Video Watermarking using Transforms

Dr. Dipti Patil, Sonali Bandgar, Kalpesh Nagmoti, Shraddha Borkar, Priyanka Rajage

Abstract— Recent years have witnessed rapid growth in Digital video watermarking. Security and copyright protection are becoming important issues in multimedia applications and services. Watermarking techniques have been proposed for these purposes in which the copyright information is embedded into multimedia data in order to protect the ownership. Although Watermarking provides a feasible solution for security, it still faces many challenges, as dealing with real time data is quite a demanding task. The proposed architecture uses DCT algorithm for embedding an image in a video. Invisible watermarks give fruitful results by securing the video and provide copyright protection. IDCT is then applied for extracting an image from video. The comparison between the images gives the end user relief from video tampering problem.

Index Terms— Digital Video Watermarking, Discrete Cosine Transform, Discrete Frequency Transform, Discrete Wavelet Transform, Frequency Domain ,Pixel Permutation, Shot Segmentation, Spatial Domain.

1 INTRODUCTION

IN recent year transfer of digital data has become the need of an hour. As the technology has changed its form, data in form of text and images was not sufficient to reflect the changing need. Digital data in form of video, audio is required in many fields. As the data is transmitted over a huge network, there is prominent need for protection of transmitted data against unauthorised access and unauthorised copy. Security in form of Watermarking provides owner authentication and thereby providing security to the transmitted data. Digital watermarking is a new technology used for copyright protection of digital media.

Digital watermarking was introduced at the end of the 20 century to provide means of enforcing copyright protection of digital data. Where, ownership information data called watermark is embedded into the digital media (image, audio, and video) without affecting its perceptual quality. In case of any dispute, the watermark data can be detected or extracted from the media and used as a proof of ownership

2 VIDEO WATERMARKING TECHNIQUES

Watermarking techniques can be broadly classified into two categories. They are spatial domain watermarking and frequency domain watermarking. Both have their own advantages and disadvantages. Majority of the present day watermarking techniques make use of the frequency domain. This is due to high robustness and ease of compression when compared to spatial domain.Watermarking a video is relatively a difficult task as compared to images. Image watermarks are easy to deal and embed. Image watermarking may not face as such a bigger problem as compared to video watermarking. So technique used for video watermarking must deal and consider all the required parameters for efficient and reliable video transfer. Accordingly the techniques are classified dealing with all the parameters.

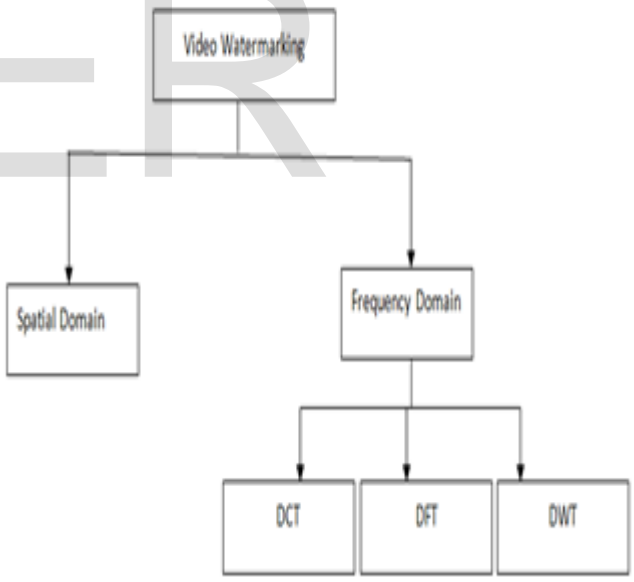

Fig 1.Watermarking Techniques

2.1 SPATIAL DOMAIN

The spatial domain is watermarking where embedding and detection of watermark is performed by directly manipulating the pixel intensity values of the video frame. Conventional Spatial domain watermarking is generally not in use due to its least reliability. In the spatial domain, pixels in randomly selected regions of the image are modified according to the signature or logo desired by the author of the product. This

method is as simple as modifying the pixel values of the original image where the watermark should be embedded [1].

