International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 2– No.6, May 2012 – www.ijais.org

DCT and Thresholding based Digital Video Watermarking

Naginder Kaur
Student,
Department of Electronics and Communication,
Lovely Professional University,
Jalandhar, India

Manie Kansal
Assistant Professor,
Department of Electronics and Communication,
Lovely Professional University,
Jalandhar,India

Gursharanjeet Singh
Assistant Professor,
Department of Electronics and Communication,
Lovely Professional University,
Jalandhar,India

ABSTRACT

A DCT based video watermarking technique is proposed in this paper. Digital media offer several distinct advantages over analog media ,such as high quality ,easy editing ,high fidelity copying. The ease by which a digital information can be duplicated and distributed has led to the need for effective copyright protection tools. Watermarking is used to hide the secret data such as the private message or the copyright into a meaningful host image to distract the attention of the observers. The watermark is inserted into the video in the frequency domain to achieve the better results and robustness of the hiding data.

Keywords

DCT, HVS, PSNR.

1. INTRODUCTION

Internet is a public transmission way and it is widely applied in many applications, of different fields we can send and receive digital data, such as images, text ,videos by connected networks, with the recent growth of communication technologies. To conceal data in transmitting message for preventing the illegal copying or to protect the secret is very important [1].With the rapid development of multimedia and computer technology, images, audio and video can be more easily produced, processed as well as stored by digital devices in recent years. Meanwhile, the high speed advancement of digital communication network has brought digitalization and networking for information release and transmission. Internet has become an ideal distribution system for digital media [2].Information network technology was widely used all over the world and it was greatly convenient for resource sharing and exchange between people. However, many new issues such as security of digital information transmission and copyright protection of digital products also emerge in the meantime. How to prevent digital products from copyright infringement, piracy and alteration without permission have become many nations' concerns needing to be resolved urgently.

2. DIGITAL WATERMARKING

Digital watermarking technology is an emerging field in cryptography, signal processing and communications. Digital Watermarking is intended by its developers as the solution to the need to provide value added protection on top of data encryption and scrambling for content protection. It is a technology being developed to ensure security and protection of multimedia data [4]. The purpose of digital watermarking is not to restrict use of multimedia resources, but rather to facilitate data authentication and copyright protection. Watermarking techniques embed information in images by introducing changes that are imperceptible to the human eye but recoverable by a computer program. Data encryption and information hiding schemes are developed to protect the secret data. Data encryption methods make the secret data into meaningless bits. Watermarking methods are based on the human visual system in which it cannot be recognized due to tiny difference. In addition, numeric watermark has great application value upon areas like identification of truth and falsehood, communication concealing, sign hiding, and etc. Watermarking techniques embed information in images by introducing changes that are imperceptible to the human eye but recoverable by a computer program. Generally, the locations in which the watermark is embedded are determined by a secret key. Doing so prevents possible pirates from easily removing the watermark. Furthermore it should be possible to recover the watermark from an altered image. Possible alterations of watermarked images include compression, filtering and cropping. These alterations are referred to as attacks. The basic components of any watermarking technique consist of a marking algorithm that inserts information, the Watermark, into an image. The watermark is inserted into the image in the spatial domain or spatial frequency domain. As part of the watermarking technique, a testing algorithm must be defined that tests an image to see if a particular watermark is contained in the image.

3. GENERAL REQUIREMENTS OF WATERMARKING

Each watermarking application has its own specific requirements. Therefore there is no universal set of requirements as such that must be met by all watermarking techniques [5]. There are some requirements mentioned below for watermarking techniques:-

3.1 Imperceptibility

There should be perceptual similarity between the original and the watermarked version of the cover work. From this perspective, the watermark system exploits the imperfect of human eyes. However, for some watermarking system, the watermarks are made to be visible on purpose.

3.2 Robustness

The watermark must be detectable after a seris of attacks on it. It must be robust enough to withstand all kinds for signal processing operations, "attacks" or unauthorized access.

3.3 Transparency

The most fundamental requirement for any Watermarking method shall be such that it is transparent to the end user. The watermarked content should be consumable at the intended user device without giving annoyance to the user. Watermark only shows up at the watermark-detector device.

3.4 Security

Watermark information shall only be accessible to the authorized parties. Only authorized parties shall be able to alter the Watermark content. Encryption can be used to prevent unauthorized access of the watermarked data.

3.5 Data capacity

The number of bits a watermarking scheme encodes within a unit of time or within a work. Different applications require different data capacities, e.g. 4-8 bits for a 5-minutes video of copy control, longer messages for broadcast monitoring.

