International Journal of Communication Networks and Security

Volume 2 | Issue 1 Article 7

January 2013

STUDY ON AUDIO AND VIDEO WATERMARKING

HARLEEN KAUR
Dept of Computer Science Engg., Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab,
herleenkaur51521@gmail.com

STUDY ON AUDIO AND VIDEO WATERMARKING

HARLEEN KAUR

M.tech, Computer Science Engg., Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab

Abstract- This paper gives the overview of audio and video watermarking. This paper introduces the basic requirements that affect the algorithms for audio and video watermarking which are perceptibility, robustness and security. The attacks which cause manipulations of the audio and video signals are also discussed. The common group of attacks on audio and video data is dynamics, filtering, conversion, compression, noise, modulation, time stretch and pitch shift, multiple watermark, cropping, rotation etc. The applications of audio and video watermarking are Fingerprinting, copyright protection, authentication, copy control etc. The audio watermarking techniques can be classified into Time-domain and Frequency-domain methods and video watermarking techniques are classified into spatial domain, frequency domain and format-specific domain.

I. INTRODUCTION

Watermarking is a popular technique for hiding proprietary information in digital media like images, digital audio or digital video. Its significance lies in protecting the authenticity of multimedia objects to prevent copies to be created, exchange, and modification of such objects. Several watermarking schemes have been proposed in recent years, based on different areas of applications of text, images, audio and video. This paper presents the comparative analysis of audio and video watermarking from different perspectives. Section II presents the audio and video watermarking basic requirements. Section III presents the various audio and video attack Problems. Section IV presents applications of text, audio and video watermarking and lastly, Section V presents audio and video techniques.

II. AUDIO AND VIDEO WATERMARKING BASICS

There could be various requirements with respect to which audio/video watermarking algorithms which must be optimized. The basic requirements or features that affect the audio/video watermarking algorithms are:-

1) Perceptibility: There are varieties of watermarks categories present. One of these is perceptible and imperceptible watermarks. Perceptible watermarks are patterns visible to the eye like logos inserted into one corner of images, whereas imperceptible are invisible to human eye. Usually copyright protection methods use imperceptible watermarks, whereas perceptible watermark is normally used for publically available digital content, where the unauthorized reproduction or usage has been prohibited.
Perceptible watermarks have been mostly used in applications involving images and video. Less study has been on perceptible watermarking in audio application. But still the imperceptible watermarking is preferred to the perceptible one both for audio and video, since the quality degradation is at minimum. In case of audio file, perceptibility relates to audio signal quality and in case of video it relates to quality of visual patterns and its audio signals.

2) Robustness: The watermark must be robust against attacks on digital content and try to remove or impair the watermark.

3) Security: The embedded information must be secure against tampering.[6]

4) Capacity: The amount of embedded information must be large enough to uniquely identify the owner of the video.[6]

III. ATTACKS ON AUDIO AND VIDEO

Attacks in audio applications results in manipulations of its audio signals whereas video applications involve attacks on its audio content and visual content. There are some common groups of attacks on audio and video data like filtering, compression, noise addition etc. There are some other categories of attacks which occur mostly on audio data, there can be sample permutation based attacks or pitch shift. On video data, most popular attacks are geometric and statistical attacks of which the most frequent are cropping, scaling and rotation, statistical averaging etc.

1) Dynamics: These modify (Increase or decrease) the loudness profile of an audio or video file. There are even frequency dependent compression algorithms which only affect a part of the frequency range.[1]

2) Filter: Filters cut off or increase a selected part of the spectrum. The most basic filters are high-pass and low-pass filters but equalizers can also be seen as filters, they are usually used to increase or decrease certain parts of a spectrum [1]. Low-pass filtering, for instance, does not introduce

considerable degradation in watermarked videos or audio, but can dramatically affect the performance, since spread-spectrum-like watermarks have non negligible high-frequency spectral contents.[5]

3) Conversion: This involves most frequent attacks which modify the format of Audio or video material. For instance, changing the sample size or sampling frequency.