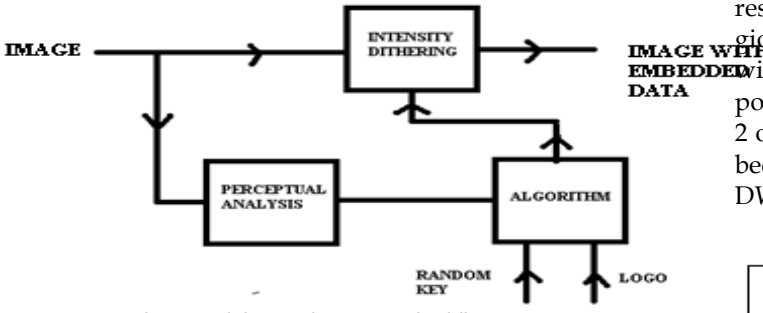

Fig.2 Spatial Domain Data Embedding System

Randomly selected image data are dithered by a small amount according to a predefined algorithm which may vary in complexity in practical systems. The algorithm defines the intensity and the position of the watermark on the original image. One of the major disadvantages of the conventional watermarking is that it can be easily extracted from the original image which makes this technique unsuitable for copyright authentication [1].

There are three factors that determine the parameters of the algorithm that is used in the spatial domain watermarking. The three factors are:

• The information associated with the signature-The signature is the watermark that we embed on the original image. The information of the signature is closely related to the size and quality of the signature.

• The secret random key- The secret key may be included in the process of watermarking to improve the security during transmission. If a key is also included, only the receiver who knows the key can extract the watermark and not any intruders.

• The masking property of the image- The masking property of the image is also related to the quality and composition of the image which signifies the clarity of the watermark on the original image.

2.2 FREQUENCY DOMAIN

2.2.1 Discrete Wavelet Transform (DWT)

DWT is more computationally efficient than other transform methods because of its excellent localization properties which provide the compatibility with the Human Visual System (HVS).

The DWT is used in a wide variety of signal processing applications. 2-D discrete wavelet transform (DWT) decomposes an image or a video frame into sub images, 3 details and 1 approximation. The approximation sub image is lower resolution approximation image (LL) however the details sub images are horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to compute multiple "scale" wavelet decomposition. The main advantage of the wavelet transform is its compatibility with a model aspect of the HVS as compared to the FFT or DCT.

This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive, such as the high resolution detail bands. Embedding watermarks in these regions allow us to increase the robustness of our watermark without any visible impact on the image quality. In the proposed algorithm, sub-bands LL and HH from resolution level 2 of the wavelet transform of the frame are chosen for the embedding process. The following figure shows the selected DWT bands.

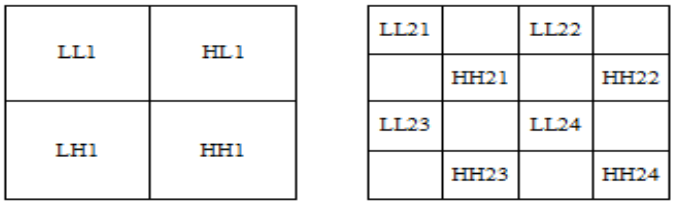

Fig.3 The model for DWT Composition

Embedding the watermark in low frequencies obtained by wavelet decomposition increases the robustness against attacks like filtering, lossy compression and geometric distortions while making the scheme more sensitive to contrast adjustment, gamma correction, and histogram equalization. Embedding the watermark in high frequency sub-bands makes the watermark more imperceptible while embedding in low frequencies makes it more robust against a variety of attacks [1].

2.2.2 Discrete Cosine Transform (DCT)

Discrete cosine transform is a process which converts a sequence of data points in the spatial domain to a sum of sine and cosine waveforms with different amplitudes in the frequency domain. The DCT is a linear transform, which maps a n-dimensional vector to set of n coefficients. A linear combination of n known basis vectors weighted with the n coefficients will result in the original vector.

The difference between DCT and DFT is that DFT applies to complex numbers, while DCT uses just real numbers. For real input data with even symmetry DCT and DFT are equivalent. There are eight different variants of DCT. There is a very slight modification between these eight variants. In JPEG compression the input data are two-dimensional, presented in 8x8 blocks. There's a need of using two-dimensional DCT. Since each dimension can be handled separately, the two-dimensional DCT follows straightforward form the one-dimensional DCT. A one-dimensional DCT is performed along the rows and then along the columns, or vice versa [3].

