

Comparison of Watermarking in Compressed Digital Video using DCT, DWT and FFT

Digvita Karekar

ETC Department, Goa, India

Abstract: Digital technologies is showing wide growth and advancements in image transmission and processing during the last few years. The image security during image transmission is one of the important areas for research. The watermark can efficiently reduce the potential danger of forgery or alteration. Robustness against many attacks with a wide range of changes is achieved. Various digital watermarking techniques are nowadays become popular for image security and copyright. But, due the rapid growth of the Internet and the development of digital multimedia technologies, illegal copying, modifying and copyright protection have become an important issues. Hence, there is a need for development of technique which will able to face these issues. There are various techniques to produce the watermark in digital images. In this paper DCT, DWT and FFT along with LSB techniques has been used for watermarking. And also we implement the h264/av cen codec in our process for transmission. The performance parameter like PSNR, is used to evaluate the watermarking performance. The experimental results are shown in this paper for various methods.

Keywords: video watermarking, DCT, FFT

1. Introduction

Image processing is any form of signal processing for which the input is an image, such as a photograph or video frame. The output of image processing may be either an image or a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. Image processing usually refers to digital image processing.

A typical video codec works by breaking the picture into discrete blocks (8×8 pixels in the case of MPEG). These blocks can then be subjected to discrete cosine transform (DCT) to calculate the frequency components, both horizontally and vertically. The resulting block is then pre-multiplied by the quantization scale code and divided element-wise by the quantization matrix, and rounding each resultant element. After decryption, however, the data are no longer protected. Watermarking, which directly embeds owner identification into the digital contents, plays a representative role in content protection and securing owner's right. Since the embedded watermark remains in the contents after the decryption of received data it should be reliable, invisible, unambiguous and difficult to be removed without significantly degrading the perceived quality of video. The embedded watermark should also survive both intentional and unintentional attacks such as image filtering. In particular, digital video is distributed in the compressed format such as MPEG or H.264. Therefore an embedded watermark must be robust to video coding processes. In this paper we present algorithms for image authentication and forgery prevention known as watermarks. Figure 1 shows the block diagram for watermarking digital images.

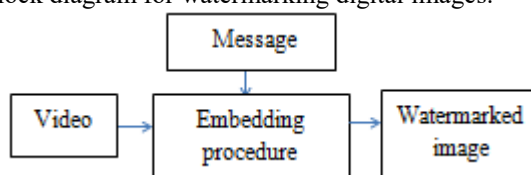


Figure 1: Block Diagram of Watermarking Algorithm

2. Related Work

Discrete Cosine Transform (DCT)

A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG) (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical for compression, since it turns out (as described below) that fewer cosine functions are needed to approximate a typical signal, whereas for differential equations the cosines express a particular choice of boundary conditions.

In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common.

The most common variant of discrete cosine transform is the type-II DCT, which is often called simply "the DCT", [1][2] its inverse, the type-III DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT". Two related transforms are the discrete sine transform (DST), which is equivalent to a DFT of real and odd functions, and the modified discrete cosine transform (MDCT), which is based on a DCT of overlapping data.

Least Significant Bit (LSB):

In another paper, where is the Image Watermarking Using Least Significant Bit (LSB). The simplest algorithm is Least Significant Bit (LSB) Insertion in which each 8-bit pixel's least significant bit is overwritten with a bit from the watermark. In a digital image, information can be inserted

directly into every bit of image information Two techniques were presented to hide data in the spatial domain of images by them. These methods were based on the pixel value's Least Significant Bit (LSB) modifications

3. Proposed Watermarking Scheme

Discrete Wavelet Transform (DWT)

In the above scenario, the multimedia data, D which is often referred to as the host data, is transformed into some other invertible domain. Typically this is the frequency domain, so the transform is a Fourier or discrete wavelet transform. The message M is also transformed or encoded. In the case of spread-spectrum signaling, the message is encoded by a spreading function. After the embedding, explored further in figures 2 and 3, the inverse transform is applied to produce the watermarked data, $D W$. The channel noise was modelled in early versions of watermarking as additive white Gaussian, but more recent efforts use a more general non-linear distortion or attack noise model. This noise modelling is one of the active areas of research in watermarking, but its mitigation is very dependent on the features of a particular watermarking algorithm and individual image statistics, and is beyond the scope of this paper. Like the traditional channel model, the detection or extraction process typically involves matched filtering or a correlation. When the spreading and de-spreading functions use different keys, the watermark is referred to as having a non-symmetric key.

