This paper proposes a new method for blind digital video watermarking in H.264 standard based on pattern consideration. The major challenging issue in designing a blind H.264 watermarking scheme is instability of the prediction modes in case of re-encoding which alters the residuals in the sequel. As a result, the blind decoding of the watermarked media is too cumbersome. In this case, most of the blind methods insert the watermark in some specific residuals. These locations are vulnerable to be identified by attackers. To overcome this problem, we analyzed the structural information of each frame and the temporal characteristics of the previous GOP in order to choose more stable locations. Another advantage of our proposed method is its ability to extract the embedded watermark rather than just to detect its presence which makes it more flexible from an application point of view.

Index Terms— Blind video watermarking, video quality, DCT analysis, watermarking security

1. INTRODUCTION

In video watermarking, the watermark can be added either to uncompressed data (raw data) or compressed bitstream. There are numerous methods for embedding the watermark in raw videos [1-3]. Applying them for compressed video sequences, however, need a full decoding process for embedding or watermark detection. In many applications it is really not practical to decode the sequence completely. Consequently, the compressed video watermarking has attracted more attentions. Different video compression standards have been appeared. The goal of each is providing more compressed data along with better quality. H.264, as the most efficient compression standard, is utilized for a wide range of applications. As a result, providing a secure watermarking method, which is appropriate for this standard, is highly desirable.

Capacity, imperceptibility, and robustness are three major challenging issues toward video watermarking. These factors are interdependent [4]. The greatest interest in H.264 video watermarking scheme has been turned to robustness; however, the security is neglected especially in blind methods. For implementing an applicable watermarking system, it is desirable to consider all these factors.

For embedding the watermark in compressed domain, there are two approaches: embedding in encoder and bit stream embedding. In bitstream embedding, the error propagates; hence, preserving quality is the main problem in such methods. In this approach, full decoding of the compressed video is not necessary. On the other hand, the second approach uses the watermarked data for next predictions; therefore, the error induced by watermark embedding does not propagate. In this scenario, bit rate increase is the major challenging issue.

In recent years, various H.264 watermarking methods have been proposed. Most of them modify I frames since they convey a wide range of information in comparison to the P and B frames. Moreover, the existing of this type of frames is vital for decoding.

The watermarking method for H.264/AVC proposed by Noorkami et al. [5] embeds the watermark in the quantized AC coefficients of I frames. However, this algorithm is not robust against common watermarking attacks. They presented a robust watermarking method in [6, 7]. Their algorithm generates a palette containing the actual location of the watermark which should be transmitted to the decoder side. Moreover, their scheme can only detect the watermark, in other words, the watermark presence can only be revealed if the watermark content is known in advance.

In another method [8], the region information of the motion vectors are used to hide copyright information. Although this method presents a good perceptual quality, the bit rate is widely increased; moreover this method is not robust even against re-encoding.

In [9], a blind robust video watermarking scheme in H.264 standard is proposed. The watermark information is embedded directly into H.264/AVC video at the encoder by modifying the quantized DC coefficients. Bit rate increase is one of the major problems of their method. In addition, since just DC coefficients are exploited for embedding, the security issues are not considered in this scheme.

The robust compressed video watermarking schemes in H.264 standard use two strategies: the first group uses non-blind embedding which restricts the scope of application.
On the other hand, the second group embeds the watermark in specified locations which are vulnerable to be identified by attackers. Furthermore, most of the presented methods so far just use detectable watermark, i.e., they can verify the existence of a predetermined watermark rather than extracting the embedded payload. Readable watermarking schemes, in which the payload can be read without knowing it beforehand, is by far more flexible since the a priori knowledge of the watermark content cannot always be granted from an application point of view [10]. Therefore, designing a robust readable method is really desirable and applicable. Needless to say that, all readable watermarking algorithms can be converted to a detectable one.

