UACEE International Journal of Advances in Computer Science and its Applications – IJCSIA
Volume 3 : Issue 2 [ISSN 2250 – 3765]
Publication Date : 05 June 2013

Significance Research Review on Real Time Digital Video Watermarking System for Video Authentication

Mr. Ashish S. Bhaisare
Department of Electronics and Telecommunication,
SSBT's COET, Bambhori, Jalgaon
Email: bhaisare.ashish@gmail.com,ashish.bhaisare@gmail.com

Prof. A. H. Karode
Department of Electronics and Telecommunication,
SSBT's COET, Bambhori,
Jalgaon , Maharashtra
Email: atil_karode@rediffmail.com

Prof. S. R. Suralkar
H.O.D Department of Electronics and Telecommunication
SSBT's COET, Bambhori,
Jalgaon , Maharashtra

----------ABSTRACT----------
The main objective of this paper is to describe an efficient hardware-based concept of a digital video WM system which features low power consumption, efficient and low cost implementation, high processing speed, reliability and invisible, semi-fragile watermarking in compressed video streams. The presented WM system can be integrated with video compressor unit and it achieves performance that matches complex software algorithms within a simple efficient hardware implementation. The system also features minimum video quality degradation and can withstand certain potential attacks i.e. cover-up attack, cropping, segment removal on video sequences. The proposed WM system is implemented using Verilog hardware description language (HDL) synthesized into a field programming gate array (FPGA) and then experimented using a custom versatile breadboard for performance evaluation is describe through various research papers which give a vital review related to digital video watermarking system for video authentication .

Keywords:- Complex software algorithms, Semi-fragile watermarking, FPGA,VHDL

I. INTRODUCTION

Now a days, digital video WM techniques are widely used in various video applications [2]-[4]. For video authentication, WM can ensure that the original content has not been altered. WM is used in fingerprinting to track back a malicious user and also in a copy control system with WM capability to prevent unauthorized copying [1], [3]. Because of its commercial potential applications, current digital WM techniques have focused on multimedia data and in particular on video contents. Over the past few years, researchers have investigated the embedding process of visible or invisible digital watermarks into raw digital video [3], uncompressed digital video both on software [3]-[5] and hardware platforms [4]-[7]. Contrary to still image WM techniques, new problems and new challenges have emerged in video WM applications.

In prior research [6,7,8] a real-time watermarking embedder-detector for a broadcast monitoring system is presented in the context of a VLIW DSP processor. The insertion mechanism involves addition of pseudo-random numbers to the incoming video stream based on the luminance value of each frame. The watermark detection process involves the calculation of correlation values. In [9], the Millennium watermarking system is presented for copyright protection of DVD video in which specific issues, such as watermark detector location and copy generation control, are addressed. In [8], a VLSI architecture for a spread spectrum based real-time watermarking system is presented. In [9], the graphics processing unit (GPU) is utilized for hardware assisted real-time watermarking.

The existing literature is rich with watermarking algorithms introduced for deferent types of multimedia objects, such as images, video, audio, and text, and their software implementations. These watermarking algorithms primarily work off-line, i.e., the multimedia objects are first acquired, and then the watermarks are inserted before the watermarked multimedia objects are made available to the user. In this approach there is a time gap between the multimedia capture and its transmission. The objective of this paper is to present research which will lead to a hardware-based watermarking system to bridge that gap
[1, 4, 6, 7, 8, 9]. The watermarking chip will be integrated into the electronic appliance which is an embedded system designed using system-on-chip (SoC) technology.

