A Digital Video Copyright Protection Scheme using Colored Watermark Embedding Algorithm : CWEA

Jabir Ali, Satya Prakash Ghrera

Computer Science & Engineering Jaypee University of Information Technology Solan, Himachal Pradesh, India

ABSTRACT

Digital Watermarking is an important and finest method of protecting the copyright of the digital media. In this paper, a secure and robust digital video watermarking algorithm is proposed, that is Color Watermark Embedding Algorithm (CWEA). This algorithm has two important parts. First, YCbCr color format is used to insert the variable size watermark. Second, embedding of detail coefficients of LUMINANCE (Y-luminance) of watermark into the detail coefficients of CHROMINANCE (Cb and Cr- chrominance) of identical frames (I-Frames) of digital video. Watermark data is inserted into the detail coefficients in an adaptive manner based on the energy of high frequency. We have performed number of tests for many video-frame manipulations and attacks. All these tests are also performed on CWEA and it provides good results. In this paper, non-blind and semi-blind watermarking systems are used where non-blind watermarking mechanism has been proved to be robust, imperceptible and efficient to protect the copyright of H.264 and MPEG-4 coded video within the video retrieval system.

Keywords : CWEA, DWT, LUMINANCE, CHROMINANCE, I-Frame, Detail Coefficient, H.264, MPEG-4.

I. INTRODUCTION

The future growth of the domestic digital copyright protection products basically depends on Real Network and Microsoft Windows Media. Large numbers of these products follow only the protection of copyright of electronic publications, magazines, journals and static images. But still, the necessity of such a platform exists which can apply the copyright protection on digital videos professionally.

A. Video Watermarking

Nowadays, a large amount of multimedia data has been exchanged over the internet and many internet users are sharing their images, videos and audios. Security provided to protect shared and transferred data over internet is not enough and many people are not aware of this security issue and control access techniques. So there are various approaches for data security such as steganography, fingerprinting, copyright protection [1, 2], and so on. In this paper, we have considered the Copyright Protection technique of data security in Digital Videos. For this, we are inserting a Digital Watermark or digital pattern (an image) inside digital video frames. Some important aspects of watermark systems include Robustness (quality of the watermark should not be degrade due to any attack, whether the attack is intentional or unintentional), Imperceptibility (the data embedded inside the video frames that should not be visible), Capacity (the number of bits that can be hidden), Security (to control the illegal use of data) and computational complexity of the embedding and detection process [4-6].

B. Types of Watermarking

For detection process of the watermark, Data hiding techniques can be divided into three categories: Blind, Semi-blind, and non-blind. In this paper, non-blind and semi-blind watermarking systems are used [7-9].

Blind systems do not require the original host data (image, video, Audio etc.) to extract the watermark. For the sake of security, some additional information (e.g., a secret "key") may be needed in order to detect or decrypt the watermark. The key can be suppressed if additional security is not needed. Meanwhile, non-blind systems need to have the original host data at the decoder in order to decode the watermark. A semi-blind watermarking system can be imagined as a communication system with side information. In such types of systems, the watermark or some information about the original host data (but not the entire host data) is required to extract the watermark sequence. This classification of watermarking system has shown in Table 1.

In this paper, digital video copyright protection using DWT is proposed. Extraction of I-frame, watermark preprocessing, watermark embedding and extraction, piracy tracking and various others are implemented in this paper. In this paper, work is done to build a professional platform which coalesces watermark embedding and extraction with source video tracking. This platform embeds a watermark in video for copyright protection to satisfy the client's requirements and then, embedded watermark is extracted from the original source video to authenticate the copyright. It also compares extracted watermark with the original watermark to verify whether the product is authorized or not.

In the literature review, we have studied that an attacker may be crack, damage or detect watermark with the help of some possible algorithms [10]. But in CWEA, it is very difficult to detect the original pattern of inserted watermark. In this paper, we have improved the robustness and security of inserted digital pattern or watermark and transparency of watermarked media. TABLE 1 has shown the classification of watermark system.

Table 1. Classification of watermark system.

Criteri	Class	Brief Description
Domain Type	Pixel	Manipulate the Pixels values to embed the watermark
	Transform	Modified the coefficients of Transform Domain to embed the watermark. These are the some popular Transform:- Discrete Cosine Transform (DCT) Discrete Wavelet Transform (DWT) Discrete Fourier Transform (DFT) Principle Component Analysis (PCA)
Watermark Type	PRNS	Detecting the presence or absence of a watermark statistically. A PRN Sequence is generated by feeding the generator with a secret seed.
	Visual	The visual quality of embedded watermark is evaluated.
Information Type	Non-blind	Both the original image and Secret key required.
	Semi-blind	Watermark and Secret key are required.
	Blind	Only secret key required.

C. Possible Attacks

Attacks create disturbances in original content. There is a list of some possible attacks in Digital video Watermarking technique.

1) **Adaptive Noise:** An Additive noise typically forces to increase the threshold values at which the correlation detection process works.

2) **Filtering:** There are two types of filtering Low pass and high pass filtering. Low pass filtering does not introduce the considerable degradation in watermarked image or watermarked signals but it can affect the performance.

