ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

A Survey of Digital Video Watermarking Techniques for Copyright Protection and Authentication

S.Elango[1], Dr.G.Thirugnanam[2], R.Shankari[3]

Associate Professor, Dept. of ECE, Arunai Engineering College, Tiruvannamalai, Tamilnadu, India [1]

Assistant Professor, Dept. of EIE, Annamalai University, Chidambaram, Tamilnadu, India [2]

Assistant Professor, Dept. of ECE, Arunai Engineering College, Tiruvannamalai, Tamilnadu, India [3]

ABSTRACT: Digital watermarking techniques have emerging techniques for copyright protection and authentication. The preferment of Cyberspace and various depot technologies made data rebooting as an increasing problem with the procreation of sharing the digital contents. Digital watermarking field has emerging articles covering creative approach, coherent reviews and attacks. Hence, analysis on patent protection and content verification mechanisms, which include watermarking as an effective solution to protect online contents. Digital watermarks encounter various attacks that include computation attacks or updated watermarking attacks. The recovery from these attacks depends upon stable detection techniques; watermarking agent provides effective solution for these attacks. It is then possible to retrieve the messages embedded at any time, even if the information undergoes certain attacks. Automation of digital watermarking is classified depending upon their domain to spatial, transform and wavelet domain watermarks. Interactive media use watermarking techniques for various applications such as copyright protection, copy control and tamper recurrence. Major interrogation involved in watermarking approach is its design considerations, choice of suitable watermarking methodology and robustness. The scope of this paper is on the emerging applications and challenges to highlight functional threats of watermarking.

KEYWORDS*:* Digital video watermarking, Image watermark, Discrete wavelet transform, Principal component Analysis.

I.INTRODUCTION

The digital revolution has changed the paradigm of multimedia distribution. High speed computer networks and the World Wide Web have revolutionized the way in which digital data is distributed. High quality copies of digital data are produced and distributed through the internet by exploiting recent network and software technologies. Video piracy has become an increasing problem particularly with the proliferation of media sharing through the advancement of Internet services and various storage technologies. Security techniques that are based on cryptography only provide assurances for data confidentiality, authenticity, and integrity during data transmission through a public channel such as transmission through an open network. However, such security techniques do not provide protection against unauthorized copying or transmitting of illegal materials. Digital watermarking is the act of hiding a message related to digital signals in different forms like an image, song, video within the signal itself. Potential applications of digital watermarking include transaction tracking, copy control, authentication, legacy system enhancement and database linking.

Using digital watermarking, copyright information can be implanted into the multimedia data by using some algorithms. Watermark information is mainly for protecting the copyright, covert communication and data file authenticity. Existing video watermarking techniques are divided into different categories as shown in Fig1. They can be divided into 3 main groups based on the domain that the watermark is embedded [2, 4].

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

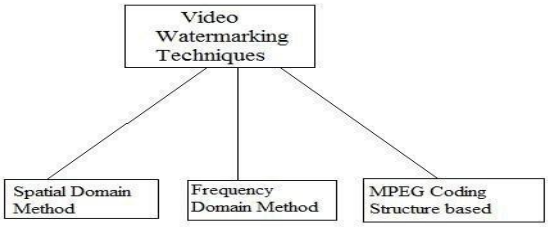

Fig1. Classification of digital video watermark techniques

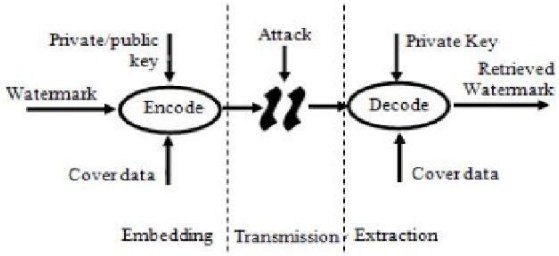

Fig2. Digital Watermarking System

The payload is the digital information being utilized in the watermarking system and it should have the capability to withstand carrier manipulations. Watermarking system is mainly of two phases embedding and extraction of watermark data. Private Key is used to embed the watermark in the original database during the embedding phase. Extraction of watermark is performed by taking suspicious database as input and original content is extracted using the same private key.