II. Watermark Implementations System : Hardware vs. Software

A WM system can be implemented on either software or hardware platforms, or some combinations of the two. In software implementation, the WM scheme can simply be implemented in a PC environment. The WM algorithm's operations can be performed as machine code software running on an embedded processor. By programming the code and making use of available software tools, it can be easy to design and implement any WM algorithm at various level of complexity. Over the last decade, numerous software implementations of WM algorithms for relatively low data rate signals (like audio and image data) have been invented [3]-[5]. While the software approach has the advantage of flexibility, computational limitations may arise when attempting to utilize these WM methods for video signals or in portable devices. Therefore, there is a strong incentive to apply hardware-based implementation for real-time WM of video streams [8]. The hardware-level design offers several distinct advantages over the software implementation in terms of low power consumption, reduced area and reliability. It enables the addition of a tiny, fast and potentially cheap watermark embedder as a part of portable consumer electronic devices. Such devices can be a digital camera, camcorder or other multimedia devices, where the multimedia data are watermarked at the origin.

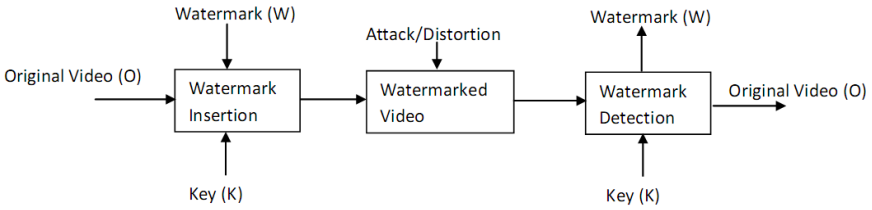

Fig. 1 : Block diagram of a proposed video WM

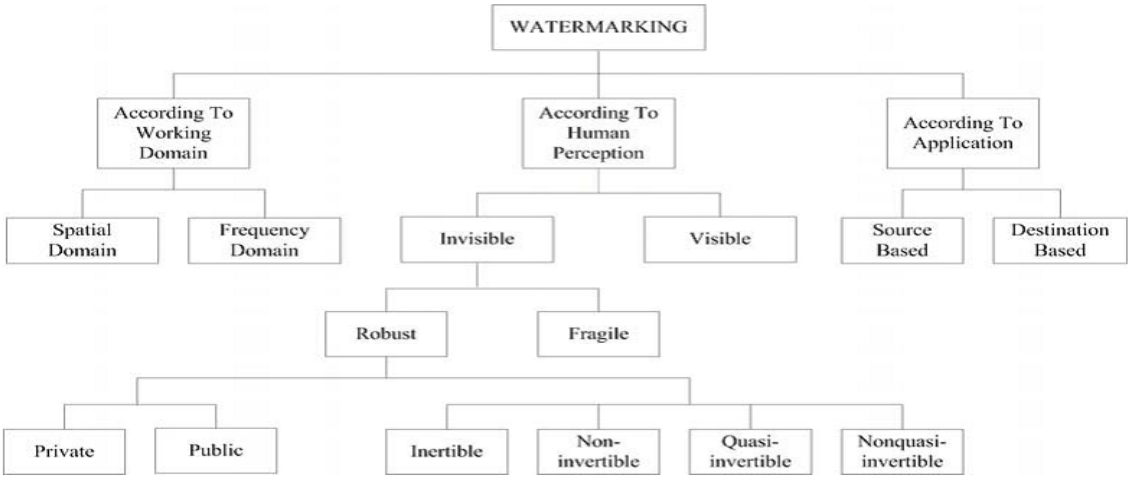

Figure 2 : General classification of existing watermarking

On the other hand, hardware implementations of WM techniques require flexibility in the implementation of both computational and design complexity.

The algorithm must be carefully designed to minimize any susceptibility as well as maintaining a sufficient level of security.

