WATERMARKING ROBUST AGAINST ANALOG VCR RECORDING

Koichi Magai, Hiroshi Ito*, Hidetoshi Mishima**, Mitsuyoshi Suzuki*, and Kohtaro Asai**

Mitsubishi Electric Corporation
*Information Technology R&D Center, 5-1-1 Ofuna, Kamakura-city, Kanagawa, Japan 247-8501
**Advanced Technology R&D Center, 1 Babazusho, Nagaokakyo-city, Kyoto, Japan 617-0828

ABSTRACT

Watermarking techniques are now in the spotlight to protect their copyrights. Enough verifications of robustness against analog VCR recording, however, have not been performed explicitly in previous work while analog copied contents have raised their fidelity. We study on a watermarking technique that has durability against analog VCR copying. We found that the watermarks well survive after D/A and A/D conversions and VCR recording when they are embedded in the wavelet transform domain with three times horizontal and one time vertical 2-to-1 decimations. Our method increases the relative power of the watermark signals using the spread spectrum technique. Additionally, it varies embedding density as well as the magnitude of the watermark signal as an adaptive control. We embedded 64-bit information into a video sequence using the proposed method and confirmed that we can detect the watermarks correctly even from the analog copies recorded with the VHS standard mode.

1. INTRODUCTION

Improvement in quality of analog processed contents in recent years has made duplication using analog VCRs a possible way to create illegal copies that can possibly be a security hole of conventional technologies.

To protect digital images from VCR based copying, several Copy Guard Signal methods are implemented such as Macrovision's ACP (Analog Copy Protection system), which prevents images from illegal analog copying by manipulating signal in VBI (Vertical Blanking Interval). The signal, however, can be removed without degradation of the original image signal.

CPTWG (Copy Protection Technical Working Group) is having a discussion on watermarking that has durability against analog processing [1]. Although VWM (Video Watermarking) Companies propose watermarking technology robust against VHS copying there, they open to the public neither detailed algorithm nor verification results of robustness against VCR recording of the method.

There are many other watermarking methods that seem to have durability against analog processing. Some of them embed watermark signal into low or middle band frequencies of transformed image data [2], but we can hardly find works that make organized measurement of analog channel interferences with a watermark signal and develop a watermarking scheme based on the result of the measurement.

To contribute the evolution of watermark schemes, it is meaningful to perform quantative measurement of influences of analog processing against watermark signal and consider a watermark scheme robust against analog processing based on the result of the measurement.

With the above background, we performed fundamental examination on a watermarking method that is robust against analog VCR recording. We confirm that we can detect 64-bit information correctly with our method from copies recorded once on a VCR with VHS standard mode.

The rest of the paper is organized as follows. Section 2 investigates the characteristics of analog channels from the viewpoint of watermarks. Based on this investigation, we describe our proposed watermarking method in Section 3. Section 4 shows some experimental results followed by concluding remarks in Section 5.

2. ANALOG CHANNEL CHARECTERISTICS

In the analog channel, there are several factors that may influence watermarks, some of which are 1) random noises, 2) frequency degradations, 3) crosstalks, 4) non-linear processing, and 5) geometric change of sampling points. Since many watermarking schemes are robust to random noises, we investigate other factors in the following.

Most analog VCRs have input terminals for the composite signal in which chrominance signals are multiplexed with the luminance signal by amplitude modulation with the 3.579545MHz subcarrier. When the composite signal is input to the VCRs, it must first be separated into the luminance and the chrominance, but the

0-7803-8554-3/04/$20.00 ©2004 IEEE.

separation is often not perfect and causes crosstalks that are called dot-interferences and cross-colors. To prevent the watermark from being affected, the frequency components carrying the information must be carefully selected; the frequency band centered on the color subcarrier (3.579545 +/- 0.5MHz) should be avoided for watermarks embedded in the luminance signal.

The bandwidths of the recorded signals are limited and the frequency spectrum is also degraded during the analog processing in the VCRs. Bandwidth of the luminance signal is limited to 3MHz in the normal VHS mode and to 5MHz in the S-VHS mode. Further, the signal is frequency-modulated with a low frequency carrier. The chrominance signals are converted into the 629KHz band that is the lower part of the frequency-modulated signal. The mixed signal is recorded on the tape. All of these processing degrade the frequency spectrum further and in most cases high frequency components are attenuated.

High frequency components are susceptible to non-linear processing in the recording as well. Parts of high frequency components of the frequency-modulated signal are clipped within some frequency range. This non-linear processing often affects the edge fidelity where the signal changes abruptly in the horizontal direction.

In addition to the above degradations, there are geometric distortions. Once the signal is converted to the analog form, the information for horizontal registration is lost. Although this kind of global desynchronization can be easily combated, local change of sampling points must be taken into consideration. Jitters caused by fluctuation in the speed of rotating heads introduce such local shifts in the recorded video signals.

All of the above investigations lead us to a scheme where the watermark is embedded in low frequency components of the video. Since most of the processing in the analog channel is done in one-dimensional domain, this applies only to the horizontal direction. Little degradation is expected in the vertical and temporal direction in the analog channel. Embedding watermarks in low frequency components conforms the strategy that places watermarks in perceptually significant part of images [3]. However, since the human visual system is sensitive to low frequency distortions if they change temporarily, there is a tradeoff between the robustness and the perceptual quality of the watermarked video.

