A NOVEL EMBEDDING METHOD FOR AN ANTI-COLLUSION FINGERPRINTING BY EMBEDDING BOTH A CODE AND AN ORTHOGONAL FINGERPRINT

Dalwon Jang and Chang D. Yoo

Dept. of EECS, Div. of EE, KAIST,
373-1, Guseong Dong, Yuseong Gu, Daejeon, 305-701, Korea
dal1@kaist.ac.kr and cdyoo@ee.kaist.ac.kr

ABSTRACT

In this paper, a fingerprint embedding method better-suited for the AND anti-collusion code (AND-ACC) is proposed. The proposed method embeds both a code and an orthogonal fingerprint using different basis vectors depending on the bit. Although the detection for the embedding method is complex, the performance of the fingerprinting system using proposed embedding method with the AND-ACC against average attack is improved compared with the AND-ACC fingerprinting scheme using code modulation embedding method. The system using the proposed embedding method is robust against the linear combination collusion attack (LCCA) whereas the system using the code modulation is not.

1. INTRODUCTION

With the increase in Internet users,, the unlawful distribution of digital data is becoming more prevalent. Digital fingerprinting is a technique to prohibit the illegal redistribution of digital multimedia data by embedding into the media a unique label, known as a fingerprint. The distributor can be identified by extracting the fingerprint from the illegally distributed media. From the standpoint of the illegal distributor, a cost-effective attack against fingerprinting is the collusion attack where a group of users combines their copies to make an illegal version of the copy. A fingerprinting system must be resistant to such an attack.

A fingerprinting can be classified as either an orthogonal or coded fingerprinting. In orthogonal fingerprinting, a unique spread spectrum sequence assigned to each user is embedded into the media[1, 2]. Whereas, in coded fingerprinting, a code which has good anti-collusion property is constructed and embedded in the media. Earlier works on coded fingerprinting focused mainly on the coding layer without considering the detection performance of the embedded information[3, 4, 5, 6]. To deal with various practical issues, the performance of fingerprinting has to be evaluated taking into account all steps involved in the fingerprinting: the embedding, the attack, the detection, and the coding[7]. Recent research deals with the embedding layer as well as the coding layer[7, 8, 9]. To construct a fingerprinting system, both the embedding and detecting methods should be considered as well as the design of the code.

Trappe et al. proposed a code known as the AND anti-collusion code (AND-ACC)[9]. In the paper, the code modulation method is used to embed the code. This method uses an antipodal signals to embed a bit. Though the signal to represent a bit with a single basis vector is efficient in signal space, it is possible to enhance the embedding method by substituting the antipodal signals by various basis vectors. In this paper, this is what is investigated.

In the proposed method, bit '0' is represented by a single basis vector, but bit '1' is represented by any one basis vector from a selection of basis vectors. By properly selecting a vector from a set of basis vectors for bit '1' depending on the bit position, an orthogonal fingerprint for each user can be constructed. Using the detecting results for both the embedded code and the orthogonal fingerprint, the colluders can be identified.

The remainder of this paper is organized as follows. In Section 2, the embedding and detection methods for the AND-ACC in [9] are explained. In Section 3, a basis vector set for embedding a single bit is explained. In Section 4, the proposed embedding and detection methods are explained. In Section 5, experimental results to verify the method are presented. Finally, Section 6 concludes the paper.

