Digital Video Watermarking Techniques and Comparative Analysis : A Review

Gopal Prasad
Electronics Department
K. P. Engineering College
Agra, UP, India

Atul Kumar Singh
Electronics Department
K. N. I. T.
Sultanpur, UP, India

Arun Kumar Mishra
Electronics Department
K. P. Engineering College
Agra, UP, India

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 first perform a survey on available video watermarking techniques then we perform a comparative analysis based on robustness and computational complexity of different watermarking algorithms.

Keywords— *Image Processing, Digital Video Watermarking, Spatial Domain, Frequency Domain, Copy Right Protection.*

1. Introduction

Today digital media is available in a large scale, which can be easily copied and rapidly spread. People can acquire the copy of a digital media very easily; it may lead to large-scale unauthorized copies, which effect the development of the publishing industry. The owner of the content has to use some protection mechanism such as encryption or digital watermarking. Encryption is no longer sufficient for copy right protection and authentication, so digital watermarking is widely used. It is an art of embedding information in invisible and robust manner. Because the copy and temper of video is quite easy, in order to protecting copy right, digital video watermarking technology taken as an important and more urgent component. Recently, video based applications such that video conferencing, wireless videos, video broadcasting, set-top box, video-on-demand, videophone and internet multimedia are becoming more and more popular and has increased the demand for a secure distribution of videos.

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 [1]-[2].

The sudden increase in watermarking interest is most likely due to the increase in concern over IPR. Today digital data security covers such topics as access control, authentication, and copyright protection for still images, audio, video, and multimedia products. A pirate tries either to remove a watermark to violate a copyright or to cast the same watermark, after altering the data, to forge the proof of authenticity. Generally, the watermarking of still image, video, and audio demonstrate certain common fundamental concepts. Numerous watermarking applications reported, depends on the services we wish to support. Thus watermarking techniques may be relevant in various application areas including Copyright protection, Copy protection, Temper detection, Fingerprinting etc.

In this paper, we present the different video watermarking techniques. The rest of the paper is organized as follows. Section 2 provides an overview to digital watermarking with different video watermarking techniques and applications of video watermarking. Section 3 briefly describes the survey on video watermarking. Section 4 provides the performance analysis of different video watermarking techniques with respect to performance parameters like imperceptibility, robustness, fragility, tamper-resistance, normalized correlation and peak signal to noise ratio (PSNR). Conclusions are given in section 5 followed by references in section 6.

2. Digital watermarking

Digital watermarking also known as watermark insertion or watermark embedding, represents the method of inserting information into multimedia data also called original media or cover media e.g. text, audio, image, video. The embedded information or watermark can be a serial number or random number sequence, ownership identifiers, copyright messages, control signals, transaction dates, information about the creators of the work, bi-level or gray level images, text or other digital data formats. In the literature large number of text [3] [4], image [5], audio [6] and video [7] [8] watermarking algorithms can be found. These algorithms modify the original media to generate the watermarked media. There may be no or little perceptible differences between the original media and the watermarked media.

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.

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 algorithms modify the original media to generate the watermarked media. There may be no or little perceptible differences between the original media and the watermarked media.

Fig.1 gives an overview of different types of watermarking methodologies depending on their working domains, cover media, perceptibility and application areas. After embedding watermark, the watermarked media are sent over Internet or some other transmission channels. Whenever the copyright of the digital media is under question, the embedded information is decoded to identify copyright owner. The decoding process can extract the watermark from the watermarked media (watermark extraction) or can detect the existence of watermark in it (watermark detection).

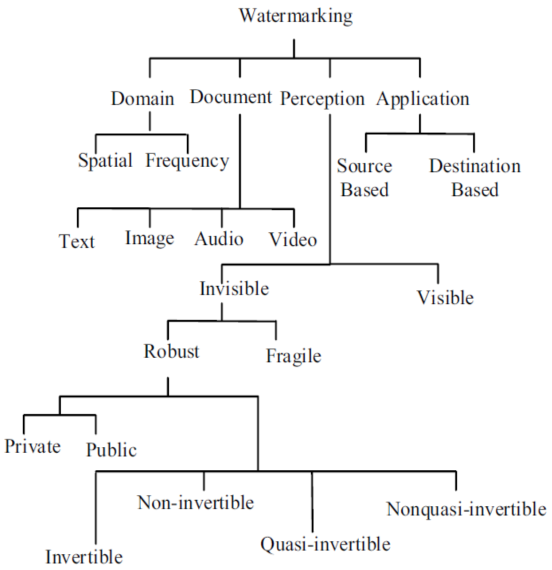

Fig.1. Different types of watermarking methodologies

The embedding or encoding process can be viewed as a function or mapping that maps the input *O* (original media), W (watermark) and/or *K* (key) to output *O '* (watermarked media) as shown in fig.2. Mathematically it can be expressed as

