International Symposium on Information Theory and its Applications, ISITA2006
Seoul, Korea, October 29–November 1, 2006

Specifying the Subtree Number of A Content Distribution Tree Using Visual Cryptography

Hyunho Kang[†], Brian Kurkoski[††] , Kazuhiko Yamaguchi[††] and Kingo Kobayashi[††]

[†] Graduate School of Information Systems
University of Electro-Communications
1-5-1 Chofugaoka, Chofu-shi, Tokyo, 182-8585 Japan
E-mail: kang@ice.uec.ac.jp

[††] Dept. of Inf. and Communications Eng.
University of Electro-Communications
1-5-1 Chofugaoka, Chofu-shi, Tokyo, 182-8585 Japan
E-mail: kurkoski, yama, kingo@ice.uec.ac.jp

Abstract

In our previous study, we have presented an approach for a video fingerprinting system [1]. Recently, we have proposed some methods for generalization and considered tree specific and endbuyer specific problem under collusion attacks [2][3]. In this paper, we use a visual cryptography scheme to minimize deterioration of tree-specific problem in our previous work. This approach is able to detect distinctly the logo image of our previous content distribution system even if the video content has been distorted by collusion attacks.

1. INTRODUCTION

In our previous work [1-3], we concentrated on tracing illegal users in DRM systems for digital video distribution. Typical uses of watermarks include copyright protection and disabling unauthorized access to content. Copyright protection watermarks embed information in the data to identify the copyright holder or content provider. 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 [4].

In this paper, we use visual cryptography to minimize deterioration of the extracted logo image (tree number) observed in our previous works and describe the revised summary of our previous works. While there can be no doubt that the logo extraction performance will be improve using visual cryptography scheme, there is some question as to the case when colluders belong to more than one tree. In [5] the authors propose an extended visual cryptography scheme, this method will be, in fact, the key to solve the problem in our opinion.

Visual cryptography [6] applies human vision visual model to protect the secret message, which can be text or an image. It represents the secret message by several different binary images called shares. It is hard to perceive any clues about a secret image from individual shares. However, when parts of all of these shares are aligned and stacked together the secret message will be revealed [7].

This paper is outlined as follows. In Section 2 we give a review of visual cryptography briefly and other considerations. Section 3 presents simulation results. Finally, Section 4 gives the conclusion.

2. PROPOSED METHOD

2.1. Summary of previous work

Content is distributed along a specified tree, with the seller (producer) as the root, and the buyers as the internal nodes or leaves (Fig. 1). Because there are a limited number of buyer areas available in each tree, we have proposed to build sub-trees, where each subtree is watermarked with a distinctive logo. In our scheme, we will use logos which are bit-mapped images of the tree number.

Definition 1. Let $\gamma \in \mathbb{Z}+$ be the unique ID for seller S, let k be the random number obtained from the seed ID γ, where k is a vector of floating point numbers from -1 to 1 of dimension $h \times v$ (the video frame size).

Definition 2. Let $\delta \in \mathbb{Z}+$ be the unique ID for buyer B, let p be the random permutation vector with the seed δ, of dimension $h \times v$ (as a video frame size).

In Fig. 1, the buyer (B_j) transmits number p to the seller (S_i). The seller generates fingerprinting information $I_j = p(k)$. S_i selling to B_j inserts I_j and $I_a, I_b, ...$ into $buyer_j$ area, where $I_a, I_b, ...$ is the fingerprinting information for the parents of B_j in the tree. Note that because the video is passed hierarchically through the tree, fingerprinting information in areas $a, b, ...$ is already present. There exists a unique

