Robust Digital Video Watermarking using Reversible Data Hiding and Visual Cryptography

Manoj Kumar[1] and Arnold Hensman[2]

School of Informatics and Engineering

Institute of Technology Blanchardstown, (ITB), Blanchardstown, Dublin.

E-mail: [1]wss.manojkumar@gmail.com [2]arnold.hensman@itb.ie

Abstract □ Watermarking is a major image processing application used to authenticate user documents by embedding and hiding some authenticated piece of information behind an image, audio or the video file. For example, copyright symbols or signatures are often used. Our proposed work is to develop and implement an improved layered approach to video watermarking. The traditional watermarking approach tends to embed an entire watermark image within each video frame or within random video frames to give the appearance of a hidden watermark to the casual observer. This work proposes a more efficient and secured approach to perform watermarking, by using sub image classification. That is to say, selected frames only will contain a fractional number of total bits from the watermark image. We take *k* bits from the watermark and store then within a video frame, depending on the size of that watermark image. Our algorithm is capable of hiding high capacity information over video frames. The novel approach is to partially distribute the watermarking data over a set of frames until the entire watermark is eventually distributed throughout the entire video. The originality our technique is that it is a histogram inspired and reversible watermarking approach as defined with visual cryptography. Our approach hides similar watermarking bits of information with frames of a similar appearance. Differing sets of watermark bits are thus embedded within dissimilar frames, thus making the system more robust. It will provide a high degree of authentication, as the extraction of information from a single frame only will not reveal the entire watermarking data, or even give any obvious indication that it contains a fraction of the watermark bits. The robustness of our technique will be tested by calculating MSE, PSNR values and by performing some common attacks upon a series of videos.

Keywords – Invisible Video Watermarking, Visual Cryptography, Wavelet Transformation.

I INTRODUCTION

Digital watermarking is a process of hiding a user signal within a standard video covert signal for the purposes of identification. Hiding a watermark within digital data helps to mitigate unauthorized access and provides copyright protection of the data. A major obstacle is achieving invisibility of the watermark and its resilience to attacks [1]. While many different watermarking techniques are used with varying robustness and performance, watermarking provides content protection and digital rights management, making it the most popular solution towards digital data and author identity protection [2]. Applications include copyright protection and control, ownership identification, forensics analysis and authentication. Robust watermarking is achieved by embedding copyright content within digital data that is vulnerable to malicious or non-malicious attacks [3]. We set out to improve on standard techniques by providing the provision of partial watermarking throughout a wide array of video frames.

Digital watermarking is classified into three categories: *Spatial Domain*, *Transformation Domain* and *Compressed Domain*. In the spatial domain, watermark information is directly embedded into the luminance values of the pixels. In compressed domain techniques such as MPEG 1-4, H.26, the information is embedded into the VLC code by modifying the motion vector information.

Transformation domain techniques include *Discrete Cosine Transforms* (DCT), *Fast Fourier Transforms* (FFT), *Fractal and Discrete Wavelet Transforms* (DWT). Among these transform techniques, wavelet based transformation is the most popular because of its spatial localization, frequency spread and multi resolution characteristics [1]. The main trade parameters that must be considered in digital watermarking are: *data payload, fidelity* and *robustness*. Data payload refers to the number of bits of information that can be embedded via the watermark. Fidelity is the imperceptibility to human observation after distortion of the watermark. Fidelity is noticed in terms of image quality. Watermark is embedded in the video that will affect the image/frame quality. So we will keep the image quality high and distortion minimum so that fidelity of the image is maintained and cannot be seen by human observer. Watermark is imperceptible, that it became difficult to distinguish the difference between the cover and marked signal. Finally, robustness is concerned with the extraction of the watermark from altered watermark data.

Our proposed model uses a wavelet transform with visual cryptography to improve on the robustness of watermarking and provide a high degree of authentication. Robustness is also evaluated on the resistance of the watermark to attacks performed on it [4]. A watermark insertion system is shown in Fig. 1. Firstly we divide the watermark image into *k* sub bits and then we embed this fractional information into the video frame. The value of K is for the sub division of the watermark but not for the individual pixel.

