Authentication and Copyright Protection Scheme for H.264/AVC and SVC

SU-WAN PARK AND SANG UK SHIN
Department of Information Security Graduate School
Pukyong National University
Busan, 608-737, Korea

This paper proposes an authentication scheme based on fragile watermarking as well as a copyright protection (CP) scheme based on non-blind watermarking for H.264/AVC and SVC. The proposed authentication scheme uses the intra prediction modes and the inter prediction modes which are optimized for blocks as watermark for authentication, and the watermark thus generated is embedded into the quantized coefficients that satisfy a given condition. This scheme offers low running time in the H.264 encoding/decoding process, but it has a little increased ratio permissible in the bit-rate. The proposed CP scheme inserts a watermark of the owner into the DCT domain of I-frames that are divided into $4 \times 4$ blocks of uncompressed content. Our CP scheme provides robust watermark not only in the content to which fragile watermarking is applied but also in the content which is re-encoded and modified as intended. Moreover, the proposed Authentication and Copyright Protection Scheme offers low computational complexity as well as low degradation of video quality.

Keywords: authentication, watermarking, copyright protection, H.264/AVC, H.264/SVC

1. INTRODUCTION

Content authentication and copyright protection are drawing much attention in the field of digital contents protection. These applications mainly use the digital watermarking schemes that describe techniques to embed the watermark into digital data. The watermarking schemes are divided into the robust, semi-fragile and fragile watermarking according to the embedding purpose. While robust watermarking is usually used for CP to insist on the ownership of the contents, fragile or semi-fragile watermarking are adopted for authenticating digital video for its integrity.

Most digital video contents are distributed and stored in the form of compressed bitstream even though the network bandwidth and the storage capacity are increasing. Currently, MPEG-2, MPEG-4 and H.264/AVC [1] are the representative video compression techniques that are most frequently used. Accordingly, many authentication schemes [2-8] and CP schemes [9-13] have been proposed with various watermarking methods applied to these compression techniques. However, studies on H.264 watermarking methods are rare compared to those on image and MPEG watermarking methods. To provide authentication in AVC coding, Zhang et al. [6] uses best partition modes only in the inter-prediction slices. Authentication information is embedded strictly based on the best mode decision.
strategy in the sense that if any spatial and temporal attacks have been undergone, the scheme can detect the tampering by the sensitive mode change. Mobasseri et al. [7] utilizes code space that is defined over the CAVLC portion of protocol. The watermark securely maps eligible CAVLC to unused portions of the code space. The watermark authentication code of the scheme proposed by Chen et al. [8] uses Block Sub-band index and coefficient modulation to embed in the quantized AC coefficient of I-frame. Block sub-band index is used to assign a number to each block, and coefficient modulation is used to modify number of block to insert watermark. To provide the CP function in AVC coding, Noorkami et al. [9] embeds watermarks into the quantized AC coefficients of selected $4 \times 4$ DCT blocks in intra-frames. The embedding locations is determined by a public key that is generated by the relative differences of the DC coefficients. Another paper by Noorkami et al. [11] embeds the watermark in the coded residuals to avoid decompressing the video, while it detects the watermark from the decoded video sequence to make the algorithm robust to intra prediction modes (IPM) changes.

Moreover, H.264/SVC (H.SVC) [14] is newly standardized for video data with streams of various qualities by JVT of ISO/IEC MPEG and ITU-T. The objective of H.SVC is to offer content in a “scalable” way, such that the content can be coded once and can then offer streams of various qualities. The base layer of H.SVC bit-stream is generally coded in compliance with AVC. Therefore, authentication and copyright protection schemes that are applicable to both AVC and H.SVC are urgently required in digital video applications, since watermarking schemes for AVC and H.SVC are few and far between and are very restrictive.

In this paper, we propose an efficient authentication scheme based on fragile watermarking as well as a CP scheme based on non-blind watermarking for both AVC and H.SVC. The proposed authentication scheme uses the prediction modes as the watermark. It can easily verify the integrity of content since its simple processing such as re-encoding by H.264 encoder easily changes the prediction modes and residuals. In addition, the proposed CP scheme utilizes the DCT domain of uncompressed I-frames to provide the robust watermark in the content to which the fragile watermarking is applied and also in the content re-compressed with the intended modification.

