

A Brief Survey on Robust Video Watermarking Techniques

Rajni Bala

Computer Science & Engg., Shoolini University, Solan, India

ABSTRACT

With growth of Internet along with the increasing availability of multimedia has spawned a number of copyright issues. One of the main areas that this growth has fuelled is digital watermarking. Digital watermarking is a process of hiding a message related to a digital signals in different forms such as an image, song, video within the signal itself. In this paper, we present review on video Watermarking for better performance, robustness and discuss the various factors used in watermarking, attributes and application area where watermarking technique needs to be used. Also survey of new work is done in video watermarking field.

Keywords-SVD, DWT, DCT, Watermarking, FFT, LSB

Date of Submission: 24 December 2014



Date of Accepted: 28 February.2015

I. INTRODUCTION

Digital Watermarking is a technique is used to protect multimedia data that transfer over the internet. Digital Watermarking is a means to embed copyright information into a digital multimedia data such as image, audio, video etc. [4]. Digital watermarking is the process by which a discrete data stream called a watermark is hidden within a multimedia signal by imposing imperceptible changes on the signal. In many proposed techniques this procedure entails the use of a secret key which must be used to successfully embed and extract the watermark. Watermarking has gained interest in applications involving the security of multimedia signals. One major driving force for research in this area is the need for effective copyright protection scenarios for digital imagery, sound and video. In such an application a serial number is watermarked into the signal to protect to mark ownership. It is expected that an attacker will attempt to remove the watermark by intentionally modifying the watermarked signal. Thus, we must strive to embed the mark such that it is difficult to remove (without the use of the key) unless the marked signal is significantly distorted. In digital watermarking a host signal is transformed to a watermark domain in which modifications are imposed on the domain coefficients to embed the watermark. The modified coefficients are then inverse transformed to produce the marked signal. Our proposed approach to improved robust watermarking is applicable to the general class of watermarking methods with the following basic properties: The watermark data stream consists of binary elements. The host signal (which refers to the original multimedia signal before watermarking) is not available or exploited for watermark extraction. The entire watermark is constantly embedded right through the signal and each duplication of the watermark is situated in a distinct localized region of the watermark domain. We will discuss this later in greater detail.

1.1 Broad Classification of Watermarking Techniques

Watermarking techniques are broadly classified in seven ways and defined as: A Visible watermark is a technique of watermarking which is used to for the protection of publicly available data. This technique is used in mostly two cases for copyright protection and indicates original ownership. An invisible watermark is another technique of watermarking; it provides the copyright protection to the contents that transmitted over the computer network. Invisible watermarking revolve around such appropriate factors that include recognizing authentic recipients, identifying the true source and non-repudiation. Robust watermarks are used to grip knowledge of ownership. Such watermarks need to remain stable to the original image to do what they advertise. The absoluteness of the watermark is a determine of its robustness. These watermarks must be able to withstand normal changes to the image such as, lossy compression of image, reduction of image size, changing the contrast of the images, etc. Fragile watermarks is complementary to robust watermarks and are as a rule, more change-sensitive than robust watermarks. They lose their resolve when they are subject even to the smallest changes. It has been changed in the original watermarked image as their use lies in being able to pinpoint the exact region. A semi-fragile watermark detects tampered regions so the images are divided small sub-blocks. They are more resilient than delicate ones in terms of their robustness. They also are better than robust watermarks in terms of locating the regions. Spatial watermarks are useful to the “spatial domain” of the image”

are said to be spatial watermarks [5]. Spectral watermarks are applied to the “transform coefficients of the image” [5].