3) **Cropping:** This is a very common attack to analyze the pattern inserted in the multimedia document and in this type of attack an attacker or intruder just select the small portion of the watermarked object and try to find the pattern that is inserted inside that particular multimedia document.

4) **Compression:** Sometimes compression is known as the unintentional attack which appears very often in multimedia applications [11].

Rotation and Scaling, Multiple Watermarking and Statistical Averaging are also the types of attacks which can be performed on digital video.

In Figure 1. we have shown the general diagram of video watermarking. Here, we have a colored watermark and original video file and applying some watermarking algorithm on both, and get the final watermarked video. After applying de-watermarking algorithm on watermarked video and get the extracted watermark and original video.

In this paper, a new digital video watermarking algorithm Color Watermark Embedding Algorithm (CWEA) is proposed. CWEA has two important parts. First, YCbCr color format is used to insert the variable size watermark. Second, Embedding of detail coefficients of LUMINANCE (Y) of watermark into the detail coefficients of CHROMINANCE (Cb & Cr) of identical frames (I-Frames) of digital video. Data is inserted into the detail coefficients in an adaptive manner based on the energy of high frequency.
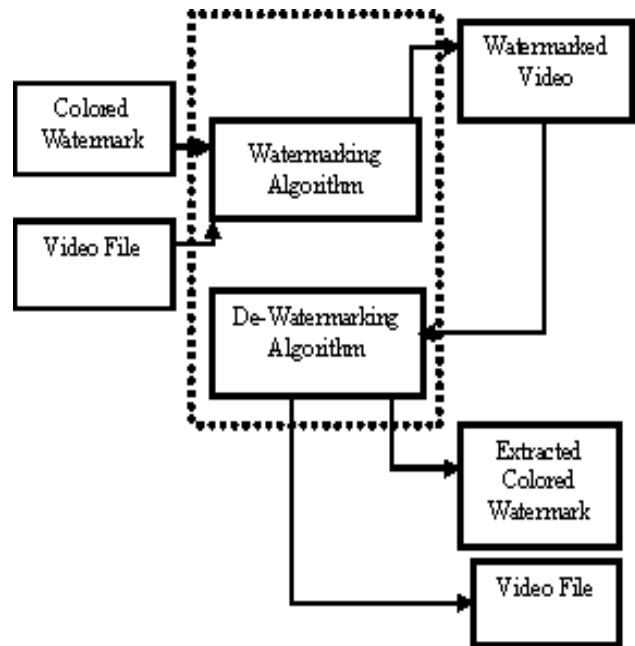

Figure 1. Block Diagram of Video Watermarking

Rest of the paper is organized as follows: In Section II, proposed scheme is illustrated which explains the embedding and extraction of watermark from video sequence. Section III shows some experimental results and evaluates the performance of the proposed technique. At the end, conclusions are drawn in Section IV and provide some future work directions.

II. PROPOSED WATERMARKING TECHNIQUE

In proposed method, A YCbCr color space model [12] is used to embed the colored watermark signal (256 x 256) in a video file to increase the imperceptibility of watermarked video and detected watermark. For embedding the colored watermark we take apart that image as in Luminance and Chrominance components. Now Only Luminance components have to be embedded inside the video file to get the high PSNR and low MSE.

Where, luminance and chrominance contains the information about the brightness and colors respectively.

For the result analysis, we have taken two video sequences, namely, 'car_race.mp4' and 'wakna_road.mp4' video sequence. After applying scene changed algorithm on these video sequences, we obtain 77 and 97 scene changed frames respectively. Before embedding the watermark inside the original media (original video), we have to preprocess the watermark and input video.
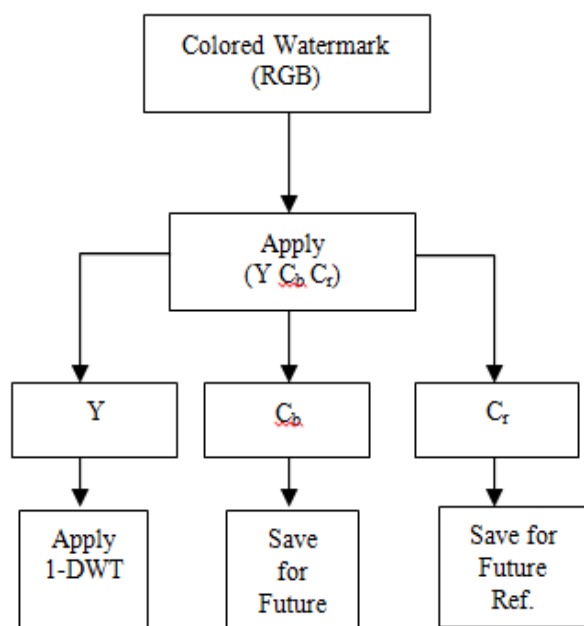
Watermark Pre-process

Figure 2. Watermark preprocesses to generate Encrypted watermark

For the process of watermark embedding, at first we have to take separately the colored watermark into YCbCr color space model. Where, Y (luminance) and Cb & Cr (chrominance) components contains the information about brightness and its color respectively.

