described the different types of threats and performance parameters to calculate the image. Hence, the assessment was completed to declare hybrid methods for different watermarking for rights coverage, information coverage, authentication, and software applications like Facebook, Twitter and Whatsapp.

In 2019, Nadesh et al. [87] implemented a hybrid technique for watermarking that includes framelet transform (FT), feature extraction method using PCA, and SVD. The developed model was more robust against watermarking threats, imperceptibility, ability, and authentication. The planned model was robust to different threats because DWT hides the data securely, and SVD was used to measure the embedded data. Results demonstrated that the technique assures the actual information using error rate and PSNR parameters. Hence, the value of MSE was 0.0035, and the peak signal rate was 43 per cent that defined the robustness approach. This method hides the high number of data in the video and assures that an unsecured can't detect or find the watermark, and only the right consumer can get the watermark with the help of the secure key.

In 2020, Alotaibi [88] proposed research work to formulate a new video watermarking framework which comprises three different phases- optimum video frame estimation watermark, the embedding procedure and watermark extraction procedure. Hence, optimum frames were identified using a novel hybrid approach such as Trial Based on Jaya-Firefly (TU-JF) approach so that the PSNR may be maximum. The data frames were allocated by mark 1 and 0, where the label-1 represents the data frame with superior peak signal to noise ratio, and mark zero (0) represents the frame with decreased peak signal to noise rate. Subsequently, the data collection was generated from acquired results where every data frame of videos was identified with the feature extraction characteristics. Hence, optimum data frame detection was carried out using a deep belief networks (DBNs); and the acquired information was then trained the model. Optimum frames were estimating consistently during testing. The main goal of the research work concerns the hidden neurons (HNs) in the DBNs context that helped to improve the prediction accuracy rate. Finally, the "watermark embedding procedure" and "extraction procedure in

watermark" was done where the image may embed in the optimum video frames.

In 2021, Sharma et al. [89] gave a hybrid and protected video watermarking scheme in order to handle the problems related to ownership and copyright protection with the use of safe graph based transform, hyperchaotic encryption and SVD methods. Further, an algorithm is implemented for suitable selection of frames of the video object to insert the watermark as embedding the watermark in all the frames would lead to time complexity. The proposed scheme is robust against several categories of attacks including compression attacks, signal-processing attacks and geometric attacks. The inclusion of supplementary security algorithm makes the scheme more secure and prompt. The authors suggested that the performance of the presented scheme can be enhanced by using different optimization algorithms to optimize the factors related to insertion of the watermark that finally returns the better values of PSNR.

In 2021, Agarwal and Husain [90] presented a novel scheme based on DVW is proposed that check and execute the valuable outlines and attributes of the video object. The complete execution of the method is based upon the circle symmetry algorithm with the use of two-dimensional(2D) LWT and Speeded-up robust features (SURF); that help in obtaining some constant attribute points on the estimation of two-2D-LWT using the luminance part of each frame of the video object. These attribute points with the highest intensity on the circumference of the half portion of a quadrant of a circle are used to find the specific location to insert the watermark. The said method is checked against several categories of temporal, compression and addition of noise attacks by evaluating various subjective and objective parameters. The outcome of the technique discloses a good value of the metrics as well as maintains the quality of the video object; thus proved to be better than the other techniques.

4.2Results and summary of some published research in the respective area

Table 6 Results and the techniques of some related research articles

S. No.	Ref. No.	Techniques	Results	Advantage	Limitation
1	[91]	DWT, Chaotic Scrambling	The overhead due to key embedding is observed to be only about 3%. Therefore, it shows that the proposed algorithm is capable of handling noise efficiently	Designed to be computationally efficient, which reduces the time and resources required for watermark embedding and extraction	If an attacker has significant knowledge of the algorithm, it may be possible to remove or modify the watermark without detection
2	[92]	Fast Fourier Transform (FFT)	Here, the strength in the prediction frame is computed which shows the number of blocks in the present, previous & next frames which finally gives the location of interference	It allows for the extraction of multiple watermarks from a video without any loss of data	Method could be its complexity and computational cost, especially if the video is large and contains multiple watermarks. This can make the extraction process time-consuming and resource-intensive
3	[93]	DCT, DWT, SVD, Selective Encryption	The combination of various frequency transform methods can withstand several categories of attacks	It is useful for various video applications where high data embedding capacity is required.	It does not provide a detailed analysis of the robustness of the proposed watermarking scheme against various attacks, such as compression, filtering
4	[94]	SVD, DWT, Chaotic map	The result after extracting the watermark from the luminance channel gives structural similarity index (SSIM) =0.8956 and chrominance channel SSIM = 0.85855. The latter shows the lesser value but the eminence of	Extraction of watermark can be done from the watermarked video without causing any distortion in the original video or	It does not provide a detailed analysis of the security and robustness of the proposed method against various attacks

S. No.	Ref. No.	Techniques	Results	Advantage	Limitation
			the video here is better as compared to other method	fingerprint. This makes it possible to use video watermarking techniques for secure fingerprint transmission	
5	[95]	DCT, DWT	PSNR value of the watermarked video comes out to be as high as almost up to 37 dB with the optimal watermarking strength. Therefore, the scheme is proved to be strong aligned with high efficiency video coding (HEVC) compression	Robust against various video processing attacks and HEVC compression	The article did not provide a comprehensive analysis of the impact of watermarking on the quality of the video
6	[96]	DWT	The size of watermark-8 x 8 and PSNR- 42.3011 & MSE-5.9673 and when the size-256 x 256 then, PSNR-39.0142 & MSE-7.8432. Thus, it showed that if watermark was small, the PSNR of watermarked frame became large, which was highly accepted	Resist common video processing operations such as frame dropping, frame averaging, and compression	Algorithm may not be able to resist more advanced video processing techniques or attacks
7	[97]	Logistic map encryption, SVD	The imperceptibility was acceptable as PSNR came greater than 40 dB. Proposed scheme proved to be robust against various image and video processing attacks and also showed superior of our scheme	It maintains good visual quality of the watermarked video	Computational complexity is one of the major issues in this scheme and moreover, it may not be applied on real-time applications
8	[98]	Change Detection Algorithm	Output showed that the eminence of the video object was elevated and the value of PSNR comes out to be 55.888 dB was calculated for 1K HD video, the method given here showed the better robustness results when the watermark object was inserted in a low frequency sub-band	Detect tampering in video inter-frame using watermarking which can be useful in ensuring the authenticity of video data	It does not provide a comparison with other tampering detection methods, so it is unclear how the proposed method performs
9	[99]	Canny Edge Detection	Results suggested that a proper region could be selected for watermarking and problem related to duplicity and synchronization in the watermark detection had been addressed by employing SURF. The study also furnished the means which can help the digital content to keep safe from unlawful replication	Robust against common attacks such as noise addition, cropping, and geometric distortions.	It is not tested on a large dataset and the effectiveness of the method may vary depending on the type of video content being watermarked
10	[100]	DWT and Encryption	The experiment was done on 20 videos captured using six cameras (4 consumer cameras and two mobile phones) and the method showed a reliable technique in digital video authentication based on local video information which gave good results, the overall classification accuracy of the method came 96.77	It uses statistical local information to detect tampering and manipulations in videos, which can be more effective than traditional cryptographic techniques	It may not be able to detect very subtle changes in the video, and it may be computationally expensive to process large video files
11	[101]	DCT, DWT, DFT	The results came out to be- With 2D DCT-51.7371.	It can effectively embed the	Robustness against common video

