ABSTRACT

In this paper, we propose a blind watermark detection scheme for digital cinema which is robust against D-A/A-D conversion attack. D-A/A-D conversion attack commonly happens during capturing cinema with a camera and is composed of various geometrical distortions as well as signal processing distortions. In many video applications, geometric distortions have been compensated by utilizing auto-correlation function (ACF). Since the ACF cannot resist projective transform but affine transform, we present a robust watermark detection scheme utilizing local auto-correlation function (LACF) with a mathematical model. Also, we suggest a way to design watermark pattern to improve performance of the LACF. We demonstrate robustness of the presented scheme against D-A/A-D conversion attacks for digital cinema as well as common video processing attacks.

Index Terms— Robust watermarking, auto-correlation function, digital cinema, D-A/A-D conversion attack.

1. INTRODUCTION

With the rapid spread of digital cinema and digital broadcasting, protecting copyright of digital cinema contents has been the most important issues. Watermarking technology seems to perfectly match the requirements of digital cinema in terms of copyright protection. This watermarking application has its own list of piracies. Many pirate copies of new digital movies are found on the Internet or black market before their official release. Since these pirate copies are filmed the projected movie with a camcorder at the back of the theater, the movie might be recorded at an angle according to the location of the pirate. Also, it can be translated or rotated during camcording. Due to these factors, the copied movie is severely degraded and the geometrical distortions applied to each frame impede drastically watermark detection [1, 2]. Therefore, the watermark should survive geometrical distortions like zooming, translation, rotation, and projection in digital cinema application.

Several papers described watermarking for digital cinema. Leest et al. [2] proposed a watermarking scheme which exploits the temporal axis to embed watermark by changing the luminance value of each frame and hence is inherently robust to geometrical distortions. But it has flickering effect due to the luminance change between frames. Delamay et al. [3] investigated the restoration of geometrically distorted digital images which are occured by the camera acquisition of images. However, since they require the unmodified image contents for detection, it is not practical in digital cinema application. Moreover, when the movie is captured video by a camcorder, the complex task of time-synchronization between the original movie and the capture video is required. Lubin et al. [4] embedded watermark into very low spatio-temporal frequency domain for satisfying three requirements of digital cinema: fidelity, robustness, and security. Especially in image applications, there have been many watermarking schemes to resist several geometrical distortions. Dong et al. [5] used image normalization and a deformable mesh to correct the distortion, but the original image was still required. Bas et al. [6] overviewed classical self-synchronizing techniques as techniques using periodical sequences, image features, template insertion, and invariant transforms. In digital cinema watermarking, watermark payload has to include the information when and where the movie is filmed. Hence, the payload about time and place has to be embedded during being showing on the screen in the theater, that is, watermark embedding process should be real-time. Using invariant transforms and image features, watermark embedding process cannot be established in real-time. Considering real-time embedding and blind detection, we use auto-correlation function to find self-synchronization [7] but it can only restore distorted images from affine transform. In digital cinema application, the watermark has to be robust against projective transform as well as affine transform.

In this paper, we propose a robust watermarking scheme to D-A/A-D conversion attacks which include geometrical distortions such as projective and affine transform as well as signal processing attacks. The scheme is a blind way without original video during the detection. Especially, we focus on resisting geometric distortions using local auto-correlation function (LACF) and establishing a related mathematical model.

The rest of paper is organized as follows. In Sec. 2, we introduce watermark design for our watermark detection scheme. In Sec. 3, we describe watermark detection scheme based on LACF. In Sec. 4, we present experiments to demonstrate the effectiveness of the proposed scheme on D-A/A-D conversion attack and Sec. 5 concludes.

2. WATERMARK DESIGN

The watermark pattern in the presented scheme is used in two ways. One is to find and restore geometrical distortions. The other is to extract the payload which has been embedded. In order to detect watermark robustly, the watermark pattern should have some properties for the better performance of ACF and LACF. That is, the watermark pattern is low pass filtered because low frequency components are

Email: mjlee@mmc.kaisf.ac.kr
affected little with common signal processing, especially D-A/A-D conversion [8]. Also, the filtered watermark pattern is repeated to vertical axis and horizontal axis and the same watermark is embedded during a certain period of time for robustness. In our scheme, watermark embedding process is done in real-time and based on spread spectrum embedding with perceptual scaling [9].