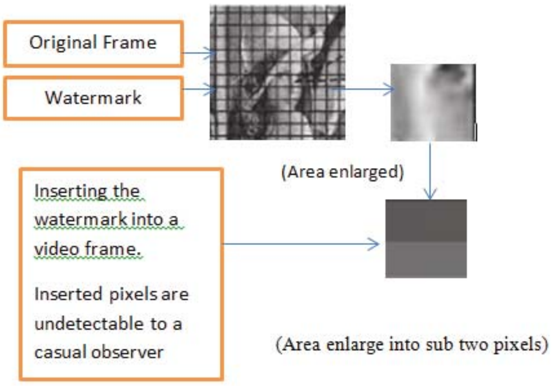
Original Frame
Watermark
(Area enlarged)
Inserting the watermark into a video frame.
Inserted pixels are undetectable to a casual observer
(Area enlarge into sub two pixels)

Fig. 1: Watermark Insertion System (Use a subset of ith from k sub pixels from the watermark)

In the traditional visual watermarking approach, we would normally be able to detect a watermark image in the video stream as a fully formed image, embedded within a single frame. Our model manipulates the fact that video is a combination of frames. When we apply a small subset of the watermark's bits to specifically chosen frames only, and then combine all frames to complete the video, the visible watermark will affectively be rendered invisible as seen in Fig. 2. In the illustration, a single watermarked video frame composed of Lena's image can be seen with both techniques applied.

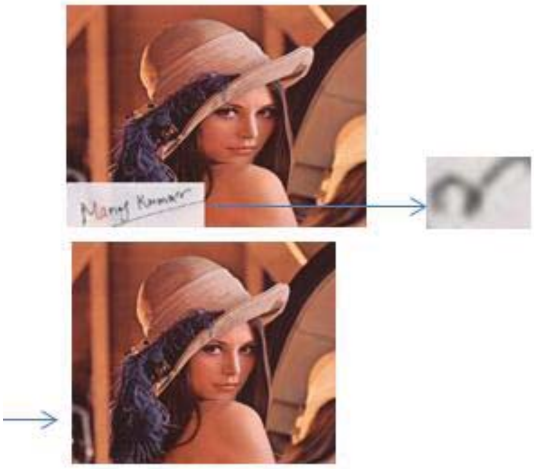

Fig. 2: Visible and Invisible Video Watermarking

II Related Works

While few video watermarking techniques can hope to resist every possible attack that might be performed against it, most schemes propose complex techniques in order to gain various advantages from different domains [10]. Various methods of watermarking have been used throughout the spatial and wavelet domains. In the spatial domain, the Least Significant Bits (LSB) of the chosen pixels in the watermark image are flipped. An improvement to this technique is to use a pseudo random number generator that chooses which pixel to embed within the watermarked data based on seed or key. This is the strength of the approach since the LSB technique is vulnerable to having the LSBs replaced with constant values. Another approach proposes a new method to exploit the patterns of additive pseudo random noise based on correlation properties as applied on the images [5] . Spatial domain watermarking schemes are not considered as robust as frequency domain techniques [6]. Threshold based watermarking is generally less effective than LSB based watermarking schemes. DCT based schemes however are considered to be very to lossy compression. While DFT based watermarking schemes can resist some attacks such as rotation, removal and sheering, DWT based schemes are more robust against noise addition in digital data

[3]. There are three primary categories of techniques used:

a) Wavelet Transform Techniques

Bhargava proposes wavelet based watermarking in which the watermark is embedded on the selected wavelet coefficients of the luminance Y of the frame [1]. In their approach, the video is firstly converted from the color space into YCbCr color space and then a 2D wavelet is applied with quantization based decomposition on the Y. The disadvantage of that technique is that it is time consuming and has some watermark detection problems. Xing Chnag et.al. consider a model which is based on a motion vector and DCT domain watermarking scheme [7]. In this hybrid version, they embed the fragile watermark within the motion vector and robust watermark in the DCT domain to achieve copyright protection and authentication.

b) Inter-frame Wavelet Transform

Zhiying Ma proposes a work frame based video watermarking technique using the inter frame wavelet transform [8] . They first divide the video frames into same frame number groups and then based on maximum levels (high frequency and low frequency frame), an inter-frame wavelet transformation is performed upon each group. In this method, only four frames are used for wavelet decomposition per frame with lower memory bands and robustness against geometrical attacks. Kalker developed a method named JAWS (Just Another Watermarking System) for broadcast monitoring applications [9]. They use the spatial domain which essentially compresses and un-compresses the video. They embed the same watermark into consecutive video frames using Gaussian and high pass filters. While more complex, it is more robust against attacks. Osama S.Faragallah presents an efficient and robust video watermarking approach based on singular value decomposition performed in DWT domain [10]. Video frames are transformed with DWT using two resolution levels, high frequency (HH) and middle frequency (LH, HL) to embed the watermark data, making it robust against video characteristic and image processing attacks.

c) Sub-Dividing the Watermark

Rupachandra Singh proposes a novel watermarking scheme based on scene change detection, DWT and visual cryptography by dividing the watermark into sub-watermark shares (although not always at the pixel level) [3]. They generate the owner share using visual cryptography and then compare pixel values of the frame with the global mean value. A.K Mostafa proposes a hybrid approach by combining DWT and PCA [11]. Experimental results show that their technique is robust against common video processing attacks.

