

DESIGN OF MULTIUSER COLLUSION-FREE HIDING CODES WITH DELAYED EMBEDDING

Byung-Ho Cha and C.-C. Jay Kuo

Ming Hsieh Department of Electrical Engineering and Signal and Image Processing Institute
University of Southern California, Los Angeles, CA 90089-2564
E-mail: byungcha@usc.edu, cckuo@sipi.usc.edu

Abstract— The design of collusion-free hiding codes for a large number of users in a media distribution scenario is considered in this work. To increase the number of users, we propose to assign the same codeword repetitively to multiple users but with a different amount of delay. It is shown that, when the proposed system is under collusion, it is equivalent to a communication system with a multipath channel. Then, the identification performance for each user code can be improved by multipath channel estimation and adaptive equalization methods. We present a set of collusion-free codes called OSIFT (Orthogonal Spreading followed by the Inverse Fourier Transform) and demonstrate that OSIFT codes are robust against a generalized collusion attack in an exemplary audio watermarking system with a large number of users by computer simulation.

I. INTRODUCTION

Multimedia contents can be easily distributed over wired and wireless networks with the development of coding and networking technologies. For example, multiple copies of the same content can be delivered to multiple users with the multi-cast technology. To protect multimedia contents, it is important to develop a traitor tracing technique to identify the unauthorized usage of media contents under distribution. One well known attack that can break the traitor tracing system easily is the collusion attack. The number of colluders in collusion attacks is an important parameter to consider in the design of a traitor tracing system. Usually, if the number of colluders increases, the attack strength becomes stronger. It is a challenging task to design collusion-free hiding codes for a large number of users, which will be the focus of this work.

Chu *et al.* [1] proposed a two-layer fingerprinting technique and applied c -secure codes for leakage identification. Although the robustness of the proposed technique against collusion attacks was not thoroughly investigated, their research direction in accommodating a large number of users appears to be promising. Wang *et al.* [2] pointed out some disadvantages of the two-layer fingerprinting design in [1] and proposed a group-oriented fingerprinting method to enhance the performance of orthogonal modulation codes under massive distribution. They assigned correlated fingerprints to potential colluders and uncorrelated fingerprints to users who are unlikely to perform the collusion attack jointly. Zhao *et al.* [3] extended the group-oriented fingerprinting technique to the video multicast scenario based on scalable video coding, and proposed a method by combining TDMA and CDMA embedding.

In this work, we investigate a method to allow a large number of users and a reasonable size of colluders with a

relatively small codeword size in the traitor tracing system. The way to increase the user capacity is to reuse the same codeword with a different amount of delay for different users. Furthermore, we show similarity between the collusion attack with delayed embedding and the multi-access with multipath channel in a wireless communication system. Then, we study the performance of collusion-free codes called OSIFT (Orthogonal Spreading followed by the Inverse Fourier Transform) in [4], which were inspired by the precoding technique in [5], [6], in the presence of the collusion attack. By leveraging the knowledge of multipath channel estimation and adaptive equalization in a multi-access and multipath environment, we can demonstrate that OSIFT codes are robust against generalized collusion attacks in an exemplary audio watermarking system.

The rest of this paper is organized as follows. The delayed codeword embedding, generalized collusion attacks, and detection with channel estimation and adaptive equalization are described in Sec. II. Then, collusion-free hiding codes with delayed embedding are described and analyzed in Sec. III. Simulation results are reported in Sec. IV using an audio system as an example. Finally, concluding remarks are given in Sec. V.

II. SYSTEM MODEL

A. Code Embedding

A code embedding system with delayed codewords is shown in Fig. 1. There are G groups and each group supports P different users. In each group, P users share the same codeword and they are distinguished by delay amount $\Delta_{l,g}$, where l is the user index and g is the group index. Thus, the total number of supportable users increases from $L = G$ to $L = PG$. Without loss of generality, we assume the codeword length for each group is the same and equal to N . Then, we can choose $\Delta_{l,g} = 0, 1, \dots, P-1$, $0 \leq \Delta_{l,g} \leq N-1$ so that the maximum number of P is N .

