Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2015, 2(1): 80-85

Research Article ISSN: 2394 - 658X

Blind Video Watermarking based on SVD and Multilevel DWT

Sakshi Batra and Rajneesh Talwar

Department of Electronics and Communication Engineering, Chandigarh Group of Colleges (CGC), Landran, India
sakshi.lpu@gmail.com

ABSTRACT

Computerized media content security has progressively turned into an imperative issue. Since video watermarking is a major technology used in copyright protection, a key prerequisite for it is the advancement of the imperceptibility and robustness. We propose a hybrid watermarking scheme for digital videos based on singular value decomposition (SVD) and multilevel Discrete Wavelet Transform (DWT). The two key aspects of watermarking schemes are copyright protection and robustness. In this, we are embedded the watermark in the video frames in two forms using SVD portioning of the watermark, the video frames are portioned into layers (RGB) and DWT sub-band decomposition of host video, for providing copyright protection as well as reliability. Since Scaling factor is an image dependent so we are providing it in the form of a matrix. First level embedding of the singular values is used for substitution of the singular values of the selected video frame layer providing efficient robustness and fidelity of the scheme. The second embedding is used hiding the U and V matrix from SVD of the watermark are converted to binary form and then embedded into the lowest energy band of the DWT transform of the selected layer. Experimental results are provided to illustrate that the proposed scheme is able to withstand a variety of video processing attacks as well as imperceptibility, especially in geometrical attacks.

Key words: Digital video watermarking (DVW), singular value decomposition (SVD), discrete wavelet transform (DWT), discrete cosine transforms (DCT)

INTRODUCTION

Whirlwind neoplasm of networks such as Internet, wireless communication and Intranet has facilitated the wide use of multimedia techniques and digital data. Ergo this galloping progression provides an accomplished nicety to embrace the knowledge. Transmission of information has become rather swift and sheer due to the same but as all good things come at a price, this in turn has multiplied the casualties of bushwhack [1] and assail on the data that is being transmitted. To fence this, many techniques have come into foray in the recent past. These techniques are broadly categorized under Copyright Protection Solutions. Such protection becomes imperative as it is pretty easy to clone digital data and doctor it as per one's requirements. The main features of information hiding are capacity, security and robustness. Capacity is the amount of information which can be hidden. Detecting the hidden information is security and robustness is the ability to resist any modification of the content before information is destroyed. Digital watermarking is a technique that can serve this purpose [2]. Various types of information is embedded in digital content using Digital Watermarking. In simpler terms, A watermark is used as information to validate the data and protect copyrights [3]. There are large number of watermarking schemes that have been proposed to hide copyright marks and other related information in digital images, video, audio and other multimedia objects. Digital watermarking otherwise called watermark insertion or watermark embedding(implanting), represents the method of inserting data into interactive media data additionally called original media or cover media e.g. text, audio, image, video [4]. Major applications include tampering detection of videos placed on the WWW and authentication of videos received from questionable sources [5]. Robust watermarks are required to remain in the watermarked video even after it has been attacked. Digital Watermarking could also be considered as a prolongation of Steganography, which has built its base as an encouraging solution for copyright protection [6]. Major applications include ownership establishment, copyright and distribution control. Data hiding watermarks, also

called steganography [7], are used to embed data in the videos with the intention to have the data recovered perfectly at the receiver. Such methods usually assume that there are no hostile or even casual attacks. Data integrity is not secure in image transfers. The copyright data may be in the form of text [8].

