olume 2, Issue 2
pril '10 - September '10

ISSN : 0974-3596

INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS IN ENGINEERING, TECHNOLOGY AND SCIENCES

IJ-CA-ETS

w.aessangli.in
w.ejournal.aessangli.in

Amoghsiddhi Education Society
Sangli

A STUDY ON VIDEO WATERMARKING TECHNIQUES

[1] T.JAYAMALAR [2] DR. V.RADHA

[1]Lecturer, Department Of Computer Science, Kovai Kalaimagal College Of Arts And Science, Coimbatore, Tamil Nadu, India.
[2]Associate Professor, Department Of Computer Science, Avinashilingam University For Women, Coimbatore, Tamil Nadu, India.

jayamalar2004@yahoo.com, radharesearch@yahoo.com

ABSTRACT:
Digital video is becoming popular more than ever due to the widespread of video-based applications such as Internet video, video phones, wireless video, video conferencing among many others. However, a byproduct of such popularity is the worldwide unauthorized copying and distribution of digital video. This creates a high demand for content protection technique like video watermarking. In this paper, a brief review of current video watermarking technologies is presented.

Key Words: Digital Video Watermarking, Copyright Protection.

1. INTRODUCTION

The tremendous development in digital media, particularly in the field of compression, has allowed a widespread use of multimedia applications. It has made it possible to distribute multimedia content via World Wide Web to a large number of people in a cost effective manner. However, this growth has also generated new challenges for content owners with copyright and security issues. In such cases, the need to protect the digital contents is to ensure its integrity and authenticity has become an absolute must [1], [2]. Traditionally, encryption, stegnographic, cryptographic techniques were used for protecting intellectual data. The past few decades has brought watermarking techniques as a solution for copyright protection [3], [4].

Watermarking is a process of embedding hidden information in a host signal. The main purpose for using watermarking techniques is for copyright protection, fingerprinting, copy protection, broadcast monitoring and data authentication. Based on the digital data used for watermarking, the techniques can be categorized as text-Based watermarking [5], image watermarking [6], [7], video watermarking [8], [2], audio watermarking [9], [10] and 3D watermarking [11]. Among them image and video watermarking are two important areas that has attracted several researchers [12], [13]. According to Gwenael and Jean-Luc [14], video watermarking is very different from image watermarking, even though some techniques can be viewed as an extension to it.

Digital video watermarking is a technology to embed and retrieve information into and from digital video data. The features desired from any video watermarking scheme is that they should ensure digital ownership, have the ability to track the source of the digital video, have quick and easy way to detect video manipulation, have no visible video degradation and should have easy implementation procedure. The basic characteristics are imperceptibility, security, reliability and low complexity of watermarking algorithm and security of the hiding place.

As a method of intellectual property protection, digital watermarks have recently stimulated significant interest and become a very active area of research. Although watermarking is a recent field of research, many techniques have already been proposed both in the academic as well as in the industry. They can be classified into different types based on the offered functionalities. In this paper, a brief review of the current video watermarking technologies is presented.

The paper is organized as below. Section 2 explains the various modules of a watermarking system. Section 3 presents the various facts revealed during the literature study and Section 4 concludes the paper with future research directions.

2. WATERMARK LIFECYCLE PHASES

Any digital watermarking algorithm is composed of three parts: watermark embedding algorithm, the watermark extraction algorithm and the watermark detection algorithm [15]. A general watermark lifecycle phases is shown in Figure 1.

A 'digital watermark' refers to the information to be embedded and the signal where the watermark is to be embedded is called the 'host signal'. During embedding process, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored. If a person makes a modification, then the digital content is said to be attacked.

