Open access Journal International Journal of Emerging Trends in Science and Technology

A Survey on Digital Video Watermarking

Authors
Ramyashree.R[1], Seetha Rama Raju Sanapala[2]
[1]M. tech (DCN) Student, Reva Institute of Technology and Management, Bangalore, India
Email: *ramyashreer475@gmail.com*
[2]Professor (ECE), Reva Institute of Technology and Management, Bangalore, India
Email: *ssrr@revainstitution.org*

Abstract
At the leading edge of the information world everything is available in the form of digital media. Digital watermarking was introduced to provide the copy right protection and owners' authentication. Digital video watermarking is the process to embed a digital code into digital video sequences. Digital video watermarking is nothing but a sequence of consecutive still images. In recent few years the applications based on video like video-on-demand, video broadcasting have become more and more popular, so the requirement of a secure video distribution has increased. This paper reviews the basic concept of digital video watermarking, its principles and major characteristics, applications, and as well as its classification based on working domains.
Index Terms - *Digital Video Watermarking, Digital Video Watermarking techniques*

INTRODUCTION

Today digital media is available in a large scale, which can be easily copied and rapidly shared. People can acquire the copy of a digital media very easily; it may lead to large-scale unauthorized copies, which effect the development of the publishing industry. The owner of the content has to use some protection mechanism such as encryption or digital watermarking. Encryption is no longer sufficient for copy right protection and authentication, so digital video watermarking is widely used. It is an art of embedding information in invisible and robust manner [1] [2] [3].Because the copy and tamper of video is quite easy, in order to protect copy right, digital video watermarking technology has become an important and urgent component [1] [3]. Recently, video based applications such as video conferencing, wireless videos, video broadcasting, set-top box, video-on-demand, videophone and internet multimedia have become more and more popular and this has increased the demand for a secure distribution of videos [3] [4].

Current video coding technologies (such as H. 264) [5], some special attacks, the blind video watermarking detection and real-time features, have brought new challenges to digital video watermarking.

PRINCIPLES AND CHARACTERISTICS OF DIGITAL VIDEO WATERMARKING

A. The principle of digital video watermarking

A complete process of digital video watermarking is described into three steps [6] namely - watermark embedding or insertion, watermarked video and watermark detection. Watermark embedding or insertion is a process in which a watermark (w) is embedded into original video using a key which may be either symmetric or public key .Then the watermarked video is transmitted or distributed over a channel. At the

receiver side, watermark detection process is used to detect a watermark (w) in original video and later the watermark is extracted using private key. A simple block diagram of watermark embedding and detection in digital video is shown in Fig. 1

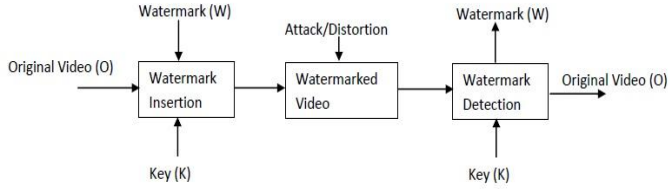

Fig.1 Block diagram of watermark embedding and detection in digital video

B. Major Characteristics of digital Video Watermarking

Video watermarking not only has the characteristics of digital image watermarking, but also has its own unique characteristics like [7]-[10]:

- High real-time: Three-dimensional video signal has more amount of data than the image does. So calculation quality is larger and embedding detection needs more time. The procession of embedding, using video compression standard for these specific structures such as motion vector coding, VLC code word etc can be achieved efficiently.
- Random detection: In video watermarking, the watermark can be easily detected in any position of the video.
- Blind detection scheme: Non-blind detection scheme needs the original host signal, but it is very inconvenient to use the original data, because of the huge video data. Blind detection scheme does not need the original host signal for watermarking.
- Perceptual Transparency: Invisibility is the degree at which an embedded watermark remains unnoticeable, when a user views the watermarked content. However this requirement conflicts with other requirements such as tamper resistance and robustness, especially against lossy compression techniques. To survive the next generation of compression techniques, it is probably necessary for a watermark to be noticeable to observer, when asked to compare the original and the marked version of the video.
- Better Robustness: Robustness is the resilience of an embedded watermark against removal by signal processing. The use of music, images and video signals in digital form, commonly involves many types of distortions, such as lossy compression. For watermarking to be useful, the watermark should be detectable even after such distortions occurred. Hence in video watermarking scheme, must ensure that it can resist almost all kinds of processing or attacks.
- Capacity: Capacity is the amount of information that can be expressed by an embedded watermark. Depending on the application at hand, the watermarking techniques should allow a predefined number of bits to be hidden.

