Review of Robust Video Watermarking Techniques

Rini T Paul
M-Tech Computer Science Specialization in Data Security
Toc h Institute of Technology, Arakkunam, Kerala

ABSTRACT
There has been a remarkable increase in the data exchange over web and the widespread use of digital media. The mounting interest with reference to digital watermarking throughout the last decade is certainly due to the increase in the need of copyright protection. Applications of video watermarking in copy control, broadcast monitoring, finger printing, video authentication, copyright protection etc is immensely rising. The main aspects of information hiding are capacity, security and robustness. The skill of anyone detecting the information is security and robustness refers to the resistance to modification of the cover content before concealed information is destroyed. Video watermarking algorithms normally prefers robustness. In robust algorithm it is not possible to eliminate the watermark without rigorous degradation of the cover content. In this paper, we introduce the notion of Video Watermarking and features required to design a robust watermarked video for valuable application and focus on various domains of video watermarking techniques.

General Terms
Video watermarking, Security, Algorithms.

Keywords
DWT, Robust Techniques, SVD, Video Watermarking.

1. INTRODUCTION
Video Watermarking is a young and rapidly evolving field in the area of multimedia. Following factors have contributed towards the triggering of interest in this field. a) The society is contaminated by the tremendous privacy of digital data, as copying of digital media has become comparatively easy.

b) This is an era where need has arise for fight against "Intellectual property rights infringements".

c) Copyright protection must not be eroded due to malicious attacks

d) Tampering of the digital data needs to be concealed at some point.

The requirement of secure communication and digital data transfer has potentially increased with the development of multimedia systems. Data integrity is not secure in image transfers. The main technique used for protection of an Intellectual Property rights and copyright protection is digital water marking. The copyright data may be in the form of text, image, audio, and video [1, 2, 3]. Watermarking may be visible or invisible. Invisible watermarking implies that the presence of the watermark is barely discernible when the watermarked signal is displayed.

There are several techniques for information hiding into digital media. They are used for several purposes as well as copyright protection. Two basic methods of information hiding are cryptography and steganography. The concept of digital watermarking is derived from steganography. The term steganography means "cover writing" and cryptography means "secret writing". Cryptography is a widely used method for protecting the digital content of the media. The message is encrypted before transmission and decrypted at the receiver end with the help of a key. No one can access the content without having the true key. The message is called the plain text and the encrypted message is called the cipher text. The information is protected before the time of transmission. But, after decryption, the information becomes unprotected and it can be copied and distributed.

In steganography, the message is embedded into the digital media rather than encrypting it in such a way that nobody except the sender and the intended recipient can even realize that there is a hidden message. The digital media content, called the cover, can be determined by anybody; but, the message hidden in the cover can be detected by only the person having the actual key. Thus steganography actually relates to covering point-to-point communication between two parties. That's why steganography methods are usually not robust against modification of the data, or have only limited robustness.

Watermark embedding may bring in diminutive distortion into the audible or visible components of the watermarked signal. If the watermark cannot be easily removed from the watermarked signal even after applying common watermarking attacks then it is referred as robust embedding.

The basic components involved in robust watermarking are watermark embedding, attack, and watermark detection. In watermark embedding, a watermark signal (Text, image or audio etc) is constructed and then embedded into an original signal (Video) to produce the watermarked signal. Once embedding is done, the watermarked video can be subjected to various attacks. During watermark detection, the watermark detector is given a test signal that may be watermarked, attacked or not. The watermark detector reports whether the watermark is present or not on examining the signal at its input.

This paper is organized five sections. The subsequent section explains the important aspects of video watermarking. Section 3 focuses the widespread applications of video watermarking. Section 4 considers the robustness aspect by elaborating on

the common attacks in video watermarking. The various domains of video watermarking are explored and a robust algorithm in each domain is considered in Section 5.

