Analysis of Robustness of Hybrid Video Watermarking against Multiple Attacks

C. N. Sujatha
Associate Professor,
ECE Dept, SNIST, Hyderabad

P. Satyanarayana
Professor, ECE Dept.,
AITS, Tirupati

ABSTRACT
An efficient video watermarking algorithm using DWT-DCT-SVD is proposed to analyze the robustness against various attacks. In this algorithm, video is divided into several groups of frames, so that each group of frames carries various watermarks. In the proposed method, each plane of video frames are decomposed using DWT and high frequency band HH, middle frequency bands LH, HL are transformed with DCT. The DCT coefficients are SVD transformed which are embedded with corresponding transformed coefficients of watermarks. The desired number of watermarks will be embedded in selected group of frames without causing noticeable distortion. The amount of inserted watermarks is controlled by Peak Signal to Noise Ratio of the watermarked frame to achieve good imperceptibility according to human visual system. The embedded watermarks are extracted from watermarked video with inverse process. Similarity between original and extracted watermarks is estimated by measuring correlation coefficient. The proposed algorithm is tested with various video sequences using MATLAB software. Reported experimental results show the watermarked frames are indistinguishable from the original frames subjectively and demonstrate the effectiveness of the proposed algorithm against the attacks of frame averaging, dropping, swapping, compression, Gaussian noise, salt & pepper noise, median filtering, average filtering, sharpening, histogram equalization, rotation, cropping.

Keywords
DWT, DCT, SVD, PSNR, CF, Attacks.

1. INTRODUCTION
Nowadays, advances in digital multimedia like Internet video, wireless video, video phones, video conferencing and many others shows great interest in protecting the copyright ownership of multimedia. Possible technique to protect ownership of digital assets is watermarking and it has extended its applications from copyright protection to content indexing, secret communication, finger printing. Now the digital video watermarking has become an attractive research area, however, several video watermarking algorithms have been proposed and researchers are focused more on security of video watermarking. The important goal of watermarking technique is to embed some useful information in the original content as much as possible, while maintaining invisibility of that information by considering human visual system properties [1]. Watermarking techniques can be classified according to their working domains, human perception and ability to resist attacks. Watermarks can be embedded either in spatial or transform domain. Spatial domain watermarking is performed by modifying values of pixel color samples of a video frame whereas in frequency domain techniques, watermarks are applied to coefficients obtained from frequency transformed frame. In all frequency domain watermarking schemes, there is a conflict between robustness and transparency. If the watermark is embedded in perceptually most significant regions, the watermark would be robust to attacks but it may be difficult to hide. If it is embedded in perceptually insignificant regions, it would be easier to hide the watermark but the scheme may be less resistant to attacks.

Earlier Singular value Decomposition (SVD) was explored for watermarking in which binary watermark is embedded in singular values of video frames [2]. Robustness, capacity and imperceptibility are the important requisites of an efficient watermarking scheme using DWT, DCT or DWT-SVD [3-5]. SVD based watermarking scheme has high imperceptibility but it failed to withstand certain attacks like sharpening, cropping and rotation etc. The algorithm in [6] embeds the gray watermark image in singular values of DCT coefficients of decomposed high frequency bands of IVUS video frames for telemedicine applications. In [7], the proposed watermarking scheme hide the singular values of gray scale watermark image into the singular values of DCT transformed DWT coefficients of LH band. The algorithm proposed in [8] uses gray scale image as watermark and embeds the watermark into SVD and DCT transformed LH or HL middle frequency bands.

In recent, one of the most difficult problems in digital video watermarking is that the recovery of watermark in the presence of attacks. The watermark should be retrievable even if common signal processing operations are applied to the watermarked video data and also be immune from geometrical operations such as rotation, translation, scaling and cropping. With the help of complete survey on the current watermarking technologies which indicate that none of the current watermarking techniques can resist all the attacks. From this point of view, in the present work, the cascading of three powerful mathematical transforms; DWT, DCT and SVD based Non blind invisible watermarking technique is used for hiding multiple watermarks within the video. Hidden watermarks can be extracted by using IDWT, IDCT and

ISVD. This algorithm offers higher capacity and robustness compared to other watermarking systems.