4. TYPES OF DIGITAL WATERMARKING

Watermarking techniques can be divided into various categories in various ways. The watermarks can be applied in spatial domain. An alternative to spatial domain watermarking is frequency domain watermarking [3]. It has been pointed out that the frequency domain methods are more robust than the spatial domain techniques. Visible watermark is a secondary translucent overlaid into the primary image. The watermark appears visible to a casual viewer on a careful inspection. The invisible-robust watermark is embed in such a way that alternations made to the pixel value is perceptually not noticed and it can be recovered only with appropriate decoding mechanism. The invisible-fragile watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark. An invisible robust private watermarking scheme requires the original or reference image for watermark detection; whereas the public watermarks do not. The class of invisible robust watermarking schemes that can be attacked by creating a counterfeit original is called invertible watermarking scheme.

Source-based watermark are desirable for ownership identification or authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed. A source-based watermark could be used for authentication and to determine whether a received image or other electronic data has been tampered with. The watermark could also be destination based where each distributed copy gets a unique watermark identifying the particular buyer. The destination -based watermark could be used to trace the buyer in the case of illegal reselling. According to the differences in capacities of thwarting attacks, digital watermarking can be classified into robust watermarking, semi-fragile watermarking and fragile watermarking. Robust watermarking is quite robust to modification and mainly used to protect intellectual property of digital products. Semi-fragile watermarking is partly robust, but it’s only fragile to intended tampering. Fragile watermarking, which is fragile to each kind of modification, is mainly used for authentication of integrity and reliability of digital products.

5. VIDEO WATERMARKING

Digital video watermarking is the technology that watermark information, such as copyright symbol, is embedded in the video. The processes of digital video watermarking system include watermark generation and embedding and detection and extraction. . The clarity of the video depends upon the number of frames present in it. If there is greater number of frames in the video then video will be clearer. Digital video watermarking can be achieved by either applying still image technologies to each frame of the movie or using dedicated methods that exploit inherent features of the video sequence. There are different embedding strategies used to make the algorithm more robust either a different watermark is inserted in each video frame or the same watermark is embedded in all the video frames. In this algorithm there is embedding of same watermark in every frame of the video as shown in figure 1.

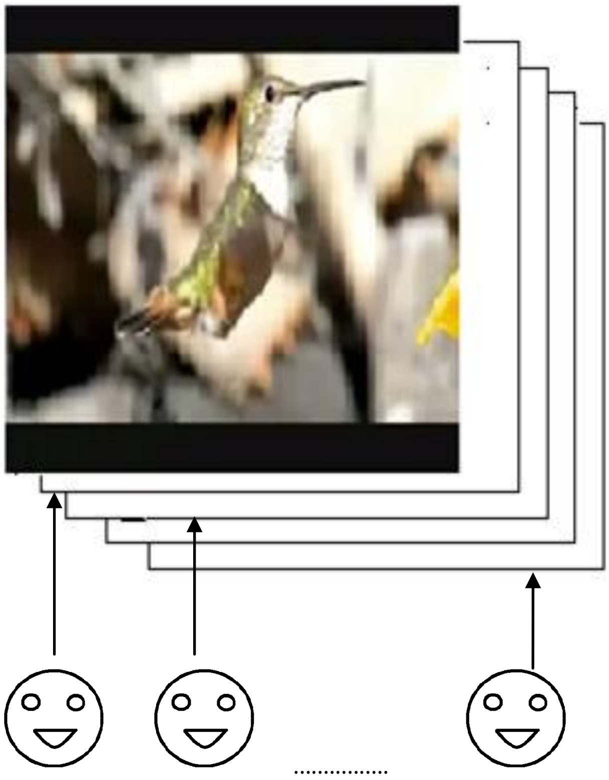


Figure 1:Embedding of same watermark in each frame of the video

5.1 Embedding Process

Watermarking on digital video is mostly considered today as watermarking a sequence of still images .The frames of video can be extracted and apply the embedding in each frame of the video by using different algorithm and again frames combined in the form of video results as watermarked video.

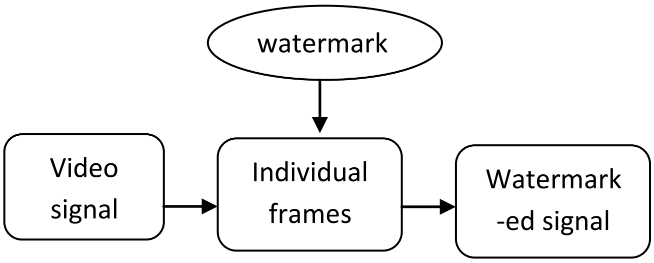


Figure 2: Video watermark insertion

The steps of embedding the watermark are as follows.

