Robustness and Quality Analysis of Video Watermarking Methods

Mr. J. O'Connor[*1] & Dr. L. Hughes[2]

[1]Department of Electronics and Communication Engineering, Trinity College Dublin, Dublin, Ireland
[2]Department of Electronics and Communication Engineering, University College Dublin, Dublin, Ireland

ABSTRACT

A digital watermark is added to a image/frame, is a more or less visible information in the form of a text, logo, audio etc. that has been added to the original image, audio or video. The added information can be more or less transparent to make it either easy or hard to recognize the watermark. Video watermarking is relatively an innovative tool that has been proposed to solve the problem of illegal manipulation and sharing of digital video. It is the process of embedding copyright information into video watermarking. In this paper, we use DWT (discrete wavelet transforms) and SVD (single vapour decomposition) for embedding video watermarking algorithm and then we use IDWT (inverse discrete wavelet transforms) for extracting the video watermarking. For this video embedded and extraction of watermarking process we include image watermarking to get easy video watermarking and better understanding. The performance of the proposed algorithm is analyzed by using MSE, PSNR by adding attacks.

KEYWORDS: Video watermarking, DWT, SVD, IDWT, MSE, PSNR, noise attack.

I. INTRODUCTION

Digital watermarking is the method of embedding data into digital multimedia content (it may be a image, video or audio). In this paper we used the multimedia content as video so it is known as Video watermarking. This is used to verify the credibility of the content or to recognize the identity of the digital content's owner. Digital watermarking can be employed for multiple purposes, such as: Copyright protection, Source tracking, Broadcast tracking, such as watermarked videos from global news organizations, Hidden communication

There are two types of digital watermarking. They are:
a)Visible Digital Watermarking: Visible data is embedded as the watermark. This can be a logo or a text that denotes a digital medium's owner.
b) Invisible Digital Watermarking: The data embedded is invisible or, in case of audio.

In this paper we used Invisible digital watermarking i.e., invisible video watermarking.

In this study, we propose a copyright protection for a video and a blind, imperceptible and robust video watermarking technique. The algorithm is based on two mathematical transforms: the Discrete Wavelet Transform (DWT) and the Singular Value Decomposition (SVD).The two transforms are different transform domain techniques and thus provide different, but complementary, levels of robustness against the same attack.

The watermark is added to the video signal that carries information about sender and receivers of thedelivered video and attacks are given to check whether watermark is attacked or not.

Important characteristics of VIDEO WATERMARKING
A good watermarking technique is expected to have following characteristics:

Robustness- robustness refers to the ability of recovering embedded watermark even after performing intentional ornon-intentional processing of watermarked image.
Imperceptibility- imperceptibility refers to the perceptual similarity between host image and watermarked image

Security- security refers to protection of embedded watermark against various attacks which try to eliminate the watermark content, inaudible.

Capacity- capacity refers to the amount of information embedded in the host image as a watermark for protection of copyright of an image

The basic components involved in robust watermarking are watermark embedding, attack, and watermark detection. In watermark embedding, a watermark (image) is constructed and then embedded into an original

video to produce the watermarked video. Once embedding is done, the watermarked video can be subjected to various attacks. The watermark detector reports whether the watermark is present or not on examining its input.

The algorithm for developing watermarks on images areextended for videos.
a) Between the frames there exists a huge amount ofintrinsically redundant data.
b) There must be a strong balance between the motions and themotionless regions
c) Strong concern must be put forth on real time and streamingvideo applications.
The following aspects are important for the design of Videowatermarking systems:
a) Imperceptibility: The watermark embedding should cause aslittle degradation to the host video as possible.
b) Robustness: The watermark must be robust to common signal processing manipulations and attempts to remove or impair the watermark.
c) Security: The embedded information must be secure againsttampering.
d) Capacity: The amount of embedded information must belarge enough to uniquely identify the owner of the video.

Applications of Video Watermarking
Digital video watermarking is used in a variety of applications.
Copyright protection: copyright protection of video data is an important issue in digital video delivery networks. There are many techniques of video watermarking for copyright protection. In one of the techniques a watermark is added to the video signal

Video Authentication: In applications involving instance videos captured by surveillance cameras, checking the integrity of the images and the video is a major issue. Fragile, semi fragile and robust watermarking are the commonly used policies. A slight modification on the cover video destroys fragile watermarks. Semi fragile watermarking can resist content conserving operations and be sensitive to content varying transforms.

Copy control: Copy protection is a widely exercised*application in video watermarking. In this a watermark is used to indicate whether a video content is copyrighted. Thiswatermark can only be removed with a severe degradation of the video sequence.*

Fingerprinting: In this technique the video is uniquely identified by its resultant fingerprint by software that recognizes extracts and then compresses distinguishing components of a video. Some of the features that are involved in video fingerprinting analysis are key frame analysis, color changes, motion changes etc. of a video sequence. In this technique watermarks are embedded as fingerprints on the video. Several fingerprinting methods extract the fingerprints on the video. The evaluation and identification of the video content is then performed by comparing extracted fingerprints.