Attacks on digital video watermarks represent all intended and unintended operations, which are executed by attacker with a goal to remove watermark from watermarked video and get possession of unmarked content. Specific attacks applied to video are frame dropping, frame averaging, and additive noise, geometrical attacks like cropping and rotation, and unintended attacks for example compression of video sequences.

This paper focuses especially on intended and unintended attacks which are frame averaging, frame dropping, frame swapping, rotation, Gaussian noise, salt & pepper noise, median filtering, average filtering, sharpening, histogram equalization, cropping and compression.

2. PROPOSED WATERMARKING SCHEME

The proposed method which performs watermarks embedding into video content is based on hybrid technique using DWT, DCT and SVD [9]. The described method is based on watermarking in still images [10].

2.1 Watermark embedding process

The video watermarking algorithm proposed will embed different logos into group of frames in the video using three powerful mathematical transforms. In this technique, original color video is split into group of frames and R, G and B planes are isolated from each color frame. By applying DWT, each plane is decomposed into four sub bands LL, LH, HL and HH. Take three of these four sub bands: LH, HL, and HH. Apply DCT to these selected sub bands and SVD is performed on the DCT coefficients to get singular value matrix along with two unitary orthonormal matrices. In the present work each group of frames should carry one individual watermark logo.

Let color logo as watermark. The same procedure is applied to the watermark also to obtain singular values matrix and orthonormal unitary matrices which plays an important role while extracting the watermark from watermarked video. The singular values of the original video frame and watermark are added at chosen scaling factor to form the modified singular values. Then perform inverse DCT followed by inverse DWT to obtain watermarked frame. Reconstruct the watermarked frames into final watermarked video. Once embedding is done, watermarked video is subjected to various attacks which are clearly mentioned in section 3.

2.2 Watermark recovery process

Watermarked video is partitioned into group of frames and separate the R, G, B planes from each frame. Each plane is decomposed into multi frequency bands using DWT. Then DCT is applied on selected sub bands: LH, HL and HH followed by SVD to separate modified singular values from watermarked frame. Watermark is extracted by subtracting the singular values obtained in the embedding process. Then inverse DCT and inverse DWT are performed to recover the color watermark. The block diagram for watermark embedding and extraction are shown in Figure 3 and Figure 4.

3. EXPERIMENTAL RESULTS

In this experiment, implementation of the proposed video watermarking algorithm has been done under the MATLAB 7.14 environment. The AVI video used is of 120 frames with 240x320 sizes and 10 different gray and color images can be embedded in selected group of 12 frames. So the maximum capacity of each frame in the proposed video watermarking algorithm is 1.9 Mega bits at most. The present method of watermarking was tested against different intended attacks which are frame averaging, frame dropping, frame swapping and unintended attacks compression. These attacks are specific for a video and most used. The proposed scheme is also tested against common image processing and geometrical attacks.

The screenshots of the original video and the corresponding watermarked video after embedding individual watermarks are presented in Figure 1 and Figure 2. The extracted watermarks are shown in Figure 5 and results of correlation factors versus various extracted logos from various groups of frames without attacks are shown in Figure 6. After embedding watermarks in video, the watermarked video can be subjected to various attacks and the hidden watermarks can be extracted from attacked watermarked video. The quality of extracted watermarks after the attacks was judge by subjective and objective aspects in terms of correlation factor which is used to verify the similarity between the original watermark and extracted watermark obtained from attacked video.