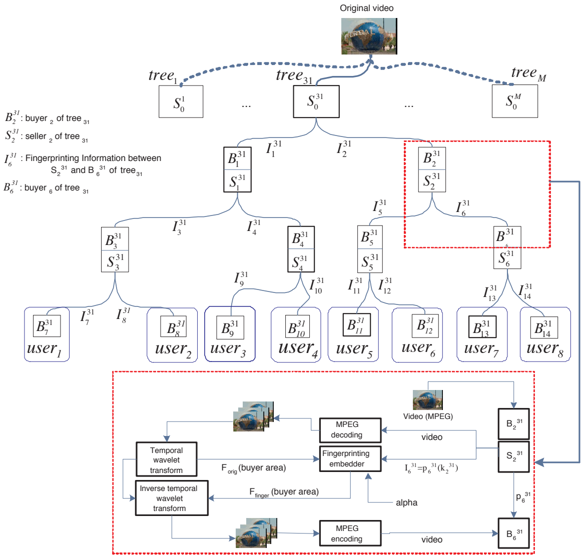

Figure 1: Content Distribution Tree and Fingerprinting Embedding Step (when node-S_2 and node-B_6 engage in a transaction). Pay attention number of tree was omitted in the text. If we have N_{sub} sub–trees (with N_{sub} logos) and N_{user} users per subtree, then we can support N_{sub} × N_{user} users.

Table 1: Fingerprinting information of $user_3$ video, example in Fig. 1 (B:buyer area, F:fingerprinting information)

B	1	2	3	4	5	6	7
F	I_1			I_1, I_4			
B	8	9	10	11	12	13	14
F		I_1, I_4, I_9					

path between the root and user, which can be extracted to distinguish between the paths. For example, when *node*-S_0 and *node*-B_1 engage in a transaction, fingerprinting information (I_1)—generated by the buyer and seller exchanging keys—is inserted into $buyer_1$ area of the transmitted video. When *node*-S_1 and *node*-B_4 engage in a transaction, fingerprinting information (I_1 and I_4) are inserted into $buyer_4$ area of the transmitted video. When *node*-S_4 and *node*-B_9 engage in a transaction, fingerprinting information (I_1, I_4 and I_9) are inserted into $buyer_9$ area of the transmitted video.

Therefore, whenever a seller distributes content to a buyer, different fingerprinting information is inserted. The fingerprinting information in $user_3$'s video is presented in Table 1.

Please refer to [1-3] for an additional discussion of our fingerprinting scheme.

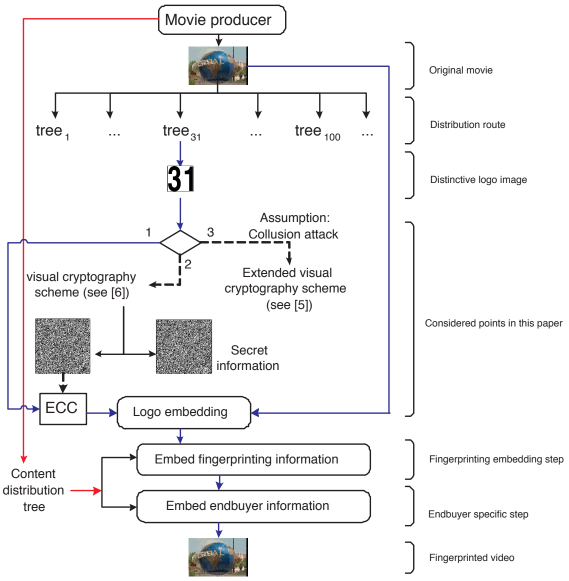
Movie producer
tree $_1$
...
tree $_{31}$
...
tree $_{100}$
...
31
1
3
2
Assumption: Collusion attack
visual cryptography scheme (see [6])
Extended visual cryptography scheme (see [5])
Secret information
ECC
Logo embedding
Content distribution tree
Embed fingerprinting information
Embed endbuyer information
Original movie
Distribution route
Distinctive logo image
Considered points in this paper
Fingerprinting embedding step
Endbuyer specific step
Fingerprinted video

Figure 2: Block diagram for fingerprinting system (embedding)

2.2. Specifying the subtree number

In this paper, we have added a visual cryptography scheme described in sub-section 2.3 (see also [5-9]) as the first part of the total fingerprinting system. Certainly the stacked image by two shares will result in a noise-like visual appearance, but the decoded image is still visible.

The embedding part falls into three steps which are tree logo embedding part using visual cryptography (which we call considered points in this paper), fingerprinting embedding step and endbuyer specific step (see Fig. 2). The logo embedding part is integrated into our previous watermarking system proposed in [10]. In particular, we may summarize the collusion attack question briefly based on the method [5](see Fig. 4).

