Survey on Digital Video Watermarking Techniques and Attacks on Watermarks

T.JAYAMALAR[1]

Lecturer, Department of computer science,Kovai Kalaimagal college of arts and science, Coimbatore, Tamil Nadu, India.

Dr. V. RADHA[2]

Associate professor, Avinashilingam Deemed University, Coimbatore, Tamil Nadu, India.

Abstract :

Digital video watermarking is a technique for embedding additional data along with video signal. Embedded data is used for copyright owner identification. A number of video watermarking techniques are proposed. These techniques exploit different ways in order to embed a robust watermark and to maintain the original video signal fidelity. In this paper, Digital video watermarking techniques and attacks on watermarks are presented.

Keywords: Digital video watermarking; Copyright Protection; Attacks.

1. Introduction

In the past several years there has been an explosive growth in multimedia technology and it's applications. This growth has escalated the necessity to build secure methods for legal distribution of the digital content. As digital multimedia works (video, audio and images) become available for retransmission, reproduction, and publishing over the Internet, a real need for protection against unauthorized copy and distribution is increased. Thus, there is a rise in apprehensions over copyright protection of digital contents [1]. Security of digital contents has turned out to be of great significance with the omnipresence of internet. Besides, the data hiding technologies for digital data like digital watermarking have attracted enormous attention recently [2].

Digital watermarking is deployed so as to prohibit illegal replication or exploitation of digital contents [3]. Digital watermarking is a technique that proffers a means to guard digital contents from illegal copying and manipulation. The procedure of embedding data into a multimedia element like image, audio or video is referred to as watermarking . It is possible to extract this embedded data at a later stage, or detected in, the multimedia element for diverse purposes including copyright protection, access control, and broadcast monitoring

.A digital watermark is an unnoticeable signal added to digital data, known as cover work, which can possibly be identified at a later stage for buyer/seller identification, ownership proof, and the like. A watermark needs to possess the following features in order to be effective [4]:

***a)* Unobtrusive:** The watermark needs to be perceptually invisible.

b)* Robust*: The watermark needs to be tedious (impossible; to be precise) to remove. When only incomplete knowledge is present (for instance, the precise location of the watermark in an image, video is unknown) then attempts to remove or demolish a watermark, should consequent in severe degradation in fidelity prior to the loss of the watermark.Especially, the watermark needs to be robust to [4]:

- Common signal processing - It is necessary that the watermark be retrievable despite common signal processing operations being applied to the data. These operations may be one among the following: digital-to-analog and analog-to-digital conversion, re-sampling, re-quantization and common signal enhancements to image contrast and color, or audio bass and treble.
- Common geometric distortions-Watermarks in video data need to be resistant towards geometric image, video operations such as rotation, translation, cropping and scaling as well.
- Subterfuge Attacks- Additionally, the watermark must be flexible to collusion by multiple individuals each possessing a watermarked copy of the data. In other words, the watermark needs to be robust to combining copies of the same data set to destroy the watermarks.

c) Universal: The same digital watermarking algorithm needs to be applicable for all three media under consideration. This is potentially helpful in the watermarking of multimedia products. This feature is favorable

for the implementation of audio and image/video watermarking algorithms on common hardware as well [4].
d) Unambiguous: Retrieval of the watermark must unambiguously recognize the owner. The storage, access and distribution of digital images, videos have developed a lot owing to the innovations occurring in the field of information and communication technology. With the exceptional raise in the necessity for sharing of digital images and videos, the requirement of copyright protection as well has grown proportionally.
In this paper, an extensive review of the digital video watermarking for copyright protection and attacks on watermarks are presented.

2. Video Watermarking

Digital watermarking can be categorized into image watermarking, video watermarking and audio watermarking depending upon the range of application. According to Gwenael and Jean-Luc [5], video watermarking is very different from image watermarking, even though some techniques can be viewed as an extension to it.