III Proposed Scheme for Invisible Video Watermarking

Our proposed approach is divided into three layers which are can be seen in the Fig. 9. Our scheme differs from previous schemes described above in the following ways.

a) *Frame Selection:* In existing models, no algorithmic scheme is specified to identify unique and repeated frames to hold a fractional part of the watermark. We use a wavelet based schemes to perform this task. We will use a histogram inspired, reversible approach to perform the watermarking. Frame is selected on the basis of similarity pattern with every frame. We are calculating similarity based on *chi*cosine*norm distance*Euclidian*entropy* of the frames. Based on this similarity unique and non-unique frames are obtained. Higher the similarity more uniqueness in the frames.

b) *Breakdown of the Watermark:* In previous works, a static definition of visual cryptography for sub-images is generally specified. In our scheme, the watermarked image will be divided into *k* sub images containing only a few pixels with the value of k being determined dynamically based on a similarity measure over the frame. Value of k is obtained by:

$$K = \frac{\text{Size of watermark image}}{\text{Number of unique frames}}$$

For example if we have watermark of 1000 pixels and having 10 unique frames then the watermark image will be spitted in 10 sub parts of 100 pixels each. Now if we have first 5 continuous similar frames then, each continuous frame will store the same 100 pixel watermark image. It means same frame will store same watermark bits of information. And as next unique frame appear next watermark sub image will be stored.

c) *Hybrid Approach:* Our presented model is a hybrid scheme using the <u>*three*</u> main approaches: (1) Visual Cryptography, (2) Wavelet Based Similarity Measure and (3) Histogram Based Reversible Watermarking.

The primary objectives of the proposed model are as follows:

a) To define a wavelet inspired similarity check that identifies the unique frames for use in embedding the watermark. These frames will determine the number of sub watermark pixels hidden over that individual image

b) To define a *k-share* visual cryptography approach that will divide the watermark image into *k* sub-images, whereupon all *k* sub-images may be collectively re-combined to form the full watermark image.

c) To define a histogram based watermarking approach that hides the sub-watermark image over the frame.

d) To perform the extraction back from the watermarked image.

e) To analyze the effectiveness of the work under different attacks.

We propose a novel technique to perform video watermarking. Instead of hiding a complete image within an individual frame over the video, a k-share visual cryptography approach is used. The watermark image will be divided to k-sub images and each sub image will contains partial image contents. These sub parts collectively form the complete watermark image. Here the factor *k* will be identified dynamically by performing a video analysis. The number of unique frames within the video defines the number of sub watermark images. The final stage of this work is to embed the watermark in this way into the video frames. The watermarking over video frames will be performed sequentially. For identical frames, same sub-watermark image will be used.

IV Wavelet Based Analysis for Unique Frame Extraction

The input that will be given to the system is in the form of a video. Instead of working with all frames, the first task is to identify the unique frames from the video based on the similarity ratio between the video frames. This step will be defined as the pre-processing stage so that a reduction in the number of processing frames may be carried out. A set of video frames with as few repeating frames as possible will increase its effectiveness. To determine a unique frame, a DWT based similarity measure will be implemented. Based on the wavelet decomposition of frames we find the similar and non-similar frames as illustrated in Fig. 3 and Fig. 4.

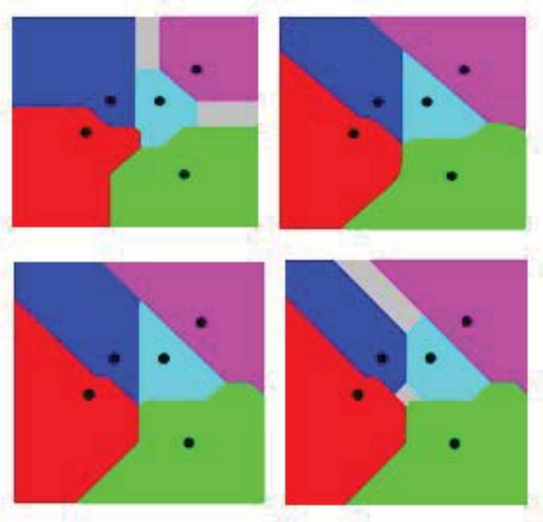

Fig. 3: Sample of non-similar video frames (output images of video)

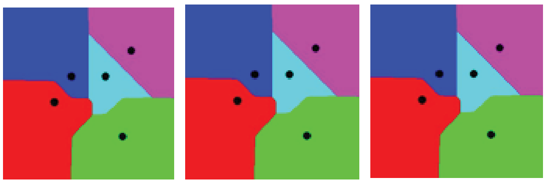

Fig. 4: Sample of similar video frames

After this decomposition, we embed the watermark image using visual cryptography.

