International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Review On Digital Video Watermarking Using DWT

Shweta Sharma[1], Sarika Chaudhary[2]

Abstract: ***In this paper, we propose a robust perceptual digital video watermarking procedure to embed a watermark image in digital video frames using the variable-temporal length 3-D DCT technique. A variable-length 3-D DCT is chosen for exploiting the redundancy of the video sequences in temporal domain properly. The variable window length is obtained by applying a scene-change detection to a sequence of 8 × 8 blocks in successive frames. The method adopted embeds the watermark (a binary logo image) in an uncompressed video sequence by modifying the values of the mid-range coefficients of individual 3-D DCT blocks, in accordance with sensitivity of the 3-D human visual system model. The sensitivity of human eye in this frequency range is known to be minimum. This preserves the perceptual quality of video sequences. Since each block consists of the both spatial as well as temporal information of the video, we could achieve to spread the watermark in both spatial and temporal domain. This makes the proposed method highly robust against common signal processing manipulations such as frame averaging, frame dropping, noise addition, cropping and lossy compression. The retrieval rate of the watermark logo image varied between 50% to 99% for various attacks. The lower limit of watermark extraction occurs, when half or more than half of total video frames is dropped and also in the case of cropping where percentage of area cropped is more than 45%.***

Keywords: Discreet, wavelet transform, DWT, Watermarking, Matlab, Video invisible watermarking, Data Hiding, Digital, Interpolation Algorithm, Enhanced Robustness

1. Introduction

The popularity of digital video based applications is accompanied by the need for copyright protection to prevent illicit copying and distribution of digital video . Copyright protection inserts authentication data such as ownership information and logo in the digital media without affecting its perceptual quality. In case of any dispute, to increase robustness of the scheme, the watermark process is carried out in the video. Our video watermarking algorithm is robust against the attacks of frame dropping, averaging and statistical analysis, which were not solved effectively in the past. In video data embedding scheme the embedded secret data is randomly segmented and reconstructed without knowing the original host video. Secret data is embedded in individual video frames using the frequency domains of DWT. Finally the PSNR reading is compared for the Original Video & Watermarked Video.

Imperceptibility authentication data is extracted from the media and can be used as an authoritative proof to prove the ownership. For the purpose of copyright protection digital watermarking techniques must meet the criteria of imperceptibility as well as robustness against all attacks for removal of the watermark. Video watermarking approaches can be classified into two main categories based on the method of hiding watermark bits in the host video. The two categories are : Spatial domain watermarking where embedding and detection of watermark are performed by directly manipulating the pixel intensity values of the video frame. Transform domain [16-18] techniques, on the other hand, alter spatial pixel values of the host video according to a pre-determined transform and are more robust than spatial domain techniques since they disperse the watermark in the spatial domain of the video frame making it difficult to remove the watermark through malicious attacks like cropping, scaling, rotations and geometrical attacks. The commonly used transform domain techniques are Discrete Fourier Transform (DFT), the Discrete Cosine Transform(DCT), and the Discrete Wavelet.

2. Properties of Video Watermark

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 lossy compression algorithms either introduce further modifications that jointly exceed the visibility threshold or remove such a signal.

Robustness: Music, images and video signals may undergo many types of distortions. Lossy 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 lossy compression. Moreover, for images and video, it is important that the watermark survive geometric distortions such as translation, scaling and cropping.

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

Computational Cost: Different applications require the embedders and detectors to work at different speeds. In broadcast monitoring, both embedders 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.

3. Life Cycle of Watermarking Mechanism

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise.