In our main system (video fingerprinting), collusion attacks such as averaging, maximum minimum, negative correlation and zero correlation collusion attacks are very powerful. Within the limits of a collusion attack on a single subtree, the attacked logo can be extracted. But if the collusion attack spans more than one subtree, distinctive logos are superimposed making it difficult to identify the subtrees of the colluding users. The technique proposed by Ateniese et al. [5] will be, in fact, the key to solve this problem. Fig. 4 indicates that an image of tree number as innocent looking images can be used in our content distribution system.

The detecting part falls into four steps which are tree check step using visual cryptography, fingerprint-

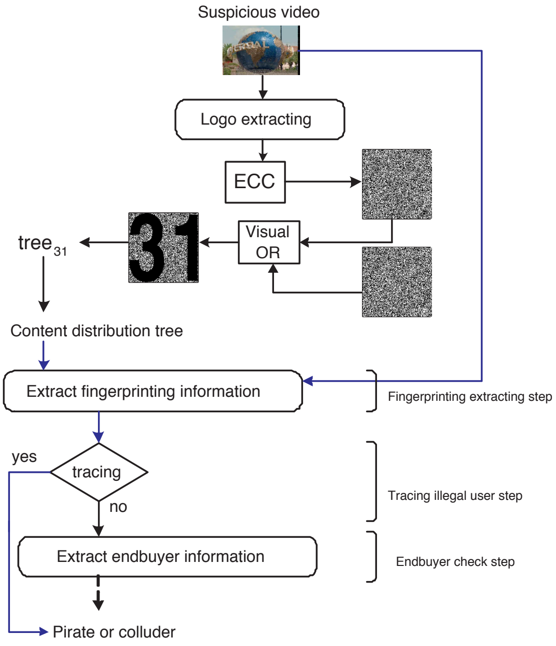
Suspicious video
Logo extracting
ECC
Visual OR
31
tree 31
Content distribution tree
Extract fingerprinting information
Fingerprinting extracting step
yes
tracing
no
Tracing illegal user step
Extract endbuyer information
Endbuyer check step
Pirate or colluder

Figure 3: Block diagram for fingerprinting system (detecting)

ing extracting step, tracing illegal user step and endbuyer check step (see Fig.3).

2.3. Considering Visual Cryptography

This scheme has already discussed fully during the last ten years [5-9], and need only briefly review it here. The basic model can be extended into a visual variant of the k out of n secret sharing problem. Given a written message, we would like to generate n transparencies so that the original message is visible if any k (or more) of them are stacked together, but totally invisible if fewer than k transparencies are stacked together. In the simplest 2-out-of-2 visual threshold problem, a pixel of the secret image is expanded to form two 2×2 blocks S_1 and S_2, which contain one half black and one half white pixels.

If a pixel is black, two of four subpixels in *Share 1* are randomly chosen to represent black and the other two represent white; while the corresponding two of four subpixels in *Share 2* represent white and the other two represent black. Hence, the authors obtain four black subpixels by stacking *Share 1* and *Share 2*. On the other hand, if a pixel is white, two of four subpixels in *Share 1* are randomly chosen to represent black and the other two represent white and *Share 2* is the same as *Share 1*. Hence, the authors observe two white subpixels and two black subpixels by stacking two shares.

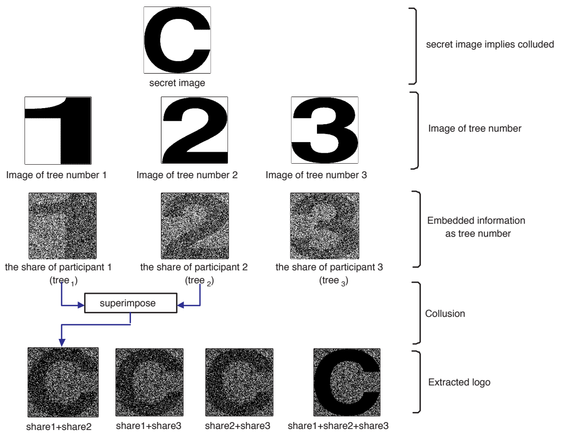

Figure 4: Considered tree number question based on EVCS [5]

It is worthwhile to note that the “stack” operation is the same as the visual OR operation [9].

