Keywords: Video watermarking, Human vision system, Patchwork algorithm, 3D-DWT.

Abstract: The digital watermarks have recently been recognized as a solution for protecting the copyright of the digital multimedia. In this paper, a new method for video watermarking with high transparency based on 3D-DWT is proposed. This algorithm is implemented on the basis of Human Vision System (HVS). By using the patchwork methods in Discrete Wavelet Transform (DWT) domain, this algorithm is robust against different attacks such as frame dropping, frame swapping, frame averaging, median filtering and MPEG-2 video encoding. The experimental results show that the embedded watermark is robust and invisible. The watermark was successfully extracted from the video after various attacks.

1 INTRODUCTION

In recent decade, information watermarking in digital environment has attracted much interest because of its ability in covering different aims. Considering the high volume of video products in recent years, special attention is focused on this type of technology. Information watermarking is embedment of a hidden message within another signal. This signals named cover signal can be text, digital image, audio or video file. Watermarking follows different aims such as authentication, reserving right of author, copy right and control of data spreading, amongst others.

Three challenges exist in the field of watermarking. In this process, data embedding must be done in such a manner that watermarked signal keeps its transparency. On the other hand, the signal including hidden information may be exposed under different processes such as filtering, geometric transformation, adding noise, etc and after these transformations, hidden message can be extractable. This significant feature is called watermarking system robustness.

With regard to application of watermarking in video signals, high robustness in related algorithms is a primary necessity. Another important challenge in these systems is capacity. Capacity is by definition the amount of information that can be put on host signal while preserving its transparency and robustness.

Many algorithms have been proposed for video watermarking. First and foremost algorithm is Hartung method (Harung, Girod, 1998). This method is based on spread spectrum algorithms and is executable on uncompressed and compressed video signals. In addition to this method, various algorithms have been considered to do watermarking on uncompressed and compressed video signals like data embedding in 3D-DCT domain (Park, Lee, and Moon, 2006) and 3D-DWT (Angiang, Jing, 2007) for uncompressed video. There are other patterns in which watermarking algorithms related to still images are used and motion characteristics of video have been used as parameters to modify presented designs.

Patchwork algorithm was used for the first time in image watermarking implemented on the basis of comparison of two groups average, variance or other signal properties (Yeo, Kim, 2003). This method has been used in different transformation fields such as DCT and DWT. (Kii, Onishi, Ozawa, 1999),
\[
F(U,V,W) = \frac{1}{2\sqrt{2}} C(U)C(V)C(W) \left[ \sum_{X=0}^{L-1} \sum_{Y=0}^{L-1} f(x,y,z) \cos \left( \frac{(2x+1)\pi}{L} \right) \right]
\]

(OSlucjak, Vargic, 2004). Patchwork algorithm in audio watermarking shows a relatively high performance leading to the high attack resistance (Khademi, Akhaee, Ahadi, Amindavar, 2009). In this paper, the patchwork algorithm is used for video watermarking based on the 3D-DWT domain (Anqiang, Jing, 2007).

2 WATERMARK EMBEDDING PROCESS

Fig. 1 shows a block diagram of the watermark embedding process in an original video signal.

2.1 Selecting of N Cube based on HVS

First, the input video signal is divided into cubes of L*L*L. Then, according to HVS, N cubes are chosen (Fig. 2).

This choosing criterion is used as a secret key to increase algorithm security. The best position for hiding watermark in video signal is where human eye is less sensitive. Human eye has two fundamental weak points:
1) Human eyes can not see details on the fast moving object
2) Human eyes are not sensitive to the distortion in the complex or high connectivity texture region

These two features can be extracted from the video signal by 3D-DCT transformation according to equation (1):

\[
\begin{align*}
C(U), C(V), C(W) & \text{ are constants. After applying equation 1 on cubes of } L^*L^*L, \\
\text{the amount of texture and objects movement are obtained by equation 2.}
\end{align*}
\]

\[
\begin{align*}
E_T = E_{T,U,V,W} & \quad \text{for } 1 \leq K \leq (L^*L^*L) \\
E_M = E_{M,U,V,W} & \quad \text{for } L^*L^*L \leq K \leq L^*L^*L
\end{align*}
\]

N is the cube number and k is pixel number inside that cube. According to equation (2), \( E_T \) is texture amount and \( E_M \) is amount of object movement inside the cube. A change in \( E_T \) and \( E_M \) results in a change in the secret key and also an increase in these parameters causes the transparency to improve and the capacity to decrease and vice versa.

