Robust MC-CDMA-Based Fingerprinting Against Time-Varying Collusion Attacks

Byung-Ho Cha, *Student Member, IEEE*, and C.-C. Jay Kuo, *Fellow, IEEE*

***Abstract*—The design of robust fingerprinting systems for traitor tracing against time-varying collusion attacks in protecting continuous media, such as audio and video, is investigated in this research. We first show that it can be formulated as a multiuser detection problem in a wireless communication system with a time-varying channel response. Being inspired by the multicarrier code-division multiaccess technique, we propose a fingerprinting system that consists of three modules: 1) codeword generation with a multicarrier approach, 2) colluder weight estimation (CWE), and 3) advanced message symbol detection. We construct embedding codes with code spreading followed by multicarrier modulation. For CWE, we show that the weight estimation is analogous to channel response estimation, which can be solved by inserting pilot signals in the embedded fingerprint. As to advanced message symbol detection, we replace the traditional correlation-based detector with the maximal ratio combining detector and the parallel interference cancellation multiuser detector. The superior performance of the proposed fingerprinting system in terms of number of users/identified colluders and the bit-error probability of symbol detection is demonstrated by representative audio and video examples.**

***Index Terms*—Collusion attack, collusion-resistant fingerprinting, embedding codes, multimedia fingerprinting, time-varying colluder weights, time-varying collusion attack.**

I. Introduction

MULTIMEDIA content can be easily distributed over wired and wireless networks today with the rapid development of audio and video coding and networking technologies. For instance, a media file can be delivered to multiple users via multicast environment. To protect the copyright of content owners, one idea is to develop a traitor tracing system that can identify unauthorized distribution or usage of media files by tracing fingerprints of illegal users (i.e., traitors). However, there exists a simple yet effective attack that can break a naive traitor tracing system easily, which is known as the collusion attacks. The design of a fingerprinting system that is robust against collusion attacks has been an active research field in the last decade. A review of previous work in this field will be given in Section II.

Manuscript received August 16, 2008; revised May 25, 2009. First published June 30, 2009; current version published August 14, 2009. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. M. Kivanc Mihcak.

The authors are with the Signal and Image Processing Institute and the Ming Hsieh Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089-2564 USA (e-mail: byungcha@usc.edu; cckuo@sipi.usc.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2009.2025849

Most previous works deal with collusion attacks with equal weights or its variants (e.g., the cascade of several collusion attacks with equal weights). Consequently, the weight of each colluder is constant throughout the collusion process. The collusion attack on continuous media such as audio and video with time-varying weights can be simply implemented. However, we are not aware of any effective solution to this type of attack. Thus, the design of a robust fingerprinting system against time-varying collusion attacks is the main focus of this work.

To meet this challenge, we first relate the fingerprinting system design to a multiuser detection (MUD) problem in a wireless communication channel. Being inspired by the multicarrier code-division multiaccess (MC-CDMA) technique, we propose a fingerprinting system that consists of three basic modules: 1) codeword generation with a multicarrier approach, 2) colluder weight estimation (CWE), and 3) advanced user message symbol detection. Since the end-to-end fingerprinting system is analogous to an MC-CDMA communication system, we call it *MC-CDMA-based fingerprinting* system. The effectiveness of the MC-CDMA-based fingerprinting system in protecting continuous media against time-variant colluder weights will be fully examined.

In the area of embedding code design, we construct codes based on code spreading followed by multicarrier modulation. When a media file is distributed to a larger number of users, there is a higher probability of more colluders participating in an attack. Typically, if the number of colluders increases, the attack strength becomes stronger. Thus, one important performance measure of any collusion-resistant fingerprinting system is the maximum number of colluders allowed in this system under a certain detection criterion. The proposed MC-CDMA-based fingerprinting system can accommodate a very large number of users and identify a significant number of colluders without accusing innocent users as colluders. In the area of CWE, the weight estimation is analogous to channel response estimation, which can be handled by the insertion of pilot signals. Thus, for time-varying colluder weights, the allocation of user codes and pilot symbols is studied. As to effective receiver design, there exist many solutions in a multiuser wireless communication system [1], [2]. This motivates us to develop a better scheme for message symbol detection. Specifically, we replace the traditional correlation-based detector with the maximal ratio combining (MRC) detector and the parallel interference cancellation (PIC) multiuser detector.

Some of the concepts presented in this paper have been discussed in our earlier conference papers [3]–[6] due to the evolutionary nature of our research over the last two years. We have done our best in minimizing the overlap between this work and

1556-6013/$26.00 © 2009 IEEE

the previous ones, offering new insights, and providing a more thorough and unified treatment on this subject. Specifically, the discussion on time-varying collusion attacks and their solutions is entirely new.

The rest of this paper is organized as follows. Related previous works for background are described in Section II. The colluder detection problem is formulated in Section III. The MC-CDMA-based fingerprinting system is described in Section IV. Time-varying collusion attack and their properties are discussed, and a CWE scheme using pilot signals is proposed in Section V. Advanced user symbol detection schemes against time-varying collusion attack are studied in Section VI. Experimental results are given in Section VII to support discussion in previous sections and demonstrate the superior performance of the proposed fingerprinting system by representative audio and video watermarking examples. Similarities and differences between the fingerprinting and the MC-CDMA communication systems are reviewed and our research contributions are summarized in Section VIII. Finally, concluding remarks are given, and future research directions are pointed out in Section IX.

II. Background Review

Traditionally, there are two main approaches to the design of robust fingerprinting systems against collusion attacks. They are briefly reviewed as follows.

The first approach, called *independent fingerprinting*, is to adopt statistically independent spreading codes, which is relatively robust against jamming interference in wireless communication systems. Cox *et al.* [7] proposed a spread spectrum modulation (SSM) and embedding technique, where codes are randomly generated by an independently identically distributed uniform or Gaussian source. The resulting codes can resist average collusion attacks to a certain degree. Wang *et al.* [8] investigated the error performance of pseudonoise (PN) codes using maximum and threshold detectors and proposed a method to estimate the size of colluders. Zhao *et al.* [9] conducted a forensic analysis for unbounded Gaussian and bounded Gaussian codes under nonlinear collusion attacks (e.g., maximum, minimum, and median operations). Research in [8] and [9] gave a thorough performance analysis on the relationship between the code length and the user/colluder number and derived lower and upper bounds on probability error functions with respect to specific collusion attack models. Recently, a new scheme was proposed by Li and Trappe [10] based on the concept of the Welch bounded equality and the sphere decoding method.

The second approach, called *coded fingerprinting*, is to develop fingerprint codes using combinatorial design. Coded fingerprinting was first developed in early 1980s to protect generic data (e.g., header files or data in the database). To design a code that resists the collusion attack, Boneh and Shaw [11] proposed a collusion-secure (CS) code that meets certain properties called the *marking assumption*. Their method can catch one out of c colluders with a high probability if these colluders do not change the state of undetectable marks. Their method has several limitations. First, it works well only for symbol sequences with bit errors. It is not suitable for media files, since media data may be modified in the transmission process such as trans-coding or requantization. Second, to support a total number of L users, the code length is proportional to $c^2 \log^2 L$, which could be too long for a large value of c. Third, if the number of colluders exceeds a preselected c value, the tracing capability of codewords is totally lost. To improve the performance of the CS code, Trappe *et al.* [12] proposed a scheme called AND-anti collusion codes (AND-ACC) using the orthogonal code modulation. AND-ACC requires shorter codewords and achieves better colluder identification performance than the CS code. He and Wu [13] extended the CS code to the traceability codes using the SSM and a cross-layer design that separates coding and modulation.