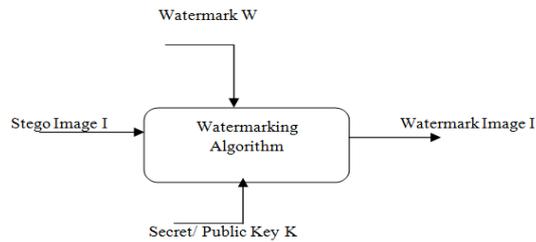


Fig. 1 Watermarking Algorithm

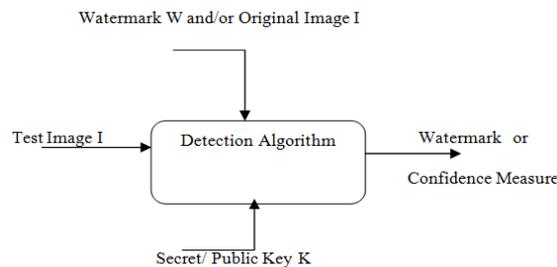


Fig. 2 Detection Algorithm

II. VIDEO WATERMARKING

A digital watermark is a model or digital signal inserted into a digital document such as text, multimedia or graphics and carries information distinctive to the copyright owner. Some watermarking methods have been delivered for video data. In a method is proposed in which video sequence is considered as a three dimensional signal with two dimensional in space and one dimensional in time. Among the delivered techniques in recent years, the ones based on the Discrete Wavelet Transform (DWT) are gaining more popularity due to their outstanding spatial localization, frequency spread and multi-resolution features [3]. Video watermarking involves embedding cryptographic information derived from frames of digital video. Usually, a user viewing the video cannot recognize a difference between the original, marked video and the unmarked video, but a watermark extraction application can read the watermark and it can obtain the embedded information. Watermark is part of the video, rather than part of the file format. In video file format this technology works independently.

III. NEED FOR VIDEOMARKING

Any image watermarking techniques can be extended to watermark video meets some challenges in reality video and motionless region real-time requirement susceptible to pirate attacks. Watermark directly inserted in the raw video data and integrated in the encoding process. After compressing the video data it can be implemented. One of the main purposes of a watermark is to protect the owner's copyright. However, for many existing watermarking schemes, an attacker can easily confuse one by manipulating the watermarked image (or video, audio) and claim that he or she is the legitimate owner. Some watermarking schemes require the original image (or video chip) to perform watermark verification. Video Watermarking can help to identify a misappropriating person, prove ownership, Broadcast Monitoring, Protect copyright of a data etc.

IV. VIDEO WATERMARKING TERMINOLOGIES

The watermarking algorithm optimized in three separate factors: Robustness is the ability of watermark to resist attempt by an attackers to destroy it by rotation, modifying the size, quality and other visual aspects of the video. Security is the ability of watermark to resist attempt by a sophisticated attackers to destroy it or remove it via cryptanalysis without modifying the video itself. Perceptual fidelity is the perceived visual quality of watermark video compared to unmarked video, the original.

4.1 VIDEO WATERMAKING APPROACHES

There are two factors for water marking which are described as spatial domain watermarking. In these watermarking techniques, embedding and detection are performed on spatial pixels values (luminance,

chrominance, color space) or on the overall video frame. Spatial-domain techniques are easy to implement, however they are not robust against common digital signal processing operations such as video compression. Transform-domain watermarking technique mostly used transforms that are Discrete Cosine Transform (DCT), Fast Fourier Transform (FFT), Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD). Which proved to be more robust and imperceptible compared to spatial domain techniques since disperse the watermark in the special domain of video frame, making it very difficult to remove the embedded watermark.

4.2 SVD TECHNIQUE: Basically the SVD (singular value decomposition) is a numerical technique which is used for diagonalizable matrices in numerical analysis. In SVD transformation, a matrix can be decomposed into a multiplication of three matrices which are linear algebra technique that decomposes a given matrix into three component matrices are left singular vectors, set of singular values and right singular vectors.

4.3. SVD WATERMARKING: SVD watermarking is designed to work on binary. For an image of $N \times N$ pixels and a binary watermark of p pixels, divided the image into $(N/4) \times (N/4)$ non overlapping blocks whose size is 4×4 pixels. Which is based to decide the positions of embedded blocks for each watermark bit. The steps are used in video watermarking are Inserting a watermark, it consists of a watermark insertion unit that uses Original video, watermark and a user key to obtain the watermarked video. Watermark insertion unit, It consists of the user key, input video and the watermark is passed through a watermark insertion unit which results in a watermarked video. Watermark Extraction Unit, It has two phases are locating the watermark and recovering the watermark information. Watermark Detection Unit consists of an extraction unit to first extract the watermark for comparing it with the original watermark inserted and the output is yes or no depending on whether the watermark is present.