S. No.	Ref. No.	Techniques	Results	Advantage	Limitation
			With DFT, - 31.0055 With, 2D DWT-56.3632. After applying the spatial as well as compression attacks on the watermarked video. Accordingly, the method using wavelet transform was considered as the best and effective as per the values shown	watermark in the chrominance model of the video which helps to maintain the visual quality of the video	processing operations such as compression, filtering, and scaling is not thoroughly evaluated
12	[102]	DCT	The method consists of indexing solar panels, matching the coordinate with global positioning system (GPS) to area's index, capturing video and data from solar farm, dividing captured video to frames (30 frames/s) and watermarking each panel frames by their related data.	This scheme facilitates access to solar panel frames and their related data using a graphic user interface	Computational complexity is high and cannot withstand attacks
13	[103]	DWT and DCT	A set of 15 videos had been used. The proportions 1:8, 1:4, 1:2, 1: 1, 2: 1, 4:1 and 8: 1 were considered of the constituent transforms for generating the HWT. Results showed that the MSE between original and retrieved watermark is minimum for HWT generated using Kekre and Haar constituent transforms. It gave better results as compared to other hybrid wavelet transforms(HWT)	Use of multiple transforms in the watermarking process can improve the robustness of the watermark against various attacks	Use of multiple transforms can also increase the computational complexity of the watermarking process, which may not be suitable for real-time applications
14	[104]	DWT and Spread Spectrum Technique, LSB modification method	In the execution of this algorithm, 20 frames out of 100 have been selected which depends upon the entropy factor and then the watermark was inserted in a specific frame after selection. As per the results, 288 frame number exhibited highest entropy with corr-0.9956 and SSIM-0.9747 value and the 202 frame number had lowest entropy value with corr-0.9024 and SSIM-0.8948	It provides a high level of security to online social network contents	The technique may have limitations in terms of computational complexity and scalability, especially for large-scale social networks
15	[105]	DWT	NC value is 1 for all the objects, showed the maximum revival of the watermark images. The PSNR value came between 33 to 41 dB which showed that the given scheme maintains the visual eminence as well as the obscurity of the watermark object	The process can improve the robustness of the watermark against various attacks	It may not be suitable for real-time applications
16	[106]	DWT	Robustness after applying rotation by 0.5° at LLLL is computed by NC=0.8513 (high) and NC= 0.38208 (low) at HH. Another attack applied is adding Gaussian noise, where SNR value comes out to be 23 with NC=0.8293 and NC=0.9853 Finally, cropping first 10 columns, the value came out to	Explores the effect of barrel distortion on watermarking techniques and proposes a method to overcome this issue in the field of digital watermarking	It does not evaluate the effectiveness of the proposed method on other types of distortions or attacks

S. No.	Ref. No.	Techniques	Results	Advantage	Limitation
			be NC=0.7715 and NC=0.7253		
17	[107]	DWT, SVD, Arnold Transform(AT)	The result showed the PSNR value as 55.0885 and 68.0292. Thus, the problem proved to give high imperceptibility. The better result of robustness was achieved by NCC value as 0.6021. Finally, the good rate of data payload was given as (N-number of motion frames)/24 images for N frame video. Encryption is also used to improve the level of security in the method	It offers high robustness against common signal processing attacks such as frame averaging, frame dropping, frame insertion, and frame swapping	It does not provide a comprehensive analysis of the performance of the proposed scheme under various attacks or the embedding capacity
18	[108]	DCT	It achieves good results in terms of imperceptibility, robustness, and security.	It is computationally efficient and does not significantly affect the quality of the video	The video frames are not compressed or transformed before being embedded with the watermark. This may limit the applicability of the scheme to certain types of videos
19	[109]	Deep neural networks (DNNs) and curriculum learning to enhance the robustness of the watermark	It outperforms some of the existing watermarking techniques in terms of robustness and security	DNNs and curriculum learning enables the scheme to learn a nonlinear mapping that is more robust than traditional watermarking technique	It may require a large amount of training data to achieve optimal results
20	[110]	A non-sampled contourlet transform (NSCT), pseudo 3D-DCT, and non-negative matrix factorization (NMF)	This scheme is tested on different video types and is shown to be robust against noise, compression, filtering, and geometric distortion	The use of NSCT, pseudo 3D-DCT, and NMF enables the scheme to extract more image features and enhance the robustness of the watermark	It may be computationally intensive, requiring significant resources to embed the watermark into large video datasets
21	[111]	An optimal key-frame selection method based on the improved gravitational search algorithm (IGSA) in the lapped wavelet transform domain.	It maintains high quality video, making it suitable for applications where lossless watermarking is required, such as in medical imaging and military applications	It is lossless, meaning that the video quality is not degraded after the watermark is embedded	The scheme may be computationally intensive due to the use of the IGSA, which may limit its practicality for real-time applications
22	[112]	A zero-watermarking algorithm for audio and video matching based on the NSCT	It maintains high audio and video quality, making it suitable for applications where zero-watermarking is required, such as in copyright protection and digital rights management	It can achieve synchronization between the audio and video signals	The use of the hash value as the watermark may limit the watermark capacity
23	[113]	The watermark embedding and extraction are performed using a temporal codes based approach	Visible watermarking feature provides additional security for digital videos by discouraging unauthorized use.	It provides both visible and imperceptible watermarking in one framework, which increases the level of copyright protection for digital videos	The extraction of frames in a video, which may increase the computational complexity of the technique, especially for longer videos
24	[114]	An efficient video watermarking algorithm based on convolutional neural networks (CNNs) with an entropy-based information	The algorithm was evaluated using the peak signal-to-noise ratio (PSNR) and the structural similarity index (SSIM), which demonstrated that the proposed	The use of CNNs in the encoding process also allows for better resistance to various attacks such as	It requires a large amount of computation power and memory to train the CNNs

S. No.	Ref. No.	Techniques	Results	Advantage	Limitation
		mapper	method provides high-quality watermarked videos while maintaining robustness against various attacks	compression, filtering, and geometric distortion	
25	[115]	The technique used is a combination of two watermarking approaches, one for visual frames and another for audio signals, which are embedded into the original video	The results show that the proposed technique achieved high accuracy in detecting fake COVID-19 videos, with an average accuracy of 97.5% and a false-positive rate of 1.3%	The advantage of this approach is that it can effectively detect and prevent the spread of fake COVID-19 videos, which have become a major issue during the pandemic	The limitation is that the proposed technique may not be effective against advanced video manipulation techniques such as deepfakes

4.3Analysis based on platforms or related tools/ datasets available

There are several online datasets available for implementing video watermarking on MATLAB R2018a. One of the popular datasets is the Uncompressed colour image database (UCID) dataset, which contains over 1300 images of various categories such as animals, nature, and people. This dataset can be used to test the performance of video watermarking techniques in the SD. Another popular dataset is the BOSSbase dataset, which contains 10,000 images of various categories such as textures, faces, and landscapes. This dataset can be used to test the performance of video watermarking techniques in the FD. There are also datasets specifically designed for video watermarking, such as the TRECVID dataset, which contains video clips of various categories such as news, sports, and entertainment. This dataset can be used to test the performance of video watermarking techniques in real-world scenarios. MATLAB R2018a provides various tools for implementing video watermarking techniques. For example, the Image Processing Toolbox can be used for image pre-processing and feature extraction, while the Communications Toolbox can be used for implementing the watermarking algorithm and evaluating its performance.