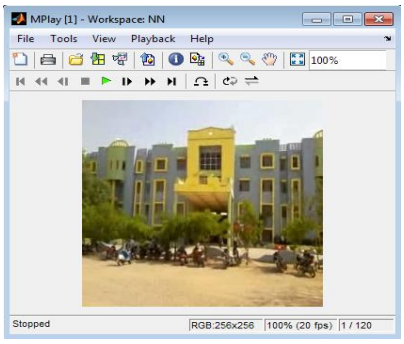


Fig 1: original video

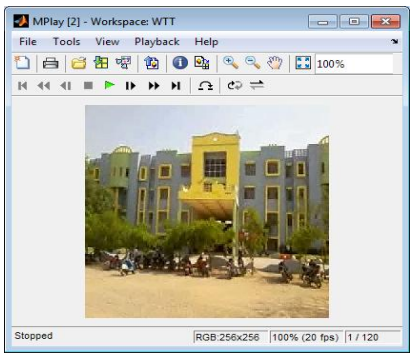


Fig 2: watermarked video

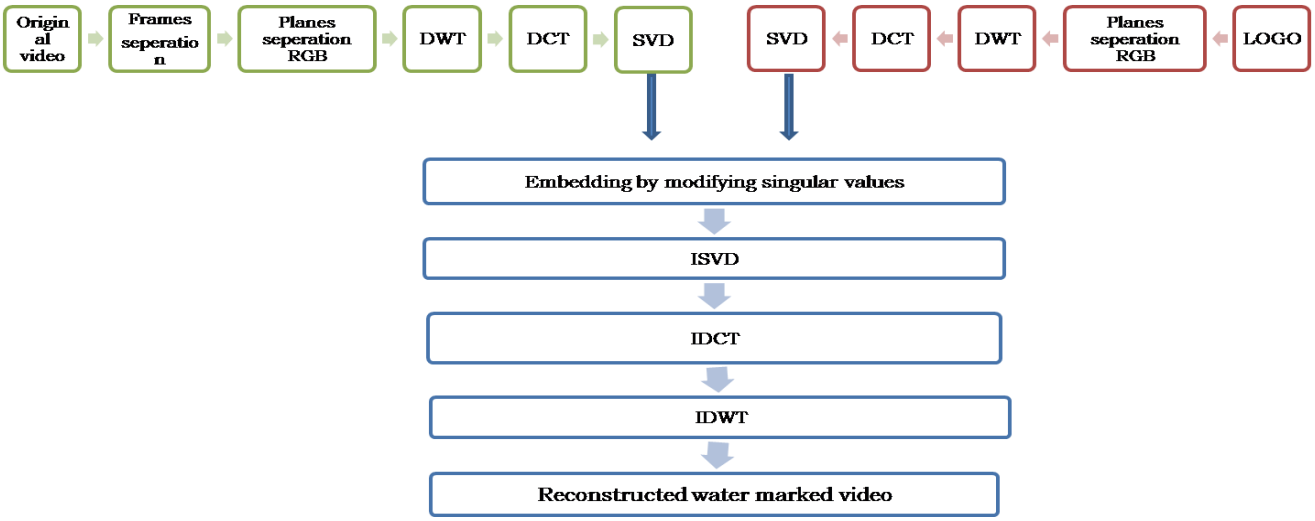


Fig 3: Block diagram for watermark embedding Process

Table 1. Similarity measure against all sort of attacks for different logos

Logo no.		1	2	3	4	5	6	7	8	9	10
S.No	Attacks										
1	Frame averaging	0.9379	0.9821	0.9826	0.9851	0.9725	0.9515	0.9972	0.9743	0.9841	0.9920
2	Frame dropping	0.9339	0.9803	0.9809	0.9839	0.9714	0.9474	0.9970	0.9736	0.9839	0.9916
3	Compression	0.9530	0.9859	0.9868	0.9892	0.9776	0.9555	0.9976	0.9758	0.9878	0.9931
4	Frame swaping	0.9379	0.9803	0.9810	0.9839	0.9712	0.9475	0.9970	0.9737	0.9837	0.9906
5	Gaussian	0.8209	0.9234	0.9363	0.9119	0.9469	0.8083	0.9635	0.9692	0.9235	0.9751
6	Salt &pepper	0.8943	0.9611	0.9669	0.9637	0.9661	0.9103	0.9882	0.9790	0.9638	0.9867
7	Rotation	0.9470	0.9768	0.9832	0.9772	0.9862	0.9564	0.9933	0.9897	0.9730	0.9918
8	Median filtering	0.9966	0.9992	0.9986	0.9979	0.9969	0.9983	0.9997	0.9982	0.9981	0.9990
9	Average filtering	0.9406	0.9570	0.9749	0.9729	0.9913	0.9766	0.9933	0.9972	0.9856	0.9955
10	Sharpening	0.9424	0.9583	0.9758	0.9739	0.9918	0.9777	0.9936	0.9975	0.9862	0.9957
11	Histogram equalization	0.9412	0.9574	0.9753	0.9734	0.9915	0.9772	0.9934	0.9974	0.9858	0.9956
12	Left cropping	0.9570	0.9890	0.9876	0.9884	0.9772	0.9592	0.9980	0.9789	0.9884	0.9932
13	Right cropping	0.9646	0.9905	0.9897	0.9921	0.9850	0.9664	0.9982	0.9787	0.9880	0.9935
14	Top cropping	0.9422	0.9830	0.9848	0.9888	0.9763	0.9511	0.9972	0.9744	0.9877	0.9938
15	Bottom cropping	0.9490	0.9844	0.9886	0.9937	0.9849	0.9518	0.9973	0.9750	0.9905	0.9952
16	w/o attack	0.9854	0.9989	0.9976	0.9997	0.9826	0.9711	0.9999	0.9704	0.9978	0.9970