Our approach is different from the above two traditional approaches. Here, we formulate the collusion-resistant code design problem as the spreading code design and symbol detection problem in the MC-CDMA communication system. Since the end-to-end fingerprinting system is analogous to an MC-CDMA communication system, it is called *MC-CDMA-based fingerprinting*. On one hand, unlike independent fingerprinting, codewords in our approach are not generated randomly but systematically (e.g., Hadamard–Walsh (HW) codes [3], [4] and carrier interferometry (CI) codes [6]). As a result, the length of codeword assigned to each user is much shorter. On the other hand, since our approach models the behavior of collusion attacks as the channel response of a wireless communication system, it provides a richer framework than coded fingerprinting in design and analysis. For example, we can estimate colluder weights and handle time-varying collusion attacks under this new framework. In contrast, these tasks are very difficult to accomplish with the coded fingerprinting approach.

It is worthwhile to mention that a sequence of papers on the design of collusion-resistant fingerprinting systems have been published by authors [3]–[6], [14]. To reduce the interference caused by multiuser access, known as the *multiple access interference* (MAI), in wireless communications, Tsai *et al.* [15] proposed to use the HW codes as spreading codes in MC-CDMA systems. It was shown in [3] and [4] that the same design can be used to obtain collusion-resistant fingerprints. Furthermore, we introduced the *delayed embedding* idea in [5] and [14] to increase the number of users. That is, a codeword can be circularly shifted to generate new codewords for other users. When these codewords are colluded, this is equivalent to a multipath fading channel. Finally, to improve fingerprint detection performance, several advanced symbol detection schemes were discussed in [6].

III. Colluder Detection Problem

After a media file is distributed to users, some users may participate in the collusion attack with an attempt to eliminate their fingerprints from the colluded media without any severe degradation of media quality. Thus, we can divide users into two groups: malicious users (or colluders) and innocent users. We use Φ to denote the set of all users and Ω the set of colluders. Clearly, Ω is a subset in Φ. Without loss of generality, we assume that there are L users and K colluders in the system. That is, $|\Phi| = L$ and $|\Omega| = K$.

Two types of collusion attacks were considered in the media fingerprinting literature, i.e., linear and nonlinear collusion attacks. They were also called *jamming attacks* in [16]. In the average collusion attack, weights of all users are equal to satisfy the fairness condition among colluders. However, the fairness condition is only meaningful with respect to correlation detection with equal power fingerprints in the statistical sense [17], [18]. It was shown in [9], [17], and [19] that nonlinear collusion attacks do not offer any advantage over average collusion attacks in terms of colluded multimedia quality. Since there may exist selfish colluders who would like to minimize their risk, the precolluded collusion attack was considered in [20], recently. In a precolluded collusion attack, colluders are divided into several groups, and an average collusion attack is first performed in each individual group. Then, another average collusion attack is performed on the outputs of all groups. The average and precolluded collusion attacks are both special cases of the weighted collusion attack. Stone [21] proposed a weighted collusion attack using randomized coefficients. Here, we consider an even more general setting, i.e., time-varying weighted collusion attack. To the best of our knowledge, this attack type has not been addressed well in the literature before.

A general time-varying weighted collusion attack can be expressed as

$$\hat{y}(i) = \sum_{k\in\Omega} h_k(i) y_k(i) + e(i) \tag{1}$$

where i is the sample (or time) index, $y_k(i)$ is the host signal embedded with colluder codeword k, $h_k(i)$ is the time-varying weight for colluder k, $e(i)$ is additive noise, and $\hat{y}(i)$ is the colluded signal. The weights need to satisfy the following constraint:

$$\sum_{k\in\Omega} h_k(i) = 1. \tag{2}$$

Note that $h_k(i)$ is not restricted to a value between 0 and 1. To provide a general attack model, we allow it to be negative and/or greater than unity. In practice, the distortion of a colluded copy should be restricted so that the colluded copy must be pleasant to human perception. This consideration may provide some limitations on the attack dynamic range in the collusion attacks [17].

For the dynamic range of colluder weights, it is a well known fact in communication science and engineering [22]–[24] that communication channels with time-varying channel responses are more challenging than those with constant channel responses. Since there exists one-to-one correspondence between time-varying channel responses and time-varying collusion attacks, time-varying collusion attacks are more challenging than constant collusion attacks studied in the literature. To the best of our knowledge, no previous fingerprint systems have been effectively designed for time-varying collusion attacks.

The colluder detection problem can be stated as follows. For received colluded signal $\hat{y}(i)$ in (1), we would like to identify all indexes in the colluder set Ω. The number of possible combinations is given by C_K^L. When all K colluders are found, the remaining $L-K$ users are automatically classified as innocent users. They form a complement set denoted by Ω^c.

We adopt the following additive embedding method for each user:

$$y_k(i) = x(i) + \alpha(i) w_k(i) \tag{3}$$

where $x(i)$ is the fingerprint-free source signal, $w_k(i)$ is the codeword (or fingerprint) of user k, and $\alpha(i)$ is a parameter related to the embedded code strength only with $x(i) > \mathrm{JND}(i)$. One way to determine $\alpha(i)$ is to use the just-noticeable-difference (JND) in human perceptual masking. That is, we choose

$$\alpha_0(i) = \begin{cases} A, & \text{if } x(i) > \mathrm{JND}(i) \\ 0, & \text{if } x(i) \le \mathrm{JND}(i) \end{cases} \tag{4}$$

where A is a value in a range of $(0,\ \infty)$, which is calculated from the JND model [25], [26]. In other words, we use the JND criterion to decide possible positions for fingerprint embedding. Let $\tilde{x}(i)$, $i = 0,\ \ldots,\ T-1$, be the sequence containing the selected samples of a host signal using the JND criterion in (4) for fingerprint embedding. Furthermore, it is assumed that $T = MN$ so that we divide it into M segments for message sequence, each of which has N samples for spreading codes as

$$\tilde{x}(i) = \tilde{x}(n + mN), \quad \begin{cases} m = 0 \ \cdots\ M-1 \\ n = 0 \ \cdots\ N-1. \end{cases} \tag{5}$$

For more details on JND and watermark embedding, we refer to [27] and [28].

Since the fingerprint detector knows $x(i)$, the detection process is typically performed by subtracting $x(i)$ from $\hat{y}(i)$. Thus, it is straightforward to derive the following equation from (1):

$$\hat{w}(i) = \sum_{k\in\Omega} h_k(i) w_k(i) + (\alpha(i))^{-1} e(i), \quad \alpha(i) \neq 0 \tag{6}$$

where $\hat{w}(i)$ is the colluded codeword and $w_k(i)$ is the codeword for colluder k. The noise energy should be limited if good quality of the colluded copy is demanded. To take the effect of noise $e(i)$ into account, we can study the problem from the angle of the fingerprint-to-noise ratio (FNR). We study the impact of colluder weights $h_k(i)$ under a sufficiently large FNR value in this work. The FNR effect will be illustrated by computer simulation in Section VII (see Examples 9 and 10).