Video watermarking is relatively a new technology that has been proposed to solve the problem of illegal manipulation and distribution of digital video [9]. Apparently any image watermarking procedure can be reached out to watermark videos, but in reality video watermarking procedures need to meet different difficulties than that in image watermarking schemes for example huge volume of inherently redundant data between frames, the unbalance between the motion and still regions, real-time requirements in the video broadcasting etc. Watermarked video sequences are very much susceptible to pirate attacks such as frame averaging, frame swapping, statistical analysis, digital-analog (AD/DA) conversion, and lossy compressions. As indicated by the working domain, video watermarking techniques are classified in pixel domain and transform domain methods. In pixel domain the watermark is embedded in the source video by straightforward expansion or bit substitution of selected pixel positions. The primary preferences of utilizing pixel domain techniques are that they are conceptually easy to comprehend and the time unpredictability of these methods are low which supports real time implementations. But these techniques generally lacks in providing adequate robustness and imperceptibility requirements. In transform domain methods, the host signal is transformed into a different domain and watermark is embedded in selective coefficients. Detection is generally performed by transforming the received signal into appropriate domain and searching for the watermarking patterns or attributes. Commonly used are the Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), the Singular Value Decomposition (SVD) and the Discrete Wavelet Transform (DWT). The transform-domain watermarking have proved to be more robust and imperceptible when compared to spatial domain transforms, as they disperse the watermark in a special domain of video frame, proving it to be very difficult to remove[10]. The main advantage of the transformed domain watermarking is the easy applicability of special transformed domain properties. For example, working in the frequency domain enables us to apply more advanced properties of the human visual system (HVS) to ensure better robustness and imperceptibility criteria. Video watermarking usually prefers robustness. In a robust algorithm to eliminate, the watermark without rigorous degradation of cover content is not possible. In this paper, we introduce the Video Watermarking with features required to robustly watermark video for a valuable application. We review several algorithms, and introduce frequently used key techniques. Thus, the following section presents some useful Techniques (SVD, DWT), Terminology of Video Watermarking, Objective, Proposed Work and finally Results.

SINGULAR VALUE DECOMPOSITION

Singular Value Decomposition (SVD) is a numerical technique for diagonalizing matrices in which the transformed domain consists of basis states that is optimal in some sense. The SVD of an N x N matrix A is defined by the operation:

$$A = U\ S\ V\ T \quad (1)$$

Where U and V Є R N x N are unitary, and S Є R N x N is a diagonal matrix. The diagonal entries of S are called the singular values of A and are assumed to be arranged in decreasing order σi > σi +1. The columns of the U matrix are called the left singular vectors while the columns of the V matrix are called the right singular vectors of A. Each singular value σi specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image layer [12 -14].

In SVD-based watermarking, a frame image is treated as a matrix decomposed into the three matrices; S, U and V T, as shown Fig. 1.

$$SVD(A) = \begin{bmatrix} U_{1,1} & \cdots & U_{1,n} \\ U_{2,1} & \cdots & U_{2,n} \\ \vdots & \cdots & \vdots \\ U_{n,1} & \cdots & U_{n,n} \end{bmatrix} \begin{bmatrix} \sigma_{11} & 0 & 0 & 0 \\ 0 & \sigma_{22} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \sigma_{m} \end{bmatrix} \begin{bmatrix} V_{1,1} & \cdots & V_{1,n} \\ V_{2,1} & \cdots & V_{2,n} \\ \vdots & \cdots & \vdots \\ V_{n,1} & \cdots & V_{n,n} \end{bmatrix}^{T}$$

Fig. 1 The SVD operation SVD (A) = U S V T

DISCRETE WAVELET TRANSFORM (DWT)

Wavelets likewise speaking to indicators in a structure closely resembling sines and cosines while tending to the issue with Fourier investigation. DWT is a change focused around recurrence space. In DWT the circulations of the recurrence is changed in each one stage of DWT, where L speaks to Low recurrence, H speaks to High recurrence and subscript behind them speaks to the amount of layers of converts. Sub diagram LL speaks to a low recurrence band the more level determination rough guess of the first feature, LH a flat high recurrence band, HL vertical high recurrence band, HH an inclining high recurrence band. In DWT, the most noticeable data in the sign shows up in

