

# All Aspects of Digital Video Watermarking Under an Umbrella

**Rakesh Ahuja**

Moradabad Institute of Technology, Moradabad, India  
 Email: [ahuja2305@rediffmail.com](mailto:ahuja2305@rediffmail.com)

**S. S. Bedi**

Institute of Engineering & Technology, MJP Rohilkhand University, Bareilly, India  
 Email: [dearbedi@gmail.com](mailto:dearbedi@gmail.com)

**Abstract**—The present review covers the video watermarking literature published from 1997 to the year 2015. Through extensive work, some selection is necessary. Therefore, only articles published by a process of peer review in archival journal are reviewed. Papers are grouped according to the implementation techniques and further divided into sub techniques. Many papers deal with fundamental of digital video watermarking, including experimental, numerical and analytical works. Others are related to application or natural system. In addition to reviewing journal articles, this review also takes papers of good conferences and meeting on video watermarking. The main aim of authors is to provide every details regarding digital video watermarking under an umbrella. In other words all aspects of video watermarking are placed together in order to helpful to those readers looking the complete literature related to video watermarking scheme.

**Index Terms**—Spatial domain, frequency domain, video watermarking.

## I. INTRODUCTION

This review is completely different from those of previous reviews because of focusing on only those papers that are related to digital video watermarking schemes. It covers implementation techniques use by the researchers, various books written on digital video watermarking and paper published by well known publishers of international journals like IEEE and ELSEVIER as well as some papers from other reputed open access journal that is publically available. All research papers have been divided into the number of groups and each group containing only those papers that deal with the same techniques. Each group is elaborated in a detailed manner and at the end of each group; a brief summary is mentioned to cover major parts of their working. Finally this review concludes with some existing challenges to implement the digital video watermarking in frequency domain and in spatial domain. At last but not least it illustrates the future trends and limitations. As in the previous years, significant attempt

has been devoted to research in traditional application such as in entertainment industries, video conferencing, broadcast monitoring, fingerprinting, video authentication, copyright protection, copy control etc. In addition to that, a huge number of papers deal with topics that are at the frontiers of both fundamental research and important promising application, such as steganography, data hiding techniques, and cryptography techniques to secure the digital contents especially for video. The proposed review covered all papers including their application area. The following Tables 1 is an index which shows the major points will be covered for describing the digital video watermarking. The next subsequent Table 2 covers the full details of books written on information hiding, steganography & digital watermarking.

Table 1. Index

I.	Introduction
II.	The Principle of Digital Video Watermarking
III.	Design issues of Digital Video Watermarking scheme
IV.	Applications of Digital Video Watermarking Scheme
V.	Robustness Evaluation Parameters
VI	Classification of Digital Watermarking
VII	Implementation Techniques of Video Watermarking
VII A.	Spatial Domain Schemes
i	Least Significant Bit (LSB)
ii	Spread Spectrum (SS)
VII B	Exploiting Frequency Decomposition Schemes
i	Singular Value Decomposition (SVD)
ii	Principal Component Analysis (PCA)
iii	Discrete Cosine Transform (DCT)
iv	Discrete Wavelet Transform (DWT)
v	Hybrid Approach
VIII	Conclusions
IX	Future Scope of Digital Video Watermarking
	References

Table 2. Books on Information Hiding, Steganography & Digital Watermarking

Title	Authors	Publisher / WebSite Link	Edition / Volume & Year of Publication
Privacy Protection and Computer Forensics	Michale A. Caloyannides	Artech House, INC., 685 Canton Street, Norwood, MA 02062	2 <sup>nd</sup> Edition, 2004
Digital Watermarking and Steganography	Ingemer C.Cox, Mattew L. Miller, Jeffery A. Bloom, Jessica Fridrich, Tom Kalker	Morgan Kaufan Publisher http://www.mkp.com	2 <sup>nd</sup> Edition, 2007
Information Hiding and Applications	Jeng-Shyang Pan, Hsiang-Cheh Huang and Lakhmi C. Jain	Springer-Verlag Berlin Heidelberg	Vol- 227,2009
Information Hiding Techniques for Steganography and Digital Watermarking	Stefan Katzenbeisser, Fabien A. P. Petitcolas	Artech House, INC., 685 Canton Street, Norwood MA 02062, Boston, London	2000
Multimedia Encryption & Watermarking	Borko Furht, Edin Muharemagic, Daniel Socek	Springer Science Business Media, INC	Vol -28 , 2005
Techniques and Application of Digital Watermarking and Content Protection	Michael Arnold , Martin Schmucker, Stephen D. Wolthusen	Artech House, INC., 685 Canton Street, MA 02062, Boston, London	2003
Fundamental of Multimedia	Ze -Nian Li, Mark S. Drew	Pearson Prentice Hall, Pearson Education, INC USA	2004

II. THE PRINCIPLE OF DIGITAL VIDEO WATERMARKING

This section covers a formal prologue to watermarking systems and the terms used in this background for their presentation. The principle of any digital video watermarking is described by two major following process.

A. Embedding Process

This part includes that what type of algorithm must be applied to embed the watermark. Generally, it depend not only on the type of video either it is original or compressed but also depends on whether the embedded watermark should be visible or non-visible. The selection of watermark is also a major concern and It depend on the application for which the system is deploying like if the application is copyright protection, owner information as watermark is being selected. If the application is developed for fingerprinting; then customer information as watermark must be inserting likewise for other application also. The embedding process is illustrated by a tuple (V, W, K, V<sub>w</sub>) Where V is the original video, W is the gathering of all watermark and K is the collection of all keys and v<sub>w</sub> is the watermarked video (see figure 1).

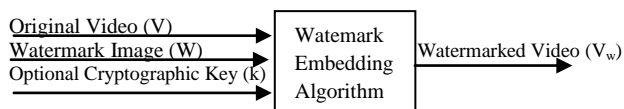


Fig.1. Generic Watermarking Embedding Process

B. Extraction Process

The watermark is extracted from the watermarked video in order to proof the copyright of the concern multimedia data or to fulfill the purpose for which the application was developed (see figure 2). The extraction of watermark is demonstrated by a tuple (Vw, V, K, W,

WE). These input parameters vary accordance with the types of watermarking systems. The extracted watermark We differs from the embedded watermark W due to possible manipulations of watermarked content (V<sub>w</sub>).

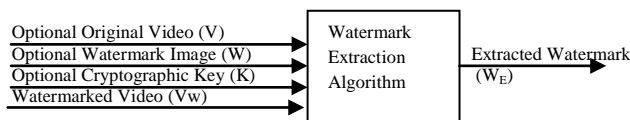


Fig.2. Generic Watermark Extraction Process

III. DESIGN ISSUES OF DIGITAL VIDEO WATERMARKING SCHEME

To design digital video watermarking, numbers of following parameters are essentially required. One challenging aspect is that there is always a tradeoff among Robustness, imperceptibility and payload capacity i.e. all these parameters cannot be evaluated simultaneously in an efficient manner.

A. Robustness

The information embedded into the host signal must be withstand even common signal processing attack i.e. the watermark must be extracted above some threshold value even the watermarked video is little distorted intentionally or non-intentionally. And the extracted watermark will be used to proof for copyright protection. Analytically robustness is evaluated by the following equation 1.

$$CC = \frac{\sum_i \sum_j W_{ij} * W'_{ij}}{\sqrt{\sum_i \sum_j (W_{ij})^2} \sqrt{\sum_i \sum_j (W'_{ij})^2}} \quad (1)$$

Where  $W_{ij}$  is the original watermark coefficient value at the  $i^{\text{th}}$  row and  $j^{\text{th}}$  column and  $W'_{ij}$  is the coefficient value of extracted watermark at  $i^{\text{th}}$  row and  $j^{\text{th}}$  column. Correlation Coefficient (CC) value must lie between 0 to 1.

### B. Perceptibility

It is defined mathematically by Peak Signal to Noise Ratio (PSNR) which is used as a benchmark to evaluate the perceptual metrics for video quality. The perceptibility factor shows that the quality of watermarked video must not be degraded from the threshold value after embedding the watermark. Principally, it seems that the original video and watermarked video must be identical at execution time. It is demonstrated as follows:

$$\text{PSNR} = \frac{10 \log_{10} 255^2}{\text{MSE}} \quad (2)$$

Where MSE is defined as mean square error and it is evaluated as:

$$\text{MSE} = \frac{1}{m * n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (f(i, j) - f'(i, j)) \quad (3)$$

$m$ :- The height of the video frame

$n$ :- The width of the video frame

$f(i, j)$ :- Original Video Frame

$f'(i, j)$ :- Watermarked Video Frame

### C. Capacity

It defines that how much amount of information can be embedded into the huge amount of video data and it must be large adequate to uniquely identify the copyright information embedded in it.

### D. Security

The embedded information must be secure by using any cryptographic technique. It solely depends on the key of choice from the large key space. The security of embedded information is required so that the unauthorized user cannot alter, manipulate or even detach it from the watermarked video.

### E. Application based Design Issue

Another most important design issue is to choose that which type of watermarking should be design. It must depend upon type of application for which the watermarking system is being developed. It can be understood by broadly classified in two following categories.

#### i. Non blind Video watermarking System

This system refers that at least one original data ((original video or original watermark or both) is required during the detection or extraction of watermark. The system will be designed for those applications where

ownership protection or copyright information is extracted to prove the ownership of original cover. Therefore it is referred to as *private video watermarking*. It is further classified in two categories. Type-1: it is used to serve two purposes. Not only detecting the watermark but also extracts the watermark from the watermarked video by using the original video signal. Type-2: it is used to detect only the presence of the watermark exist or not.

#### ii. Blind Video Watermarking System

This watermarking system neither requires original video nor original watermark to extract the watermark from the watermarked video. It is the most challenge watermarking in today's scenario. It is referred to as public video watermarking.

## IV. APPLICATIONS OF DIGITAL VIDEO WATERMARKING SCHEMES

The following section described the various applications in context with digital video watermarking. This is not an entire list but many more can be possible. All these applications collected together are shown in the Table 3.

Table 3. Digital Video Watermarking Applications and Related Function

Application	Function
Broadcast Monitoring	To monitor & verify the broadcasted video content
Video Authentication	To ensure the content of video has not been amended
Copyright Protection	Any time owner information as watermark could be extracted
Copy Control	To prevent creating multiple illegal copies
Fingerprinting	Tracing the wicked client responsible for creating multiple illegitimate copies

#### A. Broadcast Monitoring

Video signals are supervised in order to verify the content being broadcast due to sometimes some of the TV stations overbooked the air time for advertisement. There are number of solutions to rectify the problem. One of the way-out is to assign a human who observe the system and record it manually but it is very cost effective and also not trustworthy. Hence another way is to computerize the system that simulate the human behavior and monitor the content being transmit. This approach is known as *passive monitoring*. Since it compare the received data to the already stored signal into the database. Therefore comparing each time a video signals from a huge database is not considering practical. On the other hand a different mechanism must be adopted also known as *active monitoring*. In this system some identification signals represent the copyright information as watermark is being embedded into the video signal. These identification signals will be extracted from the host signal in order to verify & check the content being broadcast. In this way watermarking play a very vital role

in broadcast monitoring. Saraju P. Mohanty et al. [1] best simulated the real time digital video watermarking combined with VLSI architecture in order to embed broadcaster's logo information in real time environment.

### B. Video Authentication

The concept of video authentication arises due to the fast distribution of transfer of video data through the internet and this increases the possibility of tempering the video contents when it is in transit state. Hence the video authentication techniques must ensure that the contents of video could not be altered by any malicious user. This is provided by two methods. First efforts done by the researchers are to use the cryptographic method. But this approach has a major limitation of complete verification i.e. the received data must be exactly same as sent by the source. This is tough constraint. It doesn't necessary that the received data is changed intentionally by cruel user. It may be allowed to changed up to some acceptable limit and this may be possible like noise addition typically in the case of wireless connection or some part of the video may be cut down by sensor. Therefore the content has changed but it must be allowed to pass for authentication test. In view of all these issues, another authentication technique is being adopted by researchers known as watermark information i.e. the embedding of authentication information into the video contents itself. In this way the video authentication information is added in an incremental way into each video frame so that any amendment to the sequence of video frames can easily be observed. This methodology is very effective, less complicated and simple for detecting temporal changes of the video data. But, it may fail when there is an alteration in the contents itself. To rectify this problem, both audio and video watermarking jointly embedded. [2, 3, 4, 5, 6] exploit very effectively video authentication scheme by using digital video watermarking technology.