The said method will be assessed by considering the performance metrics and the dataset from the standardised websites [53, 54]. In the dataset, we will use some standard definition (SDD) as well as HD colour videos to implement the technique. For example- “rhinos.avi” is an SD video with three hundred sample frames. The size of each frame is approximately 320x240 pixels. Similarly, “tractor.avi” is HD video with the sample of around three hundred frames of the size 1920x1080 pixels. These videos will be used to embed an (watermark) at a particular location and the impact of several attacks will be scrutinized.

4.4Benefits and open challenges while designing an algorithm

The rapid development of digital information technology drastically transformed the general public. Currently multimedia objects can easily be created, manipulated and stored by digital data owner worldwide due to the availability of wide variety of multimedia tools [108, 109]. In addition, explosion in the development of high internet bandwidth easily transfer multimedia documents from one system to other remote system within reasonable time irrespective of the geographical location. However, these benefits have brought a major alarming issues and number of challenges that requires being determined listed below [110–114]. The research on video watermarking has addressed some challenges related to the protection of intellectual property rights in digital multimedia. However, there are still several challenges that researchers in this field face. Some of the current challenges inspired by this research include:

1) Robustness: One of the biggest challenges in video watermarking is making the watermark robust to attacks such as compression, filtering, and cropping. Attackers may attempt to remove or alter the watermark, making it difficult to identify the rightful owner of the digital media. Researchers are working on developing watermarking techniques that are more robust to these attacks.
2) Scalability: Another challenge is developing watermarking techniques that are scalable to different resolutions, frame rates, and bitrates of the video. This is important because videos can be encoded and decoded at different resolutions and frame rates, and the watermarking technique should be able to adapt to these variations.
3) Complexity: Some watermarking techniques can be computationally expensive, especially when dealing with high-resolution videos. Researchers are working on developing watermarking

techniques that are more efficient and can be applied in real-time.

4) Evaluation: Evaluating the effectiveness of watermarking techniques can be challenging. It is difficult to simulate all possible attack scenarios and test the robustness of the watermarking technique. Researchers are working on developing standardized evaluation metrics and benchmarks to enable fair comparison of different watermarking techniques.
5) Security: The security of the watermarking technique is also a challenge. If an attacker is able to extract the watermark from the video, they may be able to use it to create unauthorized copies or modify the video. Researchers are working on developing watermarking techniques that are more secure and difficult to extract.

The studies based on video watermarking has inspired several challenges related to the development of more robust, scalable, efficient, and secure watermarking techniques. Addressing these challenges will enable the protection of intellectual property rights in digital multimedia and contribute to the development of more secure and reliable multimedia systems.

As earlier discussed, digital watermarking is the probable solution to resolve these issues. DVW is still a comparatively less investigated area then image watermarking. One of the main reasons is video possessing additional high complexity and distinguishes features then image for which powerful, robust watermarking techniques and other solutions are available. In contrast to image watermarking, video watermarking research still consist many additional issues like changing frame rate, increase in bit-rate, temporal synchronization and frame based attack. The motivation towards this research is to obtain the innovative solution to protect the copyright issue for video sequences in a robust and imperceptible manner. The major attention is to have a unique image representing copyright information embedding in a video material that can later be easily extracted the supplementary information use to claim for the copyright of the concern video. Since the video consisting voluminous data therefore the video contents must be requiring to compress before storing or transfer via internet in order to minimize the storage requirements and to support the real-time requirements[115–117].

In view of this, this overview on video watermarking not only focused on non-compressed domain but also implemented the video watermarking schemes based on compressed domain. Ultimately, the major focus is to secure the video multimedia material through digital watermarking technology by analysing their applications and requirements as some challenges still required being solved. The objective is to design an innovative scheme in video watermarking technology with a qualitative study of watermarking in uncompressed and compressed domain both.

5.Discussion

This paper is started from the scratch of information security issue and techniques for multimedia objects. The scheme of DVW is identified as the lone best way for securing such objects. In continuation with it, the deep study of state of art under uncompressed and compressed domain based DVW is reviewed and concluded that motion frame based and MPEG-2 based techniques are perhaps more suitable for a given application and requirement. Generally, data is generated, stored, and dispersed digitally.

Currently, media and magazines have gone through online for providing real-time coverage of stories with maximum quality audio, fixed pictures, and video series. The progress in the use of publically available networks like the internet has considered the online availability of publishers by providing a fast and cheap way to broadcast its work. The fast growth of digital media is restricted to news administrations. Hence, music can be downloaded and purchased through the internet, standard photography sellers digitalize and the pictures in electric and digital versatile schemes provide movies vibrant pictures. Generally, newspapers and mass media digitally stored the data and susceptible through various modes.

Firstly, digital mass media may be duplicated legally or illegally at less cost without data loss. Moreover, processors permit mass media to be modified so that it is probable to integrate parts of digital indications into their owner’s work without copyright constraints.

The water marking approach is based on finding the optimal bit-pattern to make sure the embedding process will provide high quality, less data loss, secure authentication, etc. It is based on the optimization process which finds the right bits on behalf of bit thresholds and fitness, and then generates the optimal embedding sequence for outcome.

The systematic review conducted on video watermarking techniques has provided valuable insights into the current state-of-the-art in this field. However, there are certain limitations of the study that need to be acknowledged. The search was restricted to a limited number of databases, which may have resulted in the exclusion of some relevant studies.

Additionally, the review only focused on video watermarking techniques and did not consider other forms of digital watermarking, such as audio and image watermarking. Apart from these limitations, the review has highlighted several important findings and challenges in the field of video watermarking.

One of the major challenges faced by researchers is the need to develop robust and imperceptible watermarking techniques. Imperceptibility is essential to ensure that the watermarked video maintains its quality and does not affect the user experience. However, the watermark must also be robust enough to withstand various types of attacks, such as compression, cropping, and filtering.

