

DESIGN OF COLLUSION-FREE HIDING CODES USING MAI-FREE PRINCIPLE

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

Ming-Hsieh Department of Electrical Engineering and Integrated Media Systems Center
University of Southern California, Los Angeles, CA 90089-2564
E-mail: byungcha@usc.edu, cckuo@sipi.usc.edu

Abstract—A new methodology to design collusion-free hiding codes using the multi-access-interference-free (MAI-free) principle is proposed. A precoding technique was recently introduced in orthogonal frequency division multiplexing (OFDM) wireless communication systems to result in MAI-free codes [1], [2], which simplifies the receiver design greatly. Being motivated by this work, we propose a new class of collusion-free codes called the OSIFT (Orthogonal Spreading followed by the Inverse Fourier Transform) codes. It is demonstrated by computer simulation that OSIFT codes have more robust performance against collusion attacks than existing collusion-free codes in an exemplary audio watermarking system.

Index Terms—traitor tracing, collusion attacks, collusion-free codes, MAI-free principle, audio watermarking

I. INTRODUCTION

Multimedia contents can be easily distributed over wired and wireless broadband networks nowadays. Furthermore, copies of the same content can be delivered to multiple end users through multi-casting. In this context, it is important to develop a traitor tracing technique to identify unauthorized usage of distributed digital contents. A powerful attack to break the traitor tracing mechanism is the collusion attack. That is, users that have the same content embedded by different user authorization codes can merge their received copies in a certain way so as to remove authorization codes without degrading the quality of the original content.

Several hiding codes have been designed to address collusion attacks. A spread spectrum (SS) watermark embedding technique was proposed in [3], where codes are generated by an independently identically distributed (i.i.d.) uniform (or Gaussian) source. The resulting codes are robust against collusion attacks since the randomness of codes can provide the identification capability of colluded users. Furthermore, a collusion-secure (CS) code was proposed in [4], which adopts an error correction principle known as the marking assumption. As an improvement to the CS code, an anti-collusion code (ACC) was introduced in [5], which is built upon the concept of orthogonal modulation.

In this work, we consider a new approach to design collusion-free hiding codes using the multi-access-interference-free (MAI-free) principle. A precoding technique was recently introduced in orthogonal frequency division multiplexing (OFDM) wireless communication systems to result in MAI-free codes [1], [2], which simplifies the receiver design greatly. There exists a great similarity between the collusion attack model and the MAI effect. Being motivated by this work, we propose a new class of collusion-free codes called the OSIFT (Orthogonal Spreading followed by the Inverse

Fourier Transform) codes. It is demonstrated by computer simulation that the proposed OSIFT codes have more robust performance against collusion attacks than existing collusion-free codes in an exemplary audio watermarking system.

The rest of this paper is organized as follows. The collusion attack model and a typical watermark embedding and detection system are reviewed in Sec. II. A systematic framework for hiding code design is described in Sec. III. Then, the design of a collusion-free hiding code called OSIFT code is presented in Sec. IV. Computer simulation results are reported in Sec. V using an audio signal as an example. Finally, concluding remarks are given in Sec. VI.

II. RESEARCH BACKGROUND

A. Attack Model

The collusion attack is one of the cost-effective attacks to remove hiding codes without severe degradation of multimedia quality. It is achieved by a coalition of data hiding codes from multiple users. Mathematically, a general form of collusion attacks can be expressed as

$$\hat{y}(i) = \sum_{k=0}^{K-1} \lambda_k \cdot y_k(i) + e(i), \quad i = 0, \dots, N-1 \quad (1)$$

where \hat{y} is the colluded signal, y_k is the host signal embedded with user code k (called a colluder), e is the noise term, and λ_k is a weight factor for user k in the collusion attack.

We consider two specific types of collusion attacks according to the given equation (1): the average collusion attack [6] and the pre-colluded collusion attack [7]. The weights of all users are equal in the average collusion attack. In the pre-colluded collusion attack, we divide users into multiple groups, perform the average collusion attack in each individual group, and then perform another average collusion attack on the output signals of all groups. If these groups have a different number of users, this attack will result in an unequal-weight collusion attack.