This paper is organized as follows. Section 2 proposes a new authentication scheme as well as a CP scheme for both AVC and H.SVC. Section 3 describes the experimental results of our proposed scheme. The last section summarizes and concludes the paper.

2. PROPOSED AUTHENTICATION SCHEME

We propose an authentication scheme and a CP scheme that can be applied in AVC and H.SVC coder. The proposed scheme offers a video content authentication scheme based on the fragile watermarking. The authenticated content is used by the user who is authorized to have the authentication key. If the authorized user distributes the content to others after partially modifying the content for a parody, for instance, the authentication of the received content is rejected, and then the receiver cannot access the content or may obtain damaged content with a low picture quality. Moreover, in case the original or modified content is used illegally by unauthorized users or if the copyright of the content is trespassed on, the owner can claim the ownership through the inserted copyright water-
2.1 Authentication

The proposed authentication scheme first extracts the features from the content, and then the extracted features are embedded into the content as a watermark to provide authentication. The feature extraction and watermark embedding processes are combined by the H.SVC encoding process of the content provider or seller side. Then, the watermarked content is verified with the H.SVC decoding process at the content receiver or user side.

2.1.1 Watermark generation

As the feature selection is an important part in the proposed scheme, the features should be carefully selected by considering the following points.

- The feature to be selected has to be important and meaningful information in comprising content.
- It should be the value which is not easily changed whenever it is encoded.
- It has to be the value included in each frame.
- It should be a unit providing the efficiency in error resilience.

To satisfy these conditions, we use the intra and the inter prediction modes to generate a watermark. The IPMs are used in I-frame to utilize the similarity between neighboring macroblocks (MB) or blocks. There are a total of nine optional IPMs for each $4 \times 4$ luminance (luma) sub-block as shown in Fig. 2 (a), and four optional IPMs each for a $16 \times 16$ (MB) luma block and an $8 \times 8$ chrominance (chroma) block as shown in Fig. 2 (b). Inter-prediction creates a prediction model from one or more previously encoded video frames or fields using block-based motion compensation. In H.264, a range of block sizes...
Fig. 2. (a) Directions of IPM for each 4 × 4 luma; (b) Intra IPMs for each 16 × 16 luma.

Table 1. The intra and the inter prediction modes and represented values.

<table>
<thead>
<tr>
<th>Block Modes</th>
<th>Intra Modes</th>
<th>Inter Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MB prediction mode values</td>
<td>Sub_block prediction mode value</td>
</tr>
<tr>
<td>16 × 16</td>
<td>0 (mode 0)</td>
<td>SKIP</td>
</tr>
<tr>
<td></td>
<td>1 (mode 1)</td>
<td>16 × 16</td>
</tr>
<tr>
<td></td>
<td>2 (mode 2)</td>
<td>16 × 8</td>
</tr>
<tr>
<td></td>
<td>3 (mode 3)</td>
<td>8 × 16</td>
</tr>
<tr>
<td>4 × 4</td>
<td>6 (mode 4)</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>5 (mode 5)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6 (mode 6)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7 (mode 7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8 (mode 8)</td>
<td></td>
</tr>
</tbody>
</table>

16 × 16, 16 × 8, 8 × 16 and 8 × 8 are supported, and the 8 × 8 sub-MB is further divided into partitions with block sizes of 8 × 8, 8 × 4, 4 × 8 or 4 × 4 as shown in Fig. 3. Therefore, intra prediction mode (IPM) means the prediction direction of each block selected for intra prediction, and inter prediction mode means the block mode selected in various block sizes for inter prediction. These prediction modes are used as the feature values for MBs or sub-blocks.

Table 1 shows the feature values expressed by the IPMs for intra-frames and the block modes for inter-frames.
These feature (F) values are encrypted with the provider’s secret key to enhance the security, and the encrypted value is divided by \(2^P\) where \(P\) is the threshold value for controlling the bit insertion quantity. The result value of mod operation is a watermark \((W)\).

\[
W = E(F) \mod 2^P,
\]

(1)

where ‘\(E()\)’ is the encryption function and ‘\(A \mod B\)’ is the remainder after numerical division of \(A\) by \(B\).