In this paper, we propose a blind readable watermarking scheme in H.264 domain in which the structural information are considered in order to preserve the spatial quality of the marked media. In addition, the motion information is employed in order to prevent temporal flicker. Furthermore, we analyzed the mentioned information to find more stable locations for embedding. On the other hand, considering the difference between the numbers of nonzero coefficients of two chosen sub-macroblocks, as the watermark indication, provides a way to achieve a robust watermarking method.

2. PROPOSED METHOD

The proposed watermarking system utilizes the structural information of each block for imperceptible embedding. Furthermore, the structural information is employed to provide the security through generating a content based key. The security of the algorithm is provided using random block selection based on the generated key. If the same key is used for watermark embedding in all frames, the method is vulnerable to self-collision attack. Thus, an efficient algorithm uses the properties of the frames to get the appropriate feature in order to select the suitable area for embedding. These features should be enough robust in order to enhance the security and synchronizations. We categorized nine intra prediction modes into 4 groups. Since similar modes can be converted to each other after embedding, categorizing them make the public key more robust in case of alternation. Since the decision for each intra prediction mode totally depends on the structure of the 4×4 block, it is enough robust to be considered as a public key.

In I frames there are two luma prediction modes: I4 and I16. I16 is chosen for the smooth areas while I4, is selected for the detailed areas of the frame. Since I4 shows detailed area, the proposed method uses this kind of macroblock for embedding. In this paper, the statistical results of the transformed coefficients distribution in Intra coding are used. Based on histogram analysis in [11], three main structures are selected for watermark embedding. All of the I4 intra blocks should be mapped into one of these three structures. Consequently, we classify each block to one of the basis structures: DC, vertical, and horizontal. Regarding the statistical analysis given the mentioned structure, the distribution of each coefficient, and therefore, its role in structural formation is estimated. It can be concluded that the probability of each coefficient is related to its role in that structure. As a result, this distribution function can be used to select the suitable coefficient for embedding.

The distribution of each coefficient is explored in these three groups to achieve the probability of having nonzero value in specific positions. Based on the statistical results [11], we propose a strategy for modifying the coefficients considering three main aspects of the watermarking methods.

For embedding, the scrambled public key is used to determine two selected blocks in current macroblock. The difference between the numbers of nonzero coefficients shows the watermark bit.

In order to extract the motion information of a video sequence, the motion activity in each 4×4 sub-macroblock is estimated. In this case, the category of inter mode to which the current 4×4 partition belongs is extracted. This information is employed to construct a matrix called inter mode map (IMM). As a case in point, for each specified frame with size of (144×176) an IMM with size of 36×44 will be achieved in which each value shows the inter mode type in specified location. The different inter modes are : {COPY(SKIP), 16×16, 16×8, 8×16, 8×8, 8×4, 4×8, 4×4} to each of which the mode value {0,1,2,3,4,5,6,7} is assigned correspondingly. We use this information in [12] to show the importance of considering motion activity in video watermarking. In this paper, to make the algorithm more robust, we categorized the inter mode to three groups to make the IMM matrix more robust against re-encoding and common watermarking attacks.

To estimate the motion activity in current I frame, the IMM information related to previous GOP frames are exploited to construct the GOP Motion Activity Map (GMAM) as follows:

$$GMAM = \frac{\sum_{k \in \text{Previos GOP}} IMM_k}{\max_{k \in \text{Previos GOP}} \left( \sum_{\text{Previos GOP}} IMM_k \right)}$$  \hspace{1cm} (1)

The closer value to zero indicates that the corresponding 4×4 sub-macroblock has a less temporal activity than the value which is further from zero.

We use the motion information to decide whether the selected macroblock for embedding is appropriate. We avoid embedding the watermark if GMAM information is close to zero. Since this kind of macroblock is more vulnerable to be changed after re-encoding.

For embedding the watermark, some nonzero (zero) AC residuals are converted to zero (±1) in such a way that less degradations appear. To fulfill this aim, the priority matrix
(PM) is introduced. In the next section, the foundation of PM is explained.