4) Compression: This is commonly found unintentional attack in multimedia applications. Most of the digital content like Audio, video and images exchanged over Internet are generally compressed.

5) Noise: Most hardware components in an audio and video chain can induce noise into the signal. A very common attack also is to try to add noise to destroy the watermark.[1]

6) Modulation: As most audio and video processing software includes modulation effects like vibrato, chorus, amplitude modulation or flanging, they can be used as attacks to watermarks.[1]

7) Time stretch and pitch shift: These either change the length of an audio or video event without changing its pitch or change the pitch without changing the length.[1]

8) 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.[5]

9) Sample permutations: This is a group of attacks for instance, sample permutation, dropping samples and similar approaches on audio manipulation in specialized environments.

10) Cropping: This attack on video data involves attacking a small portion of the watermarked object, such as removing certain images or frames of a video sequence.

11) Rotation and Scaling: Rotation and scaling is the most frequent attacks to affect the visual content of a video.

12) Frame Dropping: unlike, scaling and cropping which affects each frame of the video sequence equally, frame dropping has unequal affects based on significance of frames for the scenes of the video.

13) Statistical Averaging: Watermark can be estimated and 'unwatermarked' by subtracting the estimate. This could be dangerous if the watermark is made independent of the data.

IV. AUDIO AND VIDEO WATERMARKING APPLICATIONS

Digital audio and video watermarking is used in a variety of applications:-

1) Fingerprinting:. Secret watermarks are embedded as fingerprints on the audio or video for unique identification of audio/video data. Some of the features that are involved in video fingerprinting analysis are key frame analysis, color changes, motion changes etc. of a video sequence [6]. In audio applications, "Fingerprint" watermarks provide information that allows one to track an audio clip's usage history and this feature is used by many record companies and advertisers as a feedback about the popularity of a particular song or the number of times a commercial was played[2].

2) Copyright protection: copyright protection of data is an important issue for distributing digital audio/video content over networks. From the watermarked multimedia data, copyright owner can be identified and the real owner will be able to prove himself in case of any multiple ownership issue.

3) Broadcast Monitoring: In broadcast monitoring (similar to TV or radio broadcasting) the content owner embeds the watermark prior to transmission and this watermark is extracted by the monitoring site that is set up within the transmission area [6].

4) Video or audio Authentication:
Checking the audio/video integrity is major issue in applications involving instance audio/videos recording. Based on the requirements fragile, semi fragile or robust watermarking can be used. A slight modification in the audio or video content destroys fragile watermarks. Semi fragile watermarking can resist content conserving operations and be sensitive to content varying transforms [6].

5) Copy control: Watermarking schemes are most commonly designed for copyright protection to resolve piracy disputes [2]. It is possible for recording and playback devices to react to embedded signals. In this way, a recording device might inhibit recording of a signal if it detects a watermark that indicates recording is prohibited [3]. In other words, illegal or unauthorized copying of data can be prevented.

V. AUDIO AND VIDEO WATERMARKING TECHNIQUES

A. Audio Watermarking Techniques

The amount of data that can be embedded into audio is considerably low than amount that can be hidden in images, as audio signal has a dimension less than two-dimensional image files. Embedding additional information into audio sequence is a more tedious

than images, due to dynamic supremacy of HAS than HVS [4].

Considering the embedding domain, audio watermarking techniques can be classified into time domain and frequency domain methods. Time domain watermarking schemes are relatively easy to implement and require less computing resources compared to transform domain watermarking methods, but are usually weaker against signal-processing attacks compared to the transform domain counterparts [8].

Phase modulation and echo hiding are well known methods in the time domain. In frequency domain watermarking, after taking one of the usual transforms such as the Discrete/Fast Fourier Transform (DFT/FFT) , the Modified Discrete Cosine Transform (MDCT) or the Wavelet Transform (WT) from the signal, the hidden bits are embedded into the resulting transform coefficients. Usually frequency domain provides excellent robustness against attacks. In fact, using methods based on transforms provides a better perception quality and robustness against common attacks at the price of increasing the computational complexity [8].