We mention some points of an extended visual cryptography scheme [9]. In implementing visual cryptography schemes it would be useful to conceal the existence of the secret message, namely, the shares given to participants in the scheme should not look as a random bunch of pixels, but they should be innocent looking images (an house, a dog, a tree, ...). We would like to share the picture **C** in such a way that the share of participant 1 is the picture **A** the share of participant 2 is the picture **B**, and the share of participant 3 is the picture **C**. This shares distribution have the property that when participants 1 and 2,or participants 1 and 3, or participants 2 and 3, or participants 1, 2, and 3 stack together their transparencies they get the secret image **S**.

In our fingerprinting system, specially, the innocent looking images will be as the image of tree number is shown in Fig. 4. Thus, extended visual cryptography can be used to solve the problem of superimposed images which was described in sub-section 2.2.

3. SIMULATION RESULTS

To evaluate the proposed system we have used the video sequence “universal-studio” with a frame size of 240×360 pixels and a total of 112 frames. A convolutional code is used as the error correction code.

The secret image with tree number is decomposed into two share images. Fig. 6 shows the results of the superimposed logo image.

The important summary of our previous fingerprinting system results are as follows. To detect the

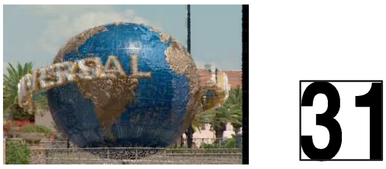

Figure 5: Test video(left), bit mapped tree number logo (right)

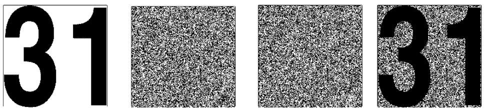

Figure 6: Secret image (left), share image 1, share image 2, superimposed logo (right)

existence or nonexistence of fingerprinting information in illegal distributions, 196 correlation computations are required (for example in $tree_{31}$, 196 =14 buyer area × 14 buyer area). To analyze the detection result, consider the content distribution tree in Fig. 1. As Fig. 7 indicates, we see that fingerprint I_1 was detected in $buyer_1$ area, fingerprints I_1 and I_4 were detected in $buyer_4$ area and fingerprints I_1, I_4 and I_9 were detected in $buyer_9$ area, corresponding to the path 1 $\rightarrow$ 4 $\rightarrow$ 9 for $user_3$. Thus, we can conclude that this video was distributed to $user_3$.

As Fig. 8 indicates, we see that fingerprint I_2 was detected in $buyer_2$ area, fingerprints I_2 and I_5 were detected in $buyer_5$ area and fingerprints I_2, I_5 and I_{12} were detected in $buyer_12$ area, corresponding to the path 2 $\rightarrow$ 5 $\rightarrow$ 12 for $user_6$. Thus, we can conclude that this video was distributed to $user_6$.

Our fingerprinting system has some built-in resilience to collusion attacks such as averaging [11], maximum-minimum, negative correlation [12] and zero-correlation collusion attack [13]. Fig. 9 correctly shows that $user_1$, $user_3$, $user_4$ and $user_7$ were colluding.

4. CONCLUSIONS

In this paper, we considered a modification of the tree specific part of previous work using visual cryptography. Although it has noise-like visual appearance, this approach is useful to detect a mixed tree number logo under the collusion attack.