Another challenge is the need to develop watermarking techniques that are resistant to collusion attacks. Collusion attacks involve multiple attackers working together to remove the watermark from the video. Such attacks are particularly challenging to defend against, as they require the watermark to be spread over multiple frames of the video. Furthermore, there is a need to develop watermarking techniques that are adaptive to the content of the video. Different types of videos have different characteristics, such as motion, texture, and color. Therefore, a watermarking technique that works well for one type of video may not work as effectively for another type of video.

Lastly, there is a need to develop evaluation metrics that accurately measure the performance of video watermarking techniques. Currently, most evaluation metrics, such as PSNR and SSIM, only measure the visual quality of the watermarked video and do not take into account the robustness of the watermark. In conclusion, while the review has provided valuable insights into the current state-of-the-art in video watermarking, there are still several challenges that need to be addressed. Future research in this field should focus on developing robust and imperceptible watermarking techniques that are adaptive to the content of the video and resistant to collusion attacks. Also, there is a need to develop evaluation metrics that accurately measure the performance of these techniques. Additionally, there are few more limitations which are given as below-

Limited Scope: The review may be limited to certain types of watermarking techniques or may only cover a specific time period, which may not fully capture the current state of the field.

Biased Literature Search: The search strategy may be biased towards certain databases or keywords, leading to a potential exclusion of relevant studies.

Heterogeneity of Studies: The included studies may have varying methods, designs, and data, which can make it difficult to compare and synthesize the results.

Publication Bias: The review may only include published studies, which may result in the exclusion of important unpublished or gray literature.

Quality Assessment: The quality of the included studies may vary, which can affect the validity and reliability of the review findings. It is important for researchers to acknowledge these limitations and provide clear justifications for their methodology and selection criteria in order to ensure transparency and rigor in their systematic review and meta-analysis. Analysis of the systematic review are shown in *Figure 10.*

A complete list of abbreviations is shown in *Appendix I.*

6.Conclusion and future scope

The overall outcome of this paper provides a significant understanding and broader scope of the area for researchers pursuing their research work in the said field. The approaches discussed above achieve a high-efficiency rate and less frame-dropping ratio. The bit selection module of the methods offers a better selection of the bits to embed and makes the video watermarking process more secure. It also works for color-based watermarking, providing security and imperceptibility. For upcoming researchers, the watermarking process could be implemented to test diverse security attacks like composite attacks, collusion attacks, and ambiguity attacks, which have not been completely explored to prove efficiency and robustness. Moreover, maintaining the equilibrium between the three major trade-offs, i.e., robustness, imperceptibility, and capacity, always remains a

challenge. Another significant challenge of DVW is maintaining the quality at the time of watermark retrieval, which can be achieved by considering various other characteristics of the watermarked object.

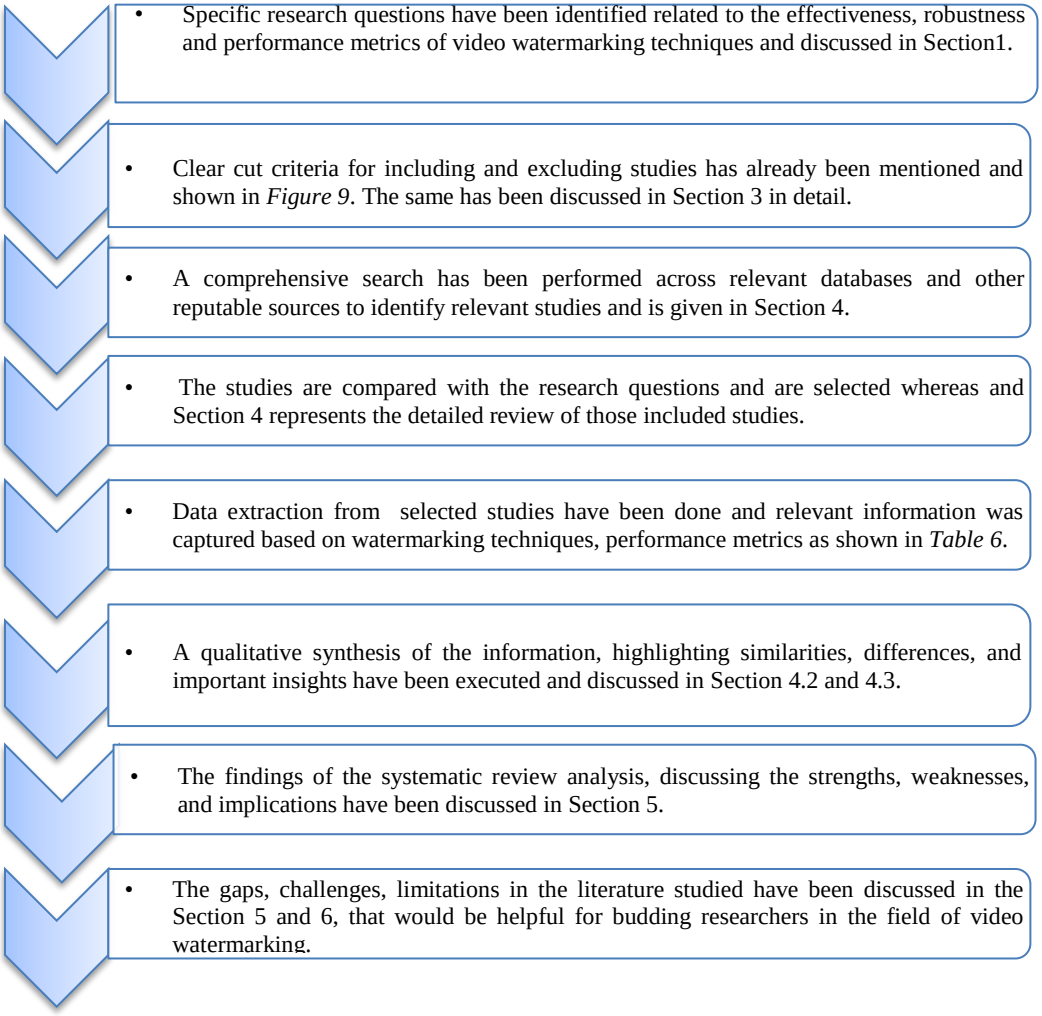

Figure 10 Analysis of the systematic review

The given systematic review on video watermarking techniques highlights the current state-of-the-art in the field and identifies several important challenges that need to be addressed. The review demonstrates that video watermarking techniques have numerous applications, including copyright protection, authentication, and TD. It also identifies several popular video watermarking techniques, such as DCT-based and DWT-based techniques, and evaluates their performance using various metrics. The review shows that the choice of technique and parameters can significantly affect the performance of the watermarking technique. Despite the progress made in video watermarking, several challenges still need to be addressed, including developing robust and imperceptible watermarking techniques, resistance to collusion attacks, and adaptability to the video content. Additionally, there is a need to develop evaluation metrics that accurately measure the performance of video watermarking techniques.