We follow the time-domain codeword embedding system proposed in [7]. Let $x_l(i)$, $i = 0, \dots, T-1$, be part of the host signal for user l of length $T = NM$. We can divide it into M segments, each of which has N samples as

$$x_{l,m}(i) = x_l(m \cdot N + i), \quad \begin{cases} m = 0 \cdots M-1 \\ i = 0 \cdots N-1 \end{cases} \quad (1)$$

Then, the additive codeword embedding method is given by

$$y_{l,m}(i - \Delta_{l,g}) = x_{l,m}(i - \Delta_{l,g}) + a_{l,m}(i - \Delta_{l,g}) \quad (2)$$

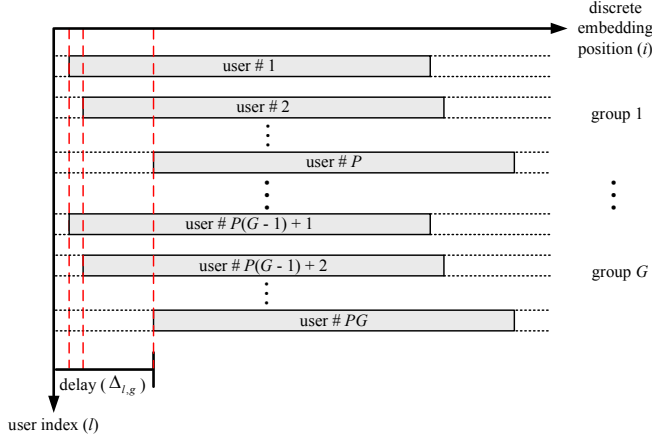


Fig. 1. The delayed embedding model.

where

$$a_{l,m}(i - \Delta_{l,g}) = \alpha |x_{l,m}(i - \Delta_{l,g})| w_{l,m}(i). \quad (3)$$

and where α is a constant that adjusts the embedded code strength, and $w_{l,m}(i)$ is the hiding code generated from user identification (ID) $u_l(i)$, spreading code $s_l(i)$, and the inverse discrete Fourier transform (IDFT) for user l , which will be detailed in Sec. III.

B. Generalized Collusion Attack

The collusion attack provides a cost-effective attack to remove hiding codes without severely degrading the quality of the host media. It is obtained by a coalition of hiding codes from multiple users [8]. Since our embedding system includes a delay factor before the coalition, a general form of collusion attacks can be expressed mathematically as

$$\hat{y}_m(i) = \sum_{k=0}^{K-1} h_{k,m} y_{k,m}(i - \Delta_{k,g}) + e(i) \quad (4)$$

where $\hat{y}_m(i)$ is the colluded signal, $y_{k,m}(i - \Delta_{k,g})$ is the host signal embedded with user code k , which is a function of group index g and delay amount $\Delta_{k,g}$, e is the noise vector, and $h_{k,m}$ is a weight for the signal of user k in the collusion attack.

C. Multipath Channel Estimation

In a communication channel, the discrete multipath channel model of user l can be given by

$$\mathbf{r}_l = \mathbf{H}_l \mathbf{c}_l + \mathbf{e}, \quad (5)$$

where \mathbf{H}_l is the discrete-time channel impulse response matrix. The multipath channel model is actually analogous with that of the generalized collusion attack model with delayed embedding. The coefficients of a tapped delay line are equivalent to the weights used in (4), and they have to be estimated in both models.

One way to estimate the coefficients of the channel impulse response is to exploit pilot symbols. That is, estimation is

conducted based on known time or frequency domain pilot symbols, which are interspersed with transmitted data symbols [9]. The channel response matrix \mathbf{H}_l in (5) can be found easily with pilot symbols known to both the transmitter (or embedder) and to the receiver (or detector). If \mathbf{e} is an i.i.d white Gaussian sequence, the individual maximum likelihood (ML) estimation of \mathbf{c}_l with observation \mathbf{r}_l is equivalent to the following least square (LS) estimate:

$$\tilde{\mathbf{c}}_l = (\mathbf{H}_l^t \mathbf{H}_l)^{-1} \mathbf{H}_l^t \mathbf{r}_l, \quad (6)$$

where \mathbf{H}_l is assumed to have the full column rank.