In the following, this tradeoff is compromised and an appropriate watermarking scheme is designed using the spread spectrum technique and the wavelet transform. We use the spread spectrum technique because of its robustness against noise and changes of a luminance level, and use the wavelet transform to extract lower band frequencies for jitter durability.

Table 1.
α values calculated in the D/A-A/D conversion

V \ H	0	1	2	3
0	0.1782	0.3565	-	-
1		0.3582	0.4988	0.5577
2		-	0.4981	0.5500
3		-	-	0.5539

Table 2.
α values calculated in the jitter simulation

V \ H	0	1	2	3
0	0.3392	0.6547	-	-
1		0.6390	0.8621	0.9555
2		-	0.8587	0.9447
3		-	-	0.9463

H and V in the tables above show the number of the wavelet conversion times in the horizontal and the vertical direction respectively.

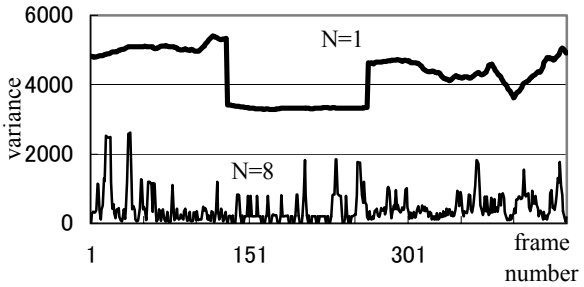

Fig.1. The attenuation of the power of N integrated image (N=1,8)

3. WATERMARKING

3.1. Choosing a base image to embed watermarks

To determine the best base image to embed the watermark, we measured remaining rate of Gaussian signals embedded in the image as a watermark, after analog processing under several decomposition levels. Using gray scale images for measurement because of its simplicity, we perform D/A-A/D conversion and add VCR jitters with a VCR simulation program as analog processing attacks to the images.

Let σ^2_{in} be a variance of the input Gaussian signals and σ^2_{out} be a variance of the Gaussian signals extract from the image after analog processing, we can see $\alpha = \sigma^2_{out} / \sigma^2_{in}$ as the remaining rate of the watermark signal. From the result of the measurement, the watermark signal remains best when the image is decomposed three times horizontally and once vertically. Table 1 and Table

2 shows a part of the values of α, for the case of A/D-D/A conversion and VCR jittering respectively. We call the decomposed low frequency image the base image hereafter.

3.2. Embedding a watermark

Consecutive frame integration after spread spectrum along the temporary direction eliminates a correlation of the resulting image signal. Fig 1 shows that if the number of integrated frames increases, power of signal of the resulting image comes to 1/N in relative power to each of the original images.

In our method, we create a spread pattern from three different patterns consisting of +1 and –1, two of which are spatial patterns and the rest is a temporal one. One of the two spatial patterns is fixed, and we have the other spatial pattern and the temporal pattern vary with pattern creation keys. This helps to avoid image degradation and to keep security of the resulting image.

Each sign of watermark values to be embedded is decided according to each corresponding sign of the spread pattern, and then the values are added to the original base image of a frame. Namely, let x_{ij} be a pixel value of the original base image at (i, j) and x'_{ij} be a value of x_{ij} after watermarking, then we have

$$x'_{ij} = w \times \delta \times \left(a_{ij} \times b_{ij} \times c_k\right) + x_{ij} \qquad (1)$$

where $\delta \in \{-1,+1\}$ represents information to be embedded as a watermark, a_{ij} is the fixed spatial pattern, b_{ij} and c_k are the spatial pattern and the temporal pattern created by each key respectively, and w represents a weighting factor for the adaptive control.

At the detection of the watermark, if we perform spread spectrum on target frames and then integrate them, the power of the original image signal will be weaken and the power of the watermark signal will increase.

3.3. Detection of the watermark

We detect the watermark in the following process.

(a) Extract subsequent *M* base images from video.

(b) Extract *N* pixels from each of the base images computed in (a). The number of extracted pixels is *NM*.

(c) Calculate the following *R* using values of the *NM* pixels extracted above;

$$R = (1/NM)\sum_{i,j,k} x^*_{ijk} \times \left(a_{ij} \times b_{ij} \times c_k\right) \qquad (2)$$

where x^*_{ijk} represents a pixel value at coordinate (i, j) of frame k in the base image in (a), and, a_{ij}, b_{ij} and c_k are the same spread patterns as created when embedding at coordinate (i, j) of frame k.

(d) With a threshold $th(\geq 0)$, $R \geq th$ and $R \leq -th$ denote detections of bit "1" and "0" respectively.