2. EMBEDDING AND DETECTION FOR AND-ACC

The AND-ACC is constructed based on the AND assumption that the estimated bit stream extracted from a colluded media should be the same as the logical AND of all fingerprint codes that colluded[9]. Thus, the embedding method must satisfy the assumption. In the AND-ACC fingerprinting system, the code modulation embedding method is used. In code modulation, the fingerprint, $\mathbf{w}_i$, is modelled as

$$\mathbf{w}_i = \sum_{j=1}^{v} b_{ij}\mathbf{u}_j \tag{1}$$

where $\{\mathbf{u}_j\},\ (j = 1, 2, \cdots, v)$ is the orthonormal basis to represent the jth bit. The coefficient b_{ij} where $b_{ij} \in \{0, 1\}$ or $b_{ij} \in \{\pm 1\}$ is determined by the fingerprint code. The embedding method is general enough to be used with any fingerprint code. The watermarked signal $\mathbf{Y}_i$ for the ith user is given by

$$\mathbf{Y}_i = \mathbf{X} + \alpha\mathbf{w}_i \tag{2}$$

where $\mathbf{X}$ is the host signal, and α is a constant used for perceptibility constraint.

The bit stream of a colluded copy is detected and determined using the correlation value of the extracted watermark of colluded copy and each basis vector[9].

3. BASIS SETS FOR EMBEDDING A BIT

In the code modulation method, a single basis vector is used to represent a bit because the antipodal signals are used. But a bit does not necessarily have to be represented by a single basis vector. It is possible to assign a different basis vector for each bit value. Moreover,

it is possible to assign a set of basis vectors to each bit value. Denoting the sets for bit '1' and bit '0' as $\mathbf{V}^{(1)}$ and $\mathbf{V}^{(0)}$ respectively, the following four exhaustive cases are considered. For set $\mathbf{A}$, $|\mathbf{A}|$ represents the cardinality of $\mathbf{A}$.

- CASE 1: $|\mathbf{V}^{(1)}| = 1$ and $|\mathbf{V}^{(0)}| > 1$.
- CASE 2: $|\mathbf{V}^{(1)}| > 1$ and $|\mathbf{V}^{(0)}| = 1$.
- CASE 3: $|\mathbf{V}^{(1)}| > 1$ and $|\mathbf{V}^{(0)}| > 1$.
- CASE 4: $|\mathbf{V}^{(1)}| = 1$ and $|\mathbf{V}^{(0)}| = 1$.

If some signals, where various orthogonal vectors are embedded respectively, are colluded, the energy of each vector is dispersed. Thus, the detection of the case is more difficult than that of the case of using only a vector for every signal. Therefore, the detection of bit '0' in the case of $|\mathbf{V}^{(0)}| > 1$ is more difficult than the detection of bit '0' in the case of $|\mathbf{V}^{(0)}| = 1$. However, because of the AND assumption of AND-ACC, the detection of vectors in $\mathbf{V}^{(0)}$ is more conclusive evidence than the detection of vectors in $\mathbf{V}^{(1)}$ to decide the bit value from the colluded copy. Thus, bit detection is more difficult in CASE1 and CASE 3 than in CASE 2 and CASE 4 when AND-ACC is embedded. Therefore, CASE 1 and CASE 3 are excluded.

The difference between the code modulation method used in paper [9] and CASE 4 is similar to the difference between the binary antipodal signals and the binary orthogonal signals used often in digital communication theory[10]. In the code modulation method, a single vector, $\mathbf{u}_i$, is used to represent both bit values as $\{\pm\mathbf{u}_i\}$ or $\{\mathbf{u}_i, \mathbf{0}\}$. But in CASE 4, two orthogonal vectors, $\mathbf{u}_i^{(0)}$ and $\mathbf{u}_i^{(1)}$ (the superscript represents the bit and the subscript represents the location) are used to represent bit '0' and bit '1,' respectively. In digital communication theory, it is known that antipodal signals can be more accurately detected than the orthogonal signals for a fixed signal energy[10]. But, the goal of fingerprinting system is not to detect the bit stream, but to identify the colluders. The detection of this case can be different from that of digital communication theory. Even though the performance is degraded, the bit stream can be detected using only the vector which represents bit '0' as the on-off keying system does[10]. The detection result of the signal used to represent bit '1' can be used as additional information. The generalization of CASE 4 is CASE 2.

