

# ADVANCED COLLUDER DETECTION TECHNIQUES FOR OSIFT-BASED HIDING CODES

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**—In this work, we examine a family of anti-collusion codes using the principle of “Orthogonal Spreading followed by the Inverse Fourier Transform (OSIFT)” as introduced in [1], [2]. The Hadamard-Walsh (HW) codes were adopted as the orthogonal spreading codes in [1], [2]. Here, we introduce another type of orthogonal spreading codes; namely, the carrier interferometry (CI) codes, which are comparable to HW codes. To detect OSIFT hiding codes against weighted collusion attacks, we propose advanced detectors that can identify a large number of colluders with weighted collusion attacks. The proposed detection schemes include the maximal ratio combining (MRC) scheme for colluder detection in the same group and the multiuser detection (MUD) scheme for colluder detection in different groups. It is demonstrated that HW- and CI-based OSIFT codes have robust performance with advanced detection schemes against weighted collusion attacks compared with conventional matched filter (MF) in an exemplary audio watermarking system.

## I. INTRODUCTION

The development of robust hiding codes to identify the unauthorized usage of media contents is essential to the fingerprinting application. One powerful mechanism to break the fingerprinting system is the collusion attack. That is, users who have the same multimedia content but with different fingerprinting codes may average their received copies in a weighted manner. Consequently, fingerprinting codes can be removed while the quality of the host media is still well preserved.

The design of robust fingerprinting codes against the collusion attack has been studied for years. The resulting codes are called the anti-collusion codes. Most previous research on anti-collusion codes has focused on code design and detection among a relatively small number of colluders *e.g.*, [3], [4]. The scalability of anti-collusion codes to meet a large number of colluders and users is a challenging problem. Furthermore, most collusion attack models considered before, is the equally weighted collusion or its variation (*i.e.*, the cascade of several stages of equally weighted collusion attack.) The performance of anti-collusion codes against a general unequally weighted collusion attack has not yet been examined carefully. We attempt to address both issues in this paper.

To provide a solution that is scalable to a larger number of users and colluders, new fingerprinting codes based on the principle of “Orthogonal Spreading followed by the Inverse Fourier Transform (OSIFT)” was proposed in [1], [2]. The Hadamard-Walsh (HW) codes were adopted as orthogonal spreading codes in [1], [2]. Here, we introduce another type of orthogonal spreading codes known as the carrier interferometry (CI) codes. With these two orthogonal spreading codes,

the main contribution of this work is to detect OSIFT codes using advanced detection schemes against general weighted collusion attacks.

The OSIFT code design is developed based on the multi-carrier code-division-multi-access (MC-CDMA) wireless communication system. To improve the colluder detection performance, many advanced receiver techniques in the context of MC-CDMA can be used here as well. Following this line of thoughts, we propose advanced detectors to detect a larger number of colluders with general weighted collusion attacks. Our detection schemes include the maximal ratio combining (MRC) scheme for colluder detection in the same group and the multiuser detection (MUD) scheme for colluder detection in different groups. The performance of different detection schemes with respect to randomly weighted collusion attacks will be compared. It is demonstrated that HW-OSIFT and CI-OSIFT codes have robust performance in an exemplary audio watermarking system with the proposed detection schemes.

The rest of this paper is organized as follows. Background material is reviewed in Sec. II, including HW-OSIFT and CI-OSIFT codes, code embedding with shifted spreading, weighted collusion attacks, and code extraction and colluder detection. Advanced detection techniques are discussed in Sec. III. Then, the detection performance of HW-OSIFT and CI-OSIFT codes is analyzed in Sec. IV. Simulation results are shown in Sec. V using an audio watermarking system as an example. Finally, concluding remarks are given in Sec. VI.

## II. SYSTEM MODEL

The overview of a general fingerprinting code design, embedding and detection system is given in Fig. 1. Each module will be elaborated in following subsections. At the end of the section, we will present a general weighted attack model.

### A. OSIFT Code Design

A family of collusion-free hiding codes, known as the OSIFT (Orthogonal Spreading followed by the Inverse Fourier Transform) codes, was proposed in [1], [2]. However, only the Hadamard-Walsh (HW) orthogonal spreading codes were considered before. Here, we introduce another type of orthogonal spreading codes called the carrier interferometry (CI) codes.