To embed, the watermark for each block is expressed as a binary watermark sequence as follows,

\[
W = w_0w_1\ldots w_{p-1}.
\]

(2)

### 2.1.2 Embedding

In the encoding process, the watermark generation is performed at the prediction step, and the watermark embedding is performed at the quantization step of difference values obtained by the prediction. The watermark is inserted as follows,

1. The proposed scheme counts the number of non-zero coefficients among the quantized values of each block.
2. If the counted number is greater than the threshold value \(Q\), the block is selected for embedding. Otherwise, the block is skipped.
3. The embedding position in the block is the last non-zero \(P\) coefficients in the zig-zag ordering, and each bit \((w_i)\) of the watermark is inserted by the following Eq. (3).

\[
\begin{align*}
\text{if } w_i = 0, 
\quad & co' = \begin{cases} 
co + 1, & \text{if } (co > 0 \text{ and } (|co| \mod 2 = 1)), \\
co - 1, & \text{if } (co < 0 \text{ and } (|co| \mod 2 = 1)), \\
co, & \text{otherwise,}
\end{cases} \\
\text{if } w_i = 1, 
\quad & co' = \begin{cases} 
co - 1, & \text{if } (co > 0 \text{ and } (|co| \mod 2 = 0)), \\
co + 1, & \text{if } (co < 0 \text{ and } (|co| \mod 2 = 0)), \\
co, & \text{otherwise,}
\end{cases}
\end{align*}
\]

(3)

where \(co\) is the original coefficient and \(co'\) is the watermarked coefficient.

Suppose that the watermark value to be inserted in one block and the threshold value \(P\) are 2 respectively, and the threshold value \(Q\) is 4. The watermark bits expressed by Eq. (2) are embedded into the last 2 coefficients in zig-zag ordering as shown in Fig. 4.

Each MB is processed by a \(4 \times 4\) block unit to produce the bit-stream. If the selected mode for the prediction is for a \(16 \times 16\) block, the watermark for \(16 \times 16\) block is repeatedly embedded into \(4 \times 4\) blocks that constitute the MB. If the selected mode for the prediction is for a \(4 \times 4\) block, the watermark is inserted into only a \(4 \times 4\) block.
2.1.3 Verification

The received content is decoded also into the MB unit. If the number of non-zero coefficients in each $4 \times 4$ block is greater than threshold value $Q$, the watermarks are extracted as follows.

1. The watermark bits are extracted from the last $P$ bits in zig-zag ordering by Eq. (4).
   \[ w_i = (|c^i| \mod 2) \quad (4) \]

2. The extracted watermark bits are combined to generate one watermark by Eq. (5).
   \[ W = w_0 \times 2^{p-1} + w_1 \times 2^{p-2} + \ldots + w_{p-1} \times 2^0 \quad (5) \]

3. The extracted watermark $W$ is decrypted with a secret key. Then, it is compared with the prediction mode ($PM$) of each block obtained from received content as follows,
   \[
   \begin{align*}
   & \text{if } D(W) = (PM \mod 2^p), \text{ MB is authenticated} \\
   & \text{else MB is not authenticated}
   \end{align*}
   \]
   \[ (6) \]
   where $'D()'$ is the decryption function.

2.1.4 Scalability

The proposed scheme is applicable not only to AVC but also to H.SVC. Generally, the base layer of H.SVC which includes much information is more important than the enhancement layer. Thus, even if our scheme is only applied on the base layer, it provides sufficient security. However, an authentication to the enhancement layer is requested in case the significance of the content is high. The method for applying the proposed scheme in the enhancement layers is the same as the way we illustrated above. In enhancement
layers, however, we should add the base layer reference mode as well as the modes in Table 1 to generate the watermark because the enhancement layers for the spatial scalability mainly predict by the base layer or lower layers. On the other hand, the features of enhancement layers for the temporal scalability are equal to the inter mode shown in Table 1 because the temporal scalability still uses the motion estimation.

2.2 Copyright Protection

The proposed scheme together provides the CP function by adding the watermark for the content owner as well as the authentication watermark. The objective of the proposed CP scheme is to provide a robust watermark not only in the content in which fragile watermarking is applied for the authentication but also in the content re-compressed after the intended modification.

