Review on Digital Video Watermarking Techniques

Alka N. Potkar
M.E. student (E&TC)
Dr. D.Y. Patil SOE, Pune

Saniya M. Ansari
Asst. Prof (E&TC)
Dr. D.Y. Patil SOE ,Pune

ABSTRACT
Electronic watermarking is a method whereby information can be imperceptibly embedded into electronic media, while ideally being robust against common signal manipulations and intentional attacks to remove the embedded watermark. This study evaluates the characteristics of uncompressed video watermarking techniques in terms of visual characteristics, computational complexity and robustness against attacks and signal manipulations.

The foundations of video watermarking are reviewed, followed by a survey of existing video watermarking techniques. Representative techniques from different watermarking categories are identified, implemented and evaluated.

General Terms
Types of watermarking, Applications, Watermarking techniques, Attacks.

Keywords
Watermark; DWT; DCT

1. INTRODUCTION
Video piracy has become an increasing problem particularly with the proliferation of media sharing through the advancement of Internet services and various storage technologies. Thus, research in copyright protection mechanisms, where one of which includes digital watermarking has been receiving an increasing interest from scientists especially in designing a seamless algorithm for effective implementation. Digital video watermarking involves embedding secret symbols known as watermarks within video data which can be used later for copyright detection purposes. There are three factors (robustness, security, perceptual fidelity) which are necessary for video watermarking system.

The fast growth of internet and applications using digital multimedia technologies has put the accent on the need to provide copyright protection to multimedia data. A digital watermark can be described as a visible or preferably invisible identification code that is permanently embedded in the data. So it can remain present within the cover media after any decoding process.

2. TYPES OF DIGITAL WATERMARK
Watermarks and watermarking techniques can be divided into various categories in various ways. The watermarks can be applied in spatial domain [3]. An alternative to spatial domain watermarking is frequency domain [3][9] watermarking. It has been pointed out that the frequency domain methods are more robust than the spatial domain techniques. Different types of watermarks are shown in the figure1.

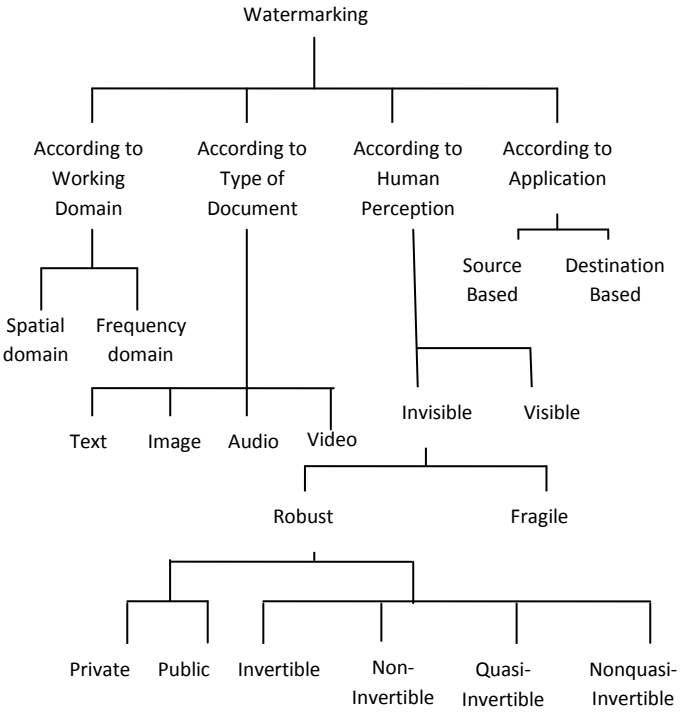

Figure 1: Types of watermarking techniques

Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows.

Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows.

- Image Watermarking
- Video Watermarking
- Audio Watermarking
- Text Watermarking

According to the human perception, the digital watermarks can be dividing into three different types as follows.

- Visible watermark
- Invisible-Robust watermark
- Invisible-Fragile watermark
- Dual watermark

Watermarking is the process of inserting secret information (watermark) into digital multimedia (images, audio and video) by taking into account the limitations of the human perception system. Digital watermarking is the process of embedding digital code into digital multimedia (images, audio and video

sequence). The embedded information or watermark can be a serial number or random number sequence, ownership identifiers, copyright messages, control signals, transaction dates, information about the creators of the work, bi-level or gray level images, text or other digital data formats.