III. DIGITAL VIDEO WATERMARKING SYSTEM

Digital watermarking is nothing but a digital code embedded into digital cover content e.g. text, image, audio and in our case video sequence. [17][18] A watermark can be any random or serial number, ownership identifier, information about the creator, date etc.[17] It can carry any unlimited information, but as more information watermark carry, the original information will be more vulnerable. So the amount of watermark must be limited by the size of an original message, here video sequence. As watermark prefers to robustness, it carries tens to thousands bits per one video frame. [19]

A. The principle of video watermark :

The complete process of digital video watermarking is described into four steps: Watermark insertion or embedding, Watermark transmission or distribution through a channel, Watermark extraction or detection and Watermark decision (Figure 1). Watermark embedding algorithm embedded a watermark into original video using a Key, which may be either public or symmetric key. Then the watermarked video transmitted over the channel. At the receiver side, watermark detection/extraction algorithm used to detect a watermark. In last step, watermark decision, watermarking system analyzes the extracted data. [20]

B. Pro pert

ark some most important characteristics or properties of watermarking process are required.[17][18] [21] Such as,

(i) *Robustness:*
The watermark should be impossible to remove from watermarked video, without the sufficient knowledge of an embedding process. The robust one is specially designed to withstand a wide range of attacks. [22]

(ii) *Imperceptibility:*
The watermark embedded into the digital video sequence should be invisible to Human Vision System (HVS).

(iii) *Unambiguous:*
The extracted watermark should uniquely identify the original owner of the video.

(iv) *Loyalty:*
A watermark has a high reliability, if the degradation it causes is very difficult to perceive for the viewer.

(v) *Computational Cost:*
Digital video watermark system includes, embedding and detecting process both should be fairly fast and should have low computational complexity.

(vi) *Interoperability:*
Watermark system must be interoperable for the compressed and decompressed operations.

(vii) *CBR (Constant Bit Rate):*
In the bit stream domain, watermarking should not increase the bit rate.

(viii) *Random detection:*
In video watermarking the detection of watermark can be done in any position of video.

(ix) *Blind detection scheme:*
Non-blind detection scheme require the original data, but for video sequence it is very inconvenient to use original data because of its huge content compare to image. While a blind detection scheme doesn't require a original data, so it is useful for video watermarking.

C. Classification Of Digital Video Watermarking

WM techniques can be divided into different categories according to various criterions [23]. The general classification of the currently available watermarks is shown in Figure 2. In [24] we have presented a decomposition of the variety of existing watermarks for still images and showed their features and possible applications, benefits and drawbacks watermarking.

Since a video stream is regarded as a three-dimensional signal with two dimensions in space (called m x n frame) and one dimension in time, we can consider a video stream as a succession of still images. Therefore, most image WM techniques are equally applicable to video if the individual frames are treated as images [25]. However, contradictory to still image WM techniques, the video WM methods usually require that the WM encoding and decoding are processed in real time. According to the domain in which video WM is performed, WM processing methods can be classified into two categories: spatial domain and frequency domain. In the spatial domain, directly applying minor changes to the values of the pixels in a minor way is mainly used. This technique makes the embedded information hardly noticeable to the human eye. For example, pseudo-random WM works by a simple addition of a small amplitude pseudo-noise signal to the original media data. In the frequency domain, the object first goes through a certain transformation, DCT or discrete wavelet transforms (DWT), the WM is embedded in the transform coefficients and then it is inversely transformed to receive the watermarked data. The frequency domain methods are more robust than the spatial domain techniques [23].

IV. PROCEDURE FOR DIGITAL VIDEO WATERMARKING SYSTEM

In this section, a detailed description of the hardware architecture of the proposed digital video WM system is provided. Fig. 3 illustrates the general block diagram of the proposed system which is comprised of four main modules: a video camera, video compression unit, watermark generation and watermark embedding units. The watermark embedding approach is designed to be performed in the DCT domain. This holds several advantages. DCT is used in the most popular stills and video compression formats including JPEG, MPEG, H.26x. This allows the integration of both watermarking and compression into a single system. Compression is divided into three elementary phases: DCT transformation, quantization and Huffman encoding. Embedding the watermark after quantization makes the watermark robust to the DCT compression with a quantization of equal or lower degree used during the watermarking process. Another advantage of this approach is that in image or video compression the image or frames are first divided into 8x8 blocks. By embedding the WM specifically to each 8x8 block, tamper localization and better detection ratios are achieved [9].