2.2 3D-DWT Transformation of Selected Cubes

There are two main methods for 3D-DWT Transformation:
1) 2D-DWT transform other each frame of cube, then 1D-DWT transform from each pixel row (Huang-yu, Ying, Cheng-ke, 2004).
2) 1D-DWT transform from each pixel row of cube, then 2D-DWT transform other each frame of cube.

In the present study, the first method has been applied. Each frame was transformed into a 2D-DWT with 3 levels and Haar filter. Then each pixel row was transformed to a 1D-DWT with 3 levels using Haar transform (Fig 3).

![Figure 2: Dividing video signal to cubes of L*L*L.](image1)

![Figure 3: 3D-DWT with 3 levels and Haar filter.](image2)
2.3 Watermark Embedding by Patchwork Method

In this step, watermark is embedded to LLLH and LLHL windows forming median frequency. By embedding watermark in this window, watermarked signal becomes robust to averaging and median filtering attacks. First, adjacent row pairs are chosen and variance of each of them is determined (Fig. 4).

![Figure 4: Median frequency window.](image)

As seen in Fig. 5, for watermarking LLL1 and LLL2 are used.

![Figure 5: LLL1 and LLL2 from LLL window.](image)

Watermarking is explained by the following algorithm:

\[
\begin{align*}
    &\text{If } m = 0 \\
    &\text{LLL1} = (\text{LLL1} + \text{LLL2}) / 2 + TH; \\
    &\text{LLL2} = (\text{LLL1} + \text{LLL2}) / 2 - TH; \\
    &\text{Else} \\
    &\text{LLL1} = (\text{LLL1} + \text{LLL2}) / 2 - TH; \\
    &\text{LLL2} = (\text{LLL1} + \text{LLL2}) / 2 + TH;
\end{align*}
\]

M is the watermark bit and TH is the threshold limit of algorithm, by increasing TH, transparency of video signal decreases while resistance against frame dropping and frame swapping attack increases. On the other hand decreasing TH increases the PSNR of the video signal and decreases the signal resistance against aforementioned attacks.

2.4 Formation of Video Watermarked

After embedding watermark, video signal is reconstructed. To do this, first, each pixel row was transformed to a 1D-IDWT with 3 levels and Haar filter, and then each frame was transformed to a 2D-IDWT with 3 levels and Haar filter. At the end, all cubes are combined together to form the watermarked video.

3 WATERMARK EXTRACTING PROCESS

Fig. 6 shows block diagram of watermark extracting from watermarked video.

![Figure 6: Watermark extracting process.](image)

As seen in Fig. 6, first the watermarked video signal is divided into cubes of L*L*L. Then, N cubes are chosen according to secret key formed in watermark embedding step. Afterwards, each cube is transformed by a 3D-DWT with 3 levels and Haar filter as mentioned in section 2.2. Adjacent pairs of pixel rows of two LLLH and LLHL windows are compared from variance point of view. The row with higher variance is chosen. According to the following algorithm, watermark is extracted by comparison of LLL1 and LLL2.

\[
\begin{align*}
    &\text{If } \text{LLL1} \geq \text{LLL2} \\
    &m = 0; \\
    &\text{Else} \\
    &m = 1;
\end{align*}
\]

4 EXPERIMENTAL RESULTS

In this experience 16*16*16 cubes are used and amount of TH (embedding watermark threshold) is 40. The video sequences used in the experiments include foreman and Stefan. The size of each frame is 352x288. It is necessary to mention that to stand up against MPEG-2 encoding attack; each class includes I-Frames (Simitopoulos, Tsaftaris and...
Boulgouris, 2002). The embedded watermark signature is a binary image (size 60x20 pixels), shown in Fig.8 (a).

![Original video frame](image1)

![Watermarked video frame](image2)

Figure 7: Original and watermarked video frame.

An original frame from each video is shown in Fig.7 (a). The corresponding watermarked frame for each is shown in Fig.7 (b). Figure 8(b) and (c) shows the watermark image after extracting from foreman and Stefan sequences.

![Original image](image3)

![Watermarked image](image4)

Figure 8: Original watermark and extracted watermark.

