Digital Video Watermarking Techniques: A Review Study

Archana Srivastava[1] Prof. Darshana Mistry[2]
[1]M.E. Student, Gujarat Technological University
[2] Professor, Computer Engineering Department
[2]Indus University, Ahmedabad

Abstract— Digital watermarking is a data hiding technique where an information or message is hidden inside a signal transparent to the user. Video Watermarking is one of the interesting fields to develop a system with authentication and copyright protection methodology embedded within an efficient video codec. Thus, this technique can be used for copyright protection, piracy tracing, content authentication, advertisement surveillance, error resilience, and so forth. In this paper, we give an overview on video watermarking technology, including its properties, applications, performance requirements, typical algorithms, and comparison among them.

Keywords— Digital Watermarking, Video Watermarking, Copyright protection, Content Authentication

I. INTRODUCTION

The rapid expansion of the Internet in the past years has rapidly increased the availability of digital data such as audio, images and videos to the public. The idea of robust watermarking of images is to embed information data within the image with an insensible form for human visual system but in a way that protects from attacks such as common image processing operations. The goal is to produce an image that looks exactly the same to a human eye but still allows its positive identification in comparison with the owner's key if necessary. In fact any image watermarking technique can be extended to watermarking videos, but in reality video watermarking techniques need to meet other challenges like video coding technologies, large volume of data, blind watermarking detection, the unbalance between motion and motionless region, some special attacks like frame averaging, frame swapping, statistical analysis and other real-time features than that in image watermarking scheme. [2][3][6].To be effective, watermark should possess the properties such as

1) Robustness: The watermark should be impossible to remove even if the algorithmic principle of the watermarking method is public.
2) Unambiguous: The retrieved watermark should uniquely identify the copyright owner of the content, or in case of fingerprinting applications, the authorized recipient of the content.
3) Loyalty: A watermark has a high reliability, if the degradation it causes is very difficult to perceive for the viewer.
4) Computational Cost: Embedding and extraction of watermark from the video both should be fairly fast and should have low computational complexity
5) Interoperability: Watermark system must be interoperable for the compressed and decompressed operations.
6) Universal: The same digital watermarking algorithm needs to be applicable for all three media under consideration. This feature is favorable for the implementation of audio and image/video watermarking algorithms on common hardware as well.
7) Unobtrusive: The watermark needs to be perceptually invisible.

II. WATERMARKING PROCESS

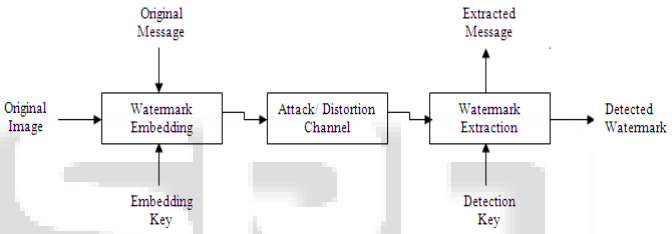

Figure.1: Block Diagram of Video Watermarking System

1) Generation and Embedding
In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal. The signal where the watermark is to be embedded is called the host signal.

2) Distribution and Possible Attacks
The distribution process can be seen as the transmission of the signal through the watermark channel. Possible attacks in the broadcast channel may be intentional or accidental.

3) Detection
Detection process allows the owner to be identified and provides information to the intended recipient.

III. .APPLICATIONS OF VIDEO WATERMARKING

The major applications of digital video watermarking includes copyright protection, video authentication, broadcast monitoring, copy control, fingerprinting, taper resistance, video tagging, ownership identification and enhance video coding. [1][2][13] Some of them are explained below:

A. Copyright protection:

In digital multimedia, watermarking is used as copyright protection to identify the copyright owner.

B. Video *authentication:*

Authentication means storing the signature into the header section, but the header field still be prone to tempering. So we can directly embed this type of authentication information directly as a watermark.

C. Broadcast monitoring:

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.

D. Copy control:

Watermarking system has the available technologies in which the information is secured into the header and it prevents from copying of that data.

E. Fingerprinting:

Pay-per-view and Video-on-demand are two real-time applications of video streaming, in which digital watermarking is used to enforce a fingerprinting policy.

F. Data Hiding (Covert Communications):

The transmission of private data is probably one of the earliest applications of watermarking. As one would probably have already understood, it consists of implanting a strategic message into an innocuous one in a way that would prevent any unauthorized person to detect it.

G. Medical Safety

Embedding the date and patient's name in medical images could increase the confidentiality of medical information as well as the security.

IV. ATTACKS ON WATERMARK

The common attacks of video watermarking are frame dropping, frame averaging, statistical analysis, lossy compression, cropping and various signal processing and geometrical attacks.

A. Frame dropping:

Frame dropping means dropping one or more frames randomly from the watermarked video sequence. If we drop too many frames, the quality of the watermarked video will decrease rapidly.

B. Frame averaging:

Frame averaging is also a significant video watermarking attack that will remove dynamic composition of the video watermarked

C. Frame swapping:

Frame swapping means switching the order of frames randomly within a watermarked video sequence. As well as frame dropping, if we swap too many frames, it will degrade the video quality.