In CASE 2, bit '1' is difficult to detect after collusion since it is represented by many different basis vectors. But, if the detector knows which basis vector was selected from a set of vectors, the detection result for bit '1' will be useful in identifying the colluders. In other words, the detection result of bit '1' has direct implication in identifying the colluders. This method is same as the detection method used in orthogonal fingerprinting. The detection of code is achieved by using a vector for bit '0,' $\mathbf{u}_i^{(0)}$. By combining the separate detection results (one for bit '0' and one for bit '1'), it is possible to achieve identification performance better than that of code modulation.

4. EMBEDDING AND DETECTION

4.1. Embedding

In this subsection, the proposed embedding method using CASE 2 is explained. The $(v, k, 1)$ code is used in this subsection. In AND-ACC, the $(v, k, 1)$ code requires v bits for $n = (v^2 - v)/(k^2 - k)$ users and provides $(k-1)$-resiliency[9].

Assume that the host signal is segmented, one bit is embedded per segment. Thus, there are v segment to embed the $(v, k, 1)$ code. To be resistant to the interleaving attack, the segmentation must be secure. The permuted subsegment embedding proposed in [8] is a good method to achieve robustness against interleaving attack.

To embed a bit in a segment, a basis vector generated using spread spectrum technique is added to the host signal[2]. For bit '0,' a single basis vector, denoted as $\mathbf{u}^{(0)}$, is used, and for bit '1', a single vector chosen from $\mathbf{V}^{(1)}$ is used. The vectors are denoted as $\mathbf{u}_{f(i,j)}^{(1)}$ where $f(i,j)$ is the vector index mapping function for the ith user and jth bit. If the number of basis vectors in $\mathbf{V}^{(1)}$ is denoted as K, $f(i,j)$ is an integer which satisfy $1 \le f(i,j) \le K$.

The fingerprint of the ith user, $\mathbf{w}_i$, is constructed by concatenating the basis vectors of all the segments. And, an orthogonal fingerprint for each user is constructed by substituting $\mathbf{u}^{(0)}$ in $\mathbf{w}_i$ as the zero vector, denoted as $\mathbf{0}$. The orthogonal fingerprint for user i is denoted as $\mathbf{w}_{i,ORTH},\ (i = 1, 2, \cdots, n)$. The vector index mapping function must be created to achieve $\mathbf{w}_{i,ORTH} \perp \mathbf{w}_{j,ORTH},\ i \neq j$. The fingerprint is embedded using equation (2).

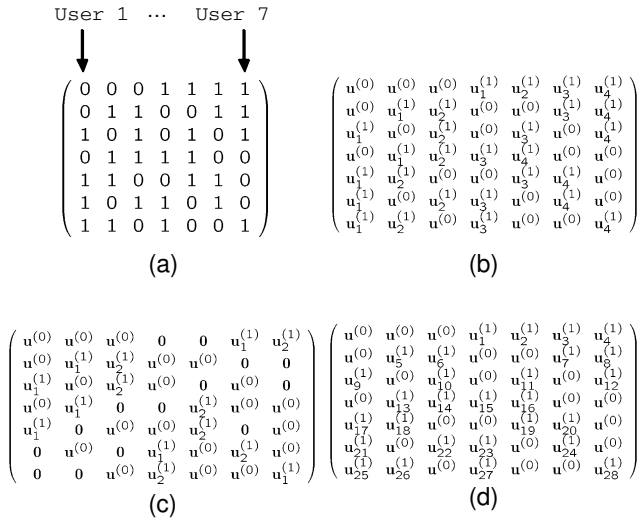


Fig. 1. Examples of constructing a fingerprint - (a) code matrix (b) fingerprint (K=4) (c) fingerprint (K=2) (d) fingerprint (K=28)