Fast Fourier Transform (FFT)

A fast Fourier transform (FFT) computes the discrete Fourier transform (DFT) of a sequence, or its inverse. Fourier analysis converts a signal from its original domain (often time or space) to a representation in the frequency domain and vice versa. An FFT rapidly computes such transformations by factorizing the DFT matrix into a product of sparse (mostly zero) factors.

In complex notation, the time and frequency domains each contain one signal made up of N complex points. Each of these complex points is composed of two numbers, the real part and the imaginary part. For example, when we talk about complex sample X , it refers to the combination of ReX and ImX . In other words, each complex variable holds two numbers. When two complex variables are multiplied, the four individual components must be combined to form the two components of the product The following discussion on "How the FFT works" uses this jargon of complex notation. That is, the singular terms: signal, point, sample, and value, refer to the combination of the real part and the imaginary part.

The FFT operates by decomposing an N point time domain signal into N time domain signals each composed of a single point. The second step is to calculate the N frequency spectra corresponding to these N time domain signals. Lastly, the N spectra are synthesized into a single frequency spectrum.

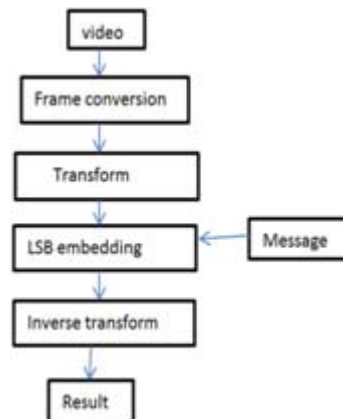


Figure 2: Encoding of watermarked video

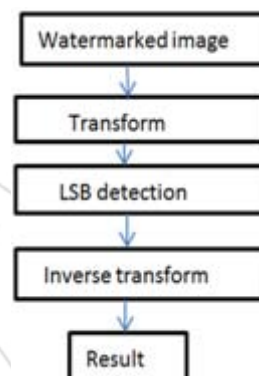


Figure 3: Decoding of watermarked video

4. Experimental Results and Analysis



Figure 4: Original video

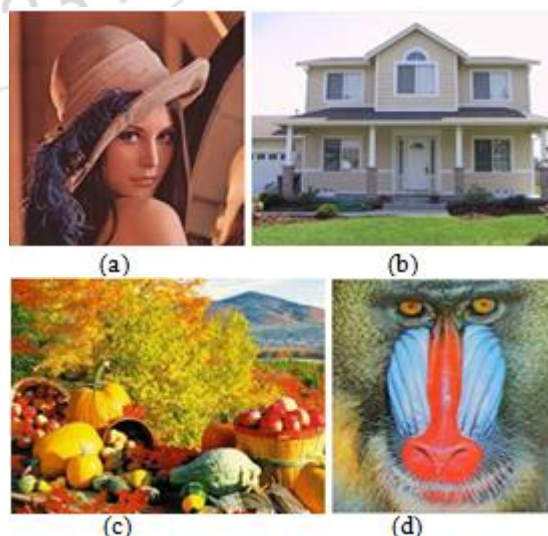


Figure 5: Message images

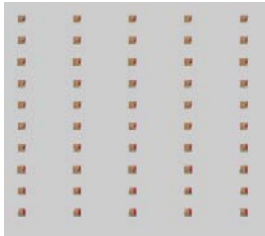


Figure 6: Frame conversion of video



Figure 7: Selected cover frame



Figure 8: 4 bit image to hide



Figure 9: watermark image(a)blue(b) green(c) red



Figure 10: Watermarked image



Figure 11: Watermarked video



Figure 12: Decoded image



Figure 13: Extracted image (a)blue(b) green(c) red



Figure 14: Reconstructed image

Table 1: Comparison of psnr between DCT, DWT and FFT

Video	Message	DCT	DWT	FFT
a	a	23.008	60.9058	41.6337
a	b	22.7989	38.9134	45.0713
b	c	22.8791	54.0975	36.6065
b	d	22.9237	43.5819	51.1514

5. Conclusion

In this paper we propose the new technique of watermarking in video domain. For video watermarking initially we separate the frames from the video. The content-based cryptography to the watermarking system increases the security of the system. The coding and encoding routines of the video codec are combined with embedding and extraction of water marks, to design efficient and low-complexity method. The MBs' and frames' indices are embedded into DCT value of the blocks for transparency to the human visual system. The suggested authentication method provides detection of spatial, temporal, and spatio temporal tampering. The experimental results show that the distortion caused by our system is very low on average. H.264 is an industry standard for video compression, the process of converting digital video into a format that takes up less capacity when it is stored or transmitted. Here we propose the novel implementation in watermark detection. In video we embedding the information with help of the