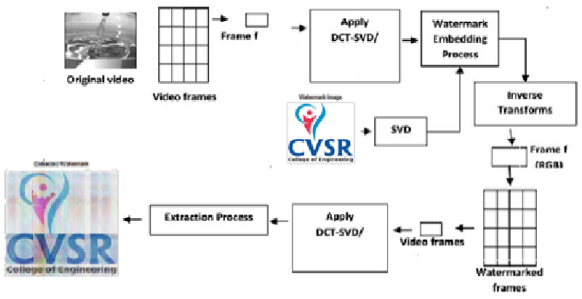
e) Broadcast Monitoring: In broadcast monitoring the content owner embeds the watermark prior to transmission. The watermark is extracted by the monitoring site that is set up within the transmission area.

Techniques in Video Watermarking
Current video watermarking techniques can be grouped into two major classes; spatial-domain watermarking techniques and watermarking frequency-domain techniques. Spatial-domain techniques embed a watermark in the frames of a given video by modifying its pixels directly. These techniques are easy to implement and require few computational resources, however, they are not robust against common digital signal processing operations such as video compression. On the other hand, transform-domain watermarking techniques modify the coefficients of the transformed video frames according to a pre-determined embedding scheme. The scheme disperses the watermark in the spatial domain of the video frame, hence making it very difficult to remove the embedded watermark.

Compared to spatial-domain techniques, frequency-domain watermarking techniques proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithm.

So, in this paper we used frequency-domain watermarking technique.

Block Diagram



The block diagram involves original video, video frames, DCT & SVD, watermark logo, IDWT, combining the video frames, watermarked video etc.

embedded and extracted of video watermarking algorithm

The necessary steps to embed the watermark into an input video data for the copy right protection purpose are as follows:

1. Divide the video into frames.
2. Select few frames which is compatible with the watermark size.
3. Perform the wavelet transformation (DWT) or different operations on the selected frames.
3. Then apply SVD then watermark was embedded into the original frames
4. Then again apply SVD to the watermarked frame followed by IDWT
5. Then we will get the Extracted watermark image.
6. Combine all the watermarked frames to create a video and compare both original video and watermarked video.
7. Apply some attacks on the watermarked frames in the video.
8. Evaluate the MSE, PSNR for embedding and extracting process before and after attacks.

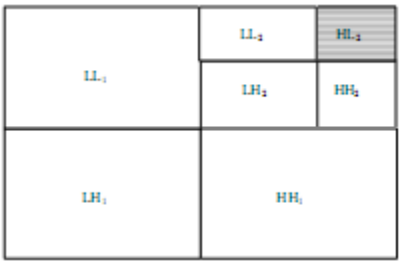
Frequency Domain WATERMARK TECHNIQUE

In this method, a watermark is embedded distributivity in overall domain of an original data, and the watermark, is hardly to be deleted once embedded. The main strength offered by transform domain techniques is that they can take advantage of special properties of alternate domains to support additional features. Besides, analysis of the host data in a frequency domain is a prerequisite for applying more advanced masking properties to enhance watermark robustness and imperceptibility.

Discrete Wavelet Transform(DWT)

The DWT (Discrete Wavelet Transform) separates an imageinto a lower resolution approximation image (LL) as well ashorizontal (HL), vertical (LH) and diagonal (HH) detailcomponents. The process can then be repeated to computemultiple “scale” wavelet decomposition. Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality.

For 2-D images, applying DWT corresponds to processingthe image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolutionsub-bands LL, LH, HL and HH. The LL sub-band represents the coarse-scale DWT coefficients while the LH, HL and HH sub-bands represent the fine-scale DWT coefficients. To obtain the next coarser scale of wavelet coefficients, the LLsub-band is further processed until some final scale N isreached