The statistics obtained in the present algorithm against attacks are shown in Table 1. These results show that the extracted watermarks from watermarked video are perceptually same as embedded watermarks in terms of similarity measure. Correlation factors between embedded and extracted logos almost nearer to unity. From these results, it has been observed that SVD is more convenient tool for watermarking in hybrid domain. The effect of every pixel in the watermark logo is reduced by means of scaling factor and also observed that the scaling factor can be chosen from a wide range of values to hide the watermark coefficients into the video frame coefficients. In DCT based watermarking algorithm, the lowest frequency coefficients are not modified because watermark transparency would be lost. But in this present algorithm, no problem is experienced in modifying these coefficients. Various attacks have been modeled on the watermarked video and in all cases, watermarks were recovered.

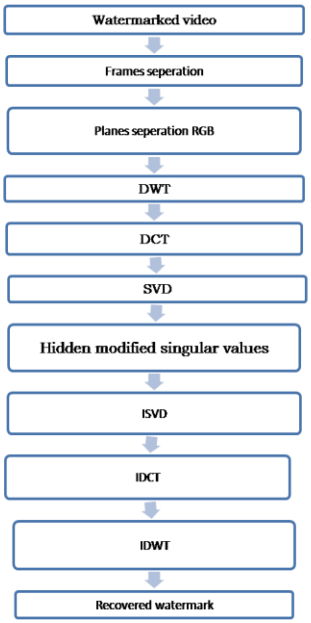


Fig 4: Watermark Extraction Process

Fig 5: Extracted watermarks

A video sequence of 120 frames with 10 different watermarks is used to test under frame averaging, dropping and swapping. In case of frame averaging attack, first three frames of each group are averaged. Thus the watermarked video is restricted to 100 frames and observed that the watermark logos are extracted with minimal amount of distortion. The frame averaged video and corresponding CF values are shown in Figure 7.

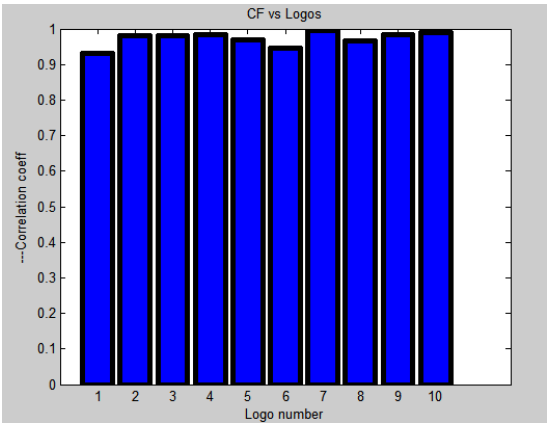


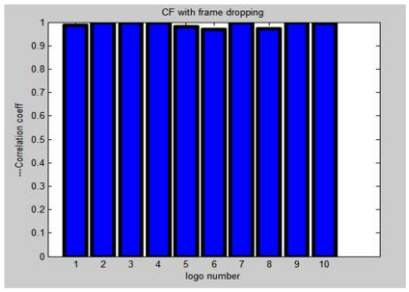
Fig 6: Correlation factors Vs Logos

To investigate the robustness of the embedded watermark, every 6 frames of each group such as 50 percent of frames are dropped from the marked video. The resultant watermarked video and CF values are shown in Figure 8. In the present work, frames of watermarked video are randomly swapped and CF values are calculated between hidden and extracted watermarks which are shown in Figure 9. The compressed video and corresponding CF values are displayed in Figure 10.