high amplitudes and the less conspicuous data shows up in low amplitudes. Information clamping might be accomplished via tossing these low amplitudes. The wavelet converts empowers high packing degrees with great nature of recreation Wavelet convert is capable of giving the time and recurrence data all the while, consequently giving a time frequency representation of the sign. DWT is accepted to all the more correctly model parts of the HVS (Human Visual System) as contrasted with the FFT or DCT. This permits to utilize higher vitality watermarks as a part of districts that the HVS is known to be less sensitive to inserting watermarks in these regions increases the vigour of watermark, extra effect on picture quality. Tentatively it is, no doubt found that insertion in the LL part of the DWT turns out to be most powerful against different sorts of assaults. Multi resolution property of DWT aides in disintegration of pictures. The picture is passed through different ortho normal channels with the goal that the picture gets isolated into four non-covering multi resolution sub-groups. These sub bands are LL, LH, HL, HH i.e. rough guess, even subtle elements, vertical points of interest and askew points of interest as appeared. One of main strengths of wavelet transform compared to the DCT and DFT is its similarity with Human Visual System (HVS) which allows the watermark to be embedded in the regions that the HVS is known to be less delicate to, for example, the high resolution detail bands LH, HL, and HH. Inserting watermarks in these regions permit us to increase the robustness of our watermark, at little to zero additional impact on image quality.

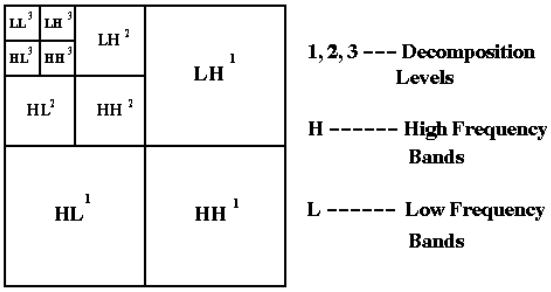

Fig. 2 DWT filter up to 3-level

TERMINOLOGIES OF VIDEO WATERMARKING

Video watermarking embeds data in the video for the purpose of identification, annotation and copyright. A number of video watermarking techniques have been proposed. These techniques exploit different ways in order to embed a robust watermark and to maintain original video fidelity. Conventional encryption algorithms permit only authorized users to access encrypted digital data. Once such data are decrypted, however, there is no way in prohibiting its illegal copying and distribution. The important terminologies pertaining to digital video watermarking are:

Digital Video
Video sequence is a accumulation of sequential and equally time spaced still images.

Payload
It is the amount of data that can be stored in a watermark. A vital idea in regards to the video watermarking payload is watermark granularity. Watermark granularity can be characterized as the amount of information is needed for embedding one unit of watermark data.

Perceptibility
Video watermarking procedure is called imperceptible if humans cannot recognize the original video from the video with embedded watermark.

Robustness
A fragile watermark should not be robust against intentional modification techniques, as failure to detect the watermark signifies that the received data is no longer authentic. In case of application such as copyright protection, it is desirable that watermark always remains in the video data, even if the video data is subjected to intentional and unintentional signal processing attacks. Hence, depending on the requirements of the application the watermark is embedded in a robust, semi-fragile or fragile manner.

Security
The security of the watermarking algorithm is ensured in the same way as in encryption methodology. According to the Kerckhoff's assumption, the algorithm for watermark embedding can be considered to be public, where as the security depend solely on the choice of a key from a large key space.

Video watermarking is not a standalone technology. It can be associated with different approaches to achieve a sophisticated system. This research can be continuous by applying this new proposed scheme to specific environment or application and examine its usefulness.

OBJECTIVE

A strong need to develop a robust watermarking system in order to secure copyright protection has pumped up research on multimedia security issues and watermarking techniques. We propose a new approach for watermarking based upon this investigation. This system uses different techniques of embedding watermarks on different layers by using Hybrid systems. As discussed earlier, this system does not need original video during watermark extraction. This process is blind as the watermark values are changed into binary values. Moreover, these values are disguised using the key value entered by the user. The binary value thus generated is embedded using the already chosen layer of the original video frame. Singular value decomposition technique is used for the same. Hence, there is no need of the original video in the extraction algorithm. This facilitates a blind check of the embedded binary signature by matching the watermark generated signature with the user key. In case the signatures do not match, it is extracted as per the second embedding algorithm. Moreover, necessary steps have been taken to overcome the chances of Visual Perceptibility Degradation caused due to watermarking so that the robustness of this technique against pirate attacks could be proved.