### C. Copyright Protection

In the era of internet, huge amount of video data is being transferred from one system to another. Since there is no difference between the original and replicated copy, so after receiving the copy of video, any unauthorized person may claim the owner of the received data. To rectify this problem, a watermark must consist information about the owner, is embedded into the host signal itself. Whenever any false claim is being done by unauthorized person, the owner of the content as watermark can be extracted from the host signal in order to prove the copyright. A very large number of researchers are working on this issue for more than last two decades and still it is the challenging domain with respect to achieving high level of robustness. The same is described in detail in section 8.

### D. Copy Control

Digital watermarking can also be used for controlling the creating of illegal duplicate copy of the original source of data. A Copy protection Technical Working Group (CPTWG) is created to handle copy protection

issue. A number of techniques like 'The Content Scrambling Methods', 'The Analog Protection System', 'The Copy generation Management System' and last but not least is 'Watermarking' method is briefly described by [7].

### E. Fingerprinting

This application is useful to track the customer who illegally distributes the digital video in the market. Because of this, a large amount of royalties was being lost by the copyright owner. Thanks again to the invention of watermarking system which can easily trace those distributor who creates multiple copies of the original video in an illegal way. This can easily been done by embedding the distributor information as watermark into the host signal itself. When an illegal copy is found then the watermark information is extracted from the host and can easily be traced the guilty distributor, therefore, a court case can be file against him. Video-on-Demand is one of the real time applications of digital video watermarking where a policy of fingerprinting is enforced to add in it.

## V. ROBUSTNESS EVALUATION PARAMETERS

Any manipulation on watermarked video may affect the robustness and it can be defined as - The watermark from the host data must be extracted successfully even though the watermarked video is intentionally or non-intentionally tempered by malicious or authenticated users respectively. The ultimate aim of attacker is to remove or change the watermark information from the host signal in order to destroy the aim for which the application was developed. The attacks directly affect on the robustness of any digital video watermarking system. Therefore any watermarking system is incomplete if there is no consideration of robustness evaluation parameters. The attacks measuring parameters are broadly categories into two major parts are as follows:

### A. Frame Specific Attacks

Since video is considered as a collection of a sequence of still images. Therefore this category includes all those attacks that can be applying on images can also be applying on video. The attacks in this category are listed below:

#### i. Geometric Attacks

This includes three attacks: First is *rotation attack*; this type of attack attempt to rotate every frame by some degree in order to distort the extracted watermark. Second is *scaling attack*; In this attack, every frame is multiplied by some value. Third is *cropping attack*: it is very common type of attack is very common to apply. In which, a small number of columns (like 5 out of 500) replaces by the values to '0' in place of actual grey scale value representing the image column values in order to reducing the strength of watermark.

#### ii. Removal Attacks

In this category of attack, attacker tries to remove the watermark from the host video content. The best example is collusion attacks where different versions of the same image or video frames are collected to produce a new image, reducing the strength of a watermark. Collusion attack is further divide in two categories: Collusion Type 1; this category includes that the same watermark is embedded into the different videos. The attacker estimate the watermark from each watermarked video and then apply the subtract operation in order to get unwatermarked data. And Type 2 includes that the different watermarks are embedded into multiple copies of same data. Again, the colluder takes the average of the combination of different watermarked data to produce the un-watermarked data.

### iii. Ambiguity Attacks

In this way, attacker creates its own watermark with equal payload capacity as of original watermark and added into the host signal to fool the original owner for claiming that he is the owner of that video signals.

### iv. Compression Attacks

Since most of the huge multimedia data is distributed through the internet. To save the bandwidth, storage requirements and time, this data is transferred in compressed form which may also collapse the watermark embedded into the multimedia data. To escape from this unintentional attack, it is preferred that the watermark must be inserted at the compression time.

### v. Noise Attacks

Image processing techniques are used to add or remove

noises in order to represent the signals in more presentable form or to distort the original signal depending upon the application. The noises may be Salt & pepper Noise, Gaussian Noise, Median Filter and Histogram Equalization. Many researchers evaluated the robustness by applying noise attack.

### B. Video Specific Attacks

These attacks are additional to image processing attacks and they are only applicable to video stream data: This category includes two types of attacks: *friendly and Non-friendly attacks*. All friendly attacks never aim to destroy the embedded watermark intentionally like *frame insertion* attack; for example, suppose some commercial break is to insert into the video. Since watermarked video has change unintentionally due to newly inserted frame, therefore the watermark may be collapse. Another attack is *frame deletion* attacks; this may require when sensor cut down some shots or scene due to some bad message pass to the society i.e. technically frames deletion requires from the original video which may also unintentionally alter or destroy the watermark. Another category is *non-friendly attacks*: *Frame averaging* is one of them; it is supposed to replace the frame with the averaging of all neighboring frames. For example, 10<sup>th</sup> frame can be replace with the (9<sup>th</sup> frame+10<sup>th</sup> frame+11<sup>th</sup> frame)/3. On the other hand, one more non-friendly attack is *frame swapping*; for example 10<sup>th</sup> and 11<sup>th</sup> frame can be interchange, which may also harm the watermark embedded into the video bit stream. A special attention towards video specific attacks must be taken while designing the video watermarking.

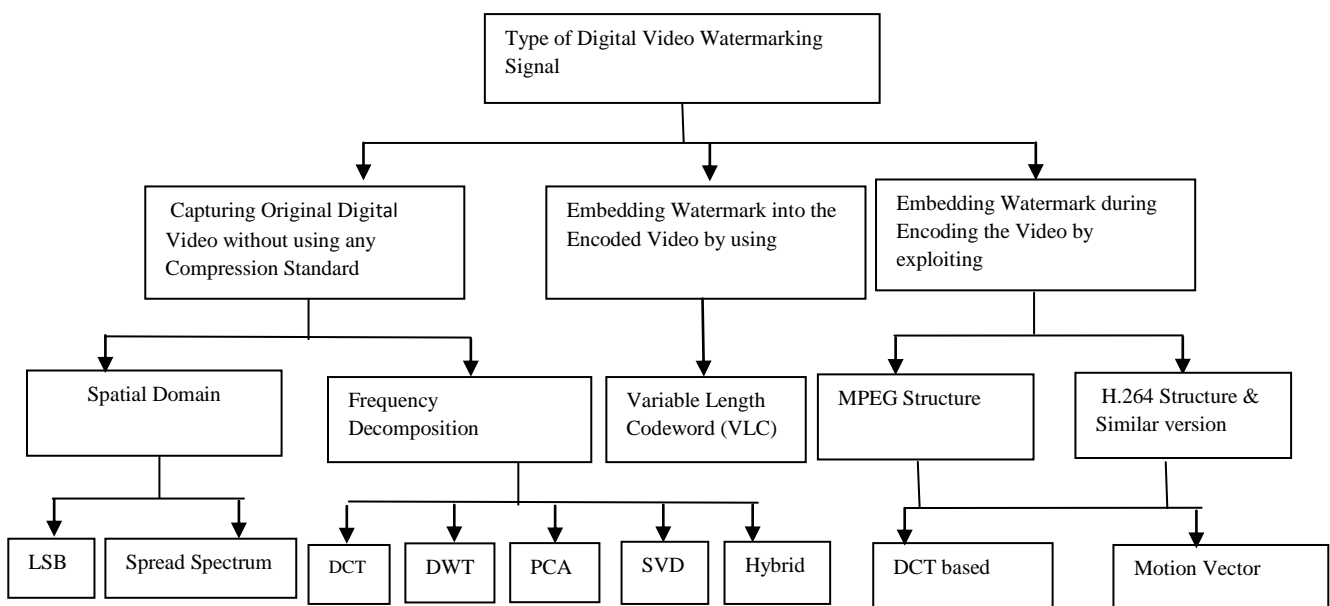


Fig.3. Classification of Digital Video Watermarking Scheme

## VI. CLASSIFICATION OF DIGITAL VIDEO WATERMARKING

There are number of ways to classify the digital video watermarking methodology such as according to working domain, according to human perception, according to application and so on. Here, the categorization is entirely based on 2 factors. First issue is based on what type of video signal can be used and second is based on what watermarking methods can be possible with that video signal as shown in figure 3. In this way all researcher papers are grouped and further sub-grouped according to type of video signal use for watermarking. First category of video watermarking includes those research papers that deal with pure original video without using any consideration of compression standard. Second group consist of those research papers in which watermark are embedded during encoding the video. Third category take account of papers in which compressed video is use to watermark the video. The classification is being mentioned in Fig. 3 This review elaborates only those papers where video is considered in uncompressed original form.

## VII. IMPLEMENTATION TECHNIQUES OF DIGITAL VIDEO WATERMARKING

Considering that the video is a collection of sequence of still images, therefore all the methods, schemes and algorithms were use to embed the watermark for motionless images will be adapted by researchers for video also. Two methods are very common in image watermarking named as ‘Spatial Domain’ and ‘Transformation techniques’ use by the following researchers for video watermarking also. First considering those papers where investigator worked on spatial domain then include those methods based on transformation techniques.

### A. *Spatial Domain Scheme*

In the spatial domain, watermark bits are directly replaced into the pixels of one or two arbitrarily selected part of a frame and are updated based on perceptual analysis of video frames. Embedding the watermark by spatial domain scheme is broadly classified in two categories as follows:

#### i. *Least Significant Bit (LSB)*

A simplest way is to replace the least bit of each selected pixels of an image or video, represented by 8 bits, with the watermark bits. Priya Porwal et al. [8] converted the encrypted watermark into the binary form to be placed into the LSB position of selected position of pixels of each frame. Their experimental result shows that the watermark is extracted successfully. But they did not evaluated the other required parameters like perceptibility and robustness.

#### ii. *Spread Spectrum (SS)*

Another scheme for embedding the watermark is to spread the watermark in the following fashion. In this scheme, message as watermark (W) is encoded to generate a noise like sequence and this sequence is added to the original host data i.e. video or video clips. Since no mathematical transformations are applied therefore such scheme is computationally more efficient as compared to other transformation scheme described in the next section. Following researchers uses the spread spectrum based technique for digital video watermarking.

Mercy George et al.[9] described the spatial domain based blind video watermarking images and video. They use the simple technique i.e. the DCT watermark coefficients of watermark image are added to the A DCT coefficients of the image excluding the dc coefficient. They also claimed that the same techniques can be use for I frame of video data. Their simulation result shows the imperceptibility and robustness by applying the JPEG compression attacks, low pass filtering, rotation attacks, cropping attack and printing and rescanning attacks. There is one major limitation as claim by the author is that the collusion attack could hit in destroying if the sufficient quantities of differently watermark copies are obtainable to the attackers.

Karen Su et al.[10] described the video watermarking by considering the problem of frame collusion, a very serious issue in video watermarking. They have proposed two watermarking techniques for handling collusion attacks named as spatially localized and image dependent sub framing respectively. Their simulation results tested Type-1 collusion attack as well as Type-2 collusion attack to estimate the watermark. As they claim that in both projected scheme, the best estimate of the watermark is acquired when only one frame is used in the judgment method.

Houmansadr et al. [11] described the video watermarking based on visual cryptograph is performed in the spatial domain and there experimental result shows that it is robust to collusion resistant attack. Their embedding and extraction process passes through various robustness challenges like covering the geometric attacks, pirate attack such as frame swapping, frame deletion and collusion attack, the major hot issue in video watermarking.

Luo Wei et al. [12] also described the digital video watermarking based on spread spectrum technique. This method modulated each watermark bit through a pseudo-random expansive sequence and embeds them in a large number of luminance DCT DC coefficients on I frame. Although they have shown the watermarked video but neither calculated PSNR mathematically nor evaluated robustness by applying the video specific attacks.