Robustness of watermarked video is tested with common attacks like Gaussian noise and Salt & Pepper noise as shown in Figure 11 and Figure 12. The difference between original and noisy video is increasing with variance of Gaussian noise. The severity of salt & pepper noise changes with density level in the form of black and white pixels on the video frames. These results show the robustness of our algorithm against noise addition. Each frame of the watermarked video is rotated by specified angle as shown in Figure 13 and embedded logos are extracted from rotated frames. And it has been observed that there is just minor degradation in recovered watermarks.

Important attacks on video are median filtering and average filtering which has shown in Figure 14 and Figure 15 respectively. Sharpened watermarked video and CF plot is shown in Figure 16. Histogram equalized watermarked video and the corresponding CF plot is shown in Figure 17. From these results, it has been proved that our present algorithm is resistant to all variety of attacks.

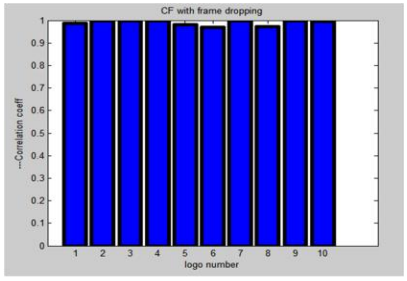
a. watermarked video



b. Plot of Correlation factors

Fig 7: effect of frame averaging

a. watermarked video

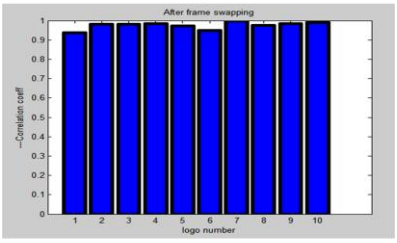


b. Plot of Correlation factors

Fig 8: effect of frame dropping

The watermarked video is cropped in four different ways like left cropping, right cropping, top cropping and bottom cropping. Even under this situation, the proposed algorithm can extract the embedded watermarks from different groups of frames with large similarity factor which has displayed in Figure 18 to Figure 21. This proves that there is no single technique which can provide all these characteristics with maximum values of correlation factors. In the present algorithm, the watermarks are found to be discernible with reasonable accuracy. This is the technique using three powerful transforms to withstand all variety of attacks that has never been used for video watermarking before.