DIGITAL VIDEO WATERMARKING: A complete digital watermarking system should include three basic parts: watermark generation, watermark embedding and watermark extraction or detection. Watermark embedding algorithm uses the symmetric key or public key to make the watermark information embed into the original carrier to get concealed carrier. Block diagram of watermark embedding and extraction is shown in Figure 2:

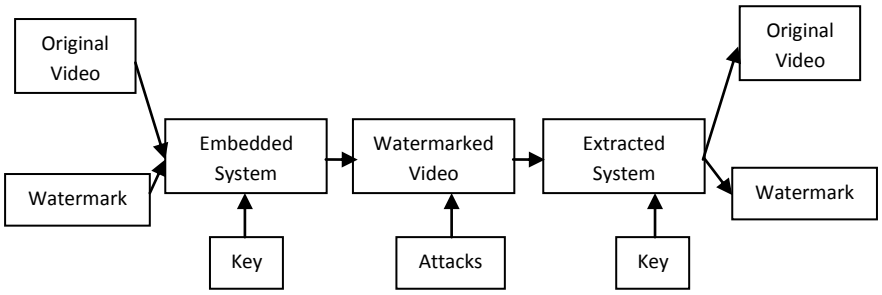

Figure 2: Block diagram of Digital Video Watermarking

3. VIDEO WATERMARKING APPLICATIONS

According to van Huyssteen thesis video watermarking has numerous applications exist, it is possible to group most of these techniques into six main application categories

3.1 Transaction Tracking

Transaction tracking is used to track how content was distributed through a system or transmitted between multiple points. A unique identifier is embedded into the media at the time of playback, which can later be extracted. In the case of illegal distribution of the content, it should ideally be possible to identify the source from where the distribution occurred, possibly identifying the misappropriating party [4].

3.2 Broadcast Monitoring

Broadcast monitoring enables broadcasters or content owners to track or verify the transmission of media in a broadcast system. The watermarks can automatically be extracted to verify if a commercial has successfully been aired or whether a certain segment of material was used in a broadcast. The content is usually watermarked by the content owner, while detection can be done by a monitoring site in the broadcast chain or a third party at the receiving end [4][1].

3.3 Copy Control

Copy control aims to disable the duplication of copyrighted material on devices equipped with special watermark detectors. The watermark is used to indicate copy control information, such as copy_never, copy_once or copy_freely. By implementing watermark extraction and embedding in devices, the user can be allowed or denied permission to duplicate content [4].

3.4 Content Authentication

Content authentication is a method that attempts to ensure the integrity of media by detecting attempted tampering of the original content. At creation, the content is usually watermarked with a semi-fragile watermark, which is designed to be affected by signal transformations. Tampering with the content should destroy or alter this semi-fragile watermark, which could then be used to determine that the content is not authentic [1].

3.5 Ownership Identification

In this application, watermarks can be used to identify the rightful owner or creator of content [34]. After the original content was watermarked, disputed ownership can be resolved by extracting the original watermark. Resolving rightful ownership can, however, be challenging as pirates may also embed their own watermark, in which case it can be difficult to determine which is the original watermark. This is known as an ownership deadlock problem [4][1].

3.6 Fingerprinting

This category is only included for clarity, as there exist at least two definitions of fingerprinting, each with specific characteristics and applications. The first definition of media fingerprinting is "the art, or algorithm, of identifying component characteristics of a source and then reducing it into a fingerprint that can uniquely identify it." These techniques do not add any additional information to the media, but rather generates a compact signature based on the unique properties of the content [4][1].

4. REQUIREMENT FOR EFFECTIVE WATERMARKING

The requirements for a watermarking technique can vary according to the intended application, most watermarks share a common set of requirements. Designing a watermark to satisfy all these requirements can be challenging, therefore it may be necessary to reach a compromise between them.

A properly designed watermarking technique is not only imperceptible to the observer, but should also provide a high data payload. The watermarking technique also needs to be robust to enable the media to undergo signal conversions and small alterations without destroying the watermark.

4.1 Imperceptibility

The artefacts produced by watermark embedding should not degrade the quality of the original content in such a way that it is perceptible to viewers. As discussed earlier, advanced techniques take the properties of the human visual system into account to achieve robustness while maintaining imperceptibility [5].

4.2 Robustness

It is desirable that a watermark must be robust against attacks to such an extent that the quality of watermarked content must be considerably degraded in order to remove a watermark. The watermark should not only be robust against intentional attacks, but also to standard video manipulations such as cropping, scaling and compression [5].

