DWT Based Blind Digital Video Watermarking Scheme for Video Authentication

Chetan K.R
Sr. Lecturer, Dept. of CS&E J.N.N.C.E,
Shimoga
India

Raghavendra K.
Lecturer, Dept. of CS&E
P.E.S.I.T & M, Shimoga
India

ABSTRACT

Digital video is one of the popular multimedia data exchanged in the internet. Due to their perfectly replicable nature many illegal copies of the original video can be made. Methods are needed to protect copyrights of the owner and prevent illegal copying. A video can also undergo several intentional attacks like frame dropping, averaging, cropping and median filtering and unintentional attacks like addition of noise and compression which can compromise the owner information thereby denying authentication. In this paper, a robust Discrete Wavelet Transform (DWT)-based blind digital video watermarking scheme with scrambled watermarks based on scene changes has been proposed for authentication of digital video, which embeds different parts of a single watermark into different scenes of a video. The video watermarking algorithm is robust against the attacks of frame dropping, averaging and compression, which are considered as some of the common types of attacks applied particularly on the video and due to the use of DWT it can also withstand geometrical attacks making the watermark perceptually invisible. Furthermore, it allows blind retrieval of embedded watermark which does not need the original video. The proposed algorithm has been compared with an existing DWT based watermarking scheme and is found to exhibit better robustness.

General Terms

Video Processing, Digital Watermarking, Video Security, Encryption

Keywords

DWT, Histogram, Scrambled Watermark, Preprocessing.

1. INTRODUCTION

Video is a three-dimensional array of color pixels. Two dimensions serve as spatial (horizontal and vertical) directions of the moving pictures, and one dimension represents the time domain [1]. Digital video offers a number of advantages over analog video, including the ease of sharing and storage, no degradation of data quality when replicated, easy and inexpensive copying and the capacity for multicasting.

Digital video also has a growing presence in the academic arena, from digitized course lectures to archival footage housed in the campus library. Video conferencing-for collaboration, Internet-based communication and teaching, video on demand are some of the key services which include video. Digital video technology can also incorporate analytical software for intelligent video, which enables capabilities such as video search, object tracking and intrusion detection.

Advancement in technology has given multimedia users the ability to tamper with, produce copies of, and illegally redistribute digital content. The fast growing internet can facilitate piracy on a large scale, with users distributing unauthorized copies via peer-to-peer file sharing. The owner of the digital content, desires to ensure that all access to the content is authorized under the rules of a license (conditional access), unauthorized reproductions cannot be easily made (copy protection), and any illegal copies that are created can be detected and traced (authentication and content tracking). Without solving these security issues, digital multimedia products and services cannot take-off in an e-commerce setting [2].

An ideal solution to this problem would be to somehow integrate the security information directly into the content of the multimedia document such that the security information should be inseparable from the document during its useful lifespan. Moreover, the additional information should be perceptually invisible as the multimedia documents are ultimately processed by human viewers or listeners and the contents should not be affected. Finally is the flexibility of the scheme. Since the document might undergo replication, it should be able to support identification of different copies of the document.

Some of the techniques that can provide this ideal solution and that could be used in this context are steganography, data hiding, data embedding and watermarking. The main difference between steganography and watermarking is that steganograpic methods rely on the fact that covert communication is a point to point communication between trusted parties alone and that is unknown to third parties. Thus, steganographic methods are typically not designed to be robust against attempted attacks. In watermarking methods the existence of the embedded information is unknown to unauthorized parties who have access to the data, and can attempt unlawful attacks.

There exists a complex trade-off between three parameters in digital video watermarking: data payload, fidelity and robustness. The data payload is the amount of information, i.e. the number of bits that is encoded by the watermark. The fidelity is another property of the watermark: the distortion that the watermarking process is bound to introduce, should remain imperceptible to a human observer. Finally, the robustness of a watermarking scheme can be seen as the ability of the detector to extract the hidden watermark from some altered watermarked data. The robustness is often evaluated via the survival of the watermark after attacks. Those three parameters are conflicting and a trade-off has to be found, which is often tied to the targeted application.

In this paper, we propose the use of watermarking techniques which can satisfy these three parameters thereby providing authentication.