PROPOSED WORK

We present the proposed innovative digital video watermarking scheme. A scene-based video watermarking scheme is proposed, which is robust against the attacks of frame rotation, cropping, median, mean and averaging which were not solved adequately in the past algorithm. Moreover, a hybrid approach is proposed, which can improve the robustness of the watermarking scheme using independent. To enhance the fidelity of the scheme, key generation and wavelet based key embedding watermarking scheme is presented. The new watermarking scheme proposed is based on hybrid model using singular values from watermark image after resizing and using singular values of the wavelet decomposed frame's selected layer and also embedding the watermark key obtained using key generation with watermarks decomposed orthogonal values and embedding in the 4-level decomposition of the selected low energy band of the decomposed band. This is a basic watermarking which is based on Multilevel DWT cascading with SVD. DWT decomposes the image into four frequency bands: LL, HL, LH, and HH band. LL band represents low frequency, HL and LH represent middle frequency and HH represents high frequency band, respectively. LL band represents approximate details, HL band gives horizontal details, LH provides vertical details and HH band highlights diagonal details of the image. In this proposal, we select HH band to embed the watermark because it contains the finer details and contributes insignificantly to the image energy. Hence watermark embedding will not affect the perceptual fidelity of cover image. Moreover, high energy LL band coefficient cannot be tweaked beyond certain point as it will severely impact perceptual quality. Also, observed that watermark inserted in HH band survives certain image processing operations like noise addition, intensity manipulation and limitation of the human visual system can be exploited by inserting watermark into HH band. HVS fails to differentiate changes made to HH band. The proposed scheme is based on the idea of replacing singular values of the HH band with the singular values of the watermark. If a watermark is selected such that its singular values lies within the given range, then the energy of the singular values of watermark will be approximately equal to the energy of the singular values of the HH band. Hence the replacement of the singular values will not affect perceptual quality of image and the energy content of HH bands. Experiments have been performed on this video watermarking scheme to prove its performance. The effectiveness of this scheme is verified through a number of experiments.

RESULTS

It uses MATLAB software for the purpose to design coding for Video Watermarking using Multilevel DWT and SVD. Thus, based on these techniques, the performance of the proposed approach has been tested on the video sequences. The performance has been evaluated in terms of imperceptibility and robustness against various attacks. The Correlation is used to measure the visual quality of watermarked and attacked frames. Hence, PSNR values for all frames, Correlation values and Similarity index for all frames has been carried out for the proposed scheme and values for selected frames shown in the following tables.

Table- 1 PSNR Values

Frame	1	7	16	22	28	32	35
PSNR	43.1	30.3	31.5	31.8	31.4	31.3	33.3

Table- 2 Correlation Values

Frame	1	7	16	22	28	32	35
Correlation values	0.7519	0.9391	0.9072	0.9051	0.9218	0.9375	0.9118

Table- 3 SSIM Values

Frame	1	7	16	22	28	32	35
SSIM values	0.9699	0.9985	0.9984	0.9984	0.9982	0.9984	0.9984

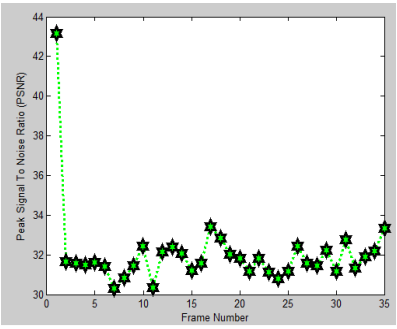

Fig. 3 PSNR all frames

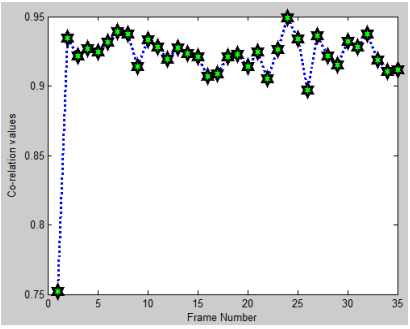

Fig. 4 Correlation Values for all frames

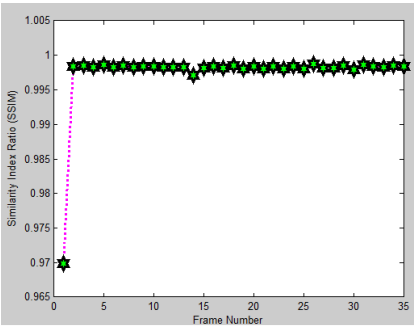

Fig. 5 SSIM values all frames

Extraction of watermark without any attack

Fig. 6 (a) Original watermark (b) Retrieved Watermark of Proposed Scheme

Extraction of watermark with various attacks

(a) (b) (c) (d) (e)

