

Novel Robust Video Watermarking Algorithm Based on Adaptive Modulation

Sang-Woo Lee, Dong-Il Seo
Information Security Division

Electronics and Telecommunications Research Institute
{ttomlee, bluesea}@etri.re.kr

Abstract— Video watermarking is a technology to protect copyright ownership. This paper presents a novel robust video watermarking algorithm based on adaptive temporal modulation. A watermark pattern is generated based on an analysis of the histogram of the host video. Then, a watermarked video is generated by temporally modulating the mean chrominance value of each chrominance channel in relation with the watermark pattern, depending on the characteristic of the original videos. Experimental results demonstrate that the proposed algorithm is robust against geometrical distortions and signal processing attacks including compression format conversion.

Keywords— Video watermarking, contents security

I. INTRODUCTION

Since digital media is easily reproduced and manipulated, the demand for protecting copyright ownership has increased [1]. A cryptographic technique is used to control access to multimedia content. In other words, the technique permits an authorized user who has a decryption key to access encrypted content. However, once such content is decrypted, there are no countermeasures to block illegal reproduction and distribution. Based on this situation, digital watermarking technology could be a complementary technique of cryptography-based protection methods [2], [3].

The main requirements of digital watermarking include imperceptibility, capacity, and robustness. The distortion caused by the watermarking process should remain imperceptible to a human observer and the watermarked video should maintain its visual quality. In other words, embedding a watermark should not have noticeable artifacts in the watermarked video. Capacity refers to the amount of information that is embedded by a watermarking algorithm in a host video. The robustness of a watermarking scheme refers to the detectability of watermarked information from watermarked content that has been modified by various attacks such as geometrical distortions and signal processing attacks. Since video processing requires significant computing resources, simplicity is another important requirement of video watermarking technology. In addition, blindness is an important requirement, as the original host video is not available for the detection procedure in many applications. It is important to note that these requirements are usually in conflict with one another. For example, if we increase watermark energy to increase the robustness, the visual quality

of the watermarked video may be decrease. Therefore, we should take this trade-off into consideration in designing a watermarking system on targeted applications.

For a long time, digital watermarking has focused mainly on still images. Currently, however, the study of watermarking algorithms for video has become a hot research topic. But while watermarking technologies for still images and video are similar, they are not identical. In particular, we can take into account the temporal dimension of a video stream. Several studies [6]-[8] have suggested robust video watermarking algorithms that do consider the temporal dimension. Leest et al. [6] proposed a watermark embedding method by increasing or decreasing the mean luminance value of each pixel of a frame. However, their algorithm requires the original video during the detection procedure. Do et al. [7] suggested a blind watermarking algorithm based on temporal modulation, but their algorithm is too complex to support real-time performance.

This paper presents a novel robust video watermarking algorithm based on adaptive temporal modulation. We employ the characteristics of video to support high robustness of the watermarking algorithm. First, the mean value of each frame is known to be resistant to geometrical distortions, signal processing attacks, and temporal frame dropping [8]-[10]. In addition, temporal modulation is resistant to these attacks. Temporal modulation refers to a watermark embedding technique that embeds a watermark bit by differentiating the pixel values between frames, depending on the watermark message. One study [7] used a temporal modulation scheme, but their algorithm cannot support real-time embedding performance for video as they employed a complex masking method based on a human visual system (HVS) to improve robustness. Nevertheless, [7] has high bit error rates in embedding a watermark in the video which has high variations of luminance and chrominance such as music shows. We suggest the simplified and robust watermarking algorithm based on adaptive temporal modulation to remove the drawback of [7].