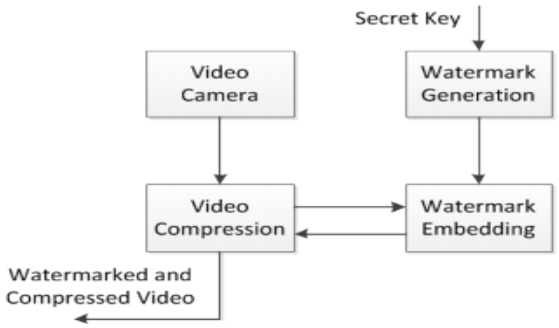

Fig 3. The general block diagram of proposed Video WM system

Each of the video frames undergoes 8x8 block DCT and quantization. Then they are passed to the watermark embedding module. The watermark generation unit produces a specific watermark data for each video frame, based upon initial predefined secret keys. The watermark embedding module inserts the watermark data into the quantized DCT coefficients for each video frame according to the algorithm detailed below. Finally, watermarked DCT coefficients of each video frame are encoded by the video compression unit which outputs the compressed frame with embedded authentication watermark data.

V. THE PROPOSED WM ALGORITHM

The proposed WM algorithm along with MPEG-2 video

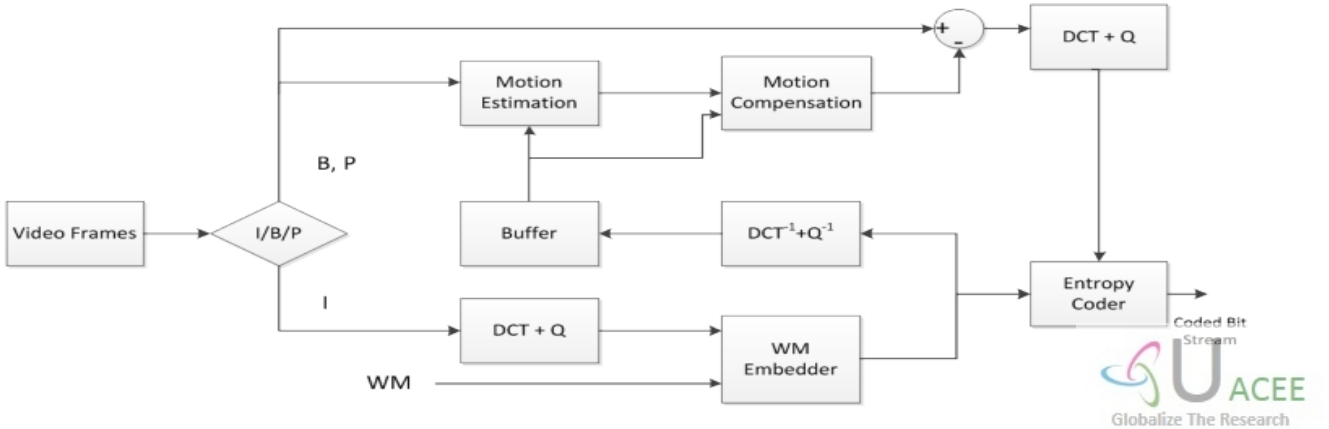

Fig 4. The Dataflow of the proposed WM System

as following: encoding standard is presented as a dataflow in Fig. 4. This can be described as following :

