Engineering Science
2016; 1(1): 22-27
http://www.sciencepublishinggroup.com/j/es
doi: 10.11648/j.es.20160101.14

Review Article

Survey of Digital Video Watermarking Techniques and Its Applications

Ponni (a) Sathya Sethuraman[*], Ramakrishnan Srinivasan

Department of Information Technology, Dr. Mahalingam College of Engineering & Technology, Pollachi, Tamilnadu, India

Email address:
sathyaashok2007@gmail.com (Ponni (a) Sathya S.)
[*]Corresponding author

To cite this article:
Ponni (a) Sathya Sethuraman, Ramakrishnan Srinivasan. Survey of Digital Video Watermarking Techniques and Its Applications. *Engineering Science.* Vol. 1, No. 1, 2016, pp. 22-27. doi: 10.11648/j.es.20160101.14

Received: October 30, 2016; **Accepted**: December 22, 2016; **Published**: January 16, 2017

Abstract: Due to the rapid development of the internet, the usages of multimedia data like audio, image and video become very popular. Transmission of digital contents is an easy task but maintaining the ownership is a difficult one, for this various techniques has been proposed. One of the main techniques to protect the copyright is digital watermarking. The concept of digital watermarking has been derived from steganography. In video watermarking is used to provide authentication for the video content. The various video watermarking techniques have been developed, but those techniques are withstand only basic attacks not resistant to video processing attacks like frame dropping, frame swapping and average and addition of noise etc. In this paper reviewed several methodologies developed by various authors and also discussed their relative merits and demerits.

Keywords: Video, Watermarking, Authentication

1. Introduction

The first and foremost technique for data hiding is steganography. It is an embedding process, in which the sender and the receiver only know that some data has been hided inside the data. It is an end to end communication, if the third person knows that data has been hided, and then accessing the data is easy.

Cryptography is another encryption process of protecting the data during the transmission. In cryptography, a key is used to encrypt the original data, in the receiver side a key is used to decrypt the original data from the encrypted data. Even though third person knows the transmission of data, due to the secret key it cannot be extracted. There are two types in cryptography

1. Symmetric key cryptography
2. Asymmetric key cryptography

In symmetric key cryptography same key (secret key) is used for both encryption and decryption. So the secret key should be transferred between the senders to the receiver through a secured medium. If this can be possible then the actual data can be transferred through that medium itself. If suppose n number of users have to send secured data to n number of users then the usage of secret key will be (n*(n-1))/2.

In Asymmetric key cryptography, two keys called public key and private key. Each user has one private key and one public key. Public key is used to encrypt the data and private key is used to decrypt the data. In the encryption process the sender has to use the receiver public key to encrypt the data. And the receiver has to use his own private key to decrypt the data. So there is no transmission of keys and maintaining the keys also reduced.

So we are in need of high robustness and we should provide copyright to the content through the entire life span of the digital content. For this purpose we are going for watermarking technique.

Comparison of data hiding techniques:

In data hiding techniques, three parameters contributes major role that are capacity, security and robustness. Capacity refers to the amount of information to be hided, robustness refers to resistance to modification of the cover content before the hidden information is destroyed and security refers to ability of anybody to detect information. Watermarking prefers robustness, while Steganography demands capacity and security. Steganography provides poor robustness and cryptography provides the security during the transmission only. In cryptography once the data has been decrypted then the receiver can itself misuse the data.

So we are in need of high robustness and we should provide copyright to the content through the entire life span of the digital content. For this purpose we are going for watermarking technique.

2. Aspects on Video Watermarking

Video watermarking is the process of embedding digital data into the video sequence, for the purpose of identification, annotation and copyright. The digital data may be text, image or video. Image watermarking Techniques can be applied for video watermarking, but due to the redundancy of data it exhibits some additional properties**.**

2.1. Terminologies Used in Video Watermarking

Digital video:

Digital video is collection of frames which are equally time spaced.

Robustness:

Robustness means ability to resist the removal or modify of watermark from the original video. As a good watermarking system, it should be robust against various watermark attacks.

Non perceptibility:

It is important to check whether the watermarked content produces perceptible changes are not. Always a good watermarking system should possess imperceptible changes (According to Human Visual System (HVS) and Human Audio System (HAS)) in the watermarked data.