The HW matrices can be recursively defined by [5]:

$$\mathbf{S}_N = \mathbf{S}_2 \otimes \mathbf{S}_{N/2} = \begin{pmatrix} \mathbf{S}_{N/2} & \mathbf{S}_{N/2} \\ \mathbf{S}_{N/2} & -\mathbf{S}_{N/2} \end{pmatrix} \quad (1)$$

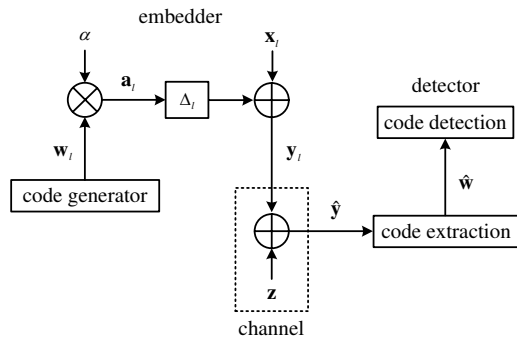


Fig. 1. The overview of a general fingerprinting code embedding and detection system.

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  $N \times N$ .

The CI codes can be represented by [6]:

$$\mathbf{S}_N = \begin{pmatrix} 1, & 1, & \dots, & 1 \\ 1, & e^{j2\pi/N}, & \dots, & e^{j2\pi(N-1)/N} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & e^{j2\pi(N-1)/N}, & \dots, & e^{j2\pi(N-1)^2/N} \end{pmatrix} \quad (2)$$

where  $N$  can be any integer number, which is different from that of HW codes. Both HW-OSIFT and CI-OSIFT codes offer excellent anti-collusion capability as demonstrated in later sections.

### B. Code Embedding

Code embedding is accomplished using a shifted spreading (delayed embedding) method to increase the number of users as proposed in [2]. Simply speaking, shifted spreading consists of  $G$  groups and  $P$  shifted users. In each group,  $P$  users share the same codeword and they are distinguished by shift amount  $\Delta_l = 0, 1, \dots, P-1$  under the condition  $P \bmod N$ . Thus, the total number of supportable users increases from  $L = G$  to  $L = PG$ .

A frequency domain audio watermarking, which has been widely used in the watermarking field [7], is implemented in this work. Let  $x_l(i)$ ,  $i = 0, \dots, T-1$ , be complex-valued samples of a host signal for user  $l$  of length  $T = NM$ . We divide it into  $M$  segments, each of which has  $N$  samples as

$$x_l(i) = x_l(m \cdot N + n), \quad \begin{cases} m = 0 \dots M-1 \\ n = 0 \dots N-1 \end{cases} \quad (3)$$

The additive code embedding method with shifted spreading is given mathematically by

$$y_l(i - \Delta_l) = x_l(i - \Delta_l) + a_l(i - \Delta_l) \quad (4)$$

where

$$a_l(i - \Delta_l) = \alpha w_l(i), \quad (5)$$

and where constant  $\alpha$  adjusts the embedded code strength, and  $w_l(i)$  is the hiding code generated from user identification (ID)  $u_l$ , spreading code  $s_l(i)$ , and the inverse fast Fourier transform (IFFT) for user  $l$ .

### C. Code Detection

We extract hiding codes from the host media via

$$\hat{y}(i) - x(i) = \sum_{k=1}^K h_k(i) \hat{w}_k(i). \quad (6)$$

After the hiding code is extracted, the fast Fourier transform (FFT) is taken before colluder detection. Colluder detection consists of two parts: i) detection of colluders in the same group and ii) detection of colluders in different groups. Colluder detection in the same user group is similar to a single user detection problem in wireless communication systems. It can be solved by channel estimation and the maximal ratio combining (MRC) or the frequency domain equalization (FEQ) techniques. Colluder detection in different user groups is closely related to users detection in a multiaccess interference (MAI) environment. The multiuser detection (MUD) technique has been developed to mitigate MAI. Two advanced detection techniques will be presented in Sec. III.

### D. Weighted Collusion Attack

A general form of weighted collusion attacks can be expressed as

$$\hat{y}(i) = \sum_{k=1}^K h_k(i) y_k(i - \Delta_k), \quad (7)$$

where  $\hat{y}(i)$  is the colluded signal,  $y_k(i - \Delta_k)$  is the host signal embedded with user code  $k$ , which is a function of shift amount  $\Delta_k$ . The value of  $h_k(i)$  is randomly generated (even with a negative value) as long as the following constraint is met:

$$\sum_{k=1}^K h_k(i) = 1, \quad i = 0, \dots, N-1.$$

## III. ADVANCED CODE DETECTION TECHNIQUES

### A. MRC Detection for Colluders from the Same User Group

The detection performance of colluders from the same user group can be enhanced by exploiting diversity through channel estimation in an MC-CDMA system. The maximal ratio combining (MRC), the equal gain combining (EGC), and the orthogonality restoring combining (ORC) techniques are adopted in MC-CDMA to achieve the minimum error probability of detected symbols.