2.2.1 Embedding

Use of prediction values and residual data in the encoding process to raise the coding efficiency of watermarking brings about perceptual quality decrease and low robustness. Thus, the proposed CP scheme inserts a watermark into the DCT domain of uncompressed content divided into $4 \times 4$ blocks. At this time, the embedding method is based on the spread spectrum watermarking technique [15]. Subsequently, the watermarked content conducts the existing H.264 encoding algorithm after again undergoing inverse DCT. We use only I-frame for watermarking since I-frames in H.SVC include the most important information and are transmitted to all content users. The watermark insertion process is as follows,

1. The ID number or the image mark of the copyright holder can be used as the watermark that can insist on the ownership of the copyright holder. The binary watermark $W$ is used after being encrypted or permuted in order to enhance the security. It is comprised of $-1$ and $1$, and expressed as follows,

$$E(W) = w_0w_1\ldots w_{K-1}$$ (7)

$$w_i \in \{-1, 1\}, \ i \in \{0, 1, \ldots, K-1\}$$

where ‘$E()$’ the cryptographically secure encryption algorithm with the length-preserving property and $K$ is the watermark image size.

2. Each $4 \times 4$ block of I-frame performs DCT.

3. Each watermark bit is inserted into the DC values in each DCT domain by the following Eq. (8).

$$DC'_j = DC_j + (DC_j \times \alpha \times w_i), \ j \in \{0, 1, \ldots, J-1\}$$ (8)

where $DC_j$ denotes the original $j$th DC value, $DC'_j$ is the watermarked $j$th DC value, $\alpha$ is a scaling parameter which adjusts watermark robustness and $J$ is the number of $4 \times 4$ blocks.

4. Watermarked DCT domain performs inverse DCT.
Video content including the copyright information is encoded by the H.264 encoding process joined with the authentication watermarking scheme.

2.2.2 Extraction

The proposed CP scheme is non-blind watermarking scheme that need the original content for watermark detection. The received content can be compared with the original content or with the content decoded after encoding. The watermark extraction process is as follows,

1. The DC values of the original content (ODC) and the DC values of the received content (RDC) are extracted respectively.
2. ODC and RDC are compared, then the watermark is extracted as follow,
   \[ w'_j = \begin{cases} 1, & \text{if } (ODC \leq RDC), \\ 0, & \text{else}. \end{cases} \]  
   (9)

   where \( w'_j \) is the watermark bit extracted from the \( j \)th block of the frame.
3. In order that each bit value of \( K \) is determined, the probability of each bit is checked through the repetitively inserted watermark. For this, \( w'_j \) is mapped in the watermark size \( K \) and the values are stored as follows,
   \[ \text{if } (w'_j = 1), \ w^*_i = w'_j \mod K + 1, \ i \in \{0, 1, \ldots, K-1\}. \]  
   (10)
4. According to the value of the obtained \( w^*_i \), each one is expressed as the value of 256 range by Eq. (11) and these are re-organized as the watermark image of the size \( K \).
   \[ \tilde{w}_i = 255 - (w^*_i \times \beta), \]  
   (11)

   where \( \tilde{w}_i \) means each pixel of recovered watermark image and \( \beta \) is weight value used to express as a gray image, which can be expressed as \( 255/\max(w'_j) \).
5. After steps 1-4 are repetitively performed in all I-frames, these watermark images are expressed as one watermark image having high accuracy.
6. The obtained watermark image is decrypted as the recognizable image mark.
   \[ W = D(\tilde{w}_0 \tilde{w}_1 \ldots \tilde{w}_{K-1}) \]  
   (12)

3. EXPERIMENTS AND ANALYSIS

The proposed scheme is evaluated using the standard video sequences of MPEG SVC to the JSVM 9.8. In this evaluation, there are 100 frames, and the GOP size is set as 8 frames and the intra period as 16 frames. All experiments were conducted with a QCIF@7.5Hz and a CIF@15Hz input files of video sequences for the combined scalability that supports a variety of spatial and temporal resolution and rate points. The scalabilities in the experiment have 2 spatial resolutions (QCIF and CIF) on the y-axis and 4
temporal resolutions (1.87, 3.75, 7.5 and 15) on the x-axis as shown in Fig. 5. We used the intra and the inter prediction modes as the watermark for authentication, and the image mark of 10 × 40 pixels is used as the watermark for copyright. The encryption function used in Eqs. (1) and (7) is the stream cipher algorithm or the count mode using block cipher with a specific key. We used RC4 stream cipher. The conditions are summarized in Table 2.