Radu et al. [13] described the watermarking method based on spread spectrum technique while asserting that their scheme is robust against three types of attacks is as temporal, spatial and compression attacks. Their experimental results are categorized in two parts. First part includes the extraction of watermark without any attack and second part includes the robustness results after applying the 7 attacks. The specialty of this research

is that it was supported by UEFISCSU, 2011, D.N. Vizireanu.

Radu Ovidiu Preda [14] described the digital video watermarking based on spatial as well as wavelet domain. As far as the spatial domain is concern, they use the spread spectrum technique to spread the watermark data as copyright information, into the video bit stream. They evaluated the robustness by evaluating the NC by applying the attacks: blurring of 2 x 2 pixels blocks, brightening, adding of Gaussian noise with mean 0 and variance 0.0003, median filter using a 3 x 3 pixel neighborhood, addition of 'salt & pepper' noise with density 0.3%, frame averaging of 20% of the frames, JPEG compression of every frame with Q=60 and MPEG compression.

Generally the spatial domain is easy to implement and low computational complexity as compared to frequency domain scheme. But it is less robust to watermarking attacks since watermark bits directly inserted into the host signal that can easily be changed or remove to distort the watermark. For example, all LSB's can be randomly reshuffled by an attacker in order to completely destroying the watermark. Therefore most of the researcher shifted to frequency transforms domain technique to implement the digital video watermarking. The number of researchers takes advantage of transform domain approach described in detail in the next subsequent section. The summarize work of researcher's work by using spatial domain is described in Table 4.

Table 4. Summary of Video Watermarking based on Spatial Domain Technique

Paper	Application	Robustness Evaluation
[8]	#	\$
[9]	Tracing Illegal copy	JPEG compression, Low pass filtering, Rotation, printing and rescanning.
[10]	Copyright Protection	Type 1 & Type 2 Linear Collusion Attack
[11]	Ownership protection	Cropping, Rotation, Scaling, MPEG Compression for different quality factor, Collusion Attack
[12]	Copyright Protection	\$
[13]	Copyright Protection	Gaussian, Median, Salt & Pepper, Fr. Averaging, JPEG 80, MPEG 2- 2Mbps, MPEG2- 4 Mbps.
[14]	Copyright Protection	Blurring of 2 x 2 pixels blocks, brightening, adding of Gaussian noise with mean 0 and variance 0.0003, median filter using a 3 x 3 pixel neighborhood, addition of 'salt & pepper' noise with density 0.3%, frame averaging of 20% of the frames, JPEG compression of every frame with Q=60 and MPEG compression.

# Did not clearly mentioned the application areas

\$ Did not evaluated the robustness parameters

### B. Exploiting Frequency Decomposition Schemes

In the *frequency transform* domain, first, we have to understand, what is frequency transform and then why there is a need of it? The answer to the first question is-

Mathematical transformations are applied to raw video signals to obtain further information from that signal that is not readily available in the raw signal. Now, the answer to the second question is- Watermark will be embedding only after converting the raw video into another form to produce more robust and imperceptible watermarked video. There are numbers of transformation are applied as follows: Discrete Fourier transform, discrete wavelet transform [15, 16, 17] discrete cosine transform and many more, described below.

#### iii. Singular Value Decomposition (SVD)

SVD is one of the most useful tools of linear algebra with several applications in image compression, and other signal processing field. It is also widely used in image as well as in video watermarking. Singular Value Decomposition is an orthogonal process, based on a theorem from linear algebra which says that a rectangular matrix A can be broken down into the product of three matrices - an orthogonal matrix U, a diagonal matrix S, and the transpose of an orthogonal matrix V. The singular values are placed at the diagonal position of the matrix and these values are generated by calculating the square roots of the Eigen values of the cross-product matrix. The theorem is usually work as shown in the equation 4.

$$A_{MN} = U_{MM} S_{MN} V_{NN}^T \quad (4)$$

where M and N are the number of rows and columns of matrix A, respectively. The columns of U are orthonormal eigenvectors of  $AA^T$  i.e. the product of A and  $A^T$  is the unitary matrix 'U' likewise the columns of V are orthonormal eigenvectors of  $A^T A$  i.e. the product of  $A^T$  and A is the unitary matrix 'V'. Finally, S is a diagonal matrix containing the square roots of Eigen values from U or V in descending order i.e. the singular values are placed at the diagonal of the matrix A and are arranged in decreasing order. The luminance of image is specified by every singular value of the matrix  $S_{MN}$ .

In *SVD based watermarking*, a video frame is treated as a matrix decomposed by SVD into the three matrices; U, S, and  $V^T$ . Mostly SVD-based watermarking algorithms add the watermark information to the singular values  $\sigma_i$  of the diagonal matrix S to meet the imperceptibility and robustness requirements. A very fewer number of researchers uses only SVD techniques for video watermarking. Instead researchers use heavily the SVD with other transformation techniques described in the consequent section to grip the robustness. Lama Rajab is few of them who described two video watermarking algorithms by using SVD technique only in the same paper is as follows. The summary details of all researchers worked on SVD domain are described in Table 5.

Lama Rajab et. al. [18] proposed two video watermarking algorithms and both the algorithms are based on the algebraic transform of Singular Value Decomposition (SVD). In the first algorithms, watermark bit information are embedded in all three matrix i.e.

matrix U, S, and V of luminance component(Y) of each frame. In the second algorithm, watermark bits are embedded in a block of matrix U as well as in the matrix V. The performances of these two algorithms are evaluated with respect to robustness and payload. The diagonal-wise based first algorithm achieved better robustness results, while the block-wise algorithms obtained higher data payload rate. The robustness of the first algorithm is checked against four attacks. The very first attack is JPEG *compression attack*, which obtained better result when watermark is embedded in the S matrix as compare to embedding in U and V matrix respectively. They provides better robustness when watermark is extracted from the first algorithm, diagonal wise in the V-matrix compared to S or U matrices for different angles against video *angular rotation type of attack*. Two types of noises (Gaussian and Salt and pepper Noise) are also added in embedded watermark video to check the robustness of watermark scheme and here the better results are obtained in V and U matrices both as compare to diagonal matrix S. Another category of attack is *frame dropping*: again, they obtained better correlation value when extracting the watermark in S matrix after dropping 60% of the frames as compared to U and V matrices. Likewise they also evaluate the robustness against frame swapping and frame averaging. They also evaluated the robustness experiments of the second algorithm. And the results are almost similar as comparison to the first algorithm. The advantage of implementing second algorithm is that the payload capacity is much higher than the first algorithms. Since two algorithms are fulfilling two separate properties of watermark. Hence both the techniques are having their own advantages. But, the only flaw is that both the algorithms have not evaluated the perceptibility of watermarked video.

Tomas kanocz [19] et al. described the digital video watermarking based on SVD. They calculated the perceptibility and robustness by applying some well known attacks as compression; frame averaging and frame resize and frame rotation on six standard videos. The title of this paper is 'Real-time digital video watermarking based on SVD'. But it is sorry to say that the author has not covered any explanation or shown any research work related to real-time. Real time video watermarking is totally a different issue as compared to normal video watermarking.

#### ❖ Applications of Singular Value Decomposition

- SVD can be used to approximate a matrix by one of low rank.
- It can be used to solve the linear equation.
- It is exploiting in signal processing i.e. to filter noise from the signal.
- This technique can be utilized to compress the image or video frame data.
- This technique is being utilized also in digital image or digital video watermarking.

#### ❖ Drawback of Singular Value Decomposition

- Solving problems by SVD may be computationally

expensive as compared to work out by Fourier transform.

- It operate on fix size matrix hence it is not suited for adaptive type of algorithms.

It is not practically suited well while using only SVD based technique for video watermarking. Therefore the researchers using SVD with other transformation technique for getting better robustness and r perceptibility issue. The summarize work of researcher's work by using SVD based technique is described in Table 5.

Table 5. Summary Details of Video Watermarking based on SVD

Paper	Application	Robustness Evaluation
[18]	To solve the problem of illegal redistribution of multimedia Data	JPEG compression, Video Angular Rotation, Gaussian Noise, Salt & Pepper Noise, Frame Dropping, frame Swapping and frame averaging and Payload capacity
[19]	#	Compression, frame averaging, frame resize and frame rotation

# Did not clearly mentioned the application areas

#### iv. Principal Component Analysis (PCA)

PCA is a powerful means for examining data. PCA is a method of recognizing samples in data. The working of PCA is that it creates the new coordinate to plots the information where the maximum energy concentration is fabricated means information with maximum covariance is designed and is known as the first principal component. Similarly, the second principal component can be obtained with second maximum covariance and likewise third and fourth principal components and so on. The other main advantage of PCA is that once these values in the data have been known, the data can be condensed by dropping the number of dimensions, without much loss of information. A complete tutorial on PCA is being described by Jon Shlens [20]. Like SVD, PCA is also use by very few researchers but combining PCA with other technique is being used by numbers of researchers as described in the subsequent section.

Hanane H. Mirza et al. [21] produced the digital video watermarking based on principal component analysis. A snapshot of this approach is that the after separating the original frame into 3 color channel: red, green and blue. Each of the three color band frames is separately subdivided into a number of blocks of equal size. Then apply PCA function for each of the sub-block to get three PCA components  $Y_R$ ,  $Y_G$  and  $Y_B$ . Finally, they selected the perceptually significant components of each of the three components to insert the watermark.

Then, the watermarked frame is constructed by applying the inverse PCA followed by combining the three color channel. This process is continued for all the frames in order to get watermarked video. The robustness is evaluated after applying geometric attacks, image processing attacks like median filter, cropping attack and



video specific attacks like frame dropping. But, the only limitation is that the algorithms have not check the other video specific attacks like frame averaging, frame swapping and collusion attacks and most important is the ambiguity problem is not covered also.

#### ❖ Limitations of Principal Component Analysis

- ❖ It is tough to calculate the exact interpretation of principal component data since the calculated variables are the linear combination of the actual variables.
- ❖ One constraint is that the mean is zero and variance is one in order to work better for PCA.

#### v. Discrete Cosine Transforms (DCT)

The Discrete Cosine Transform (DCT) domain permits a host signal (image or video) to be broken into different frequency bands. It expresses a finite succession of data points in terms of sum of cosine functions swinging at various frequencies. The original image/video frame/signal is divided into 8\*8 blocks of pixels and the 2-D DCT is applied independently to each block as shown in fig. 4. The mathematical formula for calculating 2-D DCT and inverse DCT are also shown in the equation (5) and equation (6).

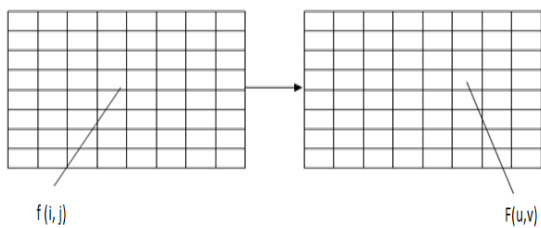


Fig.4. Original 8 x 8 Block of Image to DCT block of Same Size

Two dimensional DCT is as follows:

$$F[u, v] = \frac{1}{N^2} \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} f[m, n] \cos\left[(2m+1)u\pi/2N\right] \cos\left[(2n+1)v\pi/2N\right] \quad (5)$$

Where  $u, v =$  discrete frequency variables  $(0, 1, 2, \dots, N - 1)$ ,  $f[m, n] = M$  by  $N$  image pixels  $(0, 1, 2, \dots, N - 1)$ , and  $F[u, v]$  is the DCT result

Two-Dimensional IDCT equation:

$$f[m, n] = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} c[u]c[v]F[u, v] \cos\left[(2m+1)u\pi/2N\right] \cos\left[(2n+1)v\pi/2N\right] \quad (6)$$

$m, n =$  image result pixel indices  $(0, 1, 2, \dots, N - 1)$ ,  $F[u, v] = N \times N$  DCT result,

$$c[u], c[v] = \frac{1}{\sqrt{N}} \text{ when } u, v = 0$$

$$c[u], c[v] = \sqrt{\frac{2}{N}} \text{ when } u, v \neq 0,$$

$f[m, n] = N$  by  $N$  IDCT result.