To find a good balance between complexity and performance, we apply the MRC technique that assigns higher weights to stronger signals than weaker signals here. The MRC detection scheme can be written as

$$v_l = \sum_{n=0}^{N-1} \left( \sum_{k=1}^K \lambda_k(n) s_k(n) \right) \lambda_l^*(n) s_l^*(n) \quad (8)$$

where  $v_l$  is the statistics of detection and  $\lambda_l^*(n)$  is the frequency response. In practice,  $\lambda_l^*(n)$  can be estimated using channel estimation techniques [8]. For example, channel estimation can be achieved with pilot symbols in a wireless communication environment. A similar technique can be developed in the current context. Due to the space limitation, this is not elaborated here.

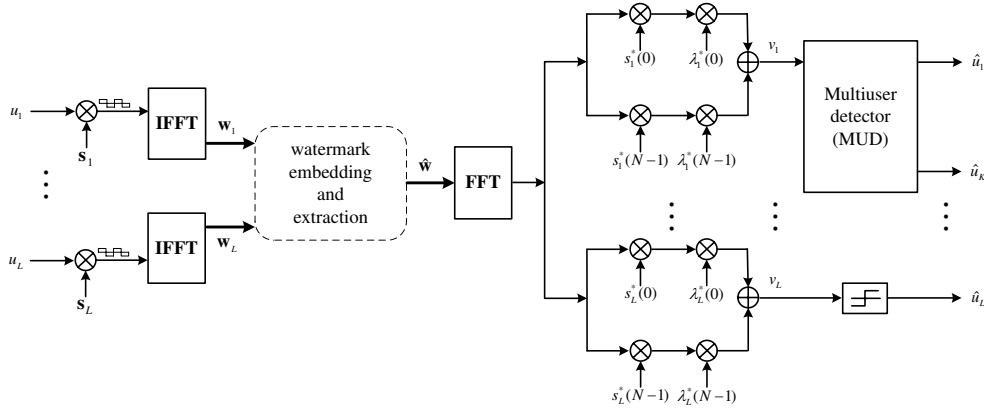


Fig. 2. The proposed OSIFT code generation and detection system.

### B. MUD Detection for Colluders from Different User Groups

More detection performance improvement for colluders from different user groups can be achieved using the multiuser detection (MUD) techniques [9]. There are linear and non-linear MUD detectors. Here, a linear MUD is applied after MRC detection. The detection relationship can be written of the vector-matrix form as

$$\mathbf{v} = \mathbf{R}\mathbf{u}, \quad (9)$$

where  $\mathbf{v} = (v_1, \dots, v_K)^t$  is obtained from (8),  $\mathbf{u} = (u_1, \dots, u_K)^t$  is the desired user signal, and  $\mathbf{R}$  is a cross-correlation matrix with dimension  $K \times K$ . One linear MUD is the decorrelating detector that decorrelates the inverse of the cross-correlation matrix by

$$\hat{\mathbf{u}} = \mathbf{R}^{-1}\mathbf{v}. \quad (10)$$

If  $\mathbf{R}$  is singular, the pseudo inverse is applied.

### C. Full OSIFT Code Generation and Detection System

We show in Fig. 2 the proper interface between the OSIFT code generation and detection modules and the general fingerprinting code embedding and extraction system given in Fig. 1. The dotted block in Fig. 2 is the same as that shown in Fig. 1.

### IV. DETECTION PERFORMANCE ANALYSIS

For an orthogonal code of length  $N$  under perfect synchronization with a fixed shift for user  $l$ , we can derive the following detection performance from Eq. (8):

$$v_l = \sum_{n=0}^{N-1} |\lambda_l(n)|^2 + \sum_{k=1, k \neq l}^K \text{MAI}_{l \leftarrow k}, \quad (11)$$

where  $\text{MAI}_{l \leftarrow k}$  is the interference of colluder group  $k$ 's code to colluder group  $l$ 's code detection. If  $\text{MAI}_{l \leftarrow k} = 0$ , the detection problem can be greatly simplified. The OSIFT codes are designed to achieve this purpose.