D. Code Detection

For code detection, synchronization is assumed to be achieved between the embedder and the detector. Thus, the delay position of each user is available at the detector. Then, we can simplify the antipodal binary hypothesis test to the following

$$\begin{cases} H_0 : \hat{y}_{l,m}(i) = w_{l,m}(i) + z_{l,m}(i), & m = +1 \\ H_1 : \hat{y}_{l,m}(i) = -w_{l,m}(i) + z_{l,m}(i), & m = -1 \end{cases} \quad (7)$$

where $\hat{y}_{l,m}(i)$ is the received signal, $z_{l,m}(i)$ denotes the effect of noise or interference and m is a binary bit of user message. The output of the correlation detector is given by

$$v_{l,m} = \frac{1}{N \tilde{\lambda}_{l,m}} \cdot \frac{\sum_{i=0}^{N-1} (\hat{y}_m(i) - x_m(i)) b_m(i) s_l(i)}{\sqrt{\sum_{i=0}^{N-1} |s_l(i)|^2}} \quad (8)$$

where $v_{l,m}$ is the statistics of detection,

$$b_m(i) = 1/(\alpha |x_m(i)|),$$

and the value of $\tilde{\lambda}_{l,m}$ can be provided by the channel estimation technique as explained in Sec. III. The statistics of $v_{l,m}$ can be used as a metric to measure the robustness of different hiding codes. From this detection statistics, we can calculate the bit error rate (BER) between the extracted user ID $\hat{u}_l(i)$ and the original user ID number $u_l(i)$, and then derive the average BER and detection rate obtained by a decision level η .

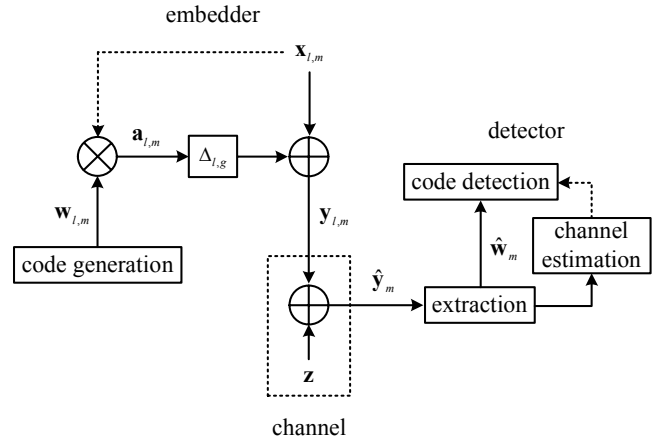


Fig. 2. The code embedding, extraction and detection system.

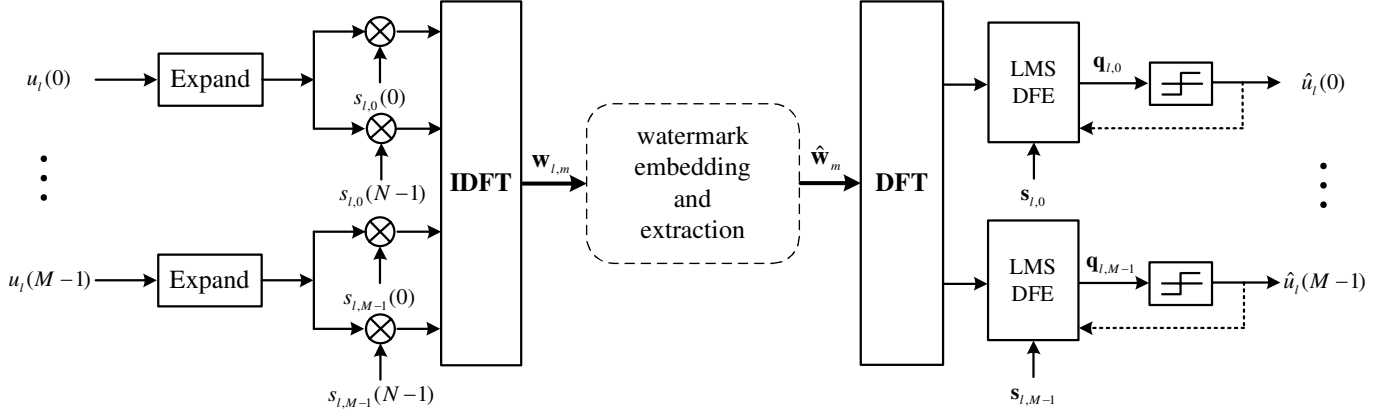


Fig. 3. The collusion-free hiding code generation and detection system.