Many digital watermarking schemes have been proposed in literature for still images and videos. Most of them operate on uncompressed videos [3], while others embed watermarks directly into compressed videos [4, 5]. The work on video specific watermarking can be further found in [6, 7, 8, 9]. The weakness of the existing algorithms, however, includes: (i) the watermark is not robust to attacks which are specifically targeted at videos and even if they do, they fail to resist when image attacks are performed on them. (ii) The bit rate of the watermark is low. Some algorithms embed only one bit information as the watermark. (iii) None of the existing watermarking schemes shows resistance to all the attacks. This is specifically because most of these techniques have been derived from the image watermarking algorithms. Video watermarking introduces a number of issues not present in image watermarking. Due to large amounts of data and inherent redundancy between frames, video signals are highly susceptible to piracy attacks, including frame averaging, frame dropping, frame swapping and statistical analysis. All the proposed algorithms in the literature do not solve these problems effectively. Hence a watermarking scheme which shows robustness against video and image attacks and yet enables blind retrieval of the watermark is proposed in this paper.

2. PROPOSED MODEL

In this section, a Blind robust Video Watermarking Scheme with Scrambled Watermark is proposed. The watermarking scheme is based on Discrete Wavelet Transform (DWT). In this scheme, a watermark is decomposed into different parts and they are embedded in corresponding frames of different scenes in the original video. This ensures the proposed method to achieve robustness against the attack of frame dropping, averaging, swapping and lossy compression. For every motionless scene in the video, the algorithm embeds an identical watermark. Independent watermarks are used for successive but different scenes. All watermarks are embedded in the middle frequency sub-band of the frames. In the detection phase, the embedded watermark will be extracted from the video channel.

2.1 Video Watermarking scheme

The proposed video watermarking scheme comprises of different modules such as video preprocess, watermark preprocess, watermark embedding, and watermark detection. The proposed video watermarking scheme is as shown in Figure 1. The following sections elaborate the proposed scheme in detail.

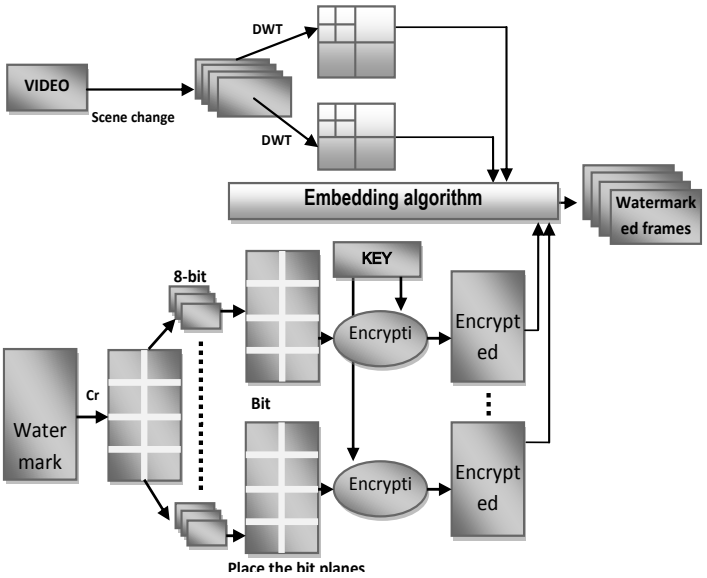


Figure 1. Proposed Video Watermarking scheme

2.2 Video Preprocess

The Video preprocessing stage consists of 3 parts: frame extraction, DWT and scene change detection. The video stream of the input video in the form of frames is extracted so that the watermarks can be embedded in the video channel. The audio channel is left untouched. All frames are transformed to wavelet domain with four levels. DWT transforms a signal into coarse and detail signals by **"**averaging and differencing**"** on the coefficients. It breaks down the signal into a coarse coefficient (DC component) and a hierarchy of detail coefficients (AC components).

DWT is chosen as it is more computationally efficient than other transform methods. The speed is faster than DCT and DFT as only sum or difference of the pixel have to be calculated. With DWT, one can achieve both spatial and frequency localization, perceptual invisibility and robustness to compression, robustness to noise, image processing techniques, and median filter (which can be considered as a case of pixel permutation), resistance to geometric transform (lots of existing algorithm do not survive) and resilience to counterfeit attempts. The scheme is robust against format conversions because the watermark is inserted before compression. Otherwise the authentication information will be lost if the video file is converted to a different compression standard.

Scene changes are detected from the video by applying the histogram difference method on the video stream. Independent watermarks are embedded in frames of different scenes. Histogram difference method is used for scene change detection. As each scene is embedded with same watermark, it can prevent attackers from removing the watermark by frame dropping. If they try to remove the frames with same watermark, they need to remove the entire scene and this would lead to significant damage to the video.

Identical watermark used within a scene can also prevent attackers from taking advantage of motionless regions in successive frames to remove the watermark by comparing and averaging the frames statistically. Moreover, due to similar frames using same watermark makes the scheme resistant to statistical analysis of the video to get the watermark. Independent watermark used for successive different scene can prevent attackers from colluding with frames from completely different scenes to extract the watermark.