With the aim of high-quality copyright protection, the information of watermark, which is we are embedding in original source video should be as small as possible. If the information of watermark embedding is too short, it will diminish the visual effect of watermark embedded video. As a result, the interval time should not be too small. In general, the interval time is less than 1s.

MPEG-4 video coding standard has the sequence of GOPs (group of pictures). The length of GOP entails at least one I-frame image but in the main, each GOP has 12 frames of images. These 12 frames of images includes: one I-frame, three P-frames and eight B-frames, managed as IBBPBBPBBPBB. Where I is an identical frame, P is predictive frame (that has the information of previous frame), B is Bidirectional frame (that has the information of previous frame and future frame or next frame.)

In Figure 2 we have original watermark juit.jpg and applied DWT to find out the detail and approximation coefficients. In the next step applied bit plane slicing on the watermark to convert it into 8-bit plane and for the next step place the bit plane side by side and finally decompose the image with a secret key to make it encrypted watermark. Fig. 3 is showing the preprocess action on a video file to find out those coefficients where we have to embed the watermark bits. So here we have taken a video file and applied Scene changed detection algorithm [13, 14].

After getting scene changed frames applied YCbCr color space model on each frame and then apply 2-Level DWT only on Cb and Cr components.
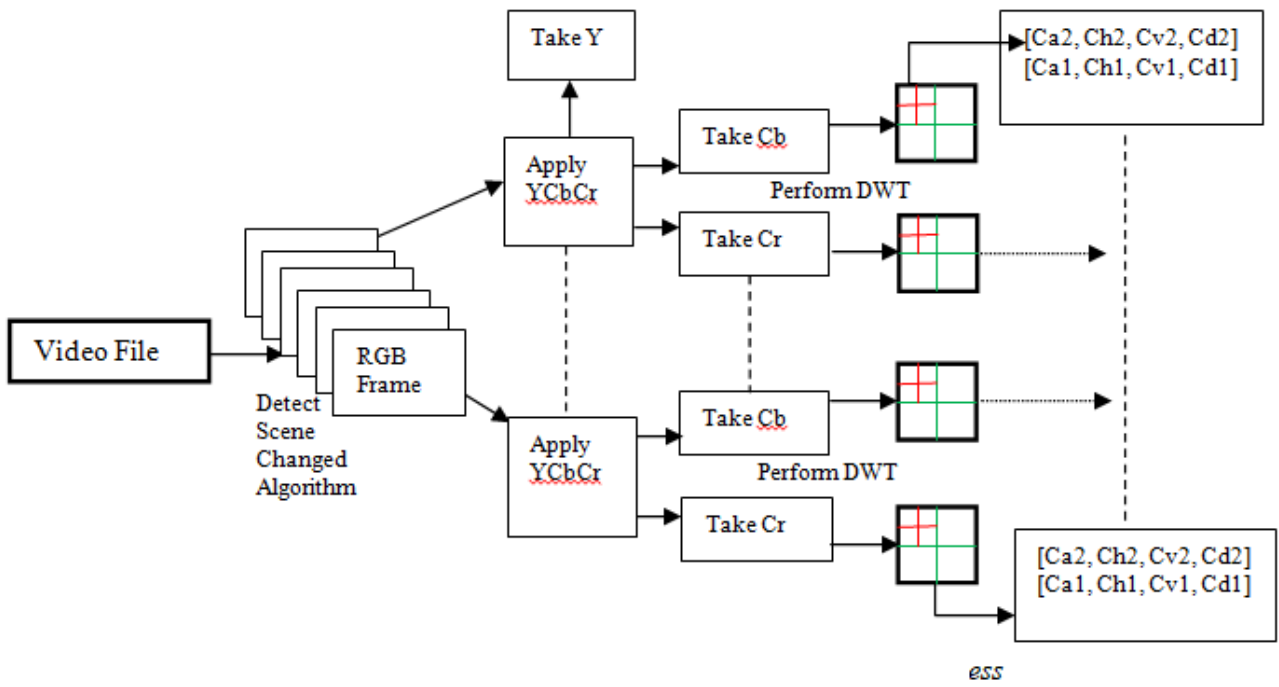
Figure 3. Video Pre-process

In Figure 3 we applied a scene changed detection algorithm [13, 14] on input video sequence and get the non-overlapping GOP (group of pictures). Each GOP has at least 1 I frame. Select that I frame with the help of identical frame selection scheme. Which said that identical frames are self dependent frames means they are not dependent on the previous (P-frames) and bidirectional (B-frames) frames.

After getting the Identical frames (I-frames) applied YCbCr color space model on each I frame. Here in the video preprocess we are not considering Luminance (Y) components and taking only Chrominance component for embedding the watermark information because luminance components having the maximum information of the frame so these components are very sensitive for embedding the watermark information.

After getting the chrominance components Cb and Cr apply 2-level DWT scheme on Cb component

only. Finally we get the target frames where we have to embed the watermark information.

Watermark embedding

1. Apply a scene changed detection algorithm [6] on the original video sequence (O_video) and then divide the each scene into non-overlapping group of pictures. Each group of pictures has an Identical frame (I). Select all I frames from input video for embedding the watermark.

$$WmI_i = k \times \left(Lf_2 \right) + q \times \left(Wm_2 \right)$$

Where

WmI_i is watermarked I frame.