E. LMS Adaptive Equalization

The DFT output is multiplied by the coefficients of the least-mean-squares decision-feedback-equalizer (LMS-DFE) [10]. The coefficients are updated by an iterative process. We take the DFT of $\hat{w}_m(i)$ and multiply the result with $\tilde{\lambda}_{l,m}(i)$, which leads to

$$q_{l,m}(i) = \tilde{\lambda}_{l,m}(i) \text{DFT}\{\hat{w}_m(i)\}, \quad i = 0 \cdots N-1. \quad (9)$$

The error signal $d_{l,m}(i)$ is calculated by the difference between decided user message \hat{u}_l and $q_{l,m}(i)$

$$d_{l,m}(i) = \hat{u}_l - q_{l,m}(i). \quad (10)$$

Then, we update $\tilde{\lambda}_{l,m}(i)$ by

$$\tilde{\lambda}_{l,m}(i) = \tilde{\lambda}_{l,m}(i) - \mu d_{l,m}(i) \text{DFT}\{\hat{w}_m(i)\}, \quad (11)$$

where μ is the step size that determines the convergence rate. The overall hiding code system is shown in Fig. 2.

III. COLLUSION-FREE HIDING CODES

In this section, we present a set of collusion-free hiding codes, known as the OSIFT (Orthogonal Spreading followed by the Inverse Fourier Transform) codes, which is robust against the generalized collusion attack. The OSIFT code generation and detection system and its interface with the hiding code embedding and extraction system are shown in Fig. 3. We consider an orthogonal code of length N under perfect synchronization with a fixed delay for user l , which has the following property

$$\sum_{i=0}^{N-1} s_l(i) s_k(i) = \begin{cases} N, & l = k \\ 0, & l \neq k \end{cases} \quad (12)$$

In particular, we choose the Hadamard Walsh (HW) codes as the orthogonal codes due to its ease of computation. Please note that the HW matrices can be recursively defined by

$$\mathbf{S}_N = \mathbf{S}_2 \otimes \mathbf{S}_{N/2} = \begin{pmatrix} \mathbf{S}_{N/2} & \mathbf{S}_{N/2} \\ \mathbf{S}_{N/2} & -\mathbf{S}_{N/2} \end{pmatrix}, \quad (13)$$

where $N = 2^n$ ($n \geq 2$) and \otimes is the Kronecker product. The HW codes of length N are column vectors of HW matrices

of dimension $N \times N$. Please note that HW codes only take 1 and -1 two values, which simplifies the spreading operation greatly.

The interference between codes of different users can be analyzed below. We calculate the correlation between hiding code $\hat{w}_{k,m}(i)$ of user k and hiding code $\hat{w}_{l,m}(i)$ of user l as

$$v_{l,m} = \frac{1}{\psi} \sum_{i=0}^{N-1} \lambda_{l,m}(i) b_m(i) |s_l(i)|^2 + \frac{1}{\psi} \sum_{k=0, k \neq l}^{K-1} \text{MAI}_{l \leftarrow k} + \frac{1}{\psi} \sum_{i=0}^{N-1} b_m(i) e(i) s_l(i) \quad (14)$$

where $\lambda_{l,m}$ is the frequency response of $h_{l,m}$ obtained by DFT,

$$\psi = N \sqrt{\sum_{i=0}^{N-1} |s_l(i)|^2} \quad \text{and} \quad b_m(i) = \frac{1}{\alpha |x_m(i)|}.$$

and

$$\text{MAI}_{l \leftarrow k} = \sum_{i=0}^{N-1} \lambda_{k,m}(i) b_m(i) s_k(i) s_l(i) \quad (15)$$

is the interference from user k to user l . Mathematically, to achieve the collusion-free property, we demand $\text{MAI}_{l \leftarrow k} = 0$, which is valid if an orthogonal code is used [11]. In the watermarking context, it is reasonable to assume $e(i) = 0$. Then, the right-hand-side (RHS) of Eq. (14) can be simplified to

$$v_{l,m} = \frac{1}{\psi} \sum_{i=0}^{N-1} \lambda_{l,m}(i) b_m(i) |s_l(i)|^2. \quad (16)$$