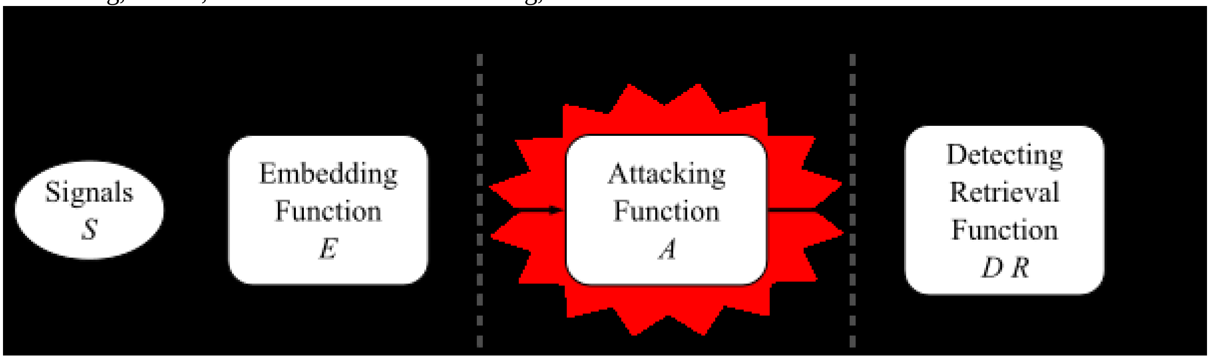


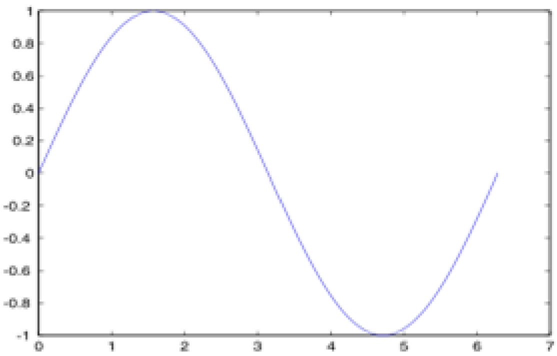
Figure : Life cycle of watermarking mechanism

4. Graphics and Graphical User Interface Programming

MATLAB supports developing applications with graphical user interface features. MATLAB includes GUIDE (GUI development environment) for graphically designing GUIs. It also has tightly integrated graph-plotting features. For example the function *plot* can be used to produce a graph from two vectors *x* and *y*. The code:

```
x = 0:pi/100:2*pi;
y = sin(x);
plot(x,y)
```

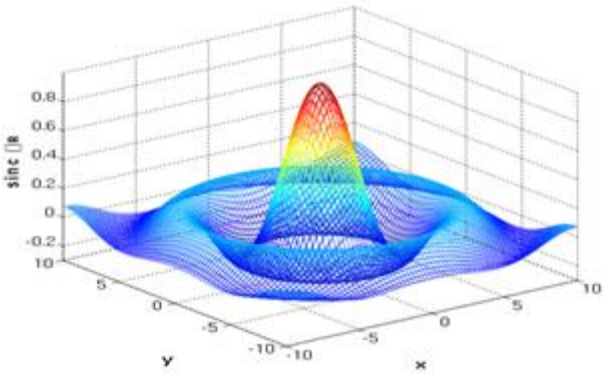
produces the following figure of the sine function



A MATLAB program can produce three-dimensional graphics using the functions *surf*, *plot3* or *mesh*.

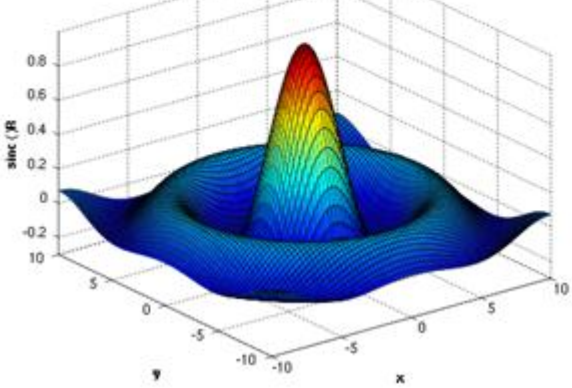
```
[X,Y] = meshgrid(-10:0.25:10,-10:0.25:10);
f = sinc(sqrt((X/pi).^2+(Y/pi).^2));
mesh(X,Y,f);
axis([-1010 -1010 -0.31])
xlabel('{\bfx}')
ylabel('{\bfy}')
zlabel('{\bfsinc} ({\bfR})')
hidden off
```

This code produces a **wireframe** 3D plot of the two-dimensional unnormalizedsinc function:



```
[X,Y] = meshgrid(-10:0.25:10,-10:0.25:10);
f = sinc(sqrt((X/pi).^2+(Y/pi).^2));
surf(X,Y,f);
axis([-1010 -1010 -0.31])
xlabel('{\bfx}')
ylabel('{\bfy}')
zlabel('{\bfsinc} ({\bfR})')
```

This code produces a **surface** 3D plot of the two-dimensional unnormalizedsinc function:



In MATLAB, graphical user interfaces can be programmed with the GUI design environment (GUIDE) tool.