II. PROPOSED WATERMARKING ALGORITHM

In general, a watermarking algorithm consists of two procedures: watermark embedding and watermark detection. In this section, we describe the proposed embedding procedure first. The blind detection procedure is then explained in detail

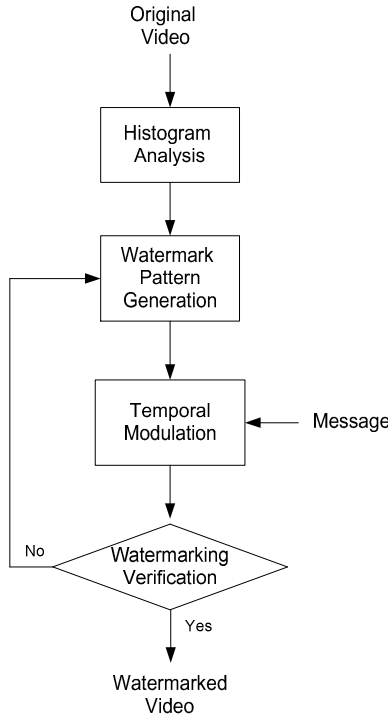


Figure 1. Watermark embedding procedure.

A. Watermarking embedding

The proposed watermark embedding algorithm is composed of three steps: watermarking pattern generation, adaptive temporal modulation, and watermark verification. Figure 1 shows the watermark embedding procedure of the proposed algorithm. A watermark pattern is generated based on a histogram analysis of the luminance channel for the original video stream. A watermarked video is then generated by temporally modulating the mean chrominance value of each chrominance channel in relation with the watermark pattern, depending on the watermark message and the mean of luminance values of the original video.

Watermark patterns are generated in the spatial domain of each frame. To generate the watermark patterns, we measure the mean luminance value of each frame because the histogram distribution of an image is approximately invariant under a geometric attack. In our watermarking algorithm, each frame of size $M \times N$ is considered. $R(x, y)$, $G(x, y)$, and $B(x, y)$ indicate three primary color values of the RGB color model. Here, (x, y) denotes the pixel position, where $0 \leq x < M$, $0 \leq y < N$. The watermark pattern generation is performed as follows:

1. All $R(x, y)$, $G(x, y)$, and $B(x, y)$ are transformed into $Y(x, y)$, $Cb(x, y)$, and $Cr(x, y)$ in the YCbCr color model.
2. Calculate the average values of $Y(x, y)$ such as

$$Y_{mean}(x, y) = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} Y(x, y) \quad (1)$$

3. The generated watermark pattern $W(x, y)$ is given by

$$W(x, y) = \begin{cases} +\alpha & \text{if } Y(x, y) \geq Y_{mean}(x, y) + (Y_{mean}(x, y) \times \beta) \\ -\alpha & \text{if } Y(x, y) < Y_{mean}(x, y) - (Y_{mean}(x, y) \times \beta) \\ 0 & \text{else.} \end{cases} \quad (2)$$

Here, α is the gain constant. We divide the watermark pattern into two parts based on the mean luminance value. One part of the watermark pattern is marked with positive value, $+\alpha$, and the other part is marked with the negative value, $-\alpha$. This α varies the result of the verification step. This scheme makes the watermarking method robust to low-pass filtering, such as converting the luminance value of each frame into the average luminance. β is the parameter used to choose the number of pixels that will be modified in one entire frame. For example, if β is 0.25, then pixels that have a value 0.25 times higher or lower than the mean luminance are marked with $+\alpha$ or $-\alpha$, respectively. The remaining part of the watermark pattern is set to zero. This means that the associated pixels maintain their original values. Therefore, β is a parameter that depends on a trade-off between robustness and invisibility. The proposed watermark patterns that are generated by analysing the mean luminance value based on the histogram do not depend on pixel location. Thus, they do not require geometric synchronization that compensates the geometrical distortions in the attacked video prior to detecting the watermark message during the detection procedure.

The watermark information is embedded in each frame of the original video by temporally modulating the mean pixel values. Depending on the watermark information, the pixel values are changed in order to differentiate the pixel value mean of the previous and following frames in the temporal axis. This is done by adding or subtracting the watermark pattern to or from the frame. Here, we modulate the chrominance channel in order to embed the watermark information, because modifications in the chromatic values are known to be less perceptible to humans than other channels [9]. The proposed temporal modulation can be presented as follows:

For $i = 1$ to the number of frames in the video

$$\begin{aligned} Cb'_i(x, y) &= Cb_i(x, y) - m \times W_i(x, y) \text{ if } i \leq \frac{K}{2}, \\ Cb'_i(x, y) &= Cb_i(x, y) + m \times W_i(x, y) \text{ if } i > \frac{K}{2}, \end{aligned} \quad (3)$$

where K refers to the number of consecutive frames; m denotes the watermark information bit and can be 1 or -1 ; $Cb_i(x, y)$ denotes the chrominance values in the i -th original frame; and $Cb'_i(x, y)$ denotes the watermarked chrominance values in the i -th watermarked frame. One bit of watermark information can be embedded in K consecutive frames. For example, assuming that K is 4, if the watermark information is 1, then the watermark patterns are subtracted from the first and second frames. The watermark patterns are added to the

third and fourth frames. If the watermark information is -1 , then the Cb values are modified to the contrary.