Each frame is coded in 24-bit image, eight bits for each color (red R, green G, blue B). Consequently, each pixel is checked and classified into different classes. Only the Red component of the frames is considered. Histograms of the corresponding frames are calculated. Then, the total difference of the whole histogram (H) is calculated, which is given by:

$$H = \sum_{i,j=0} [P_a(i) - P_b(j)]^2 \quad (1)$$

If H > threshold (T), a scene change is detected.

2.3 Watermark Preprocess

Watermark is processed before it is embedded in the video. The watermark is cropped into small images, which are used as different independent watermarks as mentioned in the previous section. In the detection stage, the watermark is reconstructed with these images. The watermark must be a 256-grey-level image, with 8 bits representing each pixel. It is first scaled to a particular size with the following equation.

$$\mathbf{2^n \leq m,\ n > 0} \quad (2)$$

where *m* is the number of scene changes and *n, p, q* are integers. The watermark is divided into 2^n small images with size *32 X 32*.

Embedding of cropped watermarks into different frames can make the watermarks resistant to attacks by frame averaging. As the watermark is scrambled, it is hard for the attackers to reconstruct the watermark without the knowledge of the cropped watermarks distribution. It prevents unauthorized embedding and makes it harder to remove the watermark thus increasing the watermark security.

In the next step, each small image is decomposed into 8 bit-planes, and a large image m_n can be obtained by placing the bit-planes side by side only consisting of 0's and 1's. These processed images are used as watermarks, and totally 2^n independent watermarks are obtained. To make the scheme more robust, the processed watermarks *m* can be encrypted. Each bit of the watermark is used to alter the frequency coefficients of the video frame.

2.4 Watermark Embedding

The watermark is added to the frames by altering the magnitude of some DWT coefficients. The required alteration condition is:

```
if W[j] = 1,
Exchange C[i] with max(C[i], C[i+1], C[i+2],
C[i+3], C[i+4],C[i+5])
 Else
 Exchange C[i] with min(C[i], C[i+1],
C[i+2], C[i+3], C[i+4], C[i+5])
```

where **C[i]** is the i^{th} DWT coefficient of a video frame, and **W[j]** is the j^{th} pixel of a certain watermark. The sequence of zeros and ones of the encrypted binary watermarks are embedded starting from the higher frequency part of the video frame. Also, only the middle frequency wavelet coefficient of the frame (middle frequency sub-band) is watermarked, i.e., DWT coefficients of HL_1, LH_1, HL_2, LH_2, HL_3, LH_3, HL_4 and LH_4 are watermarked.

Coefficients of LL (i.e. the low frequency sub-band) are not watermarked, as the video energy is concentrated on lower frequency wavelet coefficient. If they are altered, it will affect perceptual quality. Coefficients of HH (i.e. the high frequency sub-band) are also not watermarked. It can make the watermark survive MPEG lossy compression as lossy compression removes the details (i.e. the high frequency components) of the image.

After watermark is embedded in the video frames in wavelet domain, Inverse Discrete Wavelet Transform (IDWT) is applied to obtain the watermarked video frames.

2.5 Watermark Extraction and Detection

In the detection phase, video is checked for the presence of the watermark. There are two, somehow related, ways to look at watermark extraction, first is to determine to whom does this watermark belong and second is to determine whether this is the correct watermark being seeked. In a blind video watermarking scheme, it does not need the original video while detecting the watermark.

The video frames from the watermarked video are extracted. The video frames will be processed to get the video watermark. Scene changes are detected from the video. Also, each video frame is transformed to the wavelet domain with four levels. Then the watermark is extracted with the following condition:

```
if WC[i] > median(WC[i], WC[i+1], WC[i+2],
WC[i+3], WC[i+4], WC[i+5]),
                    W[j] = 1
 Else
                    W[j] = 0
```

Where **WC[i]** is the i^{th} DWT coefficient of a watermarked video frame, and **W[j]** is the j^{th} pixel of an extracted watermark.

As an identical watermark is used for all frames within a scene, multiple copies of each part of the watermark may be obtained. The watermark is recovered by averaging the watermarks extracted from different frames. This reduces the effect if the attack is carried out at some designated frames. Then, one can combine the 8 bit-planes and recover the 32 X 32 size image, i.e., $1/2^n$ part of the original watermark. If enough scenes are found and all parts of the watermark are collected, the original large watermark image can be reconstructed.