1. Split I frame and watermark data into 8 × 8 blocks.
2. For each 8 × 8 block (Both Watermark Data and I frame), perform DCT, quantization and zig-zag-scan to generate quantized DCT coefficients.
3. Identify N watermarkable cells for each block and calculate the modification value for each selected cell.
4. Modify the identified watemarkable DCT coefficients according to the modification values.
5. Perform inverse DCT and inverse quantization for each 8 × 8 block watermarked coefficients to reconstruct the original I pixel values.
6. Buffer the reconstructed watermarked I frame.
7. Perform motion estimation for B/P frames to obtain the motion vector.
8. Using the motion vector and reconstructed watermarked I frame motion compensation is done.
9. Difference between the motion-compensated prediction frame and the watermarked reference frame I is the prediction error.
10. Perform DCT, quantization and zig-zag-scan on the prediction error.
11. Perform entropy coding for the blocks of the different frames.
12. Generate compressed and watermark embedded video steam.
13. To avoid heavy computationally demanding operations and to simplify the hardware implementation, watermarking can be done with MJPEG standard video compressing unit.

Since watermark is only embedded on I frames, the steps stated above will be the same for the MJPEG video standard except for the motion estimation and motion compensation.

V. APPLICATIONS OF VIDEO WM

This section is consequently dedicated to the presentation of various applications in which digital WM can bring a valuable support in the context of video data. The following main watermarking applications are considered in the open literature and as commercial applications [1]. The reader is referred to [1]&[26] for a more thorough

Table 1 Video WM: Applications and Purposes

Applications	Purpose
Copyright protection	Proof of ownership
Video authentication	Insure that the original content has not been altered
Fingerprinting	Trace back a malicious user
Copy control	Prevent unauthorized copying
Broadcast monitoring	Identify the video item being broadcasted

ivestigation. The applications presented have been gathered in table 1.

Copyright protection: For the protection of intellectual property, the video data owner can embed a watermark representing copyright information in his data. This watermark can prove his ownership in court when someone has infringed on his copyrights. For instance, embedding the original video clip by noninvertible WM algorithms during the verification procedure happens to prevent the multiple ownership problems in some cases.

Video authentication: Popular video editing software permit today to easily tamper with video content and therefore it is not reliable anymore. Authentication techniques are consequently needed in order to ensure the authenticity of the content. One solution is the use of digital WM. In Figure 5, a sketch of a simple video

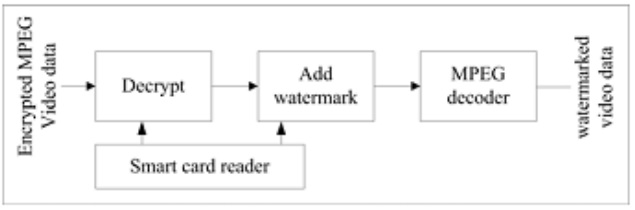

Figure 5:WM-based authentication for automatic VS

surveillance (VS) system, in which WM is used to authenticate VS data, is given [14], [15]. Timestamp, camera ID and frame serial number are used as a watermark, embedded into every single frame of the video stream. The central unit is in charge of analyzing the watermarked sequences and generating an alarm whenever a suspicious situation is detected, and then may either be sent to the security service or compressed for storage. When needed, the stored video sequence can be used as a proof in front of a court of law. It is possible to reflect any manipulation by detecting the watermarks.

Video fingerprinting: To trace the source of illegal copies, a fingerprinting technique can be used. In this application, the video data owner can embed different watermarks in the copies of the data that are supplied to different customers. Fingerprinting can be compared to embedding a serial number that is related to the customer's identity in the data. It enables the intellectual property owner to identify customers who have broken their license agreement by supplying the data to third parties.
A consumer can receive digital services, like pay TV, by cable using a set-top box and a smart card, which he has to buy and can therefore be related to his identity. To prevent other non-paying consumers from making use of the same service, the provider encrypts the video data and this protects the service during transmission. The set-top box of the consumer, who paid for the service, decrypts the data only if a valid smart card is used. Then, a watermark, representing the identity of the user, is added to the compressed video. The watermarked (fingerprinted) data can now be fed to the internal video decoder to view