Non detectable:

We can make the watermarking as non-detectable one, if it is consistent with original data. There is difference between non perceptible and non-detectable. Non perceptible is based on the human perceptions and non-detectable is based on data source and its components.

Complexity:

Complexity is based on the expenditure spend on watermark encoding and decoding. For better watermarking system it is always recommended to be more complex.

Payload:

Payload refers to the amount of information that can be embedded in the video. For a better system payload should be high, but it should not affect imperceptible and non-delectability of watermarked data.

2.2. Classification of Watermarking Techniques

2.2.1. Visible/Invisible Systems

Based on HVS (Human Visual System) we can classify the video watermarking as visible and invisible. In visible technique, the watermark will be visible to the users. In the invisible technique the watermark cannot be viewed by the user.

2.2.2. Blind/Non Blind Detection System

Non blind detection system uses original video to extract the watermark. Original data will be given as input to the decoding system and it will be compared with the watermarked vide. However video holds more amount of data than images. Keeping the original video also is a huge task. So we move to blind detection system. In blind detection system, there is no need of original video to extract watermark data. Digital video watermarking can be classified into three ways: According to domain, key and cover.

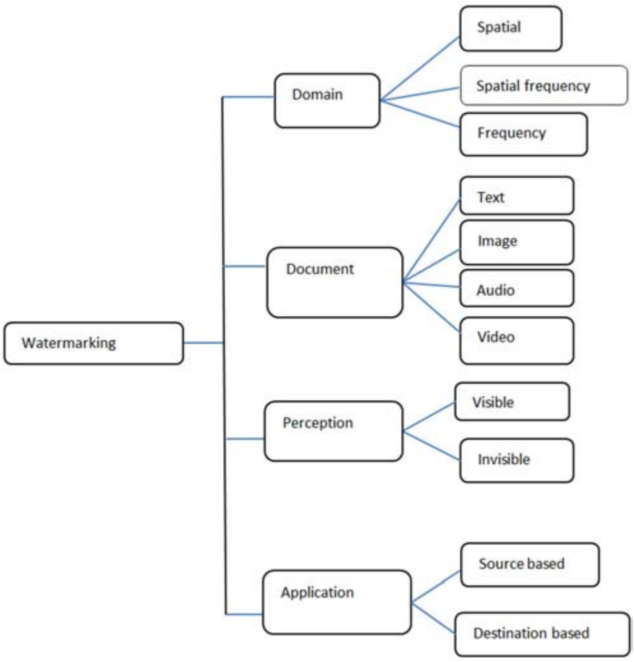

Figure 1. *Methodology in Watermarking.*

2.2.3. Based on Key

In the watermarking embedding process, keys are used to embed and extract the data. If the key used for both embedding and extracting is same then it is called symmetric watermarking. If the keys are different then it is called asymmetric key watermarking.

2.2.4. Based on Cover Data

According to the embedding process we classify this into three types: Original uncompressed video watermarking, embedding watermarking in the video encoder technique, watermarking on compressed video.

2.2.5. Uncompressed Video

In this type watermark is directly embedded in original video sequence. After that the watermarked video will be encoded. The main advantage of this method is, embedding can be done easily. But disadvantage is this will increase the bit rate of the original stream and after compression watermark may be lost.

Embedding in video encoder:

In this type of embedding watermark has been embedded in the encoder and the decoder. There are different video compression standards are available like MPEG-1, MPEG-2, MPEG-4 and H. 264. The advantage is it does not increase the bit stream of the video sequence. The disadvantage is it is relatively simple method in transform domain.

Compressed video:

In this method watermark will be embedded in the compressed video. The advantage is computational complexity is lower compared to other types. The watermark size will be low.

2.2.6. Based on Domain

Video watermarking is classified into two domains:

1. Pixel or Spatial domain
2. Frequency and Transformed domain

Some hybrid approaches are also used in the video watermarking.

i. Spatial Domain Watermarking

In spatial domain watermarking, the process deals with adding or replacing the pixels of the original content. Some of the techniques which uses spatial domain watermarking are Least Significant Bit (LSB) and correlation based technique.