D. Intentional attacks:

The intentional watermark attack includes Single frame attacks like filtering attacks, contrast and color enhancement and noise adding attack. Or statistical attacks like averaging attack and collision attack.

E. Unintentional attacks:

The unintentional attacks may be due to Degradations that can occur during glossy copying, or due to Compression of the video during re-encoding or because of Change of frame rate and Change of resolution

V. CLASSIFICATION OF DIGITAL VIDEO WATERMARKING TECHNIQUES

A. According to the types of carriers

According to the embedding strategy, video watermark algorithm can be divided into different three types (Figure 3): Original uncompressed based video watermarking (Embed 1); embedding watermark in the video encoder (Embed 2) and compression based video watermarking (Embed 3).

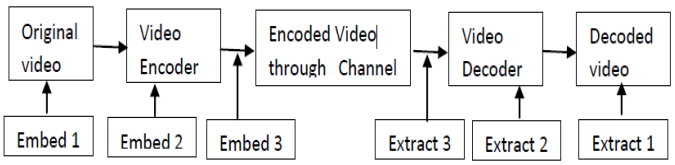

Figure.2: Block Diagram of Video Watermarking according to types of carriers

1) Embed/Extract 1:

In this type of watermarking, watermark is directly embedded into the Original video sequences and after that watermark containing video sequence is encoded. [6] Advantage of this type is we can embed watermark easily but the disadvantage is that it will increase the bit rate of video data stream and also after compression watermark may be lost.

2) Embed/Extract 2:

In this type of watermarking, watermark embedding and detection are done at the encoder and decoder. [4][6] There are different video compression standard are available today: MPEG-1, MPEG-2, and MPEG-4. [4] Advantage of this type is that it does not increase the bit rate of video data stream and it is relatively simple method of watermark embedding in the transform domain.

3) Embed/Extract 3:

In this type of watermarking, watermark is embedded into the compressed domain. Advantage of this type is computational complexity is lower compare to other types, but the disadvantage is that the compressed bit rate constraints the size of the watermark data..

B. According to types of Domain

Current video watermarking techniques can be grouped into two major classes; spatial-domain watermarking techniques and watermarking frequency-domain techniques. Spatial-domain techniques embed a watermark in the frames of a given video by modifying its pixels directly. These techniques are easy to implement and

require few computational resources; however, they are not robust against common digital signal processing operations such as video compression. On the other hand, transform-domain watermarking techniques modify the coefficients of the transformed video frames according to a predetermined embedding scheme. The scheme disperses the watermark in the spatial domain of the video frame, hence making it very difficult to remove the embedded watermark.

1) Spatial Domain Video Watermarking Techniques:
The watermark design and the watermark insertion procedures do not involve any transforms. Simple techniques like addition or replacement are used for the combination of watermark with the host signal and embedding takes place directly in the pixel domain.

2) Least Significant Bit modification (LSB):
Least Significant Bit (LSB) method is the simplest technique of this domain. In this scheme the watermark is simply embedded into the least significant bits of the original video or flips the LSB. Due to its simplicity, it is the most popular scheme, but some limitations are also there like, poor quality of the produced video, inefficient in dealing with the various attacks, least robustness and lack of imperceptibility.

3) Correlation based techniques:
A pseudo-random noise (PN) pattern W(x, y) is added to the cover image I(x, y), according to the equation shown below

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

In equation (1), k is a gain factor and Iw is the watermarked content. As we increase the value of k, it will expense the quality of watermarked contents.

4) Frequency Domain Video Watermarking Techniques:
In frequency domain techniques, the watermark is embedded by modifying the transform coefficients of the frames of the video sequence. The most commonly used transforms are the Discrete Fourier Transform (DFT), the Discrete Cosine Transform (DCT), and the Discrete Wavelet Transform (DWT). Generally, the main drawback of transform domain methods is their higher computational requirement.

5) SVD Domain Video Watermarking Technique:
Singular Value Decomposition (SVD) is a numerical technique for diagonalzing matrices in which the transformed domain consists of basis states that is optimal in some sense. The SVD of an N x N matrix A is defined by the operation:

$$A = U S V T \quad (2)$$

Where U and V Є R are unitary, and S Є R

N*N is a diagonal matrix. The diagonal entries of S are called the singular values of A and are assumed to be arranged in decreasing order σi > σi +1. Embedding watermark information in the diagonal elements of matrix U or matrix V showed more robustness against noise than embedding in matrix S.

The block-wise based embedding in the second algorithm allows larger watermark to be hidden in the host video, compared with the diagonal wise embedding of the first algorithm.