$$O' = E(O,W,[K]) \qquad (1)$$

where $E(\cdot)$ denotes the embedding process and $[\cdot]$ represents optional argument. Similarly the decoding or extraction process $D(\cdot)$ can be expressed formally as

$$W' = D(O'',[O],[K]) \qquad (2)$$

and the detection process $d(\cdot)$ can be expressed as

$$\{Yes\ or\ No\} = d(O'',[O],W,[K]) \qquad (3)$$

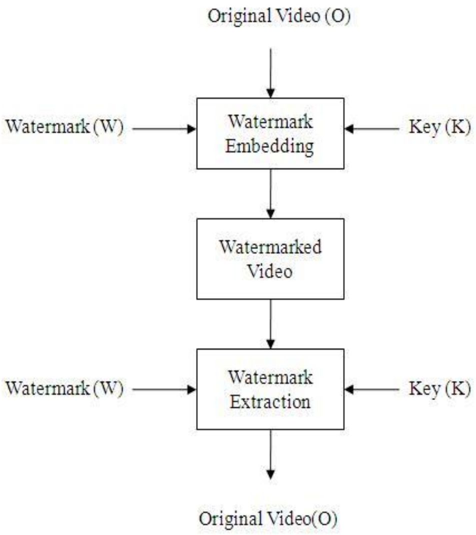

Fig.2. Block diagram of a video watermarking system

2.1. 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 [9]-[11], fingerprinting, ownership identification, authentication, taper resistance etc. or value added applications like legacy system enhancement, database linking, video tagging, digital video broadcast monitoring [12], Media Bridge [13] etc. Apart from robustness, reliability, imperceptibility and practicality the 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 pixel domain and transform domain techniques.

In pixel domain the watermark is embedded in the source video by simple addition or bit replacement of selected pixel positions. The main advantages of using pixel domain techniques are that they are conceptually simple to understand and the time complexity of these techniques are low which favors real time implementations. But these techniques generally lacks in providing adequate robustness and imperceptibility requirements.

In transform domain methods, the host signal is transformed into a different domain and watermark is embedded in selective coefficients. Commonly used transform methodologies are discrete cosine transformation (DCT) and discrete wavelet transformation (DWT). The main advantage of the transformed domain watermarking is the easy applicability of special transformed domain properties. For example, working in the frequency domain enables us to apply more advanced properties of the human visual system (HVS) to ensure better robustness and imperceptibility criteria.

2.2. 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. Some of them are explained below:

2.2.1. Copyright protection

Copyright protection is the very first targeted application for digital watermarking. In digital multimedia, watermarking is used as copyright protection to identify the copyright owner.

2.2.2. 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.

2.2.3. Broadcast monitoring of video sequences

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.

2.2.4. 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.

2.2.5. Fingerprinting (Distribution)

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.

3. Survey on video watermarking

Watermark can be either directly inserted in the raw video data or integrated during encoding process or implemented after compressing the video data. Now we shall briefly discuss some common video watermarking techniques.

Spread spectrum (SS) based watermarking technique was proposed in [11]. In the basic algorithm each bit of watermark a_j, $a_j \in \{-1, 1\}$ is spread over a large number of chips (*cr*) and modulated by a binary pseudo-noise sequence p_i, $p_i \in \{-1, 1\}$. The video and watermark are represented as vectors and scaled addition is carried out for watermark insertion. The retrieval of the watermark is carried out by high-pass filtering followed by correlation based method. The robustness of the algorithm can be increased by increasing *cr*, σ_p^2 (variance of pseudo random sequence), or μ_α (mean of locally adjustable amplitude factor). But an increase in cr reduces the data rate of the scheme, whereas increases in σ_p^2 or μ_α results in perceptibility of the watermark.