Future work in this field should focus on addressing these challenges and developing new and improved watermarking techniques. This could involve exploring new techniques, such as deep learning-based watermarking, and evaluating their performance on large-scale datasets. Additionally, research could focus on developing techniques that

are adaptive to different types of videos and can handle various types of attacks. Overall, the results of this review provide a useful guide for researchers and practitioners working in the field of video watermarking, helping to inform the development of new and improved techniques for protecting the integrity of digital video content.

Acknowledgment
None.

Conflicts of interest
The authors have no conflicts of interest to declare.

Author's contribution statement
Purnima: Conceptualization, writing-original draft, writing – review and editing. **Rakesh Ahuja:** Study conception, supervision, investigation on challenges. **Nidhi Gautam:** Design, supervision, draft manuscript preparation.

References
[1] Cox I, Miller M, Bloom J, Fridrich J, Kalker T. Digital watermarking and steganography. Morgan Kaufmann; 2007.
[2] Cox I, Miller M, Bloom J, Honsinger C. Digital watermarking. Journal of Electronic Imaging. 2002; 11(3).
[3] Petitcolas FA, Anderson RJ, Kuhn MG. Information hiding-a survey. Proceedings of the IEEE. 1999; 87(7):1062-78.
[4] Lin EI, Eskicioglu AM, Lagendijk RL, Delp EJ. Advances in digital video content protection. Proceedings of the IEEE. 2005; 93(1):171-83.
[5] Anusree K, Binu GS. Biometric privacy using visual cryptography, halftoning and watermarking for multiple secrets. In national conference on communication, signal processing and networking 2014 (pp. 1-5). IEEE.
[6] Gupta P. Cryptography based digital image watermarking algorithm to increase security of watermark data. International Journal of Scientific & Engineering Research. 2012; 3(9):1-4.
[7] Asikuzzaman M, Pickering MR. An overview of digital video watermarking. IEEE Transactions on Circuits and Systems for Video Technology. 2017; 28(9):2131-53.
[8] Singh AK, Kumar B, Dave M, Ghrera SP, Mohan A. Digital image watermarking: techniques and emerging applications. Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security. 2016: 246-72.
[9] Cayre F, Fontaine C, Furon T. Watermarking security part two: practice. In security, steganography, and watermarking of multimedia contents VII 2005 (pp. 758-68). SPIE.
[10] Jensen-link LA, Thompson C. Effective video capture techniques for educational multimedia. In proceedings frontiers in education 25th annual conference, engineering education for the 21st century 1995 (pp. 30-3). IEEE.
[11] Sen J, Sen AM, Hemachandran K. An algorithm for digital watermarking of still images for copyright protection. Indian Journal of Computer Science and Engineering. 2012; 3(1):46-52.
[12] Channalli S, Jadhav A. Steganography an art of hiding data. arXiv preprint arXiv:0912.2319. 2009.
[13] Deshpande N, Rajurkar A, Manthalkar R. Review of robust video watermarking algorithms. arXiv preprint arXiv:1004.1770. 2010.
[14] Singh S, Singh AK, Ghrera SP. A recent survey on data hiding techniques. In international conference on IoT in social, mobile, analytics and cloud 2017 (pp. 882-6). IEEE.
[15] Sunesh HK. Watermark attacks and applications in watermarking. In national workshop-cum-conference on recent trends in mathematics and computing 2011:8-10.
[16] Chang X, Wang W, Zhao J, Zhang L. A survey of digital video watermarking. In seventh international conference on natural computation 2011 (pp. 61-5). IEEE.
[17] Lee SJ, Jung SH. A survey of watermarking techniques applied to multimedia. In international symposium on industrial electronics proceedings (Cat. No. 01TH8570) 2001 (pp. 272-7). IEEE.
[18] Sharma C, Bagga A, Singh BK, Shabaz M. A novel optimized graph-based transform watermarking technique to address security issues in real-time application. Mathematical Problems in Engineering. 2021; 2021:1-27.
[19] Asikuzzaman M, Alam MJ, Lambert AJ, Pickering MR. Imperceptible and robust blind video watermarking using chrominance embedding: a set of approaches in the DT CWT domain. IEEE Transactions on Information Forensics and Security. 2014; 9(9):1502-11.
[20] Ahuja R, Bedi SS. Video watermarking scheme based on IDR frames using MPEG-2 structure. International Journal of Information and Computer Security. 2019; 11(6):585-603.
[21] Cox IJ, Miller ML, Bloom JA. Watermarking applications and their properties. In proceedings international conference on information technology: coding and computing (Cat. No. PR00540) 2000 (pp. 6-10). IEEE.
[22] Doerr G, Dugelay JL. A guide tour of video watermarking. Signal Processing: Image Communication. 2003; 18(4):263-82.
[23] Singh AK, Dave M, Mohan A. Wavelet based image watermarking: futuristic concepts in information security. Proceedings of the National Academy of Sciences, India section A: physical sciences. 2014; 84:345-59.
[24] Cox IJ, Miller ML. Review of watermarking and the importance of perceptual modeling. In human vision and electronic imaging II 1997 (pp. 92-9). SPIE.