The proposed scheme is applied to all the layers of ‘Football’ and ‘Foreman’ with QP value 30 in QCIF and QP value 32 in CIF. Figs. 6 (a) and (c) are the original I-frame and B-frame respectively in which a watermark is not inserted, and Figs. 6 (b) and (d) are the I-frame and B-frame in which the watermarks for authentication and CP are inserted. The experiment results of the proposed scheme show that the content quality of the watermarked content is not visually damaged.

Table 3 shows the peak signal-to-noise ratio (PSNR) values that provide the objective numerical values about the video quality of Fig. 6. The PSNR results show that the PSNR of the original video and the watermarked video has little difference. This means that the proposed scheme keeps high video quality in the numerical evaluation and the visual perception.

Table 4 shows the increasing ratio of bit-rate in accordance with the proposed watermarking schemes. The increasing ratio of bit-rate by the CP scheme is greater in the video in which an action is small like a ‘Foreman’. However, the proposed CP scheme can adjust the video quality decrease and the bit-rate increasing rate by watermarking the only the selected portions of the 4 × 4 blocks of image. The simpler method is to adjust the \( \alpha \) value. That is, the bit-rate increasing rate will reduce if \( \alpha \) becomes small. On the other hands, our authentication scheme attempts the optimization of bit rate-distortion since it executes the prediction mode decision stage in watermarked state. Our authentication scheme is affected by threshold value \( P \) and \( Q \). The experimental results show the about 5% bit-rate increasing rate when threshold value \( P \) and \( Q \) are 2 as shown in Table 4. The increasing ratio of bit-rate of our scheme will be reduced by decreasing the threshold value \( P \) or increasing the threshold value \( Q \). Moreover, the recently improved performance of the system and
Fig. 6. Experiment results of proposed scheme.

Table 3. PSNR[dB] results of videos.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Video size</th>
<th>Football</th>
<th>Foreman</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Original (Encoded) video</td>
<td>QCIF@7.5</td>
<td>35.25</td>
<td>39.01</td>
<td>40.67</td>
<td>36.86</td>
<td>41.14</td>
<td>42.32</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QCIF@15</td>
<td>34.53</td>
<td>39.44</td>
<td>41.15</td>
<td>35.93</td>
<td>40.80</td>
<td>43.03</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Watermarked video for CP ($\alpha = 0.03$)</td>
<td>QCIF@7.5</td>
<td>34.90</td>
<td>39.02</td>
<td>40.67</td>
<td>36.04</td>
<td>41.14</td>
<td>42.36</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QCIF@15</td>
<td>34.55</td>
<td>39.45</td>
<td>41.17</td>
<td>35.94</td>
<td>40.78</td>
<td>43.01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Watermarked video for Auth.</td>
<td>QCIF@7.5</td>
<td>34.93</td>
<td>39.03</td>
<td>40.65</td>
<td>36.59</td>
<td>41.12</td>
<td>42.35</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QCIF@15</td>
<td>34.49</td>
<td>39.44</td>
<td>41.12</td>
<td>35.86</td>
<td>40.78</td>
<td>43.06</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Watermarked video for Auth. and CP</td>
<td>QCIF@7.5</td>
<td>34.62</td>
<td>39.01</td>
<td>40.67</td>
<td>35.75</td>
<td>41.15</td>
<td>42.34</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QCIF@15</td>
<td>34.50</td>
<td>39.46</td>
<td>41.12</td>
<td>35.84</td>
<td>40.79</td>
<td>43.04</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4. The increasing ratio of bit-rate in watermarked video.

<table>
<thead>
<tr>
<th>Video sequence</th>
<th>Football</th>
<th>Foreman</th>
</tr>
</thead>
<tbody>
<tr>
<td>QCIF@7.5</td>
<td>1.52%</td>
<td>1.37%</td>
</tr>
<tr>
<td>QCIF@15</td>
<td>12.42%</td>
<td>6.74%</td>
</tr>
<tr>
<td>Watermarked video for CP ($\alpha = 0.03$)</td>
<td>4.78%</td>
<td>2.54%</td>
</tr>
<tr>
<td>Watermarked video for Auth.</td>
<td>6.02%</td>
<td>3.09%</td>
</tr>
<tr>
<td>Watermarked video for Auth. and CP</td>
<td>6.22%</td>
<td>3.72%</td>
</tr>
<tr>
<td>QCIF@7.5</td>
<td>17.74%</td>
<td>9.77%</td>
</tr>
<tr>
<td>QCIF@15</td>
<td>12.42%</td>
<td>6.74%</td>
</tr>
</tbody>
</table>

encoder is capable of supplementing the bit increasing rate generated by the proposed scheme.

