Robust Video Watermarking Techniques and Attacks on Watermark – A Review

Ankita A. Hood¹, Prof. N. J. Janwe²

¹CSE Department, Ballarpur Institute of Technology,
Ballarpur, Nagpur University, Maharashtra, India.
²Computer Technology Department, R.C.E.R.T.,
Chandrapur, Nagpur University, Maharashtra, India.

Abstract— There has been an explosive growth in the digital technique and internet usage recently. It has created a new set of challenging problems such as copyright protection, authentication and content integrity, verification of the digitized properties. Over the last few years, watermarking has proved to be the solution to these problems. Watermarking is the process of embedding some additional data along with the video signal to protect the digital media. A large portion of the watermarking literature deals with the copyright protection of the still digital images. Watermarking techniques for digital video and audio have also been proposed. In this paper, we review the proposed schemes and also the various attacks on the watermarks.

Keywords— Video Watermarking, Discrete Wavelet Transform, Principal Component Analysis, Binary Watermark, Attacks, Applications.

I. Introduction

There has been tremendous use of internet and also in multimedia technology recently. It leads to copying, tempering and distribution of digital data. A large amount of data is duplicated, edited and distributed without the owner’s permission. Hence, copyright protection for multimedia data has become an important issue. Digital watermarking emerged as a tool for protecting the multimedia data from copyright infringement. In digital watermarking an imperceptible signal “mark” is embedded into the host image, which uniquely identifies the ownership. After embedding the watermark, there should be no perceptual degradation. These watermarks should be robust against intentional and unintentional attacks. It discourages the copyright violation and help to determine the authenticity and ownership of the data.

II. Important Aspects of Video Watermarking

A watermark is a digital code permanently embedded into the digital cover content i.e. text, audio or video sequence. A watermark can carry any information you can imagine but the amount of the information is not unlimited. The amount of information that can be embedded into the video sequence is called payload. The more information a watermark carries the more vulnerable that information is. Anyway, the amount is absolutely limited by the size of particular video sequence. Watermarking prefers robustness to capacity, thus a watermark typically carries tens to thousands of hidden information bits per one video frame [11][23].

To be effective, watermark should possess the properties such as –

A. Unobtrusive -
The watermark should be perceptually invisible.

B. Robustness -
The watermark should be impossible to remove even if the algorithmic principle of the watermarking method is public. Of course, any watermark can be removed with sufficient knowledge of particular embedding process. The watermark should be robust against a wide range of attacks.

In particular, the watermark should be robust to:

1) Common signal processing: The watermark should be retrievable even if common signal processing operations (such as digital-to-analog and analog-to-digital conversion, resampling, recompression and common signal enhancements to image contrast and color) are applied to the video sequence.

2) Common geometric distortions: The watermark should be immune from geometric image operations (such as rotation, cropping and scaling).

3) Subterfuge attacks: Collusion and Forgery: The watermark should be robust to collusion by multiple individuals who each possesses a differently watermarked copy of the same content combining their copies to destroy the watermark. Moreover, it should be impossible to combine the copies to create a new valid watermark.

C. 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.

D. Loyalty -
A watermark has a high reliability, if the degradation it causes is very difficult to perceive for the viewer.

E. Computational Cost -
Embedding and extraction of watermark from the video both should be fairly fast and should have low computational complexity.
F. Interoperability

Watermark system must be interoperable for the compressed and decompressed operations.

G. 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.

III. ATTACKS ON WATERMARK

This section gives a survey of possible attacks on watermarks[11][23]. Watermark attacks can be classified as -

A. Simple attacks

These attacks attempt to damage the embedded watermark by modifications of the whole image without any effort to identify and isolate the watermark. These attacks include frequency based compression, addition of noise, cropping and correction.

B. Detection-disabling attacks

These attempts to break correlation and to make detection of the watermark impossible. 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. Mostly, they make some geometric distortion like zooming, shift in spatial or (in case of video) temporal direction, rotation, cropping or pixel permutation, removal or insertion. The watermark in fact remains in the cover content and can be recovered with increased intelligence of the watermark detector.

C. Ambiguity attacks

These attempts to confuse 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. Examples include additive attacks in which an adversary or malicious user can augment host by inserting his own watermark.

D. Removal attacks

These attacks attempt to analyse or estimate (from more differently watermarked copies) the watermark, separate it out and discard only the watermark. Examples are subtractive attacks, collusion attack, denoising or exploiting conceptual cryptographic weakness of the watermark scheme.