APPLICATIONS OF DIGITAL VIDEO WATERMARKING

Digital video watermarking has huge application in the field of digital media which as follows as:

- Copyright protection: Copyright protection is the very first targeted application for digital video watermarking. In digital multimedia, watermarking is used as copyright protection to identify the copyright owner [1].
- Video authentication: Authentication means storing the signature into the header section of digital media, but the header field is still prone to tampering. So we can directly embed this type of authentication information directly as a watermark [2].
- Broadcast monitoring of video sequences: In television network different products are distributed over the channel. A

broadcast observation system must be built, in order to check the entire broadcasted channel. Watermark is used for this type of broadcast monitoring system by putting a unique watermark for each video to broadcast [3].

- Copy control: The video watermarking system has variously available technologies in which the information is secured in header of digital media and it prevents from copying of that data. Watermarking in copy control combines every content recorder with watermark detector, when a copy prohibit watermark is detected, the recording device will refuse to copy.
- Fingerprinting: Pay-per-view and Video-on-demand are two real-time applications of video streaming, in which digital video watermarking is used to enforce a fingerprinting policy. The customer ID is embedded into the video as a watermark to track back any user breaking his license agreement [12].
- Source tracking: Watermark information is embedded in the product of some company which will have to send information from one source to a particular destination. Source tracking is used for tracking the product information which is extracted from that product and checks it with original.
- Tamper proofing: Tamper proofing refers to a watermarking system's resistance to hostile attacks. Attacks are of two types namely active attack and passive attack. In active attack the attacker tries to remove the watermark or makes it unnoticeable. In passive attack it only checks whether the watermark is present or not.

REVIEW OF DIGITAL VIDEO WATERMARKING TECHNIQUES

Many digital watermarking schemes have been proposed for still images and videos. Most of them operate on uncompressed videos [13][14][16], while others embed watermarks directly into compressed videos [15][16].Video watermarking applications can be grouped as security related like Copy control [13], fingerprinting, ownership identification, authentication, tamper resistance etc, or value added applications like legacy system enhancement, database linking, video tagging, digital video broadcast monitoring [13], Media Bridge etc.

Existing video watermarking techniques are divided into different categories as shown in Fig. 2. They are divided into three main groups based on the domain that the watermark is embedded (i.e. working domain).

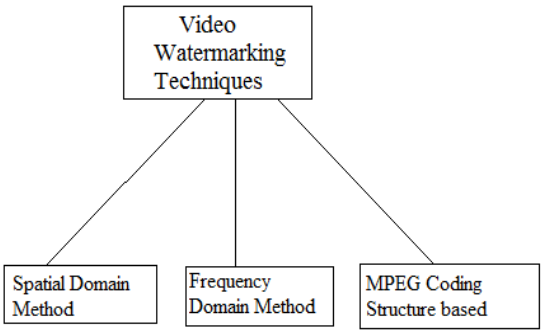

Fig. 2 Classification of digital video watermarking techniques

A. Spatial Domain Digital Video Watermarking

The spatial domain watermarking techniques embed the watermark by modifying the pixel values of the host video directly. Low computational complexities and simplicity are the main strengths of pixel domain methods. For better performance in real time these techniques are more attractive. Spatial domain watermarking technique involves two kinds of techniques namely Least Significant Bit Modification and the Correlation based technique.

- Least Significant Bit Modification (LSB)

In this technique, the Least Significant Bit of each pixel is used to embed the watermark or the copyright information. In this technique cover image is used to store the watermark, in which we can embed a smaller object multiple times. The

pixels are identified where embedding will be done using a pseudo-random number generator based on a given key.

LSB modification is suitable tool for stenography as it is a simple and powerful tool for it. But it cannot preserve robustness which is required in digital video watermarking applications.