In AND-ACC, majority of bits are '1.' For example, in a 16bit-code for 20 user, only 4 bits are bit '0.' This is one of the reason why the proposed embedding method is ideal for the AND-ACC. The disproportionate number of occurrences of each bit value makes the orthogonal fingerprint long. Longer the orthogonal fingerprint more accurate the detection. Because the number of bit '0' is k in the $(v, k, 1)$ code, we have $(v - k)$ segments to embed bit '1.' If $K < v - k$, some vectors are used more than twice in a segment. But, because it breaks the orthogonality, we append $\mathbf{u}_0^{(1)} = \mathbf{0}$ to the set of basis vector for bit '1' and use zero vector for orthogonality. With smaller K, the quality of the fingerprinted media is improved at the cost of detectability of $\mathbf{w}_{i,ORTH}$. The minimum value of K to make n orthogonal fingerprint is $\lceil \frac{n}{v} \rceil$ where $\lceil x \rceil$ is the function that rounds x to the nearest integers towards infinity.

Simple examples of fingerprint construction are shown in Fig. 1. Depending on K and $f(i,j)$, various fingerprint sets can be made, but in the example, $\mathbf{w}_{i,ORTH}$ substituted $\mathbf{u}^{(0)}$ as $\mathbf{0}$ in the fingerprint is always orthogonal to the others.

4.2. Detection

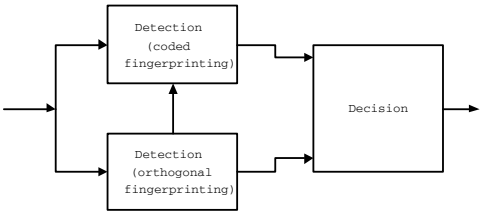


Fig. 2. Detection process: two detection processes are correlation detector and the decision process combine two detection results

The block diagram of the entire detection process is shown in Fig. 2. As shown, two detection processes are involved: the detection of coded fingerprint using bit '0' and the detection of orthogonal fingerprint using bit '1.' In coded fingerprinting detector, the correlation between $\mathbf{u}^0$ and each segment signal is computed, and the bit is determined. Similarly, in orthogonal fingerprinting detector, the correlation between the entire media and $\mathbf{w}_{i,ORTH}$ is computed.

Of the two detectors, the orthogonal fingerprint detection is first performed. The the detection result is the correlation value of each user. The highest absolute value indicates the most suspicious user. The detection process of coded fingerprint makes the set of suspicious users using the extracted code and the most suspicious user. For each segment, the correlation with $\mathbf{u}^{(0)}$ is computed, and the bit is determined[9]. If an absolute value of correlation with $\mathbf{u}^{(0)}$ is bigger than a threshold, the bit is considered as bit '0.' The threshold is dependent on the code of most suspicious user. Depending on the bit stream, the set of suspicious users is created and notified to decision process. In decision process, some users in the set are removed from the set depending on the correlation value of the orthogonal fingerprinting. After that, the colluders are identified.

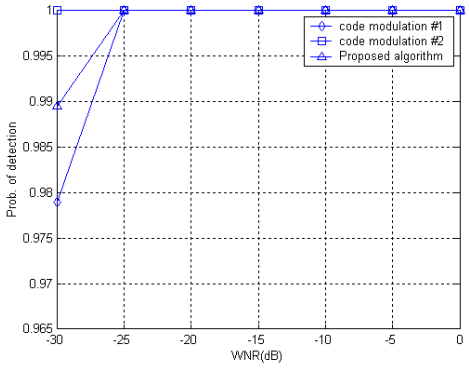
The reason to use absolute value is to cope with linear combination collusion attack (LCCA)[11]. The AND-ACC fingerprinting system with code modulation is vulnerable to the LCCA. The attack creates a pirated copy by summing $(r+1)$ copies and subtracting r copies. Because the subtracted copy is weighted by -1 in the LCCA, the absolute value is used. Using the absolute value, the robustness is improved against LCCA. Owing to the use of absolute signal, the signal embedded in the subtracting copy can be known.

In fact, the colluders are identified by combining the two detection results. By adjusting the thresholds of the two detectors, various performance in terms of false alarm and false detection can be achieved.