Lf_2 is low frequency approximation of original frame. Wm_2 is low frequency approximation of watermark image. k & q are scaling factors.

2. Take each I-frame and apply YCbCr color format on each frame.
   Where   Y= 0.299R + 0.587G + 0.114B
            Cb = 0.564 (B − Y)

$$Cr = 0.713 \ (R - Y)$$
$$Cb + Cr + Cg = 1$$
$$Cg = 1 - (Cb + Cr)$$

3. Apply 2-level DWT on CHROMINANCE (Cb & Cr-chrominance) of each frame and store LUMINANCE (Y-luminance) for future reference.

$$DWT \ (Cb) = [Ca_i, Ch_i, Cv_i, Cd_i]_o$$
$$DWT \ (Cr) = [Ca_i, Ch_i, Cv_i, Cd_i]_o$$

Where i=1, 2.

4. Let W = Digital Watermark Color Image. Take YCbCr of RGB-frame.

5. Apply 2-level DWT on LUMINANCE component and get detail coefficients of LUMINANCE .

$$DWT \ (Y) = [Ca_i, Ch_i, Cv_i, Cd_i]_w$$

Where i= 1, 2.

6. To embed the watermark in each I-frame, add detail coefficients of LUMINANCE of watermark with the detail coefficients of CHROMINANCE of I-frame of original video.

Now, for Cb

$$[Mod \ Ch_i]_{Cb} = [Ch_i]_o + [Ch_i]_w$$
$$[Mod \ Cv_i]_{Cb} = [Cv_i]_o + [Cv_i]_w$$

Now, for Cr

$$[Mod \ Ch_i]_{Cr} = [Ch_i]_o + [Ch_i]_w$$
$$[Mod \ Cv_i]_{Cr} = [Cv_i]_o + [Cv_i]_w$$

Where i= 1, 2.

7. Now, mod Ch_i and mod Cv_i are the modified coefficients of CHROMINANCE of watermark inserted identical frame.

8. Take IDWT of watermark inserted CHROMINANCE components of identical frames. Finally, get the modified CHROMINANCE (mod Cb and mod Cr) of I-frame.

9. Take LUMINANCE (Y) from step-2 and add this with the modified CHROMINANCE (mod Cb and mod Cr) and get watermark inserted I-frame. Convert YCbCr format to RGB.

10. Combine all the watermark inserted I-frame with the remaining frames and get watermarked video for transmission/braodcasting.

Watermark detecting

1. Apply a scene changed detection algorithm [6] on the watermarked video sequence (W_{video}) and then divide the each scene into non-overlapping group of pictures. Each group of pictures has an Identical frame (I). Select all I frames from input watermarked video for detecting the watermark.

2. Take the watermarked frame (W_f) (Identical frame) and original identical frames (I_i). Apply YCbCr color format on both.

3. Apply DWT of CHROMINANCE of both watermarked frame and identical frames.

4. Subtract detail coefficients of CHROMINANCE of watermarked frame from the detail coefficients of original I-frame which are mod Ch_i, mod Cv_i, Ch_i and Cv_i respectively.

Now, for Luminance

$$[NewCh_i]_{dw} = [mod \ Ch_i]_{ew} - [Ch_i]_o$$
$$[NewCv_i]_{dw} = [mod \ Cv_i]_{ew} - [Cv_i]_o$$

Where i= 1, 2.

5. Take IDWT of detail coefficients of detected LUMINANCE and add this detected LUMINANCE with the original CHROMINANCE and get the YCbCr format of detected watermark.

6. Calculate cross correlation between new values of detected watermark and the original watermark.

7. If correlation = high

Then, Stop the execution. Detected watermark is similar to original watermark.
else
Take both detail coefficients together and repeat from step 3 (initially i=1 and in repetition process the value of i=2).
Else if

Take 2-level detail coefficients and repeat from step 3 until the detected watermark will get similarity with original watermark.

else
Watermark not found.