We test the time complexity of the authentication scheme only because the watermark extraction for CP does not need to be processed in real-time. We measure the increasing rate in the processing time between the original encoding/decoding and the encoding/decoding included the watermarking and verification. The time overhead is very small as shown in Table 5, because the proposed scheme is combined with the encoding/decoding process and its computational complexity is low. Therefore, the watermarking and verification process does not greatly affect the running time of the encoding/decoding process. Thus, the proposed scheme is also appropriate for real-time applications.
Table 5. Time increasing rates of the authentication process.

<table>
<thead>
<tr>
<th></th>
<th>Encoding</th>
<th>Decoding</th>
</tr>
</thead>
<tbody>
<tr>
<td>QCIF@7.5</td>
<td>0.45%</td>
<td>0.12%</td>
</tr>
<tr>
<td>CIF@15</td>
<td>0.34%</td>
<td>0.09%</td>
</tr>
</tbody>
</table>

Next, we discuss the security and robustness of our scheme. In our authentication scheme, the watermarks will be not inserted if the MB or sub-block is skipped or if the number of non-zero coefficients is less than the threshold value $Q$. However, the proposed scheme still provides the authentication capacity of MB unit, even when the MBs do not include the watermark bits because the damaged content has a different feature value by prediction. Suppose that the content to which our scheme is applied is modified and re-encoded by someone. If any object is added on the flatted range as shown in Fig. 7 (b), it is possible for the decoding process either to prevent the user from accessing the content or provide a content compromised with low quality. In the latter case, the proposed scheme can show the compromised content, in which the residual data of damaged blocks by re-encoding are set as 0 as shown in Fig. 7 (c). The added object ‘ball’ in Fig. 7 (b) is hard to recognize in Fig. 7 (c) and it informs the damaged location only.

Our CP scheme can achieve different levels of robustness and security by adjusting two parameter settings. The first parameter is the scaling parameter $\alpha$ that is used to adjust the intensity of the inserted watermark. As $\alpha$ is enlarged, the tenacity of watermark is enlarged, but the picture quality of the image is decreased. Thus, we checked the video quality decrease and the accuracy of extracted watermark by applying $\alpha = 0.02$, $\alpha = 0.03$ and $\alpha = 0.05$ in the proposed authentication and CP scheme. It is applied only to I-frames of the ‘Football’ QCIF video with the total 65 frames. In addition, the quantization parameter (QP) value is 28 and the weight value $\beta$ is set at 15 since 5 I-frames exist in 65 frames. Table 6 shows the video quality decrease results and bit-rate increasing rates of the QCIF video according to the scaling parameter. It has a minute difference which it is too small to be differentiated visually, and the increase of 0.01 in $\alpha$ led to an increase of about 1% in bit-rate. Table 7 shows the extracted watermarks according to the scaling parameter $\alpha$ values. The second parameter is the QP values. We compared the watermark images extracted from the contents that were re-encoded with the different QP values. In this experiment, we used QP value 28 in our scheme and 30 and 32 for the re-encoding. Table 7 shows the watermark images extracted according to scaling parameters $\alpha$ and QP values. In our experiment results, each watermark image was comprised by the extracted 5 I-frames only. Thus, the real video contents including large-volume frames will be able
Table 6. PSNR[dB] and bit-rate increasing rate according to scaling parameter $\alpha$.

<table>
<thead>
<tr>
<th></th>
<th>Y</th>
<th>U</th>
<th>V</th>
<th>The increasing ratio of bit-rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original</td>
<td>36.39</td>
<td>40.11</td>
<td>41.38</td>
<td>0%</td>
</tr>
<tr>
<td>$\alpha = 0.02$</td>
<td>36.11</td>
<td>40.08</td>
<td>41.37</td>
<td>4.2%</td>
</tr>
<tr>
<td>$\alpha = 0.03$</td>
<td>35.89</td>
<td>40.09</td>
<td>41.36</td>
<td>5.6%</td>
</tr>
<tr>
<td>$\alpha = 0.05$</td>
<td>35.44</td>
<td>40.09</td>
<td>41.37</td>
<td>7.3%</td>
</tr>
</tbody>
</table>

Table 7. Watermark images extracted according to scaling parameter $\alpha$ and QP values.