B. Code Embedding and Detection

We follow the time-domain audio watermark embedding system as presented in [8] for code embedding at the transmitter end. Code detection is implemented using the traditional correlation detection method at the receiver end.

Consider signal $x(i)$, $i = 0, \dots, N-1$, of N samples as the host signal. It is divided into P segments, each of which has L samples. We can rewrite $x(i)$ for user j as

$$x_j(i) = x(p \cdot L + i), \quad \begin{cases} p = 0 \dots P-1 \\ i = 0 \dots L-1 \end{cases} \quad (2)$$

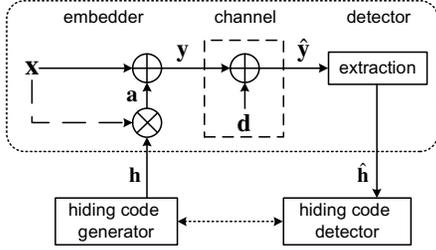


Fig. 1. The hiding code embedding and detection system.

Then, we adopt the following additive embedding method

$$y_j(i) = x_j(i) + a_j(i), \quad (3)$$

where $a_j(i)$ is the embedded code. Generally, we can express $a_j(i)$ as

$$a_j(i) = \alpha |x_j(i)| h_j(i), \quad (4)$$

where $h_j(i)$ is the hiding code for user j and α is a constant that adjusts the embedded code strength. The imperceptibility of the embedded code can be controlled by the α value.

For code detection, we consider the following antipodal binary hypothesis test:

$$\begin{cases} H_0 : \hat{y}_j(i) = h_j(i) + d_j(i), & m = +1, \\ H_1 : \hat{y}_j(i) = -h_j(i) + d_j(i), & m = -1, \end{cases} \quad (5)$$

where \hat{y}_j is the received signal, d_j 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

$$v_j = \frac{\sum_{i=0}^{L-1} (\hat{y}_j(i) - x(i)) s_j(i)}{\sqrt{\sum_{i=0}^{L-1} s_j(i) \cdot s_j(i)}}. \quad (6)$$

The statistics of v_j can be used as a metric to show the robustness of hiding codes. That is, we can calculate the bit error rate (BER) between the extracted user identification (ID) and the original user ID number u_j to evaluate the performance of different hiding codes from detection statistics. Furthermore, we can plot the receiver operating characteristics (ROC) using false positive and negative rates, which provides another good performance measure to compare different hiding codes. The overall code embedding and detection system is shown in Fig. 1.

III. FRAMEWORK FOR HIDING CODE CONSTRUCTION

The hiding code used in the watermarking field is much simpler than that in the communication field. We will demonstrate that it is advantageous to consider a more advanced hiding code so that the performance of the overall watermarking system can be enhanced. Since the hiding codes can be generated off-line, a slightly higher complexity in code generation is usually not a main concern.

A general framework for hiding code construction is illustrated in Fig. 2. This framework is motivated by the MC-CDMA (multi-carrier code division multi-access) or the PMU-OFDM (precoded multi-user orthogonal frequency division

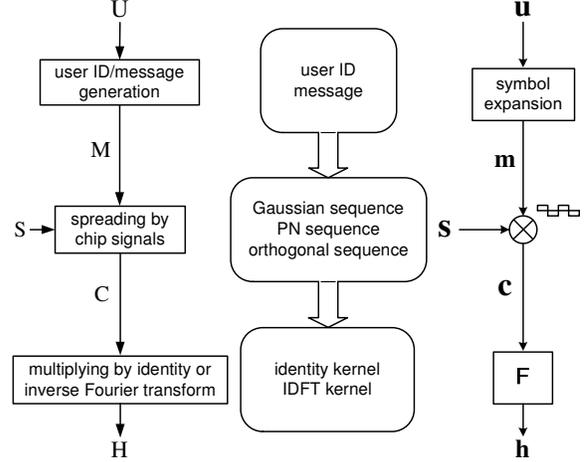


Fig. 2. A general framework for hiding code construction.

multi-access) communication systems [1], [2]. The system consists of three modules: 1) user ID/message generation, 2) spreading by chip signals, and 3) multiplication by the identity or the inverse Fourier transform matrix.