The watermark embedding approach is designed to be performed in the DCT domain. This holds several advantages. DCT is used in the most popular stills and video compression formats, including JPEG, MPEG, and H.26x. This allows the integration of both watermarking and compression into a single system.

Another advantage of this approach is that in image or video

compression the image or frames are first divided into 8 × 8 blocks. By embedding the WM specifically to each 8×8 block, tamper localization and better detection ratios are achieved.
Each of the video frames undergoes 8 × 8 blocks DCT and quantization. Then, they are passed to the watermark embedding module. The watermark generation unit produces a specific watermark data for each video frame, based on initial predefined secret keys. The watermark embedding module inserts the watermark data into the quantized DCT coefficients for each video frame according to the algorithm detailed below. Finally, watermarked DCT coefficients of each video frame are encoded by the video compression unit which outputs the compressed frame with embedded authenticationWatermark data.

2.2.3 Discrete Fourier Transform (DFT)

This approach first extracts the brightness of the to-be-marked frame, computing its full-frame DFT and then taking the magnitude of the coefficients. The watermark is composed of two alphanumerical strings. The DFT coefficient is altered, then IDFT. Only the first frame of each Group of Pictures (GOP) is watermarked, which was composed of twelve frames, leaving the other ones uncorrupted. It is good robustness to the usual image processing as linear/non-linear filtering, sharpening, JPEG compression and resist to geometric transformations as scaling, rotation and cropping [2].

3 PROPOSED SCHEME

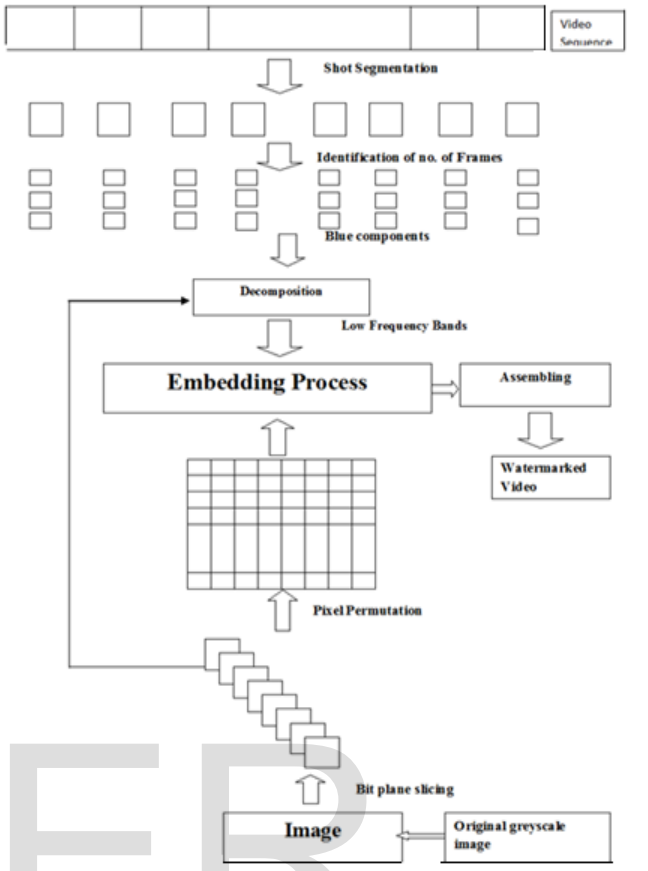

Fig.4 Proposed Architecture of Video Watermarking

The efficiency of the video watermarking technique is achieved with the aid of the following two major steps [3].
1) Watermark Embedding process
2) Watermark Extraction process

Before embedding watermark pixels into the input video sequences, the following process should carry out to enhance the security of the hiding information as well as to improve the efficiency of our proposed approach. The process includes:
1) Shot segmentation of video sequences
2) Bit plane slicing of a gray scale image
3) Pixel permutation
4) Decomposition of an image using DCT

1. Shot segmentation of video sequence

The original input video sequence is first segmented into non-overlapping units, called shots that depict different actions. Each shot is characterized by no significant changes in its content which is determined by the background and the objects present in the scene. Here, we have used Discrete Cosine Transform and correlation measure to identify the number of frames involved in each shot. At first, the first and second

frame is divided into a set of blocks of sizes and DCT is applied to every block of the frame.

