A Viable System for Tracing Illegal Users of Video

Hyunho Kang[1], Brian Kurkoski[2], Youngran Park[3],
Sanguk Shin[3], Kazuhiko Yamaguchi[2], and Kingo Kobayashi[2]

[1] Graduate School of Information Systems,
University of Electro-Communications,
1-5-1, Chofugaoka, Chofu-shi, Tokyo 182-8585, Japan
kang@ice.uec.ac.jp
[2] Dept. of Inf. and Communications Eng.,
University of Electro-Communications,
1-5-1, Chofugaoka, Chofu-shi, Tokyo 182-8585, Japan
{kang, kurkoski, yama, kingo}@ice.uec.ac.jp
[3] Department of Information Security, Pukyong National University,
599-1 Daeyeon-3Dong,
Nam-Gu, Busan 608-737, Republic of Korea
Podosongei@hanmail.net, shinsu@pknu.ac.kr

Typical uses of watermarks include copyright protection and disabling unauthorized access to content. Especially, copyright protection watermarks embed some information in the data to identify the copyright holder or content provider, while receiver-identifying watermarking, commonly referred to as fingerprinting, embeds information to identify the receiver of that copy of the content. Thus, if an unauthorized copy of the content is recovered, extracting the fingerprint will show who the initial receiver was [1][2]. In this paper we generalize our previous work [3] of a video fingerprinting system to identify the source of illegal copies. This includes a logo embedding technique, generalization of the distribution system and detailed investigation of the robustness against collusion attacks.

In our method, ECC is integrated into the watermarking system proposed in [4]. ECC based on convolutional codes are easy to implement and fast to encode and decode, so we use this type of code to correct errors in the logo which are introduced by attacks, compression and fingerprinting. The resulting system is evaluated under our fingerprinting channel with collusion attacks and MPEG compression. In our experiment, a 3-level temporal wavelet transform was performed on 112 frames of video, resulting in 8 types of frames (LLL, LLH, LHL, LHH, HLL, HLH, HHL, HHH

Table 1. Symbols used in our system with examples

	# of sub-tree	Depth of sub-tree	Order of sub-tree	# of video frame	# of max user	Wavelet level	Buyer area	# of total user
symbol	M	d	r	f	$N=r^d$	$l=\left\lfloor \log_2 \frac{f}{N} \right\rfloor$	$(L)^{l-1}H$	$M\times N$
example	1,000	3	2	112	8	3	*LLH*	8,000
	100,000	5	4	172,800	1,024	7	*LLLLLLH*	1.024×10^8

H. Chen et al. (Eds.): WISI 2006, LNCS 3917, pp. 156 – 158, 2006.

where L and H stand for low and high frequency respectively). In the experiment, the 14 sequential frames from the LLH (low-low-high) frames were selected because it was found to have the minimum errors. The channel equivalent to the fingerprinting system was found to be a random error channel therefore we have reliable decoding using ordinary error correcting codes. This fact will give us better visibility for the extracted logo. Table 1 shows the generalized decision method of embedding areas in video content.

A powerful attack against digital fingerprinting is the collusion attack. The results of our experiment show that the algorithm has some built-in resilience to collusion attacks, since the algorithm uses a long, uniformly distributed random number as fingerprinting information.

A powerful collusion attack is the maximum-minimum collusion attack proposed by Stone [5]. The attacked video is created by taking the average of the maximum and minimum values across the components of the fingerprinted video. The new zero correlation attack [6] is a modification method from Stone's collusion attack. This attack selects a fingerprinted video from a number of available fingerprinted videos. In this attack, some fingerprinting information is destroyed. However, we know that $user_1$, $user_3$, $user_4$ and $user_7$ were colluding (see Fig. 1).

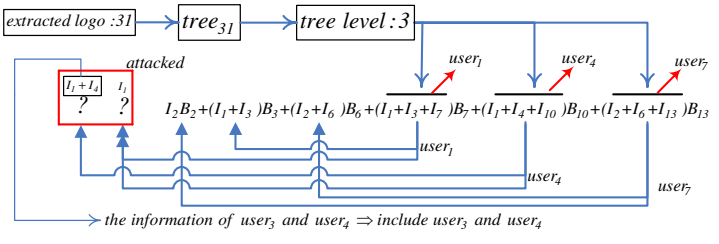

Fig. 1. Tracing illegal users under zero correlation attack

We also considered the averaging collusion attack of Cox, et al. [7] and the negative correlation collusion attack which drives the correlation coefficients to a negative value [5], and obtained similar good results. We have presented an approach for tracing illegal users in content distribution networks using video fingerprinting implementation. The video embedding method is robust to various attacks because of the use of the temporal wavelet transform. We improved the robustness of the tree number logo by using ECC, which permits support of a large number of users.

References

1. Judge, P., Ammar, M.: Security Issues and Solutions in Multicast Content Distribution. IEEE Network, Vol.17. (2003) 30-36
2. Furht, B., Kirovski, B.: Multimedia Security Handbook, CRC Press, (2005)

3. Kang, H.H., Kurkoski, B., Park, Y.R., Lee, H.J., Shin, S.U., Yamaguchi, K., Kobayashi, K.: Video Fingerprinting System using Wavelet and Error Correcting Code. WISA'05, Lecture Notes in Computer Science, Vol. 3786. Springer-Verlag, (2005) to appear
4. Kang, H.H., Park, Y.R., Park, J.H.: Blind Watermarking based on the Spatial Domain. Conference on Korea Multimedia Society, Vol. 5, No.1, (2002)
5. Stone, H.: Analysis of Attacks on Image Watermarks with Randomized Coefficients. NEC Technical Report. (1996)
6. Wahadaniah, V., Guan, Y.L., Chua, H.C.: A New Collusion Attack and Its Performance Evaluation. IWDW'02, Lecture Notes in Computer Science, Vol. 2613. Springer-Verlag, (2003) 64-80
7. Cox, I.J., Kilian, J., Leighton, T., Shanmoon, T.: Secure Spread Spectrum Watermarking for Multimedia. IEEE Trans. On Image Processing, Vol. 6, No. 12, (1997) 1673-1687