

A Survey and Comparative Analysis on Video Watermarking

Ramanjeet Kaur, Arwinder Kaur, Shalini Singh

Department of Computer Science and Engineering, CGC-CEC, Landran, Punjab, India

ABSTRACT

The escalating interest with digital watermarking is attributable to the increase in the need of copyright protection. There are various functions of video watermarking like finger printing, copy control, video authentication, copyright protection, broadcast monitoring, forensic tracking etc. Capacity, security and robustness are the key facets of information hiding. Video watermarking algorithms normally prefer to be robust. In robust algorithm, it is not potentially to eradicate the watermark with no factual deprivation of the cover content. In this paper, a survey is carried out on the presented video watermarking techniques and then a comparative analysis is done on different watermarking algorithms.

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

I. INTRODUCTION

Watermarking is a way of hiding the information in digital media like photographs, digital video or digital music. The digital content can be replaced over the Internet has raised copyright infringement issues. Over peer-to-peer networks copyrighted material can be exchanged easily and it produces the interest to the content providers who produce these digital contents. Watermarking techniques which are used on images can also be used on videos.

A visible watermark is constrained in many ways as it is susceptible to attack through direct image processing. A watermark may contain additional information to identify the purchaser of a particular copy of the material.

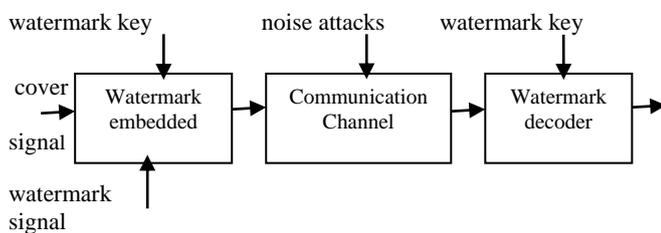


Figure 1. Watermarking basic principle

Embedding the digital watermarks into multimedia data is the scheme to defend intellectual property rights (IPR). The watermark is a digital code inserted in the host data and it includes the information about origin, status, and/or destination of the data.

Watermark insertion or watermark embedding are another names that are given to digital watermarking, which depicts the practice of adding information into multimedia data that is termed as the original media or cover media e.g. text, audio, image, video. There are numerous text, image, audio and video watermarking algorithms exist. These algorithms are used to transform the original media and generate the watermarked media. There may be no or minute distinctness among the original media and the watermarked media.

II. METHODS AND MATERIAL

A. Types of Watermarking

There are two types of watermarking:

1. Visible watermarking: In visible watermarking, the information is demonstrable in the contour or video. The information may be a text or a logo which be aware of the owner of the media.

2. Invisible watermarking: Information is associated with digital data to audio, picture or video, but cannot be documented. It is described as invisible watermarking and hidden information can be detected in invisible watermarking. There is two differentiate ways of embedding invisible information in a digital image:

- Watermarking in Spatial Domain
- Watermarking in Transformed domain

B. Video Watermarking Terminologies (Classifications)

The process of entrenching information in video data is called video watermarking. In digital video watermarking different terminologies are used:

1. Payload: It is the amount of information that can be stored in a watermark. An important perception related to the video watermarking is payload i.e. watermarks granularity. Watermark granularity can be signified as, how much data is prescribed for embedding one unit of watermark information.

2. Perceptible watermarks and imperceptible watermarks: Perceptible watermarks are noticeable to human eye while imperceptible watermarks are unseen. The perceptible watermarks are functional for primary application i.e. for statement ownership or authorship. So, for this reason it should be visible. On the other hand imperceptible watermarks are useful for intricate applications such as document identification in which content being watermarked must appear in unchanged form. Examples of visible (perceptible) watermarks are logos on TV watermark and that of invisible (imperceptible) watermarks are ATT, NEC/MIT, UU etc.

3. Robust watermarks and fragile watermarks: Robust or fragile is nothing but level to which watermarks can resist any modifications of any sort caused due to the diffusion or lossy compression. Perceptible watermarks are more robust in nature than imperceptible one. But meaning of this is not that imperceptible watermarks are delicate one. Robust watermarks are those watermarks which are hard to confiscate from the article in which they are embedded whereas fragile watermarks are those watermarks which can be easily shattered by any attempt to mess about with them.

