ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

VIDEO WATERMARKING USING DCT AND DWT TRANSFORMS

Saranya.U[1], Dr. C.Gowri shankar[2],
Student Member, IEEE,P. G. Scholar, K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India[1]
Associate Professor (Sr), K.S.R. College of Engineering, Tiruchengode, Tamil Nadu,India[2]

ABSTRACT: Now a day's security is main concern when we entered into digital world but the steps to develop such security system and how we take optimum use of available or rather advanced techniques for developing such systems that can also fulfils our requirement are much important. Digital video watermarking scheme based on Discrete Ridgelet Wavelet Transform with SVD is addressed in this paper. Design of this scheme using Matlab Simulink is proposed. Embedded watermark is robust against various attacks that can be carried out on the watermarked video. Technology can be carried out by various algorithms like DWT, DCT in frequency domain. In this paper, combined DWT and DCT transforms are used to watermark data in video with minimum quality loss. Combined approach makes system robust as making use of multi-resolution DWT with energy compaction DCT. Results are evaluated for every frame in video by three parameters PSNR, MSE and NC. Design of proposed scheme is using MATLAB R 2013a.

KEY WORDS— DWT, DCT, PSNR, MSE, NC

I. Introduction

The development of multimedia applications makes digital media brings about conveniences to the people by easy processing of data. At the same time, it enables the illegal attackers to attack the works. For the protection of data, there has been growing interest in developing effective techniques to discourage the unauthorized duplication of digital data. Among cryptography and Steganography, only the watermarking provides the copyright protection and authentication. High speed computer networks, the Internet and the World Wide Web have revolutionized the way in which digital data iss 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 right management. Digital watermarking is a technology that can serve this purpose. A large number of watermarking schemes have been proposed to hide copyright marks and other information in digital images, video, audio and other multimedia objects. A watermark is a digital 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. The main purpose of digital watermarking is to embed information imperceptibly and robustly in the host data. Typically the watermark contains information about the origin, ownership, destination, copy control, transaction etc.

Potential applications of digital watermarking include transaction tracking, copy control, authentication, legacy system enhancement and database linking etc. Growing popularity of video based applications such as Internet multimedia, reless 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. Different video Encoder Decoders (CODECs) have evolved to meet the current requirements of video application based products. Among various available standards H.264 / Advanced Video Codec (AVC) is becoming an important alternative regarding reduced band width, better image quality in terms of peak-signal-to-noise-ratio (PSNR) and network friendliness [26], but it requires higher computational complexity. Different watermarking techniques have been proposed for different video CODECs, but only a few works on H.264/AVC can be found in the literature. H.264/AVC uses different transformation and block sizes than MPEG series, so development of new algorithms is required to integrate robust watermarking techniques for different profiles of H.264/AVC.

II. Implementation of Video Watermark

1. Fidelity: The watermark should not be noticeable to the viewer nor should the watermark degrade the quality of the content. In earlier work, we had used the term imperceptible", and this is certainly the ideal. However, if a signal is truly imperceptible, then perceptually based loss compression algorithms either introduce further modifications that jointly exceed the visibility threshold or remove such a signal.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