In the first module, we assign each user a data sequence of sufficient length called the message sequence. For a system with L users, we use $U = \{\mathbf{u}_j \in \mathbb{Z}, j = 1, \dots, L\}$ and $M = \{\mathbf{m}_j \in \mathbb{Z}, j = 1, \dots, L\}$ to denote the set of user ID numbers and the set of user message sequences, respectively. To identify a user uniquely from the observed message sequence, we can define a one-to-one mapping between U and M . The message sequence can be a one-bit or a multi-bit sequence [9].

In the second module, we choose a code (or a chip signal) for each user to modulate each symbol in his/her message sequence. The spreading code may take the binary value (*i.e.*, 1 and -1), the m -bit value, or the real value. The Gaussian and pseudo-noise (PN) sequences have been used as the spreading code. The maximal length sequences, Gold sequences and Kasami sequences are examples of PN sequences. The PN sequence has a noise-like spectrum so that code detection can be efficiently done by de-spreading if there is no collusion attack. However, under the collusion attack, since PN sequences have weak cross-correlation, codes of different users tend to interfere with each other in the despreading process. In contrast, orthogonal codes have zero cross-correlation between codes of different users so that they are more robust against the collusion attack. However, the price to pay is that the spike of their self-correlation spectrum is not as sharp as that of the PN sequences, which makes the code detection task more challenging. Examples of orthogonal codes include Hadamard-Walsh (HW) codes, Orthogonal Gold codes, Multirate OGold codes, and so on. When the collusion attack is considered, it appears that orthogonal codes are a more attractive choice than the Gaussian and PN codes.

In the third module, we select one from the following two choices: multiplied by the identity matrix or the inverse Fourier Transform (IFT) matrix. For the former case, the system is analogous to CDMA, which is a single carrier communication

scheme. For the latter case, the system is analogous to a multi-carrier communication scheme, which includes MC-CDMA and PMU-OFDM as special cases. It is well known that the multi-carrier communication system is more robust against frequency selective fading and has been widely used in broadband communication systems such as ADSL, Wi-Fi and WiMax.

We can also understand their difference from the following viewpoint. If the identity matrix is used, it means that the code design in the first and the second modules are conducted in the time domain. On the other hand, if the inverse Fourier transform matrix is used, it implies that the code design in the first and the second modules are actually conducted in the frequency domain. The flexibility of code design in the frequency domain allows the power of the resulting codes to be more uniformly distributed over a broader spectrum. As a result, it is more robust against the narrow-band interference [10].

IV. COLLUSION-FREE HIDING CODE: OSIFT

In this section, we consider the design of hiding codes that are robust against the collusion attack. Based on the hiding code construction framework described in the last section, we propose a specific hiding code called OSIFT (Orthogonal Spreading followed by the Inverse Fourier Transform) as follows. The following tasks are conducted in each individual module.

- 1) Assign L different messages of the same length to L users.
- 2) Each symbol in the message is spread by the orthogonal Hadamard-Walsh (HW) codes of length L .
- 3) The inverse Fourier transform is used.

The OSIFT code generation and detection system and its interface with the watermark embedding and extraction system are shown in Fig. 3. In this figure, E in the first stage denotes the user ID/message conversion, and S in the last stage denotes the statistics calculation and thresholding in the detector. Generally speaking, the watermark embedding/extraction

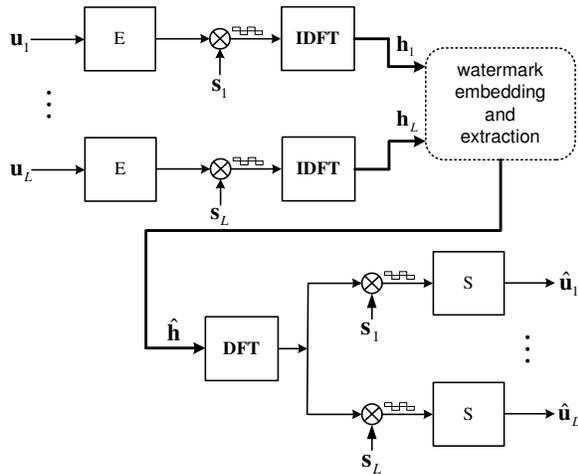


Fig. 3. The OSIFT code generation and detection system and its interface with the watermark embedding and extraction system.

system can be decoupled from the hiding code generation and detection system. In the fingerprinting and traitor tracing application, we often perform the watermark embedding/extraction process in real time, but do the hiding code generation and detection operation off-line. It is worthwhile to point out that the N -point inverse discrete Fourier transform (IDFT) yields complex-valued OSIFT codes. However, the $2N$ -point IDFT will result in real-valued OSIFT codes, which are more desirable.