Figure 4 shows the procedure of embedding the watermark on to the video. Video sequence taken and applied scene change detection algorithm to get the identical frames. After extracting the scene changed frame, YCbCr color space model was introduced on each identical frame.
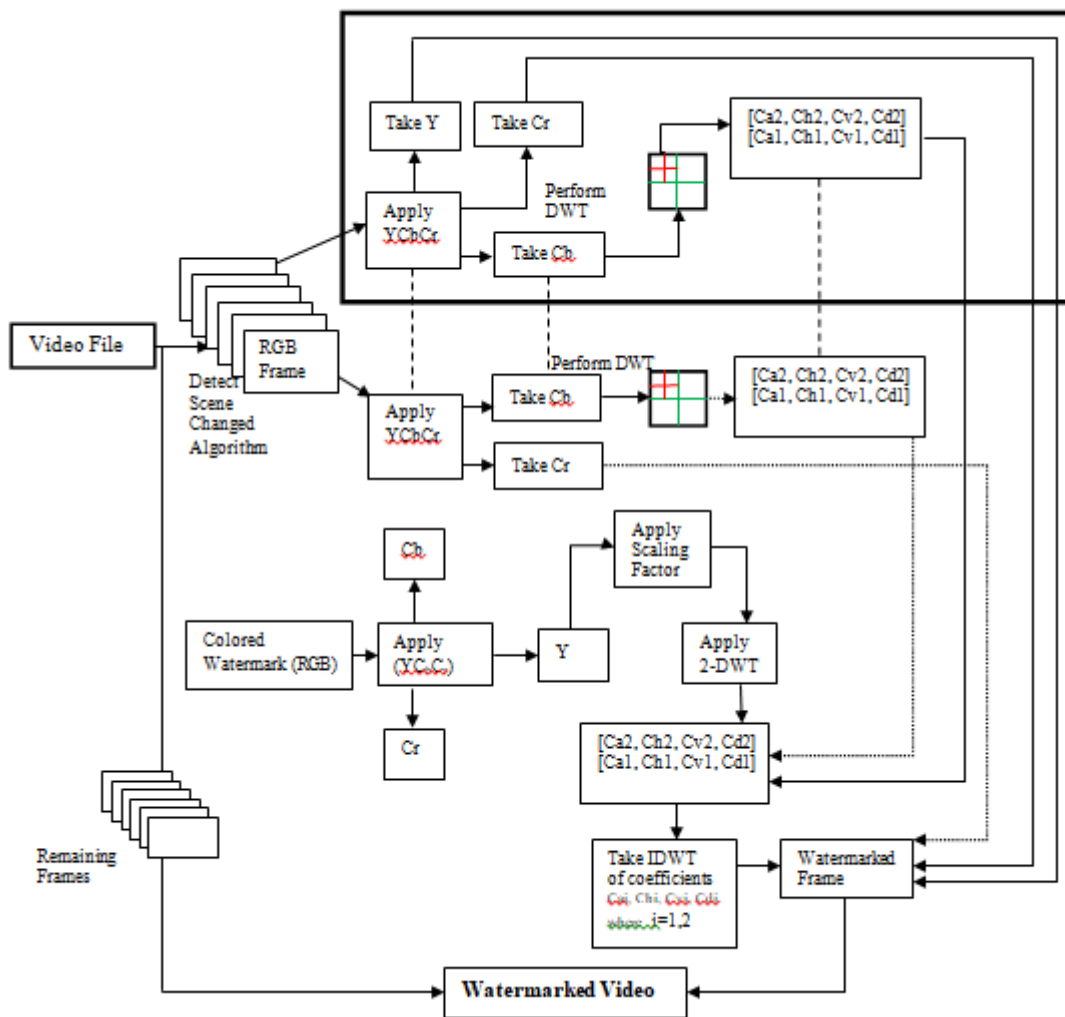
Figure 4. Watermark embedding process

In this color space model Y represent Luminance and CbCr represents chrominance, where Luminance depicts the information of brightness and CbCr about color of the frame. Blue chroma (Cb) was taken and applied with 2-level DWT (Discrete Wavelet Transform).

For the next process of embedding the watermark in to the video, colored watermark was taken and applied YCbCr. Now by HVS (Human Visual System) [15] indicated that Luma (Y) Component has the maximum information of the watermark. So, firstly scaling factor was applied on the Matrices of Luma to

reduce the size of the matrices and then applied a 2-level DWT [16-18]. Then the coefficients of blue chroma of original frames were merged with the coefficients of Luma of watermark. Lastly, inverse of Discrete Wavelet Transform was applied and added to the luma and Cr of the original frame with the merged coefficients.

III. EXPERIMENTAL RESULTS AND ANALYSIS

To implement this technique we have used original video 'wakna road' and 'car race' at the dimension of 320 x 240 and 640 x 360 respectively and the size of original watermark image is 256 x 256. Figure 5, 6 & 7 shows original video frames (wakna road, car race and foreman respectively) and their YCbCr components. Figure 8 shows original watermark image and its YCbCr components. The value of scaling factor k is varied from 0.2 to 0.6 for embedding the watermark into the original video frame and q will be 0.6 to 1.0 for all frames. Where 'k' is used for luminance (Y) of original watermark and 'q' is used for chroma (Cb) of original video frame.

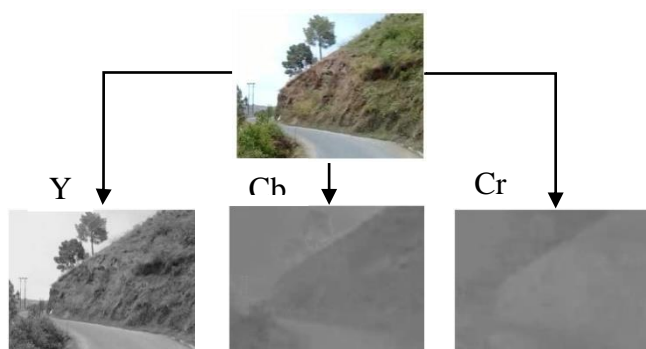When 'k' is 0.3 and 'q' is 0.6 we get the adequate result for embedding and extracting process also.