4.3 Data Capacity

The data capacity or payload size of a watermark is an indication of the amount of information that can be embedded with a watermark. The payload size varies with the application, but in general an identifier packet of 64 bits is considered appropriate for most applications

It is necessary to determine the number of bits that a watermarking technique can embed and how many useful information bits this results in if error correction techniques are applied [5].

4.4 Security

The watermarking technique should adhere to Kerckhoffs's principle, which states that a crypto-system must be secure even if the attacker knows everything about the system, but does not have the correct key. Therefore, even if an attacker has access to the exact algorithm used for watermarking and knows that a watermark is present, he or she must be unable to detect or decrypt the data in a reasonable amount of time [5].

4.5 Cascadability

Different watermarks may already be applied to the content by the time the content tracking watermark is inserted. It is desirable for the watermarks to co-exist in media without affecting the performance of the watermarking extraction processes [5].

4.6 Low error probability

It is desirable to ensure that a watermark payload can be extracted with high confidence and minimum error. Two types of errors can occur, namely a detection error and payload recovery error. A detection error refers to the case where a watermark is detected, but one is not present (false alarm). The second case is where a watermark exists, but is not detected (false negative). A payload recovery error refers to a case where a watermark is correctly detected, but the payload incorrectly extracted [5].

5. ATTACKS ON VIDEO WATERMARKS

A successful attack on a watermarking technique refers to a case where the watermark has been removed or modified to prevent successful extraction, without degrading the quality of the watermarked content significantly. A successful attack on a watermark does not necessarily mean that the content was restored to the original, unwatermarked state, but instead that the watermark detection and extraction processes were defeated. A summary of common attacks is shown in Figure 3. These can be grouped into two main categories, namely intentional and unintentional attacks [1]. Intentional attacks are deliberate attempts to prevent successful extraction of embedded watermarks. Unintentional attacks, on the other hand, are caused by normal signal conversions and compression that may be introduced in a distribution chain. Normal signal conversion operations to which a video watermark should be robust include:

- analog to digital (A/D) and digital to analog (D/A) conversion;
- scaling and cropping operations;
- aspect-ratio conversion;
- frame rate conversion;
- quantisation;
- noise addition; and
- compression.

Intentional attacks that are common to video watermarking techniques are now discussed.

5.1 Geometrical Attacks

In this category of attacks, minor geometric distortions are applied to video frames in an attempt to de-synchronise the watermark extraction process with the embedded watermark. These attacks include simple transforms like rotation, scaling and spatial shifting. Geometrical attacks usually alter every frame of a video sequence, which are referred to as single-frame attacks [5]. Artefacts induced by these attacks can be perceptually negligible, while succeeding in defeating the watermarking scheme.

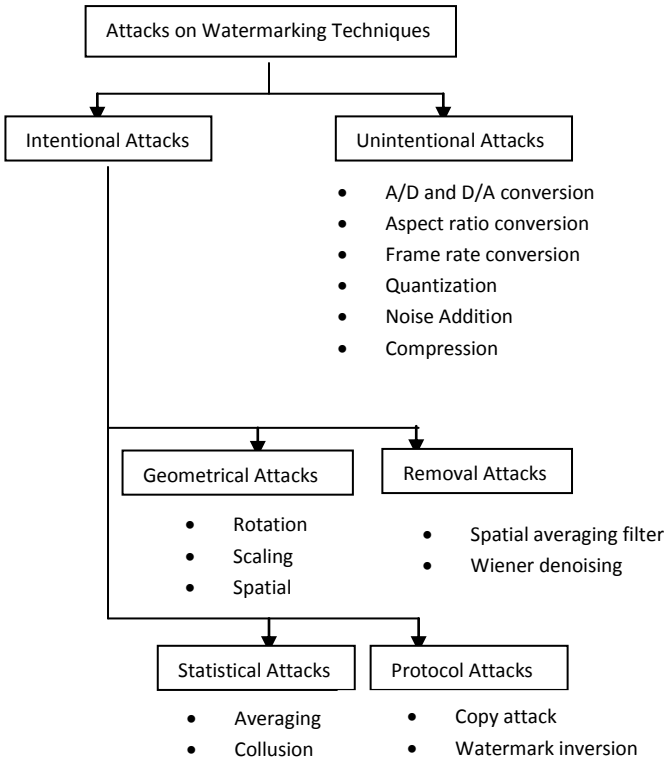

Figure 3: A summary of common attacks that may defeat watermarking techniques.