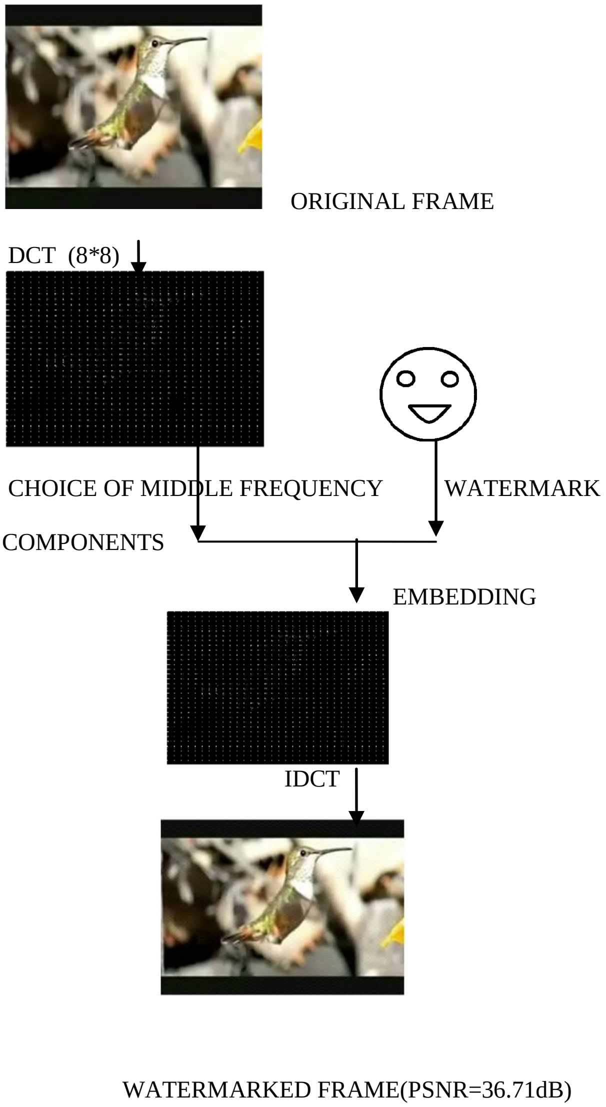


Figure 3: Watermark insertion on one frame of video

Steps followed:

1. The video signal is converted in to number of frames.
2. Take the first frame and extract the luminance part of the frame.
3. Divide the luminance part of the frame in to 8*8 blocks and two-dimensional DCT is applied to the first block.
4. For embedding take the threshold value ‘a’ from -0.10 to 0.10. if the value of watermark pixel is 1 then embedd 0.10 otherwise -0.10 on the position where we want to embedd.
5. Move to the next block and repeat the procedure.
6. Perform Inverse DCT to have the final watermarked frame.
7. The next frame is taken and step 2 to 6 are repeated until the last frame comes.
8. All the watermarked frames are combined to make the watermarked video.

5.2 Performance Evaluation

MSE: Mean square error (MSE) is one of the simplest methods to measure the distortion. For one 256*256 block, MSE can be calculated using the following formula:

$$MSE=1/M*N \sum\sum\{(f(x,y)-f'(x,y))^2\} \qquad (1)$$

where f(x, y) is original frame of the video and f’(x, y) is watermarked frmae of video.

PSNR: Peak signal to noise ratio (PSNR) is also used to measure the distortion, it is calculated as:

$$PSNR= 10.\log[R^2/MSE] \qquad (2)$$

MSE is root mean square error and R is the maximum fluctuation in the input image data type. PSNR provides an overall evaluation of the difference between watermarked and host image.

Table 1. Values of PSNR in each frame

Frame no.	PSNR (dB)
1	36.71
2	36.76
3	36.85
4	36.77
5	36.77
6	36.80
7	36.82
8	36.76

5.3 Extraction Process

The steps of proposed watermark extracting algorithm are very similar to that of watermark embedding.

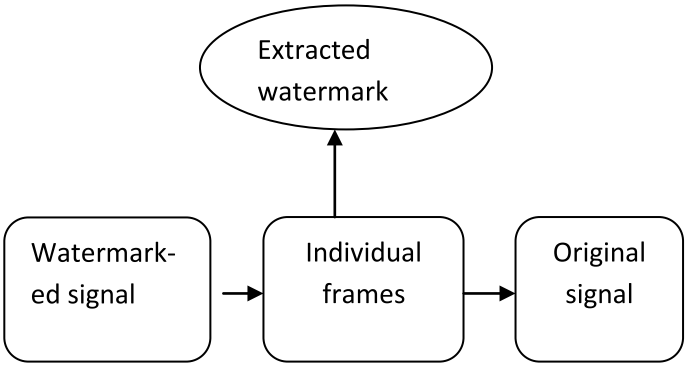
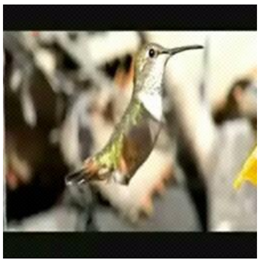


Figure 4: Video watermark extraction

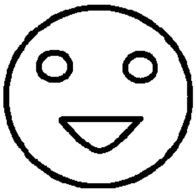
The steps for watermark extraction are briefly listed as follows.