IV. APPLICATIONS

This section describes the various field where video watermarking techniques are used for security purpose. The major applications of digital video watermarking includes video authentication, copyright protection, broadcast monitoring, copy control, fingerprinting, taper resistance, ownership identification, video tagging and enhance video coding. Some of them are explained below[9][23]:

A. Copyright protection:

Copyright protection is the very first targeted application and hence the main issue in digital data delivery networks. In digital multimedia, watermarking is used as copyright protection to identify the copyright owner. There are many techniques of video watermarking for copyright protection. In one of the techniques a robust watermark is added to the video signal that carries information about sender and receiver of the delivered video.

B. Video authentication:

In applications involving instance videos captured by surveillance cameras, checking the integrity of the images and the video is a major issue. Fragile, semi fragile and robust watermarking are the commonly used policies. 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. The scheme is robust to content-preserving manipulations and sensitive to content-changing manipulations.

C. Broadcast monitoring of video sequences:

In broadcast monitoring the content owner embeds the watermark prior to transmission. The watermark is extracted by the monitoring site that is set up within the transmission area. 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:

Copy protection is a widely used application in video watermarking. A watermark is used to indicate whether a video content is copyrighted. Watermarking system has the available technologies in which the information is secured into the header and it prevents from copying of that data. This watermark can only be removed with a severe degradation of the video sequence.

E. Fingerprinting (Distribution):

In this technique the video is uniquely identified by its resultant fingerprint by software that recognizes extracts and then compresses distinguishing components of a video. Key frame analysis, color changes, motion changes are some of the features involved. 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. The customer ID is embedded into the video as a watermark to track back any user breaking his license agreement.

V. VIDEO WATERMARKING TECHNIQUES

Different digital video watermarking algorithms have been proposed. Video watermarking techniques are classified according to their working domain [11]. Some techniques embed watermark in the spatial domain by modifying the pixel values in each frame extracted from the video. These methods are not robust to attacks and common signal distortions. In contrast, other techniques embed the watermark in the frequency domain, which are comparatively more robust to distortions.

A. Spatial Domain Watermarks

The spatial domain watermarking techniques embed the watermark by modifying the pixel values of the host image/video directly. In case of attacks destroying data, a single surviving watermark can be considered a success. Although they are robust to attacks like cropping, noise, lossy compression, etc, 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 major advantages of pixel based methods are that they are conceptually simple and have very low computational complexities. Therefore they are widely used in video watermarking where real-time performance is a primary concern. However, they also exhibit some 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.

1) Correlation based techniques:

In correlation based technique[23], the watermark W(x,y) is added to the original content O(x,y) according to the equation (1).

\[ O'(x,y) = O(x,y) + kW(x,y) \]  

(1)

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

2) Least Significant Bit modification (LSB):

The most frequently used technique is Least Significant bit (LSB)[23]. 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. There are some limitations like, poor quality of the produced video, inefficient in dealing with the various attacks, least robustness and lack of imperceptibility.

B. Frequency Domain Watermarks

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). 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 watermarked image/video is finally obtained by applying the inverse transform. Several researches concentrated on using DWT because of its multi resolution characteristics, it provides both spatial and frequency domain characteristics so it is compatible with the Human Visual System (HVS). Also the recent trend is to combine the DWT with other algorithms to increase robustness and invisibility.

1) DCT:

Discrete Cosine Transform (DCT) is an important method for video watermarking. A lot of digital video watermarking algorithms embed the watermark into this domain[23]. 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.

2) DWT:

Discrete Wavelet Transform (DWT) is a transform based on frequency domain.

As shown in figure 1 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.

VI. RELATED WORK

In this section we review various schemes of watermarking that have been proposed. Different schemes are proposed to achieve more robustness and imperceptibility. Previous work had been done on watermarking using DCT, DWT and other techniques to achieve robustness without affecting the quality of the video.

Hanane H. Mirza et al. [3] propose a digital video watermarking scheme based on Principal Component Analysis. An imperceptible watermark is embedded into the three different RGB channels of the video frame separately using PCA transform. The main advantage of this approach is that the same or multi-watermark can be embedded into the three color channels of the image in order to increase the robustness of the watermark. Using PCA transform allows choosing the suitable significant components into which to embed the watermark. The preliminary results show a high robustness against most common video attacks, especially frame dropping, cropping and rescaling for a good perceptual quality.

Sadik. A.M . Al-Taweel et. Al. [13] proposed a novel DWT-based video watermarking algorithm based on a three-level DWT using Haar filter which is robust against geometric distortions such as Downsampling, Cropping, and Rotation. It is also robust against Image processing attacks such as low pass filtering (LPF), Median filtering, and Weiner filtering. Furthermore, the algorithm is robust against Noise attacks such as Gaussian noise, Salt and Pepper attacks. The embedded data rate is high and robust. The experimental results show that the embedded watermark is robust and invisible. The watermark was successfully extracted from the video after various attacks.