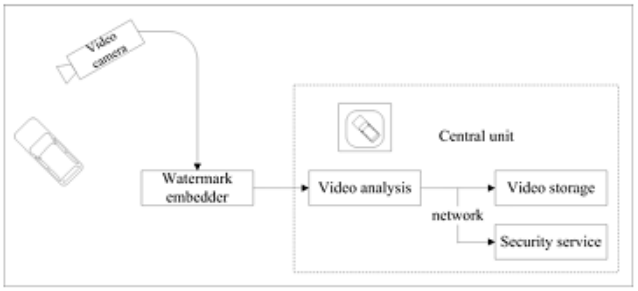

Figure 6: Set-top box with WM

the video. A set-top box with WM capabilities is depicted in Figure 6.Copy control: The information stored in a watermark can directly control digital recording devices for copy protection purposes. In this case, the watermark represents a copy-prohibit bit and watermark detectors in the recorder determine whether the data offered to the recorder may be stored or not. For example, in the copy

protection scheme using WM techniques shown in Figure 7, consumers can make copies of any original source, but they cannot make copies of copies. This copy Protection system checks all incoming video streams for a

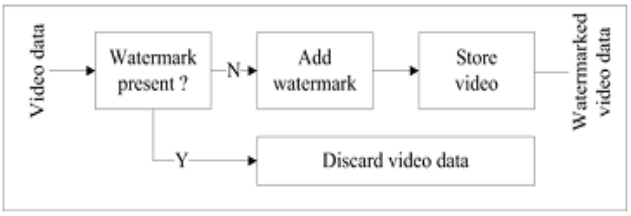

Figure 7: Video recorder with copy protection.

Predefined copy-prohibit watermark. If such a watermark is found, the incoming video has already been copied before and is therefore refused by the recorder. If the copy-prohibit watermark is not found, the watermark is embedded and the watermarked video is stored. This means that video data stored on this recorder always contains a watermark and cannot be duplicated if the recorder is equipped with such a copy protection system.

Broadcast monitoring: By embedding watermarks in commercial advertisements an automated monitoring system can verify whether advertisements are broadcasted as contracted. Not only commercials but also valuable TV products can be protected by broadcast monitoring. News items can have a value of over 100.000 USD per hour, which makes them very vulnerable to intellectual property rights violation. A broadcast surveillance system can check all broadcast channels and charge the TV stations according to their findings.

REFERENCES

[1] A. D. Gwenael, and J. L. Dugelay, "A guide tour of video watermarking," Signal Process. Image Communication.,vol. 18, no.4, pp. 263–282, Apr. 2003.

[2] Y. Shoshan, A. Fish, X. Li, G. A. Jullien, and O. Yadid-Pecht, "VLSI watermark implementations and applications," International Journal on Information Technologies and Knowledge, vol. 2, no. 4 pp. 379–386, June 2008.

[3] S. P. Mohanty, "Digital watermarking: a tutorial review," Dept. of Computer Eng., Univ. South Florida, 1999.

[4] A. Shan, and E. Salari, "Real-time digital video watermarking," 2002 Digest of Technical Papers: International Conference on Consumer Electronics, June 2002, pp. 12 – 13.

[5] L. Qiao, and K. Nahrstedt, "Watermarking methods for MPEG encoded video: towards resolving rightful ownership," in Proc. IEEE Int. Conf. Multimedia Computing and Systems, June 1998, pp. 276–285.

[6] L. D. Strycker, P. Termont, J. Vandewege, J. Haitsma, A. Kalker, M. Maes, and G. Depovere, "Implementation of a real-time digital watermarking process for broadcast monitoring on Trimedia VLIW processor," Proc. Inst. Elect. Eng. Vision, Image Signal Proc. , vol. 147, no. 4, pp. 371–376, Aug. 2000.

[7] L. D. Strycker, P. Termont, J. Vandewege, J. Haitsma, A. Kalker, M. Maes, G. Depovere, An Implementation of a Real-time Digital Watermarking Process for Broadcast Monitoring on a Trimedia VLIW Processor, in: Proceedings of the IEE International Conference on Image Precessing and Its Applications (Vol. 2), 1999, pp. 775–779.