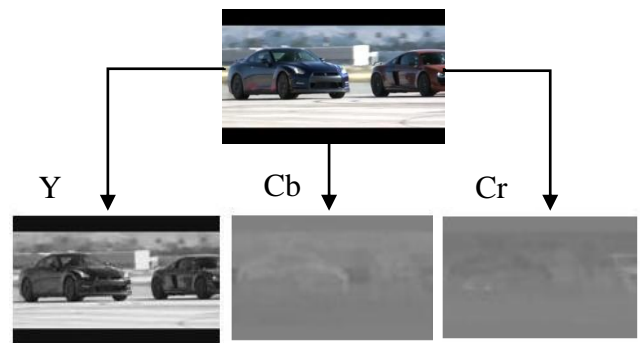**Figure 5.** Wakna road original video frame and its YCbCr color components

Figure 6. Car race original video frame and its YCbCr color components
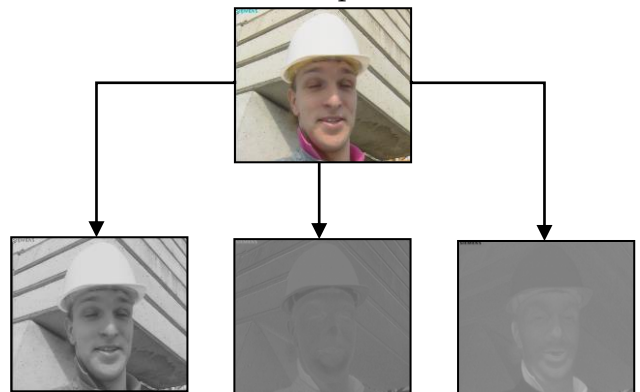

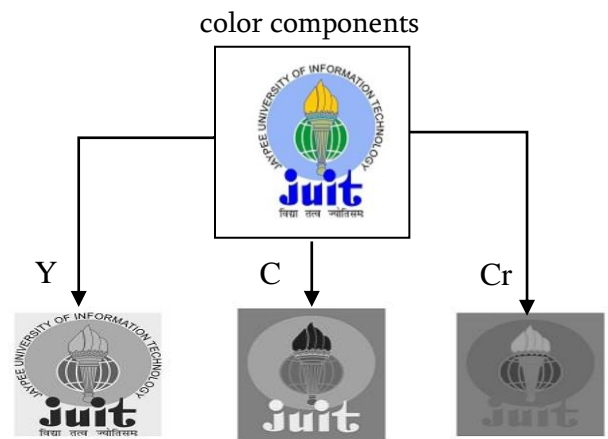**Figure 7.** Foreman original video frame and its YCbCr color components

Figure 8. Original watermark and its YCbCr color components.

Embedding watermark into I-frame is more suitable and robust because I frame is independent and it has its own information only. The watermark embedding algorithm based on I-frame, entrenches watermark only in I-frame but simultaneously it guarantees the knowledge of embedded watermark to each GOP.

In Figure 9 we have explain the module of 2-level 'haar' discrete wavelet transform. In this figure we have 4 images, in which the lower right corner is having de-composition image and this is showing low frequency and high frequency parts of original watermark. We have chosen the 2-level low frequency image as the watermark because as we can see in this figure this part is having the maximum information of the original image.

In Figure 10. We have shown the procedure of embedding and extraction of the watermark. Here in this figure we have taken an original video frame and luma part of original watermark. After embedding the watermark we add some noise in watermarked frame. After extraction of watermark we add the original Cb&Cr of original watermark with the extracted watermark and we get a good quality watermark with the PSNR of 46.22.
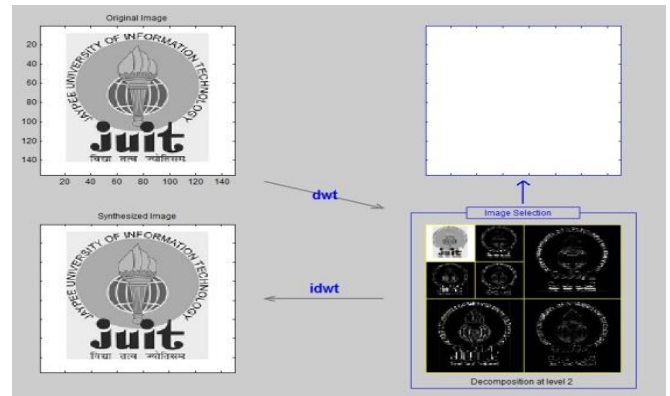