As DCT is a linear transformation and watermark is independent of the picture, the watermark can be added in the DCT domain. The 1D watermark vector is rearranged into frame structure and by transforming it to 8×8 DCT domain; the watermark can be added directly to a partially decoded video stream. Since the size and transfer rate of watermarked video should be identical to the original video, DCT coefficients of watermark and video frame are combined only if the resulting VLC code is of same length of the original one. Again drift compensation is required to cancel out watermark components from P and B frames, as motion compensated prediction or interpolation from other frames are added by the decoder to construct the P and B frames.

A 2D spread spectrum method for video watermarking (just another watermarking system, JAWS) was proposed in [12], which is used for monitoring video data transmitted over different broadcast links. This pixel domain watermarking scheme is distinctive for its enhanced payload capabilities and shift invariance.

A novel collusion resistant (CR) video watermarking approach is proposed in [14]. This is a practical frame by frame video watermarking technique. Here a basic $s \times s$ watermark pattern is first created and this pattern is repeatedly embedded so that it is centered on a fixed number of selected points known as anchors in every video frame. The part of the video frame where the basic watermark is embedded is called the footprint. Anchor points are calculated using feature extraction algorithm. As the content of the video frames changes, so do the selected feature points? As a result of that watermark footprints evolves with the video. After generating these watermark frames with in a given host frame, spatial masking is applied on it to ensue robustness and imperceptibility criteria. Then the scaled watermark is embedded in the host data using addition.

Watermarking using CDMA modulation was proposed in [15]. In this proposed methodology one of the four least significant bitplanes are replaced by watermark planes. The bitplanes to be replaced are selected according to a random periodic quaternary sequence. The watermark plane is generated using 1D spread spectrum methodology. For detection of the watermark, the author proposed a two-level hierarchical correlation methodology.

One of the first transformed domain video watermarking methods (TDC) was proposed by Cox et al. in [16]. The authors proposed and stressed on the importance of embedding the watermark into perceptually significant components to increase robustness against signal processing and lossy compression techniques. The watermark of length n was populated from a standard normal distribution apart from a binary PN sequence in order to enhance robustness. This method uses a non-blind approach for watermark detention. Detection is performed by transforming the original and test frame in the DCT domain and correlating the difference vector with the expected watermark pattern.

4. Performance analysis

4.1. Attacks on watermarks

In the field of digital watermark, there are various categorizations of attacks on watermarks. These can be categorized as follows

4.1.1. 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.

4.1.2. 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.

4.1.3. 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.

4.1.4. 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.

4.1.5. 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.

4.1.6. 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.

4.1.7. 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.

4.1.8. 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.

4.2. Performance Parameters

4.2.1. Imperceptibility

The watermark should not noticeably distort or degrade the host data in order to preserve the quality of the marked document.

4.2.2. Robustness

To measure robustness the watermark must be reliably detectable against signal processing schemes including data compression.

4.2.3. Fragility

These kinds of watermark are embedded in host data in such a way that they do not survive in the case of any modification even copying.

4.2.4. Tamper-resistance

The tamper-resistance property is focused on the intentional attacks in contrast to robustness.

4.2.5. Normalized Correlation

The key component of the images detection is the normalized correlation.

4.2.6. PSNR

Peak signal to noise ratio, should be as high as possible.

Table 1 shows performance analysis of different video watermarking techniques with respect to different performance parameters.

Table 1

Performance Parameters ⇒ **Watermarking Techniques** ⇓	**R**	**I**	**F**	**PSNR**	**NC**	**TC**
FMT	A	G	A	P	P	A
DCT	G	A	P	P	A	A
DFT	A	G	A	A	P	A
DWT	G	G	A	G	G	A
PCA	G	G	G	G	G	G
SS	G	A	G	G	A	A

FMT - Fourier-Mellin Transform, DCT - Discrete Cosine Transform, DFT - Discrete Fourier Transform, DWT - Discrete Wavelet Transform , PCA – Principle Component Analysis & SS- Spread spectrum. P- Poor, A- Acceptable, G- Good.

5. Conclusions

We have reached the conclusion that robustness, geometric attack, imperceptibility, PSNR (Peak Signal to Noise ratio) & NC (Normalized Correlation) are the most important requirements for a watermarking system. The performance analysis shown in this paper for different watermarking techniques is considering different Parameters. From the literature survey the performance is analyzed accordingly poor, acceptable and good. By observing this paper one can say the DWT (Discrete Wavelet Transform) and PCA (Principle Component Analysis) techniques have superior performance as compared to other techniques.