We assume that the average values of K consecutive frames do not vary too greatly. In general, this assumption is correct. However, in case of the video which has high variation of luminance and chrominance, this assumption cannot be applied. Therefore, we adopt the verification step which calculates the correlation of two watermarked frames. This step can be presented as the following equations:

$$Corr_{1st} = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} Cb'_{1st}(x, y) \times W_{1st}(x, y),$$

$$Corr_{2nd} = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} Cb'_{2nd}(x, y) \times W_{2nd}(x, y), \quad (4)$$

where Cb'_{1st} denotes the chrominance values of a frame in the first half of K consecutive frames, and Cb'_{2nd} denotes the chrominance values of a frame in the second half. W_{1st} denotes the generated watermark pattern of a frame in the first half of K consecutive frames, and W_{2nd} denotes the generated watermark pattern of a frame in the second half. $Corr_{1st}$ denotes the correlation value between Cb'_{1st} and W_{1st} . $Corr_{2nd}$ denotes the correlation value between Cb'_{2nd} and W_{2nd} . Due to the watermark embedding procedure, the correlations will increase or decrease in relation with the watermark information bits.

The extracted bit m' is determined by comparing two correlation values as follows:

$$m' = \begin{cases} 1 & \text{if } Corr_{1st} \leq Corr_{2nd} \\ -1 & \text{if } Corr_{1st} > Corr_{2nd} \end{cases} \quad (5)$$

If the extracted bit m' is not equal with the embedded bit m , then the watermark pattern generation step should be repeated with increased gain constant α .

B. Watermark extraction

The proposed watermark detection procedure consists of two steps: watermark pattern generation and computation of the correlation between the watermark pattern and the watermarked frame.

Figure 2 illustrates the proposed watermark detection procedure. As shown in the figure, the proposed watermark detection does not require the original video. That is, the proposed watermarking algorithm supports blind detection. First, the watermark pattern generation step is performed, which is the same step as in the watermark embedding procedure. Then, the correlation between the generated watermark pattern and watermarked frame is computed as same as the watermark verification step in the embedding procedure.

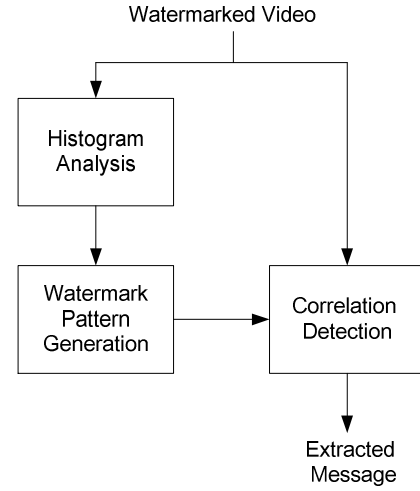


Figure 2. Watermark detection procedure.

Notice that the generated watermark patterns in the watermark detection procedure are usually not equal to those in the watermark embedding procedure because the watermarked video could be changed due to geometrical distortions and signal processing attacks. Although the watermarked frames and watermark patterns are modified, it does not affect the detection of a watermark information bit. This is because the proposed detection algorithm determines the watermark information bit depending on the comparison results of the two correlation values as in (5). In other words, even though the correlation values of the attacked videos are different from those of the original video, we can detect the correct watermark message on the condition that the comparison results of the two correlation values are maintained. This is a benefit of the temporal modulation scheme.

III. EXPERIMENTAL RESULTS AND ANALYSIS

In this section, we explain the performance of the proposed watermarking algorithm. We fixed some parameters in order to evaluate our algorithm. The length of the message was set as 36 bits. This is a reasonable length of watermark information as we consider that the watermarking data payload is required to be a minimum of 35 bits in digital cinema specifications [11]. For embedding the algorithm parameters, we set α (initial value) = 1, β = 0.25, and K = 4.