After extracting and refining the watermark, the user can compare the results with the referenced watermarks subjectively. However, since the subjective measurement will be affected by the factors of the image size, expertise of the observers, and the experimental conditions, a quantitative measurement is required to provide objective judgment of the extracting fidelity. Quantitative measurement is given by a parameter called Normalized Correlation (NC). NC is defined as a similarity measurement of the extracted and the referenced watermarks. It is given by:

$$NC = \frac{\sum_i \sum_j W_{ij} \times RW_{ij}}{\sum_i \sum_j W_{ij}^2} \quad (3)$$

It is the cross-correlation normalized by the reference watermark energy to give unity as the peak correlation. This is used for evaluating the performance of the proposed scheme.

3. PERFORMANCE ANALYSIS

As the watermarking algorithm has several phases the performance of the algorithm can be evaluated by considering the performance of the individual phases.

Let T be the total number of frame in a video and $n_1 \times n_2$ be the size of the video frame and *m* the total number of scene change in the video.

Size of the video frame = $n_1 \times n_2$

Number of frames = *T*

Number of scene changes = *m*

To prepare the watermark for the scheme, a watermark is scrambled into small parts in preprocess, and they are embedded into different scenes. The watermark is first scaled to a particular size with the following Equation.

$$2^n \le m,\ n > 0 \quad (4)$$

With the above equation

$$p + q = n, \quad p, q > 0 \quad (5)$$

where *m* is the number of scene changes and *n, p, q* are positive integers. The size of the watermark should be

$$32 \text{ X } 2^p \text{ X } 32\text{X}2^q \quad (6)$$

Then the watermark is divided into *2n* small images with size *32 X 32*.

If size of watermark is smaller than video frame, complexity is of order *O (m1m2).* If size of watermark is greater than video frame, the complexity is of order,

$= O(64 \times 64 \times 2^n) = O(m) = O(max[(m1,m2),m])$

Generating different part of watermark=2^nx64x64=*O(m)* (7)

Total running time of the watermark preprocessing algorithm is

$$= O(logm)+O(1) + O(max[(m1,m2), m]) + O(m) = O(max[(m1,m2), m]) \quad (8)$$

Scene changes are detected from the video by applying the histogram difference method on the video stream. The histogram difference method is used for scene change detection. Each frame is coded in 24-bit image, eight bits for each color (red R, green G, blue B). Consequently, each pixel is checked and classified into different classes. For efficiency purpose, only the most significant two bits for each color are considered. Then, the total difference of the whole histogram (H) is calculated by Equation (1).

Scanning to generate the histogram for 1 frame = $n_1 \times n_2$
Create histogram = $n_1 \times n_2$
Compare the histogram = *64* x *64*
Total running time = $[2(n_1 \times n_2) + 64] \times T = O(n_1 n_2 T)$ (9)

The watermarking scheme is based on four level DWT. All frames in the video are transformed to the wavelet domain. The frame is decomposed in four level subband frame by separable 2-D wavelet transform. It produces a low frequency sub-band LL_4, and three series of high frequency subbands LH_j ,HL_j ,HH_j , where j < 4.

Running time for DWT

$$= 2\left[n_1 \times n_2 + n_1 \times \frac{n_1}{2} \times 2\right] + 2\left[\frac{n_1}{2} \times \frac{n_1}{2} + \frac{n_1}{2} \times \frac{n_1}{4} \times 2\right] + 2\left[\frac{n_1}{4} \times \frac{n_1}{4} + \frac{n_1}{4} \times \frac{n_1}{8} \times 2\right] + 2\left[\frac{n_1}{8} \times \frac{n_1}{8} + \frac{n_1}{8} \times \frac{n_1}{16} \times 2\right]$$

$$= 4n_1n_2 + 2n_1n_2 + n_1n_2 + \frac{n_1n_2}{2}$$

$$= \frac{15n_1n_2}{2}$$

$$= O(n_1n_2) \quad (10)$$

When embedding the watermark, only the middle frequency wavelet coefficient of the frame (middle frequency sub-band) is watermarked, i.e., DWT coefficients of HL_1, LH_1, HL_2, LH_2, HL_3, LH_3, HL_4 and LH_4 are watermarked.