[8] M. Maes, T. Kalker, J. P. M. G. Linnartz, J. Talstra, G. F. G. Depovere, J. Haitsma, Digital Watamarking for DVD Video Copyright Protection, IEEE Signal Processing Magazine 17 (5) (2000) 47–57

[9] N. J. Mathai, A. Sheikholesami, and D. Kundur, "Hardware implementation perspectives of digital video watermarking algorithms", IEEE Trans. Signal Process, vol. 51, no. 4, pp. 925 – 938, Apr. 2003.

[10] N. J. Mathai, A. Sheikholesami, and D. Kundur, "VLSI implementation of a real-time video watermark embedder and detector," Pro. Intl. Symposium on Circuits and Systems, vol. 2, pp. 772–775, May 2003.

[11] T. H. Tsai, and C. Y. Wu, "An implementation of configurable digital watermarking systems in MPEG video encoder," in Proc. of Intl. Conf. on Consumer Electronics, pp. 216–217, Jun. 2003.

[12] M. Maes, T. Kalker, J. P. Linnartz, J. Talstra, G. Depoyere, and J. Haitsma, "Digital watermarking for DVD video copy protection," IEEE Signal Process. Mag., vol. 17, no. 5, pp. 47–57, Sep. 2000.

[13] Y.-J. Jeong, K.-S. Moon, J.-N. Kim, "Implementation of Real Time Video Watermark Embedder Based on Haar Wavelet Transform Using FPGA", in proceedings of the Second International Conference on Future Generation Communication and Networking Symposia (FGCNS), 2008, pp. 63 – 66.

[14] G. Petitjean, J. L. Dugelay, S. Gabriele, C. Rey, J. Nicolai, "Towards Realtime Video Watermarking for Systems-On-Chip", in Proceedings of the IEEE International Conference on Multimedia and Expo (Vol. 1), 2002, pp. 597–600.

[15] S. P. Mohanty, "A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management", Journal of Systems Architecture, Volume 55, Issues 10-12,October-December 2009, pp. 468-480.

[16] S. P. Mohanty and E. Kougianos, "Real-Time Perceptual Watermarking Architectures for Video Broadcasting", Journal of Systems and Software, Vol. 84, No. 5, May 2011, pp. 724-738.

[17] Sourav Bhattacharya, T. Chattopadhyay and Arpan Pal, "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC".

[18] Vivek Kumar Agrawal, "Perceptual watermarking of digital video using the variable temporal length 3D-DCT",IIT, Kanpur, 2007.

[19] Martin Zlomek,"Master thesis on Video Watermarking",Prague, April 19, 2007.

[20] Xing Chang, Weilin Wang, Jianyu Zhao, Li Zhang,"A Survey of Digital Video Watermarking",2011 Sevent International Conference on Natural Computation,61-65.

[21] Luo Wei, "A Improved Video Watermarking Scheme Based on Spread-spectrum Technique", 2010 International Conference on Networking and Digital Society, 511-514.

[22] C. Navya Latha,K. Sumanth, "Digital Video Watermarking".

[23] Sin-Joo Lee, and Sung-Hwan Jung, "A survey of watermarking techniques applied to multimedia". IEEE International Symposium on Industrial Electronics, Korea, June 2001. Vol. 1, pp. 272 – 277.
[24] Y. Shoshan, A. Fish, X. Li, G. A. Jullien, O. Yadid-Pecht, "VLSI Watermark Implementations and Applications," IJ Information and Knowledge Technologies, Vol.2, 2008.
[25] Watermarking World, http://www.watermarkingworld.org.
[26] M. Barni, F. Bartolini, J. Fridrich, M. Goljan, and A. Piva, "Digital watermarking for the authentication of AVS data," in EUSIPCO00, 10th Eur. Signal Processing Conf., Tampere, Finland, Sept. 2000.