A watermark attack is an attack on digital data where the presence of a specially crafted piece of data can be detected by an attacker without

knowing the encryption key. Special attention has to be paid to the kind of attacks as they can help to develop better watermarking techniques and defined better benchmarks. According to Hartung *et al.* [16], Watermark attack can be classified into four main groups:

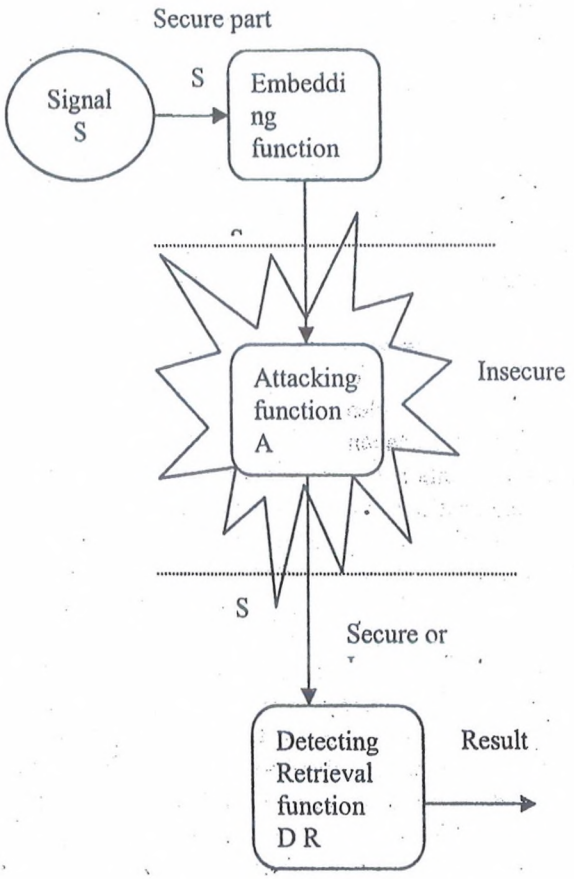

Figure 1 : Watermark Lifecycle Phases

(i) **Simple attacks** These types of attacks attempt to damage the embedded watermark by modifications of the whole frame without any effort to identify and isolate the watermark.

(ii) **Detection-disabling attacks** These are attacks that attempt to break the correlation and to make detection of the watermark impossible.

(iii) **Ambiguity attacks** These attacks the detector by producing fake watermarked data to discredit the authority of the watermark by embedding several additional watermarks so that it is not obvious which was the first, authoritative watermark.

(iv) **Removal attacks** The removal attacks estimates the watermark, separate it out and discard only the watermark.

Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark is still present and it can be extracted. In robust watermarking applications, the extraction algorithm should be able to correctly produce the watermark, even if the modifications were strong. In fragile watermarking, the extraction algorithm should fail if any change is made to the signal.

Any watermarking technique has to be evaluated to judge its performance. Capacity, Robustness, Visibility are the three factors that must be considered while evaluating a video watermarking algorithm.

These factors are inter-dependent; for example, increasing the capacity will decrease the robustness and/or increase the visibility. Therefore, it is essential to consider all three factors for a fair evaluation or comparison of watermarking algorithms.

3.VIDEO WATERMARKING TECHNIQUES

Many digital watermarking schemes have been proposed in the literature for still images and videos. These techniques mostly work on the raw uncompressed video data [17] and recent approaches are embedding watermarks into compressed video data also [18], [19].

A variety of robust and fragile video watermarking methods have been proposed to solve the illegal copying and proof of ownership problems as well as to identify manipulations. Although a number of broad claims have been made in the field of robustness of various digital watermarking methods, it is still difficult to handle combined or non-linear geometric transformations [20]. In general, Video watermarking is based on the following concepts to hide a watermark by modifying some of its characteristics:

- Spatial domain
- Frequency domain
- Format-specific

3.1 Spatial Domain Watermarks

The spatial domain watermarking techniques embed the watermark by modifying the pixel values of the host image directly [21], [22], [23]. Least Significant bit (LSB) technique is the most frequently used method [24]. In this technique, the LSB of each pixel is used to embed the watermark or the copyright information. This technique is the most-straight forward method and uses the entire cover image to store the watermark, which enables a smaller object to be embedded multiple times. In case of attacks destroying data, a single surviving watermark can be considered a success. They are robust to attacks like cropping, noise, lossy compression, etc. But an attack that is set on a pixel to pixel basis can fully uncover the watermark, which is the major drawback of the system. The LSB technique was later improved by Johnson and Katezenbeisser [25], which included an additional security, by using an pseudo-random number generator to determine the pixels to be used for embedding based on a given "seed" or key. The algorithm is vulnerable if the pseudo-random constant is uncovered.