Watermark information can be embedded into the later two data stream. If watermark is embedded into DCT coefficients, it is often embedded into those of I-frames because there are large number of DCT coefficient in I-frames while small in P-frames and B-frames. Most of the following researcher papers explore this idea.. The summary details of all the researchers using DCT for digital video watermarking is shown in Table 6.

Earlier the DCT based watermarking has been initiated for image type of data. The same has been extended in video sequence by Chiao-Ting Hsu [22] by exploiting the GOP structure of MPEG compression standard. They described the watermarking for intra frame (I-frame) as well as for non-intraframe (P or B frame). They performed several experiments to judge the robustness after applying some image processing attacks by using the similarity measurements of the original and the extracted watermark by calculating the NC value. The algorithm did not evaluated the video specific attacks like frame averaging, frame swapping, frame dropping and collusion attacks and most important is the ambiguity problem.

Lian-Shan Liu et al. [23] proposed the DCT based blind digital video watermarking in the paper. They randomly selected the frame to embed watermark is, and its Y component is transformed by 16-by-16 DCT. The low frequency coefficients of the DCT blocks are chosen to embed the watermarks which are chosen by its DC coefficient values. The watermark was extracted by evaluating the correlation between the absolute values of the low frequency coefficients of the blocks selected by DC values and the watermark. In order to judge the robustness of the watermarking method they uses MPEG-2 compression attacks in different bit rate, like the watermarked video frames are compressed respectively with the constant bit rate of 6Mbps, 4Mbps, 3Mbps and 2Mbps, and then decompressed.

Alper Koz et al. [24] proposed the embedding method mainly consists of two parts. In the first part, the video sequence is separated into shots and transformed into the  $(u, v, z)$  domain by the method of applying spatial 2-D DCT transform. The output of this is followed by a DFT transform in the temporal direction. In the second step, watermark information is embedded by means of adjusting one of the arbitrarily chosen coefficient pairs in the transform domain. Their experimental results are categorized in four parts named as case1 to case4 are as follows. Case1 include: Equal Watermark Energy Insertion under various attacks, Case 2: Invisibility under various attack, Case3: Equal BER during extraction for compression attacks and Case 4: Capacity under various attacks.

Further the same video watermarking method is presented by Luo Wei [25]. But the only difference is they embedded the watermark bits in a large amount of DCT DC coefficient of Y component of I frame only

instead of B and P frame. They extracted the watermark image without any attacks applying means robustness evaluation has not carried out, which is a very serious issue in any type of watermarking.

Neeta Deshpande et al. [26] described the video watermarking based on DCT. Their embedding proposal divided in three categories. The categories are (a) Algorithm for embedding audio as an invisible watermark (b) B. Algorithm for embedding IMAGE AS an invisible watermark.(c) Algorithm for embedding video as an invisible watermark. They evaluated the DCT of watermark image and added it to the DCT of extracted component of R, G, and B separately all the three categories of digital video watermarking. Their experimental results calculated the MSE and PSNR value after applying the various noise and filter attacks for evaluating the robustness and perceptibility of the watermarked video. Although they have claimed that their experimental results are also verified by video watermarking attacks like frame dropping and frame averaging in the last part of 'Abstract' yet they have not evaluated analytically.

Hui -Yu Huang et al.[27] proposed the digital video watermarking method based on the psedo 3D DCT i.e. the DCT transformation twice and quantization index modulation (QIM) in the uncompressed way. They embedded one watermark into every 20 frames. They used three videos in their experimental results. In order to verify the robustness, wide variety of intentional or unintentional attacks has been applied except the compression attack. On the other hand, PSNR has also been evaluated under the ratio of different watermark size.

Lufang Liao et al. [28] also proposed the method of digital video watermarking based on DCT with and without using HVS. In the very first case, they embedded the watermark into the video without HVS, using the stable strength 30 and 8 separately. Secondly, they embedded the watermark based on the HVS by using the stable strength. The algorithm challenged the inter-frame attack, cut attack, general stability attack (such as noise attack, filter attack, re-sampling etc.), jpeg compression attack. After these attacks, they successfully extracted the watermark. But they claim that the algorithm can't effectively resist against geometric attacks (such as rotation).

Seong-Whan-Kim [29] presented a watermarking scheme for digital videos that are based on human visual system characteristics. They inserted perceptually invisible watermark in Discrete Cosine Transform (DCT) domain. And it can be used in the Moving Picture Experts Group (MPEG) compression scheme. Their watermark is transparent and robust to video compression. They used MPEG-1 video coding with 44:1 compression ratio resulting in 22.1 dB (PSNR) on average. The limitation of this approach is that they have not covered attacks except video in compressed form for checking the robustness of watermark.

Yuk Ying Chung [30] described DCT based digital watermarking scheme for MPEG-2 video and implemented. The system embeds a watermark into the

quantized DCT coefficient during the MPEG-2 video encoding process. One watermark bit is embedded into the LSB of the DCT coefficient block of I-frames. This achieves the optimal tradeoff between watermark payload and distortion to video quality due to the embedded watermark bits. The watermark based on an error correcting code (ECC). The proposed watermark scheme was developed under the triple contradictory constraint of imperceptibility, robustness and capacity. To improve the performance in terms of watermark robustness, they combine the watermarking scheme with three error correcting codes: BCH(31,8), Turbo(3,1) and Conv(2,1,3). They found BCH(31,8) achieved higher error correcting capacity than Turbo (3,1) and Conv(2,1,3) under the simulated noise test. Seven cases of noise were simulated and tested. Although they tested and corrected the bit stream for the digital video watermarking scheme, yet the limitations of this approach is that they have not tested the imperceptibility as well as payload capacity which is the major trade off.

Sadik Ali M. Al Taweel [31] proposed the simple method to embed the watermark into the host signal. First, they transform the spatial watermark bits to the frequency domain by using the DCT domain and then they are added to the frame of the video coefficients directly. They tested the robustness of a digital watermarking for MPEG-2 video against the global geometric attacks such as cropping, scaling and rotation. There paper declares that their future work will be on improving the DCT and comparing it with the existing methods. In addition to this, the same scheme could be apply by using the Discrete Wavelet Transform that is relatively new and has useful properties for the image processing applications. The summarize work of researcher's work by using DCT based technique is described in Table 6.

Table 6. Summary Details of Video Watermarking based on DCT

Paper	Application	Robustness Evaluation
[22]	Copyright Protection	Cropping, MPEG Compression
[23]	Copyright Protection	Frame insertion, deletion, frame statistical averaging, Collusion attack
[24]	#	All four experiments consisting the attacks: Additive White Gaussian Noise, Video Coding at different bit rates, Temporal Shifting.
[25]	Copyright Protection	\$
[26]	Copyright Protection	Gaussian Noise, Poisson Noise, Salt & pepper Noise, Speckle Noise, Compression, Wiener, Median filter Attack
[27]	#	Wiener, Median filter Attack, Gaussian Noise, Salt & pepper Noise, Luminance Modification (lightened, darkened)
[28]	#	Gaussian Noise, Rotation Attack
[29]	Copyright Protection	MPEG-1 Video coding with 44:1 Compression
[30]	Copyright Protection	3 Error correcting codes are used to improve the robustness.
[31]	Copyright Protection	JPEG compression, Geometric distortions like Rotation, and Gaussian noise

# Did not clearly mentioned the application area

\$ Did not evaluated the robustness

#### ❖ *Limitations of DCT*

One of the major limitations of using DCT approach is that it produces real values after processing blocks of 8 x 8 consisting of integer values. Therefore an additional step of quantization is being needed to convert real values into integer values. Another limitation of DCT is that the image may be distorted due to higher compression ratio and therefore the picture may appear as strangely large pixel chunks. There is one more limitation is the false contouring effects. This is due to deep quantization of the transform coefficients. Hence the researchers showed their interest in another transformation also like DWT as described in the following next section.

#### vi. *Discrete Wavelet Transform (DWT)*

Among these, discrete wavelet transform is most popular and widely used in digital image processing applications due to its multi resolution characteristics. Wavelet transform decompose a video frame into four non-overlapping multi-resolution sub-bands (LL1, LH1, HL1, and HH1) which can be reassembled to reconstruct the original frame without error. The sub-band LL1 represents the coarse-scale DWT coefficients while the LH1, HL1, and HH1 represent the fine-scale of DWT coefficients. Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In general most of the energy is concentrated at the lower sub-bands LLx and therefore embedding watermarks in these sub-bands may degrade the image significantly. However, it could increase robustness significantly. On the other hand, the high frequency sub-bands HHx include the edges and texture of the image and the human eye is generally sensitive to changes in such bands. This allows the watermark to be embedded without being perceived by the human eye. The compromise adopted by many DWT-based watermarking algorithms is to embed the watermark in the middle frequency sub-bands LHx and HLx where acceptable performance of imperceptibility and robustness could be achieved. The following is the description of all those researchers who uses only DWT techniques to embed the watermark and final summary of all following papers covered only DWT domain has mentioned in Table 7.

C.V. Serdean [32] described a blind video watermarking system based on DWT with higher payload capacity and also evaluating the robustness by applying the geometric attacks such as shift, rotation, scaling and cropping. But the limitation of this approach is that it is restricted on geometric attacks only.

Yang Gaobo [33] overcome some of the limitations by applying a novel approach i.e. genetic algorithm based video watermarking in the DWT domain. They introduced some common attacks like average additive noise and lossy compression and video specific attacks such as frame dropping, frame averaging. But, the *limitations* of both the above approaches are that they overlooked the imperceptibility factor, which is also an

important concept in digital video.

Pik Wah Chan [34] proposed varieties of hybrid digital watermarking scheme based on the scene change analysis and error correction codes. In scene based watermarking system, a watermark is decomposed into different parts which are embedded in corresponding frames of different scenes in the original video. With this mechanism, the proposed method is robust against the attack of frame averaging, dropping, swapping and statistical analysis. But this scheme is not robust against the attack of image processing on the video frames. Therefore they propose a different approach known as hybrid to improve the performance and the robustness of the watermarking scheme. They improved the scene based analysis by creating two approaches named as visual audio hybrid watermarking scheme and hybrid approach with different watermarking scene. As the name, the visual-audio hybrid watermarking scheme applies both video and audio watermarks in the video. Error correcting codes are extracted from the video watermark and embedded as audio watermark in the audio stream. This approach takes the advantages of watermarking the audio channel because it provides an independent means for embedding the error correcting codes, which carry extra information for watermark extraction. Therefore, the scheme is more robust than other schemes which only use video channel alone. Another approach is hybrid with different watermarking schemes by considering the fact that no scheme can resist all watermark attacks. It is further classified into two major streams. First one is the 'different schemes for different scenes' and another is 'different schemes for different parts of each frames'. In the very first case, a watermark is still decomposed into different parts which are embedded in the corresponding frames of different scenes in the original video. Each part of the watermark is embedded with different scheme. Within the scene, all the video frames are watermarked with same part of the watermark by the same watermark scheme. When there is an attack on the watermark video, different watermark schemes are resistant against it. The merit is that only one part of the watermark is damaged if the watermark video is attacked. The disadvantage of this scheme is that the accuracy of the extracted watermark is lower as compared to the other scheme specified to a particular attack. In another scheme 'different schemes for different parts of each frames', four different watermarking schemes are applied to each frames. Each video frames is divided into four part, and the watermark for that frame is also divided into four parts. Then, each part of the watermark is also divided into four parts. Finally, each part of the watermark is embedded into the frames in different domains. Again, when a watermarked video is attacked, part of the watermark in each frame may still survive. Therefore, information for every part of the watermark can be retrieved and the watermark can be approximately estimated. Their experimental results shows that the scheme is robust against attacks by frame dropping, frame averaging, and statistical analysis and the robustness against the image processing attacks is tested with Stirmark 4.0 benchmark.