Equation (6) can be reinterpreted in the context of wireless up-link communication. That is, Ω is the set of mobile users that send out their messages simultaneously to the same base station, $w_k(i)$ is the message of user k, and $h_k(i)$ is the channel response of the wireless link between user k and the base station at time i. The received message at the base station is $\hat{w}(i)$. The base station needs to detect user messages $w_k(i)$, $k \in \Omega$. Since we need to know the colluder messages to identify colluders, the colluder detection problem is equivalent to the MUD problem in the wireless up-link communication.

The problem given in (6) is an ill-posed one that allows multiple solutions. However, it is possible to solve by considering the following three factors.

1) Codeword design.
   We can impose constraints on user codewords (e.g., orthogonality) so that they can be conveniently separated at the receiver end.

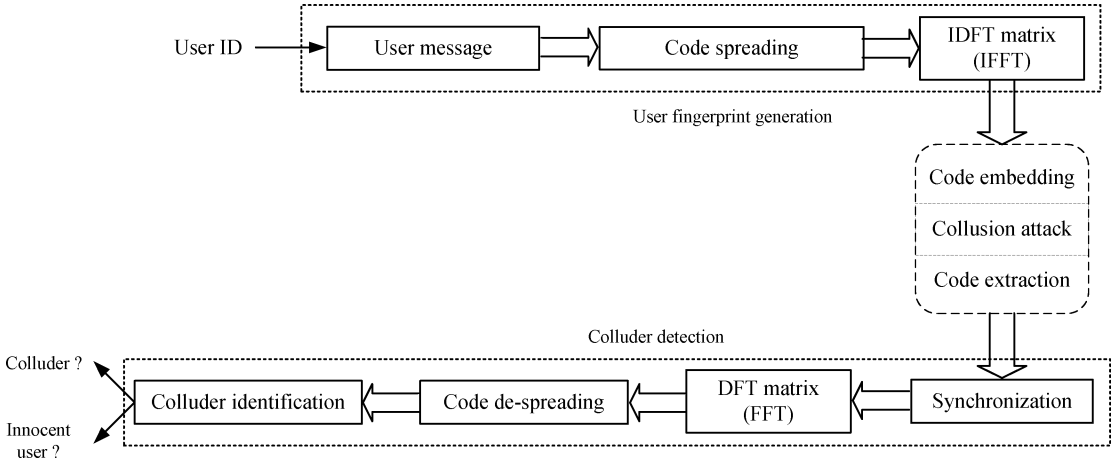

Fig. 1. Block-diagram of the proposed MC-CDMA-based fingerprinting system.

2) Colluder weight (or channel response) estimation.
   We can insert common pilot signals for all users so that the weight sequence $h_k(i)$ of each user can be found accordingly.
3) Advanced message symbol detection.
   We can adopt more advanced detection schemes at the receiver to enhance the detection performance.

These will be examined in detail in the following sections.

IV. MC-CDMA-Based Fingerprinting System

A. System Overview

The block-diagram of the proposed MC-CDMA-based fingerprinting system is shown in Fig. 1, which is motivated by the MC-CDMA communication system [15], [29]. It consists of three main modules: 1) user fingerprint generation, 2) collusion attack analysis, and 3) symbol detection and colluder identification. In this section, we will discuss tasks in modules 1 and 3 briefly. Although some concepts were discussed in our previous work before [3]–[6], [14], we have incorporated new ingredients such as error correction codes (ECCs) and the analysis of identified colluders. Time-varying collusion attacks will be discussed in the next two sections, which are entirely new.

The user fingerprint generation module consists of three blocks: 1) message generation, 2) spreading by the codeword, and 3) multiplication by the inverse discrete Fourier transform (IDFT) matrix. They are shown in the top row of Fig. 1.

The first block maps the ID of user l to the message of user l using ECCs. We use

$$U = \{\, u_l(i) \in \mathbb{B},\ i = 0,\ \ldots,\ U-1\}$$

and

$$M = \{\, m_l(i) \in \mathbb{B},\ i = 0,\ \ldots,\ M-1\}$$

where $\mathbb{B} = \{1, -1\}$, to denote the sets of user IDs and messages, respectively. For the sake of code spreading, the antipodal model [30] is used for symbol sequence representation in single-carrier (SC)- and multicarrier (MC)-CDMA systems. That is, a binary symbol takes values of 1 or -1. Since we cannot differentiate a symbol sequence with positive and negative signs, there are only 2^{U-1} distinctive users with U-bit IDs. Similarly,

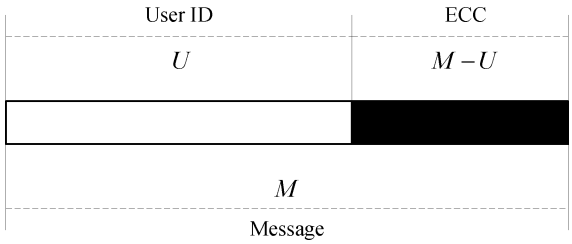

Fig. 2. ECC for the proposed MC-CDMA-based fingerprinting system.

there are 2^{M-1} distinctive user messages with M-bit messages in the output.

A block channel code that maps a U-bit input to an M-bit output, with $M > U$, is called an (M, U) code, which has the code rate

$$\rho = \frac{U}{M}, \quad 0 < \rho \le 1 \tag{7}$$

as shown in Fig. 2. Basically, we use $M - U$ bits as redundant bits to protect the leading U independent bits.

If code (M, U) has the minimum Hamming distance $d_{\min}$, it can correct all error patterns of bits up to

$$\upsilon = \left\lfloor \frac{1}{2}\left(d_{\min} - 1\right) \right\rfloor \tag{8}$$

which is called the random error correcting capability of the (M, U) code. If this block code is applied for error correction in a binary symmetric channel with transition probability p_υ, the probability with erroneous decoding is bounded by

$$\Pr(e) \le \sum_{i=\upsilon+1}^{M} \binom{M}{i} p_\upsilon^i \left(1 - p_\upsilon\right)^{M-i}. \tag{9}$$

Generally speaking, the error correction capability of a block code is determined by its minimum distance. It is desirable to construct a block code with a larger minimum distance. Previous research efforts have resulted in several classes of block codes [31], including Hamming, Reed–Muller, Golay, Bose–Chaudhuri–Hocquenghem (BCH), and low-density parity-check codes, etc.

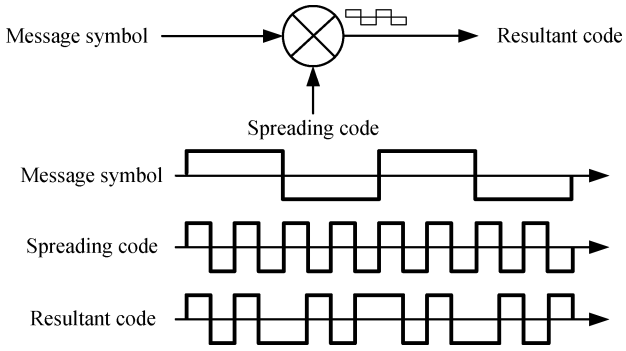

Fig. 3. Code generation via the product of the message symbol and the spreading code.