This paper, deals with the aspect of copyright protection and authentication of contents. As the challenges in video are different from image watermarking, mainly due to the nature of video data itself that consists of large amount of frames with a high level of redundancy. Attacks may not cause fidelity loss to the signals and may compromise the watermarks. Hence, fidelity, robustness and imperceptibility are amongst the critical indicators for an effective technique [2]. Other requirement of video watermarking is elaborated in Section II. Critical review of the available watermarking algorithms is presented in section III. Comparison between three different techniques used to embed watermark in three different domains using the same data-set are discussed in section IV. Section V concludes the paper with recommendations for further work.

II.CHARACTERISTICS OF DIGITAL WATERMARKING

Watermarking is a technique of embedding hidden data in multimedia system information observably, like image, video, audio and text information for the purpose of identification and copyright. The fundamental characteristics for effective watermark are as follows:

Robustness: The watermark should endure all geometric distortions and attacks, even after processing the signal. Optimal watermarking bears watermark deportation attacks and distortions which are categorized under malignant attacks. Watermarking level depends upon specific applications. Improvement in security techniques will also embellish the robustness of the algorithm.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

Imperceptibility and Fidelity: Watermarked image should resemble the original input image. The observer must not identify the embedded watermark. Active watermarking should endure high fidelity level. Distortion level exhibited during embedding phase should not exceed the maximal range.

Speed: Emerging trends in high accelerating hardware made speed as least requirement in watermarking. In cost effective devices main consideration is about less weight and simple watermarking algorithms.

Capacity: The amount of embedded information must be large enough to uniquely identify the owner of the video. Capacity refers to a maximum number of bits are allowed to embed in a cover media. In video watermarking capacity is not a high priority requirement due to the nature of cover object which is big size. The size of the watermark depends on the application which determines the type of watermark data and embedding policy.

III.TECHNIQUES OF WATERMARKING

Spatial Domain Video Watermarking: In digital video watermarking, the elementary and accessible method is by replacing the video frame pixel values by watermark pixels without employing any transformation. This can be done by the spatial domain method, but they are unreliable for various attacks like geometric misrepresentation. Spatial domain watermarking is of three assorted categories: Least Significant Bit Watermarking, Correlation based watermarking and Spread spectrum based watermarking. In LSB mode, each pixel values of video frame get replaced by the watermark pixel bits. Correlation based method involves the computation of correlated values of both original video frame and watermark.

Watermark signal is fixed into the original video frame by the following representation:

V w(x, y) = V(x, y) + k*W(x, y). Here V w(x, y) – watermarked video frame, V(x, y) – original video frame and K-gain factor.

In Spread Spectrum based watermarking, size of the watermark is scaled equal to the original cover video frame and modulated using a pseudo random noise sequence. In this way a single watermark bit can be spread all around the object. After resizing, watermark can be inserted into the cover image using scalar addition. The procedure for extracting the watermark include passing of watermarked video frame through the high pass filter and then threshold based correlation method can be applied. This method has an advantage of high payload capacity and a robust watermark. Thus watermark can be protected even after going through the attacks like cropping, scaling and compression.

Frequency Domain Video watermarking: In frequency domain watermarking, transformation is applied to the original video frame, and then watermark is inserted in that portion of the video frame, which is perceptually more significant according to the Human Visual System. Frequency domain transforms are segregated into following types:

Discrete Fourier Transform (DFT) based watermarking: It is the most popular and known transform used for watermarking. Fourier Transform is used to convert digital signals from spatial domain to frequency domain. So, DFT Transform results in different magnitudes of frequency bands. Generally watermark is embedded in the highest magnitude frequency bands, so that there is minimum loss in image fidelity.