The watermark system proposed by Ren-Junn *et al.* [26] embeds the watermark in saturation on the HIS (Hue, Saturation, Intensity) color space. The results proved that the system was able to resist only certain type of attacks. In a similar fashion, Huang *et al.*[21] used the DC components of the color image in spatial domain to embed the watermark and their results showed robust performance with all types of attacks except for rotate and scaling attacks.

A variable block size based adaptive watermarking, in spatial domain was proposed by Kimpan *et al.* [27], where the original image was divided into different blocks of varied size and the watermark was embedded into the blocks by analyzing and adjusting the brightness of a block. In a later period, Verma *et al.* [23] proposed a probability block based watermarking method for color image with fixed block size. In this method, the image was initially divided into blocks of size 8*8 and manipulated the pixel intensity to embed a watermark bit. The constraint used by this method is that the number of total bits of the watermark must be less or equal to the half of the total number of 8*8 blocks and redundant information is added to the watermark using convolutional code. The disadvantage of using convolutional code is that it is required a constant high amount of decoding operations, even if few or no errors occurred [28]. Both these methods were robust against all common image processing operations, such as median filter, scaling, rotation, etc. But failed with crop attack as the watermark bits were embedded into the whole image, hence some data was lost during cropping. Recently, a novel digital watermark algorithm based on chaotic maps was proposed by Wu and Guan [22] where the chaotic maps were used to determine the pixel bit for embedding.

The main advantages of pixel based methods are that they are conceptually simple and have very low computational complexities and therefore are widely used in video watermarking where real-time performance is a primary concern. However, they also exhibit some major limitations. The need for absolute spatial synchronization leads to high susceptibility to de-synchronization attacks; lack of consideration of the temporal axis results in vulnerability to video processing and multiple frame collusion; and watermark optimization is difficult using only spatial analysis techniques.

3.2 FREQUENCY DOMAIN WATERMARKS

Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT) are the three main methods of data transformation. In transform domain technique, the watermark is embedded distributively in overall domain of an original data. Here, the host image is first converted into frequency domain by transformation techniques. The transformed domain coefficients are then altered to store the watermark information. The inverse transform is finally applied in order to obtain the watermarked image.

A subsample based watermarking technique was proposed by Lu *et al.* [29], where the DCT coefficients of the subimages were utilized to store the watermark. The method was considered complex and involved high computations, because of the complicated calculations involved in the forward and inverse transformation process. The method, however, was robust against attacks than spatial domain methods.

Some proposed methods in frequency domain focus on embedding two or three watermarks. The authors of Cheng *et al.* [30], proposed an algorithm which was based on embedding the watermark image in three times at three different frequency bands, namely, low, medium and high and the results proved that the watermark cannot be totally destroyed by either low pass, medium or high pass filter. In Chun-Shien *et al.* [31], two complementary watermarks were embedded into the host image in order to make it difficult for attackers to destroy both of them.

The main benefit obtained from these techniques is that they can take advantage of properties of alternate domains to address the limitations of pixel-based methods or to support additional features. For example, using DCT in the watermark algorithm lead to better implementation compatibility with popular video coding algorithms like MPEG-2 and in the shift and rotation-invariant Fourier domains facilitates the design of watermarks that inherit these attractive properties. Besides, analysis of the host signal in a frequency domain is a prerequisite for applying more advanced masking properties of the HVS to enhance watermark robustness and imperceptibility. Generally, the main drawback of transform domain methods is their higher computational requirement.