In the second block, we choose a codeword (also called a chip signal) for users to modulate each symbol in their message sequence. The spreading code also takes a binary value (i.e., 1 and -1). Two spreading codes, i.e., HW codes [32] and CI codes [33], were discussed before in [3]–[6] and [14]. They are particularly of interest since they yield very low interference between user messages spread by these codewords. In this work, we will consider the HW codes due to their simplicity. The HW matrices can be recursively defined by [34]

$$\mathbf{S}_N = \mathbf{S}_2 \otimes \mathbf{S}_{N/2} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} \mathbf{S}_{N/2} & \mathbf{S}_{N/2} \\ \mathbf{S}_{N/2} & -\mathbf{S}_{N/2} \end{pmatrix} \quad (10)$$

where $N = 2^r$ ($r \geq 2$) and $\otimes$ is the Kronecker product. The HW codes of length N are column vectors of HW matrices of dimension $N \times N$. For a given binary message symbol sequence, a periodic spreading code can be spread over the message symbol, as shown in Fig. 3. That is, the resultant code is equal to the multiplication of the message sequence and the periodic spreading code sequence. The orthogonality among users can be preserved after the spreading if the length of a message symbol is equal to an integer multiple of the period of the spreading code.

In the third block, we perform the IDFT operation to achieve multicarrier modulation. Note that if the IDFT and the discrete Fourier transform (DFT) blocks in the block-diagram of Fig. 1 are replaced by the identity matrix, the MC-CDMA system is reduced to the SC-CDMA system [29]. The comparisons of both MC-CDMA and SC-CDMA in the fingerprinting construction can be found in our previous work [3], [35].

Next, we embed fingerprints into a target media file using the additive embedding method as shown in (3). We may select the embedding domain, strength, and locations. The embedding domain can be time, discrete cosine transform coefficients, or wavelet coefficients. The frequency-domain code embedding technique has been widely studied for continuous media before, e.g., [28], [36]–[39]. A similar embedding approach is implemented in this work. Collusion attacks are unknown but have to be estimated by the proposed system. They will be discussed later in this paper.

To detect colluders, we first extract embedding codes from the host media in the proper domain by subtracting the host media from the received colluded file. Proper synchronization is needed in finding the start position of user messages. This can be achieved by embedding a known bit sequence, call a pilot signal, to all users. Then, we apply the DFT to extracted fingerprints and perform code despreading. Finally, we detect the symbol sequence for colluder identification. The relationship between symbol sequence detection and colluder identification will be elaborated in Section V.

TABLE I
COMPARISON OF THREE FINGERPRINT BIT ALLOCATION SCHEMES

Scheme	B_{id}	B_r	B_m	B_n	B_f	L
A	24	8	32	8	256	$2^{23} \times 8 = 2^{26}$
B	256	0	256	1	256	2^{255}
C	1	0	1	256	256	$2^8 = 256$

B. Fingerprint Bit Assignment

Suppose that the MC-CDMA-based fingerprinting system has a spreading code of B_n bits, a user ID of $B_{\rm id}$ bits, and B_r redundant bits for error correction. Then, the user message bit B_m is

$$B_m = B_{\rm id} + B_r \quad (11)$$

and after code spreading, the user fingerprint length becomes

$$B_f = B_n \times B_m. \quad (12)$$

For a fixed fingerprint length, there are different ways to allocate bits over $B_{\rm id}$, B_r, and B_n. Three exemplary schemes are given in Table I. The last column shows the number of users L that can be supported by the corresponding bit allocation scheme, where L is computed via

$$L = 2^{(B_{\rm id}-1)} \times B_n. \quad (13)$$

Since the antipodal model [30] is used for symbol sequence representation, there are only $2^{(B_{\rm id}-1)}$ distinctive users with $B_{\rm id}$ user ID bits.

In Scheme A, we distribute the total number of a fingerprint bits more evenly among the lengths of spreading codewords, user ID, and redundant bits. Schemes B and C are two extremes. In Scheme B, all bits are used for the user ID while the spreading codeword has only one bit. As a result, the multicarrier system is reduced to the single-carrier system. In Scheme C, all bits are used for the codeword representation while the user ID has only one bit. Thus, there are 256 groups, each of which has only one user.

If we target more users, it intends to go with Scheme B. However, Scheme B is very vulnerable to any type of attack. If there is a single bit error in the fingerprint detection process, this error will lead to a miss and a false alarm since it will be interpreted as another user ID by mistake. On the other hand, Scheme C is robust to any type of attack. To take the HW codes as an example, any two codewords are orthogonal to each other. In addition, one half of bits in any two codewords are identical while the other half differ by the sign. Intuitively speaking, they are well separated in the code space and, therefore, it is relatively easier to find the correct group for a user even in the presence of bit

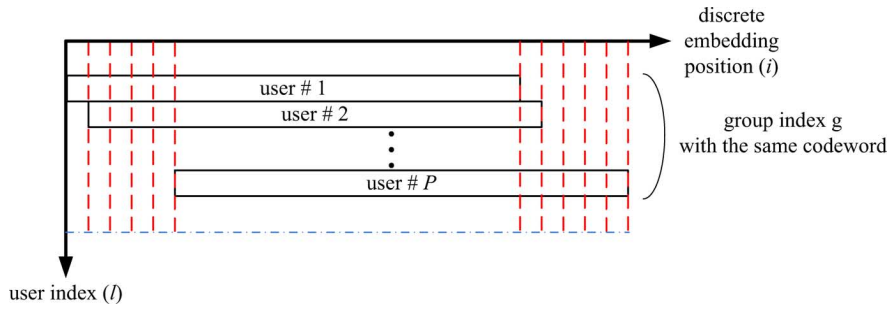

Fig. 4. Codeword reuse via circular shift in one user group.

errors in symbol detection. However, its robustness is achieved at the cost of a smaller number of users and higher computational complexity in symbol detection. For the latter, we will show that code despreading in the fingerprint detection module demands N correlation operations of two vectors of length N in Section IV-D.

Scheme A provides a better tradeoff between user capacity and robustness in colluder detection than Schemes B and C. However, finding the optimal bit allocation for a given fingerprint length is still an open problem. We choose parameters B_{id}, B_r, and B_n in our experiments in an ad hoc manner. The optimal choice of B_{id}, B_r, and B_n with respect to certain collusion attacks is an open research problem.

It is worthwhile to point out that the bit assignment in (11)–(13) can accommodate many more users than the SSM in [7]. The SSM assigns different spreading codes to different users for the identification purpose. For well-designed spreading codes (e.g., orthogonal codes), their length is typically proportional to the number of users L. Thus, the bit assignment of the SSM is similar to Scheme C in the above example.

C. Codeword Reuse Via Circular Shift

Although longer codewords are more robust to attacks, there is a restriction on their length due to the consideration of number of users and computational complexity in detection. The idea of *codeword reuse* was proposed in [5] and [14] to increase number of users. That is, we perform a circular shift on a codeword by Δ_l bits, where $\Delta_l = 0,\ 1,\ \ldots,\ P-1$, as illustrated in Fig. 4. Usually, we have $P \ll N$. Users with the same shifted codeword for code spreading form a subgroup, and there are P subgroups in a group. Then, the maximum number of users allowed becomes

$$L = 2^{(B_{\mathrm{id}}-1)} \times B_n \times P. \tag{14}$$

Again, there is a tradeoff between small and large P values. When P is larger, the user capacity is higher at the cost of detection errors. With the codeword reuse via circular shift, the collusion attack in (1) can be rewritten as

$$\hat{y}(i-\Delta_k) = \sum_{k\in\Omega} h_k(i-\Delta_k) y_k(i-\Delta_k) + e(i-\Delta_k) \tag{15}$$

where Δ_k is a shift amount for user k. Then, the additive embedding method in (3) for each user can be written as

$$y_k(i-\Delta_k) = x(i-\Delta_k) + \alpha(i-\Delta_k) w_k(i). \tag{16}$$

It was shown in [5] and [14] that if colluders are from the same group, in which codewords are related via circular shift, the collusion attack is equivalent to the response of a P-path fading channel. Then, colluder weights can be viewed as fading coefficients. Symbol detection in the presence of a multipath fading channel is well studied in wireless communication. Typically, we conduct channel estimation and combining in the frequency domain to enhance the message symbol detection performance, which will be detailed in Sections V and VI.