4. Private watermarks and public watermarks:

Private watermarks require at least inventive data to recover watermark information. Private watermarks are also known as secure watermarks and to interpret or retrieve private watermark, it is needed to have secret key. But, public watermarks require neither original data nor embedded watermarks to recover watermark information and it can be recovered by anyone using specialized algorithm. So, public watermarks are not secure.

C. Applications of Digital Watermarking

Watermarking finds enormous interesting applications in the field of multimedia, ecommerce etc. Some of the applications are:

1. Owner Identification: It presents the ownership of the content.

2. Copy Protection: It evades people from generated illegal copies of copyright content.

3. Authentication of Content: A sign of untrue authentication to spot alterations of the content.

4. Fingerprinting: It traces back illegal duplication. By inserting a unique serial number in duplication content like watermark, is a good way to perceive customers who break their license agreement.

5. Broadcast Monitoring: It is used for advertisements and in entertainment industries to monitor the content.

6. Medical Applications: It provides authentication and confidentiality without affecting the medical image.

7. Data Hiding (Covert Communications):

The transmission of private data is probably one of the earliest applications of watermarking. It consists of implanting a strategic message into an innocuous one in a way that would prevent any unauthorized person to detect it.

8. Forensic Tracking- Forensic tracking locates the source of content, especially illegitimate content. (A

unique customer identification number can be embedded into the watermark this is called fingerprinting).

9. Remote Triggering- Identifies content and causes automatic action during distribution.

D. Classification Of Attacks

Attacks seek at deteriorating the watermarking algorithm. These attacks can be generally classified as non-malicious (unintentional) such as compression of a legally attained watermark image or video file and malicious (intentional) such as an attempt by a multimedia pirate to destroy the embedded information and prevent tracing of illegal copies of watermarked digital video. There are several kinds of malicious attacks which result in a partial or even total destruction of the embed identification key and for which more advanced watermarking scheme should employed;

1. Active Attacks: In this attack, the hacker tries deliberately to confiscate the watermark or simply make it undetectable. This is a big concern in copyright protection, copy control , fingerprinting etc

2. Passive attacks: In the passive attack, the attacker is not annoying to eliminate the watermark but simply trying to determine if a given mark is present or not. Protection against passive attacks is of the most importance in covert communications.

3. Collusion attacks: In collusive attacks, the goal of the hacker is the same as for the active attacks but the method is a little different. In order to remove the watermark, the hacker uses several copies of the same data. This is a problem in fingerprinting applications.

4. Forgery attacks: This is probably the main issue in data authentication. In forgery attacks, the hacker aims at embedding a new valid watermark rather than removing one. It allows him to modify the protected data as he wants and then re-implants a new given key to replace the destructed (fragile) one. It makes the corrupted image seems genuine.

E. Techniques of Digital Watermarking

Many algorithms are used to hide the secret information. These algorithms can be divided into two domains called Spatial domain and Frequency domain.

1. Spatial domain: It modifies the pixels of one or two randomly selected subsets of an image. The major merits

of pixel based techniques are that they are very simple and have very low computational complexities. Therefore, they are widely used in video watermarking. However, they also exhibit some limitations. To de-synchronization attacks, there is need for absolute spatial synchronization which leads to high susceptibility; vulnerability to processing of video and multiple frame collision due to the loss of temporal axis. By using only spatial techniques, optimization of watermark is difficult.

2. Least significant bit modification: The easiest watermarking method in spatial domain is to instantly flip the Least Significant Bit (LSB) of chosen pixels in a frame. A smaller object may be inserted numerous times in this method, specifically high channel capacity of utilizing the entire cover for transmission even if the most of these objects are off-track due to attacks, a single presented watermark would be consider a success.

3. Correlation based techniques: In correlation based technique, the watermark $W(x,y)$ is added to the original content $O(x,y)$ according to the equation.

$$O_w(x,y) = O(x,y) + kW(x,y)$$

k is gain factor
O_w is watermarked content

As we increase the value of k, it will cost the quality of watermarked contents.

4. Frequency domain: By using any transformation methods such as Fourier transform, discrete cosine transform (DCT) or discrete wavelet transform (DWT) the image is first converted to the frequency domain. In the values of transform coefficient the information is added and then applying the inverse transform, which gives the marked coefficients form the embedded image [10]. The merit of transform domain techniques is addressing the restraints of spatial method and shows special features to represent a different view of a signal. The disadvantage of frequency domain is high computational requirement.