3.3 MPEG BASED WATERMARKING SCHEMES

There is a number of MPEG-2 and -4-based techniques that have been proposed, including approaches based on GOP modification [32], high frequency DCT coefficient manipulation [33], DCT block classification [34], [35] proposed a video object watermarking which is based on the structure of MPEG-4. In their method, a scrambling technique that allows adapting any classical spread spectrum watermarking scheme operating in the spatial domain to the Mpeg-4 requirements concerning VO manipulation was proposed. This technique could be easily added to the embedding and detection schemes without changing the

watermarking algorithm. It modified some predefined pairs of quantized DCT coefficient in the luminance block of pseudo-randomly selected MBs and was based on spread-spectrum techniques. In this method, the image was first divided into equal sized blocks, where a binary sequence generated using secret key is embedded to the image.

Swanson, et al. [36] presented an object-based transparent watermarking procedure for copyright protection into video sequences. To address issues associated with video motion and redundancy, individual watermarks were created for objects within the video. Each watermark was created by shaping a pseudo-random sequence according to the perceptual masking characteristics of the video. This resulted in a watermark that could adapt to each video and ensured invisibility and robustness. Furthermore, their experimental results showed that the noise like watermark was statistically undetectable to prevent unauthorized removal.

Mobasseri [37] proposed a direct sequence watermarking using m-frames. This scheme applied a direct sequence spread spectrum model to the watermarking of the digital video. First, video signal was modeled as a sequence of bit planes arranged along the time axis. Watermarking of this sequence is a two layer operation. A controlling m-sequence, first establishes a pseudorandom order in the bit plane stream for later watermarking. Watermark, defined as m-frames, supplant the tagged bit planes. Moreover, attempts in corrupting the image to destroy the watermark render the video useless before damaging the seal itself. The watermarked video was also robust to video editing attempts such as sub sampling, frame reordering etc. The watermark is also identifiable from very short segment of video. Individual frames extracted from the video also contained the copyright information.

Video watermarking techniques that use MPEG-1, -2 and -4 coding structures as primitive components are primarily motivated by the goal of integrating watermarking and compression to reduce overall real-time video processing complexity. Compression in block-based schemes like MPEG-2 is achieved by using forward and bi-directional motion prediction to remove temporal redundancy, and statistical methods to remove spatial redundancy. One of the major drawbacks of schemes based on MPEG coding structures is that they can be highly susceptible to re-compression with different parameters, as well as conversion to formats other than MPEG.

4. CONCLUSION

The review of literature conducted reveals the fact that there are numerous innovative and inventive watermarking approaches and most of them focus on image watermarking. As the field of image watermarking technique is mature, researchers have now started exploring a more challenging topic called 'digital video watermarking'. Most of the proposed video watermarking schemes are based on image watermarking schemes and are applied directly to raw video or compressed video. However, the usage of image watermarking techniques to video introduces some new issues, which are present in image watermarking. The amount of data in video is very high and has inherent redundancy between frames. These properties are highly susceptible to attacks like frame averaging, frame dropping, frame swapping, statistical analysis, etc. To use an image as watermark in each frame of the video also raises certain problems while maintaining the statistical and perceptual invisible of the watermark. In these situations, it can be seen that the watermark in the frames are fixed while the video data in the frame changes. These fixed regions may be statistically compared or averaged to remove independent watermarks. Additionally, the existing video watermarking schemes advices not to use the original video during watermark detection as the video usually is in very large size and it is inconvenient to store it twice. These problems clearly indicate that further research in the area of video watermarking is needed. The future research direction is planned to produce solutions to some of the above mentioned problems.

5. REFERENCES

[1] Piva, A., Bartolini, F. and Barni, M. (2002) Managing copyright in open networks, IEEE Transactions on Internet Computing, Vol. 6, Issue. 3, Pp. 18-26.