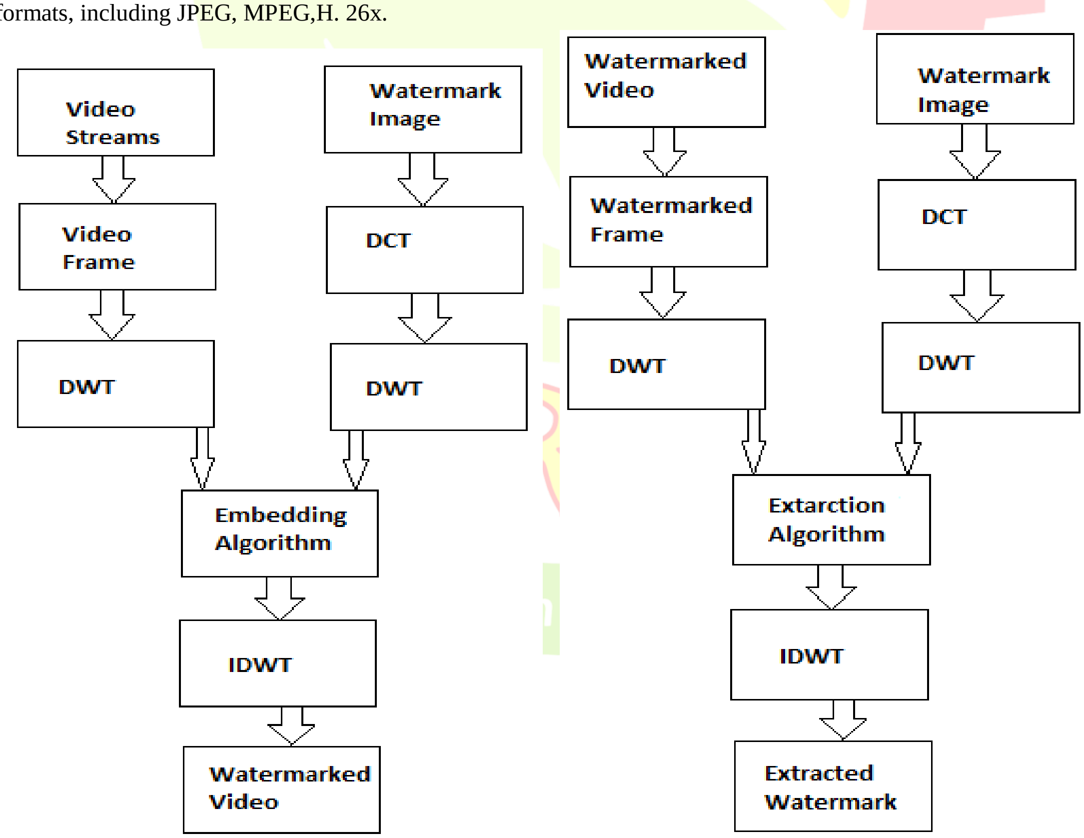
2. Robustness: Music, images and video signals may undergo many types of distortions. Loss compression has already been mentioned, but many other signal transformations are also common. For example, an image might be contrast enhanced and colors might be altered somewhat, or an audio signal might have its bass frequencies amp lied. In general, a watermark must be robust to transformations that include common signal distortions as well as digital-to-analog and analog-to-digital conversion and loss compression. Moreover, for images and video, it is important that the watermark survive geometric distortions such as translation, scaling and cropping.

3. Invisibility: The digital watermark embedded into the video data should be invisible to the human observer.

4. Computational Cost: Different applications require the embedded and detectors to work at different speeds. In broadcast monitoring, both embedded and detectors must work in real time so they need to be fairly fast and should have low computational complexity. On the other hand, a detector for proof of ownership will be valuable even if it takes days to find a watermark. Such a detector will only be used during ownership disputes, which are rare, and its conclusion about whether the watermark is present is important enough that the user will be willing to wait.

III. Proposed Video Watermarking Technique

A detailed description of the Software MATLAB architecture of the proposed digital video WM system is provided. Fig. 1 illustrates the general block diagram of the proposed system that is comprised of four main modules: a video camera, video compression unit, watermark generation, and watermark embedding units. 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,H. 26x.



(a)Embedding algorithm for video **(b) Extracting algorithm for video**

It provides three frequency element which are as follows low, mid and high. Low frequency components are most significant part of image and high frequency components can be easily removed through compression and attacks. The watermark is embedded into middle frequency to avoid quality loss of reference video. They are LL, LH, HL, and HH respectively which is

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

known as first level decomposition of DWT. Watermark is embedded into LH and HL sub-bands to avoid the degradation of host video.

This allows the integration of both watermarking and compression into a single system. Compression is divided into three elementary phases: DCT transformation, quantization, and Huffman encoding. Embedding the watermark after quantization makes the watermark robust to the DCT compression with a quantization of equal or lower degree used during the watermarking process. 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 [25].