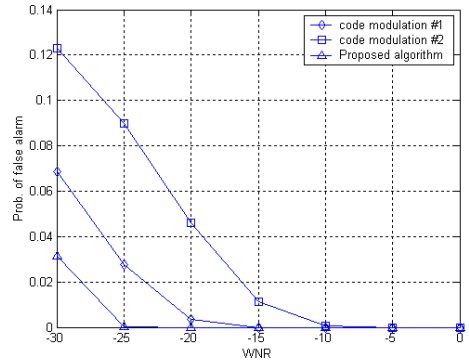
Since a code modulation detector is included, the proposed detector is more complex than a code modulation detector by itself. The number of correlation computation in code modulation detector is proportional to v. But, the number of correlation computation in the proposed detector is proportional to $v + nK$ (if $K \leq v - k$) or $v + n(v-k)$ (if $K > v - k$).

5. EXPERIMENTAL RESULT

To verify the effectiveness of the method, experiment is performed using image with various watermark-to-noise ratios (WNR). The $(16, 4, 1)$ code, which is for 20 users and is possible to capture at most 3 colluders, is embedded using the proposed method and the code modulation method. The probability of detection and false alarm of he proposed method is compared with those of the code



(a) Probability of detection



(b) Probability of false alarm

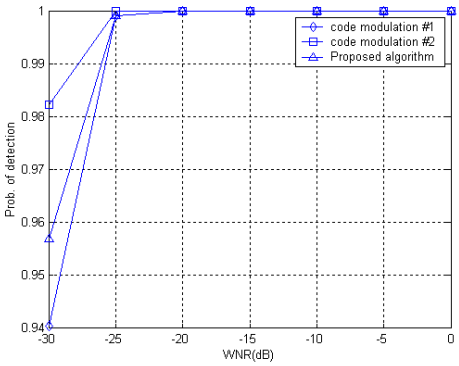
Fig. 3. Experimental result against average attack(2 colluders)

modulation method. The probability of the detection is presented in the sense of 'capture-1 colluder.' To evaluate the performance of the embedding methods, the average attack and the LCCA are used. In the detector, non-blind detection is assumed. Hard decision is used, and two different thresholds are used for the code modulation. We use $K = 15$, and peak signal-to-noise ratio (PSNR) of fingerprinted image is about 47dB for all cases.

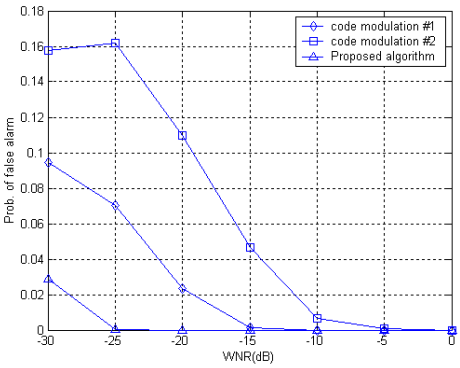
The experimental results against average attack are shown in Fig. 3 and 4. As shown in the figures, the performance of the proposed in terms of the probability of detection is about average compared to the code modulation method; however, in terms of the probability of false alarm, the proposed method exhibits the best results. The experimental results against the LCCA (3 colluders) are shown in Fig. 5. As described in [11], the method in [9] is not robust against LCCA, but the figure shows the colluder can be identified with high probability using the proposed method.