2. Bit plane slicing of a grayscale image

Bit-Plane Slicing is a technique in which the image is sliced at different planes. Imagine the image is composed of 8 bits, 1-bit planes ranging from bit plane1-0 (LSB) to bit plane 7 (MSB). In terms of 8-bits bytes, plane 0 contains all lowest order bits in the bytes comprising the pixels in the image and plane 7 contains all high order bits. The high-order bits usually contain most of the significant visual information and the lower-order bits contain subtle details. The advantage of doing this method is to get the relative importance played by each bit of the image.

3. Pixel permutation

After the bit plane slicing process, the sliced images are allowed to permute each pixel value to enhance the security of the hiding information. In this scheme, each group of pixels is taken from the image. The pixels in the group are permuted using the key selected from the set of keys.

4. Decomposition of an image

Using DCT Like other transforms, the Discrete Cosine Transform (DCT) attempts to de-correlate the image data. After decorrelation each transform coefficient can be encoded independently without losing compression efficiency.

4 CHALLENGES AND ATTACKS

4.1 Multiple Watermarking

An attacker may watermark an already watermarked object and later make claims of ownership.

4.2 Cropping

In this attack, attacker may interest in only some part of image or a frame of video.

4.3 Additive Attack

In this attack, attacker inserts his own watermark W on images that completely overrides the original watermark which is not identified by the owner also.

4.4 Subtractive Attack

In this attack, the unauthorized user tries to find the location of the watermark and tries to extract it from host. An effective subtractive attack is one where the cropped object has retained enough original content to still be of value.

4.5 Statistical Averaging

An attacker may try to estimate the watermark and then 'unwater mark' the object by subtracting the estimate. This is dangerous if the watermark does not depend substantially on the data.

5 COMPARATIVE STUDY OF VIDEO WATERMARKING TECHNIQUES

TABLE 1

Performance analysis of different video

Parameters / *Technique*	*Robustness*	*Imperceptibility*	*Fragility*	*PSNR*	
DCT	*Good*	*Acceptable*	*Poor*	*Acceptable*	
DFT	*Acceptable*	*Good*	*Acceptable*	*Acceptable*	
DWT	*Good*	*Good*	*Acceptable*	*Good*	

REFERENCES

[1] Nisreen I Yassin, Nancy 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.

[2] Rajesh Kannan Megalingam, Mithun Muralidharan Nair, Rahul Srikumar, Venkat Krishnan Balasubramanian and VineethSarmaVenugopalaSarma,"A Comparative Study on Performance of Novel, Robust Spatial Domain Digital Image Watermarking with DCT Based Watermarking", International Journal of Computer Theory and Engineering, Vol. 2, No. 4, August, 2010.

[3] Palaiyappan, Raja JeyaSekhar, "A Block Based Novel Digital Video Watermarking Scheme Using DCT", IOSR Journal of Electronics and Communication Engineering, Volume 5, Issue 2 (Mar. - Apr. 2013) PP 34-44.

[4] Kareem Ahmed, Ibrahim El-Henawy and Ahmed Atwan, "Novel DWT video watermarking schema", Machine Graphics & Vision Internatio al Journal archive, Vol. 18, No. 3, pp. 363-380, 2009.12

[5] Patrick Bas and Teddy Furon, "A New Measure of Watermarking Sec rity: The Effective Key Length", IEEE Transactions on information forensics and security, Vol. 8, NO. 8, August 2013.

[6] Xiaoyu Feng, Hongting Zhang, Hsiao-Chun Wu, "Xiaoyu Feng, Hongting

Zhang, Hsiao-Chun Wu", IEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 10, OCTOBER 2011.

[7] Narges Ahmidi and Reza Safabakhsh, "A Novel DCT-based Approach for Secure Color Image Watermarking", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04).

[8] Yan Liua and Jiying Zhao ," A new video watermarking algorithm based on 1D DFT and Radon transform ",Signal Processing, Vol. 90, No. 2, pp. 626-639, 2010.13.