The interference between codes of different users can be analyzed below. Given the colluded system in (1) and under the assumption of an additive embedding and a correlation detection scheme, we can calculate the correlation between code h_k of user k and code h_j of user j as

$$\begin{aligned}
 v_j &= \sum_{i=0}^{L-1} (\hat{y}(i) - x(i))s_j(i) \\
 &= \sum_{i=0}^{L-1} \left(\sum_{k=0}^{K-1} \lambda_k s_k(i) + e(i) \right) s_j(i) \\
 &= \lambda_j \sum_{i=0}^{L-1} |s_j(i)|^2 \\
 &\quad + \underbrace{\sum_{k=0, k \neq j}^{K-1} \lambda_k \sum_{i=0}^{L-1} s_k(i)s_j(i)}_{MAI_{j \leftarrow k}} + \sum_{i=0}^{L-1} e(i)s_j(i).
 \end{aligned} \tag{7}$$

Mathematically, to achieve the collusion-free property, we demand $MAI_{j \leftarrow k} = 0$, which is valid if an orthogonal code is used [11]. Here, we choose the HW codes due to their computational simplicity. Please note that the HW matrices can be recursively defined by

$$\mathbf{S}_L = \mathbf{S}_2 \otimes \mathbf{S}_{L/2} = \begin{pmatrix} \mathbf{S}_{L/2} & \mathbf{S}_{L/2} \\ \mathbf{S}_{L/2} & -\mathbf{S}_{L/2} \end{pmatrix} \tag{8}$$

where $L = 2^n$ ($n \geq 2$), \otimes is the Kronecker product, and

$$\mathbf{S}_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

The HW codes of length L are column vectors of HW matrices of dimension $L \times L$. Please note that HW codes only take 1 and -1 two values, which simplifies the spreading operation greatly. Since the proposed OSIFT codes are formed by L orthogonal HW codes, they can be assigned to L users to offer the collusion-free property.

V. SIMULATION RESULTS

In our simulation, a 16-bit audio music signal sampled at 44.1KHz is used as the host. The code strength α is set to 0.05, and the length L of the spreading codes is chosen to be 256. Thus, we can assign $L = 256$ different codes to 256 users. The length of user message is set to $P = 32$, which is generated randomly. Three spreading codes are considered: bounded Gaussian (BG), pseudo-noise (PN) and orthogonal HW codes (OS). By integrating them with the identity and the IFT transform in the third stage, we obtain six schemes: BG, PN, OS, BGIFT, PNIFT and OSIFT.

For the equal-weight collusion attack, we calculate the BER when the number of colluded users, N_c , ranges from 2 to 240 out of a total of 256 users. For the unequal-weight collusion attack, the number of pre-colluded users, N_p , ranges from 2 to 120 to yield one colluded copy in the first stage. Then, this copy is colluded with the other N_p users that do not participate in the collusion process before, which leads to an unequal-weight colluded copy in the second stage. After getting the individual BER for each colluded user, we average the BERs among all colluded users for performance comparison. Our simulation results are based on a total of 1000 simulation runs.

The BER results of the equal-weight collusion attack with six hiding codes are shown in Fig. 4. We see that the PN code and the OS code have non-zero BER when the number of colluded users is greater than 10 and 200, respectively. However, the OSIFT codes still have a zero BER even with 240 colluded users. The BER results of the unequal-weight collusion attack with the six codes are shown in Fig. 5. Again, we see that the OSIFT code gives the best performance while BG and BGIFT are the worst.