Audio watermarking popular techniques involve:

1) Least Significant Bit Coding

This simple approach in watermarking audio sequences is to embed watermark data by altering certain LSBs of the digital audio stream with low amplitude [4].

2) Phase coding

The basic idea is to split the original audio stream into blocks and embed the whole watermark data sequence into the phase spectrum of the first block [4].

3) Quantization Method

A scalar quantization scheme quantizes a sample value x and assign new value to the sample x based on the quantized sample value. In other words, the watermarked sample value y is represented as follows:

$$y = q(x,D) + D / 4 \text{ if } b = 1,$$
$$y = q(x,D) - D / 4 \text{ otherwise} \quad (1)$$

In (1) q (·) is a quantization function and D is a quantization step. A quantization function q (x) is given as $q(x,D) = [x / D].D$, where [x] rounds to the nearest integer of x. A sample value x is quantized to q(x, D). Let q (x, D) denote anchor. If the watermarking bit b is 1, the anchor is moved. Otherwise, the cross (×) stands for the watermarking bit 0 [4].

4) Spread-Spectrum Method

This scheme spreads pseudo-random sequence across the audio signal. The wideband noise can be spread into either time-domain signal or transform domain signal. Frequently used transforms include DCT, DFT, and DWT [4].

5) Replica Method

Replica modulation embeds part of the original signal in frequency domain as a watermark. Echo hiding embeds data into an original audio signal by introducing an echo in the time domain. Multiple echoes can be added [4]. Recovery of the watermark is accomplished by using signal analysis techniques to detect echos in the transmitted signal to discern which type of echo occurs in each segment of the signal. By translating the series of echo types into a binary string, the watermark can be recovered [7].

B. 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 [5].

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

1. Spatial domain
2. Frequency domain
3. Format-specific

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. Compared to spatial-domain techniques, frequency-domain watermarking techniques proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithms[6].

1). Spatial Domain Video Watermarking Technique

Spatial methods involve simple techniques of embedding watermark with the host signal and embedding that takes place directly in the pixel domain, being mostly found attractive for real-time video watermarking applications [6].

1.1 Least Significant Bit Modification

Technique used is to insert a watermark into the LSB of pixels that are located in the vicinity of image contours. As the LSB technique was implied, modifications of LSB's destroyed the watermark However, the LSB techniques also exhibit some major limitations-

• Since absolute spatial synchronization is required, susceptibility to de-synchronization attacks is increased.
• Multiple frame collusions may occur due to lack of consideration of the temporal axis.
• Watermark optimization is difficult using only spatial analysis techniques [6].

1.2 Correlation-Based Techniques
Another technique for watermark embedding is to exploit the correlation properties of additive pseudo-random noise patterns which is a two-dimensional signal and was transformed in the DCT domain, the new bit rate is compared with the original and, depending on the bit rate; the original DCT block is selected [6].

2.) Frequency Domain Video Watermarking Techniques
Frequency domain watermarks are hard to be deleted once embedded, addresses the limitations of pixel-based methods and support many additional features. 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 [6].

2.1 DWT Domain Video Watermarking Techniques
All frames of the video are decomposed in 4-level sub band frames by separable two-dimensional (2-D) wavelet transform. Scene changes are detected from the video by applying the histogram difference method on the video stream. Independent watermarks are embedded in frames of different scenes. The watermark is then embedded to the video frames by changing position of some DWT coefficients [6]. It is believed to be more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to [6].

2.2 SVD Domain Video Watermarking Technique
Singular Value Decomposition (SVD) is a numerical technique for diagonal zing 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:

$$A=U\ S\ V^T$$

Where U and V Є R N x N are unitary and S Є R N x 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. The columns of the U matrix are called the left singular vectors while the columns of the V matrix are called the right singular vectors of A. Each singular value σ_i specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image layer. In SVD-based watermarking, an image is treated as a matrix decomposed by SVD into the three matrices; U, S and V^T. By virtue of the fact that slight variations in the elements of matrix S does not affect visual perception of the quality of the cover image, most existing SVD-based watermarking algorithms add the watermark information to the singular values of the diagonal matrix S in such a way to meet the imperceptibility and robustness requirements of effective digital image watermarking algorithms [6].