C. Discrete Fourier Transform Video Watermarking Technique:

This approach first extracts the brightness of the watermarked frame, computing its full-frame DFT taking the magnitude of the coefficients. The watermark is composed of two alphanumerical strings. The DFT coefficient is altered, then IDFT. Only the first frame is watermarked, which was composed of twelve frames, leaving the other ones uncorrupted. It is good robustness to the usual image processing as linear/non-linear filtering, sharpening, JPEG compression and resist to geometric transformations as scaling, rotation and cropping. The watermark design and the watermark insertion procedures do not involve any transforms. Simple techniques like addition or replacement are used for the combination of watermark. DFT-based watermarking scheme with template matching can resist a number of attacks, including pixel removal, rotation and shearing. The purpose of the template is to enable resynchronization of the watermark payload spreading sequence. It is a key dependent pattern of peaks, which is also embedded into DFT magnitude representation of the frame.

D. Discrete Cosine Transform Video Watermarking Technique:

Discrete Cosine Transform (DCT) is an important method for video watermarking. A lot of digital video watermarking algorithms embed the watermark into this domain. The usability of this transform is because that most of the video compression standards are based on DCT and some other related transforms. In this domain some DCT coefficients of the video are selected and divided into groups, and then the watermark bits are embedded by doing adjustment in each group.

E. Discrete Wavelet Transform Video Watermarking Technique:

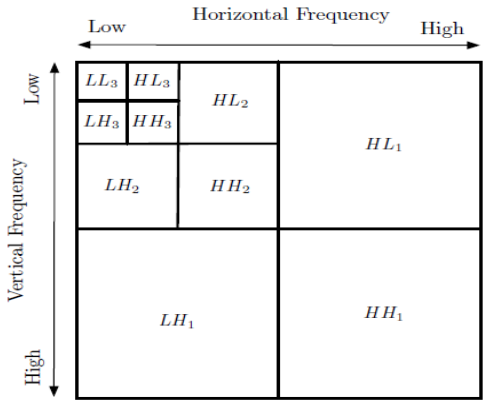

Fig. 3 DWT in Square mode

As shown in figure 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 figure 3.

F. Principal Component Analysis Video Watermarking Technique:

Principal component analysis (PCA) is a mathematical procedure that uses an orthogonal transformation to convert a set of observations of correlated variables into a set of values of uncorrelated variables called principal components. PCA plots the data into a new coordinate system where the data with maximum covariance are plotted together and is known as the first principal component. Similarly, there are the second and third principal components and so on. The first principal component has the maximum energy concentration. In the proposed scheme, a binary image is embedded in the LL DWT sub-bands of level 2 of each decomposed frame in the video. Also, the same binary image is embedded in the HH DWT sub-band of level 2 of each decomposed frame. Embedding the watermark in both LL and HH makes the scheme robust to a variety of low and high frequency characteristic attacks. [7, 9]

ACKNOWLEDGMENTS

I would like to thank my guide, Prof. Darshana Mistry, for his professional leadership and valuable advice.

REFERENCES

[1] S. Tripathi, R.C. Jain," Novel DCT and DWT based Watermarking Techniques for Digital Images", The 18th IEEE International Conference on Pattern Recognition, 2006
[2] F. P´erez-Gonz´alez and J.R. Hernandez, "A tutorial on Digital Watermarking", Dept. Technologies de las Comunicaciones, ETSI Telecom., Universidad de Vigo, 36200 Vigo, Spain
[3] S. Bhattacharya, T. Chattopadhyay and A. Pal, "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC", IEEE, 2006
[4] A.Essaouabi and F.regragui, "A Wavelet-Based Digital Watermarking for Video", International Journal of Computer Science and Information Security, Vol. 6, No.1, pp 29-33, 2009
[5] P. Goč-matis, T. Kanócz, R. Ridzoň and D. Levický, "Video watermarking based on DWT", 10th Scientific Conference of Young Researchers,2010
[6] H.Patel, J. Patoliya, P.Panchal,R. N. Patel," Digital Robust Video Watermarking Using 4-Level Dwt", International Journal of Advanced Engineering Technology, Vol.1, Issue 3, pp. 101-113, Oct.-Dec.,2010
[7] S.Sinha, P.Bardhan, S.Pramanick, A.Jagatramka, "Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis", International Journal of Wisdom Based Computing, Vol. 1 (2), pp. 7-12,August 2011
[8] R.T. Paul," Review of Robust Video Watermarking Techniques", IJCA Special Issue on "Computational Science - New Dimensions & Perspectives", pp. 90-95, NCCSE, 2011
[9] N. I. Yassin, N. M. Salem, and M. I. E Adawy," Block Based Video Watermarking Scheme Using Wavelet Transform and Principle Component Analysis", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, pp. 296-301, January 2012
[10] S. Voloshynovskiy, S. Pereira, and T. Pun, "Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks," IEEE Comm. Magazine, pp. 118-126, Aug. 2001
[11] P. K. sharma and Rajni, " Analysis of Image Watermarking using Least Significant Bit Algorithm" International Journal Of Information Science and Techniques, Vol2 ,No.4, 95-101, July 2012
[12] Dongbing Pu, Yinghua Lu, Jiangyan Dai "Video Watermarking Approach Based on Temporal Difference And Discrete Wavelet Transform", 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), pp. 346-350,2010
[13] Darshana Mistry, "Comparison of Digital Water Marking methods", International Journal on Computer Science and Engineering, Vol. 02, No. 09, pp 2905-2909,2010