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 authentication watermark data.

3.1 Video Compression

Currently, all popular standards for video compression, namely MPEG-x (ISO standard) and H.26x formats (ITU-T standard), use the same basic hybrid coding schemes that apply the principle of motion compensated prediction and block based transform coding using DCT [18]. MPEG-2 video compression standard has been described below as a representative case for utilizing the WM algorithm for more advanced DCT based compression methods. Generally, a video sequence is divided into multiple group of pictures (GOP), representing sets of video frames which are neighboring in display order. An encoded MPEG-2 video sequence is made up of two frame-encoded pictures: intraframes (I frame) and interframes (P-frame or B frame). P-frames are forward prediction frames and B-frames are bidirectional prediction frames. Within a typical sequence of an encoded GOP, P-frames may be 10% of the size of I-frames and B frames are about 2% of the I-frames. There can be two types of redundancies in video frames: temporal redundancy and spatial redundancy. MPEG-2 video compression technique reduces these redundancies to compress the images.

Within a GOP, the temporal redundancy among the video frames is reduced by applying temporal differential pulse code modulation (DPCM). The major video coding standards, such as H.261, H.263, MPEG-1, MPEG-2, MPEG-4, and H.264, are all based on the hybrid DPCM/DCT CODEC, which incorporates motion estimation and motion compensation function, a transform stage and an entropy encoder [19], [20]. It has been illustrated in Fig. 2 that an input video frame F_n is compared with a reference frame (previously encoded) F_{n-1} and a motion estimation function finds a region n matches the current macro-block in F_n. The offset between the current macro-block position and the chosen reference region is a motion vector, d_k. Based on this d_k, a motion compensated prediction F_n is generated, and it is then subtracted from the current macro-block to produce a residual or prediction error, e [20]. For proper decoding this motion vector, d_k, has to be transmitted as well. The spatial redundancy in the prediction error, e (also called the displaced frame difference) of the predicted frames, and the I-frame is reduced by the following operations: each frame is split into blocks of 8 × 8 pixels that are compressed using the DCT followed by quantization (Q) and entropy coding (run-level-coding and Huffman coding) (Fig. 2). Software implementation of MPEG-2 standard is not that simple. For simplifying the implementation of the video compressor module, the motion JPEG (MJPEG) video encoding technique rather than the MPEG-2 can also be considered.

IV. Result Analysis

The algorithm is applied to a sample video sequence video.mpg using binary watermark logo. The original sampled frame and its corresponding watermarked frame appears visually identical to the original. The performance of algorithm can be measured in terms of its imperceptibility and robustness against the possible attacks. Watermarked frame is subjected to a variety of attacks such as Gamma correction, Contrast adjustment, Histogram equalization etc. In case of geometric attacks scheme is tested against Frame resizing, Frame rotation, Frame cropping To evaluate the performance of any watermarking system, Peak Signal to Noise Ratio (PSNR) is used as a general measure of the visual quality of the watermarking system.

PSNR: The Peak-Signal-To-Noise Ratio (PSNR) is used to measure deviation of the watermarked and attacked frames from the original video frames and is defined as: $PSNR=10\log_{10}(255^2/MSE)$ (4.1)

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

Where MSE (mean squared error) between the original and distorted frames (size m x n) is defined as:

$$MSE=(1/mn)\sum_{i=1}^{m}\sum_{j=1}^{n}[I(i,j - I'(i,j))] \qquad (4.2)$$

Where I and I′ are the pixel values at location (i, j) of the original and the distorted frame respectively. Higher values of PSNR indicate more imperceptibility of watermarking. It is expressed in decibels (dB).