V. RELATED WORK

Gayyer 2006, study that spatial watermarking can also be applied using color separation, in which the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing, though, the mark appears immediately when the colors are separated for printing. The document useless for the printer unless the watermark can be removed from the color band. This approach is used commercially for journalists to inspect digital pictures, photo- stock house before unmark versions [2]. Behal et. al 2012, presents the gap in Frequency domain and Spatial-domain methods, frequency-domain methods are more widely applied than spatial domain. The intent is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients [8]. Chang et. al 2005, described that DCT (Discrete cosine transform) like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image [9]. Harrison et. al 2008, described that the basic idea of DCT in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequencies [10]. Szczypiński et. al 2001, described that discrete wavelet transform derived features used for digital image texture analysis. Wavelets appear to be a suitable tool for this task, because they allow analysis of images at various levels of resolution [11]. Delaigle, 2002 study the main features of human visual system (HVS) to be translated into watermarking technology and highlights the need for dedicated inputs from the human vision community and not to provide a thorough description of the HVS. In a synthetic way and from an engineering perspective, HVS features on which the designer of a watermarking algorithm can rely, i.e. its sensitivity and masking capabilities.[7]. Ahmad et. al 2010 suggested absolute values of DCT coefficients that are divided into an arbitrary number of segments and the energy of each segment is calculated. Watermarks are then embedded into the selected peaks of the highest energy segment. Watermarks are extracted by performing the inverse operation of watermark embedding process. Simulation results indicate that our proposed watermarking method is highly robust against various kinds of attacks such as noise addition, cropping, re-sampling, re-quantization, MP3 compression, and echo, and achieves similarity values ranging from 13 to 32. In addition, our proposed method shows SNR (signal-to-noise

ratio) values ranging from 13 dB to 24 dB. [6]. Manaf et. al 2011 presented watermarking embedded in frequency domain using DWT or DCT can affect the imperceptibility and robustness of watermarking, this paper studies the effect of embedding domain on the imperceptibility and robustness in genetic watermarking. Results of watermark image quality and attacks based on peak signal-to-noise ratio (PSNR) numerical correlation (NC) is analyzed through the paper sections, the DWT results showed more robustness high imperceptibility than DCT in watermarking based on GA. [12]. Khanna et. al 2013 presented digital image watermarking is used for copyright protection of digital information, with the widespread of internet; the intellectual properties are accessible and manipulated easily. It demanded to have different ways to protect data. Digital watermarking provides a viable and promising solution. In this paper, we have described about the three different watermarking techniques (LSB, DCT, DWT) along with the various performance parameters required to evaluate the best technique out of them. This can help us to propose and implement new technique to achieve maximum robustness against various attacks. [13].

TABLE 1: COMPARISON OF VIDEO WATERMARKING METHODOLOGY

YEAR	AUTHOR NAME	Title	METHOD	PERFORMANCE
2001	Szczypinski et. Al	Discrete wavelet transforms – derived features for digital image texture analysis.	DWT with image resolution.	Features used for digital image textual analysis.
2002	Delaigle	Human Visual System features enabling watermarking.	HVS on sensitivity and masking capabilities.	Synthetic way in HVS to rely the algorithm.
2005	Chang et. Al	A Survey of Digital Image Watermarking Techniques.	DCT based watermarking techniques.	Represent data in frequency space rather than amplitude space.
2006	Mahmoud EL Gayyer	Watermarking Techniques Spatial Domain Digital Rights Seminar.	Spatial domain and Color Separation.	Inspect digital photos.
2008	Harrison et. al	A Study of Digital image watermarking.	Image processing with DWT.	Decompose image into different spatial domain.
2010	Ahmad et. Al	A new DCT-based watermarking method for copyright protection of digital audio	Audio Watermarking on DCT.	Copyright performance with SNR.
2011	Manaf et. al	Study of the effect 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.
2012	Behal et. al	A Study of Digital image watermarking.	DWT/DCT/HVS Presents the gap in Frequency domain and spatial-domain methods.	Embed the watermark in coefficient spectral.