2.3 DCT Domain Video Watermarking Technique
The watermark signal is not only designed in the spatial domain, but sometimes also in a transform domain like the full image discrete cosine transform (DCT) domain or block-wise DCT domain.

The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high Frequency). The DCT transforms a signal or image from the spatial domain to the frequency domain. DCT-based watermarking scheme is the most robust to lossy compression [6].

2.4 Feature Domain PCA based Video Watermarking Technique
The mathematical procedure of transforming a number of possibly correlated variables into a smaller number of uncorrelated variables is called Principal component analysis (PCA). The smaller numbers of uncorrelated variables are called principal components. Given a data set, the principal component analysis reduces the dimensionality of the data set. The video shots are detected based on informational content, and color similarities. The key frames of each shot are extracted and each key frame is composed of three color channels. Embedding of the watermark is done in the three color channels RGB of an input video file [6].

2.5 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 of each GOP 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 [6].

3.) Format- specific technique: MPEG based watermarking schemes

Video watermarking techniques that use MPEG-1, -2 and -4 coding structures as primitive components are primarily motivated with a 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].

VI. CONCLUSION AND DISCUSSION

This paper introduces the watermarking of audio and video data. In this paper, the basic requirements viz perceptibility, robustness and security that must be optimized by the audio and video algorithms, are discussed. The attacks which cause manipulations on the content of audio and video data are also discussed. The common attacks on audio and video data are filtering, conversion, compression, noise, time stretch and pitch shift, cropping, rotation and scaling etc. Digital audio and video watermarking is used in variety of applications such as Fingerprinting, Copyright protection, Audio or video authentication, copy control etc.

In this paper, various audio and video watermarking techniques are also discussed. The audio watermarking techniques can be classified into time-domain and frequency-domain methods. Time-domain methods are relatively easy to implement and require less computing resources compared to transform-domain. On the other hand, time-domain methods are usually weaker against signal processing attacks compared to transform domain counterparts. Similarly, the video watermarking techniques are classified into spatial domain, frequency domain and format-specific domain methods. Spatial domain techniques are easy to implement and require few computational resources; however they are not robust against common digital signal processing operations such as compression. On the other hand, frequency-domain techniques proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking techniques.

REFERENCES

[1] Steinebach, Petitcolas, Raynal, Dittmann, Fontaine, Seibel, Fates, Croce-Ferri, "StirMark Benchmark: Audio watermarking attack," Int. Conference on Information Technology: Coding and Computing (ITCC 2001), April 2 - 4, Las Vegas, Nevada, S. 49 - 54, ISBN 0-7695-1062-0, 2001.

[2] Adam Brickman, "Literature Survey on Audio Watermarking," EE381K - Multidimensional Signal Processing March 24, 2003.

[3] Vivek Kumar Agrawal, "Perceptual Watermarking Of Digital Video Using The Variable Temporal Length 3d-Dct," 2007.

http://www.security.iitk.ac.in/contents/publications/more/Vi-vek_thesis.pdf

[4] L. Robert, T.Shanmugapriya, "A Study on Digital Watermarking Techniques," International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009.

[5] T.JAYAMALAR, Dr. V. RADHA, "Survey on Digital Video Watermarking Techniques and Attacks on Watermarks," International Journal of Engineering Science and Technology , Vol. 2(12), 2010, 6963-6967

[6] Rini T Paul, "Review of Robust Video Watermarking Techniques," IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011

[7] Fred Hatfull, "Watermarking Audio Data: A Survey And Comparison of Techniques for Audio Steganography," CASE WESTERN RESERVE UNIVERSITY, 2011,

http://fredhatfull.com/media/talks/watermarking_audio/Wat-ermarking%20Audio%20Data.pdf

[8] M. Fallahpour and D. Megias, "High capacity audio watermarking using the high frequency band of the wavelet domain," Journal Multimedia Tools and Applications, April 2011, Volume 52, Issue 2-3, pp 485-498

◈◈◈