Total number of pixels to watermark:

$$= \frac{n_1 \times n_2}{2} + \frac{\frac{n_1}{2} \times \frac{n_2}{2}}{2} + \frac{\frac{n_1}{4} \times \frac{n_2}{4}}{2} + \frac{\frac{n_1}{8} \times \frac{n_2}{8}}{2}$$

$$= \frac{n_1n_2}{2} + \frac{n_1n_2}{8} + \frac{n_1n_2}{32} + \frac{n_1n_2}{128}$$

$$= \frac{85n_1n_2}{128}$$

$$= O(n_1n_2) \quad (11)$$

Number of operations for watermark:

$$= \frac{85n_1n_2}{128} \times T$$

$$= O(n_1n_2T) \quad (12)$$

After the watermark is embedded, the video frame is inverse-DWT. Running time for IDWT:

$$= 2\left[n_1 \times n_2 + n_1 \times \frac{n_1}{2} \times 2\right] + 2\left[\frac{n_1}{2} \times \frac{n_1}{2} + \frac{n_1}{2} \times \frac{n_1}{4} \times 2\right] + 2\left[\frac{n_1}{4} \times \frac{n_1}{4} + \frac{n_1}{4} \times \frac{n_1}{8} \times 2\right] + 2\left[\frac{n_1}{8} \times \frac{n_1}{8} + \frac{n_1}{8} \times \frac{n_1}{16} \times 2\right]$$

$$= 4n_1n_2 + 2n_1n_2 + n_1n_2 + \frac{n_1n_2}{2}$$

$$= \frac{15n_1n_2}{2}$$

$$= O(n_1n_2) \quad (13)$$

Total running time for embedding watermark

$$= O(n_1n_2T) + 2O(n_1n_2T)$$

$$= O(n_1 n_2 T) \quad (14)$$

Finally, Running Time

$$= O(max[m_1, m-2, m]) + O(n_1 n_2 T) + O(n_1 n_2 T) \qquad n_1 n_2 \geq m_1, m_2$$

$$= O(n_1 n_2 T) \quad (15)$$

4. SIMULATION RESULTS AND ANALYSIS

The algorithm was simulated using MATLAB programming language. The original video sample consists of about 274 frames of size 360 X 240. For testing purposes the video was scaled to a size of 512 X 256 with frame numbers varying from 10-60.

4.1 Video Preprocess

The video preprocessing consists of detecting the scene changes in the given video. The test video was subjected to the scene change detection algorithm. The Threshold value was taken to be greater than 4500 to get enough number of scenes for testing. Only the histogram for the red component of the frames was applied. About four scene changes were detected by the algorithm in frames 6, 7, 8 and 9 respectively. Their histograms are shown in the Figure 2.

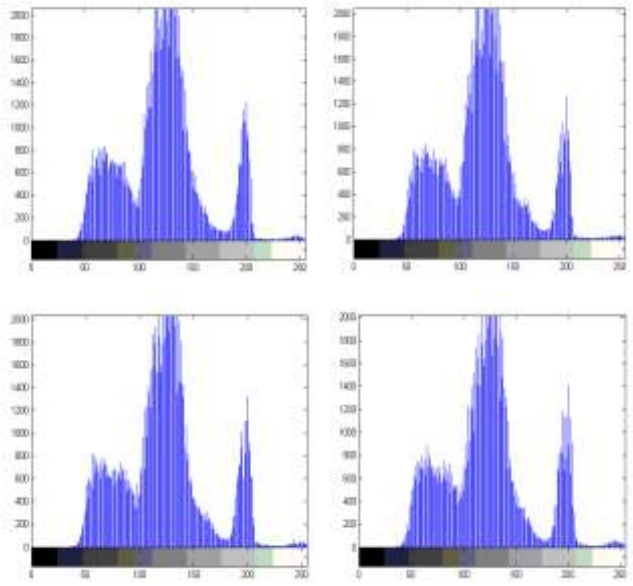


Figure 2. Histograms of the scene change frames.

4.2 Watermark Preprocess

The test video contains four scene changes and hence according to Equation (2) the value of *n=2* and the value of *p*=1 and *q*=1. The size of the watermark is *64 X 64*. For watermark, a grey scale image of the specified dimensions was preprocessed. The original watermark was cropped into four separate watermarks of dimensions *32 X 32*. The cropped watermarks are bit sliced and four independent watermarks m_0-m_3 were obtained. The results are shown in Figures 3 and 4.