5. Steps of Digital Video Watermarking

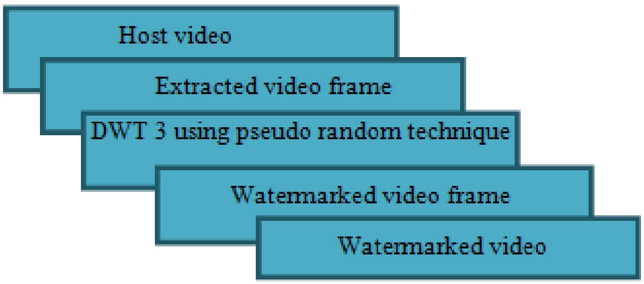


Figure 5.1: Steps of Digital Video Watermarking

1) **Host Video**
   It is the original video which is used as an input to the process of digital video watermarking.
2) **Extracted Video Frame**
   Many video frames combined to form a video. So, the video frames are extracted from the host video.
3) **DWT-3 using Pseudo Random Technique**
   Each original extracted video frame is combined with a pseudo random key generated by pseudo random technique. Multi-level discrete 3-D wavelet transform is applied to each extracted video frame combined with key.
4) **Watermarked Video Frame**
   After following the above three steps, each video frame get watermarked and watermarked video frame is obtained.
5) **Watermarked Video**
   All the watermarked frame combined to form a watermarked video and at last watermarked video is obtained.

6. Proposed Watermarking Technique

This section illustrates overall technique of the proposed technique for digital video watermarking based on multi-level discrete 3-D wavelet transform. Firstly, the formation of multi-level discrete 3-D wavelet transform is presented. Then, the proposed embedding process which includes video frame extraction and key generation technique is discussed in detail.

6.1 Multi-Level Discrete 3-D Wavelet Transform

The basic idea of discrete wavelet transform is to multi-differentiated decompose the frame into sub-frame of different spatial domain and independent frequency district. Discrete wavelet transform offers multi-resolution representation of frame and gives perfect reconstruction of decomposed frame. It decompose a frame in basically three spatial directions i.e., horizontal, vertical and diagonal in result separating the frame into four different components namely LL, LH, HL and HH. 3-D discrete wavelet transform decomposes a signal in to high and low frequency. At each level there are four sub-bands. In first level of decomposition, there are four sub-bands: LL1, LH1, HL1 and HH1 in which LL1 is a low frequency sub-band which is used for further decomposition. To achieve second level of decomposition, LL1 will have four sub-bands: LL2, LH2, HL2 and HH2. Now, the discrete wavelet transform is applied again to the low frequency band i.e., LL2. At third level of decomposition, there will have again four sub-bands of low frequency signal which is LL2. And the four sub-bands are LL3, LH3, HL3, HH3.

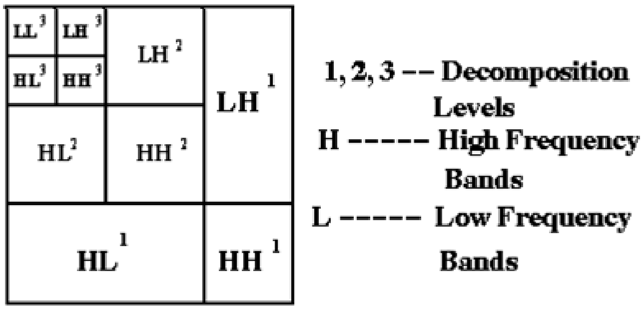


Figure 5.2.1: Decomposition levels of discrete wavelet transform

References

[1] Yui-Lam and Wan-Chi Siu, “Variable Temporal-Length 3D Discrete Cosine Transform,” IEEE Transaction on image processing, Vol. 6,No 5, May. 1997.
[2] Raymond K.W. Chan and M.C.Lee, “3D-DCT Quantization as a Compression Technique for Video sequences ,” in Proc. of Intl. Conf. on Virtual system and Multimedia,Geneva, Switzerland ,10-12 Sep ,1997
[3] F. Hartung and B. Girod, “Watermarking of Uncompressed and Compressed Video”, in Signal Processing, vol. 66, no. 3 (Special issue on Watermarking), pp. 283-301, May 1998.
[4] H. Kinoshita, “An image digital signature system with ZKIP for the graph isomorphism”,in Proc. IEEE Int. Conf. on Image Processing,vol. III,Lussane,Switzerland,Sept 16-19,1996.
[5] G. Langelaar, I. Setyawan, R. Lagendijk, “Watermarking Digital Image and Video Data”,in IEEE Signal Processing Magazine, Vol. 17, pp. 20-43, Sept. 2000.
[6] JiwuHuang,YunQ.Shi,“Embedding strategy for image watermarking in DCT domain” in Asia-