6. References

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

[2] I. J. Cox and M. L. Miller, "Electronic watermarking: the first 50 years". Fourth, IEEE Workshop on Multimedia Signal Processing, 2001, pp. 225-230.

[3] J. Brassil, S. Low, N. Maxemchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," IEEE J. Select. Areas Commun., vol. 13, pp. 1495–1504, Oct. 1995.

[4] S. Low and N. Maxemchuk, "Performance comparison of two text marking methods," IEEE J. Select. Areas Commun.(Special Issue on Copyright and Privacy Protection), vol. 16, pp. 561–572, May 1998.

[5] F. M. Boland, J. J. K. Ó Ruanaidh, and W. J. Dowling, “Watermarking digital images for copyright protection,” in Proc. Int. Conf. Image Processing and Its Applications, vol. 410, Edinburgh, U.K., July 1995.

[6] L. Boney, A. H. Tewfik, and K. H. Hamdy, “Digital watermarks for audio signals,” in Proc. EUSIPCO 1996, Trieste, Italy, Sept. 1996.

[7] F. Hartung and B. Girod, “Digital watermarking of raw and compressed video,” in Proc. SPIE Digital Compression Technologies and Systems for Video Commun., vol. 2952, Oct. 1996, pp. 205–213.

[8] F. Jordan, M. Kutter, and T. Ebrahimi, “Proposal of a watermarking technique for hiding/retrieving data in compressed and decompressed video,” ISO/IEC Doc. JTC1/SC29/WG11 MPEG97/M2281, July 1997.

[9] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for images, audio and video,” in Proc. IEEE Int. Conf. Image Processing (ICIP 96), Lausanne, Switzerland, Sept. 1996.

[10] J. S. Pan, H. C. Huang, L. C. Jain, “Intelligent Watermarking Techniques”.

[11] 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).

[12] T. Kalker, G. Depovere, J. Haitsma, M. Maes, “A video watermarking system for broadcast monitoring”, proceedings of the SPIE, vol. 3657, pp. 103-112, (1999).

[13] Digimarc Company Website: http://www.digimarc .com.

[14] K. Su, D. Kundur and D. Hatzinakos, “A novel approach to collusion-resistant video watermarking”, Proceedings of the SPIE, vol. 4675, pp. 491-502.

[15] B. G. Mobasseri, “Exploring CDMA for watermarking of digital video”, (1999) proceedings of of the SPIE, vol. 3675, pp. 96-102.

[16] I. J. Cox, J. Kilian. F. T. Leighton and T. Shamoon, “Secure spread spectrum watermarking for multimedia”, IEEE transactions on image processing, vol. 6, pp. 1673-1687, (1997).

Authors

Gopal Prasad was born in Mathura, UP, India. He received the Bachelor degree in Electronics and Communication Engineering from Uttar Pradesh Technical University, Lucknow, UP, India and completed his Master in Engineering Systems from Dayalbagh Educational Institute, Agra, UP, India, in 2011 and 2013 respectively. He was awarded with the Honors in B.Tech and University Gold Medal in M.Tech. Currently he is working as Assistant Professor in K. P. Engineering College, Agra, UP, India. His areas of interest include digital image and signal processing, video and audio compression, digital watermarking and encryption, script identification, fuzzy systems and applications, image denoising, pattern recognition.

Atul Kumar Singh was born in Farrukhabad, UP, India. He received the Bachelor degree in Instrumentation & Control Engineering from Bundel Khand University, Jhansi, UP, India in 2008 and pursuing Master in Electronics Engineering from KNIT, Sultanpur, UP, India. His areas of interest include digital systems, instrumentation systems (analog & digital), digital signal processing, digital watermarking, image denoising, control systems & process control.

Arun Kumar Mishra was born in Faizabad, UP, India. He received the Bachelor degree in Electronics Engineering from Kamla Nehru Institute of Technology, Sultanpur, UP, India and Master in Digital Communication & Networking from University B. D. T. College of Engineering, Davangere, Karnataka, India in 1995 and 2006 respectively. He has more than 14 years of teaching experience. Currently he is working as Assistant Professor in K. P. Engineering College, Agra, UP, India. His areas of interest include digital and wireless communication, digital signal processing, digital watermarking, microwave, signals and systems.