5.2 Removal Attacks

Removal attacks aim to remove the watermark embedded in the content, usually through filtering. The most basic approach is a spatial averaging filter, while a more advanced denoising technique is the Wiener denoising filter.

5.3 Statistical Attacks

Statistical attacks take advantage of the temporal redundancy in video sequences in order to remove the watermark. It is important to note that, although still image watermarking

techniques can be applied to video sequences, video watermarking poses some unique challenges not necessarily applicable to image or audio watermarking. Because of the inherently redundant data between frames in a watermarked video sequence, watermarking techniques are susceptible to attacks such as frame averaging, frame swapping and statistical analysis

5.4 Protocol attacks

Protocol attacks do not focus on removing or destroying watermarks, but rather on attacking the application for which the watermark is used. An example of this is the copy attack, where a watermark is copied from one image to another without any information about the watermarking technology used. It follows that if a scheme is not resistant to the copy attack, watermarks used for verification cannot be trusted, as it may have been copied from another source. Another example of a protocol attack is the watermark inversion attack.

6. VIDEO WATERMARKING TECHNIQUES

Video watermarking introduces some issues not present in image watermarking. Due to large amounts of data and inherent redundancy between frames, video signals are highly susceptible to pirate attacks, including frame averaging, frame dropping, frame swapping, statistical analysis, etc. Applying a fixed image watermark to each frame in the video leads to problems of maintaining statistical and perceptual invisibility. Applying independent watermarks to each frame is also a problem. Regions in each video frame with little or no motion remain the same frame after frame.

The watermarking techniques found in the literature can mostly be grouped into six main categories which are now reviewed.

6.1 Spatial Domain Watermarking

Spatial Domain (SD) or spread-spectrum techniques refer to a method of watermark embedding and extraction that is performed in the spatial domain, without the need to apply mathematical transforms on the original content. The watermarks are usually encoded to form a noise-like sequence and then added to the original content, while extraction is usually performed with a correlation-based receiver. Since no mathematical transforms are required, these techniques are relatively computationally efficient. This is advantageous in real-time applications or where resources available for embedding are limited.

6.2 Discrete Fourier Transform Watermarking

Discrete Fourier Transform (DFT) techniques take advantage of properties of the DFT to gain robustness against attacks such as spatial and temporal shifts. In order to embed the watermark [3], a DFT is performed on the original content after which the watermark is embedded by modifying elements in the frequency domain. After the watermark is embedded, an inverse DFT is performed to obtain the watermarked content.

6.3 Singular Value Decomposition Watermarking

The Singular Value Decomposition (SVD) is a technique that can be used in image compression techniques, but can also be applied to watermarking. The SVD is performed, after which the singular values are usually modified to embed the watermark. A pseudo-inverse SVD is then applied to obtain the original content. The SVD can be used on its own for watermarking, but is also often used in hybrid techniques such as [94] which combines the SVD and the discrete cosine transform. The SVD is relatively computationally complex, but by applying it in hybrid techniques it may not be necessary to perform an SVD on the entire image, lowering the computational complexity.

6.4 Discrete Wavelet Transform Watermarking

In this watermarking scheme, the watermark is decomposed into different parts and embedded in the corresponding frames of different scenes in the video. As identical watermark is used within each motionless scene and independent watermarks are used for successive different scenes, the proposed method is robust against the attack of frame dropping, averaging, swapping, and lossy compression.

Video is divided into different scenes by scene change detection and each frame is transformed to wavelet domain before watermark is embedded. And the watermark needs to be preprocessed, being cropped crop into different parts.

6.4 Discrete Wavelet Transform

This watermark scheme is based on 4 levels Discrete Wavelet Transform (DWT). All frames in the video are normalized to 256 X 256 pixel size. Normalization will be perform in both insertion and detection phase; this can make the watermark to be robust to resizing of the video frame [13].

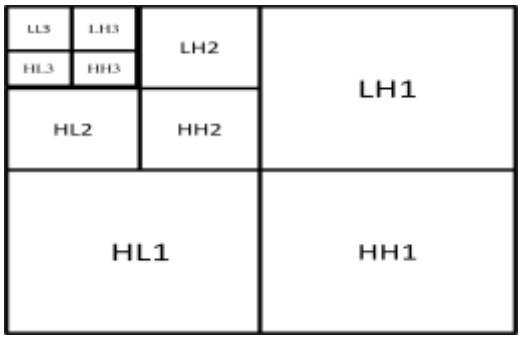

Figure 4: 3-level DWT

The scheme is robust against format conversions because the watermark is inserted before compression. Otherwise, the drawback of the techniques is that, since the code is directly embedded into the compressed stream such as mpeg-4, the copyright information is lost if the video file is converted to a different compression standard, such as mpeg-2 [3].