[25] Kaur M, Jindal S, Behal S. A study of digital image watermarking. Journal of Research in Engineering and Applied Sciences. 2012; 2(2):126-36.
[26] Moniruzzaman M, Hawlader MA, Hossain MF. Wavelet based watermarking approach of hiding patient information in medical image for medical image authentication. In international conference on computer and information technology 2014 (pp. 374-8). IEEE.
[27] Bakhtiari S, Ibrahim S, Salleh M, Bakhtiari M. JPEG mage encryption with elliptic curve cryptography. In international symposium on biometrics and security technologies 2014 (pp. 144-9). IEEE.
[28] Ouslim M, Sabri A, Mouhadjer H. Securing biometric data by combining watermarking and cryptography. In 2nd international conference on advances in biomedical engineering 2013 (pp. 179-82). IEEE.
[29] Han Y, He W, Ji S, Luo Q. A digital watermarking algorithm of color image based on visual cryptography and discrete cosine transform. In ninth international conference on P2P, parallel, grid, cloud and internet computing 2014 (pp. 525-30). IEEE.
[30] Ghosh S, De S, Maity SP, Rahaman H. A novel dual purpose spatial domain algorithm for digital image watermarking and cryptography using extended hamming code. In 2nd international conference on electrical information and communication technologies 2015 (pp. 167-72). IEEE.
[31] Kumar S, Dutta A. A novel spatial domain technique for digital image watermarking using block entropy. In international conference on recent trends in information technology 2016 (pp. 1-4). IEEE.
[32] Shahid M, Kumar P. Digital video watermarking: issues and challenges. International Journal of Advanced Research in Computer Engineering & Technology. 2018; 7(4):400-5.
[33] Hartung F, Kutter M. Multimedia watermarking techniques. Proceedings of the IEEE. 1999; 87(7):1079-107.
[34] Seenivasagam DV, Subbulakshmi S, Radhamani S. A survey on video watermarking and its applications. International Journal of Advanced Research in Computer Science and Software Engineering. 2014; 4(3):3015-8.
[35] Singh P, Chadha RS. A survey of digital watermarking techniques, applications and attacks. International Journal of Engineering and Innovative Technology. 2013; 2(9):165-75.
[36] Bhattacharya S, Chattopadhyay T, Pal A. A survey on different video watermarking techniques and comparative analysis with reference to H. 264/AVC. In international symposium on consumer electronics 2006 (pp. 1-6). IEEE.
[37] Mane GV, Chiddarwar GG. Review paper on video watermarking techniques. International Journal of Scientific and Research Publications. 2013; 3(4):1-5.
[38] Panchal H, Acharya K, Panchal P, Thakar N. Digital watermarking on extracted key frames from uncompressed color video using 4-level DWT. In international conference on emerging trends in networks and computer communications 2011 (pp. 331-5). IEEE.
[39] Varaprasad SA, Srinivas P, Vidya T, kumara CA. LSB modification, correlation, transform based digital image watermarking techniques. International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering. 2015; 3(12):136-9.
[40] Wang Y, Ostermann J, Zhang Y. Video formation, perception, and representation. Signal Processing, Prentice Hall. 2001.
[41] Comesana P, Pérez-freire L, Pérez-gonzález F. Fundamentals of data hiding security and their application to spread-spectrum analysis. In international workshop on information hiding 2005 (pp. 146-60). Berlin, Heidelberg: Springer Berlin Heidelberg.
[42] Bas P, Cayre F. Achieving subspace or key security for WOA using natural or circular watermarking. In proceedings of the 8th workshop on multimedia and security 2006 (pp. 80-8).
[43] Cayre F, Fontaine C, Furon T. Watermarking security part one: theory. In security, steganography, and watermarking of multimedia contents VII 2005 (pp. 746-57). SPIE.
[44] Cayre F, Fontaine C, Furon T. Watermarking security: theory and practice. IEEE Transactions on Signal Processing. 2005; 53(10):3976-87.
[45] Hartung FH, Su JK, Girod B. Spread spectrum watermarking: malicious attacks and counterattacks. In security and watermarking of multimedia contents 1999 (pp. 147-58). SPIE.
[46] Holliman MJ, Macy WW, Yeung MM. Robust frame-dependent video watermarking. In security and watermarking of multimedia contents II 2000 (pp. 186-97). SPIE.
[47] Ahuja R, Bedi SS. Video watermarking scheme based on candidates I-frames for copyright protection. Indonesian Journal of Electrical Engineering and Computer Science. 2017; 5(2):391-400.
[48] Ahuja R, Bedi SS. Robust video watermarking scheme based on intra-coding process in MPEG-2 Style. International Journal of Electrical & Computer Engineering. 2017; 7(6):3332-43.
[49] Harish NJ, Kumar BB, Kusagur A. Hybrid robust watermarking techniques based on DWT, DCT, and SVD. International Journal of Advanced Electrical and Electronics Engineering. 2013; 2(5):137-43.
[50] Sridhar B, Arun C. Secure video watermarking algorithm based on wavelet with multiple watermarks. Latin American Applied Research. 2015; 45(3):207-12.
[51] Zhang X. Reversible data hiding in encrypted image. IEEE Signal Processing Letters. 2011; 18(4):255-8.
[52] Biswas SN, Nahar S, Das SR, Petriu EM, Assaf MH, Groza V. MPEG-2 digital video watermarking technique. In international instrumentation and measurement technology conference proceedings 2012 (pp. 225-9). IEEE.

[53] Yu X, Wang C, Zhou X. A survey on robust video watermarking algorithms for copyright protection. Applied Sciences. 2018; 8(10):1-26.
[54] Kaur P, Laxmi DV. Review on different video watermarking techniques. International Journal of Computer Science and Mobile Computing. 2014; 3(9):190-5.
[55] Mohal D, Sharma S. Image encryption strategies to enhance security of image: an exhaustive analysis. International Journal of Advanced Research in Computer Science. 2017; 8(9):351-61.
[56] Jadhav A, Kolhekar M. Digital watermarking in video for copyright protection. In international conference on electronic systems, signal processing and computing technologies 2014 (pp. 140-4). IEEE.
[57] Mohanty SP, Kougianos E. Real-time perceptual watermarking architectures for video broadcasting. Journal of Systems and Software. 2011; 84(5):724-38.
[58] Langelaar GC, Setyawan I, Lagendijk RL. Watermarking digital image and video data. a state-of-the-art overview. IEEE Signal Processing Magazine. 2000; 17(5):20-46.
[59] Podilchuk CI, Delp EJ. Digital watermarking: algorithms and applications. IEEE Signal Processing Magazine. 2001; 18(4):33-46.
[60] Leelavathy N, Prasad EV, Kumar SS. Video watermarking techniques: a review. International Journal of Computer Applications. 2014; 104(7):24-30.
[61] Zhang Y. Digital watermarking technology: a review. In ETP international conference on future computer and communication 2009 (pp. 250-2). IEEE.
[62] Jayamalar T, Radha V. Survey on digital video watermarking techniques and attacks on watermarks. International Journal of Engineering Science and Technology. 2010; 2(12):6963-7.
[63] Paul RT. Review of robust video watermarking techniques. IJCA Special Issue on Computational Science. 2011; 3:90-5.
[64] Shoemaker C. Hidden bits: a survey of techniques for digital watermarking. Independent Study, EER. 2002; 290:1673-87.
[65] Chan PW, Lyu MR, Chin RT. A novel scheme for hybrid digital video watermarking: approach, evaluation and experimentation. IEEE Transactions on Circuits and Systems for Video Technology. 2005; 15(12):1638-49.
[66] Hazim HT, Alseelawi N, Alrikabi HT. A novel method of invisible video watermarking based on index mapping and hybrid DWT-DCT. International Journal of Online & Biomedical Engineering. 2023; 19(4):155-73.
[67] Liu S, Bo-wei CD, Gong L, Ji W, Seo S. A real-time video watermarking algorithm for authentication of small-business wireless surveillance networks. International Journal of Distributed Sensor Networks. 2015; 11(9):1-11.
[68] Singh N, Joshi S, Birla S. Cover dependent watermarking against ambiguity attacks. Procedia Computer Science. 2020; 171:1137-46.
[69] Doërr G, Dugelay JL. Collusion issue in video watermarking. In security, steganography, and watermarking of multimedia contents VII 2005 (pp. 685-96). SPIE.
[70] Doërr G, Dugelay JL. Security pitfalls of frame-by-frame approaches to video watermarking. IEEE Transactions on Signal Processing. 2004; 52(10):2955-64.
[71] Lei B, Song I, Rahman SA. Robust and secure watermarking scheme for breath sound. Journal of Systems and Software. 2013; 86(6):1638-49.
[72] Agrawal P, Khurshid A. DWT and GA-PSO based novel watermarking for videos using audio watermark. In advances in swarm intelligence: 5th international conference, ICSI 2014, Hefei, China, proceedings, Part II 5 2014 (pp. 212-20). Springer International Publishing.
[73] Guo J, Zheng P, Huang J. Secure watermarking scheme against watermark attacks in the encrypted domain. Journal of Visual Communication and Image Representation. 2015; 30:125-35.
[74] Arab F, Abdullah SM, Hashim SZ, Manaf AA, Zamani M. A robust video watermarking technique for the tamper detection of surveillance systems. Multimedia Tools and Applications. 2016; 75:10855-85.
[75] Han J, Zhao X, Qiu C. A digital image watermarking method based on host image analysis and genetic algorithm. Journal of Ambient Intelligence and Humanized Computing. 2016; 7:37-45.
[76] Sridhar B, Arun C. An enhanced approach in video watermarking with multiple watermarks using wavelet. Journal of Communications Technology and Electronics. 2016; 61:165-75.
[77] Kumar GD, Teja DP, Reddy SS, Sasikaladevi N. An efficient watermarking technique for biometric images. Procedia Computer Science. 2017; 115:423-30.
[78] Shukla D, Sharma M. A novel scene-based video watermarking scheme for copyright protection. Journal of Intelligent Systems. 2018; 27(1):47-66.
[79] Yoo G, Kim H. Real-time video watermarking techniques robust against re-encoding. Journal of Real-Time Image Processing. 2017; 13:467-77.
[80] Himeur Y, Boukabou A. A robust and secure key-frames based video watermarking system using chaotic encryption. Multimedia Tools and Applications. 2018; 77:8603-27.
[81] Zear A, Singh AK, Kumar P. A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimedia Tools and Applications. 2018; 77:4863-82.
[82] Shukla D, Sharma M. Robust scene-based digital video watermarking scheme using level-3 DWT: approach, evaluation, and experimentation. Radioelectronics and Communications Systems. 2018; 61:1-12.
[83] Nouioua I, Amardjia N, Belilita S. A novel blind and robust video watermarking technique in fast motion