3. WATERMARK DETECTION

In watermark detector, the detection process consists of three operations: 1) watermark estimation, 2) watermark registration, and 3) watermark extraction.

3.1. Watermark Estimation

Since a blind detector is used, we should estimate the embedded watermark. For this, we employed both wiener filtering and SPOMF (symmetrical phase only matched filtering) [10] as whitening filters. The goal of the whitening filtering is to decorrelate the received data \( R \) to obtain an approximately spectrally white version of \( R \). Wiener filtering is performed in the spatial domain, but SPOMF is computed in Fourier domain. We experimentally decided what filtering is used to estimate for each frame depending on their performance.

3.2. Watermark Registration

The captured video by a camcorder can be projective-distorted at the worst from a mathematical point of view. That means in case of projective transform the number of degree of freedom (DOF) of the transform matrix is the most. We can describe projective transform as a matrix transformation:

\[
\begin{pmatrix}
\bar{x}' \\
\bar{y}' \\
w
\end{pmatrix} = H \begin{pmatrix}
x \\
y \\
q
\end{pmatrix}, \quad \text{where} \quad H = \begin{pmatrix}
a & b & c \\
d & e & f \\
g & h & i
\end{pmatrix} \quad (1)
\]

where \( w \neq 0, q \neq 0, (x', y') = (x'/w, y'/w)^T \), and \((x, y)^T = (x/q, y/q)^T \). \((x', y')^T \) stands for the coordinate of the original video frame and \((x, y)^T \) stands for the coordinate of projective-distorted video frame. Even though given matrix \( H \) consists of nine constants, the DOF of the matrix is eight and we can assume \( i = 1 \) in matrix \( H \). Therefore we need at least the transformation description of four points for watermark registration after any geometrical distortion. This can be done by defining multiple sets of shifts. In order to get the set of four points that any set of three of them cannot be collinear, the sets of shifts are arranged in two-dimension. The registration process is performed as follows:

**Step 1.** Find the distorted interval and angle between the extracted peak resulted from local auto-correlation function(LACF) on the estimated watermark.

**Step 2.** Obtain the transformation description of four points using the interval and the angle from Step 1 and put them into proposed mathematical model in Sec. 3.2.2.

**Step 3.** Obtain the inverse transformation matrix \( H^{-1} \) of geometrical distortion using four pairs of points from Step 2.

**Step 4.** Recover as closely as possible to the original data through inverse matrix operation in Sec. 3.2.3.

3.2.1. Local Auto-Correlation Function(LACF)

Kutter et al. [7] proposed the principle of the self-synchronization scheme which identifies affine transform such as rotation, scaling, and translation by auto-correlation function from the distorted image. Their scheme, however, cannot identify projective transform representing horizontal projection, vertical projection, and combined projection from the distorted image using auto-correlation of the whole image. To overcome their problems, we compute auto-correlation function of two local areas of the image that are parallel to each other instead of computing auto-correlation of the whole image. Fig. 1 shows that our LACF of the estimated watermark identifies projective distortion from the extracted peak locations while global auto-correlation function does not. The locations of the peaks of the result of auto-correlation function (ACF) clearly illustrate the multiple embedding of the watermark at horizontally and vertically shifted locations as shown in Fig. 1(a). For the distorted Lena image horizontally projected by 10 degrees, Fig. 1(b) shows that previous ACF cannot correctly extract the correlation peaks of the watermark, while our LACF extract all the peaks of two local areas as depicted in Fig. 1(c). In right figure of Fig. 1(c), the distance between the extracted peaks of left local area is longer than that of right local area as a result of the horizontal projection. It means that
3.2.2. Mathematical Modeling

We can obtain the angle and the interval of extracted peaks resulted from LACF. We need at least the transform description of four points to estimate eight DOF of coefficient matrix of projective transform as mentioned in Sec. 3.2. We construct a mathematical model for extracting four distorted points. It is assumed that the watermark pattern is embedded in the center of the host image and we know the location of 4 pairs of original points.