Figure 9. 2-Level DWT of Luma (Y) of original watermark.
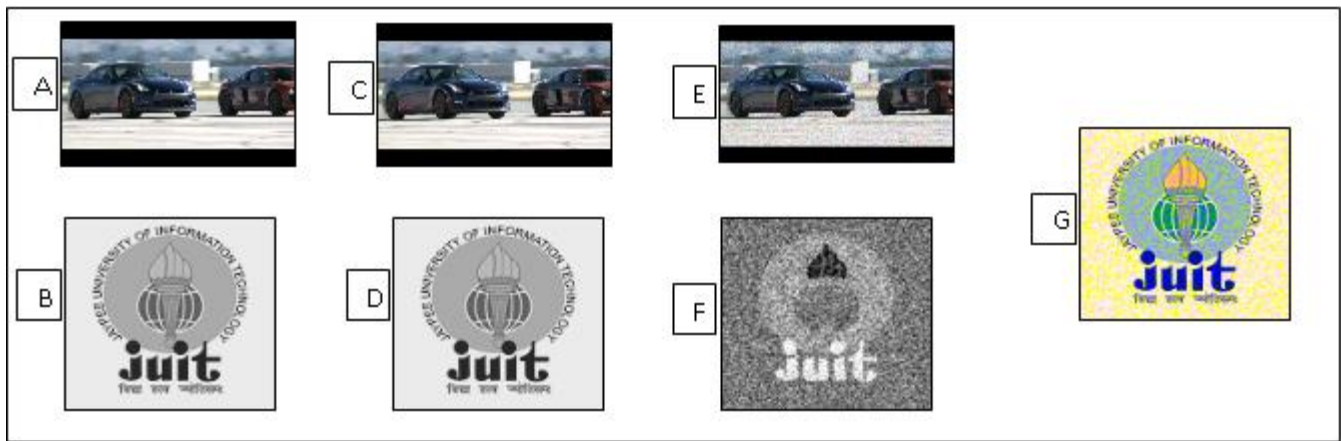

Figure 10. Watermark extraction

(A)Original Car race frame (B) Original luma of colored watermark (C) Watermarked Car race frame (D) Extracted Watermark (E)Noisy watermarked car race frame (F) Extracted watermark from noisy frame (G)Added (Cb & Cr) of original watermark with extracted watermark
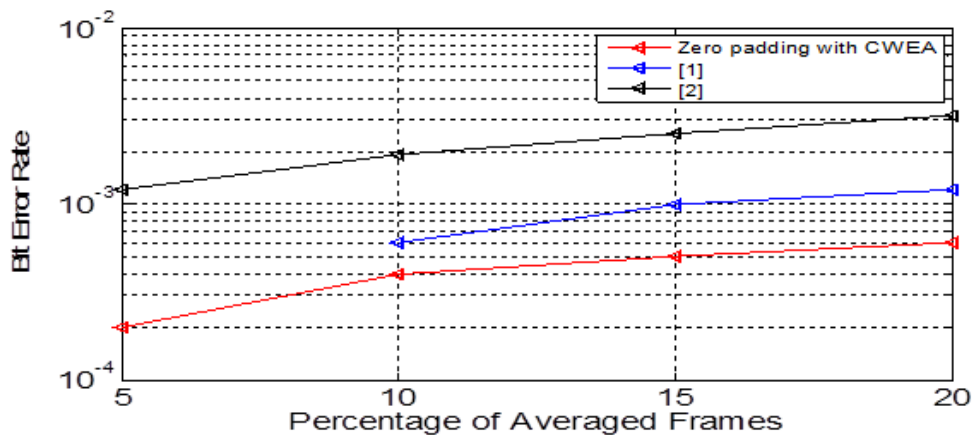

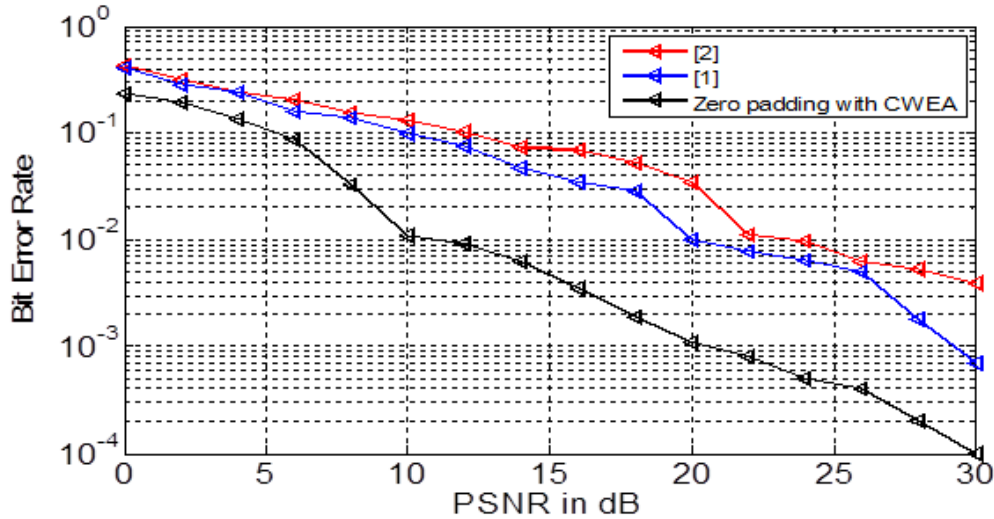**Figure 11.** BER (log scale) under temporal attack (Frame Averaging)

Figure 12. BER (log scale) under spatial attack (Uniform noise)

In figure 11 we have shown the results against temporal attack (Frame Averaging). Where BER (log scale) on x-axis and percentage of averaged frames on y-axis are showing the result graph and a red indicator is showing our results. In figure 12 we have shown the results against spatial attack (Uniform Noise). Where BER (log scale) on x-axis and PSNR on y-axis are showing the result graph and a black indicator is showing our results. In figure 13 we have shown the averaged PSNR of car race video after embedding the watermark in all I-frames.