V K-Share and Visual Cryptography

Visual cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that the decryption may be performed by the human visual system without the aid of computers [12]. Image is a multimedia component that can be sensed by the human eye. In this work, we will divide the complete watermark image into *k* sub images based on bit information extraction. The complete image will first be divided into *n* size sub blocks, and then each *n* block will be divided into *k* sub blocks. The *ith* block from this k block sequence will be taken to build the ith sub image. In the same way, all sub images will be composed to generate the cryptography watermark. Fig. 5 shows the decomposition of a watermark image into k fractional sub-blocks and Fig. 6 illustrates how we apply these fractions to the video frames

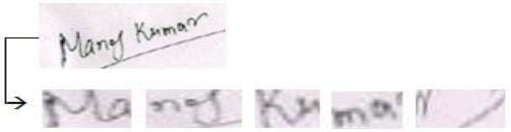

Fig. 5: Original Watermark image and its divided sub-blocks

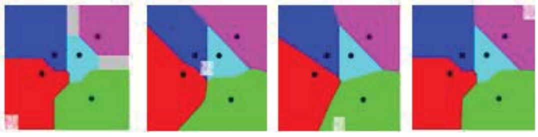

Fig. 6: Each sub-block is embedded throughout a specific video frames on different pixel areas

The highlighted area on the frames shows the watermark sub-block upon each video frame. After combining these frames, the output renders the watermark invisible within the video. Fig. 7 and Fig. 8 show that our expected appearance of the video frame before and after watermarking may look like the same original video frame.

Fig. 7: Original Video Frame

Fig. 8: Video Frame after Watermarking

VI Histogram Based Watermarking

We define a histogram based process to perform the watermarking of each sub-watermark image into a video frame. A permutation will be generated over the histogram bits under some specified rule, based on which the watermark will be performed. The permutation here is the PN Sequence (is the random sequence generated to store data over the image at arbitrary positions) that will generate to define the position where the watermark will be stored. We are using the reversible watermarking approach. For example sequence is identified based on the even and odd random sequence of the video frames for embedding the information.

The histogram analysis will be performed to identify the area where the watermark will be embedded. In this work, a multi bit approach is used for watermarking depending on the size of watermarked image.

Our three layered scheme can be seen in Fig. 9.

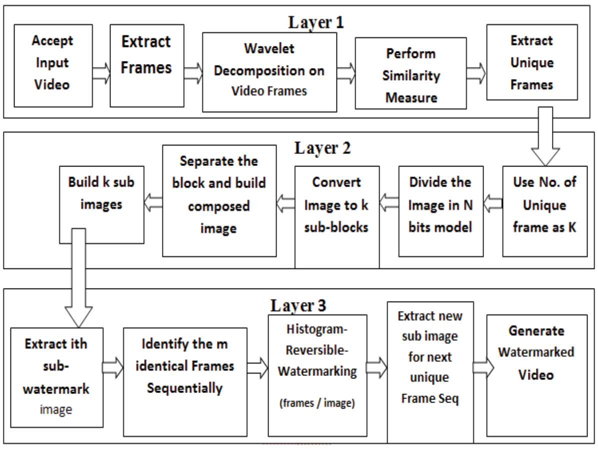
Layer 1
Accept Input Video
Extract Frames
Wavelet Decomposition on Video Frames
Perform Similarity Measure
Extract Unique Frames
Layer 2
Use No. of Unique frame as K
Divide the Image in N bits model
Convert Image to k sub-blocks
Separate the block and build composed image
Build k sub images
Layer 3
Extract ith sub-watermark image
Identify the m identical Frames Sequentially
Histogram-Reversible-Watermarking (frames / image)
Extract new sub image for next unique Frame Seq
Generate Watermarked Video

Fig. 9: Layered design of the proposed approach

VII Discreet Wavelet Transform (DWT)

In this work the DWT will be used in estimating the similarity measure between the frames. DWT offers multi-resolution representation of an image and DWT gives perfect reconstruction of the decomposed image. The image itself is considered as a two-dimensional signal. When an image is passed through a series of low pass and high pass filters, DWT decomposes the image into sub bands of different resolutions [13]. Decompositions can be done at different DWT levels. Single-Level DWT decomposition is indicated in Fig. 10. It has been widely accepted that maximum energy of most of natural images is concentrated in 'approximate (LL) sub-band', the low frequency sub-band. Hence, modification of the coefficients of these low frequency sub-bands would cause severe and unacceptable image degradation.