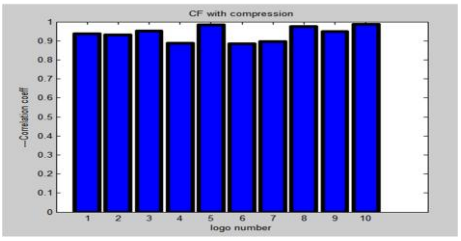
a. watermarked video



b. Plot of Correlation factors

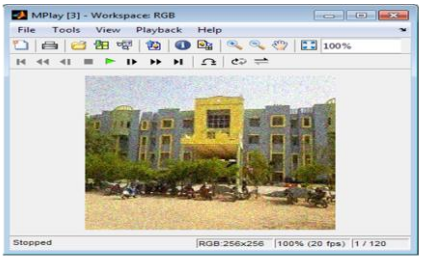
Fig 9: effect of frame swapping

a. watermarked video

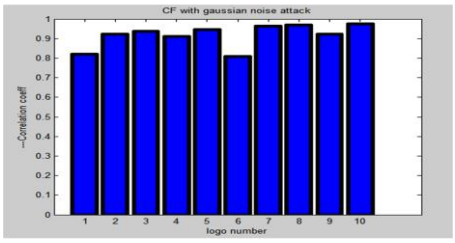


b. Plot of Correlation factors

Fig 10: effect of compression

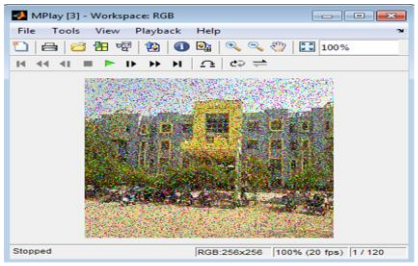


a. watermarked video

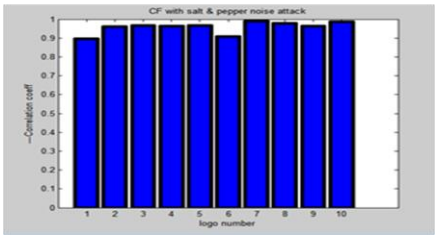


b. Plot of Correlation factors

Fig 11: effect of Gaussian noise attack



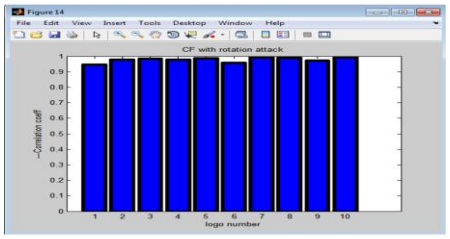
a. watermarked video



b. Plot of Correlation factors

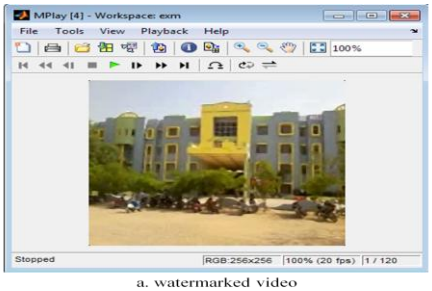
Fig 12: effect of Salt & pepper noise attack

a. watermarked video

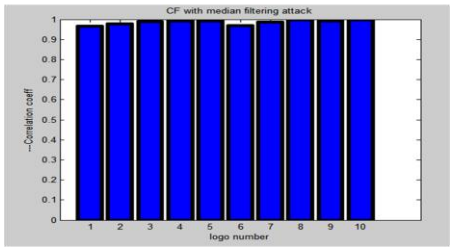


b. Plot of Correlation factors

Fig 13: effect of rotation



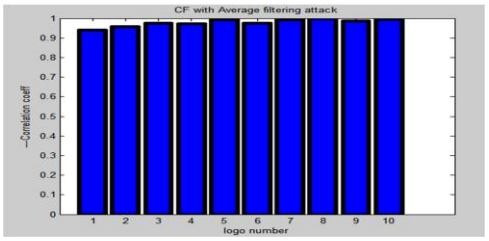
a. watermarked video



b. Plot of Correlation factors

Fig 14: effect of median filtering

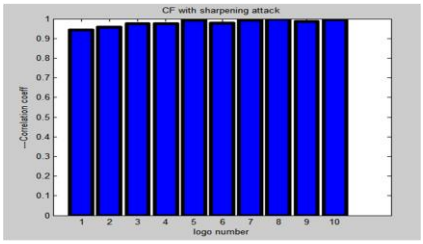
a. watermarked video



b. Plot of Correlation factors

Fig 15: effect of average filtering

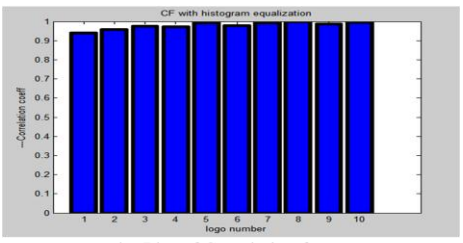
a. watermarked video



b. Plot of Correlation factors

Fig 16: effect of sharpening

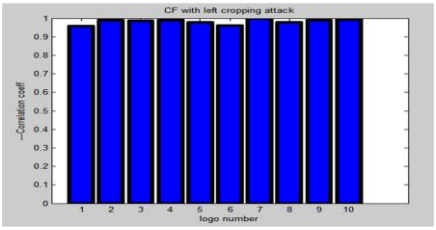
a. watermarked video



b. Plot of Correlation factors

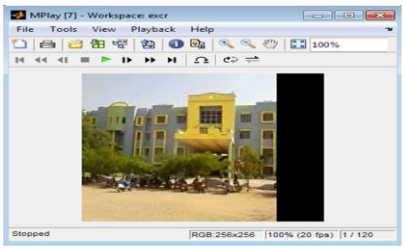
Fig 17: effect of histogram equalization