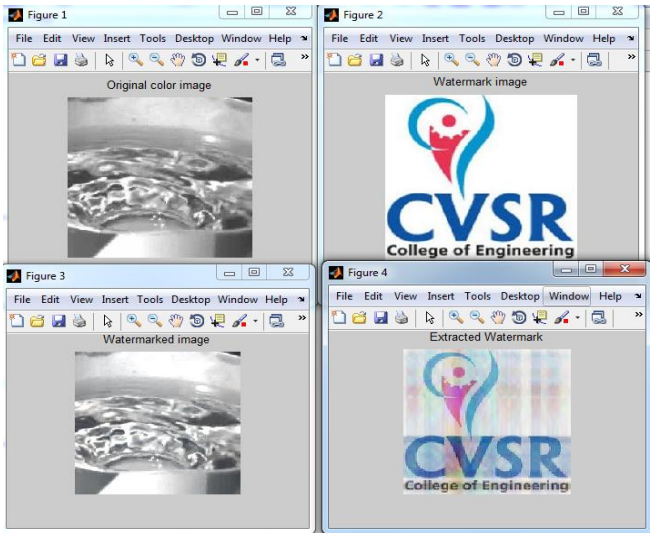
2. Video pre-process: - All frames of the video are decomposed in 4-level sub band frames by separable two-dimensional (2-D) wavelet transform. Scene changes are detected from the video by applying the histogram difference method on the video stream. Independent watermarks are embedded in frames of different scenes.
3. Watermark embedding: - The watermark is then embedded to the video frames by changing position of some DWT coefficients with the following condition:
If Wj= 1 then
Exchange (Ci, Ci+1, Ci+2, Ci+3, Ci+4);
else
Exchange (Ci, Ci+1, Ci+2, Ci+3, Ci+4);
end if
Where Ci is the ith DWT coefficient of a video frame, and Wj is the jth pixel of a corresponding watermark image.
4. Watermark detection
The video is processed to detect the video watermark
The detection is done by the following logic
If (WC (i) > median (WCi, WCi+!, WCi+2, WCi+3,WCi+4);
Then EWj
Else EWj = 0
end if

Singular Value Decomposition(SVD)
Singular Value Decomposition (SVD) is a numericaltechnique for diagonal zing matrices in which the transformeddomain consists of basis states that is optimal in somesense.

The SVD of an N x N matrix A is defined by the operation:

$$A = U S V^T$$

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



Evaluation of watermarking schemes

Many watermarking techniques are available but their use is restricted to specific areas. An evaluation metrics is needed to assess the performance and watermark security of a watermarking algorithm. A criteria which will analyze the watermarking scheme:

Imperceptibility:

Imperceptibility refers to the quality of watermarked media as noticed visually. Hence, imperceptibility depends on human visual system. Since digital watermarking embeds the watermark into a cover, image and is not directly visible to observer. Obviously, there would be distortion introduced to the digital watermarked content caused by embedding process. It is therefore desirable that an algorithm used for watermarking should add minimal distortions to the digital content. Evaluation criteria are mainly based on the following parameters explained below:

i) Mean Squared Error (MSE)

It is a method to check distortions between cover image and watermarked image. With the calculation of mean square error, we can detect any change in the watermarked image.

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(f_i - y_i)^2$$

where N is the number of data points,
f_i the value returned by the model and
y_i the actual value for data point i.

ii) Peak-Signal-to-Noise Ratio

PSNR is a better test to check distortions between original image and watermarked image because it uses mean squared error also. We can calculate PSNR by the following formula.

$$PSNR = 10\ log\frac{(2^n - 1)^2}{MSE}$$

$$PSNR = 10\ log\frac{(255)^2}{MSE}$$

PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not.

VIPCONCENTRICITY VIDEO WATERMARKCVSR 213*213	
Img1	
MSE: 64.491040	PSNR: 30.069805 dB
MSE: 50.349446	PSNR: 31.144852 dB
MSE: 16.935705	PSNR: 35.876767 dB>>psnrvalues
Img2	
MSE: 65.704269	PSNR: 29.988863 dB
MSE: 50.342811	PSNR: 31.145425 dB
MSE: 15.911459	PSNR: 36.147699 dB>>psnrvalues
Img3	
MSE: 66.874804	PSNR: 29.912174 dB
MSE: 53.343781	PSNR: 30.893961 dB
MSE: 13.844938	PSNR: 36.751889 dB>>psnrvalues
Img4	
MSE: 67.211113	PSNR: 29.890388 dB
MSE: 59.832551	PSNR: 30.395424 dB
MSE: 13.633759	PSNR: 36.818643 dB>>psnrvalues

Robustness
It is a property to check resistance against any external attacks. Now a day in many applications the strength of the watermarked image to bear noise is important. The researchers can check robustness of watermarked image through doing attacks on watermarked image, by this way they can measure the strength of robustness.

Noise Attack
Salt and Pepper: A hiding scheme must be designed to be robust enough against various watermarking attacks. We are particularly interested in investigating and designing a scheme that is robust against salt and pepper attack. Salt and Pepper noise alter the pixel value to either minimal(0) or maximal(255) for 8 bit gray scale image. Consequently, salt and pepper.

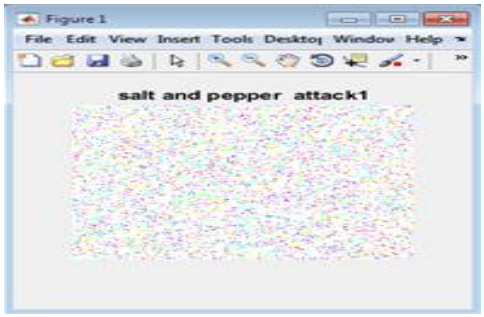


Fig1.discretely modifies the original content of the picture in both spatial and frequency domain.