6. CONCLUSION

In this paper, it is shown that a set of basis vectors can be used to represent a bit value. Based on this, the embedding method for AND-ACC is proposed. While a single vector is used to represent bit '0,' a set of basis vectors are used to represent bit '1' in the method. Moreover, the vectors representing bit '1' are used as an orthogonal fingerprint. The proposed detection method incorporates many

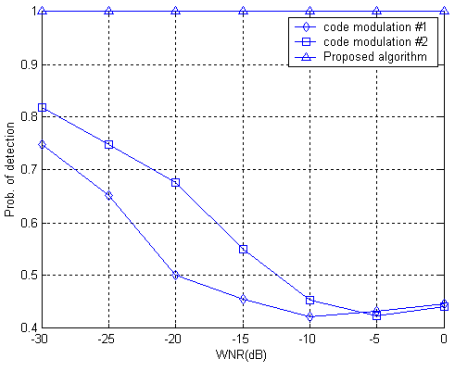


(a) Probability of detection

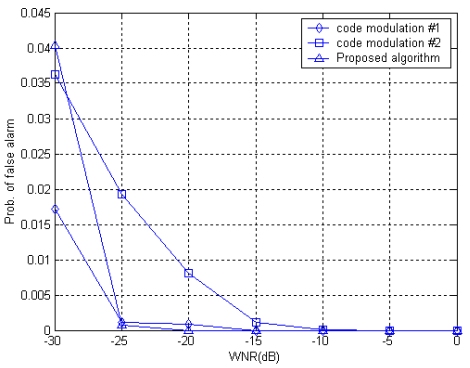


(b) Probability of false alarm

Fig. 4. Experimental result against average attack(3 colluders)



(a) Probability of detection



(b) Probability of false alarm

Fig. 5. Experimental result against LCCA (3 colluders)

of the concepts used in the orthogonal fingerprinting as well as the coded fingerprinting. Experimental results in terms of probability of detection and miss show the effectiveness of the proposed embedding method. As a trade-off, the proposed method requires more processing time. This idea and the proposed method are not only appropriate but well matched for the embedding of the AND-ACC.

7. ACKNOWLEDGMENTS

This work was supported by grant No. R01-2003-000-10829-0 from the Basic Research Program of the Korea Science and Engineering Foundation and by University IT Research Center Project.

8. REFERENCES

[1] Z. J. Wang, M. Wu, H. V. Zhao, W. Trappe, and K. J. R. Liu, "Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation," *IEEE Trans. on Image Processing*, vol. 14, no. 6, June, 2005

[2] I. J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Trans. on Image processing*, vol. 6, pp. 1673-1687, Dec. 1997.

[3] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Information Theory*, vol. 44, no. 5, pp. 1897-1905, Sep., 1998

[4] F. Sebe and J. Domingo-Ferrer, "Collusion-secure and cost-effective detection of unlawful multimedia redistribution", *IEEE trans. on systems, man, and cybernetics*, vol. 33, no. 3, 2003

[5] J. Domingo-Ferrer and J. Herrera-Joancomarti, "Short collusion-secure fingerprints based on dual binary hamming codes," *Electron. Lett.*, vol. 36, no. 20, pp. 1697-1699, 2000.

[6] J. Dettman, P. Schimitt, E. Saar, J. Schwenk, and J. Ueberberg, "Combining digital watermarks and collusion secure fingerprinting for digital images," *SPIE J. Electron. Imaging*, vol. 9, no. 4, pp. 456-467, 2000

[7] S. He and M. Wu, "Performance of ECC-based collusion-resistant multimedia fingerpriting," *Proc. 38th CISS*, Mar. 2004.

[8] S. He and M. Wu, "Improving collusion resistance of error correcting code based multimedia fingerprinting," *ICASSP '05*, vol. 2, pp. 1029-1032, Mar. 2005.

[9] W. Trappe, M. Wu, Z. J. Wang, and K.J.R. Liu, "Anti-collusion fingerprinting for multimedia," *IEEE Trans. on Signal processing* vol. 51, no. 4, pp. 1069-1087, APR. 2003.

[10] J. G. Proakis, "Digital Communication," *Mcgraw-Hill*, 2000

[11] Y. Wu, "Linear Combination Collusion Attack and its Application on an Anti-Collusion Fingerprinting," *Proc ICASSP 05*, vol. 2, pp. 13-16, Mar. 2005.