For the HW-OSIFT codes, the MAI term is equal to

$$\text{MAI}_{l \leftarrow k} = \sum_{n=0}^{N-1} \lambda_k(n) \lambda_l^*(n) s_k(n) s_l^*(n) \quad (12)$$

To be free from interference, we demand

$$\sum_{n=0}^{N-1} s_k(n) s_l^*(n) = \begin{cases} N, & l = k, \\ 0, & l \neq k. \end{cases} \quad (13)$$

For the CI-OSIFT codes, the MAI term is

$$\text{MAI}_{l \leftarrow k} = \sum_{n=0}^{N-1} \lambda_k(n) \lambda_l^*(n) e^{j \frac{2\pi k n}{N}} e^{-j \frac{2\pi l n}{N}} \quad (14)$$

To be free from interference, we require

$$\sum_{n=0}^{N-1} e^{j \frac{2\pi(k-l)n}{N}} = \begin{cases} N, & |k-l| = 0, \\ 0, & \text{else.} \end{cases} \quad (15)$$

If the number of colluders is less than a threshold, it is possible to get an interference free system. For more details, we refer to [8]. However, if the number of colluders is larger than the threshold, we need the MUD detector to resolve the interference among different user groups as discussed in Sec. III-B.

### V. SIMULATION RESULTS

We study the performance of HW-OSIFT and CI-OSIFT codes against the weighted collusion attack with various detectors. Three detection schemes are compared. They are the conventional correlation detector (*i.e.*, the matched filter), the MRC detector only and the advanced detection scheme (*i.e.*, the MRC detector followed by decorrelating MUD detector). An audio music signal sampled at 44.1KHz is used as the host signal. The code strength  $\alpha$  is set to 0.05, and the length  $N$  of spreading codes is chosen to be 256 as a basic unit. The length of user message is set to  $M = 32$ . We use the bit error probability (BEP) and the detection rate as two performance metrics. Simulation results are obtained from a total of 2000 simulation runs. Other parameters in our simulation include the following: the total number of users  $L = 512$ , codeword length  $N = 256$  and shifted spreading with  $P = 2$ . Weights in the collusion attack are generated randomly using a Gaussian distribution with zero mean.

The average BEP and the detection rate are plotted as a function of the number of colluders in Fig. 3 (a) and (b),

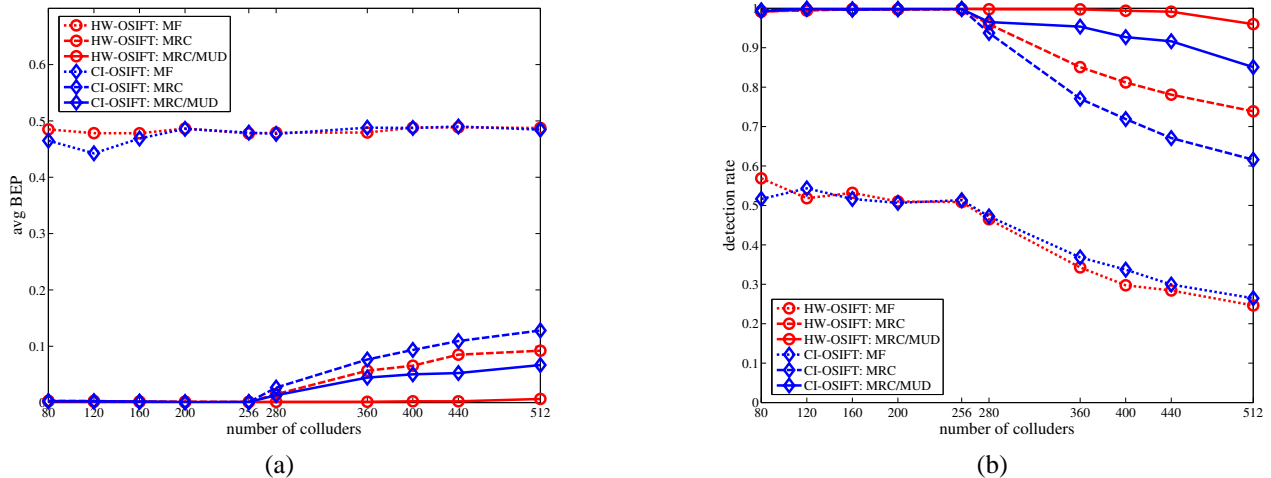


Fig. 3. Detection performance comparison using the matched filter (MF), the maximal ratio combining (MRC) only, and the integrated MRC/MUD scheme using HW-OSIFT and CI-OSIFT codes: (a) the BEP and (b) the detection rate.