Discrete Cosine Transform (DCT) based watermarking: A digital signal can be converted into different frequency components using discrete cosine transform. DCT can be both one-dimensional as well as two dimensional, and can be applied on images, audio or video signals. The equation for DCT Transform includes only the cosine functions to work like basis functions. DCT operates only on real-valued signals and spectral coefficients. Generally the middle frequency components are selected to insert the watermark. This is followed by the inverse discrete cosine transform procedure to get the final watermarked video frame. DCT based video watermarking is very efficient and the imperceptibility of the watermarked signal is found to be good.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

Discrete Cosine Transform (DCT) based watermarking: A digital signal can be converted into different frequency components using discrete cosine transform. DCT can be both one-dimensional as well as two dimensional, and can be applied to images, audio or video signals. The equation for DCT Transform includes only the cosine functions to work like basis functions. DCT operates only on real-valued signals and spectral coefficients. Generally the middle frequency components are selected to insert the watermark. This is followed by the inverse discrete cosine transform procedure to get the final watermarked video frame. DCT based video watermarking is very efficient and the imperceptibility of the watermarked signal is found to be good.

Discrete Wavelet Transform (DWT) based watermarking: The DWT (Discrete Wavelet Transform) is very much useful are mostly used in watermarking applications. With the help of DWT, a digital signal is decomposed into lower frequency approximation components (LL), horizontal (HL), vertical (LH) and diagonal (HH) detailed components. The DWT transform can be of various levels (2, 3, 4 or even more). Generally up to 3 levels DWT decomposition is used. Spatial localization and multi-resolution makes an effective and robust DWT. Many watermarking techniques have been developed by combining DWT with other mathematical concepts like SVD [3, 4, 7], or with other transforms like PCA in [2, 3, 7].

Random Transform based Watermarking: The Random Transform used for digital watermarking is very much similar to the Fourier Transform. The image is considered as a set of projections in different directions [4]. Random Transform of an image is basically the line integral of the image along a space of straight lines.

Principle Component Analysis (PCA) based watermarking: PCA transform is an orthogonal transform. It provides the energy compaction capability by converting the co-related variables of a signal into possibly unrelated principle components.

Lifting Wavelet Transform based watermarking: It is an integer based transform based on DWT with perfect digital signal reconstruction property. This approach relies on merging and sequential split technique. This is a better transform than DWT in terms of time complexity and robustness of watermarked image.

Original and watermark images undergo primary color separation and then it gets isolated into multiple blocks. To generate larger integer constant, transitional frequency terms are utilized based on DCT. Then watermarked content is transformed into vector notations of 0 and 1. Inverse transformation is applied to N image blocks. The secret key is used to obtain the relevant information and can also compute the large variance and correlated values using the Chinese remainder theorem [4]. To achieve unique watermark, vector based conversion techniques are used. This enhances robustness of watermarking system and also solves the complication of visual distortion.

The SVD is used to be utilized in the spatial domain while the 2DPCA [6] is employed for embedding in the time domain. The framework of the DPCA and SVD transformation are effective with arbitrary signal channels in multichannel video. Proposed singular value decomposition approach yields watermarked video without any perceptible distortion.

A compressive approach of embedding the watermark image into the original video frame, each video frame is disintegrating into sub images by applying Principal Component Analysis and DWT [7]. Each video frame is divided into and it is converted from RGB format to YUV. By modifying wavelet coefficient values watermark is embedded into sub bands of the original video frame. Then the watermark is converted into vector form and frame can be reconstructed by applying the inverse transformation. The compressive approach of video watermarking is efficient against various attacks like Gaussian, salt and pepper noise and geometric distortions.