6.5 Discrete Cosine Transform Watermarking

Discrete Cosine Transform (DCT) techniques are often used to watermark compressed video streams. DCT coefficients in video streams can be modified without having to first uncompress the video or compress it again after watermarking.

7. RELATED WORK

In order to provide imperceptibility and robustness of video watermarking many researchers has performed analysis on it using different watermarking algorithm like DCT DWT on hardware and software. Watermarking has tremendous range of applications in variety of fields as discuss above.

According to Lijing Zhang,Aihua Li [21], Discrete Wavelet Transform (DWT) is a transform based on frequency domain. Figure 3 shown the distribution of the frequency is transformed in each step of DWT, where L represents Low

frequency, H represents High frequency and subscript behind them represents the number of layers of transforms. Sub graph LL represents the lower resolution approximation of the original video, while high-frequency and mid-frequency details sub graph LH, HL and HH represents vertical edge, horizontal edge and diagonal edge details. The process can be repeated to compute the multiple scale wavelet decomposition as shown in figure 4.

According to Lu Jianfeng, Yang Zhenhua, Yang Fan, Li li [22], Discrete Cosine Transform (DCT) is a classic and quite an important method for video watermarking. A lot of digital video watermarking algorithms embed the watermark into this domain. The usability of this transform is because that most of the video compression standards are based on DCT and some other related transforms. In this domain some DCT coefficients of the video are selected and divided into groups, and then the watermark bits are embedded by doing adjustment in each group.

Comparative study of different papers is discussed in table1 below.

Table1. Comparative study of different video watermarking technique

Sr. No	Proposed Paper	Authors	Methodologies Used	Highlights Of Research
1.	Hardware Implementation of a Digital Watermarking System for Video Authentication[17]	Sonjoy Deb Roy, Xin Li, Yonatan Shoshan, Alexander Fish(2013)	It works in the discrete cosine transform (DCT) domain	The proposed hardware based watermarking system features low power consumption, low cost implementation, high processing speed, and reliability
2.	Implementation and performance analysis of DCT-DWT-SVD based watermarkingalgorithms for color images[18]	Nidhi Divecha, Dr. N. N. Jani (2013)	Apply two different watermarking schemes based on DCT-DWT-SVD	Check effectiveness of both techniques for Imperceptibility and robustness PSNR and NCC parameters are used
3.	A Digital Video Watermarking Technique Based on Identical Frame Extraction in 3-Level DWT [19]	Tamanna Tabassum, S.M.Mohidul Islam (2012)	3-Level Discrete Wavelet Transform (DWT)	Strong robustness against some common attacks such as cropping, Gaussian noise adding, Salt & pepper noise adding, frame dropping and frame adding
4.	A Robust Scheme for Digital Video Watermarking based on Scrambling of Watermark [20]	Mahesh R. Sanghavi, Dr. Mrs. Archana M. Rajurkar, Prof. Dr. Rajeev Mathur ,Kainjan S. Kotecha(2011)	The frames are decomposed in 4-level sub-band by separable two-dimensional (2D) wavelet transform	Provides a solution by applying the scene change detection algorithm with video watermarking scheme, to make the scheme robust against various video attacks like frame dropping.
5.	Combined DWT-DCT Digital Image Watermarking[12]	Ali Al-Haj (2007)	frequency-domain watermarking, Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) is used	Imperceptibility and robustness of the system is calculated based on PSNR values.

8. CONCLUSION

In this paper we surveyed the current literature on digital video watermarking. We classified watermarking technique based on the transform domain in which the watermark is embedded. We also tried to classify the digital watermarking in all the known aspects. We have studied different attacks that can apply to watermark.

Future scope of the video watermarking is very broad. Video watermarking avoids video piracy in broadcast video monitoring. Previously using SVD watermarking is done which is less efficient but recently DWT & DCT techniques are used which will increase the robustness of the system. Now a day's data hacking is very serious problem on internet services that can be avoided using different watermarking techniques.

9. ACKNOWLEDGMENTS

My sincere thanks to my honorable guide Prof. Saniya M.Ansari and others those who have contributed towards the preparation of paper.