NC: The normalized coefficient (NC) gives a measure of the robustness of watermarking and its peak value is 1.

$$NC = \frac{\sum_i\sum_j W(i,j).W'(i,j)}{\sqrt{\sum_i\sum_i W(i,j)}\sqrt{\sum_i\sum_j W'(i,j)}} \qquad (4.3)$$

Where W and W′ represent the original and extracted watermark respectively.

a) Original Video

b) Watermarked Video

c) Video frames after rotation

d) Video frames after Resizing by 120 degrees

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

e) Input image of watermark **f) Secured watermark image**

Table 4.1 Shows the values of PSNR and NC of DWT with DCT video watermarking

ATTACKS	PSNR	NC
Rotation	24.3	0.41
Resizing	35.52	0.48
Gamma Correction	21.40	0.36

V. Conclusion

Here implementation of digital video watermarking scheme based on DWT is proposed. Due to multiresolution characteristics of DWT this scheme is robust against several attacks. Software model is design by using MATLAB/Simulink. There is no noticeable difference between the watermarked video frames and the original frames and robust watermarking technique for relational databases to resolve ownership issues.

The proposed technique watermarks data without any perturbations to the dataset. Since technique is distortion less, it is suitable for any data type attribute such as numeric, non-numeric etc. The robust technique resolves ownership issues. Primary key independent hash partitioning technique is proposed. Three-level security strategy is implemented to make technique secure. Technique proposed is 400 per cent robust against tuple addition attack, 100 per cent against alteration attack and 96 per cent robust against deletion attacks. The technique is resilient to additive and inevitability attacks. The area of digital watermarking is rife with challenges and ample research is still ongoing. Our future research will be directed towards increasing the level of resilience against several sources of attacks in the watermarking method. Additionally, multilevel authentication aspects will be added to enhance the security of the proposed technique.

VI REFERENCES

[1] Anumol, k. (2013), "Improving the robustness of DCT-based image watermarking against JPEG compression", International Journal of Computer Science and Mobile Computing, vol. 8, issue. 15, pp. 607-617.

[2] Bas, p., Chassery, J. M. & Macq, B. (2010), "Image watermarking: an evolution to content based approaches Pattern Recognition", vol. 35, issue. 6 pp. 545–561.

[3] Gwenael, A. D. & Dugelay, J. L. (2013), "A guide tour of video watermarking," signal process. Image common. vol. 18, No. 4, pp. 263–282.

[4] Jack, K. (2012), Video Demystified: "A Handbook for the Digital Engineer", 2nd edition. Eagle Rock, VA: LLH Technology Publishing.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016
[5] Mohanty, S. P. & Kougianos, E. (2013),"Real-time perceptual watermarking architectures for video broadcasting," J. System Software., vol. 84, no. 5, pp. 724–738.

[6] Majid Masoumil, Sherwin Amir. (2014), "Copyright Protection of Color Video Using Digital Watermarking", IJCSI International Journal of Computer Science Issues, vol. 9, issue. 4, no. 2, ISSN (Online): 1694-0814.

[7] Nitin, A., Shelke, P. N. & Chatur. (2010), "Blind Robust Digital Video Watermarking Scheme using Hybrid Based Approach", International Journal of Computer Science and Information Technologies, Vol. 5, pp. 312-324.

[8] Potdar, V. M., Han, S. & Chang, E. (2011), "A survey of digital image watermarking techniques," IEEE International Conference and Informatics, vol. 134, pp. 709–716.

[9] Piva, Bartolini & Barni, M. (2008), "Managing copyright in open networks," IEEE Transaction. Internet Computer. Vol. 6, no. 3, pp. 18–26.

[10] Richardson, I. E. G. & Julian, G. (2012), "A simplified approach for designing secure random number generators in hardware," in Process. IEEE International Conference. Electron Circuits System, vol. 12, no. 8, pp. 372–375.

[11] Shoshan, Y., Fish, A., Li, X., Julian, G. A & Yadid-Pecht, O. (2012), "VLSI watermark implementations and applications," International. J. Information Technology. Knowledge, vol. 2, no. 4 pp. 379–386.

[12] SanjanaSinha, R., Prajnat Bardhan, S., Swarnali Pramanick, Ankul Jagatramka, Dipak, K., Kole & Aruna Chakra borty. (2013), "Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis" International Journal of Wisdom Based Computing, vol. 1 (2) no. 6 pp.238-252.