Digital Video Watermarking using Reversible Data Hiding and Visual Cryptography [8] method involves the development and implementation of the luminous approach for watermarking by sub image classification. Wavelet based transform is applied to select the similar pattern of frames from the entire video frame to identify the uniqueness among frames. Based on the size of the watermark, K bits are extracted and stored within a video frame. So that it can hide huge capacity of information. K bit value is found by calculating the watermark image size to the total no of

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

unique frames. This data hiding approach is mainly based on visual cryptography, wavelet and histogram based watermarking. Wavelet based method analyses the unique frames and this will determine the no of sub watermark pixels over the image. A watermark is subdivided into k sub images and again emerged to obtain the entire watermarked image in cryptography. Histogram hides the image over the entire frame.

IV.APPLICATIONS OF WATERMARKING

Digital watermarking is well entrenched research area with plenty of applications. The major applications of digital video watermarking includes digital copyright protection, video authentication, broadcast Synchronization System, copy control, fingerprinting, tamper resistance, video tagging, ownership identification and enhance video coding

Broadcast Monitoring Watermarking is obviously a suitable technique for information monitoring. This has major application is commercial advertisement broadcasting where the entity who is advertising wants to monitor whether their advertisement was actually broadcasted at the right time and for right duration. The watermark exists within the content and is compatible with the installed base of broadcast equipment. The watermarks can automatically be extracted to verify if a commercial has successfully been aired or whether a certain segment of material was used in a broadcast. The content is usually watermarked by the content owner, while detection can be done by a monitoring site in the broadcast chain or a third party at the receiving end.

Transaction Tracking is often called fingerprinting, where each copy of the work is uniquely identified, similar to the fingerprint that identifies an individual. A unique identifier is embedded into the media at the time of playback, which can later be extracted. In the case of illegal distribution of the content, it should ideally be possible to identify the source from where the distribution occurred, possibly identifying the misappropriating party.

Content Authentication is a method that attempts to ensure the integrity of media by detecting attempted tampering of the original content. The content is usually watermarked with a semi-fragile watermark, which is designed to be affected by signal transformations. Tampering with the content should destroy or alter this semi-fragile watermark, which could then be used to determine that the content is not authentic.

Digital Fingerprinting is a technique used to detect the owner of the digital content. Fingerprints are unique to the owner of the digital data. Hence a single digital content can have different fingerprints because they related to different users.

Tamper Detection When database content is used for very critical applications such as commercial transactions or medical applications, it is important to ensure that the content was originated from a specific source and that it had not been changed, manipulated or falsified. This can be achieved by embedding a watermark in the underlying data of the database. Tamper detection is also useful in court of law where digital images could be used as a forensic tool to prove whether the image is tampered or not.

Copyright protection is a technique used to embed the ownership rights in a multimedia work by its creators. Watermarking can be used to protecting redistribution of copyrighted material over the untrusted network like Internet or peer-to-peer (P2P) networks.

V.WATERMARKING COMPARATIVE RESULTS AND DISCUSSION

We used sample rhino video sequences of length 114 frames as a cover video and two different watermarks with a frame size of 160 X 120 and fingerprint image of size 250 X 250.Figure. 4(a) and 4(b) shows the original and the watermarked video frame respectively.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

Fig3. Original Video Frame

Fig4. Watermarked Video Frame

Table.1. Comparative analysis of Video Watermarking Techniques

Features	**Least significant bit watermarking**	**Discrete Cosine Transform**	**Discrete Fourier Transform**	**Discrete Wavelet Transform**	**Singular Value Decomposition**
Imperceptibility	Less	High	High	Better	Better
Security	Less secure usually depend on the choice of key	Better	High	Better	High
Robustness against geometric distortions	Less robust against geometric distortions	High robust against geometric distortions	High robust against geometric distortions	High robust against geometric distortions	High robust against geometric distortions
Payload	Less limited data can be added	High	Average	High	High
Time Complexity	Less	High	High	Very High	High
Computational Cost	Less	Reliable cost	Reliable cost	Very High	High
Reliability	Better for multiple watermarking	High	High	Very High	High

Comparative analysis of DWT-SVD method: We conclude the value of PSNR ratio between DCT based watermarked and Hybrid method (DWT-SVD) based watermarked below in table no.2