D. Two-Stage Colluder Identification

To identify colluders, we need to decode message sequence $\mathbf{m}_l$ and determine group and subgroup indexes of colluders using all possible spreading codes $\mathbf{s}_l$ and user IDs $\mathbf{u}_l$ with different shift amounts, respectively. The determination of the shift amount is similar to the synchronization process in wireless communication. Synchronization in wireless communication is not a trivial problem [40]. However, the problem is easier in our context since the basic shift unit Δ_p, which is a subset of Δ_l, is known. After the shift amount is found, it is reduced to a symbol-synchronous wireless communication problem. Then, the fast Fourier transform (FFT) can be applied to each synchronized position, and the determination of group/subgroup indexes and the recovery of user IDs can be performed.

In the first stage, we determine group/subgroup indexes of colluders via code despreading. This can be done by the correlation detector, whose output with respect to spreading code $s_l(n)$ can be written as

$$v_l = \sum_{n=0}^{N-1} [\hat{y}(n) - x(n)]\, s_l^*(n) + \sum_{n=0}^{N-1} e_l(n) s_l^*(n). \tag{17}$$

Equation (17) can be reorganized into

$$v_l = \sum_{n=0}^{N-1} \sum_{k\in\Omega} h_k(n) w_k(n) s_l^*(n) + \sum_{n=0}^{N-1} e_l(n) s_l^*(n) \tag{18}$$

where $\hat{y}(n)$ is the colluded output and $x(n)$ is the host signal. We can consider the following two cases.

Case I: The group with spreading code $s_l(n)$ has at least one colluder.

If colluders are from different groups, there exists intergroup interference (IGI), which is analogous to the MAI in wireless

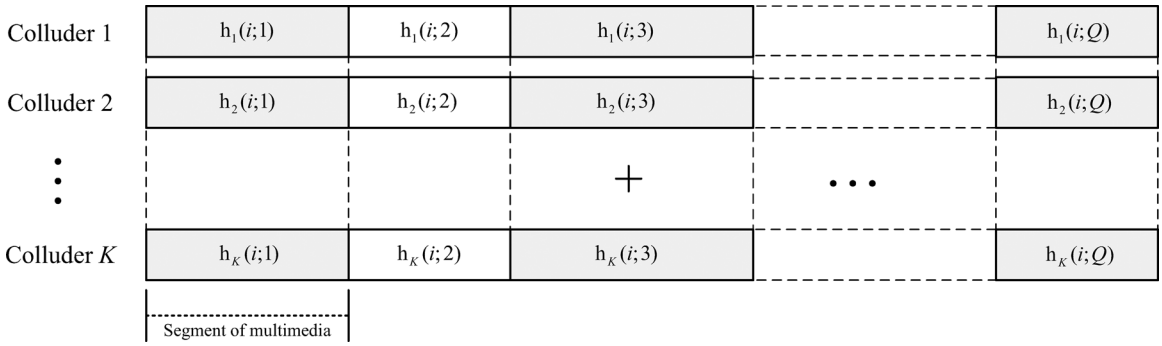

Fig. 5. Illustration of a time-varying collusion attack.

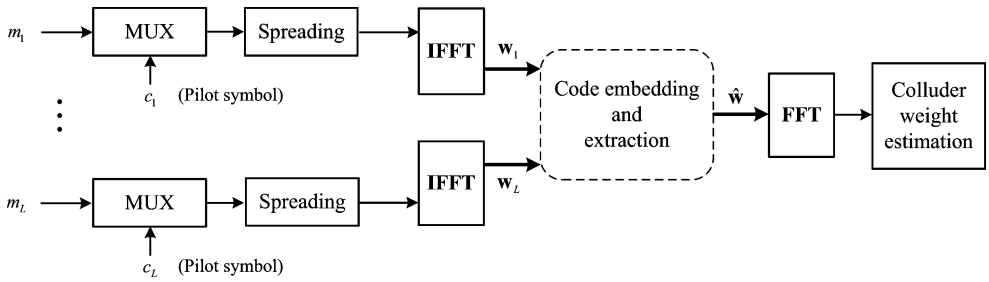

Fig. 6. CWE with pilot symbols.

communication. We can simplify (17) as

$$v_l = m_l \sum_{n=0}^{N-1} \lambda_l(n) + \sum_{k\in\Omega, k\neq l} \mathrm{IGI}_{l\leftarrow k} + \sum_{n=0}^{N-1} e_l(n) s_l^*(n) \quad (19)$$

where

$$\mathrm{IGI}_{l\leftarrow k} = \sum_{n=0}^{N-1} \lambda_k(n) s_k(n) s_l^*(n)$$

is the IGI term, and $\lambda_l(n)$ is the frequency response of colluder weight. It was shown in [15] that, when the HW codes are used, this term becomes negligible. In addition, the Gaussian noise term is also small. Thus, we can approximate the correlator output as

$$v_l \approx m_l \sum_{n=0}^{N-1} \lambda_l(n). \quad (20)$$

Case II: The group with spreading code $s_l(n)$ has no colluders.

We can simplify (17) as

$$v_l \approx \sum_{n=0}^{N-1} \sum_{j\notin\Omega} \lambda_j(n) s_j(n) s_l^*(n) + \sum_{n=0}^{N-1} e_l(n) s_l^*(n) \approx 0. \quad (21)$$

The first approximation is valid under the slow fading assumption and the second approximation holds due to the orthogonality of spreading codes and negligible Gaussian noise. Based on (20) and (21), we can use the following criterion to decide whether a group has at least one colluder:

$$|v_l| > \tau \quad (22)$$

where τ is a threshold to distinguish subgroup in one group.

In the second stage, we focus on groups that have at least one colluder. When there are multiple users in the same group, some of them may be colluders while others are not. We need to separate them. The sequence of message symbols for user l, $\mathbf{m}_l$, is converted back to the -1 or 1 sequence by $\mathrm{sgn}[\mathrm{Re}\{v_l\}]$, where sgn is the sign function, and Re takes the real part of a complex number. Then, block sequence $\mathbf{m}_l$ is decoded into the block of user ID $\mathbf{u}_l$.

Sometimes, there may exist errors in received bits in user messages so that there could be some confusion in finding the proper colluder ID. Generally speaking, the detector can identify a large number of colluders with a high level of confidence. By comparing the received message and the original message for each of the identified colluders, the detector can determine its bit-error probability (BEP). The lower the BEP, the higher the confidence level. The number of identified colluders can be determined by applying a fixed decision level η to the BEP of each colluder. Note that BEPs of colluders and of innocent users are different since only colluders participate in the collusion attack and their fingerprints remain in the colluded copy. In contrast, there should be no fingerprints of innocent users in the colluded copy in an ideal scenario. It is desirable that the BEP of colluders is as low as possible while that of innocent users is as high as possible. Generally, the wider the gap, the better the detection performance. We will re-examine this topic in Example 1 of Section VII. To avoid accusing any innocent user as a colluder, we choose η conservatively in our experiments in Section VII. That is, we do not allow any false alarm at the expense of a lower colluder detection rate.