Sourour Karmani et al. [35] presented an efficient architecture of 2-D Scan based wavelet watermarking for image and video. Among several applications, one of the applications of video watermarking is broadcast monitoring. This paper is designed in view of this application i.e. video sequence for High Definition television (HDTV). In addition to this, this article also supports DVD protection and access control. Since the watermarking techniques using the 2D-DWT needs an , therefore they developed a special insertion technique combined with a scan based to optimize the hardware implementation in order to convenient for video content. The main attraction of this algorithm is that original video is not needed at the time of extracting the watermark. Such type of scheme can be useful for public watermarking applications, where the original video is not available for watermark extraction. Another characteristic of this approach is the security aspect, which is employed by several level of pseudo-random permutation along the watermark treatment. The key for this watermarking algorithm contains many parameters used to perform each level of permutation. The third feature of this scheme is invisibility of watermark. The performance is evaluated through real test sequence attached to the watermarking architecture. The major limitation of this scheme is that the robustness of watermarking is not tested at all, which is the primary requirement of any video watermarking scheme. Although they have calculated the PSNR value to judge the imperceptibility of quality of watermarked video but they have not shown any non correlation value to check the percentage of extraction of watermark from watermarked video.

Radu et al. [36] embedded the watermark in the wavelet coefficient of the LH, HL and HH sub-bands of the second wavelet decomposition level by quantization. They spread every bit of the watermark over a number of wavelet coefficients with the use of key.. They have tested the resilience of the watermarking algorithm against the series nine different attacks for different videos and improved the decoding BER by redundant embedding of the same watermark in different frames and by using an error correction code. The nine attacks are frame averaging, frame removal, JPEG compression of every frame with quality factor  $Q=70$ , MPEG-2 compression at 4 and 2 Mbps, Adding 'Salt and pepper noise with density  $d=0.05$ , Adding Gaussian noise of mean 0% and variance 0.05 %. Blurring using blocks of  $2 * 2$  pixels, Brightening by adding  $Y0=$  to the luminance of every pixel and Median filtering using a  $3 * 3$  pixel neighborhood. Their experimental result shows that the embedded watermark is invisible and robust to attack. The proposed algorithm achieves good resilience again a series of different attacks in the spatial, temporal and compressed domain. The performance of the algorithm is improved by using error correcting codes and by redundantly embedding the same watermark in different frames of the video. But the limitations of this approach are that it can be tested for more attacks such as geometric attacks like scaling, translation and rotation.

And the perceptual quality of the watermarked videos can also be improved by using a Human Visual System approach. One more major limitation is that it is non-blind approach.

Majid Masoumi et al. [37] presented an algorithm based on wavelet transformation. First the motion part of color video is detected by scene change analysis and then they applied the 3d wavelet transformation to decompose it upto 3<sup>rd</sup> level and choose the coefficient of HH, LH and HH. Finally, they use spread spectrum technique to embed the watermark into the selected coefficient. The main characteristic of this algorithm is that original video is not needed at the time of extracting the watermark. The performance is evaluated through several video specific attacks like frame averaging, frame dropping, frame swapping and image processing attacks like filtering, injection of impulse noise, MPEG-2 and H.264 compression. They obtained better results by comparing the same obtained by previous researchers. Therefore they achieve better robustness. Some of the limitations are also associated with this scheme, such as they have not tested the robustness of video watermarking scheme against some video specific attacks such as frame insertion which may be a unintentional attack like attaching the commercial break in the video and some image processing attacks such as blurring, sharpening, scaling and rotation.

The Rupachandra Singh et al. [38] proposed the video watermarking scheme based on visual cryptography, scene change detection and discrete wavelet transform. They propose the special scheme in which different segment of a single watermark is embedded into different scenes for production of the owner's part from the original video based on the frame mean and generation of the identification contribution based on the frame mean of probably attacked video i.e. their approach uses an identical sub-watermark for the successive frames in the same scene but different parts in different scene. These two shares after bundled can represent the copyright ownership. For conducting the experimental research, they cascaded eight video sequences. Each sequence consists of 300 frames, the size of each frame is 352 x 288 and the total numbers of frames in the video is 2400. The performance is evaluated through several video specific attacks like frame averaging, frame dropping, frame swapping and image processing attacks like filtering, injection of impulse noise, compression, blurring, sharpening, scaling and rotation. They obtained better results by comparing the same obtained by previous researchers. Therefore they achieve better robustness. The effectiveness of this approach is that they can identify the ownership without the need of original host video to hide the invisible watermark. The security of this algorithm is that it is not possible to recover the invisible identification share without the secret key. There are numbers of limitations of this scheme, such as they have not tested the robustness of video watermarking scheme against some video specific attacks such as frame deletion. Moreover, they deal with compression attacks but they could not specify the

category of compression like JPEG, MPEG-2, and MPEG-4 and at which data rate.

Mitchell et al.[39] divided the robustness in two categories and measured the same for both types. The first is to accept the video by extracting the watermark successfully even after the number of image processing attacks and video specific attacks. The other is to reject a video if the watermark is not present in the video. The criteria they adopted is to create the hypothesis that the large similarity indicates that the watermark is present( $H_0$ )while the low similarity shows the lack of watermark( $H_1$ ). They also tested the ability to detect watermark in the presence of other watermark.

Mahesh et al.[40] described the digital video watermarking by using 3-D wavelet transform. [33] embedded the watermark to the coefficient of all high pass wavelet coefficients. Robustness is evaluated by introducing MPEG compression by all researchers. In addition to that [33] evaluated the robustness by digital half-toning attacks.

Majid Masoumi et al.[41] proposed the DWT based robust, blind digital video watermarking based on scene change. The scene is described to evaluate the authenticity of digital video. The specialty of this algorithm is that they creates the numbers of parts of the single watermark and embed embedded the different parts into different scene of a video. Robustness is being evaluated against number of attacks image processing attacks may be geometric attacks, median filter attacks and image enhancement attacks as well as video specific attack either unintentional or intentional attack.

Hitesh Patel et al.[42] proposed the robust blind digital video watermarking based on DWT decomposed up to 4 levels. The innovatively of this algorithm is that the watermark is itself a colored video. The video is first divided into frames and then they took 3 images for each frame. They evaluated the imperceptibility by calculating the PSNR value between the range of 31 and 44DB.

Jamal Hussein et al.[43] has introduced the video watermarking scheme in which the watermark is embedded into the motion regions. The HL and LH bands are used that maintains the quality of the extracted watermark. The watermark used is the random Gaussian distribution. The proposed scheme has a higher degree of invisibility against the attack of frame dropping, adaptive quantization, and frame filtering. It can also be used for audio layer in video codec standards for future purpose.

Abdulfetah et al.[44] incorporated HVS model in DWT domain that shows effective results against imperceptibility and robustness.

S.S.Bedi et al.[45] described the video watermarking based on 2 level DWT. The video sequence clip for resolving the issue of copyright protection was being used from the India movie 'Hum Aapke Hai Kaun'. Robustness was evaluated by applying three attacks as 'Geometric attack- Rotation' and Gaussian Noise and cropping attack. The major limitation of this approach is that the robustness can be evaluated by implementing more video frame attack. The summarize work of researcher's work by using DWT based technique is described in Table 7.

Table 7. Summary Details of Video Watermarking based on DWT

Paper	Application	Robustness Evaluation
[32]	#	Scaling upto 180%, Rotation upto 70%, frame shifting, Cropping, MPEG Compression as low as 2-3 Mbps
[33]	#	Frame dropping, frame averaging, white noise sequence with zero mean and 1 variance, lossy video compression by the video standard H.264
[34]	Multimedia Security & Multimedia Copyright Protection i.e. worked on both video watermark & audio watermark	Lossy compression, Median filter, Row/column removal, cropping, rescale, Rotation, affine for DWT based watermarking and scene based watermarking, frame dropping, frame averaging, statistical analysis
[35]	Broadcast Monitoring , DVD protection and access control	\$
[36]	Video Copyright Protection	Blurred, brightness, Gaussian, Median, Salt & Pepper, frame averaging, frame removal, JPEG Q-80, MPEG-2 4Mbps, MPEG-2 2 Mbps
[37]	Copyright Protection	Median filtering, Gaussian noise, frame dropping, frame averaging, frame swapping, lossy compression including MPEG-4, MPEG-2, and H.264
[38]	Multimedia security and copyright protection	Gamma Correction frame dropping, frame averaging, cropping, filtering, injection of impulse noise, Compression, Blurring, sharpening, rotation and scaling
[39]	Copyright Protection	Detection of other watermark in presence of other watermark i.e. ambiguity watermark attack, MPEG coding, Printing & Rescanning, Frame averaging
[40]	Multimedia security and multimedia copyright	Frame dropping, Statistical Averaging, cropping attack
[41]	Public Watermarking Applications	Median Filtering, Gaussian Noise, Frame Dropping, Frame Averaging, frame swapping, MPEG-4 compression
[42]	Video Copyright Protection	\$
[43]	Video Copyright Protection	Low pass filter, High pass Filter
[44]	Video Copyright Protection	Sharpening, Low pass filter, Salt & Pepper , JPEG compression, Rotation, Resize, Histogram Equalization, Gaussian Noise, Cropping
[45]	Video Copyright Protection	Gaussian Noise, Rotation and Cropping

# Did not clearly mentioned the application area

\$ Did not evaluated the robustness

❖ *Limitations of Discrete Wavelet Transform*

- i. The cost of computing with DWT in video watermarking or in other application like image compression is always higher than DCT.
- ii. In case of processing larger DWT basis functions or wavelet filters surely produces the blurring and noise near the regions of edges in video frames or images.

vii. *Hybrid Approach*

Since every transformation scheme has its own properties and very powerful and they have also having some sort of limitations therefore the researchers shifted to hybrid approach i.e. combining more than one transformation techniques for carrying the advantages of each one to provide more robustness of . described below.

Jason Kaufman [46] described a digital video watermarking technique using singular value decomposition (SVD) and 2D principal component analysis (2DPCA). They applied the SVD which is operated in the spatial domain where the two dimensional Principal Component Analysis is engaged for embedding in the time domain. Their research result indicates that the method yield watermarked video with little perceptible distortion. Their task could be extended to test the robustness against applying the various attacks.. The summary details of all the researchers using hybrid approach i.e. combining 2 or more transformation for digital video watermarking is shown in Table 8.

Lama Rajab [47] extended the work of Jason Kaufman by proposing an effective blind digital video watermarking algorithm. The usefulness of algorithm is conveyed by virtue of applying two commanding mathematical transform: the very first is singular value decomposition (SVD) covered in the section 6.1.2.1 and the other one is discrete wavelet transform, covered in the section 6.1.2.4. They obtained better result against for evaluating the robustness against various image specific attacks like JPEG compression, rotation, Gaussian and Salt & Pepper attack and video specific attack like frame dropping, frame swapping and frame averaging as compare to the results reported in [41] and [42].

Maher EL'ARBI [48] described a blind video watermarking system invariant to geometric attacks. Their scheme embeds different parts of a single watermark into different shots of a video under the wavelet domain. A multi resolution motion estimation (MRME) is adopted to allocate the watermark to coefficient containing motion. In addition, embedding and extraction of the watermark are based on relationship between a coefficient and its neighbor. Experimental results show that inserting watermark where picture content is moving is less perceptible. Their embedding process is broadly classified into 3 steps. First step is to select the embedding regions, which are motion detection and details detection mechanisms. They use only middle frequency wavelet coefficient of the frames for embedding the watermark. In the second step, they

described the watermark embedding strategy. In the final step, they proceed to wavelet network training, which will be use later in the watermark embedding process. To evaluate the performance of the video watermarking scheme, several experiment have been done. They include frame shifting, cropping, scaling, rotation and change of aspect ratio. They also evaluated the PSNR value which is obvious from their results that they have less distortion due to watermark embedding process. They also calculated the NC values of the extracted watermark with different aspect ratio change. Not only this, they evaluated the NC value after rotation, resize and cropping attacks.