Least Significant Bit:

LSB is one of the simplest technique in which the watermark is embedded in the least bits of the original video. Robustness of this type of watermarking is low. It can be easily affected by various attacks and possess low imperceptibility.

Correlation based technique:

In correlation based technique, watermark W (x, y) is added with the original signal O (x, y), by the following equation.

$$O_w\ (x,\ y)=O\ (x,\ y)+K*W\ (x,\ y) \qquad (1)$$

K is the gain factor

If the values of K get increased, the qualities of the content get increased.

Spread spectrum technique (SS):

In spread spectrum based technique each bit of watermark wj, wj£{-1, 1} is spread over a large number of chips (cr) and modulated by a binary pseudo-noise sequence pi, pi £{-1, 1}. The video and watermarks are represented as vectors and scaled addition is carried out for watermark insertion. To retrieve the watermark the watermarked data will passed through the high pass filter and then correlation method is applied. The robustness of the watermark is increased by increasing cr, σ2p (variance of pseudo random sequence), or μα (mean of adjustable amplitude factor). But increases in cr reduces the data rate of the scheme, whereas increase in σ2p, μα results in perceptibility of the watermark.

Characteristics of spatial domain watermarking:

Embedding processes are simple. Since time complexity is low it can be applied for real time applications. Receiver side watermark is detected by correlating the original signal with watermarked signal. Watermark is embedded in the redundant part of the carrier.

ii. Frequency Domain Watermarking

In the frequency domain the watermark embedding happens after the host signal is transformed into another domain.

iii. Transformed Domain Watermarking

Importance of embedding watermark into perceptually significant components to increase robustness against signal processing and lossy compression techniques. The watermark length is populated from a standard normal distribution apart from a PN sequence in order to enhance robustness. This is a non-blind method. Detection is performed by transforming the original and test frame in the DCT domain and correlating the difference vector with expected watermark pattern.

Discrete Fourier Transform:

In this method the brightness of watermarked frame extracted first, computing its full-frame DFT by taking magnitude of the coefficient. Watermark is composed of two alphanumeric strings DFT coefficient and IDFT. Here the first frame of each GOP is watermarked, which is composed of twelve frames, leaving the other ones uncorrupted.

It is one of the good robustness methods for linear/non-linear filtering, sharpening, JPEG compression etc. The DFT watermark procedures do not involve any transformations, simply addition, replacement used for combination of watermark.

The DFT technique with template matching can resist a number of attacks, including pixel removing, rotation and shearing. The template is to enable resynchronization of the watermark payload spreading sequence, which is also embedded into DFT magnitude representation.

Discrete Cosine Transform:

In this technique the image is allowed to broken up into high, low and middle frequency bands. Here the watermark is allowed to embed in middle frequency band in order to avoid the perceptibility of the video. Here the frequency components (low, middle, high) are arranged in sequential order and it is easy for the selection of components. If most of the high frequency coefficients are zero a smooth block is represented and if low frequency coefficients have large absolute values an edge block is represented.

DCT watermarking technique is one of the most robust watermarking techniques to lossy compression. DCT is faster and it can be implemented in O (n log n) operations.

Discrete Wavelet Transform:

In this technique a frame is separate into lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH). This separation process repeats to compute multiple "scale" wavelet decomposition

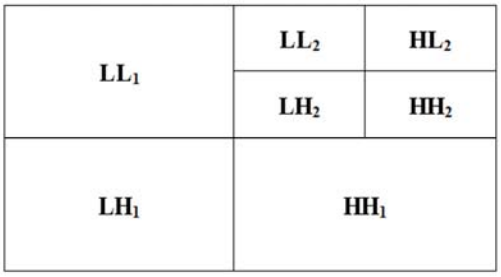

Figure 2. *Frame's 2-level DWT Sub-bands.*

Wavelet transform is one of the best techniques when compared to FFT and DCT in the aspects of HVS accurate model. This allows us to use higher energy watermarks in regions where the HVS is known to be less sensitive in high resolution LH, HL, HH bands. Embedding watermarks in these regions allows us to increase the robustness with no additional impact on image quality.