3.4. Adaptive control

To vary the strength of the watermark as an adaptive control, we alter embedding density of the watermark as well as its magnitude. If the strength of the watermark is the same, the more the magnitude of the power of high frequency component in the region where watermark is embedded, the less the perceptive image degradation is, generally. Although applying wavelet decomposition once on a image yields three high frequency component images, LH, HL and HH, we make use of only the LH component to decide the strength of watermark adaptively because the result of subjective estimation on the degradation of watermarked images in which the strength of the watermark was decided adaptively according to LH value was the best. The reason seems that factors of motion are also reflected in the LH component in the case of interlaced scanning. We determined parameters of watermark strength experimentally based on the result of an actual VCR recording (Fig 2).

4. EXPERIMENTAL RESULTS

4.1. Bitwise detection

In order to evaluate the proposed watermarking method, we took three standard images from ITE [4], "Japanese Room", "European Market" and "Walk through the Square", and embedded 64-bit information in 450 frames of motion pictures and detected them from copies after analog VCR recording. In our experimentation, we confirmed image shifts mentioned in Section 2, about 3 to 5 pixels horizontally and about 0 to 1 pixels vertically. Therefore the video images should be synchronized temporally and spatially before the detection process in practice. We made synchronization by correlation with the original image frames now. We are studying synchronization scheme using embedded pattern but have not implemented it yet.

The rate of correct bit detection from copies recorded once on VHS tapes by the standard mode were 99.997% for Japanese Room, 99.941% for European Market, and 99.997% for Walk through the Square respectively.

4.2. Influence of VCR recording on the watermark

To evaluate the influence of analog VCR recording on the watermark signal, we measured the normalized ratio of $\overline{R}$ values before and after VCR recording, where $\overline{R}$ values are the average of 64 R values given by equation (2) with M=10 when embedding 64 1's in images. We also measured the normalized ratio of standard deviations (STD) of the R values.

From the result of the measurement, average values over 450 frames (the ratio of $\overline{R}$ s, the ratio of STD of Rs) became (0.70, 1.16) for Japanese Room, (0.73, 1.21) for European Market and (0.83, 1.24) for Walk through the Square respectively. These results indicate that the watermark signal was attenuated to about 70% and the dispersion of R values increased by about 20% after recording once over the analog VCR.

4.4. Measurement of the effects of the adaptive control

To investigate if the adaptive control took effect, we measured the correct detection rate when embedding 64 1's in images with the adaptive control mentioned in section 3.4, where we set the threshold value $th = 0$. We also took the same measurement on images where the watermark was embedded at the fixed 50% density.

From the result, we could confirm the effect of the adaptive control. For example, in the "European Market" image sequence, the error rate decreases to about 1/30, from the error rate of 1.7% to 0.06% approximately.

We also measured the average and the STD of R values extracted from watermarked images with and without the adaptive control. In Fig 3, we can see that the average values of R increase and the watermark strength changes according to scenes.

5. CONCLUSION

We examined the watermarking method that is robust against analog processing and confirmed the possibility to detect 64-bit information of watermark correctly even after recording once on a VHS tape by the standard mode.

We measured remaining rate of the watermark signal and confirmed that it is possible for the watermark to have durability against D/A-A/D conversion and VCR jittering if it is embedded in a base image extracted by subband decompositions of wavelet transform performed three times for horizontal and once for vertical directions. Then we used a spread spectrum technique to embed a watermark. We confirm that our method increases the power of the embedded watermark signal relative to the original image signal while avoiding image degradation

ALV	0	2	4	6	8	10	14	18
DST(%)	0	25	50	75	100	50	75	100
MAG	0	1	1	1	1	2	2	2

ALV: average of LH absolute values
DST: density to embed
MAG: magnitude

Fig.2. Experimental parameters for the adaptive control

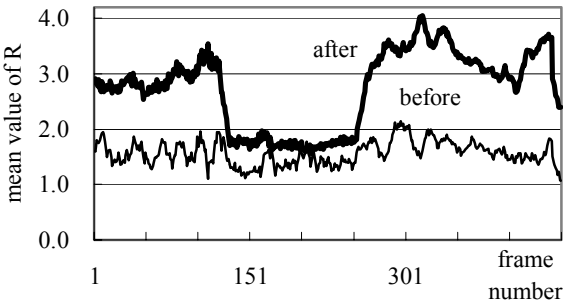

Fig.3. Mean values of R before/after the adaptive control

and keeping security of the resulting image by using a spread pattern that varies with pattern creation keys. As an adaptive control, we propose a method that alters embedding density of the watermark as well as magnitude of pixel values according to LH component values of wavelet transform, and we confirm the method works well.

For the purpose of practical use, we are going to make further studies on (a) Auto-recovery of spatial and temporal synchronization for detection, (b) Improvement of adaptive control for detection accuracy improvement, (c) Establishment of a method to estimate the reliability of detected values, and (d) Durability to HD-SD down conversion.

This work is being performed as a part of the contract research, "Research and development on the watermark technology robust against analog processing", from National Institute of Information and Communications Technology (NICT).

6. REFERENCES

[1] http://www.cptwg.org/
[2] "Watermarking Digital Image and Video Data", IEEE SIGNAL PROCESSING MAGAZINE, Sep. 2000.
[3] I. J. Cox, et al., "Secure spread spectrum watermarking for multimedia," NEC Research Institute, TR95-10, 1995.
[4] http://www.ite.or.jp/