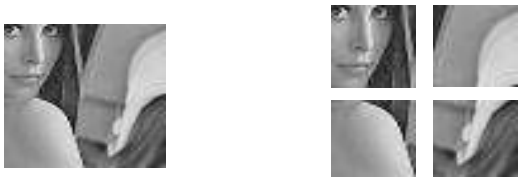


Figure 3. Original and Cropped Watermarks

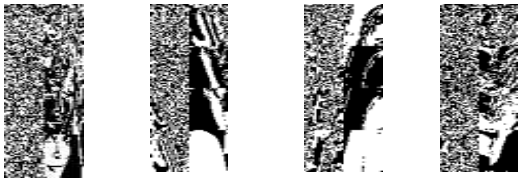


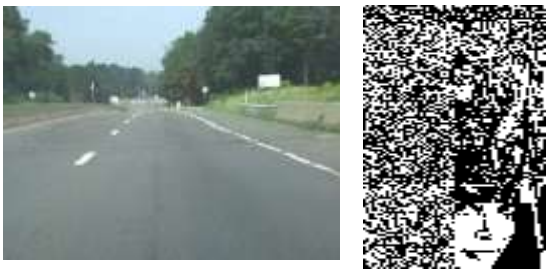
Figure 4. Independent bit-sliced Watermarks m0-m3.

4.3 Watermark Embedding

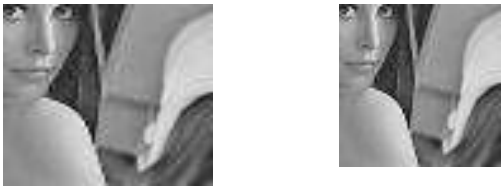
The independent binary watermarks were embedded into the transformed frames according to the embedding algorithm. The DWT coefficients of the middle frequency sub-band namely LH4, HL4, LH3, HL3, LH2, HL2, LH1, HL1 are watermarked. The frames from 1-6 of the test video was watermarked with m_0, frame 7 with m_1, frame 8 with m_2, frame 9 with m_3 and for the remaining frames the watermarks were repeated. Once all the frames are watermarked, inverse DWT is applied to get the watermarked frames and subsequently the watermark video.

4.4 Recovery

The recovery of the watermarks is done by applying the extraction algorithm to the frames of the watermarked video. The scene changes in the watermarked video are detected. Based on these scene changes, different parts of the watermark are extracted. Once all the parts of the watermark become available, the entire watermark is reconstructed. As an illustration, the extracted watermark of the first scene, as well as the recovered watermark is shown in Figure 5. The NC value of the extracted watermark is found to be 0.9751.



(a) Watermarked frame (b) Extracted bit-sliced watermark



(c) Original watermark (d)Extracted Watermark

Figure 5. Results of Recovery stage.

4.5 Attack Scenarios

DWT inherits many advantages in resisting the attacks on the watermarked frames. It achieves both spatial and frequency localization, perceptual invisibility and can resist attacks by image processing techniques. To test the robustness of watermark, different incidental attacks were mounted on watermarked video. The embedded watermark was retrieved using the proposed algorithm and the NC value of the recovered watermark was recorded for different attack scenarios. NC values for all the attack scenarios are well above 0.5, and this guarantees the robustness of the proposed scheme.

4.6 Attack Analysis

The video watermarking scheme is robust against the video specific attacks like frame dropping, averaging, lossy compression and image processing attacks like video cropping, noise, median filtering. To analyze performance, the proposed algorithm is compared with an existing DWT-based watermarking scheme [10] which embeds an identical watermark in all frames. Tables 1 to 6 gives attack parameters and NC values of the recovered watermark for both the schemes and the corresponding comparison graph is plotted in Figures 6 to 11 respectively. It was observed that the proposed scheme shows great robustness than the earlier DWT based scheme. The algorithms ability to make the watermark resistant to these attacks was analyzed and better results were inferred from the graph.

Table 1. Frame Dropping.

Drop percentage	Proposed Scheme	Existing DWT based scheme
10	0.9611	0.945
20	0.9611	0.873
30	0.9611	0.826
40	0.9582	0.754
50	0.9582	0.700
60	0.6712	0.640
70	0.6712	0.569

Table 2. Frame Averaging

Percentage of frames averaged	Proposed Scheme	Existing DWT based scheme
0	0.975	0.963
10	0.819	0.645
20	0.791	0.521
30	0.799	0.578
40	0.796	0.547
50	0.766	0.512
60	0.758	0.509

Table 3. Lossy Compression

Quality factor	Proposed Scheme	Existing DWT based scheme
10	0.7175	0.5331
20	0.7236	0.5362
30	0.7225	0.5510
40	0.7273	0.6011
50	0.7327	0.6408
60	0.7519	0.6705
70	0.7605	0.6769
80	0.7694	0.6901
90	0.7755	0.7411

Table 4. Cropping

Cropping Ratio	Proposed Scheme	Existing DWT based scheme
10	0.9522	0.875
20	0.9075	0.825
30	0.8491	0.775
40	0.8238	0.711
50	0.7723	0.652
60	0.3981	0.621
70	0.2220	0.578
80	0.1226	0.542
90	0.1101	0.525