frames based on SVD and MR-SVD. Security and Communication Networks. 2018; 2018:1-7.
[84] Arab F, Zamani M, Poger S, Manigault C, Yu S. A framework to evaluate the performance of video watermarking techniques. In 2nd international conference on information and computer technologies 2019 (pp. 114-7). IEEE.
[85] Singh R, Singh S, Sharma N. A review of digital watermarking technique. International Journal of Computer Applications. 2015:1-6.
[86] Mohanarathinam A, Kamalraj S, Prasanna VGK, Ravi RV, Manikandababu CS. Digital watermarking techniques for image security: a review. Journal of Ambient Intelligence and Humanized Computing. 2020; 11:3221-9.
[87] Nadesh RK, Arivuselvan K, Aishwarya K. A hybrid Approach for video watermarking using DWT and SVD. In innovations in power and advanced computing technologies 2019 (pp. 1-6). IEEE.
[88] Alotaibi SS. Optimization insisted watermarking model: hybrid firefly and Jaya algorithm for video copyright protection. Soft Computing. 2020; 24(19):14809-23.
[89] Sharma C, Amandeep B, Sobti R, Lohani TK, Shabaz M. A secured frame selection based video watermarking technique to address quality loss of data: combining graph based transform, singular valued decomposition, and hyperchaotic encryption. Application-Aware Multimedia Security Techniques. 2021; 2021:1-19.
[90] Agarwal H, Husain F. Development of payload capacity enhanced robust video watermarking scheme based on symmetry of circle using lifting wavelet transform and SURF. Journal of Information Security and Applications. 2021; 59:102846.
[91] Neena PM, Narayanan SA, Bijlani K. Copyright protection for E-learning videos using digital watermarking. In fifth international conference on advances in computing and communications 2015 (pp. 447-50). IEEE.
[92] Singh AK, Kumar B, Singh SK, Ghrera SP, Mohan A. Multiple watermarking technique for securing online social network contents using back propagation neural network. Future Generation Computer Systems. 2018; 86:926-39.
[93] Panyavaraporn J, Horkaew P. DWT/DCT-based invisible digital watermarking scheme for video stream. In 10th international conference on knowledge and smart technology 2018 (pp. 154-7). IEEE.
[94] Kumar NU, Sandhya G, Bachu S. Security of finger prints with video watermarking techniques based on DWT and SVD. In IOP conference series: materials science and engineering 2021 (pp. 1-8). IOP Publishing.
[95] Li J, Liu H, Huang J, Shi YQ. Reference index-based H. 264 video watermarking scheme. ACM Transactions on Multimedia Computing, Communications, and Applications. 2012; 8(2S):1-22.
[96] Keerthana P, Nikita E, Lakkshmi R, Devi RS. Tampering detection in video inter-frame using watermarking. International Journal of Research in Engineering, Science and Management. 2019; 2(3):251-4.
[97] Rao R. Video watermarking algorithm using the SVD transform. International Journal of Engineering Research and Development. 2013; 8(11):1-8.
[98] Isac B, Santhi V. A study on digital image and video watermarking schemes using neural networks. International Journal of Computer Applications. 2011; 12(9):1-6.
[99] Bahrami Z, Akhlaghian TF. A new robust video watermarking algorithm based on SURF features and block classification. Multimedia Tools and Applications. 2018; 77:327-45.
[100] Al-athamneh M, Kurugollu F, Crookes D, Farid M. Video authentication based on statistical local information. In proceedings of the 9th international conference on utility and cloud computing 2016 (pp. 388-91). ACM.
[101] Velickovic ZS, Milivojevic ZN, Velickovic MZ. A secured digital video watermarking in chrominance model. In international scientific-professional conference on information technology 2018 (pp. 1-4). IEEE
[102] Lafkih S, Zaz Y. Digital video watermarking for solar panel indexation and monitoring. In 3rd international renewable and sustainable energy conference 2015 (pp. 1-5). IEEE.
[103] Kulkarni TS, Dewan JH. Digital video watermarking using hybrid wavelet transform with Cosine, Haar, Kekre, Walsh, Slant and Sine transforms. In international conference on computing communication control and automation 2016 (pp. 1-5). IEEE.
[104] Dhevanandhini G, Yamuna G. An efficient lossless video watermarking extraction process with multiple watermarks using artificial jellyfish algorithm. Turkish Journal of Computer and Mathematics Education. 2021; 12(6):3048-55.
[105] Patel SV, Yadav AR. Invisible digital video watermarking using 4 level DWT. In national conference on recent trends in engineering & technology 2011 (pp. 1-6).
[106] Verma Y, Singh M. Implementation the effects of barrel distortion in field of digital video watermarking. International Journal of Science, Engineering and Technology Research. 2017; 6(6):2278-7798.
[107] Shanmugam M, Chokkalingam A. Performance analysis of 2 level DWT-SVD based non blind and blind video watermarking using range conversion method. Microsystem Technologies. 2018; 24:4757-65.
[108] Al-gindy A, Omar AA, Mashal O, Shaker Y, Alhogaraty E, Moussa S. A new watermarking scheme for digital videos using DCT. Open Computer Science. 2022; 12(1):248-59.
[109] Ke Z, Huang H, Liang Y, Ding Y, Cheng X, Wu Q. Robust video watermarking based on deep neural network and curriculum learning. In international conference on e-business engineering 2022 (pp. 80-5). IEEE.