V. Colluder Weight Estimation

A. Time-Varying Collusion Attack

Since the size of a media file is usually large, a segment-based approach is adopted in the collusion attack. That is, colluders change their colluder weights segment-by-segment in the same media

$$h_k(r;q), \quad r = 0, \ldots, R(q)-1 \quad \text{and} \quad q = 1, \ldots, Q \quad (23)$$

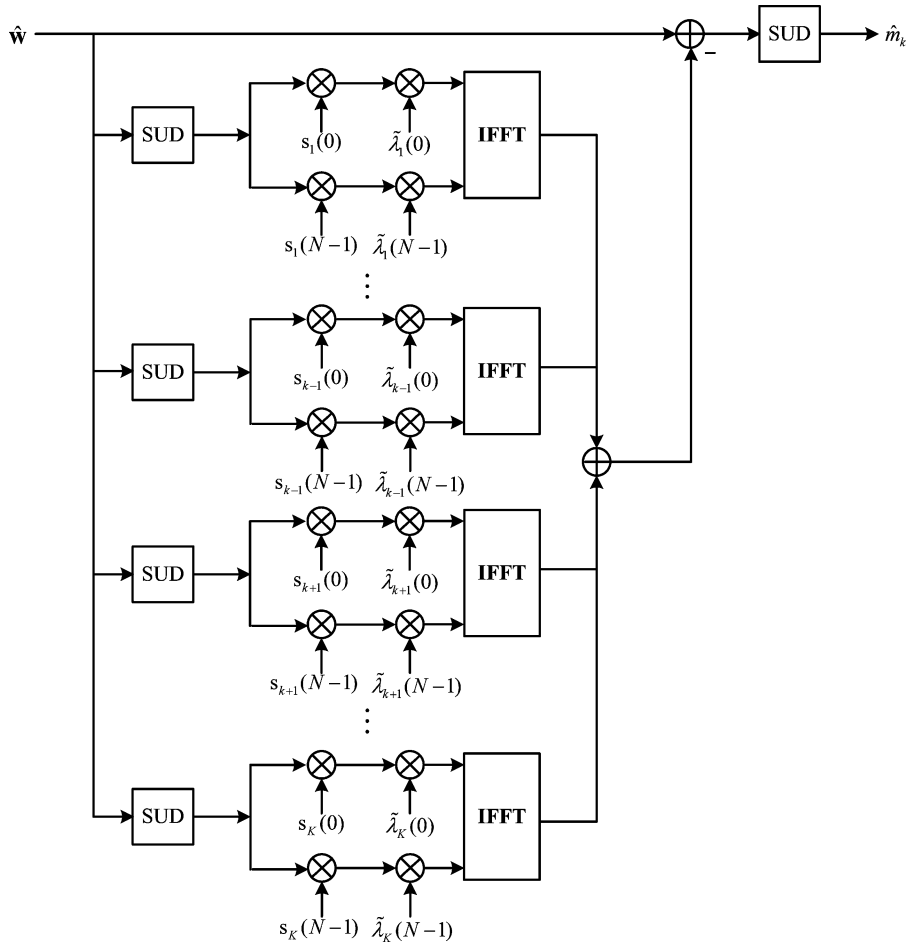

Fig. 7. Structure of the PIC Detector.

where $R(q)$ represents the number of samples in one segment, which can vary from one segment to the other, and Q represents the number of segments in a media as shown in Fig. 5. The time-varying collusion attack was examined in [17] before, and it was observed that as the changing speed gets higher (i.e., smaller segments), the distortion of a colluded media file is larger. In other words, colluders have to face the trade-off between the effectiveness of the attack and the quality degradation of the colluded media. In addition, if the segment is shorter, the computational complexity will become higher for a media file of fixed length. Colluders have to select suitable $h_k(r;q)$, $R(q)$, and Q to eliminate their fingerprints from the colluded media file while preserving its quality.

B. CWE Using Pilot Symbols

The estimation of colluder weights can be performed in the same manner as the uplink of multiuser communication. The receiver has to have some knowledge of channels in order to apply advanced symbol detection techniques. In practice, the channel information is estimated using channel estimation techniques. We follow the same idea and use the CWE technique to find the colluder weight information (CWI). Many channel estimation techniques exist in the literature [29], [41]. One technique is to employ pilot symbols [42]–[44].

Each circularly shifted codeword has its own colluder weight $h_k(i;q)$. The weights of colluders from the same group denoted by subscript k can be written in vector form as

$$\mathbf{h}_k = (h_k(0;q) \ \cdots \ h_k(P-1;q)). \tag{24}$$

The pilot-aided CWE method depicted in Fig. 6 can be used to estimate colluder weights. Let $\mathbf{F}$ be the $N \times N$ DFT matrix with

$$[\mathbf{F}]_{k,l} = \frac{1}{\sqrt{N}} e^{-j(2\pi kl/N)}, \quad k = 0, \ \ldots, \ N-1 \quad \text{and} \quad l = 0, \ \ldots, \ N-1. \tag{25}$$

Matrix $\mathbf{F}_p$ can be derived from (24) and the DFT matrix in (25)

$$\mathbf{F}_P = \mathbf{F} \begin{pmatrix} \mathbf{I}_P \\ \mathbf{0} \end{pmatrix}.$$

Then, the channel estimate vector is given by

$$\mathbf{\Lambda}_k = \mathbf{F}_P \mathbf{h}_k. \tag{26}$$

We refer to [15] and [41] for the justification of the algorithm described above.

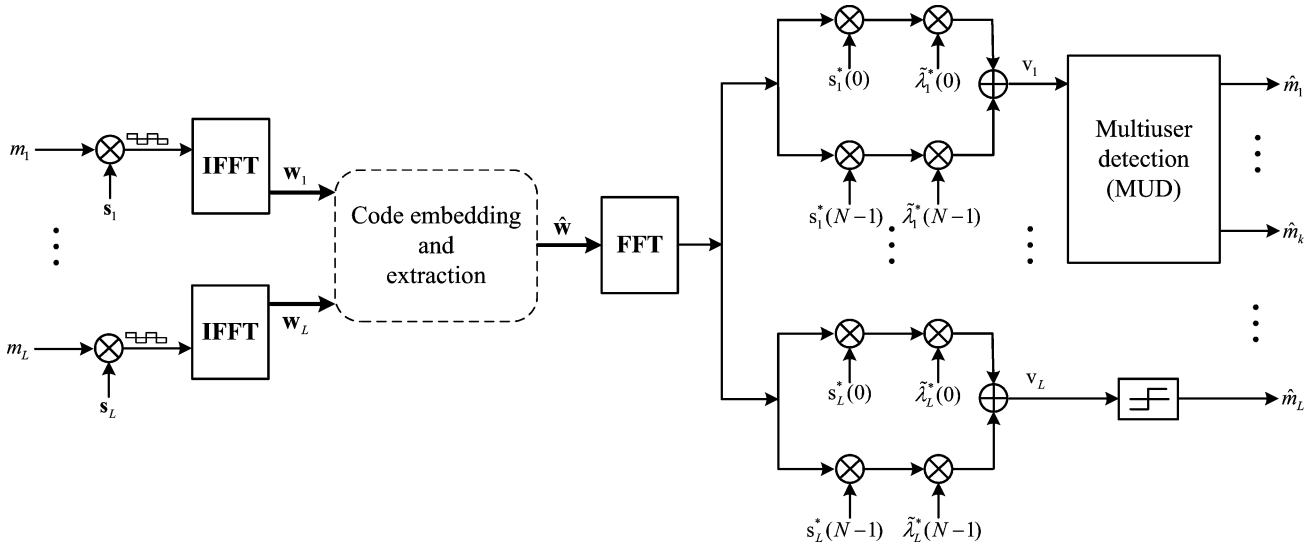

Fig. 8. Illustration of the MC-CMDA-based fingerprinting generation and detection system, where colluder detection is performed using the cascade of MRC and PIC detectors.