DWT, FFT along with LSB. Finally the video will be encoded with the h264 encoding

References

- [1] **"Tampering Detection in Compressed Digital Video Using Watermarking"** Mehdi Fallahpour, Shervin Shirmoham madi, Senior Member, IEEE, Mehdi Semsarzadeh, and Jiying Zhao, Member, IEEE, 2014
- [2] **"Complete Video Quality-Preserving Data Hiding"** KokSheik Wong, Student Member, IEEE, Kiyoshi Tanaka, Member, IEEE, Koichi Takagi, and Yasuyuki Nakajima, Member, IEEE, 2009
- [3] **"A Novel Block based Video in Video Watermarking Algorithm using Discrete Wavelet Transform and Singular Value Decomposition"** L. Agilandeeswari [1] K. Muralibabu [2] School of Information Technology & Engineering, HOD / Department of ECE, VIT University, Vellore – 632 014, India. Global Institute of Engineering & Technology, Vellore, India. 2013
- [4] **"A Realtime Spatio-temporal watermarking scheme for H.264/AVC"** Mehdi Fallahpour¹, Mehdi Semsarzadeh¹, Shervin Shirmohammadi^{1,2}, Jiying Zhao¹ School of Electrical Engineering and Computer Science (EECS) in University of Ottawa, Canada² Istanbul Şehir University, Turkey {mfallah | msemsarzadeh | shervin | jyzhao}@site.uottawa.ca
- [5] **"DWT Based Digital Image Watermarking, De-Watermarking & Authentication"** Pravin M. Pithiyal, H.L. Desai² 1PG Student, Department of Electronics & Communication Engineering SPCE, Visnagar, Gujarat, India ²Assistant Prof. Department of Electronics & Communication Engineering SPCE, Visnagar, Gujarat, India
- [6] **"A Blind Video Watermarking Algorithm Resisting to Rotation Attack"** XU Guo-juan CKC software lab, NingBo University NingBo, 315211, China e-mail: xuguojuan1210@163.com WANG Rang-ding CKC software lab, NingBo University NingBo, 315211, China e-mail: wangrangding@nbu.edu.cn
- [7] **"A Noble Reversible Data Embedding Method for Source Authentication and Tamper Detection of H.264/AVC Video"** Sutanu Maiti Department of Computer Science and Engineering National Institute of Technology Karnataka, Surathkal, Indiamaiti.sutanu.cs09@gmail.com Mahendra Pratap Singh Department of Computer Science and Engineering National Institute of Technology Karnataka, Surathkal, India Mps_82@aol.in. 2011
- [8] **"MPEG-2 DIGITAL VIDEO WATERMARKING TECHNIQUE"** Satyendra N. Biswas¹, Sabikun Nahar¹, Sunil R. Das², 3, Emil M. Petriu³, Mansour H. Assaf⁴, and Voicu Groza³ ¹School of Engineering and Computer Science Independent University, Dhaka 1329, Bangladesh ²Department of Computer Science, College of Arts and Sciences Troy University, Montgomery, AL 36103 USA ³School of Information Technology and Engineering, Faculty of Engineering University of Ottawa, Ottawa, ON K1N 6N5, Canada ⁴Faculty of Science and Technology University of South Pacific, Suva, Fiji. 2012
- [9] **"Chaotic Watermarking for Video Authentication in Surveillance Applications"** Siyue Chen and Henry Leung IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 18, NO. 5, MAY 2008
- [10] **"Digital image processing"** by Rafael c. Gonzalez and Richard e. woods 3 edition
- [11] **"Analysis and Design of Secure Watermark-Based Authentication Systems"** Chuhong Fei, Student Member, IEEE, Deepa Kundur, Senior Member, IEEE, and Raymond H. Kwong, Member, IEEE
- [12] P.-C. Su, C.-S. Wu, I.-F. Chen, C.-Y. Wu, and Y.-C. Wu, **"A practical design of digital video watermarking in H.264/AVC for content authentication,"** Signal Process, Image Commun., vol. 26, nos. 8–9, pp. 413–426, Oct. 2011.
- [13] S. Chen and H. Leung, **"Chaotic watermarking for video authentication in surveillance applications,"** IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 5, pp. 704–709, May 2008.