Table 5. Addition of Noise

Noise Ratio	Proposed Scheme	Existing DWT based scheme
10	0.9030	0.701
20	0.8760	0.594
30	0.8512	0.551
40	0.8477	0.516
50	0.8426	0.500
60	0.8244	0.511
70	0.8151	0.522
80	0.7799	0.521
90	0.7167	0.501

Table 6. Median Filtering

Median filtering n-by-n Neighborhood	Proposed Scheme	Existing DWT based scheme
3	0.7403	0.539
4	0.6422	0.532
5	0.6287	0.529
6	0.5893	0.539
7	0.6323	0.549
8	0.5900	0.537
9	0.5896	0.528

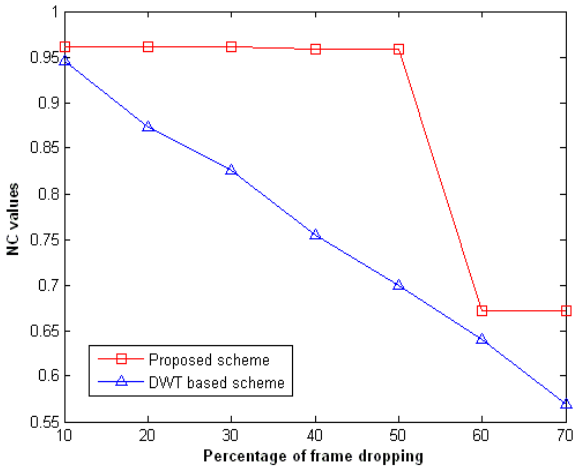


Figure 6. Performance under Frame Dropping

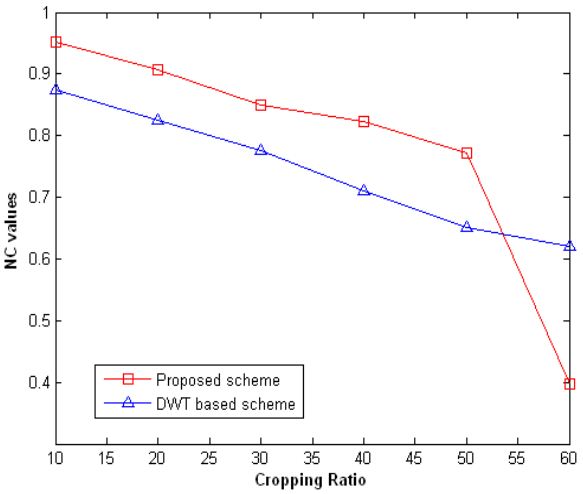


Figure 9. Performance under Cropping

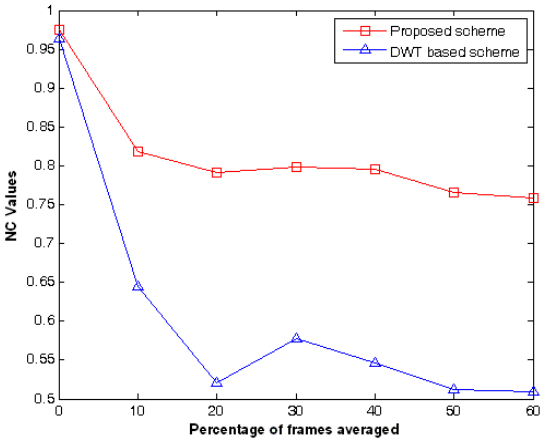


Figure 7. Performance under Frame Averaging

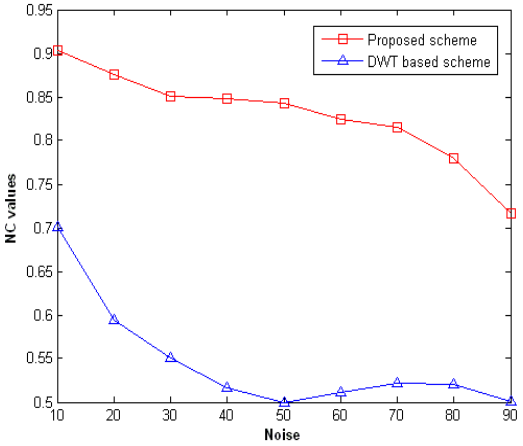


Figure 10. Performance under Addition of Noise

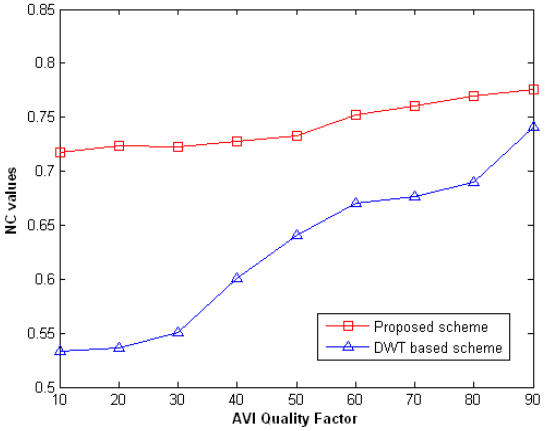


Figure 8. Performance under Lossy Compresssion

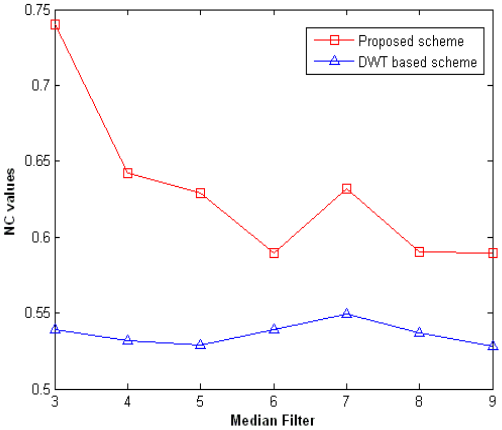


Figure 11. Performance under Median Filtering

5. CONCLUSION

With DWT, the watermarking scheme takes the major advantages in resisting the attacks and partial removal of the watermark. The results also show that the scheme is robust against different image processing attacks like addition of noise, median filtering and cropping. A comprehensive analysis was conducted in order to determine the feasibility of the embedding and extracting algorithm and the performance of the scheme was evaluated. The analysis reveals that the use of DWT has better performance and fidelity when compared with the other transform techniques such as DCT or DFT. The approach cultivates an innovative idea of embedding different parts of a watermark in the DWT domain according to scene changes, and its advantages were clearly seen from the experimental results. A video usually contains two separate channels namely video channel and the audio channel respectively, an effort can be made to make use of the audio channel as a carrier of error correcting codes which can help in the refinement of the extracted watermark. This can considerably increase the robustness of the watermark since most of the specified attacks are on the video channel.