Emad E. Abdullah [49] uses the scene change analysis to embed the watermark repetitively into the singular values of high order tensors computed from the DWT coefficient of selected frames of each scene. Their experimental results shows that the perceptual invisibility and robustness against common attack as scaling, frame dropping and frame averaging is improved. But, again this approach is non-blind i.e. at the time of verification; original video as well as original watermark is needed.

Sanjana Sinha, et al. [50] proposed a comprehensive approach for watermarking digital video. It is based on hybrid digital video watermarking scheme consisting two powerful transformations as Discrete Wavelet Transform (DWT) and Principal Component Analysis (PCA). PCA helps in reducing correlation among the wavelet coefficients obtained from wavelet decomposition of each video frame thereby dispersing the watermark bits into the uncorrelated coefficients. The video frames are first decomposed by the help of DWT and the binary watermark is embedded in the principal components of the low frequency wavelet coefficients. The imperceptible high bit rate watermark embedded is robust against various attacks that can be carried out on the watermarked video, such as filtering, contrast adjustment, noise addition and geometric attacks. As a future work the video frames can be subject to scene change analysis to embed an independent watermark in the sequence of frames forming a scene, and repeating this procedure for all the scenes within a video.

Tahani Al-Khatib Et al. [51] has introduced an algorithm that extracts the watermark from each frame by using two powerful transformations DWT and SVD. The proposed scheme evaluated the robustness by applying the various attacks like video compression, video rotation, Gaussian noise, salt and pepper noise etc.

Satyanarayana Murty et al. [52], propose three robust and semi-blind digital video water marking algorithms. These algorithms are based on hybrid transforms which uses the combination of Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) and the combination of three of them i.e. Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). Here the original video is divided to number of frames. On one frame they apply correspond three hybrid transform algorithms. The

process is repeated as well for all the remaining frames. The performance of the proposed algorithms was evaluated with respect to imperceptibility and robustness. The results show that proposed algorithms give a good Peak Signal to Noise Ratio (PSNR), however limitation is that their performance varied with respect to robustness. In these proposed algorithms DWT-SVD has good imperceptibility. When considered the robustness of these algorithms the DWT-DCT-SVD algorithm was good.

Fung [53] propose a different method to embed the watermark i.e. insert information in the side view, dissimilar the regular approaches that add on the frames. In the very first step, they change the video references of the frames of videos. Secondly, they process the DWT-SVD approach to insert a gray scale image on the luminance (Y) of YUV converted video. They tested the imperceptibility by calculating the PSNR value, which is 47.33, which indicate that the watermark have a high level of fidelity and can't be deducted by human visual system. In addition to this, they check the robustness against various attacks listed as Filtering and noise addition, frames attacks, compression. Among these, frame attacks are the current issue in video applications. They tested two attacks named as *frame dropping* and *frame swapping*. They generate video samples for 10%, 30%, 50% and 70% of frame dropping and the calculated corresponding correlation values are 0.9864, 0.8340, 0.3946, and 0.0792. They also swap two random frames of the video and obtained the 0.9976 correlation value. There have mentioned the only limitation, the use of non blind approach. And due to the use of a non-blind watermark, the requirements for the extraction process are the original watermark and video, therefore the common application for this method are temper detection and authentication. There are some more things could be tested such as evaluating a multi-watermarking process that embedded some watermark on other side planes of the video. This approach can improve the capability of the data inserted on the cover video. Other unintentional attacks on video are video editing, i.e. inserting commercial brake, cut some portion of video, changing the content could be checked, through this robustness could be achieved in a better way.

M. Omidyeganeh et al.[54] presented an event based technique for digital video watermarking. They identified the spatial features by employing the multi resolution singular value decomposition (MR-SVD) from each video frame in order to construct the features matrix of parameters. And then the features matrix is stalled by the temporal decomposition. First they convert the watermark bits into 1 and -1 and then embedded into the target matrix. They evaluated the robustness by applying various image processing attacks like median filter attack, JPEG compression attack, collusion attack and noise attack. In addition to that they also evaluated the robustness against video specific attacks like frame swapping, frame averaging, frame dropping attack and MPEG-2 attacks. They draw the graphs between bit error rate and PSNR for each type of robustness evaluation.

Salwa A.K Mostafa et al. [55] presented a technique for embedding a binary watermark into digital video frames. They claim that the proposed scheme is an imperceptible and a robust hybrid video watermarking scheme. First DWT is applied to each video frame and they PCA is applied to each block of the two bands namely LL and HH. The watermark is embedded into the principal components of the LL blocks and HH blocks in dissimilar ways. They evaluated the PSNR and NC value by applying the various attacks like Gamma Correction, automatic Equalizer, contrast adjustment attack and geometric attack (Cropping, rotation) and resize attack, JPEG compression attack and MPEG compression attack. Robustness is increases by applying PCA on DWT coefficients. So, their scheme satisfies the requirement of imperceptibility and robustness for a feasible watermarking scheme.

Soumik Das et al. [56] described two digital video watermarking schemes. First algorithm is based on LSB of 'Blue' value of each pixel of every blocks of Y component of each frame in order to embed the colored watermark information. Second algorithm is based on four IC (8:1 MUX). The whole embedding and extraction concept is explained in their paper. They also evaluated the robustness against intentional attacks like frame dropping, frame averaging and frame swapping.

Hee-Dong Kim et al. [57] described the hybrid watermarking scheme for Creative Common Licence (CCL) applied video contents. They embedded two watermarks: robust watermark and fragile watermark into the video frames known as hybrid watermark. 6 video clips have been used to evaluate the efficiency of the scheme. To test the fidelity, they calculate the PSNR for each video. Robustness is also successfully evaluated after applying 4 types of attack. At the last, their experimental results also tested the fragile test in order to judge whether the target video has been manipulated for geometric attack like cropping and scaling and for frame rate test also.

Ashish M. Kothari Et. Al. [58] has introduced the scheme that combines the features of DCT and SVD to embed the message behind the video. Proposed scheme is robust against compression, Gaussian LP filtering, Gaussian noise, Salt & Pepper noise and Spackle noise. It is concluded that this scheme fails in average filtering, median filtering, motion blur, rotation and intensity adjustment attacks.

K. Thaiyalnayaki et al. [59] described the video watermarking in which the watermark is encrypted by singular value decomposition procedure and it is embedded into the discrete wavelet transformed (dwt) coefficient of video frame. Their experimental results shows that the watermark is successfully extracted from the watermarked video. The algorithm was also tested the robustness by applying the compression attack and cropping attack.

Nisreen I. Yassin et al. [60] implemented the video watermarking by using two powerful transformation as 2 level DWT and Principal Component Analysis (PCA). A numbers of video sequences have been used for testing

the scheme. Robustness is being passes through various test like Histogram equalization, Gaussian attack, contrast adjustment attack, JPEG compression, resize, cropping and rotation attack but did not produce any frame specific attack. They also compared the PSNR value with some renowned researchers. They also evaluated the Bit error rate.

Himanshu Ag et al. [61] proposed the video watermarking based on hybrid approach by using DWT and SVD. Their experimental result focused on robustness and perceptibility issue. Two time experiment have been perform by using two different grey scale images, 'logo.tif' and 'cameraman.tif'. The performance is almost good and reasonable for calculating the correlation coefficient (CC) and PSNR before and after the attacks.

Ashish M. Kothari et el. [62] has combined DWT and DCT techniques. In this proposed scheme the watermark strength depends on the Gain Factor as the value of Gain Factor increases the perceptibility decreases but results in increased watermark strength.

Osama S. Faragallah et al. [63] presented the video watermarking based on SVD and DWT. First video frames are transformed into 2 levels DWT. The high frequency and middle frequency transformed coefficients were passed through SVD and then the watermark is hidid. The robustness was evaluated for image processing attack as well as video specific attack. These attacks are blurring, brightness, Gaussian and median filter, scaling, cropping, rotation and Hi264 compression and joint attacks.

Nisreen I. Yassin et al. [64] described the digital video watermarking scheme based on DWT and PCA. First they applied the DWT thrice time on each video frame to get numbers of sub-bands. The maximum entropy blocks were choose and transformed using Principal Component Analysis (PCA). The PCA sub-bands blocks containing maximum coefficients is quantized by using Quantization Index Modulation (QIM). Such quantized blocks are used to embed the watermark. They evaluated the robustness by applying the gamma correction, resize, rotate, contrast adjustment, histogram equalization and JPEG compression. The main feature of this scheme is that the secret key is established at the time of embedding the watermark and this key is used to retrieve the watermark.

Divjot Kaur Divot et al. [65] suggested the digital video watermarking scheme based on DWT and SVT. Robustness is being evaluated by applying the different attacks like Gaussian noise, Poisson Noise, Salt and pepper Noise, Blurring, Frame averaging and rotation attacks also.

Neeta Deshpande et al. [66] described the video watermarking scheme based on spatial and frequency domain both. The scheme embedded dual watermark into the video. First binary image as watermark is embedded in spatial and another invisible binary watermark is embedded in the DCT frequency component of video

frames. In this way it serves dual purposes i.e. protecting the public watermarking as well as private watermark in the same scheme. Robustness is being evaluated after applying various attacks like blurring, scaling, average filtering, sharpening and Gaussian filtering.

Ta Minh Thanh et al. [67] used the KAZA features in order to provide the robust semi blind watermarking based on a frame-patch matching. The watermark information is embedded in Discrete Cosine Transform (DCT) domain of randomly generated blocks in the equivalent region. The purpose of choosing the KAZA features is to engaged for comparing the features points of frame-patch with all the frames of video for finding the embedding and extracting areas. Again the robustness is also successfully by evaluating the normalized correlation value (NC) by applying the attacks are summarized as follows: Rotation w. crop ( $-20^\circ$ ), ( $-10^\circ$ ), ( $-5^\circ$ ), ( $+5^\circ$ ), ( $+10^\circ$ ), and ( $+20^\circ$ ), Scaling 0.3, 0.5, 0.8 and 1.2, frame dropping 10%, 20%, frame insertion 10%, 20%, frame transposition 10%, 20%, frame averaging 10%, 20%, Blurring, Gaussian  $3 \times 3$  and MPEG-4 attack. The application covered by this approach is not only the copyright protection, but also detecting prohibited redistribution and distinguishing authorized user.

Shoab et al.[68] embedded the watermark by using the 3 level DWT algorithms and they also use a secret key to insert as well as the same key is use to extract the watermark.

Jianzhong Li et al.[69] proposed the digital video watermarking method to embed the binary watermark on the low frequency coefficients of wavelet sub-bands by implementing GOP with a quantization algorithm. The algorithm is being tested for robustness against several different categories of attacks. The categories are temporal attacks, image processing unintentional attacks including brightness and contrast, geometric attacks, compression attacks and noise insertion attacks.

The summarize work of researcher's work by using hybrid approach is described in Table 8.

#### ❖ *Summarization of Hybrid Approach*

Although using hybrid approach, the investigator may get better result but the above described approach fails whenever real time environment comes into the picture i.e. generally video data either movie, video conferencecing, broadcast monitoring or any other video watermarking application contain huge data i.e. in gigabytes. This large amount of data requires to compress first to tranfer via network. Hence the researchers thought that it is better to embed the watermark either at compression time or after compression by using some compression standard like MPEG2, MPEG4 or any other. Finally, the investigator move towards compressed domain to fullfill both challenges: compression as well as embedding. And finally the papers covering these techniques will be covered in next issue of review.