Consequently, the embedded watermark can be reconstructed by adaptively equalizing the channel frequency response through the multiplication of $\tilde{\lambda}_{l,m}^{-1}$, where $\tilde{\lambda}_{l,m}$ is estimated channel response. One can obtain $\tilde{\lambda}_{l,m}$ by the pilot-assisted scheme and update it by the LMS-DFE technique.

IV. SIMULATION RESULTS

In this section, we study the performance of our OSIFT codes against the generalized collusion attack. Three hiding codes, which are frequently used in the watermarking research,

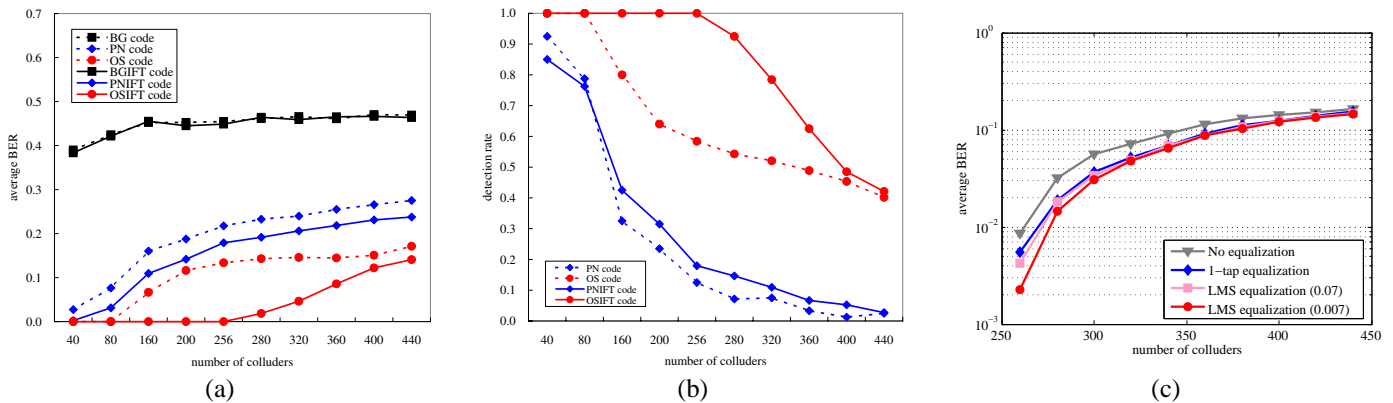


Fig. 4. Simulation results with delayed embedding $\Delta_{l,g} = 64, 128$ and $P = 2, N = 256, L = 512$: (a) the average BER, (b) the detection rate, and (c) average BER performance comparison with different equalization schemes.

are compared with our OSIFT codes. They are bounded Gaussian (BG), pseudo-noise (PN) and orthogonal HW codes (OS). An audio music signal sampled at 44.1KHz is used as the host. The code strength α is set to 0.05, and the length N of spreading codes is chosen to be 256. The length of user message is set to $M = 32$. A delayed embedding situation is adopted in all simulations. To compute the detection rate, we fix threshold $\eta = 0.1$ and false alarm rate $f_a < 10^{-3}$. Simulation results are obtained using a total of 2000 simulation runs.

We set $\Delta_{l,g} = 64, 128, P = 2, N = 256$, and the total number of users $L = 512$ in the simulation, and the results are shown in Fig. 4. It is clear from Figs. 4 (a) and (b) that the proposed OSIFT codes have the best performance in the average BER as well as the detection rate. The delay embedding technique leads to an increased average BER value. We see that all test hiding codes cannot sustain 80 more colluders except the OSIFT codes. Four equalization-related schemes in the OSIFT codes are compared in Fig. 4 (c). They include: no equalization (as a benchmark), 1-tap equalizer, and two LMS equalizers with step size $\mu = 0.07$ and 0.007 . When the number of colluders is below 300, the LMS equalization with $\mu = 0.007$ gives the best result. When the number of colluders is above 300, the performance gaps becomes very small since user codes are severely broken by interference.

