International Journal of Image Processing and Vision Science

Volume 1 | Issue 2 Article 3

October 2012

# REAL-TIME VIDEO WATERMARKING FOR COPYRIGHT PROTECTION BASED ON HUMAN PERCEPTION

B. SUMANA PRIYANKA
*Bharat Institute of Engineering and Technlogy, Hyderabad*, sp20.mtech@gmail.com

N. SAGAR
*Bharat Institute of Engineering and Technlogy, Hyderabad*, snayakanti@gmail.com



Recommended Citation
PRIYANKA, B. SUMANA and SAGAR, N. (2012) "REAL-TIME VIDEO WATERMARKING FOR COPYRIGHT PROTECTION BASED ON HUMAN PERCEPTION," *International Journal of Image Processing and Vision Science*: Vol. 1 : Iss. 2 , Article 3.
DOI: 10.47893/IJIPVS.2012.1015
Available at: https://www.interscience.in/ijipvs/vol1/iss2/3

# REAL-TIME VIDEO WATERMARKING FOR COPYRIGHT PROTECTION BASED ON HUMAN PERCEPTION

**B.SUMANA PRIYANKA**
M.Tech in Embedded systems
Bharat Institute of Engineering and Technlogy, Hyderabad
Email: sp20.mtech@gmail.com

**N.SAGAR**
M.Tech in Embedded systems
Bharat Institute of Engineering and Technlogy, Hyderabad
Email: snayakanti@gmail.com

***Abstract*— There is a need for real-time copyright logo insertion in emerging applications, such as Internet protocol television (IPTV). This situation arises in IP-TV and digital TV broadcasting when video residing in a server has to be broadcast by different stations and under different broadcasting rights. Embedded systems that are involved in broadcasting need to have embedded copyright protection. Existing works are targeted towards invisible watermarking, not useful for logo insertion. MPEG-4 is the mainstream exchangeable video format in the Internet today because it has higher and flexible compression rate, lower bit rate, and higher efficiency while superior visual quality.**

**The main steps for MPEG-4 are color space conversion and sampling, DCT and its inverse (IDCT), quantization, zigzag scanning, motion estimation, and entropy coding. In this work a watermarking algorithm that performs the broadcaster's logo insertion as watermark in the DCT domain is been presented. The robustness of DCT watermarking arises from the fact that if an attack tries to remove watermarking at mid frequencies, it will risk degrading the fidelity of the image\video because some perceptive details are at mid frequencies. The suggested methods has implemented in matlab.**

***Keywords*—** Copyright Protection, IP-TV, MPEG-4, robustness, Watermarking.

## I. INTRODUCTION

The rapid proliferation of multimedia over internet demands sophisticated technique for secure and efficient access to information. There is growing need to discourage unauthorized duplication and use of digital data. With the advent of digital video, issues of copyright protection have become more important, since the duplication of digital video signals does not result in an inherent decrease in quality normally suffered by analog video. Steganography, data hiding, data embedding and watermarking are techniques used for the invisible embedding of information in the host data, with the intent information is stored/transmitted together with the host data retaining secret information.

High speed computer networks, the Internet and the World Wide Web have revolutionized the way in which digital data is distributed. The widespread and easy accesses to multimedia contents and possibility to make unlimited copy without loss of considerable fidelity have motivated the need for digital rights management. Digital watermarking is a technology that can serve this purpose. A watermark is a data embedded in multimedia objects such that the watermark can be detected or extracted at later times in order to make an assertion about the object. Growing popularity of video based applications such as Internet multimedia, wireless video, personal video recorders, video-on-demand, set-top box, videophone and videoconferencing have a demand for much higher compression to meet bandwidth criteria and best video quality as possible. Although the main motivation behind the watermarking is the copyright protection, its applications are not that restricted. By embedding watermarks into commercial advertisements, the advertisements can be monitored whether the advertisements are broadcasted at the correct instants by means of an automated system. The system receives the broadcast and searches these watermarks identifying where and when the advertisement is broadcasted. The same process can also be used for video and sound clips. Musicians and actors may request to ensure that they receive accurate royalties for broadcasts of their performances.