1. The watermarked video is converted into the number of frames.
2. Take the first frame and extract the luminance part of the frame.

3. Divide the luminance part of the frame in to 8*8 blocks and two-dimensional DCT is applied to the first block.
4. Take the zero matrix of 32*32.
5. The pixel value of frame on which we embed the watermark If the value is greater than or equal to 0 then print 1 on the zero matrix otherwise 0.
6. Move to the next block and repeat the procedure.
7. Perform Inverse DCT to have the final frame.
8. The next frame is taken and steps 2 to 6 are repeated until the last frame comes.



(a)



(b)

Figure 5: (a) Watermarked picture(of 1 frame) with PSNR=36.71dB and (b) is the extracted watermark with NC=1

6. CHALLENGES FOR VIDEO WATER-MARKING

Video media is susceptible to increased attacks than any other media and sensitive to subjective quality and Watermarking may degrade the Quality. Video compression algorithms are computationally intensive and hence there is less headroom for Watermarking computation. Video is bandwidth hungry so it is mostly carried in compressed domain. Therefore, Watermarking algorithm shall be adaptable for compress domain processing. For low-bit rate video, Watermarking poses additional challenges, as there is less room for watermark data. During video transmission, frame drops are very usual. If watermark data spreads over many frames, in case of frame drops, watermark data may become irretrievable. Watermarking should be robust enough against this phenomenon.

7. ATTACKS ON VIDEO WATERMARKING

A watermarked image is likely to be subjected to certain manipulations, some intentional such as compression and transmission noise and some intentional such as cropping, **filtering**, etc.

7.1 Lossy Compression

Lossy compression is a data encoding method that compresses data by discarding (losing) some of it. The procedure aims to minimize the amount of data that need to be held, handled, and/or transmitted by a computer. Many compression schemes like JPEG and MPEG can potentially degrade the data's quality through irretrievable loss of data.

7.2 Geometric distortions

Geometric distortions are specific to images videos and include such operations as rotation, translation, scaling and cropping.

7.3 Common signal processing operations

Common signal processing include the followings.

- D/A conversion
- A/D conversion
- Resampling
- Requantization
- Dithering distortion
- Recompression
- filtering

8. CONCLUSION

This paper presented robust video watermarking method based on DCT transform. The watermarking research is progressing very fast and numerous researcher from various fields are focussing to develop some workable scheme. Transform domain method is attracting more and more concern for its characteristics. The advantages of transform domain over space domain that the majority of signal processing operations can be well explained and a lot of good visual models are established in the transform domain .The methods of embedding and extracting of watermark in individual frames is quite simple.

9. REFERENCES

[1] Jiun-Jian Liaw, Lin-Huang Chang, Yu-Sheng Liao, “An Improvement of Robust and Blind Data Hiding Based on Self Reference in Spatial Domain” International Conference on Computer Engineering and Applications, 2007.

[2] Yigang Zhou Jia Liu, “Blind Watermarking Algorithm Based on DCT for Color Images” , 2009.

[3] Deng Jianghua, “Color Image Digital Watermarking Algorithm Based on Singular Value Decomposition”, International Conference on Multimedia Information Networking and Security,2009.

[4] Saraju P. Mohanty, “Digital Watermarking”, Indian Institute of Science, Bangalore,1999.

[5] Ajay Goel, O.P. Sahu, Rupesh Gupta, Sheifali Gupta,“Improved Digital Watermarking Techniques and Data Embedding In Multimedia”, International Journal on Computer Science and Engineering, 2010.

[6] Xianyi Cheng, Liu Ding, Fei Gao, “Adaptive Robust Watermarking Algorithm Based On Dct-Domain”,2009.

[7] Ruiling Zhu, Xin Wang, “Efficient Digital Watermarking in DCT Domain”, International Forum on Information Technology and Applications,2009.

[8] Yixin Yan, Wei Cao, Shengming Li, “Block based Adaptive Image Watermarking Scheme using Just Noticeable Difference ”, International Workshop on Imaging Systems and Techniques, 2009.