2.1. The priority matrix

The PM is utilized in order to identify the most appropriate coefficient for modifying. To select the suitable coefficients, the quality of watermarked video, its bit rate, and also security have been taken into consideration. For each demand, a priority matrix is devised respectively as \( M_q, M_b \), and \( M_s \). These matrices from which the PM is constructed is explained in the following.

To select the appropriate coefficients respect to quality demand, structure type of the 14 block is determined first. Considering the pdf of each coefficient given the structure type, effectiveness of each coefficient can be specified. As a result, the probability of being nonzero for each coefficient in specific structure is considered as the quality priority matrix, termed as \( M_q \). In this paper, we use the reports of the analysis in [11].

Moreover, one of the most important challenging issues in video watermarking is bit rate increase. Merely noticing the quality in designing the PM may increase the bit rate and will be impractical. To prevent the bit rate increase, it is necessary to modify the coefficients in a manner that the zigzag order of the watermarked block does not alter intensively. Consequently, the priority for each coefficient in \( M_b \), is defined considering the zigzag ordering scan.

On the other hand, to strengthen the security in addition to random selection of 4×4 blocks, another policy is the random selection of the coefficients. Therefore, a pseudorandom matrix is defined as \( M_s \). This random matrix is generated based on a seed extracted from the unused bits of the generated key.

Finally, the PM is calculated via weighted summation of these three matrices:

\[
PM = W_q M_q + W_b M_b + W_s M_s
\]

where \( W_q + W_b + W_s = 1 \) (2)

In which \( M_q, M_b \) and \( M_s \) illustrate the quality, bit rate, and security probability matrices. \( W_q \), \( W_b \) and \( W_s \) show the weight of involvement of these parameter in generating PM respectively. The higher weight for the specified controlling parameter leads to achieving the results considering that parameter more than the two other factors.

2.2. Watermark embedding

The difference between the numbers of nonzero coefficients in two selected 4×4 block (namely \( A \) and \( B \)) indicates the watermark bit. Wherever the watermark bit is opposite to the sign of the result, the modification should be applied. In order to prevent quality degradation, the modification is applied on the 4×4 blocks satisfying the following condition:

\[
\text{if } |\text{nnz}(A) - \text{nnz}(B)| \leq T
\]

Where the \( \text{nnz}() \) indicates the numbers of nonzero AC coefficients in a selected 4×4 block, and the threshold \( T \), can vary depending on the application requirement.

If the watermark bit equals to one \( (W_i=1) \), then the condition \( \text{nnz}(A) - \text{nnz}(B) \geq 0 \) should be met; otherwise, the coefficient should be altered until this condition is satisfied. In doing so, the suitable nonzero coefficient in \( B \) (based on PM) have to be converted to zero. In this case, the least probable coefficient in PM is selected for modifying. If the mentioned condition is not satisfied yet, the appropriate zero coefficient in block \( A \) should be converted to \((±1)\) randomly. These process repeats as long as the condition is fulfilled.

In the reverse manner, if \( W_i=0 \), then the condition \( \text{nnz}(A) - \text{nnz}(B) < 0 \) should be fulfilled in a similar procedure.

In order to strengthen the robustness of the proposed algorithm, it is necessary to prevent conversion of the unwatermarked macroblock to watermarked one. Therefore, the unwatermarked macroblock which are vulnerable to be considered as watermarked one after re-encoding, i.e., \( T < |\text{nnz}(A) - \text{nnz}(B)| \leq T + 2 \), should be modified to satisfy the following condition

\[
|\text{nnz}(A) - \text{nnz}(B)| > T + 2
\]

Consequently, the watermarked block can be identified after re-encoding or applying attack without ambiguity.

3. EXPERIMENTAL RESULTS

We implement the proposed method using the H.264 reference software version 15.0 [13]. To evaluate the watermarking method fairly, different kinds of video stream such as “Mobile”, “Salesman”, and “Claire” are selected.

We apply the algorithm for 35 successive frames of “Mobile” sequence with ten intra period in main profile with CAVLC entropy coding with \( QP=28 \). The bitstream embedding is used in this algorithm. Table 1 demonstrates the results of bit rate increase, average PSNR of frames, and the achieved capacity for different threshold value, different weight factors, and GMAM threshold parameter.