As broadband Internet is widely available, multimedia resources are openly accessed and distributed quickly and widely. From this trend, it is predicted that as more and more music, movies, and images are exchanged on the Internet, download multimedia sales will eventually surpass traditional sales. This development will benefit the multimedia product owners as sales will increase. However, it will also pose challenges to their ownership as most multimedia products are distributed in unsecured formats. This situation is further aggravated by the fact that duplicating digital multimedia products is almost cost-free and fast due to the availability of free or low cost tools. To legal authorities, arbitrating the ownership of multimedia products is not easy, unless a mechanism guarantees the genuine integrity of copyright. For a watermark to be useful it must be perceptually visible or invisible and robust against any possible attack and image processing by those who seek to corsair the material, researchers have considered various approaches like MPEG compression, geometric distortions and noising.

The rest of the paper is organized as follows: In Section II, we discuss about watermarking literature. In Section III, we describe overview of the MPEG-4. In Section IV, We introduce the watermarking algorithm. In Section V, we present the implementation results of both Visible and Invisible watermarking. Finally, in Section VI, conclusions are made.

## II. LITERATURE SURVEY

Before the concept of watermarking can be explored further, three important definitions must first be established. A host signal is a raw digital audio, image, or video signal that will be used to contain a watermark. A watermark itself is loosely defined as a set of data, usually in binary form, that will be stored or transmitted through a host signal. It may be a copyright notice, a secret message, or any other information. Watermarking is the process of embedding the watermark within the host signal which is shown in Fig 1.

Fig 1 Example of a U.S. ten-dollar bill watermark.

### A. TYPES OF WATERMARKING

We have a good decomposition of the variety of watermarks currently available (see Fig 2). One thing to point out of this classification is that video watermarking is an extension of image watermarking, which utilizes characteristics of the Human Visual System (HVS) to embed the watermark. HVS methods take advantage of the way the human eye processes images in order to add watermarks to the images. Watermark processing methods fall into two categories: spatial domain and frequency domain. Spatial domain usually changes the value of the pixels in a minor way so it is not perceived by the human eye and the watermark is scattered through the entire object. Frequency domain watermarking transforms the object into its frequency counterpart and then embeds the watermark in the transform coefficients, distributing the watermark over the entire frequency distribution of the object. The frequency domain watermarking methods are relatively robust to noise, image processing and compression compared with the spatial domain methods. The Discrete Cosine Transform (DCT) methods are the most widely used among these types of methods.

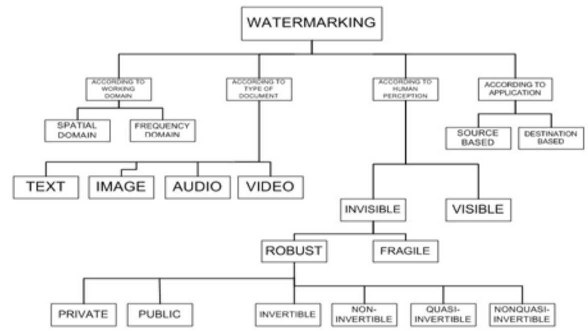



Fig 2 Types of digital watermarking schemes

### B. VIDEO WATERMARKING

Today however, growing popularity of video based applications such as Internet multimedia, wireless videos, personal video recorders, video-on-demand, set-top box, videophone and videoconferencing has increased the demand for a secure distribution of videos which is shown in Fig 3. Apparently any image watermarking technique can be extended to watermarking videos, but in reality video watermarking techniques need to meet other challenges than that in image watermarking schemes. Some of the video characteristics that impact watermarking include:

• High correlation between successive frames. If independent watermarks are embedded on each frame, an attacker could perform frame averaging to remove significant portions of the embedded watermark.
• Some applications like broadcast monitoring require real time processing and therefore should have low complexity.
• The unbalance between the motion and motionless regions.
• Watermarked video sequences are very much susceptible to pirate attacks such as frame averaging, frame swapping, statistical analysis and lossy compressions.