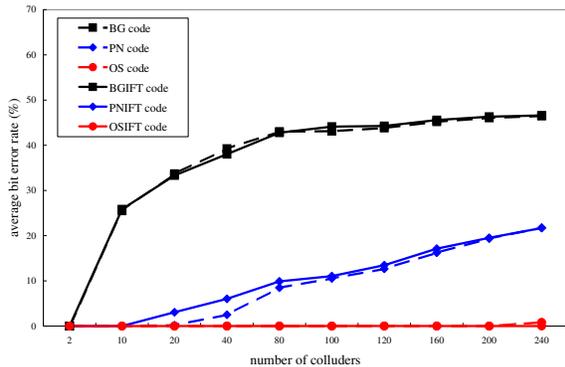


Fig. 4. The average BER results of BG, PN, OS, BGIFT, PNIIFT, and OSIFT codes against the equal-weight collusion attack.

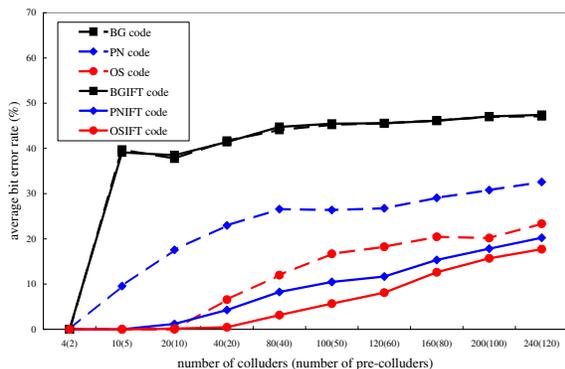


Fig. 5. The average BER results of BG, PN, OS, BGIFT, PNIIFT, and OSIFT codes against the unequal-weight collusion attack.

The ROC results of the six codes against the unequal-weight collusion attack are shown in Fig. 6. There are 128 colluded users with 64 pre-colluded users from colluded users, and other parameters are the same as that of the BER

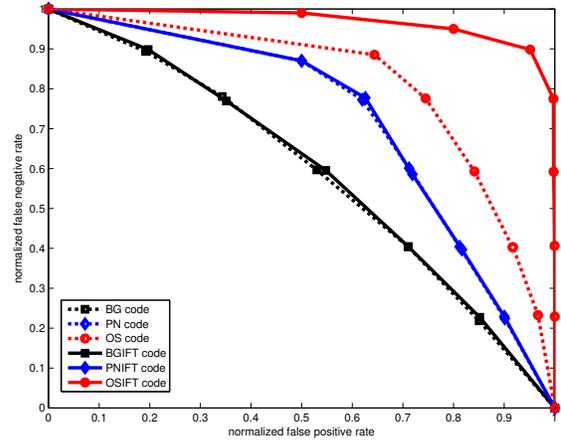


Fig. 6. The ROC curves of BG, PN, OS, BGIFT, PNIIFT, and OSIFT codes against the unequal-weight collusion attack.

simulation. This result is derived by 2000 simulation runs. We see from the result that the OSIFT code gives the best detection performance.

VI. CONCLUSION AND FUTURE WORK

Being inspired by multicarrier communication systems, a general framework of hiding code construction was presented and a collusion-free code called the OSIFT codes was proposed. It was shown by simulation results that OSIFT is robust against collusion attacks. Besides the collusion-free property, other properties of OSIFT codes are under our current study.

REFERENCES

- [1] 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.
- [2] 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.
- [3] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, pp. 1673–1687, December 1997.
- [4] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Transactions on Information Theory*, vol. 44, pp. 1897–1905, Sept. 1998.
- [5] 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.
- [6] H. S. Stone, "Analysis of attacks on image watermarks with randomized coefficients," Tech. Rep. Rep. 96-045, NEC Res. Inst. Tech., Princeton, NJ, 1996.
- [7] H. V. Zhao and K. J. R. Liu, "Risk minimization in traitors within traitors in multimedia forensics," in *Proc. IEEE Int'l Conf. Image Processing*, Genova, Italy, Sept. 2005, pp. 89–92.
- [8] 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.
- [9] M. Wu and B. Liu, "Data hiding in image and video: part I—fundamental issues and solutions," *IEEE Transactions on Image Processing*, vol. 12, pp. 685–695, June 2003.
- [10] 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, England, 2004.
- [11] M. K. Simon, J. K. Omura, R. A. Sholtz, and B. K. Levitt, *Spread spectrum communications handbook*, McGraw-Hill, Electronic edition, 2002.