Table 8. Summary Details of Video Watermarking based on Hybrid Approach

Paper	Application	Robustness Evaluation
[46]	#	\$
[47]	Copyright Protection	JPEG compression, Gaussian Noise, Rotation, Salt & Pepper Noise, frame dropping, frame averaging.
[48]	#	Rotation, Horizontal flip, Vertical Flip, Resize
[49]	Copyright Protection	Salt & pepper, Gamma Correction, Rescaling, , MPEG Compression, Frame Dropping Low pass Filter, JPEG compression, Cropping. Histogram Equalization, Sharpening, Motion Blurring, Frame Swapping and combination of these attacks
[50]	Multimedia Security and Copyright Protection	Cropping , Rotation , Resizing, Median Filtering , Gaussian Noise , Salt & Pepper Noise, Gamma, Correction , Sharpening, Filter, Contrast Adjustment, Automatic Equalization Attack
[51]	Copyright Information	Video Compression, Gaussian Noise, Video Rotation, Salt & Pepper Noise
[52]	Protection of Intellectual Property right of Multimedia	Motion Blur, Histogram Equalization, Cropping, Resize, Median Filter, Average Filtering, Gaussian Noise , Salt & pepper , Rotation Attack and JPEG Compression attack
[53]	Copyright Information	Gaussian noise, Salt & Pepper, Gaussian Filter, Poisson noise, Frame swapping, Frame dropping, MPEG Compression
[54]	#	Frame swapping, Frame dropping, Frame averaging, Median filter, MPEG Compression, Collusion Attack, Motion JPEG attack, Salt & Pepper, Gaussian Filter
[55]	Security and Copyright Protection	Gamma Correction, Automatic Equalization, Contrast Adjustment attack, Resize, Rotation and Cropping , Gaussian Noise Attack, JPEG Compression Attack, MPEG Compression Attack and Sharpening Attack
[56]	Copyright protection, Fingerprinting and Copy Control	Frame dropping, Frame averaging and Frame swapping.
[57]	Copyright Protection issues	Fidelity test, Scaling, Cropping, Frame Rate Change, Temporal Clipping,
[58]	Copyright Protection and Proof of Ownership	JPEG compression Attack, Gaussian LPF Attack, Gaussian Noise Attack, Salt and Pepper Attack, Spackle Noise Attack
[59]	Copy Protection and Copyright Protection	Cropping and Lossy compression.
[60]	Copyright Protection	Salt & Pepper Noise , Gaussian noise, Sharpening, Rotate, Smoothing
[61]	Copyright Protection	Poisson Noise , JPEG Compression Quality Factor Q =25, Indeo5 Compression, Quality Factor Q =25, Frame Swapping (Swap Six Frames), Frame Averaging, (Average Two Frames), Frame Insertion Ten Frames Inserted), Intensity Adjustment Between [ .2 .3 .1 ] to [ .6 .7 1 ] , Cropping 40 Columns), Rotation 0.5o, Salt and Pepper Density 0.01, Speckle Noise Variance 0.001
[62]	Copyright Protection	Average filtering, Compression attack, Linear Motion of the Camera, Gaussian Noise with zero mean and variable variance, Gaussian Noise with Variable Mean 0.0005 Variance , Color reduction, GLPF with sigma values
[63]	Copyright Protection	Blurring, Brightness, Gaussian, Median Filter, Salt & Pepper, Frame averaging, JPEG compression, MPEG compression at 4 and 2 Mbps, frame rotation and joint attack like first scaling then rotating the video frame.
[64]	Copyright Protection	The gamma correction, resize, rotate, contrast adjustment, histogram equalization and JPEG compression
[65]	Copyright Protection	Gaussian noise, Poisson Noise, Salt and pepper Noise, Blurring, Frame averaging and rotation attacks also.
[66]	Publicly available data, prohibit ting of illegal redistribution of data	Blurring, scaling, average filtering, sharpening and Gaussian filtering.
[67]	Copyright Protection	Rotation with cropping, Scaling, Gaussian filter, frame dropping, Frame insertion, frame translation, compression, blurring, frame averaging.
[68]	Copyright Protection	\$
[69]	Copyright Protection	Temporal attack, Filtering attack, Noise addition attack, Compression, Translation, Brightening, and Temporal attacks.

# Did not clearly mentioned the application areas

\$ Did not evaluated the robustness parameters

### VIII. CONCLUSION

In this literature various video watermarking techniques proposed by the academician or industrialist in various spatial and transformation domains covering the terms of robustness, imperceptibility and their payload capacity is reviewed. A brief summary has been mentioned for each created group of video watermarking

techniques in order to ease for reader at the end of each group. Certainly new algorithms are anticipated to come and may coalesce existing advance. However many challenges still under consideration like ambiguity of watermarks, collusion attack, elapsed time to embedding the watermark, video specific attacks and applying more than one attack at a time and more important is the 'video watermarking in real time environment' and many more issues. As mentioned earlier, this review detailed most of

those papers where video is considered in uncompressed original form. The rest part of video watermarking will be reviewed very soon in which watermark is embedded in encoded video or during the encoding.

#### IX. FUTURE SCOPE OF DIGITAL VIDEO WATERMARKING

- i. After an exhaustive survey it has been found that very few investigators take care about the efficiency of the embedding algorithm. One of them is Yuan-Gen Wang [70] who did calculation for finding the latency time for embedding watermark in original video.
- ii. Most of the researchers focused on inserting the watermark by using transformation domain of original video content not compressed. Since most of the video comes in market in compressed domain due to heavy storage requirement therefore it becomes necessary to insert the watermark in compressed domain.
- iii. There are number of attacks as described in section five may be use by attacker to distort the watermark. Most researcher check the robustness by applying some of them generally geometric attack, noise attack or low or high pass filter attack. Very few of them judge the robustness by applying video specific attack either intentional or unintentional.

#### REFERENCE

- [1] Saraju P. Mohanty, Elias Kougiannos, "Real-time perceptual watermarking architectures for video broadcasting", *The Journal of Systems and Software*, Volume 84 Issue5, Elsevier Science Inc. New York, NY, USA, May 2011, pp. 724-738.
- [2] Cross, D.; Mobasser, B.G., "Watermarking for self-authentication of compressed video, *Image Processing. 2002. Proceedings. 2002 International Conference on*, vol.2, IEEE 2002, pp. 913-916.
- [3] Saadi, K.S.; Bouridane, A.; Gessoum, A., "H.264/AVC video authentication based video content," *5th International Symposium on*. Sept. 30 2010-Oct. 2010, pp.1-4.
- [4] Sun, Q.; Dajun He; Qi Tian, "A Secure and Robust Authentication Scheme for Video Transcoding," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol.16, no.10, Oct. 2006 , pp.1232,1244.
- [5] Dawen Xu, Rangding Wang, Jicheng Wang, "A novel watermarking scheme for H.264/AVC video authentication", *Signal Processing: image communication*, ELSEVIER, 2011, pp. 267-279.
- [6] Po-Chyi Su Chin-Song Wu, Ing-Fan Chen, Ching-Yu Wu, Ying-Chang Wu, "A practical design of digital video watermarking in H.264/AVC for content authentication", *Signal Processing: image communication*, ELSEVIER, 2011, pp. 413-426.
- [7] Gwenaél Do. err, Jean-Luc Dugelay, " A guide Tour of Video Watermarking", *Signal Processing: Image Communication*, ELSEVIER, 18, 2003, pp. 263–282.
- [8] Priya Porwal, Tanvi Ghag, Nikita Poddar, Ankita Tawda, "Digital Video Watermarking using modified LSB and DCT technique", *Int. Journal of Research in Engineering and Technology*, Vol 3, issue 4, 2014, pp. 630- 6634.
- [9] Mercy George, Jean-Yves Chouinard, and Nicolas Georganas, "Spread Spectrum Spatial and Spectral Watermarking for Images and Video", *Proc. Of IEEE Can. Workshop in Information Theory*, Kingston, 1999.
- [10] Karen Su, Deepa Kundur and Dimitrios Hatzinakos, "A Novel Approach to Collusion-resistant Video", *Security and Watermarking of Multimedia Contents IV*, Edward J. Delp III, Ping Wah Wong, 2002, pp. 491-502.
- [11] Houmansadr, Amir, and Shahrokh Ghaemmaghami. "A novel video watermarking method using visual cryptography." *Engineering of Intelligent Systems*, IEEE International Conference on. IEEE, 2006, pp. 1-5.
- [12] Luo Wei, "A improved video watermarking scheme based on spread-spectrum technique," *Networking and Digital Society (ICNDS)*, 2010 2nd International Conference on, vol.1, no30-31 May 2010, pp. 511-514.
- [13] Radu Ovidiu Preda, Nicolae Vizireanu, "New Robust Watermarking Scheme For Video Copyright Protection In The Spatial Domain, U.P.B. Sci. Bull., Series C, Vol. 73, Iss. 1, ISSN 1454-234x, 2011 pp. 93-104.
- [14] Radu Ovidiu Preda, Cristina Oprea, Ionuț Pirmog, Lucian Andrei Perișoara, "Robust Digital Video Watermarking in the Spatial and Wavelet Domain", 2012: *The Seventh International Conference on Digital Telecommunications*, 2012, pp. 78-83.
- [15] C. S. Woo, J. Du and B. Pham, "Performance Factors Analysis of a Wavelet-based Watermarking Method", *Proc. 3rd Australasian Information Security Workshop (AISW2005)*, CRPIT, vol. 44, 2005, pp. 89-97.
- [16] S. Pereira, S. Voloshynovskiy and T. Pun, "Optimized Wavelet Domain Watermark Embedding Strategy Using Linear Programming", *Wavelet Applications VII (part of SPIE AeroSense 2000)*, Apr. 2000, pp. 490-498.
- [17] Jana Dittmann, Anirban Mukherjee, Martin Steibach, "Media independent watermarking classification and the need for combining digital video and audio watermarking for media authentication", 2002, pp. 62-67.
- [18] Lama rajab, Tahani Al- Khatib and Ali Al haj, "Video Watermarking Algorithm using the SVD transform", *European Journal of Scientific Research*, ISSN 1450-216X, Vol-30, No.3, 2009, pp. 389-401.
- [19] Tomas kanocz, Peter go - Matis, Patrik gallo, Dusan levicky, "Real-time Digital Video and audio watermarking Based on SVD", *Proceeding of IEEE 2011*, pp. 1-4.
- [20] Shlens, Jonathon. "A tutorial on principal component analysis." *arXiv preprint arXiv: 1404.1100*, 2014.
- [21] Hanane H. Mirza, Hien D. Thai, Yasunori Nagata, Zensho Nakao, " Digital video watermarking based on Principal Component Analysis", *IEEE Transaction* , 2007, pp. 290-290.
- [22] Chiao-Ting Hsu, Ja-Ling Wu, "DCT –Based Watermarking for video", *IEEE transactions on Consumer electronics*, Vol 44, No.1, Feb-1998, pp. 206-216.
- [23] LIAN-SHAN LIU, REN-HOU LI, QI GAO, "A Robust Video Watermarking Scheme Based On DCT", *IEEE Proceedings of the Fourth International Conference on Machine Learning and Cybernetics*, Guangzhou, 18-21 August 2005, pp. 5176-5180.
- [24] Alper Koz, A. Aydin Alatan,, "Oblivious Spatio-Temporal Watermarking of Digital Video by Exploiting the Human Visual System", *IEEE Transactions On Circuits And Systems For Video Technology*, Vol. 18, No. 3, March 2008, pp. 326-337.
- [25] Luo Wei, "A Improved Video Watermarking Scheme Based on Spread-spectrum Technique", *IEEE International Conference on Networking and Digital Society*, 2010, pp-511-514.