<table>
<thead>
<tr>
<th></th>
<th>QP = 28</th>
<th>QP = 30</th>
<th>QP = 32</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha = 0.02$</td>
<td>PKNU</td>
<td>PKNU</td>
<td>PKNU</td>
</tr>
<tr>
<td>$\alpha = 0.03$</td>
<td>PKNU</td>
<td>PKNU</td>
<td>PKNU</td>
</tr>
</tbody>
</table>

to get the more exact watermark image. In addition, these watermarks are extracted from contents applied our authentication method. Therefore, our scheme has the robust watermark against the damage by the authentication watermarking and the quantization loss by the re-encoding.

Moreover, our CP scheme has the robustness in the partly modified content since the watermark is repeatedly inserted in the every I-frames and can also be extracted from one frame or the specific frames. That is, our scheme has the robustness in spatial modification such as object insertion and temporal attack such as frame dropping.

The proposed schemes need to be compared with the existing papers proposed by the same purpose. However, the performance comparison with the existing works is highly limited because the published papers on H.SVC authentication are few and far between. Nevertheless, we tried to compare with the papers proposed for AVC on the following three standpoints.

- **Video quality through PSNR:** Our scheme embedding watermarks for authentication and CP has little PSNR difference between the original video and watermarked video as shown in Table 3, while [6] and [8] have a degradation of at least 1dB and 2.5dB respectively through a watermarking. Therefore, the proposal scheme provides an excellent video quality.

- **The number of region inserting the authentication watermark:** Reference [7] provides the number of CAVLCs that are watermarkable code space. The total MB number and the total number of unique CAVLCs that actually occur in ‘Foreman’ are 88,632 4 × 4 blocks and 25,232, respectively. Among them, the number of CAVLCs that meets the watermarking criteria is 2,136. On the other hand, our scheme has 1,584 4 × 4 blocks and 971 usable blocks in I-frame of H.SVC base layer. Among them, the average blocks number which can be watermarked by a condition is about 560. Therefore, the proposal scheme is more efficient than [7] when considering the frame size.

- **The number of watermark bits inserted for copyright:** The number of watermark bits embedded in I-frame of our scheme is about 1584 which are all 4 × 4 blocks for comprising QCIF. On the other hand, reference [9] has watermark bits between 22 and 81, and reference [11] has watermark bits of average 1004. This means that the proposed scheme is superior to [9] and [11] in the amount of insertion bits.
4. CONCLUSIONS

This paper proposed an efficient authentication scheme based on fragile watermarking and a CP scheme based on non-blind watermarking for AVC and H.264. The proposed authentication scheme uses the intra or inter prediction mode optimized for each MB as watermark for authentication. Then, the generated watermark is embedded into the quantized coefficients satisfying a given condition. Even though the domain in which a watermark is not actually inserted exists, this scheme verifies the integrity of all areas of a frame with the MB unit. Our scheme has low video quality decrease and the little overhead of the running time in the encoding/decoding process. Since it has a little increased ratio in the bit-rate, however, it is left as future work we will carry out. The proposed CP scheme inserts a watermark of the owner into the DCT domain of 4 × 4 block of uncompressed content. The watermarking is applied only to I-frames which are transmitted to all content users. Our CP scheme shows the robust watermark not only in the content to which fragile watermarking is applied for authentication but also in the content which is re-encoded with the modification intended. Moreover, the CP scheme provides low quality degradation and low computational complexity. The simulation results of our combined scheme show the efficiency about the visual security, the increasing ratio of bit-rate and the time increasing rates.

REFERENCES


Su-Wan Park (朴秀婉) received the B.S. degrees from Kosin University, Korea, in 2002, and the M.Ed. degree from Pukyong National University, Korea, in 2005. She has been a Ph.D. candidate at Pukyong National University, Korea since 2006. Her research interests include image/video processing and multimedia security.

Sang Uk Shin (申翔旭) received his M.S. and Ph.D. degrees from Pukyong National University, Busan Korea in 1997 and 2000, respectively. He worked as a senior researcher in Electronics and Telecommunications Research Institute, Daejeon Korea from 2000 to 2003. He is currently an Associate Professor in the Division of Electronics, Computer and Telecommunication Engineering of Pukyong National University. His research interests include cryptographic protocol, mobile/wireless network security and multimedia content security.