If there is no IGI, a single user channel estimation can be adopted for each shifted codeword, and the result is given by

$$\tilde{\lambda}_k(n) = \lambda_k(n)s_k(n)s_k^*(n) + \sum_{l\in\Omega, l\neq k} \lambda_l(n)s_l(n)s_k^*(n) + e_k(n)s_k^*(n) \quad (27)$$

where we assume pilot symbol $c_l(m) = 1$ and IGI term $\sum_{l\in\Omega, l\neq k} \lambda_l(n)s_l(n)s_k^*(n) = 0$. However, if there is IGI, the estimation performance can be degraded by the IGI effect [15]. Then, we can apply the diversity and interference cancellation techniques to determine the colluder weight vector, which is of the following form:

$$\tilde{h}_k(p) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \tilde{\lambda}_k(n) e^{j(2\pi np/N)}, \quad p = 0, \ldots, P-1. \quad (28)$$

For more detail, we refer to [29] and [45].

VI. Advanced Colluder Detection

The colluder detection performance can be improved by two advanced techniques. We can use the diversity combining technique to identify colluders in the same user group more accurately. The resulting detector, called the MRC detector, is discussed in Section VI-A. However, the performance of the MRC detector is limited by interference from colluders in other user groups. To improve this, we can apply the MUD technique [46]. The PIC technique is examined in Section VI-B.

A. MRC Detector

We can allow more users in the fingerprinting system via codeword reuse through circular shift. However, it introduces impairments of multipath propagation in the collusion attack. To overcome the multipath effect in the receiver, the detection performance of colluders from the same user group can be enhanced by exploiting diversity through channel estimation in an MC-CDMA system. Examples include the MRC, the equal gain combining, and the orthogonality restoring combining techniques. The MRC technique, which assigns higher weights to stronger signals, provides a good trade-off between complexity and performance. It is examined here. The MRC detection scheme can be written as

$$v_k = \sum_{n=0}^{N-1} \left(\sum_{l\in\Omega} m_l \lambda_l(n)s_l(n) \right) \tilde{\lambda}_k^*(n)s_k^*(n) \quad (29)$$

where v_k is the statistics of detection and $\tilde{\lambda}_k^*(n)$ is the conjugated frequency response of the colluder weight estimated from (27). If the number of colluders is small, we can get good performance by applying MRC only. However, if the number of colluders is larger, we need the MUD detector to resolve the interference among different user groups.

B. PIC Detector

There are two nonlinear MUD techniques [47], [48]: PIC and successive interference cancellation (SIC). Only PIC is examined in this work. We show one PIC stage in Fig. 7. The PIC stage can be conducted iteratively, and the interference among colluders reduces gradually.

The initial estimate $\hat{m}_k^{(0)}$, $k = 1, \ldots, K$ $(K \leq L)$ of PIC can be obtained from the hard decision of the single user detection (SUD) algorithm, e.g., MRC. That is, we have

$$v_k^{(0)} = m_k \sum_{n=0}^{N-1} |\lambda_k(n)|^2 + \sum_{l\in\Omega, l\neq k} m_l \sum_{n=0}^{N-1} \lambda_l(n)s_l(n)\tilde{\lambda}_k^*(n)s_k^*(n) + \hat{e}_k \quad (30)$$

where the first and the second terms in (30) correspond to the multipath term and the IGI term for the user group of index k, respectively, and

$$\hat{e}_k = \sum_{n=0}^{N-1} e_k(n)\tilde{\lambda}_k^*(n)s_k^*(n).$$

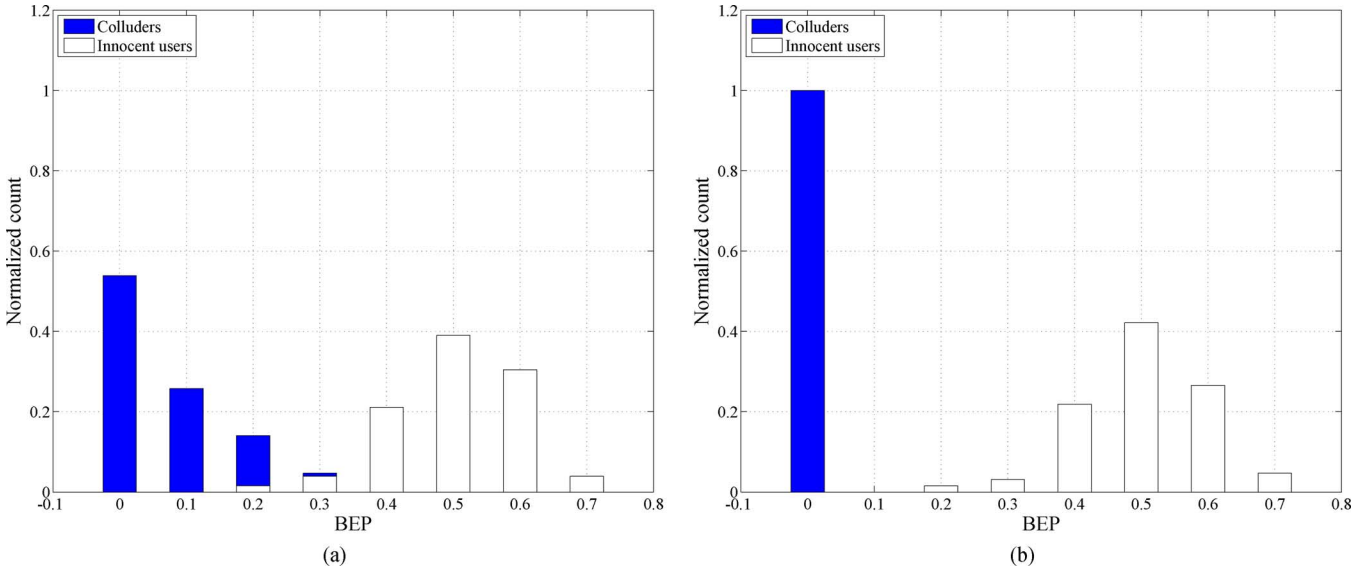

Fig. 9. Comparison of BEP histograms of colluders and innocent users with (a) the MF detector and (b) the MRCPIC detector.