Fig 3 Example of a visible watermarking of an Image.
Left picture: Watermark. Right picture: Watermarked image

## III. WATERMARKING IN MPEG-4

There is a need for real-time copyright logo insertion in emerging applications, such as internet protocol television (IPTV). This is demonstrated in Fig 4. The visible-transparent watermarking unit accepts broadcast uncompressed video and the broadcaster's logo. The output is real-time compressed video with the logo embedded. Embedded systems that are involved in broadcasting need to have embedded copyright protection. Existing works are targeted towards invisible watermarking, not useful for logo insertion. The main steps for MPEG-4 are color space conversion and sampling, DCT and its inverse (IDCT), quantization, zigzag scanning, motion estimation, and entropy coding. A simpler approach is a single watermarking step in the compression framework because the computation requirements of watermarking are comparable to these steps.

The sampling rate is chosen to be 4:2:0 so that in a 4 pixel group, there are four Y pixels, a single Cb pixel and a single Cr pixel to meet digital TV broadcasting standards.

### A. COLOR SPACE CONVERSION

The conversion from RGB colorspace to YCbCr colorspace is performed using the following expression:

$$Y = 0.299R + 0.587G + 0.114B$$
$$Cb = 0.564(B - Y)$$
$$Cr = 0.713(R - Y)$$

### B. DCT OR IDCT

DCT is one of the computationally intensive phases of video compression. The two dimensional DCT and IDCT algorithms can be implemented by executing the one-dimensional algorithms sequentially, once horizontally (row-wise) and once vertically (column-wise).

### C. QUANTIZATION

After the DCT, the correlation of pixels of an image or video frame in the spatial domain has been de-correlated into discrete frequencies in the frequency domain. Since human visual system (HVS) perception is more acute to the DC coefficient and low frequencies, a carefully designed scalar quantization approach reduces data redundancy while maintaining good image quality. In the MPEG-4 video compression standard, a uniform scalar quantization is adopted. The feature of the scalar quantization scheme is an adaptive quantized step size according to the DCT coefficients of each macro block. For computational efficiency the scalar quantization step size can be chosen from predefined tables.

### D. ZIGZAG SCANNING

Zigzag scanning sorts the matrix of DCT coefficients in ascending order. For progressive frames and interlaced fields, zigzag scanning routes are provided by predefined Tables.

### E. MOTION ESTIMATION

Prior to performing motion estimation, an image (videoframe) is split into smaller pixel groups, called macroblocks, as the basic elements of the image rather than a single pixel. This is driven by a compromise between efficiency and performance to analyze a video's temporal model. A macroblock commonly has a size of 16×16 pixels. With the macroblock in the base frame and its two dimensional motion vector, the current frame can be predicted from the previous frame. In the MPEG-4 standard, the region in which the macroblock is bought for match could be a square, diamond, or of arbitrary shape. For most applications, a square region is considered. For example, if the macroblock has pixel size, the searching region will be a pixel block. The similarity metric for two blocks is the minimized distance between them. For simplicity, the sum of the absolute difference (SAD) is applied as the criterion for matching.

$$SAD(x,y) = \begin{cases} \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} |c(i,j) - p(i,j)|, & (x,y) = (0,0), \\ \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} |c(i,j) - p(i+x, j+y)| \end{cases}$$

where c(i, j) are the pixels of the current block, i, j=0,1, . . ., N−1; p(m, n) are the pixels of the previous block in the searching region, and m, n =−R, −R+1, . . ., 0,1, . . ., R +N−1, where the size of the macroblock is R pixels. Motion estimation is in the critical path of video compression coding and most time delay will occur at this step. The SAD algorithm will search the square target region exhaustively to find a matching macroblock. The output of this procedure is the prediction error for motion compensation and the motion vector.

### F. ENTROPY CODING

After DCT and quantization compression, additional compression can be achieved via entropy coding, which includes Huffman coding, Arithmetic coding, etc. Unlike lossy compression, as in the color space, DCT and quantization procedures, the entropy coding compression is lossless. The entropy coding efficiency depends on the precision of calculating the probability of occurrence of each coefficient. However, calculating probabilities of all the coefficients is impossible in real-time MPEG-4 coding and watermarking. The approach we followed is to utilize pre-calculated Huffman code.