2. IMPORTANT ASPECTS OF VIDEO WATERMARKING

Video watermarking embeds data in the video for the purpose of identification, annotation and copyright. A number of video watermarking techniques have been proposed [4]. These techniques exploit different ways in order to embed a robust watermark and to maintain original video fidelity Conventional encryption algorithms permit only authorized users to access encrypted digital data. Once such data are decrypted, however, there is no way in prohibiting its illegal copying and distribution.

Many algorithms for developing watermarks on images are extended for videos.

a) Between the frames there exists a huge amount of intrinsically redundant data.

b) There must be a strong balance between the motions and the motionless regions

c) Strong concern must be put forth on real time and streaming video applications.

The following aspects are important for the design of Video watermarking systems.

a) Imperceptibility: The watermark embedding should cause as little degradation to the host video as possible.

b) Robustness: The watermark must be robust to common signal processing manipulations and attempts to remove or impair the watermark.

c) Security: The embedded information must be secure against tampering.

d) Capacity: The amount of embedded information must be large enough to uniquely identify the owner of the video.

3. APPLICATIONS OF VIDEO WATERMARKING

Digital video watermarking is used in a variety of applications.

a) Fingerprinting: 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. Some of the features that are involved in video fingerprinting analysis are key frame analysis, color changes, motion changes etc. of a video sequence. In this technique watermarks are embedded as fingerprints on the video. Several fingerprinting methods extract the fingerprints on the video. The evaluation and identification of the video content is then performed by comparing extracted fingerprints.

b) Copy control: Copy protection is a widely exercised application in video watermarking. In this a watermark is used to indicate whether a video content is copyrighted. This watermark can only be removed with a severe degradation of the video sequence.

c) Broadcast Monitoring: 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.

d) 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. A slight modification on the cover video destroys fragile watermarks. Semi fragile watermarking can resist content conserving operations and be sensitive to content varying transforms.

e) Copyright protection: copyright protection of video data is an important issue in digital video delivery networks. There are many techniques of video watermarking for copyright protection. In one of the techniques a watermark is added to the video signal that carries information about sender and receiver of the delivered

4. COMMON ATTACKS IN VIDEO WATERMARKING

The common attacks of video watermarking are frame dropping, frame averaging, statistical analysis, lossy compression, cropping and various signal processing and geometrical attacks[9].

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

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

5. TECHNIQUES IN VIDEO WATERMARKING

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 pre-determined 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. 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.

Video watermarking refers to embedding watermarks in a video sequence in order to protect the video from illegal copying and identify manipulations [5]. The necessary steps to embed the watermark into an input video data for the copy right protection purpose are as follows:

1. Extract loaded color video into frames.

2. Apply block matching motion estimation techniques on the subsequent frames.

3. Select only those frames that have sufficient number of motion blocks which is compatible with the watermark size.

4. From the selected frames use a given threshold to select the best blocks during the matching process.

5. Perform the wavelet transformation or different operations on the selected best blocks.

6. Embed a random Gaussian distribution as a proposed watermark into the selected blocks.

7. Extract the embedded watermark.

8. Apply some attacks on the watermarked frames in the video.

9. Evaluate the conducted results using PSNR for embedding and similarity for extracting process before and after attacks.

Color image is used as cover data the RGB value of each pixel is converted into RGB color spaces in which only R components constitute R color space, G components constitute G color space and B components constitute B color space. Watermark can be hidden in any one or in the three color channels. Since pixel values are highly correlated in RGB color spaces, information can be hidden in YUV color spaces. The RGB components of color image is converted into RGB color spaces which in turn is converted into YUV color spaces using below equation. The YUV color spaces consists of luminance (intensity) and chrominance (color) components YUV refers to the color resolution of digital component video signals, which is based on sampling rates. This means that some color information in the video signal is being discarded, but not brightness (luma) information. For these reasons the watermarking is added only to the Y component.

$$Y = 0.2989 * R + 0.5866 * G + 0.1145 * B$$

$$U = -0.1687*R-0.3312*G+0.5*B$$

$$V = 0.5 * R - 0.4183 * G - 0.0816 * B$$

Many algorithms have been proposed in the scientific literature for robust watermark embedding in video. In this paper we explore some most commonly used techniques for video watermarking.