For constructing the mathematical model, we use the example described in Fig. 2. In this case, we designate four corner points A, B, C, D as original points. The goal of this section is to obtain the coordinates of projective-distorted points A', B', C', D. First, we assume that the correlation peaks are found on the line $\Pi N$ and $\Pi O$ from the result of LACF. E is the center point of $\Pi D$ and M is an intersection point of extension lines of $\Pi N$ and $\Pi O$. We denote $K$ as an intersection point of $\Pi N$ and $\Pi E$, and $G$ as an intersection point of $\Pi O$ and $\Pi M$. Then we obtain the length of $K G$ as the distance from two parallel line $\Pi N$ and $\Pi O$.

$$\Pi K = I_{\Pi N} \times \frac{r}{2} \quad \Pi G = I_{\Pi O} \times \frac{r}{2}$$

$I_{\Pi Y}$ stands for the interval between peaks on the line $\Pi Y$ and $r$ is the times of repetition of basis pattern in watermark pattern. We also denote $J$ as an intersection point of $\Pi M$ and $\Pi F$ and $K$ as an intersection point of $\Pi K M$ and the extension line of $\Pi O$. In this example, we need to compute the coordinates of B' and C' because the positions of A and D are not changed, therefore, we need to know the length of $B'L(= \Pi C')$. Similarity of triangle is used for computing coordinates.

First of all, we use the similarity of triangle $\Delta HKM$ and $\Delta IG M$ to obtain the length of $G M$.

$$GM = \frac{KG \cdot IG}{HK \cdot IG} \quad (2)$$

Now we obtain the length of $JK$ using the ratio of $JK$ to $HK$ as same as the ratio of the height of the image $h^i$ to the height of the original watermark $h^w$.

$$JK = \frac{h^i \cdot HK}{h^w} \quad (3)$$

The length of $EK$ can be obtained using $KM$, $JK$ and similarity of triangle $\Delta JKM$ and $\Delta AEM$.

$$EK = AE \cdot \frac{KM}{JK}$$

where $AE = h^i/2$. Using Eq. 2, 3, 4, we can get $B'L(= \Pi C')$.

$$B'L = \frac{h^i \cdot (EM - w^i)}{2 \cdot EM} \quad (5)$$

where $w^i$ stands for the width of the image. Finally, the coordinates of B' and C' are $(w^i, h^i/2 - B'L)$, $(w^i, h^i/2 + B'L)$, respectively.

3.2.3. Watermark Restoration

Now we compute the coefficient matrix of projective transform using estimated pairs of four points and Eq. 1. If it is estimated that the host image was horizontal perspective transformed, $b = h = 0$, or vertical perspective transformed, $b = g = 0$ in Eq. 1. In case of horizontal projective distortion, we compute the equation for the distorted coordinates as Eq. 6.

$$x' = \frac{ax + c}{gx + 1}, \quad y' = \frac{dy + e}{gy + 1} \quad (6)$$

Four pairs of points in Fig. 2 are transformed as follows:

$$\begin{align*}
A(0,0) & \Rightarrow A(0,0) \\
B(w^i,0) & \Rightarrow B'(w^i,h^i/2 - B'L) \\
C(w^i,h^i) & \Rightarrow C'(w^i,h^i/2 + B'L) \\
D(0,h^i) & \Rightarrow D(0,h^i)
\end{align*}$$

We obtain nine constants of $H$ in Sec. 3.2 by substituting above coordinates in Eq. 6. Finally, we get

$$\begin{align*}
a &= \frac{h^i}{2B'L} \\
b &= c = f = h = 0 \\
d &= \frac{(h^i)^2 - 2B'L \cdot h^i}{4 \cdot B'L \cdot w^i} \\
e &= i = 1 \\
g &= \frac{h^i - 2B'L}{2 \cdot B'L \cdot w^i}
\end{align*}$$

3.3. Watermark Extraction

The watermark extraction is performed by normalized cross correlation. That is, the cross correlation is computed by correlating the restored watermark to the basic patterns. If the resulting correlation value exceeds a preset threshold, the hidden messages are correctly extracted. Experimentally, we determine the preset threshold depending on an error probability model which follows Gamma distribution model, since we take the maximum value from cross correlation [11].