5. SVD (Singular Value Decomposition) technique: It is a numerical technique that is used in numerical analysis for diagonalizable matrices. In this technique, a matrix can be divided into a multiplication of three matrices which are linear algebra technique that divides

a given matrix into left singular vectors, set of singular values and right singular vectors (three component matrices) [13]. It consists of matrix which contains real or complex entries of mathematics. This kind of algorithms has proven to be robust in watermarking systems.

6. Discrete Fourier Transformation: DFT controls the frequency of the host signal therefore it is considered in the field of watermarking. In this technique the watermark is embed into the magnitude of its coefficients. Given a two-dimensional signal $f(x, y)$, the DFT is defined by using equation-

$$F(u, v) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) e^{-j2\pi(ux/M+vy/N)}$$

For $u = 0, 1, 2, \dots, M-1, v = 0, 1, 2, \dots, N-1$ and $j = \sqrt{-1}$

The inverse DFT (IDFT) is calculated by using:

$$f(x, y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u, v) e^{j2\pi(ux/M+vy/N)}$$

where, (M, N) are the dimensions of the image.

The DFT is profitable for watermarking purposes because it helps to pick out the sufficient parts of the image for inserting, in order to obtain the highest invisibility and robustness.

7. Discrete Cosine Transform Technique: It is an essential method for video watermarking. The various digital video watermarking algorithms embed the information of watermark into this domain. This method is used mostly because video compression standards are based on DCT. In this domain the host video coefficient are picked and division is done into associations, and then the bits of watermarks are embedded in each association.

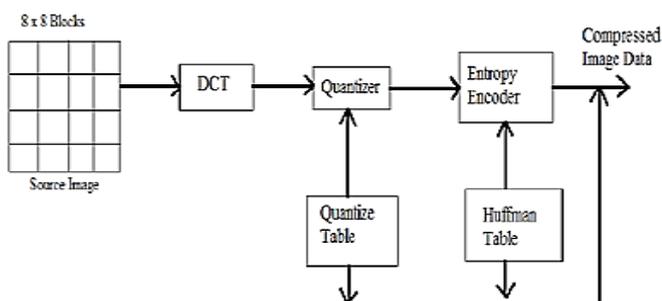


Figure 2. Process of Discrete Cosine Transform (DCT)

DCT is speedy and can be implemented by using $O(n \log n)$ operations. The DCT allows an image is broken into different frequency band and make it easy to embed the information into the middle bands of frequency of an image. The middle frequency bands are selected which avoids the most visual important parts of the image (low frequencies) without exposing themselves to removal through compression and noise attacks (high Frequency). The DCT converts a signal or image from the spatial domain to the frequency domain. It is the most robust to lossy compression.

8. Discrete Wavelet Transform: In signal processing applications the most popular technique is DWT. 2D Discrete Wavelet Transform (DWT) decomposes frames of video into sub images, 3 details and 1 approximation. The approximation sub images is lower resolution approximation image (LL) and the details sub images are horizontal (HL), vertical (LH) and diagonal (HH) detail components. The major advantage of wavelet transform is its compatibility with model aspect as compared to FFT or DCT [14]. By changing some positions of DWT coefficient the watermark is embedded into video frames.

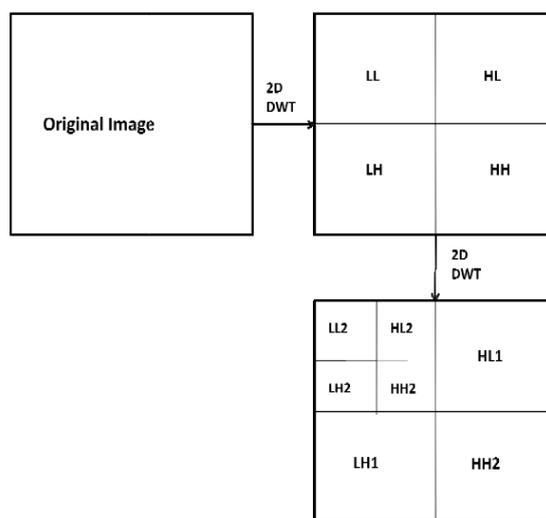


Figure 3. A two scale DWT

DWT is more computationally efficient as compared to another transforms methods. The speed is faster than DCT and DFT as we calculate the sum or difference of the pixel. By using DWT, one can achieve both spatial and frequency localization, perceptual invisibility and robustness to compression, robustness to noise, image processing techniques, and median filter, resistance to geometric transform and resilience to counterfeit attempts. The watermark is inserted before compression

that's why this scheme is robust against format conversions. If the video file is converted to a different compression standard, then authentication information will be lost.