Video watermarking refers to embedding watermarks in a video sequence in order to protect the video from illegal copying and identify manipulations. 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 [6]. The methods can be divided into techniques that work on compressed or uncompressed data. Various types of watermarking schemes have been proposed for different applications. The watermarking techniques have been applied either in the spatial domain or in the frequency domain using (Fourier, DCT, DWT, Fractal, etc) transforms.

2.1. Video watermarking terminologies

The important terminologies pertaining to digital video watermarking are:

Digital Video: Video sequence is a collection of consecutive and equally time spaced still images.
Payload: It is the amount of information that can be stored in a watermark. An important concept regarding the video watermarking payload is watermark granularity. Watermark granularity can be defined as how much data is required for embedding one unit of watermark information.
Perceptibility: Video watermarking methodology is called imperceptible, if it is not able to find the difference between the original video from the video with inserted watermark.
Robustness: *A* fragile watermark should not be robust against intentional modification techniques, as failure to detect the watermark signifies that the received data is no longer authentic. In case of application such as copyright protection, it is desirable that watermark always remains in the video data, even if the video data is subjected to intentional and unintentional signal processing attacks. Hence, depending on the requirements of the application the watermark is embedded in a robust, semi-fragile or fragile manner.
Security: *T*he security of the watermarking algorithm is ensured in the same way as in encryption methodology. According to the Kerckhoff's assumption, the algorithm for watermark embedding can be considered to be public, where as the security depend solely on the choice of a key from a large key space.

2.2. Video watermarking techniques

Apparently any image watermarking technique can be extended to watermark videos, but in reality video watermarking techniques need to meet other challenges than that in image watermarking schemes such as large volume of inherently redundant data between frames, the unbalance between the motion and motionless regions, real-time requirements in the video broadcasting etc. Watermarked video sequences are very much susceptible to pirate attacks such as frame averaging, frame swapping, statistical analysis, digital-analog (AD/DA) conversion, and lossy compressions.

Video watermarking applications can be grouped as security related like Copy control [7], fingerprinting, ownership identification, authentication, taper resistance etc. or value added applications like legacy system enhancement, database linking, video tagging, digital video broadcast monitoring [8], Media Bridge etc. Apart from robustness, reliability, imperceptibility, practicality, and video watermarking algorithms should also address issues such as localized detection, real time algorithm complexity, synchronization recovery, effects of floating point representation, power dissipation etc.

According to the working domain, video watermarking techniques are classified in to

- Spatial domain
- Frequency domain
- Format-specific

2.2.1. Spatial domain watermarks

The spatial domain watermarking techniques embed the watermark by modifying the pixel values of the host image/video directly. Least Significant bit (LSB) technique is the most frequently used method [9]. 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 [10], 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.

A variable block size based adaptive watermarking, in spatial domain was proposed by Kimpan *et al.* [11], 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.* [12] 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 . 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.

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.

2.2.2.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/video 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/video.

A subsample based watermarking technique was proposed by Lu *et al.* [13], 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.

The authors of Cheng *et al.* [14], 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.* [15], 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. Generally, the main drawback of transform domain methods is their higher computational requirement.

2.2.3.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, high frequency DCT coefficient manipulation, DCT block classification. Vassaux *et al.*[16] 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. [17] 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.

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.

3. Attacks on watermarks

In the field of digital watermark, there are various categorizations of attacks on watermarks. These can be categorized by Ajit Kulkarni [18] as follows

a) Subtractive Attack

In this attack the adversary or malicious user tries to detect the presence, location of the watermark and tries to extract it from the host. An effective subtractive attack is one where the cropped object has retained enough original content to still be of value.

b) Distortive Attack

If an adversary or malicious user applies some distortive transformation uniformly over the object in order to degrade the watermark so that it becomes undetectable/unreadable. An effective distortive attack is one where one can no longer detect the degraded watermark, but the degraded object still has value to the adversary.