The 2-D frames are processed by 2-D filters in each dimension and the filter which divides the frame 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 represents the fine-scale DWT coefficients. The LL sun-band is further processed to obtain the next coarser scale of wavelet coefficients until some fine scale N is reached. DWT based watermark scheme is most robust to noise addition.

Advantages of frequency domain watermarking:

Embedding watermark in the original digital content is not a limiting factor to some pixels but it is distributed to all the pixels in that domain. For video compression standards this method is compatible. In the encoding process some of the human perceptual system can be integrated.

3. Related Work

Various researchers in the recent past have developed different watermarking schemes to provide video authentication [4]-[14]. Each scheme has its own advantages and disadvantages with reference to robustness of the watermarking schemes and perceptibility of the watermark.

Ejima et al [4] proposed Wavelet based watermarking for digital images and Video. In this paper wavelet packets were applied to the video and identical watermark was embedded in to the LL sub band of all frames in the video. In this method, the watermark was not robust to some of the image processing and video processing attacks like frame swapping, frame averaging, median filtering etc., because the algorithm used for image processing was applied as such to the video data. The processing time was also high because the identical watermark was embedded to all the frames.

Da-Wen et al [5] proposed a blind video watermarking algorithm based on 3D wavelet transform. They divided the original video frames into 3D-blocks. According to HVS properties, the motive block with complex texture was selected to embed the watermark. The proposed watermarking algorithm was robust against attacks like additive Gaussian noise, frame dropping, frame averaging and lossy compression but was not resistant to some of the image processing and filtering attacks.

Sadik et al [6] proposed robust video watermarking based on 3D-DWT Domain. In this paper three level DWT was applied and watermark was embedded in to the selected coefficients of LL sub band. This algorithm was robust against some of the image processing attacks, but was not robust for addition of noise and all video processing attacks.

Chetan et al [7] proposed a DWT based blind digital video watermarking scheme for video authentication. In this paper DWT was applied to the selected video and different scrambled watermark was embedded in to different scenes of the video. In this algorithm embedding process was performed in the middle frequency band HL and LH. This watermarking algorithm was robust against the attacks like frame dropping, averaging and compression but was not resistant against filtering, frame swapping attacks and some of the image processing attacks.

Cruz-Ramos [8] proposed a blind video watermarking scheme robust to frame attacks. In this algorithm the video was embedded with 2D binary visually recognizable patterns such as company trademarks and owner’s logotype, in the DWT domain of the video frames. This method was robust against MPEG-2 compression, noise contamination, collusion attacks, frame dropping and swapping but was not resistant for filtering, geometric distortions and some of the video processing attacks.

Radu O. Preda [9] proposed robust digital watermarking scheme based on multi-resolution wavelet decomposition. A binary watermark image was embedded in the wavelet coefficients of the LH, HL and HH sub-bands of the second wavelet decomposition level by quantization. Every bit of the watermark was spread over a number of wavelet coefficients with the use of a key and error correction code. This algorithm was robust against the attacks such as scaling, translation and rotation but was not robust against some of the video processing attacks. It had some detection problems after median filtering.

Ray-Shine Run et al [10] proposed blind watermarking scheme based on wavelet tree quantization. In this scheme, a large significant difference was present while embedding a watermark bit 1 and a watermark bit 0 based on adaptive threshold value. This method was more robust against common attacks such as median filtering, average filtering and Gaussian noise but does not resist video processing attacks.

Dragos Nicolae et al [11] proposed robust wavelet-based video watermarking scheme for copyright protection using the human visual system. In this paper binary watermark image was embedded in the detail wavelet coefficients of the middle wavelet sub bands. The method was a combination of spread spectrum and quantization-based watermarking. This algorithm was robust against only spatial, temporal and compression attacks but not for video processing attacks.

Osama S. Faragallah [15] proposed video watermarking based on singular value decomposition in the discrete wavelet transform domain. In this paper video frames were transformed with the DWT using two resolution levels. The high frequency band HH and the middle frequency bands LH and HL were SVD transformed and the watermark was hidden in them and then an error correction code was found and the watermark was embedded with spatial and temporal redundancy. This method was robust against common image processing attacks but does not resist the video processing attacks like frame swapping, frame dropping and filtering.