As it is shown, the threshold has almost a reverse effect in quality of the watermarked video. In addition, increasing \( W_q \) leads to a better quality as it is expected. It is obvious that if only the security parameter is considered, the bite rate will increase along with quality degradation.

To evaluate the robustness of the proposed method after re-encoding, we compare the percentage of extracted bit with the method proposed in [5]. \( GMAM \) is selected as \([0.5,1] \) and \( T \) is considered as 2. The results are shown in Table 2.
Table 1. Simulation Results for “Mobile” Sequence

<table>
<thead>
<tr>
<th>Wq</th>
<th>Wb</th>
<th>Ws</th>
<th>T</th>
<th>GMAM</th>
<th>Capacity</th>
<th>Bit Rate Increase per embedded bit</th>
<th>Average PSNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.33</td>
<td>0.33</td>
<td>0.33</td>
<td>2</td>
<td>[0.6 1]</td>
<td>58</td>
<td>-0.0006</td>
<td>41.17</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>[0.6 1]</td>
<td>58</td>
<td>-0.0005</td>
<td>41.35</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>[0.6 1]</td>
<td>58</td>
<td>-0.0007</td>
<td>40.13</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>[0.6 1]</td>
<td>58</td>
<td>0.00067</td>
<td>34.95</td>
</tr>
<tr>
<td>0.33</td>
<td>0.33</td>
<td>0.33</td>
<td>2</td>
<td>[0 0.6]</td>
<td>23</td>
<td>-0.0008</td>
<td>43.68</td>
</tr>
<tr>
<td>0.33</td>
<td>0.33</td>
<td>0.33</td>
<td>3</td>
<td>[0.6 1]</td>
<td>77</td>
<td>-0.0005</td>
<td>39.19</td>
</tr>
<tr>
<td>0.33</td>
<td>0.33</td>
<td>0.33</td>
<td>4</td>
<td>[0.6 1]</td>
<td>99</td>
<td>-0.0006</td>
<td>37.12</td>
</tr>
</tbody>
</table>

Table 2. The comparison of the proposed method with [5]

<table>
<thead>
<tr>
<th>Video Sequence</th>
<th>Proposed Method</th>
<th>[5]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Re_encoding</td>
<td>Bit Rate Increase per embedded bit</td>
</tr>
<tr>
<td></td>
<td>Recovery Rate</td>
<td>Rate</td>
</tr>
<tr>
<td>Carphone</td>
<td>84%</td>
<td>0.0007%</td>
</tr>
<tr>
<td>Claire</td>
<td>83%</td>
<td>-0.0028%</td>
</tr>
<tr>
<td>Mobile</td>
<td>85%</td>
<td>-0.0006%</td>
</tr>
<tr>
<td>Mother</td>
<td>59%</td>
<td>0.0005%</td>
</tr>
</tbody>
</table>

As it is depicted in Table 2, in most cases our method outperforms the proposed scheme in [5]. Moreover, the robustness of the proposed method against three kinds of attacks including additive white Gaussian noise, salt and pepper noise and circular averaging filter is shown in Figure 1.

Figure 1. The robustness result of the proposed method against three kinds of attacks (salt & pepper noise density=0.0001, Gaussian noise (0,0.0001), circular averaging filter r=0.6)

4. CONCLUSION

In this paper, a blind H.264 watermarking method is presented. Regarding to preserving spatial quality, the structural information of each block is explored to select the appropriate coefficients for embedding. To avoid temporal flicker, the motion information of previous GOP is exploited. To make the algorithm robust against re-encoding and common signal processing attacks, we embed the watermark data in appropriate macroblock based on motion analysis. In contrast to most of the blind H.264 watermarking scheme, the proposed method uses random block selection based on a content based key which provides the reasonable level of security. Moreover, the proposed method can control the bit rate increase efficiently.

5. REFERENCES