a. watermarked video

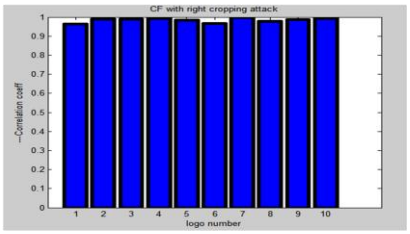


b. Plot of Correlation factors

Fig 18: effect of left cropping



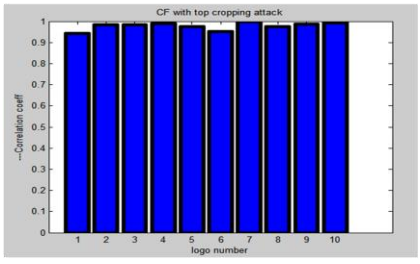
a. watermarked video



b. Plot of Correlation factors

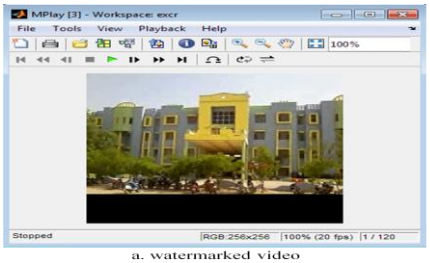
Fig 19: effect of right cropping

a. watermarked video

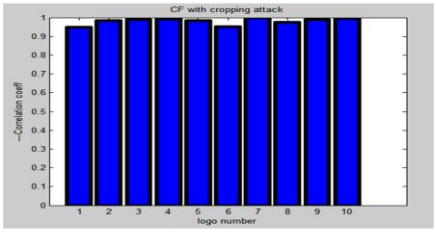


b. Plot of Correlation factors

Fig 20: effect of top cropping



a. watermarked video



b. Plot of Correlation factors

Fig 21: effect of bottom cropping

4. CONCLUSIONS

The proposed DWT-DCT-SVD based watermarking algorithm was found to be a very robust method of non-blind watermarking which can be used to embed copyright information in the form of color or gray scale visual watermark and hidden watermarks can be recovered even from the attacked watermarked video. Experimental results illustrate that the proposed watermarking scheme based on hybrid technique is robust against all sorts of unintended and intended attacks. The present scheme has very high data hiding capacity. The improvement of robustness against attacks can be achieved by increasing scaling factor. The experimental results prove that the quality of the watermarked video is better. Furthermore, the recovered watermark can be easily identified.

5. REFERENCES

[1] Potdar VM, Han S, Chang E, "A Survey of digital image watermarking techniques", Proceedings of *IEEE* international Conference on industrial informatics, 2005, pp. 709-716.

[2] Wenhai Kong, Bian Yang, Di Wu and Xiamu Niu, "SVD Based Blind Video Watermarking Algorithm ", Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06), IEEE, 2006.

[3] Sadik Ali M. Al-Taweel, Putra Sumari, Saleh Ali K. Alomari and Anas J.A. Husain, "Digital Video Watermarking in the Discrete Cosine Transform Domain", Journal of Computer Science, Vol. 5 (8), 2009, pp. 536-543.

[4] A.Essaouabi and F.Regragui and E.Ibnelhaj, "A Wavelet-Based Digital Watermarking for Video", International Journal of Computer Science and Information Security (IJCSIS), Vol. 6, No.1, 2009, pp. 29-33.

[5] Rajab. L, Al-Khatib. T and Al-Haj. A, "Hybrid DWT-SVD Video Watermarking", International Conference on Innovations in Information Technology, pp. 588-592, Dec. 2008.

[6] Nilanjan Dey, A. B. Roy, P. Das and A. Das, "DWT-DCT-SVD Based Intravascular Ultrasound Video Watermarking", World Congress on Information and Communication Technologies (WICT), 30th Oct – 2nd Nov 2012, pp. 224-229.

[7] Satyanarayana Murty. P and Rajesh Kumar. P, "A Method for Watermarking in Digital Videos by usingHybrid Transforms and Edge Detection", International Journal of Computer Applications (IJCA), Volume 71, No.13, May 2013, pp.16-23.

[8] Hoda Farag Ibrahim Farag and Said E. El-Khamy, "Adaptive Video Watermarking Based on Multiband DWT & DCT & SVD", Proceedings of the International Conference on Computer Graphics, Multimedia and Image Processing, Malaysia, 2014, pp. 28-35.

[9] C. N. Sujatha and P. Satyanarayana, "High Capacity Video Watermarking based on DWT-DCT-SVD ", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 2, Feb. 2015, pp.245-249.

[10] C. N. Sujatha and P. Satyanarayana, "An Improved Hybrid Color Image Watermarking under Various Attacks", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 4, Issue. 3, Mar. 2015.