[2] Lin, E., Podilchuk, C., Kalker, T. and Delp, E. (2001) Streaming Video and Rate Scalable Compression: What Are the Challenges for Watermarking?, Proceedings the SPIE International Conference on Security and Watermarking of Multimedia Contents III, Vol. 4314, San Jose, CA, 22-25.

[3] Lee, J. and Jung, S. (2001) A survey of watermarking techniques applied to multimedia," Proceedings 2001 IEEE International Symposium on Industrial Electronics (ISIE2001), Vol. 1, Pp. 272-277.

[4] Eskicioglu, A. and Delp, E.(2001) An overview of multimedia content protection in consumer electronics devices, Proceedings Signal Processing Image Communication, Vol. 16 Pp. 681-699.

[5] Kim, Y., Moon, K. and Oh, I. (2003) A text watermarking algorithm based on word classification and inter-word space statistics, Proceedings Seventh International Conference on Document Analysis and Recognition, Pp.775-779.

[6] Craver, S., Wu, M. and Liu, B. (2001) What can we reasonably expect from watermarks?, Proceedings IEEE Workshop on the Applications

of Signal Processing to Audio and Acoustics, Pp. 223-226.

[7] Foo, S., Yeo, T. and Huang, D. (2001) An adaptive audio watermarking system, Proceedings IEEE Region 10 International Conference on Electrical and Electronic Technology, Vol. 2, Pp. 509-513.

[8] Lu, C. and Liao, M. (2001) Video object-based watermarking: a rotation and flipping resilient scheme," Proceedings 2001 International Conference on Image Processing, Vol. 2, Pp.483-486.

[9] Sachs, D., Anand, R. and Ramchandran, K. (2000) Wireless image transmission using multiple-description based concatenated codes,Proceedings Data Compression Conference DCC 2000, P. 569.

[10] Bassali, H., Chhugani, J., Agarwal, S., Aggarwal, A. and Dubey, P. (2000) Compression tolerant watermarking for image verification, Proceedings 2000 International Conference on Image Processing, Vol. 1, Pp. 430-433.

[11] Hartung, F. and Kutter, M.(1999) Multimedia Watermarking Techniques", Proc. of IEEE, Tutorial, Survey, & Special Issue on Data Hiding & Security, Pp.1079-1107.

[12] Wang, C., Nie, X., Wan, X., Wan, W.B. and Chao, F. (2009) A Blind Video Watermarking Scheme Based on DWT," iih-msp, 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Pp.434-437,

[13] Mohammed, A.A. and Hussein, J.A. (2009) Efficient Video Watermarking Using Motion Estimation Approach, 2009 Eight IEEE/ACIS International Conference on Computer and Information Science (icis 2009), Pp.593-598.

[14] Gwenael, D. and Jean-Luc, D. (2003) A guide tour of video watermarking, Signal Processing Image Communication, Vol. 18, No. 4, Pp. 263-282.

[15] Zhang, Y. (2009) Digital Watermarking Technology: A Review, 2009 ETP International Conference on Future Computer and Communication, Pp.250-252.

[16] Hartung, F., Su, J.K. and Girod, B. (1999) Spread Spectrum Watermarking: Malicious Attacks and Counterattacks. Security and Watermarking of Multimedia Contents.

[17] Ejima, M. and Miyazaki, A. (2001) A wavelet-based watermarking for digital images and video, Proceedings International Conference on Image Processing (ICIP-2000), Vancouver, Canada, Vol. 3, Pp. 678-681.

[18] Hartung, F. and Girod, B. (1998) Watermarking of Uncompressed and Compressed Video, IEEE Transaction Signal Processing, Vol. 66, no. 3 (Special issue on Watermarking), Pp. 283-301.

[19] Arena, S. and Caramma, M. (2000) Digital watermarking applied to MPEG2 coded video sequence exploiting space and frequency masking, Proceedings International Conference on Image Processing (ICIP-2000), Vancouver, Canada, Vol. 3, Pp. 438-441.