2013	Khanna et. al	A Study on Spatial and Transform Domain Watermarking Techniques.	LSB/DCT/DWT to find best technique out of them.	Implement new techniques for achieving maximum robustness.
------	---------------	--	---	--

VI. CONCLUSION

Watermarking is a vast field and a lot of research is going on in this area. There are commercial players who are vying for dominance in this field. Though a clear-cut winner has not been declared yet, a combination of other cryptographic techniques (such as encryption) and watermarking together will definitely provide copyright protection for images. Depending on the intended requirements and the level of security required, an appropriate watermarking algorithm can be chosen. Nowadays it the strong need for blind video watermarking due to copyright protection. This technique of SVD is different from image watermarking. This paper gives a brief review of current technology. The paper also proposed contribution in using SVD characteristics. The main contributions in this paper are a novel perceptual technique, a new prospective vision in utilizing the SVD Properties. The algebraic background of this method is very clearly studied. This technique optimizes the robustness factor. This paper focuses on survey of the current literature on digital video watermarking. We classified watermarking algorithms based on the transform domain in which the watermark is embedded. Also, discusses about the watermarking attributes, applications and techniques used. In future work we are working on video technique such as svd for better performance.

REFERENCES

[1] Hesrnandez, J.R., "Image Processing," IEEE Signal Processing Society," Vol. 9, pp. 55-68, 2000
 [2] M. El. Gayyer, "Watermarking Techniques Spatial Domain Digital Rights Seminar," 2006
 [3] F. Hartung, B. Girod, "Watermarking of compressed and uncompressed video," signal process. Vol. 66, pp. 283-301 1998.
 [4] C. I. Podilchuk, E. J. Delp, " Digital Watermarking: Algorithms and Applications, " IEEE Signal Processing Magazine," pp.33-46, 2001
 [5] B. Zhu, M. D. Swanson, A. Tewfik, "Transparent Robust Authentication and Distortion Measurement Technique for Images", 1997.
 [6] P. K. Dhar, M. I. Khan, S. Ahmad, "A New DCT - Based Watermarking Method For Copyright Protection of Digital Audio", International journal of computer science and information technologies(IJCSIT), Vol.2, No. 5, 2010
 [7] Delaigle, J.F. , "Human Visual System features enabling watermarking", IEEE international conference, Vol. 2 pp. 489-492, 2002.
 [8] M. kaur, S. Jindal, S. behal, "A Study of Digital image watermarking", Volume2, Issue 2, 2012.
 [9] V. M. Potdar, S. Han, E. Chang, "A Survey of Digital Image Watermarking Techniques," 3rd IEEE International conference on Industrial Informatics (INDIN), 2005.
 [10] E. Brannock, M. Weeks, R. Harrison, "Watermarking with Wavelets: Simplicity Leads to Robustness", IEEE, pp. 587-592, 2008.
 [11] M. Kociolek, A. Materka, M. Strzelecki P. Szczypiński, "Discrete wavelet transform – derived features for digital image texture analysis," Interational Conference on Signals and Electronic Systems, pp. 163-168, 2001.
 [12] A. Shaamala, Shahidan M. Abdullah, A. A. Manaf, "Study of the effect DCT and DWT domains on the imperceptibility and robustness of Genetic Watermarking", International journal of computer science issue, Vol.8, issue 5, No.2, 2011.
 [13] P. Dabas, K. Khanna, "A Study on Spatial and Transform Domain Watermarking Techniques", International journal of computer application, vol.71, No.14, pp. 38-41, 2013.