respectively. The detection rate is determined by applying a fixed decision level to each BEP (*i.e.*,  $\eta = 0.10$ ) with a bound on the false alarm rate, *i.e.*,  $R_{fa} < 10^{-3}$ . The false alarm rate is an important measure since the fingerprinting system should not accuse innocent users as colluders. We see from Figs. 3 (a) and (b) that the MRC detector followed by decorrelating MUD detector gives the best performance (indicated by solid lines) for both HW-OSIFT and CI-OSIFT codes while the MF detector gives the worse performance (indicated by dotted lines). The performance of the MRC detector only lies in between (indicated by dashed lines). The HW-OSIFT and CI-OSIFT codes have comparable performance in the average BEP as well as the detection rate. Furthermore, their detection rate is equal to almost 100% when the interference-free conditions given in (13) and (15) are met. The performance of conventional matched filter is severely degraded due to randomly generated weights.

To compare HW-OSIFT and CI-OSIFT, we consider four scenarios in Table I, where the amount of shifts,  $P$ , is equal to 3 or 4 and the total number of users,  $L$  is set to 768 or 1024. As shown in Table I, both OSIFT codes can support more than 540 colluders for  $N = 256$  in case of 3 shifts and more than 768 colluders in case of 4 shifts with high detection rate situation. Also, we see that HW-OSIFT performs slightly better than CI-OSIFT.

## VI. CONCLUSION AND FUTURE WORK

Two anti-collusion codes, HW-OSIFT and CI-OSIFT, were introduced and their colluder detection performance using the MRC detector followed by the decorrelating MUD detector were studied in this work. It was shown by simulation results that both OSIFT codes are robust against weighted collusion attacks. We will consider the issue of weight coefficients determination in the near future.

## REFERENCES

[1] 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.

TABLE I  
COMPARISONS OF HW-OSIFT AND CI-OSIFT CODES.

HW-OSIFT with MRC followed by Decorrelator							
$\Delta_l = 0, 1, 2, P = 3, N = 256, L = 768$							
$K$	60	120	192	255	300	420	540
detection rate	0.99	0.99	0.99	0.99	0.99	0.99	0.97
$\Delta_l = 0, 1, 2, 3, P = 4, N = 256, L = 1024$							
$K$	80	160	256	340	400	560	720
detection rate	0.99	0.99	0.99	0.99	0.99	0.99	0.97
CI-OSIFT with MRC followed by Decorrelator							
$\Delta_l = 0, 1, 2, P = 3, N = 256, L = 768$							
$K$	60	120	192	255	300	420	540
detection rate	0.99	0.99	0.99	0.99	0.99	0.97	0.93
$\Delta_l = 0, 1, 2, 3, P = 4, N = 256, L = 1024$							
$K$	80	160	256	340	400	560	720
detection rate	0.99	0.99	0.99	0.99	0.99	0.96	0.92

[2] B.-H. Cha and C.-C. Jay Kuo, "Design of multiuser collusion-free hiding codes with delayed embedding," in *Proc. IEEE Int'l Conf. Intelligent Information Hiding and Multimedia Signal Processing*, Kaohsiung, Taiwan, November 2007.

[3] W. Trappe, M. Wu, Z. J. Wang, and K. J. R. Liu, "Anti-collusion fingerprinting for multimedia," *IEEE Transactions on Signal Processing*, vol. 51, pp. 1069–1087, April 2003.

[4] Z. Li and W. Trappe, "Collusion-resistant fingerprints from WBE sequence sets," in *Proc. IEEE Int'l Conf. Communications*, Seoul, Korea, May 2005, pp. 1336–1340.

[5] M. K. Simon, J. K. Omura, R. A. Sholtz, and B. K. Levitt, *Spread spectrum communications handbook*, McGraw-Hill, Electronic edition, 2002.

[6] B. Natarajan, C. R. Nassar, S. Shattil, M. Michelini, and Z. Wu, "High-performance MC-CDMA via carrier interferometry codes," *IEEE Transactions on Vehicular Technology*, vol. 50, pp. 1344–1353, November 2001.

[7] M. D. Swanson, B. Zhu, A. H. Tewfik, and L. Boney, "Robust audio watermarking using perceptual masking," *Signal Processing*, vol. 66, pp. 337–355, May 1998.

[8] 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.

[9] S. Verdú, *Multiuser detection*, Cambridge University Press, Cambridge, UK, 1998.