TABLE 1. TEST VIDEOS.

No.	Test video	Size	FPS	Frame
1	High way	352 x 288	29.97	2000
2	Paris	352 x 288	29.97	1065
3	Music show 1	640 x 352	29.97	1000
4	Music show 2	640 x 352	29.97	1000

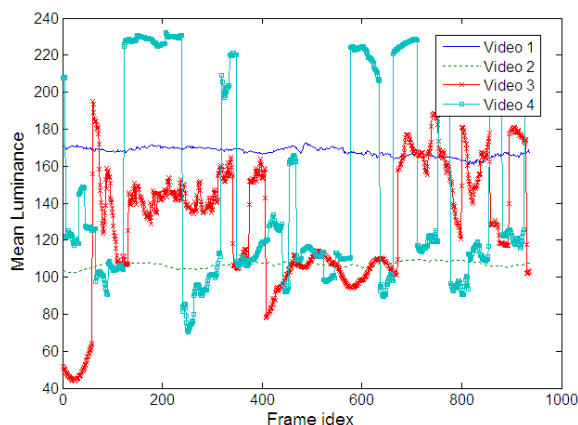


Figure 3. Mean luminance values of the test videos.

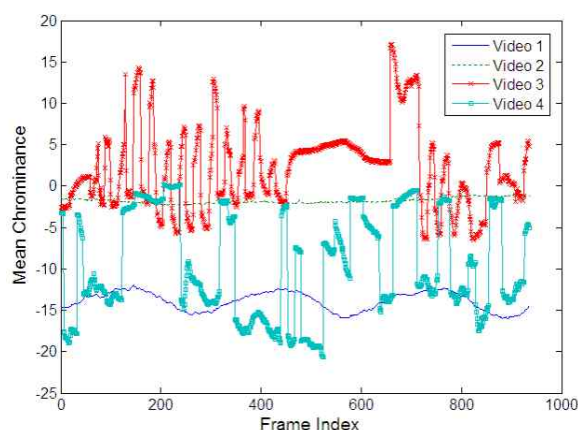


Figure 4. Mean chrominance values of the test videos.

Also, we set the increase of α as 1. The proposed watermarking algorithm was tested on four test videos, as shown in Table 1. Videos 1 and 2 are frequently used as video watermarking tests. Videos 3 and 4 are music shows. The mean luminance values and the mean chrominance values of the test videos are illustrated in Figs. 3 and 4, respectively. Two famous video clips, Highway and Paris, have an approximately constant mean luminance and chrominance. However, Videos 3 and 4 have much higher variations of luminance and chrominance than the other videos because the stage lighting of music shows change quite frequently. This characteristic has a large effect on the robustness of the watermarking algorithm.

To evaluate the robustness to various attacks, we measured average bit error rates of the attacked videos in the watermark detection procedure. We used VirtualDub to attack the watermarked videos. This application is widely used as a video editor. The robustness of each test video is summarized in Table 2.

First, we evaluated the robustness to geometric distortions. A rotation attack was performed by rotating the watermarked video clockwise and anti-clockwise by 15 degrees. For a cropping attack, we kept the central part of the watermarked video.

TABLE 2. THE BIT ERROR RATES OF TEST VIDEOS.

	Video 1		Video 2		Video 3		Video 4	
	[7]	This	[7]	This	[7]	This	[7]	This
Rotation 15°	0	0	0	0	4.16	0	3.13	0
Cropping 10%	0	0	0	0	3.12	0	2.08	0
Scaling 0.5	0	0	0	0	4.16	0	2.08	0
Projective	0	0	0	0	3.12	0	3.13	0
Smoother	0	0	0	0	3.12	0	2.08	0
Sharpening	0	0	0	0	4.16	0	3.13	0
H.264/AVC	0	0	0	0	4.16	0	3.13	0

We cut 10 percent of the upper, lower, left, and right sections of the watermarked video. We also scaled the watermarked video to half of its original size. Recorded copies from a camcorder suffer geometric transformations including rotation, scaling changes, and non-linear transformation caused by an angle difference between the camcorder and screen. A projective transform is the modeling of video distortion by a camcorder recording. The experimental results show that the proposed watermarking algorithm is robust to geometric distortions such as rotation, scaling, cropping, and projective transform.