Alam et al [12] proposed a technique on video watermarking using 2D DWT and 2-level SVD. In this algorithm the video was decomposed in to number of frames and a binary watermark image was embedded in the wavelet coefficients of the LL, HL sub-bands. Then dual SVD was applied on that sub bands. This algorithm was robust against the attacks such as Gaussian filtering, median filtering, frame rotation, contrast adjustment and sharpness attack. Some of the image processing and video processing attacks like addition of noise, frame dropping, frame swapping and frame averaging were not supported by this algorithm.

Divjot Kaur Thind [13] proposed video watermarking based on DWT and SVD. This paper combines discrete wavelet transform (DWT) and Singular value decomposition (SVD) in which watermarking was done in the high frequency sub band. This algorithm was robust against the image processing attacks but not for video processing attacks. In this algorithm watermark was embedded in to all the frames in the video hence the process of embedding and extraction takes more time.

Lama Raja b et al [14] proposed a blind DWT-SCHUR based digital video watermarking technique. In this paper two level DWT was applied to the video scene followed by SCHUR decomposition, in which the binary watermark bits were embedded in the resultant block upper triangular matrix of HL sub band. This algorithm was robust against some of the image and a video processing attack like Gaussian noise, salt and pepper, frame averaging and swapping but was not robust against the frame dropping attack.

Table 1. *Different video watermarking algorithms.*

S. No.	Algorithm Name	Author
1.	Least significant bit (LSB)	Chandramouli R, Memon N
2.	Threshold-based correlation	Langelaar G, Setyawan I, Lagendijk R
3.	Direct sequence watermark using mframe	Mobasseri B
4.	Discrete Fourier transform (DFT) with feature point detection and image normalization	Lu W, Lu H, Chung F
5.	Discrete wavelet transform (DWT)	Guzman V, Ramos C, Miyatake M, Meana H
6.	Discrete cosine transform (DCT)	Wang J, Liu JCL, Masilela M
7.	Fast walsh transform (FWT) based spread spectrum	xMaity SP, Kundu MK, Maity S
8.	Radom transform based watermarking scheme	Ramalingam A, Krishnan S
9.	Hybrid quasi-3D DWT/DCT and SVD video watermarking algorithm	Niu K, Yang X, Xiang L
10.	DFT of 3D chunks of a video scene	Deguillaume F, Csurka G, ÒRuanaidh J, Pun T
11.	A novel adaptive watermarking scheme based on error correction code and human visual system (HVS) in 3D-DWT	Anqiang L, Jing L
12.	DWT-based watermarking scheme using scene change detection.	Chetan KR, Raghavendra K
13.	A non-blind video watermarking in 3D ridgelet domain	Khalilian H, Ghaemmaghami S, Omidyeganeh M
14.	Wavelet based watermarking scheme which embeds an identical watermark in all frames	Ejima M, Miyazaki A
15.	Blind watermarking method which embeds the CDMA encoded watermark into the selected sub-block of wavelet coefficients	Da-Wen X

Table 2. *Video watermarking applications and Purposes.*

Applications	Purpose of the embedded watermark
Steganography	Convey secret information
Labelling	Bind semantic meaning to the host content
Data compression	Transmit enhancement features (color, audio)
Error recovery	Convey additional information to enable error control
Proof of ownership	Identify the video copyright holder
Access control	Prevent unauthorized playback and copying
Broadcast monitoring	Identify the broadcasted video items
Fingerprinting	Identify the source of leakage in a content distribution network
Authentication	Ensure that the original video has not been tampered

4. Conclusion

In this paper various kinds of watermarking techniques are revisited and the specific algorithms in various domains were discussed and the important applications of watermarking are listed. The weakness of the existing algorithms, however, includes:

The video watermark is not robust to attacks such as frame dropping, averaging and statistical analysis, swapping and addition of noise. From the survey it is concluded that the frequency based algorithm is resistant to all kinds of attacks.

References

[1] Min-Jeong Lee a, Dong-Hyuck Im a, Hae-Yeoun Lee b, Kyung-Su Kim a, 1, Heung-Kyu Lee, Real-time video watermarking system on the compressed domain for high-definition video contents: Practical issues, Digital Signal Processing 22 (2012) 190–198.