c) Additive Attack

An adversary or malicious user can augment host by inserting his own watermark W (or several such marks).An effective additive attack is one in which adversary's mark completely overrides original mark, so that it can no longer be extracted or it is impossible to detect that the original mark temporally precedes the adversary's mark.

d) Filtering

Low-pass filtering, for instance, does not introduce considerable degradation in watermarked images, videos or audio, but can dramatically affect the performance, since spread-spectrum-like watermarks have non negligible high-frequency spectral contents.

e) Cropping

This is a very common attack since in many cases the attacker is interested in a small portion of the watermarked object, such as parts of a certain picture or frames of a video sequence. With this in mind, in order to survive, the watermark needs to be spread over the dimensions where this attack takes place.

f) Compression

This is generally an unintentional attack which appears very often in multimedia applications. Practically all the audio, video and images that are currently being distributed via Internet have been compressed. If the watermark is required to resist different levels of compression, it is usually advisable to perform the watermark insertion task in the same domain where the compression takes place. For instance, DCT domain image watermarking is more robust to JPEG compression than spatial domain watermarking.

g) Rotation and Scaling

It has been very successful with still images. Correlation based detection and extraction fail when rotation or scaling is performed on the watermarked image because the embedded watermark and the locally generated version do not share the same spatial pattern anymore. Obviously, it would be possible to do exhaustive search on different rotation angles and scaling factors until a correlation peak is found, but this is prohibitively complex.

h) Statistical Averaging

An attacker may try to estimate the watermark and then 'unwatermark' the object by subtracting the estimate. This is dangerous if the watermark does not depend substantially on the data.

Note that with different watermarked objects it would be possible to improve the estimate by simple averaging. This is a good reason for using perceptual masks to create the watermark.

i) Multiple Watermarking

An attacker may watermark an already watermarked object and later make claims of ownership. The easiest solution is to timestamp the hidden information by a certification authority.

i) Attacks at Other Levels

There are a number of attacks that are directed to the way the watermark is manipulated. For instance, it is possible to circumvent copy control mechanisms discussed below by super scrambling data so that the watermark is lost or to deceive web crawlers searching for certain watermarks by creating a presentation layer that alters they way data are ordered. The latter is sometimes called 'mosaic attack'.

4. Conclusion

Digital video Watermarking is a new and merging area of research. It mainly deals with adding hidden messages or copyright notices in digital video. This paper reviews various techniques for video watermarking and attacks on watermarks. As a result, video watermarking is a potential approach for protection of ownership rights on digital video.

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] Tosihiro Akiyama, Fumiaki Motoyoshi,Osamu Uchida and Shohachiro Nakanishi "Hybrid Digital Watermarking for Color Images Based on Wavelet Transform," IADIS International Conference Applied Computing 2006, San Sebastian, Spain, February 2006.

[3] G. Voyatzis and I. Pitas, "The use of watermarks in the protection of digital multimedia products," IEEE Proceedings, Vol. 87, No. 7, pp 1197-1207, July 1999.

[4] Hernandez, J.R., Perez-Gonzalez, F., "Statistical analysis

[5] of watermarking schemes for copyright protection of images", Proceedings of the IEEE, Vol. 87, No. 7, pp. 1142 - 1166, July 1999.

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

[7] F. Hartung and M. Kutter, "Multimedia watermarking techniques", Proceedings of the IEEE, vol. 87, no. 7, July 1999.

[8] J. A. Bloom, I. J. Cox, T. Kalker, J. –P. M. G. Linnartz, M. L. Miller,and C. B. S. Traw, "*Copy protection of DVD video*", Proceeding of the IEEE, vol. 87, pp. 1267-1276, (1999).

[9] T. Kalker, G. Depovere, J. Haitsma, M. Maes, "*A videowatermarking system for broadcast monitoring*", proceedings of theSPIE, vol. 3657, pp. 103-112, (1999).

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] S wanson, 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. February 2006.

[19] http://www.wseas.us/e-library/conferences/2005argentina/papers/503-192.pdf