5.1 Frequency Domain Video Watermarking Techniques

In these methods, a watermark that one wishes to embed distributively in overall domain of an original data, and the watermark, is hardly to be deleted once embedded. The main strength offered by transform domain techniques is that they can take advantage of special properties of alternate domains to address the limitations of pixel-based methods or to support 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.

5.1.1 DWT Domain Video Watermarking Techniques:

The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to compute multiple "scale" wavelet decomposition. One of the many advantages over the wavelet transform is that that it is believed to 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, such as the high resolution 32 detail bands LH, HL, HH. Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality[8]. DWT-based water-marking scheme is the most robust to noise addition.

For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub-bands LL, LH, HL and HH. The LL sub-band represents the coarse-scale DWT coefficients while the LH, HL and HH sub-bands represent the fine-scale DWT coefficients. To obtain the next coarser scale of wavelet coefficients, the LL sub-band is further processed until some final scale N is reached.

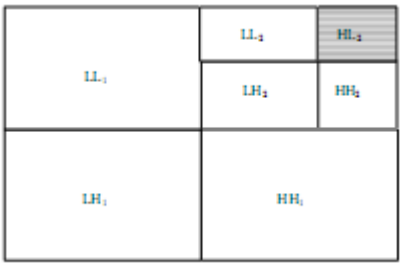

Figure 1. Frame's 2-level DWT sub-bands

The basic embedding algorithm in the paper can be summarized as

1. Watermark pre-process: - A watermark is scrambled into small parts as a part of pre-process. The watermark is first scaled to a particular size as

$$2 \wedge n <= m;\ n > 0 \text{ ---------- (1)}$$

$$p + q = n;\ p, q > 0 \text{ ---------- (2)}$$

Where m – No of scene changes and p, q, n – No of positive integer.

Size of watermark is determined by,

$$64.2 \wedge p * 64.2 \wedge q \text{ ---------- (3)}$$

Then the watermark is divided into 2^n small images with size 64.In the next step, each small image is decomposed into 8 bit-planes, and a large image can be obtained by placing the bit-planes side by side only consisting of 0s and 1s. These processed images are used as watermarks.

2. Video pre-process: - 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.

3. Watermark embedding: - The watermark is then embedded to the video frames by changing position of some DWT coefficients with the following condition:

If Wj= 1 then

Exchange (Ci, Ci+1, Ci+2, Ci+3, Ci+4);

else

Exchange (Ci, Ci+1, Ci+2, Ci+3, Ci+4);

end if

Where Ci is the ith DWT coefficient of a video frame, and Wj is the jth pixel of a corresponding watermark image.

4. Watermark detection

The video is processed to detect the video watermark.

The detection is done by the following logic

If (WC (i) > median (WCi, WCi+!, WCi+2, WCi+3,WCi+4);

Then EWj

Else EWj = 0

end if

5.1.2 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[6].

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 $\sigma i = \sigma i + 1$. 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 σi 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.

5.1.3 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. Features of DCT

a) The Characteristics of DCT coefficients must utilize few coefficients for providing excellent signal approximations.

b) Since the frequency components are ordered in a sequential order, starting with low frequency, mid frequency and high frequency components, a proper selection of the components can be prepared.

c) A smooth block is represented, if most of the high frequency coefficients are zero.

d) An edge block is represented, if the low frequency coefficients have large absolute values.

DCT is faster and can be implemented in O (n log n) operations. 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.

5.1.4 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.

5.1.5 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.