III. RESULTS AND DISCUSSION

A. Comparison of Video Watermarking Methodology

AUTHOR NAME	Title	METHOD	PERFORMANCE
Szczypinski et. Al (2001)	Discrete wavelet transforms – derived features for digital image texture analysis.	DWT with image resolution.	Features used for digital image textual analysis.
Delaigle (2002)	Human Visual System features enabling watermarking.	HVS on sensitivity and masking capabilities.	Synthetic way in HVS to rely the algorithm.
Chang et. Al (2005)	A Survey of Digital Image Watermarking Techniques.	Watermarking techniques based on DCT.	Represent data in frequency space rather than amplitude space.
Mahmoud EL Gayyer (2006)	Watermarking Techniques Spatial Domain Digital Rights Seminar.	Spatial domain and Color Separation.	Inspect digital photos
Harrison et. al (2008)	A Study of Digital image watermarking.	Image processing with DWT.	Decompose image into different spatial domain
Ahmad et. al (2010)	A new DCT-based watermarking method for copyright protection of digital	Audio Watermarking on DCT.	Copyright performance with SNR

	audio		
Manaf et. al (2011)	Study of the effect of DCT and DWT domains on the imperceptibility and robustness of Genetic Watermarking.	DWT and DCT on Genetic watermarking.	More robustness, high imperceptibility than DCT in watermarking on genetic algorithm
Behal et. al (2012)	A study of digital image watermarking	DWT/DCT/HVS Presents the gap in Spatial domain and Frequency domain methods	Embed the watermark in coefficient spectral
Khanna et. al (2013)	A study on spatial and transform domain watermarking techniques	LSB/DCT/DWT To find the best technique out of them	Implement new techniques for achieving maximum robustness

Table 1: Comparison of watermarking methods

B. Performance Parameters

- 1. Imperceptibility:** The watermark should not evidently deform or debase the host data in order to conserve the quality of the marked document.
- 2. Robustness:** To measure robustness the watermark must be reliably detectable against signal processing schemes including data compression.
- 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. Tamper-resistance:** The tamper-resistance property is focused on the intentional attacks in contrast to robustness.
- 5. Normalized Correlation:** The key component of the images detection is the normalized correlation.
- 6. PSNR:** Peak signal to noise ratio, should be as high as possible.

IV. CONCLUSION

It has been concluded that the watermark strength is dependent on both the host image content and the visible watermark features. The visible watermark preserves good watermark visibility under various signal processing operations. In this paper that robustness, geometric attack, imperceptibility, PSNR (Peak Signal to Noise ratio) & NC (Normalized Correlation) are the most important requirements for a watermarking system. This paper presents the survey of video watermarking techniques applying spatial domain and transform domain. Also, advantages and disadvantages of different video watermarking techniques are discussed in this paper. Finally, this paper concludes that there is a need to develop the new technique that can overcome the limitations of video watermarking. So, Future work will combine pseudo random chaotic map and human visual perception to develop a new visible watermarking which offers authorized removal of the visible watermark from the watermarked image by using a private key.