4. EXPERIMENTAL RESULTS

We performed experiments to determine both fidelity and robustness of our scheme. A watermark payload of 40 bits was embedded into each five-minutes HD-size clip of digital cinema to adhere to DCI (Digital Cinema Initiatives) [12] as shown in Fig. 3. The same bit is repeatedly embedded during two seconds. The 2-D basic pattern whose size is 96×96 is repeated eight times to vertical axis and horizontal axis, respectively. Thus, the watermark pattern is formed 768×768 dimensions and placed in the middle of the frame. The average PSNR value is 43.66dB for 'Documentary', 44.82dB for 'Fantasy', and 44.36dB for 'Drama'.

Fig. 2. An example of horizontally projected image.
4.2. Robustness testing

To measure the robustness, experiments have been performed against D-A/A-D conversion in practice, which include projective and affine transform as well as signal processing distortions. Clips are projected on a screen with same environment in Sec. 4.1 and captured with a SONY HDR-FX1 camcorder tripod-mounted subsequently. The camcorder is placed approximately three picture heights away from the screen. Table 1 shows the results as normalized correlation in real video processing.

4.1. Fidelity testing

We performed similar fidelity testing as described in [4]. Clips were displayed using an EPSON EMP-TW1000 projector, onto a wide screen. The horizontal length and vertical length of projected clip are about 2.20m and 1.24m. Four expert observers who know the detail of our scheme and adept at visual detection tasks participated in a two alternative forced choice experiment in which each trial consisted of two presentations of the same clip, once with and once without the watermark present. Observers viewed the screen from two picture heights and they were required to indicate which of the two clips contained the watermark. Each source clip was used in four such trials which lasted five minutes. No observer could determine the identity of the watermarked clip surely in any case.

Table 1. Results of the robustness against attacks in the proposed watermarking system. (1) D-A/A-D conversion, (2) MPEG-1 conversion, (3) MPEG-4 conversion, (4) Framerate change(30fps → 24fps), (5) Scaling to VGA

<table>
<thead>
<tr>
<th>Attack</th>
<th>Documentary</th>
<th>Fantasy</th>
<th>Drama</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>0.33</td>
<td>0.31</td>
<td>0.34</td>
</tr>
<tr>
<td>(1)→(2)</td>
<td>0.32</td>
<td>0.32</td>
<td>0.30</td>
</tr>
<tr>
<td>(1)→(3)</td>
<td>0.27</td>
<td>0.31</td>
<td>0.35</td>
</tr>
<tr>
<td>(1)→(4)</td>
<td>0.28</td>
<td>0.34</td>
<td>0.33</td>
</tr>
<tr>
<td>(1)→(5)</td>
<td>0.28</td>
<td>0.36</td>
<td>0.30</td>
</tr>
</tbody>
</table>

[threshold=0.11]

5. CONCLUSION

D-A/A-D conversion attack is common in digital cinema by capturing with a camera. Since this attack includes various geometrical distortions such as projection and RST as well as signal processing distortions, the general ACF scheme was vulnerable to D-A/A-D conversion attack. In this paper, we presented the robust watermark detection scheme against D-A/A-D conversion attack. We exploited LACF and constructed a mathematical model for watermark detection. Experimental results showed that the presented scheme is robust to D-A/A-D conversion attack as well as frame rate change, format conversion, scaling attack after camcording.

Acknowledgement

This work was in part supported by the KOSEF grant NRL program funded by the Korea government (MOST) (No. R0A-2007-000-20023-0), and the IT R&D program of MKE/IITA(2007-S017-01, Development of user-centric contents protection and distribution technology).

6. REFERENCES