For a spreading code of length $N = 256$, Table I compares two situations with $P = 2$ and 4, which can support $L = 512$ and 1024 users, respectively. We consider the following two scenarios: (i) $\Delta_{l,g} = 64, 128$ for $L = 512$ and (ii) $\Delta_{l,g} = 0, 64, 128, 192$ for $L = 1024$. As shown in Table I,

TABLE I
COMPARISON OF OSIFT CODES WITH LENGTH $N = 256$.

$\Delta_{l,g} = 64, 128, P = 2, L = 512$							
K	40	80	120	160	200	256	280
Detection rate	1.00	1.00	1.00	1.00	1.00	1.00	0.93
$\Delta_{l,g} = 0, 64, 128, 192, P = 4, L = 1024$							
K	40	80	120	160	200	256	280
Detection rate	1.00	1.00	1.00	1.00	1.00	1.00	0.91

both systems can support up to 256 colluders (*i.e.* $K = 256$) without any detection errors.

V. CONCLUSION AND FUTURE WORK

The performance of the OSIFT collusion-free codes with delayed embedding was investigated in this paper. The application of OSIFT codes with delayed embedding can help increase the number of users (*i.e.* user capacity) by re-using the same spreading codes. It was shown that OSIFT is robust against a generalized collusion attack by leveraging the channel estimation and adaptive equalization techniques developed in wireless communication systems. Advanced channel estimation and equalization techniques to improve the detection performance will be studied furthermore in our future work.

REFERENCES

- [1] H. Chu, L. Qiao, and K. Nahrstedt, "A secure multicast protocol with copyright protection," in *Proc. ACM SIGCOMM*, Pittsburgh, PA, April 2002, pp. 42–60.
- [2] Z. J. Wang, M. Wu, W. Trappe, and K. J. R. Liu, "Group-oriented fingerprinting for multimedia forensics," *EURASIP Journal on Applied Signal Processing*, vol. 14, pp. 1242–2162, November 2004.
- [3] H. V. Zhao and K. J. R. Liu, "Fingerprint multicast in secure video streaming," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 12–29, January 2006.
- [4] B.-H. Cha and C.-C. Jay Kuo, "Design of collusion-free hiding codes using MAI-free principle," in *Proc. IEEE Int'l Conf. Acoustics, Speech, and Signal Processing*, Honolulu, HI, April 2007, pp. 145–148.
- [5] S.-H. Tsai, Y.-P. Lin, and C.-C. Jay Kuo, "A precoded multiuser OFDM (PMU-OFDM) transceiver for time asynchronous systems," in *Proc. IEEE GLOBECOM*, St. Louis, MO, November 2005, pp. 2214–2218.
- [6] S.-H. Tsai, Y.-P. Lin, and C.-C. Jay Kuo, "MAI-free MC-CDMA based on Hadamard-Walsh codes," *IEEE Transactions on Signal Processing*, vol. 54, pp. 3166–3179, August 2006.
- [7] P. Bassia, I. Pitas, and N. Nikolaidis, "Robust audio watermarking in the time domain," *IEEE Transactions on Multimedia*, vol. 3, pp. 232–240, June 2001.
- [8] H. S. Stone, "Analysis of attacks on image watermarks with randomized coefficients," Tech. Rep. 96-045, NEC Res. Inst. Tech., Princeton, NJ, 1996.
- [9] L. Hanzo, M. Munster, B. J. Choi, and T. Keller, *OFDM and MC-CDMA for broadband multi-user communications, WLANs and broadcasting*, John Wiley & Sons, West Sussex, UK, 2004.
- [10] J. G. Proakis, *Digital Communication*, McGraw-Hill, New York, NY, 1995.
- [11] M. K. Simon, J. K. Omura, R. A. Sholtz, and B. K. Levitt, *Spread spectrum communications handbook*, McGraw-Hill, Electronic edition, 2002.