- Correlation Based Techniques

The most straight forward way to add a watermark to an image in the spatial domain is to add a pseudo random noise pattern to the luminance values of its pixels. A Pseudo-random Noise (PN) pattern W (x, y) is added to the cover image I (x, y), according to the given below equation:

$$Iw(x, y) = I(x, y) + k * W(x, y) \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where 'k' denotes a gain factor and 'Iw' the watermarked image. The robustness of the watermark is increased by increasing the value of k at the expense of the quality of the watermarked image.

B. Frequency Domain Digital Video Watermarking

The frequency domain video watermarking methods are comparatively more robust than the spatial domain video watermarking schemes, mainly in cropping, scaling, noise intrusion, lossy compression, pixel removal, frame removal, frame averaging and rotation. Frequency domain watermarking techniques involves three different methods/techniques in it namely Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) respectively.

- Discrete Cosine Transform(DCT)

DCT is faster and is highly used method in image/video watermarking. Using the Discrete cosine transform image get decompose into different frequency bands, but more focused in middle frequency band. In this band watermark information is easily embedded. The middle frequency bands are chosen because it avoids the most visual important parts of the image which is off low frequency, without exposing themselves to removal through compression and noise attacks. This is important method for video processing. DCT gives accurate result in video watermarking also and shows the resistance against various attacks. Discrete cosine transform has a advantage that it break a video frame is into different frequency bands, which make it more easier to embed watermarking information into the middle frequency bands of an video frame.DCT also improve the peak signal to noise ratio and is more robust against various attacks such as frame averaging, frame dropping etc.[17].

- Discrete Fourier Transform(DFT)

The frequency of the host signal is controlled by the Discrete Fourier Transform. It is a multi-bit watermarking technique for video sequences. An N-bit message is embedded in one unit of video fragment, in which a scene is employed as a watermarking unit. This technique is fundamentally based on the three-dimensional discrete Fourier transform (DFT). In order to generate a watermark with optimum weighting factors, the perceptual properties for all the three-dimensional DFT coefficients should be computed, but this strategy seems to be undesirable due to its high computational complexity. So, it's needed to design a perceptual model of an image in the DFT domain, and then apply it to the video watermarking. This perceptual model is expected to give high fidelity and effectiveness. This DFT method will select the good area where watermark information can be embedded such that it provides more perceptibility and robustness [18].

- Discrete Wavelet Transform(DWT)

Discrete wavelet transform (DWT) is a tool for continuously decomposing an image. DWT is the multi-resolution description of an image. Discrete Wavelet Transform (DWT) is a transform based on frequency domain.

As shown in Fig. 3 the distributions 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 Fig. 3[19].

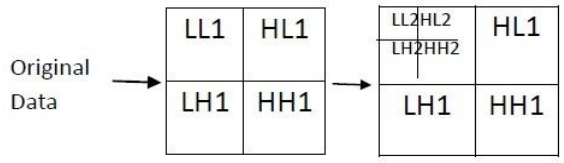

Fig.3 Frequency distribution after DWT

C. Watermarks Based on MPEG Coding Structures

This digital Video watermarking technique/ method make uses of MPEG-1, MPEG-2 and MPEG-4 coding structures as primitive components ,which are mainly used with the aim of combining watermarking and compression to reduce real-time video processing complexity. One of the major disadvantages of this method based on MPEG coding structures is that they are highly susceptible to re-compression with different parameters, as well as conversion to formats other than MPEG.

The motivation of combining the compression with watermarking introduced in the technique makes use of MPEG-2 or MPEG- 4 coding structure as the basic components. These techniques are applied for real time applications to reduce the overall time of processing. The method of block based compression such as MPEG-2 remove the temporal redundancy by using forward and bi-directional prediction, and statistical methods used to remove spatial redundancy. The main drawbacks of this method are re-compression with different parameters or converting the compression format to another format is not being able to be done. It is easy for employing cloud watermark for authenticating compressed MPEG-2 videos, which is also able to differentiate malicious attacks from natural processing. In this technique, the video is initially separated into video shots and the feature vectors are extracted. These feature vectors act as watermarks which will be embedded into the videos. The authentication process is done by comparison, between the watermark derived from the extracted cloud drops and modulated features of the received video shots. Tamper detection is promised in this work although very limited attacks have been tested on this method, so the performance still remained a question. However, they could make an improvement by using some unique characteristics of each shot in cloud generating [20].