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

Table 2: DCT and Hybrid watermarking method a comparative study

Alpha =0.001			
DCT BASEDWATERMARKVIDEO		HYBRID BASEDWATERMARKVIDEO	
Time	111.8546	Time	55.6587
Original PSNR in db	3.6548	Original PSNR in db	2.8795
DCT PSNR in db	57.6522	DCT PSNR in db	16.5486
Alpha =0.0012			
DCT BASEDWATERMARKVIDEO		HYBRID BASEDWATERMARKVIDEO	
Time	103.84	Time	70.54
Original PSNR in db	3.7584	Original PSNR in db	2.5487
DCT PSNR in db	57.8558	DCT PSNR in db	14.5004
Alpha =0.0013			
DCT BASEDWATERMARKVIDEO		HYBRID BASEDWATERMARKVIDEO	
Time	111.26	Time	56.25
Original PSNR in db	3.1455	Original PSNR in db	2.2525
DCT PSNR in db	573.4588	DCT PSNR in db	14.7854
Alpha =0.0014			
DCT BASEDWATERMARKVIDEO		HYBRID BASEDWATERMARKVIDEO	
Time	101.5689	Time	60.45
Original PSNR in db	3.7545	Original PSNR in db	2.2412
DCT PSNR in db	56.3535	DCT PSNR in db	2.2235
Alpha =0.0015			
DCT BASEDWATERMARKVIDEO		HYBRID BASEDWATERMARKVIDEO	
Time	108.7545	Time	57.8541
Original PSNR in db	3.8545	Original PSNR in db	2.5986
DCT PSNR in db	57.3578	DCT PSNR in db	14.2110
Hybrid Method		Embedded process: 88.28 sec Extracted process: 1.02 sec	
DCT Method		Embedded process: 202.56 sec Extracted process: 203.45 sec	

VI.CONCLUSIONS

In this paper, we focus on emerging techniques, highlighting practical challenges and applications of digital video watermarking. Challenges include design considerations, requirements analysis, choice of watermarking techniques, speed, robustness, and the trade-offs involved. We describe common attributes of watermarking systems and discuss the challenges in developing real world applications.

REFERENCES

[1] Ekta Miglani, Sachin Gupta, "Digital Watermarking Methodologies - A Survey," International Journal of Advanced Research in Computer Science and Software Engineering, Vol.4, Issue 5, May 2014
[2] Gopika V Mane*, G. G. Chiddarwar ,"Review Paper on Video Watermarking Techniques," International Journal of Scientific and Research Publications, Vol. 3, Issue 4, April 2013 1 ISSN 2250-3153
[3] Shraddha S. Katariya., "Digital Watermarking: Review," International Journal of Engineering and Innovative Technology (IJEIT), Vol.1, Issue 2, February 2012
[4] Sanjana Sinha, Prajnat Bardhan, Swarnali Pramanick, Ankul Jagatramka, Dipak K. Kole, Aruna Chakraborty., "Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis, " International Journal of Wisdom Based Computing, Vol. 1 (2), August 2011
[5] Paramjit Kaur et al,, "Review on Different Video Watermarking Techniques," IJCSMC, Vol. 3, Issue. 9, September 2014, pg.190 – 195.
[6] Manoj Kumar and Arnold Hensman, "Robust Digital Video Watermarking using Reversible Data Hiding and Visual Cryptography," ISSC 2013, LYIT Letterkenny, June 20-21
[7] Wiem Trabelsi, Mohamed Heny Selmi, "Multi-signature robust video watermarking," 1st International Conference on Advanced Technologies for Signal and Image Processing - ATSIP'2014 March 17-19, 2014, Sousse, Tunisia
[8] Chunlin Song, Sud Sudirman, Madjid Merabti, "Recent Advances and Classification of Watermarking Techniques in Digital Images" ISBN: 978-1-902560-22-9 © 2009 PGNet