LL1: **Approximate Sub-band**	**LL2**	**HL2**
	LH2	**HH2**
LH1: **Vertical Sub-band**	**HH1:** **Diagonal Sub-band**	

Fig. 10: Single-Level and Two-Level Image Decomposition

VIII Expected Outcomes and Conclusion

The proposed work is capable of hiding high capacity information by embedding a partial number of pixels from the watermark over a large series of single video frames to provide a high degree of authentication. The analysis is performed in terms of MSE and PSNR values to evaluate the robustness of watermarking. Higher the value more robust is this approach. The objective is to extract a fully formed watermark that is un-corrupted after an attack. We will perform some common attacks like frame dropping; frame averaging, contrast and color enhancement, cropping, filtering attacks, adding some noise in the frames, change of resolution etc. on the video to check its resilience.

Our scheme addressed the lossless retrieval of the information while maintaining high security of the data. The primary goal is to design and implement an invisible video watermarking technique robust enough to carry a high payload by implementing a distributed secure watermark throughout a video file. The layered approach of this model makes to correctly extract the watermark information once the watermark has been embedded within a video, hence improving the security of the system. The resulting analysis will be performed in terms of extraction of the watermarked image from the video under analytical parameters such as mean square error (MSE) and peak signal to noise ratio (PSNR). Our results will be compared with the recently obtained data from other systems in terms of robustness and payload.

The proposed scheme is also capable of reversible data hiding. We propose a hybrid model of video watermarking, that incorporates visual cryptography, histogram and wavelet based approaches. It is expected that our technique will improve the robustness of the watermark data and copyright image, as well as payload. This work is also capable of extracting the original information after various distortion attacks have been performed.

REFERENCES

[1] D. N. V. Rado O Preda, "A robust digital watermarking scheme for video copyright protection in the wavelet domain," *ELSEVIER,* vol. 43, no. 10, pp. 1720-1726, 2010.

[2] S. M. a. B. Bhargava, "invisible watermarking based on creation and robust insertion-extraction of image adaptivewatermarks," *ACM Journal,* vol. 5, no. 2, pp. 1-24, Feburary 2008.

[3] K. M. S. ,. R. Th. Rupachandra Singh, "Robust Video Watermarking Scheme Based on Visual Cryptography," IEEE, 2012.

[4] J.-L. D. Gwenael Doerr, "A guide tour of video watermarking," *Elsevier Science direct,* vol. 18, no. 4, pp. 263-282, 2003.

[5] I. S. a. R. L. G. Langelaar, "Watermarking digital image and video data," *IEEE signal processing magazine,* vol. 17, pp. 20-43, sept. 2000.

[6] N. Memon, "Analysis of LSB based image steganography technique," in *IEEE Proc. ICIP*, Oct. 2001.

[7] W. W. J. Z. L. Z. Xing Chang, "A Survey of Digital Video Watermarking," in *IEEE (Seventh International Conference on Natural Computation)* , Donghua University, Shanghai,China, 2011.

[8] X. Y. W. Zhiying Ma, "Frame-based video watermarking," *Computer Engineering and Science,* vol. 32, no. 5, pp. 143-146, 2010.

[9] G. D. J. H. a. M. M. T. Kalker, "A video watermarking system for broadcast monitoring," *in Proc. SPIE IS&T/SPIE's 11th Annu. Symp., Electronic Imaging '99: Security and Watermarking of Multimedia Contents, ,* vol. 3657, jan 1999.

[10] OsamaS.Faragallah, "Efficient Video Watermarking based on singular value decomposition in the discrete wavelet transform domain," *International Journal of Electronics and Communications (AEU),* vol. 67, no. 3, pp. 189-196, 2013.

[11] Salwa A.K Mostafa et. al., "Video Watermarking Scheme Based on Principal Component Analysis and Wavelet Transform," *IJCSNS International Journal of Computer Science and Network Security,* vol. 9, no. 8, pp. 45-52, August 2008.

[12] M. N. a. A. Shamir, "Visual cryptography," *In EUROCRYPT,* pp. 1-12, 1994.

[13] Sanjana Sinha et. al., "Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis," *International Journal of Wisdom Based Computing,* vol. 1, no. 2, pp. 7-12, August, 2011.