PSNR (peak signal to noise ratio) is one commonly objective in perceptual quality measure. PSNR is defined as:

$$PSNR = 10 \cdot \log 10\left( \frac{255^2}{MSE} \right)$$

In this equation, mean squared error (MSE) is formulated as:

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left| X(i, j) - X'(i, j) \right|^2$$

Where, X's are the coefficients of the original video and X'’s are the coefficients of the watermarked video. M and N stand for the height and width of the image, respectively.

In order to evaluate the performance of the watermarking algorithm objectively, BER (Bit Error Rate) and NC (Normalized Cross-Correlation Function) are introduced.

$$BER = \frac{1}{M} \sum_{i=0}^{M-1} \left\{ \frac{1}{N} \sum_{j=0}^{N-1} \left[ w_i \neq w'_i \right] \right\}$$

$$NC(W, W_0) = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} w(i, j) w'_i(i, j)}{\sqrt{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} w^2(i, j) \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} w'^2(i, j)}}$$

In equation (5), w is the extracted watermark, and w is the original watermark. In equation (6), w(i, j) denotes the original watermark image, and w'(i, j) denotes the extracted watermark image.

Without any attack, the experimental results are shown in Table.1. The extracted watermark signature is obviously similar to the original watermark.

In order to test the robustness of this watermarking scheme, a set of attack experiments were performed.

4.1 Median Filtering Attack

The system performance against 3*3 median filtering is shown in Table.1.

4.2 Frame Averaging Attack

Frame averaging is another significant attack to the video watermark. In this experiment, we use the average of current frame and its two nearest neighbours to replace the current frame which are formulated as:

$$f_k(x, y) = \frac{f_{k-1}(x, y) + f_{k+1}(x, y) + f_{k+2}(x, y)}{3}$$

Experimental results are shown in Table 1.

4.3 Lossy Compression

The MPEG lossy compression is one of the most basic attacks to video watermark. Table 1 shows the results after MPEG-2 Lossy compression.

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Foreman</th>
<th>Stefan</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Attack</td>
<td>0.9965</td>
<td>0.9945</td>
</tr>
<tr>
<td>Median Filtering</td>
<td>0.9632</td>
<td>0.9576</td>
</tr>
<tr>
<td>Averaging</td>
<td>0.9557</td>
<td>0.9527</td>
</tr>
<tr>
<td>MPEG2</td>
<td>0.9288</td>
<td>0.9189</td>
</tr>
</tbody>
</table>
4.4 Frame Dropping and Frame Swapping Attack

Frame dropping and swapping are very simple and common attacks because of data redundancy. To investigate the robustness of the proposed method against these kinds of attacks, extraction of the watermark after dropping and swapping different rates of frames in the video clips was performed. Experimental results are shown in Table 2.

Table 2: Results after frame dropping and frame Swapping attack.

<table>
<thead>
<tr>
<th></th>
<th>1/32</th>
<th>1/16</th>
<th>1/8</th>
<th>1/4</th>
</tr>
</thead>
<tbody>
<tr>
<td>forman</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dropping</td>
<td>0.9878</td>
<td>0.9745</td>
<td>0.9588</td>
<td>0.9398</td>
</tr>
<tr>
<td>Swapping</td>
<td>0.9912</td>
<td>0.9813</td>
<td>0.9722</td>
<td>0.9532</td>
</tr>
<tr>
<td>Stefan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dropping</td>
<td>0.9897</td>
<td>0.9867</td>
<td>0.9689</td>
<td>0.9478</td>
</tr>
<tr>
<td>Swapping</td>
<td>0.9932</td>
<td>0.9889</td>
<td>0.9713</td>
<td>0.9529</td>
</tr>
</tbody>
</table>

According to the above experimental results, the watermarking scheme is robust against a variety of common video processing attacks such as median filtering, frame averaging, frame dropping, frame swapping and MPEG2 lossy compression. The extracted watermark is highly similar to the original watermark.

This method is compared with non-blind method (X. Niu, shenghe Sun, 2000) and blind method (A. Essaouabi, E. Ibnelhaj, 2009) for Stefan sequences. Figure 9.(a) and (b)

5 CONCLUSIONS

This paper presented semi-blind video watermarking based on wavelet transform. By using the secret key in embedding algorithm, this algorithm has high security. Image that is used as a watermark is a binary image. Procedure of this method includes video processing, video embedding and video detection that are described in details. This method is a powerful method against attacks such as frame averaging, frame swapping, frame dropping, median filtering and MPEG2 lossy compression.

REFERENCES