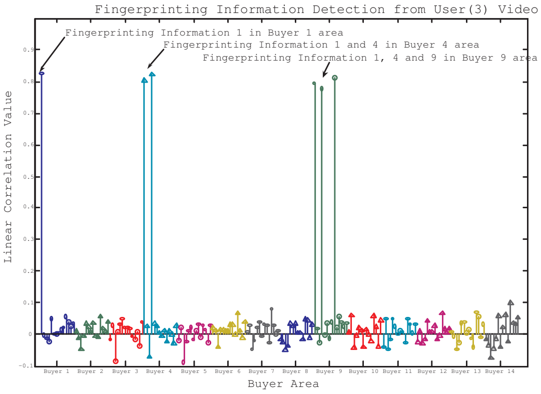

Figure 7: Detection result from $user_3$ video

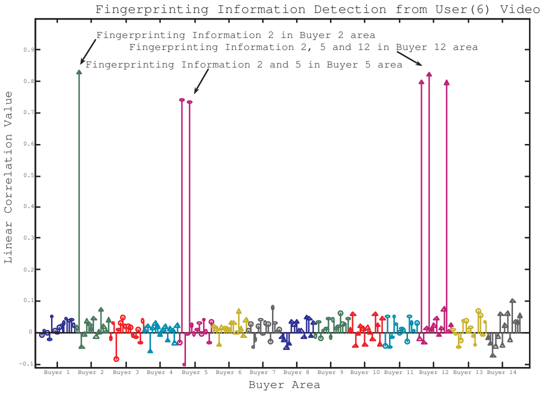

Figure 8: Detection result from $user_6$ video

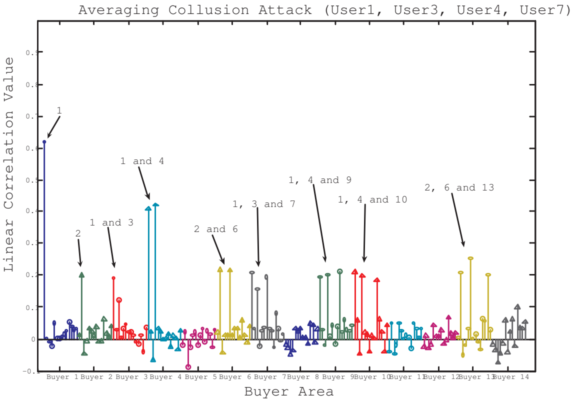

Figure 9: Detection result after averaging collusion

References

[1] H. Kang, B. Kurkoski, Y. Park, H. Lee, S. Shin, K. Yamaguchi, and K. Kobayashi: "Video fingerprinting system using wavelet and error correcting code," *Lecture Notes in Computer Science*, vol.3786, Springer-Verlag, pp.150–164, 2006.

[2] H. Kang, B. Kurkoski, Y. Park, S. Shin, K. Yamaguchi, and K. Kobayashi: "A viable system for tracing illegal users of video," *Lecture Notes in Computer Science*, vol.3917, Springer-Verlag, pp.156–158, 2006.

[3] H. Kang, B. Kurkoski, K. Yamaguchi, and K. Kobayashi: "Tracing Illegal Users of Video: Reconsideration of Tree-Specific and Endbuyer-Specific Methods," *Lecture Notes in Computer Science*, Springer-Verlag, will be published in 2007.

[4] P. Judge, and M. Ammar: "Security Issues and Solutions in Multicast Content Distribution," *IEEE Network*, vol.17, pp.30–36, 2003.

[5] G. Ateniese, C. Blundo, A. Santis, and D. Stinson: "Extended Schemes for Visual Cryptography," *Theoretical Computer Science*, vol.250, pp.143–161, 2001.

[6] M. Naor, and A. Shamir: "Visual Cryptography," *Lecture Notes in Computer Science*, vol.950, Springer-Verlag, 1995.

[7] G. Tai, and L. Chang: "Visual Cryptography for Digital Watermarking in Still Images," *Lecture Notes in Computer Science*, vol.3332, Springer-Verlag, 2004.

[8] D. Stinson: "Visual cryptography and threshold schemes," *IEEE Potentials*, vol.18, pp.13–16, 1999.

[9] T. Chen, and D. Tsai: "Owner-customer right protection mechanism using a watermarking scheme and a watermarking protocol," *Pattern Recognition*, vol.39, Issue.8, ELSEVIER, pp.1530–1541, 2006.

[10] H. Kang, Y. Park, and J. Park: "Blind watermarking based on the spatial domain," *Conference on Korea Multimedia Society*, vol.5, no.1, 2002.

[11] I. J. Cox, J. Kilian, T. Leighton, and T. Shanmoon: "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Trans. on Image Processing*, vol.6, no.12, pp.1673–1687, 2002.

[12] H. Stone: "Analysis of Attacks on Image Watermarks with Randomized Coefficients," *NEC Technical Report*, 1996.

[13] V. Wahadaniah,Y. L. Guan, and H. C. Chua: "A New Collusion Attack and Its Performance Evaluation," *Lecture Notes in Computer Science*, vol.2613, pp.64–80, 2003.