IV. CONCLUSION

The proposed approach is more proficient because the quality of extracted watermark is better than A.K. Verma et. al. in "Robust Temporal Video Watermarking using YCbCr Color space in Wavelet Domain" in terms of PSNR and BER. We have taken Cb of the video frame for embedding the watermark because, as per HVS (Human Visual System), we cannot identify the changes in Cb (Blue chroma) because of its low resolution. Compression attack will not degrade the quality of the embedded watermark because we embed the same watermark at every scene changed frame so at the time of extraction we can extract that watermark from the couple of frames

and finally collect the entire extracted watermark and find out the best possible pattern on the basis of image collaboration technique. Secondly, we added the (Cb & Cr) of original watermark with extracted watermark image that is giving a best quality of extracted watermark. Thirdly, it is hard to know the spot where it is inserted, because it is inside the blue chroma (Cb). Another advantage of this technique is that the quality of the watermarked video also will not degrade because we have embedded the watermark inside the blue chroma (Cb) that has a very low sensitivity. Video watermarking is an essential need of copyright protection and a lot of research is still going on to find out the new methods for security and privacy of the multimedia contents. Current methods for video copyright protection techniques are extended form of image watermarking and there is a great scope of innovation. Research can be carried out to establish new strategies for digital video copyright protection.

V. REFERENCES

[1]. C. Langlaar, et al, "Watermarking Digital Image and Video Data", in IEEE Signal Processing Magazine, September 2000.

[2]. I. J. Cox, et al, "Digital Watermarking and Steganography," in 2nd ed. San Mateo, CA, USA: Morgan Kauffman, 2008.

[3]. T. Al-Khatib, et al, "A Robust Video Watermarking Algorithm," in Journal of Computer Science, 4(11):6~9.1280, 2004.

[4]. Wang, Y., et al, "A Blind MPEG-2 video watermarking robust against geometric attacks: a set of approaches in DCT domain," in IEEE Trans. Image Process, 15(6), 1536–1543, 2006.

[5]. Lin, et al, "An embedded watermark technique in video for copyright protection," in Proc. Int. Conf. Pattern Recog. 4, 795–798, 2006.

[6]. J. Shieh, et al, "A semi-blind digital watermarking scheme based on singular value decomposition," In Computer Standard International, vol. 28, no. 4, pp. 428–440, Apr. 2006.

[7]. H. Khalilian, et al, "Multiplicative video watermarking with semi- blind maximum likelihood decoding for copyright protection," in Proc. IEEE Pacific Rim Conf. Commun., Comput. Signal Process, pp. 125–130, Aug. 2011.

[8]. S. Gandhe, U. Potdar, and K. Talele, "Dual watermarking in video using discrete wavelet transform," in Second International Conference on Machine Vision, ICMV '09, pp. 216 –219, Dec. 2009

[9]. A. Murshid, et al, "Blind compressed video watermarking in DCT domain robust against global geometric attacks. Proceeding of the International Cryptology Workshop and Conference, 2008.

[10]. S. Bhattacharya, T. Chattopadhyay, and A. Pal, "A survey on different video watermarking techniques and comparative analysis with reference to h. 264/avc," in IEEE Tenth International Symposium on Consumer Electronics, ISCE'06. IEEE, pp. 1–6, 2006.

[11]. J. Y. Park, J. H. Lim, G. S. Kim, C. S. Won, "Invertible Semi-fragile Watermarking Algorithm Distinguishing MPEG-2 Compression from Malicious Manipulation", in International Conference on Consumer Electronics, pp. 18-19, June 2002.

[12]. A. K. Verma, M. Singhal, C. Patvardhan, "Robust Temporal Video Watermarking Using YCbCrColor Space in Wavelet Domain", In 3rd IEEE International Advance Computing Conference (IACC), 978-1-4673-4529, Dec. 2013.

[13]. B. Yeo, et al, "Rapid scene change detection on compressed video," in IEEE Trans. Circuits Syst. Video Technol., vol. 5, no. 6, pp. 533–544, Dec. 1995.

[14]. B Shahraray "Scene Change Detection and Content-Based Sampling of Video Sequences," in SPIE 2419 (Digital Video Compression: Algorithms and Technologies): 2–13, 1995.

[15]. Y.Yang, M. Yang, S. Huang, "Multifocus Image Fusion Based on Extreme Learning Machine and HumanVisual System" in IEEE Access Volume:PP, Issue: 99Pages: 1-1, 2017

[16]. E. Ganic, Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies," In Proceedings of the ACM Multimedia and Security Workshop, pp. 166–174, 2004.

[17]. X. Niu, S. Sun, "A new wavelet-based digital watermarking for video," In Proceedings of the IEEE Digital Signal Processing Workshop, pp. 1–6. Texas, 2000.

[18]. F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," in Signal Process., vol. 66, no. 3, pp. 283–301, May 1998.