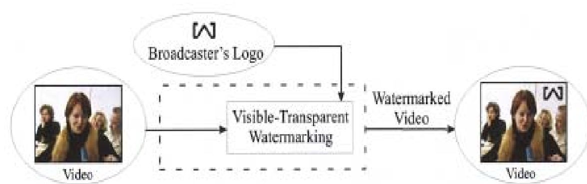



Fig 4. Real-time logo insertion through watermarking

## IV. THE PROPOSED WATERMARKING ALGORITHM

- Convert RGB color frames to YCbCr frames for the input video.
- Resample YCbCr frames according to 4:2:0 sampling rate.
- Split Y frame and watermark image into 8 x 8 blocks.

- Perform DCT for each 8 x 8 block to generate DCT coefficients.
- Perform perceptual analysis of the host video frame.
- Compute scaling and embedding factor for different blocks.
- Each block of Y DCT matrix is watermarked with an 8 x 8 watermark DCT matrix at same location as at DCT domain.
- Perform 2-D IDCT for each 8 x 8 watermarked matrix to transform it back to Y color pixels.
- Buffer watermarked Y component, non watermark Cb and Cr frames which holds a GOP.
- Split Y component into 16 x 16 blocks and Cb and Cr into 8 x 8.
- Perform motion estimation for Y component.
- Obtain the motion vectors (MV) and prediction errors of residual frame for motion compensation (MC) for Y component.
- Obtain motion vector and prediction error for Cb , Cr components and residual frame for motion compensation.
- Perform 2-D DCT on blocks of different frames.
- Quantize 2-D DCT coefficient matrix.
- Zigzag scan quantized 2-D DCT coefficient matrix.
- Entropy coding re-ordered 2-D DCT coefficient matrix and motion vector.
- Build structured compressed stream from the buffer.

The robustness of DCT watermarking arises from the fact that if an attack tries to remove watermarking at mid frequencies, it will risk degrading the fidelity of the image because some perceptive details are at mid frequencies. The other important issue of visible watermarking, transparency comes from making the watermark adaptive to the host frame. The proposed watermarking algorithm is presented as a flow chart in Fig 5. For gray scale, the watermark is applied to Y frames. For a color watermark image, the *Cb* and *Cr* color space are watermarked using the same techniques for Y frames. To protect against frame interpolating attacks on watermarking, all I, B, P frames must embed the watermark. The watermark embedding approach used is formulated as:

$$C_w(i,j) = \alpha_n C(i,j) + \beta_n W(i,j)$$

where $C_w(i,j)$ is a DCT coefficient after watermark embedding, $\alpha_n$ is the scaling factor and ,$\beta_n$ is the watermark strength factor, C(i, j) is the original DCT coefficient, and W (i, j) is the watermark DCT coefficient. The relative values of $\alpha_n$ and $\beta_n$ determine the strength of the watermark. Their values are computed based on characteristics of the host video frame. Given that human perception is sensitive to image edge distortion, for edge blocks the value of $\alpha_n$ should be close to its maximum value $\alpha_{max}$ while the value of, $\beta_n$ should be close to its minimum value, $\beta_{min}$. The user inputs that serve as quality control parameters are $\alpha_{max}$, $\alpha_{min}$, $\beta_{min}$, and , $\beta_{max}$. Since the watermark DCT coefficients will be added to the video frame DCT coefficients, it will be advantageous to adjust the strength of the watermark such that the distortion of these coefficients is minimal.

**TESTING OF WATERMARKING QUALITY**

We performed exhaustive simulations to make assessment of watermarking quality with a large variety of watermark images and video clips. Standard video quality metrics mean square error *(MSE)* and peak-signal-to-noise-ratio *(PSNR)* are applied to quantify the system's performance.

$$MSE = \frac{\sum_{m=1}^{M}\sum_{n=1}^{N}\sum_{k=1}^{3}[p(m,n,k) - q(m,n,k)]^2}{3 \times M \times N}$$

$$PSNR = 10 \times \log_{10}\left(\frac{(2^l - 1)^2}{MSE}\right)$$

Where *p(m, n, k)* and *q(m, n, k)* are the pixels after and before processing, respectively. It may be noted that the low *P S N R* did not degrade the perceptual quality of the video, as the low value is due to the fact that the watermark logo inserted is visible and consequently becomes noise for the host video and affects the *PSN R.*

## V. EXPERIMENTAL RESULTS & ANALYSIS

The proposed work is done in matlab. The visible and invisible watermarking is done in DCT domain. Here we take different video clips and we perform the PSNR values. These values are better when compared to previous works.