V. REFERENCES

- [1] R. van Schyndel, A. Tirkel, and C. Osborne, "A digital watermark," Proceedings of the IEEE International Conference on Image Processing, vol. 2, pp. 86-90, Austin, Texas, November 1994.
- [2] R. Wolfgang and E. Delp, "A watermark for digital images," Proceedings of the IEEE International Conference on Image Processing, vol. 3, pp. 219-222, 1996.
- [3] D. Kundur and D. Hatzinakos, "Towards a telltale watermarking technique for tamper-proofing," Proceedings of the IEEE International Conference on Image Processing, vol. 2, pp. 409-413, Chicago, Illinois, October 1998.
- [4] J. Fridrich, "Image watermarking for tamper detection," Proceedings of the IEEE International Conference on Image Processing, vol. 2, pp. 404-408, Chicago, Illinois, October 1998.
- [5] M. Swanson, M. Kobayashi, A. Tewfik, "Multimedia data-embedding and watermarking technologies," Proceedings of the IEEE, vol. 86, no. 6, pp. 1064-1087, June 1998.
- [6] N. Memon, S. Shende, and P. Wong, "On the security of the YuengMintzer authentication Watermark," Final Program and Proceedings of the IS&T PICS 99, pp. 301-306, Savanna, Georgia, April 1999.
- [7] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual Watermarks for Digital Images and Video", Proceedings of the IEEE, vol. 87, no. 7, pp. 1108-1126, July 1999.
- [8] R. Wolfgang and E. Delp, "Fragile watermarking using the VW2D watermark," Proceedings of the IS&T/SPIE Conference on Security and Watermarking of Multimedia Contents, pp. 204-213, San Jose, California, January 1999.
- [9] S. Pankanti and M. Yeung, "Verification watermarks on fingerprint recognition and retrieval," Proceedings of the IS&T/SPIE Conference on Security and Watermarking of Multimedia Contents, pp. 66-78, San Jose, California, January 1999.
- [10] Frank hartung, "Multimedia Watermarking Techniques", Proceedings of the IEEE, Vol. 87, No. 7, July 1999.
- [11] G. Langelaar, I. Setyawan, R.L. Lagendijk, "Watermarking Digital Image and Video Data", in IEEE Signal Processing Magazine, Vol 17, pp 20-43, September 2000.
- [12] J.R. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis And a New Structure", in IEEE Trans. Image Processing, vol. 9, pp 55-68, Jan. 2000.
- [13] Sin-Joo Lee, "A survey of watermarking techniques applied to multimedia", IEEE, 2001.
- [14] Vidyasagar M. Potdar, "A Survey of Digital Image Watermarking Techniques", 3rd IEEE International Conference on Industrial Informatics (INDIN), 2005.
- [15] Sourav Bhattacharya, "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC", IEEE, 2006.
- [16] Sadik Ali M. Al-Taweel, "Digital Video Watermarking in the Discrete Cosine Transform Domain", Journal of Computer Science, 536-543, 2009.
- [17] Mrs Neeta Deshpande, "Review of Robust Video Watermarking Algorithms", International Journal of Computer Science and Information Security, Vol. 7, No. 3, March 2010.
- [18] Mrs Neeta Deshpande, "Review of Robust Video Watermarking Algorithms", International Journal

- of Computer Science and Information Security, Vol. 7, No. 3, March 2010.
- [19] Chetan K.R,“ DWT Based Blind Digital Video Watermarking Scheme for Video Authentication”, International Journal of Computer Applications (0975 – 8887)Volume 4– No.10, August 2010.
- [20] Rini T Paul,“ Review of Robust Video Watermarking Techniques”, IJCA Special Issue on “Computational Science - New Dimensions & Perspectives” NCCSE, 2011.
- [21] Swati Patel,“ A Survey on Digital Video Watermarking”, Int. J. Comp. Tech. Appl., Vol 2 (6), 3015-3018, Nov-Dec 2011.
- [22] Bibi Isac,“ A Study on Digital Image and Video Watermarking Schemes using Neural Networks”, International Journal of Computer Applications Volume 12– No.9, January 2011.
- [23] Gopal Prasad,“ Digital Video Watermarking Techniques and Comparative Analysis : A Review”, International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 11, November – 2013.
- [24] Mr Mohan A Chimanna,“ Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery”,International Journal of Engineering Research and Applications (IJERA), Vol. 3, Issue 2, pp.839-844, March -April 2013.
- [25] Ankita A. Hood,“ Robust Video Watermarking Techniques and Attacks on Watermark – A Review”, International Journal of Computer Trends and Technology- volume4Issue1- 2013.
- [26] Gopika V Manem,“ Review Paper on Video Watermarking Techniques”, International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 .
- [27] Hamid Shojanazeri, “Video Watermarking Techniques for Copyright protection and Content Authentication”, International Journal of Computer Information Systems and Industrial Management Applications. ISSN 2150-7988 Volume 5, pp. 652–660,2013.
- [28] Hai Tao, “Robust Image Watermarking Theories and Techniques: A Review”, Journal of Applied Research and Technology, Vol.12,122-138,February 2014.
- [29] Deepti Shukla,“ Survey on Digital Watermarking Techniques”, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.8, No.9 (2015), pp.121-126,2015.
- [30] Rajni Bala,“ The International Journal Of Engineering And Science (IJES)”, Volume 4 , Issue 2, PP.41-45, 2015.
- [31] Maninder kaur,“ Digital Video Watermarking Techniques: A Review Study”, International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 4, Issue 5, May 2015.