10. REFERENCES

[1] Prabhishek Singh, R S Chadha "A Survey of Digital Watermarking Techniques, Applications and Attacks" International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013, pg no.165-175

[2] Vidyasagar M. Potdar, Song Han, Elizabeth Chang "A Survey of Digital Image Watermarking Techniques" 3rd International Conference on Industrial Informatics(INDIN 2005)

[3] Ankita A. Hood "A Review on Video Watermarking and Its Robust Techniques" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 1, Januaryr- 2013 ISSN: 2278-0181, page no.1-6

[4] Amit Singh, Susheel Jain, Anurag Jain "A Survay: Digital Video Watermarking" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013 ISSN 2229-5518 page no. 1261- 1265

[5] Farooq Husain"A Survey of Digital Vatermarking Techniques for multimedia data", MIT International Journal of Electronics and communication Engineering, Vol 2,No.1, Jan 2012 PP.(37-43) ISSN 2230-7672

[6] Harleen Kaur "STUDY ON AUDIO AND VIDEO WATERMARKING", International Journal of Communication Network Security ISSN: 2231 – 1882, Volume-2, Issue-1, 2013, PP-34-38.

[7] Charu Kavadia, Vishal Shrivastava "A Literature Review on Water Marking Techniques", International Journal of Scientific Engineering and Technology, 01 Oct. 2012, Volume No.1, Issue No.4, (ISSN : 2277-1581), pp : 08-11.

[8] Mei Jiansheng, Li Sukang and Tan Xiaomei "A Digital Watermarking Algorithm Based On DCT and DWT" Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107

[9] Gopika V Mane, G. G. Chiddarwar "Review Paper on Video Watermarking Techniques" International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013, ISSN 2250-3153 pg no.1-5

[10] Prof. N. R. Bamane, Dr. Mrs. S. B. Patil "Comparison & Performance Analysis of different Digital Video Watermarking Techniques" International Journal of Scientific & Engineering Research Volume 4, Issue 1, January-2013 ISSN 2229-5518 pg no.1-6

[11] Nikita Kashyap, G. R. SINHA "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)" I.J. Modern Education and Computer Science, 2012, 3, 50-56

[12] Ali Al-Haj **"**Combined DWT-DCT Digital Image Watermarking" Journal of Computer Science 3 (9): 740-746, 2007 ISSN 1549-3636 pg no. 740-746

[13] Tamanna Tabassum, S.M. Mohidul Islam "A Digital Video Watermarking Technique Based on Identical Frame Extraction in 3-Level DWT" 978-1-4673-4836-2/12/©2012 IEEE pg no.101-106

[14] Anilkumar Katharotiya, Swati Patel and Mahesh Goyani "Comparative Analysis between DCT & DWT Techniques of Image Compression", Journal of Information Engineering and Applications, ISSN 2224-5758 (print) ISSN 2224-896X (online) Vol 1, No.2, 2011,PP-9-17

[15] A.M.Kothari, A.C.Suthar, R.S.Gajre. "Performance Analysis of Digital Image watermarking Technique-Combined DWT-DCT over individual DWT" Published in International Journal of Advanced Engineering & Applications,Jan2010.

[16] Syed Ali Khayam "The Discrete Cosine Transform (DCT):Theory and Application", Department of Electrical & Computer Engineering Michigan State University *March 10th 2003.*

[17] Sonjoy Deb Roy, Xin Li, Yonatan Shoshan, Alexander Fish and Orly Yadid-Pecht "Hardware Implementation of a Digital Watermarking System for Video Authentication", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 23, NO. 2, FEBRUARY 2013, Pg-289-301

[18] Nidhi Divecha and Dr. N. N. Jani "Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color images", 2013 International Conference on Intelligent Systems and Signal Processing (ISSP), 2013 IEEE, PP-204-208

[19] Tamanna Tabassum, S.M. Mohidul Islam "A Digital Video Watermarking Technique Based on Identical Frame Extraction in 3-Level DWT" in 2012 IEEE, PP-101-106

[20] Mahesh R. Sanghavi, Dr. Mrs. Archana M. Rajurkar, 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*

[21] Lijing Zhang,Aihua Li, "A Study on Video Watermark Based-on Discrete Wavelet Transform and Genetic Algorithm", 2009 First International Workshop on Education Technology and Computer Science, 374-377.

[22] Lu Jianfeng, Yang Zhenhua, Yang Fan, Li li, "A MPEG2 Video Watermarking Algorithm Based on DCT Domain", 2011 Workshop on Digital Media and Digital Content Management, 194-197.