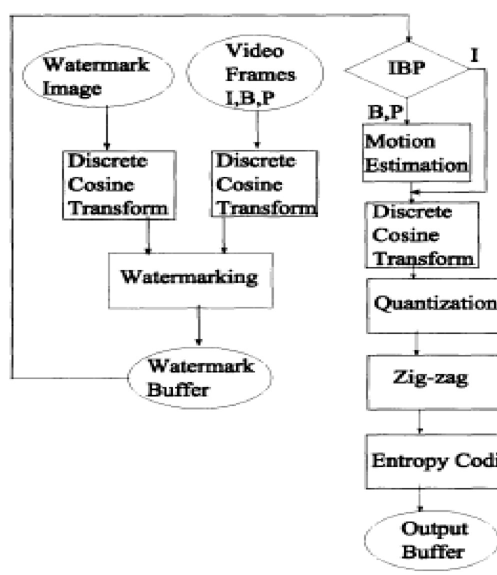



Fig 5. The flow of the proposed video watermarking algorithm

Table 1: Video quality metrics for visible watermark

| CLIPS | WATER MARKING | DOMAIN | PSNR(DB) |
|---|---|---|---|
| Math works video | Visible | DCT | 40.4636 |
| Terminator Movie | Visible | DCT | 57.0602 |

| | | | |
|---|---|---|---|
| Vcd cutter video | Visible | DCT | 36.3409 |
| Flying plane video | Visible | DCT | 32.5059 |

Table 2: Video quality metrics for Invisible watermark

| CLIPS | WATER MARKING | DOMAIN | PSNR(DB) |
|---|---|---|---|
| Math Works video | Invisible | DCT | 59.8538 |
| Terminator Movie | Invisible | DCT | 86.2401 |
| Vcd cutter video | Invisible | DCT | 61.9656 |
| Flying plane video | Invisible | DCT | 76.5855 |

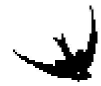
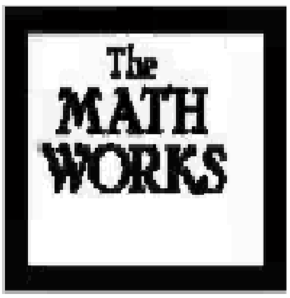


Fig 6. Watermark image

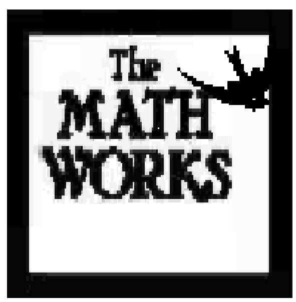
Tables I & II gives the PSNR values for visible and Invisible watermarking. Fig 6 is the watermark image which is going to be embedded in to the original number series video. We performed exhaustive simulations to make assessment of watermarking quality with a large variety of watermark images and video clips. For brevity we present selected examples of watermarked video in Fig. 7.



(a)Original math works video


(h) Visible watermarked vcd cutter video

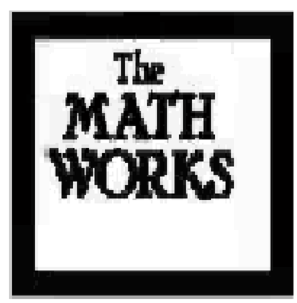

(d) Original Terminator movie



(b)Visible watermarked math works video


(g) Original vcd cutter video


(e) Visible watermarked Terminator video



(c)Invisible watermarked math works video



(i) Invisible watermarked
vcd cutter video

(f) Invisible watermarked
Terminator video

(j) Original Flying plane video

(k) Visible watermarked
Flying plan video

(l) Invisible watermarked
Flying plan video

Fig 7.Sample watermarked visible and invisible videos using watermark

## VI. CONCLUSIONS

Watermarking is a copy protection system that allows tracking back illegally produced copies of the protected multimedia content. Compared with other copy protection systems like Digital Rights Management, the main advantage of watermarking is that the watermark is embedded permanently in visual data of the content but at the cost of slight loss in fidelity. We presented a visible watermarking algorithm for MPEG4 video. The algorithm and its implementation are suitable for real-time applications such as video broadcasting, IP-TV and digital cinema. The watermark is embedded before video compression, thus resulting in balanced quality and performance. We also presented a invisible watermarking algorithm for security of the video.

