CWEA: A Digital Video Copyright Protection Scheme

Jabir Ali\(^1\), Satya Prakash Ghrera\(^2\)

\(^1\)Jaypee University of Information Technology, Waknaghat, Solan, HP, 173234, India
Jabirali.cse@gmail.com

\(^2\)Jaypee University of Information Technology, Waknaghat, Solan, HP, 173234, India
sp.ghrera@juit.ac.in

Abstract: Digital Watermarking is an important method of protecting the intellectual property and copyright of the digital media. 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-luminance) of the watermarked image detail coefficients of CHROMINANCE (Cb and Cr- chrominance) 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. A number of tests have been executed 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 the 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 for 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 the 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 [1-3]. 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 degraded 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 the 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 the 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 the inserted watermark. In this paper, we have improved the robustness and security of inserted digital pattern or watermark and transparency of watermarked media. TABLE I has shown the classification of watermark system.

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

Table 1. Classification of watermark system.

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 the 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 the de-watermarking algorithm to 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 the 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, the proposed scheme is illustrated which explains the embedding and extraction of the watermark from a 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 the 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 contain 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.

A. Watermark Pre-process

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 contain 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 GOP (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 include: one I-frame, three P-frames, and eight B-frames, managed as IBBPBBPBBPBB. Where ‘I’ is an identical frame, ‘P’ is a predictive frame (that has the information of previous frame), and ‘B’ is a bidirectional frame (that has the information of previous frame and future frame or next frame.)

In Fig.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 the 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 an 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.

B. Video Pre-process

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 contain 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 GOP (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 include: one I-frame, three P-frames, and eight B-frames, managed as IBBPBBPBBPBB. Where ‘I’ is an identical frame, ‘P’ is a predictive frame (that has the information of previous frame), and ‘B’ is a bidirectional frame (that has the information of previous frame and future frame or next frame.)

In Fig.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 the 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 an 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.
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.

C. Watermark embedding

1. Apply a scene changed detection algorithm [6] on the original video sequence (O_video) and then divide each scene into a 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.

\[ W_{ml} = k \times (L_{f_2}) + q \times (W_{ml}) \]

Where

\[ W_{ml} \] is watermarked I frame.

\[ L_{f_2} \] is low-frequency approximation of original frame. \( W_{ml} \) 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.

   \[ \text{DWT (Cb)} = [Cai, Chi, Cvi, Cdi]_o \]
   \[ \text{DWT (Cr)} = [Cai, Chi, Cvi, Cdi]_o \]

   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.

   \[ \text{DWT (Y)} = [Cai, Chi, Cvi, Cdi]_w \]

   Where i=1, 2.

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

   Now, for Cb
   \[ [\text{Mod \ Chi}]_{Cb} = [\text{Chi}]_o + [\text{Chi}]_w \]
   \[ [\text{Mod \ Cvi}]_{Cb} = [\text{Cvi}]_o + [\text{Cvi}]_w \]

   Now, for Cr
   \[ [\text{Mod \ Chi}]_{Cr} = [\text{Chi}]_o + [\text{Chi}]_w \]
   \[ [\text{Mod \ Cvi}]_{Cr} = [\text{Cvi}]_o + [\text{Cvi}]_w \]

   Where i=1, 2.

7. Now, mod Chi and mod Cvi are the modified coefficients of CHROMINANCE 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 the watermarked video for transmission/broadcasting.

D. Watermark detecting

1. Apply a scene changed detection algorithm [6] on the watermarked video sequence (W_video) and then divide each scene into the 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_i) (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 Cb, mod Cvi, Chi and Cvi respectively.

   Now, for Luminance
   \[ [\text{NewCh}]_{iw} = [\text{mod \ Chi}]_{iw} - [\text{Chi}]_o \]
   \[ [\text{NewCvi}]_{iw} = [\text{mod \ Cvi}]_{iw} - [\text{Cvi}]_o \]

   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 the detected watermark.

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

7. If correlation = high

Then, Stop the execution. Detected watermark is similar to the 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 the original watermark.

else

Watermark not found.

Fig.4 shows the procedure of embedding the watermark on to the video. Video sequence was 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.

In this color space model Y represent Luminance and CbCr represents chrominance, where Luminance depicts the information of brightness and CbCr about the 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 into the video, the colored watermark was taken and applied with 2-level 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 to 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 the watermark. Lastly, the 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 the original watermark and ‘q’ is used for chroma (Cb) of the 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

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 that entrenches the watermark only in I-frame but simultaneously it guarantees the knowledge of embedded watermark to each GOP.

In Figure 9 we have explained the module of 2-level ‘haar’ discrete wavelet transform. In this figure, we have 4 images, in which the lower right corner is having a decomposition 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 the watermarked frame. After extraction of the 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 8.** Original watermark and its YCbCr color components.

**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) 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 the x-axis and percentage of averaged frames on the y-axis are showing the resulting 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 the y-axis are showing the resulting 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.

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 a 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 the original watermark with extracted watermark image that is giving the 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 for 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 for innovation. Research can be carried out to establish new strategies for digital video copyright protection.

References


Author Biographies

Jabir Ali received the B.Tech degree in Information Technology from Invertis Institute of engineering & technology, Bareilly in 2009, and M.Tech degree in Computer Science & engineering from Jaypee University of Information Technology, Solan, India, in 2011 and he joined Translam institute of technology & management in 2011 and Sunderdeep Group of colleges as an Assistant Professor in 2012. In 2013, he joined the Jaypee university of information Technology, Waknaghat Solan, India, where he is currently pursuing Ph.D. degree. His current working domain is Image and Video copyright protection. His research interest includes image security, Video watermarking, Signal Processing and Network Security.

Professor Satya Prakash Ghera received the B.Sc (honors) degree in electronics from Regional engineering college, Kurukshetra (now NIT) in 1971, and the ME (Honours) in Computer Science from Thapar Institute of engineering and Technology, Patiala in 1995 and Ph.D. in Computer Science & engineering in 2012. Currently, he is HOD and Professor in the Computer Science and engineering department. He is the reviewer of many reputed journals. He Served in Indian Army as a brigadier. He was awarded Commendation Card during Jan 2004 for exemplary work in Computer Training and IT infrastructure management. He Was awarded Commendation Card during Jan 88 for exemplary work in development of computer software (MIS for Army).