Fig. 7 (a) Crop attack (b) mean attack (c) noise attack (d) median attack (e) rotation Attack

CONCLUSION

We have seen from experimental results that before applying attacks, almost we have extracted the watermark successfully. The results are also better for one group of attack such as Crop attack, then another group of attacks (Mean and Median) on the watermark embedded in video frames. Since applying DWT coefficients of multiband increases the robustness of the algorithm. Moreover, A Blind process is carried out so it does not need original data at the time of Extraction and also it does not need any information in the detection process and the proposed scheme as discussed is robust against attacks like Crop, Mean, Median, Noise and Rotation attacks. So, the proposed scheme satisfies the requirement of imperceptibility and robustness for a feasible watermarking scheme. In the future research work, we will incorporate other attacks like sharpening, brightening compression, resize, and many more to get more robustness towards the digital watermark extraction.

REFERENCES

[1] N R Bamane and S B Patil, Comparison and Performance Analysis of different Video Watermarking Techniques, *International Journal of Scientific and Engineering Research*, **2013**, Vol.4, Issue.1

[2] S Batra and H K Khattra, An Improved Data Transfer Technique Using Steganography with Watermarking and Visual Cryptography, *International Journal of Innovative Technology and Exploring Engineering*, **2013**, Vol. 3, Issue. 7.

[3] Prachi V Powar and S S Agrawal, Design of Digital Video Watermarking Scheme Using MATLAB Simulink, *IJRET*, **2013**, Vol.2, Issue. 5.
[4] H Shojanazeri, W Azizun, S Mumtadzah and S Ahmad, Video Watermarking Techniques for Copyright Protection and Content Authentication, *International Journal of Computer Information Systems and Industrial Management Applications*, **2013**, Vol.5, p. 652–660.
[5] Mohan, A Chimanna and S R Khot, Video Watermarking Techniques for Secure Multimedia Creation and Delivery, *International Journal of Engineering Research and Applications*, **2013** , Vol. 3, Issue. 2.
[6] S S Bedi, Rakesh Ahuja and Himanshu Agarwal, Copyright Protection using Video Watermarking based on Wavelet Transformation in Multiband, *International Journal of Computer Applications*, **2013**, Vol. 66 Issue. 8.
[7] S Nafees Ahmed, B Sridhar and C Aru, Robust Video Watermarking based on Discrete Wavelet Transform, *International Journal of Computer Network and Security*, **2012** ,Vol. 4 No 1.
[8] R A Sadek, SVD Based Image Processing Applications: State of the Art, Contributions and Research Challenges, *International Journal of Advanced Computer Science and Application*, **2012**, Vol. 3, p.26-34.
[9] M Mohamed Sathik and S S Sujatha, A Novel Based Invisible Watermarking Technique for Digital Images, *International Arab journal of e-Technology*, **2012,** Vol. 2, No. 3.
[10] J Madia, K Dave,V Sampat and P Toprani, Video Watermarking using Dynamic Frame Selection Technique, *International Journal of Computer Applications (IJCA)*, **2012**, p.31-34.
[11] C Cruz Ramos, R Reyes-Reyes, M Nakano-Miyatake and H Perez-Meana, A Blind Video Watermarking Scheme Robust to Frame Attacks Combined with MPEG2 Compression, *Journal of Applied Research and Technology*, **2010,** Vol.8, Issue. 3, p.323-339.
[12] P Tsai Chang and C Lin, SVD-based Digital Image Watermarking Scheme, *Pattern Recognition Letters*, **2005**, Vol. 26, p.1577-1586.
[13] Y Wu, On the Security of SVD-Based Ownership Watermarking, *IEEE Trans Multimedia*, **2005,** Vol**.** 7, p. 624-627.
[14] Liu and T Tan, A SVD-based Watermarking Scheme for Protecting Rightful Ownership, *IEEE Trans Multimedia*, **2002**, Vol. 4, p.121-128.