In future, advanced MPEG-4 features, such as N-bit resolution, advanced scalable textures, and video objects will be utilized. It is anticipated that, with modest hardware complexity increase, performance will be significantly improved with the inclusion of these additional features. RTL level subsystem optimization will also be used to improve resource utilization and minimize execution time. Further research is under way to extend the real-time performance of the system to HDTV and higher resolutions and to improve the *PSNR.*

## REFERENCES

[1] M. Bami, F. Bartolini, and N. Checcacci. Watermarking of MPEG-4 video objects. *IEEE Transactions on Multimedia,*7(1):23-31, Feb 2005.

[2] M. Bami and et al. A DCT-domain system for robust image watermarking. *Signal Processing,* 66(3):357-372, May 1998.

[3] S. Biswas, S. R. Das, and E. M. Petriu. An adaptive compressed MPEG-2 video watermarking scheme. *IEEE Transactions on Instrumentation and Measurement,* 54(5):1853-61, Oct 2005.

[4] 1. Chen and et al. *Design ofDigital Video Coding Systems – A Complete Compressed Domain Approach.* Marcel Dekker, New York, 2002.

[5] M. Maes, T. Kalker, 1. P. M. G. Linnartz, 1. Talstra, G. F. G. Depovere, and J. Haitsma. Digital Watamarking for DVD Video Copyright Protection. *IEEE Signal Processing Magazine,* 17(5):47-57, Sep 2000.

[6] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli. A DCT Domain Visible Watermarking Technique for Images. In *Proceedings ofthe IEEE International Conference on Multimedia and Expo,* pages 1029-1032,2000.

[7] L. Qiao and K. Nahrstedt. Watermarking Methods for MPEG Encoded Video: Towards Resolving Rightful Ownership. In *Proceedings ofthe IEEE International Conference on Multimedia Computing and Systems,* pages 276-285, 1998.

[8] I. E. G. Richardson. ***H.264 and MPEG-4 Video Compression.*** John Wiley and Sons, Ltd, England, 2003.

[9] L. D. Strycker, P. Termont, J. Vandewege, 1. Haitsma, A. Kalker, M. Maes, and G. Depovere. Implementation of a Real-Time Digital Watermarking Process for Broadcast Monitoring on Trimedia VLIW Processor. lEE Proceedings on Vision,Image and Signal Processing, Aug 2000, 147(4):371-376,.

[10] T. H. Tsai and C. Y. Wu. An Implementation of Configurable Digital Watermarking Systems in MPEG Video Encoder. In Proceedings of the IEEE International Conference on Consumer Electronics, 2003, pages 216-21 7.

[11] G.W. Braudaway, K.A. Magerlein, F. Mintzer, Protecting publicly available images with a visible image watermark, in: Conf. 2659 Ð Optical Security and Counterfeit Deterrence

Techniques, San Jose, February 1996, SPIE Electronic Imaging: Science and Technology.
[12] O. Bruyndonckx, J.J. Quisquater, B. Macq, Spatial method for copyright labelling of digital images, Proc. IEEE Workshop on Non-Linear Processing, June 1995, pp. 456Ð459.
[13] G. Caronni, Assuring ownership rights for digital images, Proc. Reliable IT Systems, VIS 95, June 1995.
[14] S. Comes, Les traitements perceptifs dÕimages nume« rise« es, Ph.D. Thesis, Universite« Catholique de Louvain, June 1995.
[15] I.J. Cox, J. Kilian, T. Leighton, T. Shamoon, Spread spectrum watermarking for multimedia, Proc. SPIE 2420 (February 1995) 456Ð459.