Salwa A.K Mostafa et. al. [4] presents a novel technique for embedding a binary logo watermark into video frames. PCA is applied to each block of the two bands (LL – HH) which result from Discrete Wavelet transform of every video frame. The watermark is embedded into the principal components of the LL blocks and HH blocks in different ways. Experimental results show no visible difference between the watermarked frames and the original frames and show the robustness against a wide range of attacks such as MPEG coding, JPEG coding, Gaussian noise addition, histogram equalization, gamma correction, contrast adjustment, sharpen filter, cropping, resizing, and rotation. Combining the two transforms improved the performance of the watermark algorithm.

Manish Choubisa et. al. [7] proposed algorithm of digital watermarking technique based on DCT (Discrete Cosine Transformation) using permuting the image. Through adjusting the block DCT coefficient of the image the watermarks are invisible. The images are first permuted and then converting into block allowing to 8x8 pixel and thus the watermark images are embedded through adjusting their DCT coefficient.

Sanjana Sinha et. al. [2] proposed a comprehensive approach for watermarking digital video by using a hybrid digital video watermarking scheme based on Discrete Wavelet Transform (DWT) and Principal Component Analysis (PCA). PCA helps in reducing correlation among the wavelet coefficients obtained from wavelet decomposition of each video frame thereby dispersing the watermark bits into the uncorrelated coefficients. The video frames are first decomposed using DWT and the binary watermark is embedded in the principal components of the low frequency wavelet coefficients. The imperceptible high bit rate watermark embedded is robust against various attacks that can be carried out on the watermarked video, such as filtering, contrast adjustment, noise addition and geometric attacks.

Nisreen I Yassin et. al. [1] introduced a comprehensive approach for digital video watermarking, where a binary watermark image is embedded into the video frames. Each video frame is decomposed into sub-images using 2 level discrete wavelet transform then the Principle Component Analysis (PCA) transformation is applied for each block in the two bands LL and HH. The watermark is embedded into the maximum coefficient of the PCA block of the two bands. Experimental results show high imperceptibility where there is no noticeable difference between the watermarked video frames and the original frames. The proposed scheme shows high robustness against several attacks such as JPEG coding, Gaussian noise addition, histogram equalization, gamma correction, and contrast adjustment.

U. Mehraj Ali, et. al. [5] proposed a wavelet based watermarking technique with the combination of PCA transform. DWT is more computationally efficient than other transform methods like DFT and DCT. Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify areas in the host video frame where a watermark can be embedded imperceptibly. PCA is basically used to hybridize the algorithm as it has the inherent property of removing the correlation amongst the data i.e. the wavelet coefficients and it helps in distributing the watermark bits over the sub-band used for embedding thus resulting in a more robust watermarking scheme that is resistant to almost all possible attacks. The watermark is embedded into the luminance component of the extracted frames as it is less sensitive to the Human Visual System (HVS).
Nikita Kashyap et. al. [6] have implemented a robust image watermarking technique for the copyright protection based on 3-level discrete wavelet transform (DWT). In this technique a multi-bit watermark is embedded into the low frequency sub-band of a cover image by using alpha blending technique. The insertion and extraction of the watermark in the grayscale cover image is found to be simpler than other transform techniques. The proposed method is compared with the 1-level and 2-level DWT based image watermarking methods by using statistical parameters such as peak-signal-to-noise-ratio (PSNR) and mean square error (MSE). The experimental results demonstrate that the watermarks generated with the proposed algorithm are invisible and the quality of watermarked image and the recovered image are improved.

Gaurav Bhatnagar et. al. [8] proposed a wavelet packet transform (WPT)-based robust video watermarking algorithm. A visible meaningful binary image is used as the watermark. First, sequent frames are extracted from the video clip. Then, WPT is applied on each frame and from each orientation one sub-band is selected based on block mean intensity value called robust sub-band. Watermark is embedded in the robust sub-bands based on the relationship between wavelet packet coefficient and its 8-neighbour (DB) coefficients considering the robustness and invisibility. Experimental results and comparison with existing algorithms show the robustness and the better performance of the proposed algorithm.

VII. CONCLUSION

In this paper we revised various proposed video watermarking algorithm and characteristics of a watermark. Also we reviewed the various common attacks on the watermark. Embedding the watermark in low frequencies obtained by wavelet decomposition increases the robustness against attacks like filtering, lossy compression and geometric distortions while making the scheme more sensitive to contrast adjustment, gamma correction, and histogram equalization. Embedding the watermark in high frequency sub-bands makes the watermark more imperceptible while embedding in low frequencies makes it more robust against a variety of attacks. As a result, video watermarking is a potential approach towards protecting the ownership rights.

REFERENCES