[20] Su, K. (2001) Digital Video Watermarking Principles for Resistance to Collusion and Interpolation Attacks, Master of Applied Science thesis, University of Toronto.

[21] Huang, P.S., Chiang, C.S., Chang, C.P. and Tu,T.M. (2005) Robust spatial watermarking technique for colour images via direct saturation adjustment, Vision, Image and Signal Processing, IEEE Proceedings, vol. 152, Pp. 561-574.

[22] Wu, X. and Guan, Z.H. (2007) A novel digital watermark algorithm based on chaotic maps, Physics Letters A, vol. 365, Pp. 403-406.

[23] Verma, B., Jain, S., Agarwal, D.P. and Phadikar, A. (2006) A New color image watermarking scheme, Infocomp, Journal of computer science, vol. 5,N.2, Pp. 37-42.

[24] Lee, Y.K. and Chen, L.H. (2000) High capacity image steganographic model, Vision, Image and Signal Processing, IEEE Proceedings, vol. 147, Pp. 288-294.

[25] Johnson, N. and Katezenbeisser, S. (1999) A Survey of Steganographic Techniques in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, Pp. 43-75.

[26] Ren-Junn, H., Chuan-Ho, K. and Rong-Chi,C. (2002) Watermark in color image," Proceedings of the first International Symposium on Cyber Worlds, Pp. 225-229.

[27] Kimpan, S., Lasakul, A. and Chitwong, S. (2004) Variable block size based adaptive watermarking in spatial domain, IEEE International Symposium on Communications and Information Technology, ISCIT 2004, vol. 1, Pp. 374-377.

[28] Hueske, K., Geldmacher, J. and Gotz, J. (2007) Adaptive decoding of convolutional codes, Advanced in radio science, vol. 5, Pp. 209-214.

[29] Lu, W., Lu, H. and Chung, F.L. (2006) Robust digital image watermarking based on subsampling, Applied Mathematics and Computation, vol. 181, Pp. 886-893.

[30] Cheng, L.M., Cheng, L.L., Chan, C.K. and Ng,K.W. (2004) Digital watermarking based on frequency random position insertion, Control, Automation, Robotics and Vision Conference, vol. 2, Pp. 977-982.

[31] Chun-Shien, L., Shih-Kun, H., Chwen-Jye, S. and Mark, L.H. (2000) Cocktail watermarking for digital image protection," IEEE Transactions on Multimedia,vol. 2, Pp. 209-224.

[32] Linnartz, J. and Talstra, J. (1998) MPEG PTY-marks: Cheap detection of embedded

copyright data in DVD video, Proceedings 5th European Symposium on Research in Computer Security, Pp. 221-240.

[33] Chung, T., Hong, M., Oh, Y., Shin, D. and Park, S. (1998) Digital watermarking for copyright protection of MPEG2 compressed video, IEEE Transactions on Consumer Electronics, Vol. 44, Issue. 3, Pp. 895-901.

[34] Holliman, M., Memon, N., Yeo, B. and Yeung, M. (1997) Adaptive public watermarking of DCT-based compressed images, Proceedings SPIE, Vol. 3312, Pp. 284-295.

[35] Vassaux, B., Nguyen, P., Baudry, S., Bas, P. and Chassery, J. (2002) Scrambling technique for video object watermarking resisting to mpeg-4, Proceedings Video/Image Processing and Multimedia Communications 4th EURASIP-IEEE Region 8 International Symposium on VIPromCom, Pp. 239-244.

[36] Swanson, M., Zhu, B., Chau, B. and Tewfik, A. (1997) Object-Based Transparent Video Watermarking, Proceedings IEEE Signal Processing Society 1997 Workshop on Multimedia Signal Processing, Princeton, New Jersey, USA.

[37] Mobasseri, B. (1998) Direct sequence watermarking of digital video using m-frames," Proceedings International Conference on Image Processing (ICIP-98), Chicago, Illinois, Vol. 3, Pp. 399-403.