- [26] Neeta Deshpande, Dr. Archana Rajurkar, Dr. R. Manthalkar, "Robust DCT based Video Watermarking algorithms for Assorted Watermarks", "IEEE 2nd International Conference on Signal Processing Systems (ICSPS)", Vol 6, 2010, pp. 320-324.
- [27] Hui-Yu Huang, Cheng-Han Yang, and Wen-Hsing Hsu, "A Video Watermarking Technique Based on Pseudo-3-D DCT and Quantization Index Modulation", IEEE Transactions On Information Forensics And Security, Vol. 5, No. 4, 2010, pp. 625-637.
- [28] Lufang Liao, Xiaoshi Zheng Yanling Zhao ,Guangqi Liu, "A New Digital video Watermark Algorithm Based on the HVS", IEEE International Conference on Internet Computing and Information Services, 2011, pp. 446-448.
- [29] Seong-Whan Kim, Shah Suthaharan, Heung-Kyu Lee, K.R. Rao, "Perceptually Tuned Robust Watermarking Scheme for Digital Video Using Motion Entropy Masking", Proc. Of IEEE, 1999, pp. 104-10.
- [30] Yuk Ying Chung, Fan Fei Xu, Faith Choy, "Development of Digital Video Watermarking for MPEG-2 Video, Proc of IEEE, 2006, pp. 1-4.
- [31] Sadik Ali M. Al Taweel, Putra Sumari, Saleh Ali K. Alomari and Anas j.A.Husain, " Digital Video Watermarking in the Discrete Cosine Transform Domain", Journal of Computer Science 5(8): ISSN 1549-3636© 2009 Science Publication, 2009, pp. 536-543.
- [32] C. V. Serdean, M.A.. Ambroze, M. Tomlinson and J.G. Wade, "Adding Robustness to Geometrical Attacks to a Wavelet Based, Blind Video Watermarking System", Proc. Of IEEE 2002, pp. 557-560.
- [33] Yang Gaobo, Sun Xingmig, Wag Xiojing, "A genetic Algorithm based Video Watermarking in the DWT Domain", Proc. Of IEEE 2006, pp.1209-1212.
- [34] Pik Wah Chan, Student Member, IEEE, Michael R. Lyu, Fellow, IEEE, and Roland T. Chin, "A Novel Scheme for Hybrid Digital Video Watermarking: Approach, Evaluation and Experimentation", IEEE transactions on circuits and systems for video technology, vol. 15, no. 12, december 2005, pp. 1638-1649.
- [35] Sourour Karmani, Ridha Djemal, Rached Tourki, "Efficient hardware architecture of 2D-scan based wavelet watermarking for image and video", Computer Standard & Interface (Elsevier), Oct 2008, pp. 801-811.
- [36] Radu O. Preda, Dragos N. Vizireanu, "A robust digital watermarking scheme for video copyright protection in the wavelet domain", Proceeding of ELSEVIER journal of Science Direct, 2010, pp. 1720-1726.
- [37] Majid Masoumi, Shevin Amiri, "A Blind Scene based watermarking for video copyright protection", International Journal of Electronics and Communication (Elsevier), 28 Nov. 2012, pp. 528-535.
- [38] The Rupachandra Singh, Kh Manglem Singh, Sudipta Roy, "Video Watermarking Scheme based on visual cryptography and scene change detection", International Journal of Electronics and Communication (Elsevier), jan 2013, pp. 189-196.
- [39] Mitchell D. Swanson, Member, IEEE, Bin Zhu, Member, IEEE, and Ahmed H. Tewfik, Fellow, IEEE, "Multiresolution Scene-Based Video Watermarking Using Perceptual Models", IEEE journal on selected areas in communications, vol. 16, no. 4, may 1998. pp. 540-550.
- [40] Mahesh R. Sanghvi, Dr. Mrs. Archana M., Prof. Dr. Rajeev Mathur, Kainjan S Kotecha, "A Robust Scheme for Digital Video Watermarking based on Scrambling of Watermark", International Journal of Computer Applications (0975 – 8887) Volume 35– No.2, December 2011, pp. 31-38.
- [41] Majid Masoumi, Shervin Amiri, "A blind scene-based watermarking for video copyright protection", International Journal of Electronics and Communications, 2013, pp. 1-8.
- [42] Hitesh Patel, Jignesh Patoliya, Pradip Panchal, R. N. Patel, "Digital robust video watermarking using 4-level DWT", International Journal of Advanced Engineering Technology, 2010, pp. 101- 113.
- [43] Jamal HUSSEIN and Aree MOHAMMED, "Robust Video Watermarking using Multi-Band Wavelet Transform", IJCSI International Journal of Computer Science Issues, Vol. 6, No. 1, 2009.
- [44] A.A.Abdulfetah, X.Sun, H.Yang, "Robust adaptive video watermarking scheme using visual model in DWT Domain, Information Technology Journal 9(7): ISSN 1812-5638, 2010, pp. 1409-1414.
- [45] S. S. Bedi, Rakesh Ahuja, Himanshu Agarwal, "Copyright Protection using Video Watermarking based on Wavelet Transformation in Multiband", International Journal of Computer Applications (0975 – 8887) Volume 66– No.8, March 2013, pp. 1-5.
- [46] Jason kaufman, Mehmet Celenk, "Digital Video Watermarking using Singular Value Decomposition and 2D principal Component Analysis", IEEE international Conference on Image Processing", 2006, pp 2561-2564.
- [47] Lama rajab, Tahani Al- Khatib and Ali Al haj, "Hybrid DWT-SVD Video Watermarking", Proceeding of IEEE, 2008, pp. 588-592.
- [48] Maher EL'ARBI, Chokri BEN AMARI and Henri NICOLAS2, "Video watermarking based on neural networks", IEEE- 2006, pp.1577-1580.
- [49] Emad E. Abdallah, A. Ben hamza, " Video Watermarking using wavelet transform and tensor algebra", Springer, DOI 10.1007/s 11760-009-0114-7, 2010, pp. 233-245.
- [50] Sanjana Sinha, Prajnat Bardhan, Swarnali Pramanick, Ankul Jagatramka, Dipak K. Kole, Aruna Chakraborty, "Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis", International Journal of Wisdom Based Computing, Vol. 1 (2), August 2011, pp 7-12.
- [51] Tahani Al-Khatib, Ali Al-Haj, Lama Rajab and Hiba Mohammed, "A Robust Video Watermarking Algorithm", Journal of Computer Science 4 (11) 2008, pp. 910-915.
- [52] Satyanarayana Murty. P, K. Venkatesh, Rajesh Kumar "A Semi-Blind Reference Video Watermarking using Hybrid Transforms for Copyright Protection" International Journal of Computer Applications (0975 – 8887) Volume 51– No.9, August 2012, pp. 1-11.
- [53] Fung, C.W.H., W. Godoy, "A new approach of DWT-SVD Video Watermarking", Third International Conference on Computational Intelligence, Modelling and Simulation (CIMSIM), DOI: 10.1109/CIMSIm.2011.48, 2011, pp. 233-236.
- [54] M. Omidyeganeh, H. Khalilian, S. Ghaemmaghami, S. Shirmohammadi, "Robust Digital Video Watermarking in an Orthogonal Parametric Space", Proc. Of IEEE, 2010, pp. 2258-2263.
- [55] Salwa A.K Mostafa, A. S. Tolba , F. M. Abdelkader, Hisham M. Elhindy, "Video Watermarking Scheme Based on Principal Component Analysis and Wavelet Transform", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009, 45.
- [56] Soukim Das, Dr. Monalisa banerjee, "Uncompressed Video Authentication Through a Chip Based Watermarking Scheme", Proc. Of IEEE computer society, 2011, pp. 395-398.

- [57] Hee-Dong Kim, Tae-Woo Oh, Ji-Won and Heung-Kyu Lee, "A hybrid watermarking scheme for CCL-applied video contents", Proc. Of IEEE, 2011, pp. 199-204.
- [58] Ashish M. Kothari, Ved Vyas Dwivedi, "Hybridization of DCT and SVD in the Implementation and Performance Analysis of Video Watermarking", I.J. Image, Graphics and Signal Processing, 2012, 5, pp. 14-20.
- [59] K. Thaiyalnayaki and R. Dhanalakshmi, "A Chaos Encrypted Video Watermarking Scheme For The Enforcement Of Playback Control", International Journal of Advances in Engineering & Technology, July 2012, IJAET, ISSN: 2231-1963, Vol. 4, Issue 1, pp. 165-175.
- [60] Nisreen I. Yassin, Nancy M. Salem and Mohamed I. El Adawy, "Block Based Video Watermarking Scheme Using Wavelet Transform and Principle Component Analysis", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, ISSN (Online):, January 2012, pp. 1694-0814.
- [61] Himanshu Agarwal, Rakesh Ahuja, S.S.Bedi "Highly Robust and Imperceptible Luminance Based Hybrid Digital Video Watermarking Scheme for Ownership Protection", I.J. Image, Graphics and Signal Processing, DOI: 10.5815/ijigsp.2012.11.07,2012, 11, pp. 47-52.
- [62] Ashish M. Kothari, Ved Vyas Dwivedi, "Video Watermarking – Combination of Discrete Wavelet & Cosine Transform to Achieve Extra Robustness", I.J. Image, Graphics and Signal Processing, 2013, 3, pp. 36-41.
- [63] OsamaS.Faragallah, "Efficient Video Watermarking based on Singular Value Decomposition in the Discrete Wavelet Transform Domain", Elsevier, International Journal of Electronics and Communication (07), 2013, pp. 189-196.
- [64] Nisreen I. Yassin, Nancy M. Salem, Mohamed I. El Adawy, "QIM blind video watermarking scheme based on Wavelet transform and principal component analysis", Alexandria Engineering Journal of Elsevier, 53, 2014, pp. 833-842.
- [65] Divjot Kaur Thind, Sonika Jindal, "A Semi Blind DWT-SVD Video Watermarking", International Conference on Information and Communication Technologies (ICICT 2014), Elsevier Proceedings of Computer Science 46, 2015, pp. 1661 – 1667.
- [66] Neeta Deshpande, Archana Rajurkar, R.R. Mathalkar, "Robust dual watermarking scheme for video derived from strategy fusion", I.J. Image, Graphics and Signal Processing in MECS, 5, 2014, pp. 19-27.
- [67] Ta Minh Thanh, Pham Thanh Hiep, Ta Minh Tam, Keisuke Tanaka, "Robust semi-blind video watermarking based on frame-patch matching", International Journal of Electronics and Communications of Elsevier Proceeding, 68, 2014, pp. 1007-1015,
- [68] Shoaib, S. Mahajan, R.C., "Authenticating using secret key in digital video watermarking using 3-level DWT," International Conference on Communication, Information & Computing Technology (ICCICT), doi: 10.1109/ICCICT.2015.7045664,2015, pp.1-5.
- [69] Jianzhong Li; Ping Zhong; Yinghui Zhu; Cai Guo, "Robust wavelet-based watermarking scheme for video copyright protection," *Image and Signal Processing (CISP), 2014 7th International Congress on*, vol., no, 14-16 Oct. 2014, pp.125-129.
- [70] Yuan-Gen Wang, Zhe-Ming Lu, Liang Fan, Yun Zheng, "Robust dual watermarking algorithm for AVSvideo", Elsevier, Signal Processing: Image Communication 24, 2009 pp. 333–344.

### Authors' Profiles



**Rakesh Ahuja**, male, completed his B.Tech in Computer Science & Engineering degree from BIET Jhansi, (U.P) India, M.Tech Degree from Uttar Pradesh Technical University, India. He is currently an Associate Professor at Moradabad Institute of Technology, Moradabad, (U.P) India. He is having total nineteen years of experience in the area of industrial, academic and administration. He is currently pursuing the Ph.D degree from IFTM University, Moradabad (U.P) India. His research interest includes in development schemes of cryptography, information and multimedia security including text, video and image watermarking and Database Management System



**S. S. Bedi**, male, secured B.E degree from Guru Nanak Dev Engineering Collge, Bidar, India, M.Tech Degree from NIT-TTR (An Autonomous Institute Est. by Ministry of HRD, Govt. of India), Chandigarh and Ph.D Degree from IIT, Gwalior, (M.P) India. He is having Twenty years of experience in the area of academics, research and administration at MJPR University, Bareilly (U.P). He is member of various professional societies such as International Association of Engineers-China, Computer Society of India and IEEEUSA. His research interests include Information and Multimedia Security and digital watermarking. He was honoured by Rashtriya Shikshak Ratan Award, AIBDA, New Delhi and also honoured for best paper at World Congress on Engineering, London. U.K.

**How to cite this paper:** Rakesh Ahuja, S. S. Bedi, "All Aspects of Digital Video Watermarking Under an Umbrella", IJIGSP, vol.7, no.12, pp.54-73, 2015.DOI: 10.5815/ijigsp.2015.12.08