6. REFERENCES

[1] K. Su, "*Digital Video Watermarking Principles for Resistance to Collusion and Interpolation Attacks*", Master of Applied Science thesis, University of Toronto, Sept. 2001.

[2] F. Deguillaume, G. Csurka, J. Ruanaidh, and T. Pun, "*Robust 3D DFT video watermarking*", Proceedings Electronic Imaging' 99: Security and Watermarking of Multimedia Contents, Vol. 3657, San Jose, CA, Jan. 1999.

[3] M. Ejima and A. Miyazaki, "*A wavelet-based watermarking for digital images and video*", Proceedings International Conference on Image Processing (ICIP-2000), Vol. 3, pp. 678-681, Vancouver, Canada, 2001.

[4] S. Arena and M. Caramma, "*Digital watermarking applied to MPEG2 coded video sequence exploiting space and frequency masking*", Proceedings International Conference on Image Processing (ICIP-2000), Vol. 3, pp. 438-441, Vancouver, Canada, 2000.

[5] F. Hartung and B. Girod, "*Watermarking of uncompressed and compressed video*", Proceedings Signal Processing, Vol. 66, pp. 283-301, 1998.

[6] C. Serdean, M. Ambroze, M. Tomlinson, and G. Wade, "*Combating geometrical attacks in a dwt based blind video watermarking system*", Proceedings Video/Image Processing and Multimedia Communications 4th EURASIP-IEEE Region 8 International Symposium on VIPromCom, pp. 263-266, 2002

[7] M. Barni, F. Bartolini, R. Caldelli, A. De Rosa, and A. Piva, "*A Robust Watermarking Approach for Raw Video*", Proceedings 10th International Packet Video Workshop PV2000, Cagliari, Italy, May 1-2, 2000

[8] C. Lu and M. Liao, "*Video object-based watermarking: a rotation and flipping resilient scheme*", Proceedings 2001 International Conference on Image Processing, Vol. 2, pp.483-486, 2001.

[9] B. Mobasseri, "*Direct sequence watermarking of digital video using m-frames*", Proceedings International Conference on Image Processing (ICIP-98), Vol. 3, pp. 399-403, Chicago, Illinois, Oct. 4-7, 1998.

[10] Ejim, M., & Miyazaki, A. "*A wavelet-based watermarking for digital images and video*", International Conference on Image Processing, ICIP 00, vol. 3, pp. 678-681, 2000.