Second, we evaluated the robustness to signal processing attacks. The results for videos suffering smoothing and sharpening attacks show that our watermarking algorithm is resistant to low-pass and high-pass filtering, respectively.

Finally, the watermarked videos were compressed into H.264/AVC format. Since end-users are likely to display downloaded content on portable devices that have smaller storage, they will commonly convert their video into MPEG-4 format. The experimental results show that the proposed watermarking algorithm is robust to compressed format conversion.

The experimental results are shown in Table 2. We compared the proposed algorithm with [7]. In case of Video 1 and 2, both algorithms showed high robustness. However, in case of Video 3 and 4, [7] showed high bit error rates since these videos have high variations in luminance and chrominance. On the contrary, our watermarking algorithm showed high robustness because the proposed algorithm compensates watermark gain at the watermarking verification step in the watermark embedding procedure.

IV. CONCLUSION

This article presented a novel robust video watermarking algorithm based on adaptive temporal modulation. A watermarked video is generated by temporally modulating the mean chrominance value of each chrominance channel in relation to the watermark pattern according to the watermark message. The watermark pattern is generated based on a histogram analysis of the luminance channel. In particular, the proposed watermarking algorithm improved the robustness by modulating watermark power adaptively depending on the

characteristic of host videos. The experimental results showed that the proposed watermarking algorithm is resistant to geometrical distortions such as rotation, cropping, scaling, and projective transforms. The proposed watermarking algorithm is also robust against signal processing attacks including compression format conversion.

REFERENCES

- [1] Shiguo Lian and Zhongxuan Liu, "Secure Media Content Distribution Based on the Improved Set-Top Box in IPTV," *IEEE Transactions on Consumer Electronics*, vol. 54, no. 2, May 2008.
- [2] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," *Proceedings of the IEEE*, vol. 87, no. 7, July 1999, pp. 1079-1107.
- [3] G. Doërr and J. Dugelay, "A Guide Tour of Video Watermarking," *Signal Processing: Image Communication*, vol. 18, no. 4, Apr. 2003, pp. 263-282.
- [4] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoan, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, 1997, pp. 1673-1687.
- [5] K. Kim, H. Lee, D. Im, and H. Lee, "Practical, Real-time, and Robust Watermarking on the Spatial Domain for High-Definition Video Contents," *IEICE Transactions on Information and System*, vol. E 91-D, no. 5, May 2008, pp. 1359 - 1368.
- [6] A. Leest, J. Haitsma, and T. Kalker, "On Digital Cinema and Watermarking," *Proceedings of the SPIE*, vol. 5020, 2001, pp. 526-535.
- [7] H. Do, D. Choi, H. Choi, and T. Kim, "Digital Video Watermarking Based on Histogram and Temporal Modulation and Robust to Camcorder Recording," *Proceedings of 8th IEEE International Symposium on Signal Processing and Information Technology*, December, 2008, pp. 330-335.
- [8] C. Chen, J. Ni, and J. Huang, "Temporal Statistic Based Video Watermarking Scheme Robust against Geometric Attacks and Frame Dropping," *Proceedings of IWDW 2009*, LNCS 5703, 2009, pp. 81-95.
- [9] C. Lin, D. Chan, H. Su, and W. Hsieh, "Histogram-oriented Watermarking Algorithm: Colour Image Watermarking Scheme Robust against Geometric Attacks and Signal Processing," *IEE Proc.-Vis. Image Signal Process.* vol. 153, no. 4, August 2006, pp. 483-492.
- [10] S. Xiang, H. Kim, and J. Huang, "Invariant Image Watermarking Based on Statistical Features in the Low-Frequency Domain," *IEEE Transactions on Circuit and Systems for Video Technology*, vol. 18, no. 6, June 2008, pp. 777-790.
- [11] Digital Cinema Initiatives, LLC, Digital Cinema System Specification Version 1.2, March 2008.