5.2 Spatial Domain Video Watermarking Technique

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. The watermark is applied in the pixel or coordinate domain The main strengths of pixel domain methods are that they are conceptually simple and have very low computational complexities[10]. As a result they have proven to be most attractive for video watermarking applications 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 temporal axis results in vulnerability to video processing and multiple frame collusion and watermark optimization is difficult using only spatial analysis techniques.

5.2.1 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.

5.2.2 Correlation-Based Techniques

Another technique for watermark embedding is to exploit the correlation properties of additive pseudo-random noise patterns as applied to an image. A pseudo-random noise (PN) pattern W(x, y) is added to the cover image I(x, y), according to the equation shown below

$$I_w(x,y) = I(x,y) + k \times W(x,y)$$

K denotes a gain factor, and IW the resulting watermarked image. Increasing k increases the robustness of the watermark at the expense of the quality of the watermarked image. To retrieve the watermark, the same pseudo-random noise generator algorithm is seeded with the same key, and the correlation between the noise pattern and possibly watermarked image computed. If the correlation exceeds a certain threshold T, the watermark is detected, and a single bit is set. This method can easily be extended to a multiple-bit watermark by dividing the image up into blocks.

6. CONCLUSION

In the paper we revised various video watermarking technique proposed in the literature in various domains. New approaches are expected to come out and may merge existing approaches. For example cascading two powerful mathematical transforms; the Discrete Wavelet Transform (DWT) and the Singular Value Decomposition (SVD). The two transforms are different transform domain techniques and thus provide different, but complementary, levels of robustness against the same attack.

7. REFERENCES

[1] G. Langelaar, I. Setyawan, and R. Lagendijk, "Watermarking Digital Image and Video Data: A State-of Art Overview," IEEE Signal Processing Magazine, vol. , pp. 20-46, Sep. 2000.

[2] G. Doerr and J. Dugelay, "A Guided Tour to Video Watermarking," Signal Processing: Image Communication, vol. 18, pp. 263-282, 2003.

[3] D. Kundur, K, Su, and D. Hatzinakos, "Digital Video Watermarking: Techniques, Technology, and Trends," in Intelligent Watermarking Techniques , chapter 10, P. Pan, H. Huang, and L. Jain, eds., World Scientific Computing, pp. 265-314, 2004.

[4] H. Hartung and B. Girod, "Watermarking of Compressed and Un-Compressed Video," Signal Processing, vol. 66, no. 3, pp. 283-301, May 1998. Cox, I. J., Miller, M. L., and Bloom, J. A. Digital Watermarking. Morgan Kaufmann Publishers, San Francisco, CA, 2002, pp. 26–36

[5] M. Rehan et al, A New Motion-Estimation Technique for Efficient Video Compression, IEEE Pacific Rim Conference, No. 1, pp. 326-330, 1997.

[6] H. Andrews and C. Patterson, "Singular Value decompositions and Digital Image Processing," IEEE Trans. on Acoustics, Speech, and Signal Processing, vol. 24, no. 1, pp. 26-53, Feb. 1976.

[7] P. Chan and M. Lyu, "A DWT-Based Digital Video Watermarking Scheme with Error Correcting Code," in Proceedings of the 5th International Conference on

Information and Communications Security, 2003, pp. 202-213.

[8] X. Niu and S. Sun, "A New Wavelet-Based Digital Watermarking for Video," in Proceedings of the 9th IEEE Digital Signal Processing Workshop, 2000, pp. 241-245.

[9] S. Voloshynovskiy, S. Pereira, and T. Pun, "Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks," Comm. Magazine, vol., pp. 118-126, Aug. 2001.

[10] E. Ganic and A. M. Eskicioglu, "Secure DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies," ACM Multimedia and Security Workshop 2004, Magdeburg, Germany, September 20-21, 2004.

[11] J. Lee et al, A survey of watermarking techniques applied to multimedia, IEEE International Symposium on Industrial Electronics, Vol. 1, pp. 272-277, 2001.