CONCLUSION

This paper has provided the brief description about Digital Video Watermarking and its major characteristics, applications as well. It also represents the various kinds of digital video watermarking techniques based on its working domain. Through the comparison between different schemes reviewed in this paper, it has shown that video watermarking techniques in frequency domain have better performance than techniques proposed in spatial domain. Frequency domain watermarking schemes are more resistant against incidental modifications such as lossy compression, rotation, noise addition and cropping and also provides a better robustness and capacity for digital videos.

REFERENCES

1. Gwena.el Do.err, Jean-Luc Dugelay, "A guide tour of video watermarking", Signal Processing: Image Communication 18 (2003), 263–282.
2. Sourav Bhattacharya, T. Chattopadhyay and Arpan Pal, "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC".

3. Vivek Kumar Agrawal, "Perceptual watermarking of digital video using the variable temporal length 3D-DCT", IIT, Kanpur, 2007.
4. Luo Wei, "A Improved Video Watermarking Scheme Based on Spread-spectrum Technique", 2010 International Conference on Networking and Digital Society, 511-514.
5. Berna Erol, Adriana Dumiltras, Faouzi Kossentini, Anthorry Joch, Gary Sullivan, "MPEG-4, H.264/AVC, and MPEG-7: New Standards for the Digital Video Industry. Handbook of Image and Video Processing" (Second Edi.), 2005, 849-875.
6. Xiangwei Kong, Yu Liu, Huajian Liu, DeliYang "Object watermarks for digital images and Video", Image and Vision Computing 2004, 22(08)583-595.
7. Wugang Yuan, "Robust video waterma-rking Technology" Huazhong University of Science and Technology 2007
8. Jianjun Qin "The research of digital video Watermarking", Hunan Normal University 2010.
9. Wei Qu "Video Watermarking Algorithm" Shanghai Jiao tong University 2009.
10. T. Jayamalar, Dr. V. Radha, "Survey on Digital Video Watermarking Techniques and Attacks on Watermarks," International Journal of Engineering Science and Technology, vol. 12, 6963- 6967, 2010
11. Fernando Perez-Gonzalez and Juan R. Hernandez, "A tutorial on Digital Watermarking".
12. Hamid Shojanazeri, Wan Azizun Wan Adnan, Sharifah Mumtadzah Syed Ahmad,, M. Iqbal Saripan "Analysis of Watermarking Techniques in Video" 2011 IEEE.I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350
13. K. Su, D. Kundur and D. Hatzinakos, "A novel approach to collusion-resistant video watermarking", Proceedings of the SPIE, vol. 4675, pp. 491-502.
14. R. B. Wolfgang, C. I. Podilchuk and E. J. Delp, "Perceptual watermarks for digital images and video", Proceedings of the IEEE, vol. 87, pp. 1108-1126, (1999).
15. M. M. Reid, R. J. Millar and N. D. Black, "Second-generation image coding: An overview", ACM Computing Surveys, vol. 29, pp. 3-29.
16. F. Deguillaume, G. Csurka, J. Ruanaidh, and T. Pun, "Robust 3D DFT video watermarking," Proceedings Electronic Imaging' 99: Security and Watermarking of Multimedia Contents, Vol. 3657, San Jose, CA, Jan. 1999.
17. Sadik Ali M. Al -Taweel, Putra Sumari, and Saleh Ali K. Alomar, "Digital Video Watermarking in the Discrete Cosine Transform Domain" Journal of Computer Science 5 (8): 536 543, 2009.
18. Young-Yoon Lee, Han-Seung Jung and Sang-Uk Lee "3D DFT-based Video Watermarking Using Perceptual Models" 2004 IEEE
19. Lijing Zhang,Aihua Li, "A Study on Video Watermark Based-on Discrete Wavelet Transform and Genetic Algorithm", 2009 First International Workshop on Edu. Tech. and Computer Science, 374-377.
20. Ming Jianga, b, Zhao-Feng Mao, b, Xin-xin Niua, Yi-Xian Yang, "Video Watermarking Scheme Based on MPEG-2 for Copyright".
21. Hartung F and Girod B 1998" Watermarking of uncompressed and compressed video." Signal Processing 66(3): 283–301