[110]Fan D, Zhang X, Kang W, Zhao H, Lv Y. Video watermarking algorithm based on NSCT, pseudo 3D-DCT and NMF. Sensors. 2022; 22(13):1-18.
[111]Singh R, Mittal H, Pal R. Optimal keyframe selection-based lossless video-watermarking technique using IGSA in LWT domain for copyright protection. Complex & Intelligent Systems. 2022; 8(2):1047-70.
[112]Fan D, Sun W, Zhao H, Kang W, Lv C. Audio and video matching zero-watermarking algorithm based on NSCT. Complexity. 2022; 2022:1-14.
[113]Velazquez-garcia L, Cedillo-hernandez A, Cedillo-hernandez M, Nakano-miyatake M, Perez-meana H. Imperceptible–visible watermarking for copyright protection of digital videos based on temporal codes. Signal Processing: Image Communication. 2022; 102:116593.
[114]Bistroń M, Piotrowski Z. Efficient video watermarking algorithm based on convolutional neural networks with entropy-based information mapper. Entropy. 2023; 25(2):1-26.
[115]Tarhouni N, Masmoudi S, Charfeddine M, Amar CB. Fake COVID-19 videos detector based on frames and audio watermarking. Multimedia Systems. 2023; 29(1):361-75.
[116]Ali J, Ghrera SP. A secure method of copyright protection for digital videos using split watermark embedding algorithm. In fourth international conference on image information processing 2017 (pp. 1-5). IEEE.
[117]Ram B. Digital image watermarking technique using discrete wavelet transform and discrete cosine transform. SSRN. 2013: 1-7.

Ms. Purnima is a Research Scholar at the Department of CSE, Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab. She holds a BSc (CS) degree from Panjab University, Chandigarh, an MCA degree from Kurukshetra University, Haryana, and an MPhil (CS) degree from Periyar University, Salem, Tamilnadu. With more than 12 years of teaching experience, she has established herself as an experienced educator. Her research interests encompass various areas, including Cyber Security, Image Processing, Multimedia Security, Digital Video Watermarking, Digital Right Management, Pattern Recognition, and Information Hiding. Currently, she is actively working in the field of Copyright Protection and Ownership Authentication in Digital Video Watermarking using Machine Learning.
Email: purnima.arvind@gmail.com

Dr. Rakesh Ahuja holds a PhD degree in the field of Computer Science & Engineering. He has 25 years of experience in Academic, Research, Administration and Industries. Currently, he serves as a Professor in the CSE department at Chitkara University, Punjab, India. His research area primarily focuses on Digital Right Management, Multimedia Security, Pattern Recognition, and Information Hiding. Dr. Ahuja is particularly interested in the development of schemes related to Cryptography, Information and Multimedia Security, including Text, Video, and Image Watermarking, and Database Management System. Furthermore, he is actively engaged in solving problems in the healthcare sector through the application of machine learning and deep learning technologies.
Email: rakesh.ahuja@chitkara.edu.in

Dr. Nidhi Gautam is currently serving as an Assistant Professor of Computer Science at the University Institute of Applied Management Sciences, Panjab University, Chandigarh since 2008. She holds B.Tech, M.Tech, and a PhD in the field of Computer Science and Engineering. Alongside her academic role, she teaches in the sectoral MBA programs specializing in IT and Telecommunications. With more than 16 years of teaching and research experience in Computer Science, she has made significant contributions to the field. Dr. Gautam has previously taught at UIET, Panjab University Chandigarh, LPU Jalandhar, and CIIS, handling International Programmes as well. She actively participates in various committees at the University level and currently holds the additional responsibility of a Hostel Warden. Moreover, she has an impressive publication record, with over 30 papers published in various Conferences and Journals of International repute. Additionally, she has served as an editor for a book.
Email: nidhi.uiams@pu.ac.in

Appendix I

S. No.	Abbreviation	Description
1	2D	Two-Dimensional
2	3D	Three-Dimensional
3	AF	Actual Frame
4	AT	Arnold Transform
5	ATK	Arnold Transform Key
6	BER	Bit Error Rate
7	BPS	Bit Plane Slicing
8	BPNN	Back Propagation Neural Network
9	BR	Bit Rate
10	CAR	Confidentiality, Availability and Reliability
11	CE	Chaotic Encryption
12	CI	Cover Image
13	CNNs	Convolutional Neural Networks
14	Cov	Covariance Matrix
15	DBNs	Deep Belief Networks

16	DCT	Discrete Cosine Transform
17	DFT	Discrete Fourier Transform
18	DNNs	Deep Neural Networks
19	DVD	Digital Video Disc
20	DVW	Digital Video Watermarking
21	DWT	Discrete Wavelet Transform
22	E	Eigen Value
23	ETD	Effective Tamper Detection
24	FC	Frame Collusion
25	FD	Frequency Domain
26	FFT	Fast Fourier Transform
27	FT	Framelet Transform
28	GA	Genetic Algorithm
29	GA-PSO	Genetic Algorithm-Particle Swarm Optimization
30	GDSD	Gradient Degree Similarity Deviation
31	GPS	Global Positioning System
32	HCS	Homomorphic Cryptosystem
33	HD	High Definition
34	HECC	Hamming Error Correction Code
35	HEVC	High Efficiency Video Coding
36	HI	Host Image
37	HNs	Hidden Neurons
38	HP	Human Perception
39	HVS	Human Visual System
40	HWT	Hybrid Wavelet Transform
41	IA	Image Authentication
42	IGSA	Improved Gravitational Search Algorithm
43	LSB	Least Significant Bit
44	LWT	Lifting Wavelet Transform
45	LH	Low, High
46	MPEG-2	Moving Picture Experts Group-2
47	MPEG-4	Moving Picture Experts Group-4
48	MSE	Mean Square Error
49	NCC	Normalized Correlation Coefficient
50	NMF	Non-negative Matrix Factorization
51	NSCT	Non-Sampled Contourlet Transform
52	PCA	Principal Component Analysis
53	PSNR	Peak-to-Signal-Noise-Ratio
54	PVRs	Personal Video Recorders
55	RGB	Red Green Blue
56	SBD	Shot Boundary Detection
57	SCD	Scene Change Detector
58	SD	Spatial Domain
59	SDD	Standard Definition
60	SI	Similarity Index
61	SSIM	Structural Similarity Index
62	SURF	Speeded-Up-Robust-Features
63	SVD	Singular Vector Decomposition
64	TD	Tamper Detection
65	TU-FS	Trial Based on Jaya- Firefly
66	WI	Watermarked Image
67	WF	Watermarked Frame
68	TV	Television
69	UCID	Uncompressed Colour Image Database
70	V	Eigen Vector
71	VS	Video Stream
72	WMV	Windows Media Video