[2] He Yingliang, Yang Gaobo∗, Zhu Ningbo, A real-time dual watermarking algorithm of H. 264/AVC video stream for Video-on-Demand service, International Journal of Electronics and Communications (AEÜ) 66 (2012) 305–312.

[3] Masataka EJIMA & Akiyo MIYAZAKIA” Wavelet based watermarking for digital images and Video” IEICE Trans. Fundamentals, VOL. E83-A, NO. 3, March 2000.

[4] Da-Wen X. A blind video watermarking algorithm based on 3D wavelet transform. International conference on computational intelligence and security. 2007. p. 945–9.

[5] Sadik. A. M, Robust Video Watermarking Based On 3D-DWT Domain, Al-Taweel School of Computer Sciences University Sains Malaysia 11800, Penang, 2009.

[6] Chetan K. R & Raghavendra K. DWT Based Blind Digital Video Watermarking Scheme for Video Authentication 2010, International Journal of Computer Applications (0975–8887)Volume 4–No. 10, August 2010.

[7] C. Cruz-Ramos, R. Reyes-Reyes, M. Nakano-Miyatake & H. Perez- Meana ”A Blind Video Watermarking Scheme Robust To Frame Attacks Combined With MPEG2 Compression” Journal of Applied Research and Technology, December 2010.

[8] Radu O. Preda & Dragos N. Vizireanu, A robust digital watermarking scheme for video copyright protection in the wavelet domain, Journal of Electronic Imaging 20 (1), 013022 (Jan–Mar 2011).

[9] Ray-Shine Run, Shi-Jinn Horng, Wei-Hung Lin, Tzong-Wann Kao, Pingzhi Fan & Muhammad Khurram Khan, An efficient wavelet-tree-based watermarking method, Int. Jour on Expert Systems with Applications 38 (2011) 14357–14366.

[10] Osama S. Faragallah, Efficient Video Watermarking based on singular value decomposition in the discrete wavelet transform domain, International Journal of Electronics and Communications (Elsevier) 2012; AEUE-50941.

[11] Alam Naved1 & Yadav Rajesh, Dual Band Watermarking using 2-D DWT and 2-Level SVD for Robust Watermarking In Video, International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, September 2013.

[12] Divjot Kaur Thind & Sonika Jindal, A Semi Blind DWT-SVD Video Watermarking Procedia Computer Science 46 (2015) 1661–1667, Elsevier.

[13] Lama Rajab, Tahani Al-Khatib & Ali Al-Haj, A Blind DWT-SCHUR Based Digital Video Watermarking Technique, Journal of Software Engineering and Applications, 8, 224-233., 2015.

[14] Ramalingam A, Krishnan S. Robust image watermarking using a chirp detection-based technique. IEE Vis Image Signal Process 2005; 152 (6): 771–8.

[15] Niu K, Yang X, Xiang L. Hybrid quasi-3D DWT/DCT and SVD video watermarking. In: Proceedings of ICSESS. 2010. p. 588–91.

[16] Deguillaume F, Csurka G, ÒRuanaidh J, Pun T. Robust 3D-DFT video watermarking. In: Proceedings of security watermarking multi content. 1999. p. 113–24.

[17] Anqiang L, Jing L. A novel scheme for robust video watermark in the 3D-DWT domain, First international symposium on data, privacy and e-commerce. 2007.

[18] Khalilian H, Ghaemmaghami S, Omidyeganeh M. Digital video watermarking in 3D ridgelet domain, 11th international conference on advanced communication technology, ICACT 2009, vol. 3. 2009. p. 1643–6.

[19] Ejima M, Miyazaki A. A wavelet-based watermarking for digital images and video. In: Proceedings of ICIP. 2000. p. 678–81.

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

[21] F. Petitcolas (Eds) “Information hiding techniques for steganography and digital watermarking Stefan Katzenbeisser,” Artech House Books, Dec. 1999.

[22] CHAN Pik-Wah, Techniques for Secure Multimedia Creation and Delivery, Thesis, 2005.