Security
Security is related with the strength of embedded watermark protection in watermarked media. The security is assessed on the basis of length of time it takes to break the watermarking algorithm and reveal the hidden watermark.

II. CONCLUSION

In this paper video watermarking technique was proposed in frequency domain with better improvement in its performance. New approaches are expected to come out and may merge existing approaches. The two transforms (the Discrete Wavelet Transform (DWT) and the Singular Value Decomposition (SVD) are different transform domain techniques and thus provide functionalities, but complementary, levels of robustness against the same attack.

III. FUTURE SCOPE

Watermarking Technology is still in the evolutionary stages. Possibilities for future work include implementing a more advanced watermarking system, preferably one that could persist through compression, and implementation of the cryptographic components of the watermarking system. Any future work should be more comprehensive and realistic testing.

Normally the security technology is hackable. However, if the technology is combined with proper legal enforcement, industry standards and respects of the privacy of individuals seeking to legitimately use intellectual property; digital watermarking will encourage content creators to trust the internet more. There is a tremendous amount of money at stake for many firms. The value of illegal copies of multimedia content distributed over the internet could reach billions of dollars a year. It will be interesting to see how the development and adoption of digital watermarking plays out. With such high stakes involved for entertainment and other multimedia companies, they are likely to keep pushing for a secure technology that they can use to track and reduce copyright violation and capture some of their foregone revenues.

According to this, more encryption techniques to increase security can be used. Also different watermarking techniques can be used.

IV. REFERENCES

[1] Jashandeep Kaur Kang, Rakesh Kumar, KamaljeetKainth, Review paper on video watermarking‖ International journal of advanced research in computer science and software engineering, vol.6, issue 6,june 2016.

[2] Nisreen I. Yassin, Nan cy M. Salem, and Mohamed I. El Adawy "Block Based Video Watermarking Scheme Using Wavelet Transform and Principle Component Analysis" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, January 2012.

[3] HananeH.Mirza, HienD.Thai, Yasunori Nagata and ZenshoNakao" Digital Video Watermarking Based on Principal Component Analysis" in Department of Electrical and Electronics Engineering, University of the Ryukyus Okinawa 9030213,Japan, 2011.

[4] SanjanaSinha,PrajnatBardhan,SwarnaliPramanic k, AnkulJagatramka, Dipak K. Kole, ArunaChakraborty.."Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis"International Journal of Wisdom Based Computing, Vol. 1 (2), August 2011.

[5] Snehal V. Patel, Prof. Arvind R. Yadav "Invisible Digital Video Watermarking Using 4-level DWT" National Conference on Recent Trends in Engineering & Technology, 14 May 2011.

[6] Kesavan Gopal, Dr. M. MadhaviLatha"Watermarking of Digital Video Stream for Source Authentication" IJCSI International Journal of Computer Science Issues,Vol. 7,Issue 4, No 1, July 2010.

[7] Salwa A.K Mostafa, A. S. Tolba, F. M. Abdelkader, Hisham M. Elhindy, „"Video Watermarking Scheme Based on Principal Component Analysis and Wavelet Transform"" IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[8] Mandeep Singh Saini, VenkataKranthi B, Gursharanjeet Singh Kalra., "Comparative Analysis of Digital Image Watermarking Techniques in Frequency Domain using MATLAB SIMULINK", International Journal of Engineering Research and Applications (IJERA)ISSN: 2248-9622 Vol. 2, Issue 4, May-Jun 2012.

[9] Mrs Neeta Deshpande, Dr. Archana rajurkar ,Dr. R. manthalkar ,"Review of Robust Video Watermarking Algorithms" International Journal of Computer Science and Information Security, March 2010.

[10] Keshav S Rawat, Dheerendra S Tomar,"Digital watermarking schemes for authorization against copying or piracy of color images" IndianJournal of Computer Science and Engineering Vol. 1 No. 4 295-300. [10] HananeMirza, Hien Thai, and ZenshoNakao,"Digital Video Watermarking Based on RGB Color Channels and Principal Component Analysis", KES 2008, Part II, LNAI 5178, pp. 125–132, 2008.

[11] Yuan Y., Huang D., Liu D., "An Integer Wavelet Based Multiple Logo- watermarking Scheme", In IEEE, Vol-2, pp. 175-179, 2006.

[12] X. Niu and S. Sun, "A New Wavelet-Based Digital Watermarking for Video," in Proceedings of the 9th IEEE Digital Signal Processing Workshop, 2000, pp. 241-245.

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