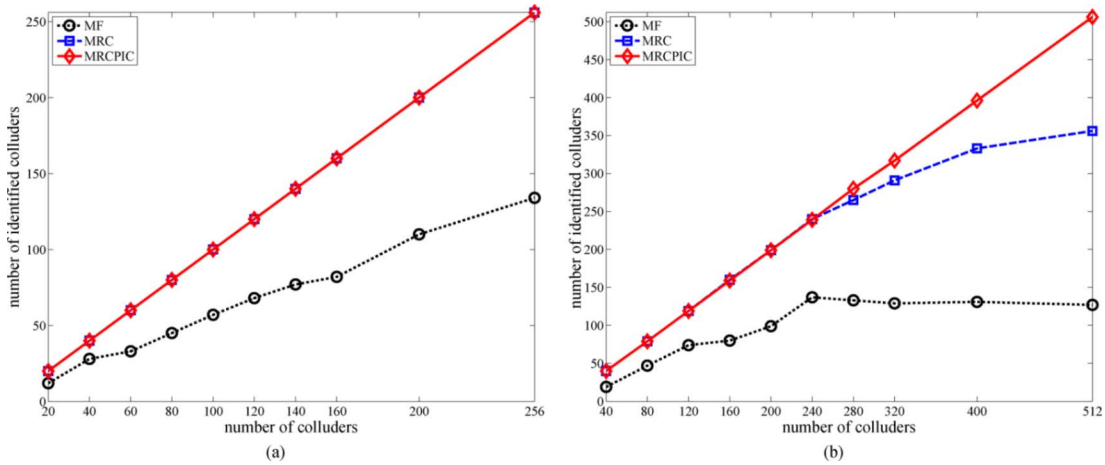

Fig. 10. Comparison of the colluder identification performance with three detectors (MRC, MRCPIC, and MF) and (a) no shift and (b) 1-bit shift in codeword reuse.

Given estimate $v_k^{(c)}$ in the cth stage, we perform SUD for these K colluders in parallel in the $(c+1)$th stage as

$$v_k^{(c+1)} = v_k^{(c)} - \sum_{l\in\Omega, l\neq k} \operatorname{sgn}\left[\operatorname{Re}\left\{v_l^{(c)}\right\}\right] \sum_{n=0}^{N-1} \lambda_l(n) s_l(n) s_k^*(n) \tilde{\lambda}_k^*(n) + \hat{e}_k \tag{31}$$

to mitigate the interference from other colluders furthermore. By substituting $v_l^{(c)}$ in (30) from (31), we have

$$\begin{aligned} v_k^{(c+1)} = {} & m_k \sum_{n=0}^{N-1} |\lambda_k(n)|^2 \\ & + \sum_{l\in\Omega, l\neq k} \sum_{n=0}^{N-1} \lambda_l(n) s_l(n) s_k^*(n) \tilde{\lambda}_k^*(n) \\ & \cdot \left(m_l - \operatorname{sgn}\left[\operatorname{Re}\left\{v_l^{(c)}\right\}\right]\right) + \hat{e}_k. \end{aligned} \tag{32}$$

The bit of user's message in the $(c+1)$th PIC stage can be obtained by

$$\hat{m}_k^{(c+1)} = \operatorname{sgn}\left[\operatorname{Re}\left\{v_k^{(c+1)}\right\}\right]. \tag{33}$$

Finally, we show the proper interface between the fingerprint generation and detection modules in Fig. 8, where the detection module is formed by the cascade of MRC and PIC detectors. This is called the MRCPIC detector. The performance of the MRC and MRCPIC detectors will be studied in the next section.

VII. Experimental Results

The performance of proposed MC-CDMA-based fingerprinting system against time-varying collusion attacks is examined in this section. The MC-CDMA-based fingerprinting system is implemented by MATLAB, and the source codes are available in the following website: http://byunghopaulcha.googlepage.com.

We simulated the MC-CDMA system by following the description in [35] with three detection schemes: the MRC

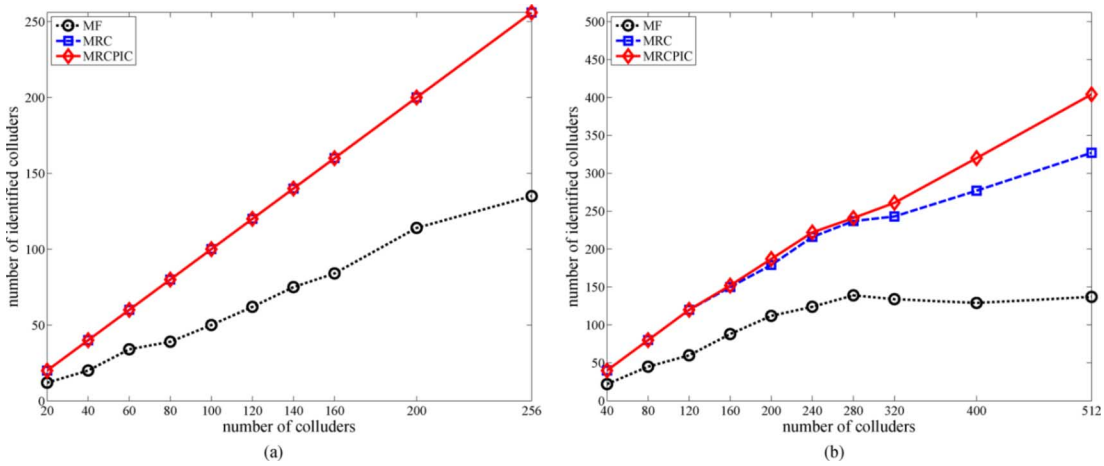

Fig. 11. Performance comparison of three detectors (MRC, MRCPIC, and MF) with estimated CWI: (a) no shift and (b) 1-bit shift.

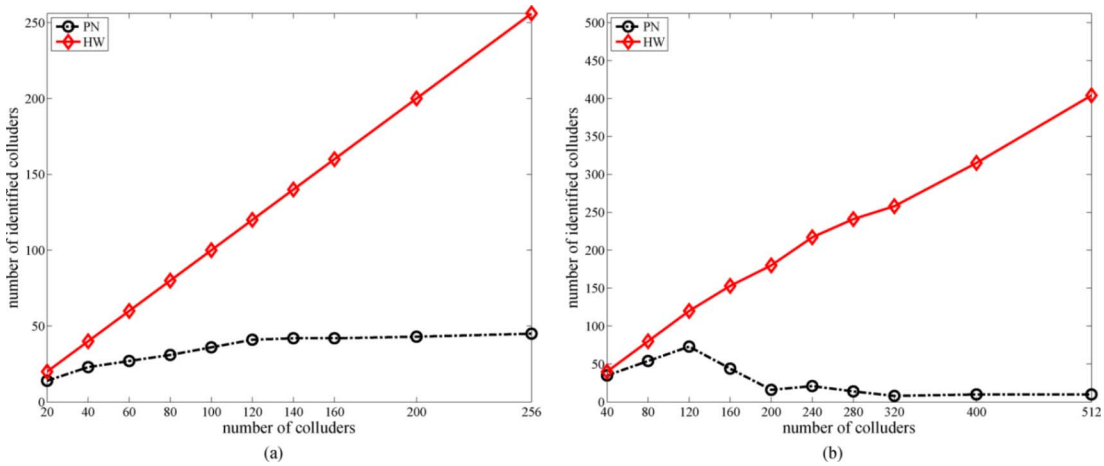

Fig. 12. Comparison of PN and HW spreading codes: (a) no shift and (b) 1-bit shift.

detector only, MRC followed by PIC-MUD (denoted by MRCPIC), and the conventional correlation detector (i.e., the matched filter (MF) detector). Both MRC and PIC-MUD were conducted based on the knowledge of CWI, which was estimated from pilot symbols. The MF detector is widely used in the fingerprinting, and it was implemented for performance bench-marking. The PN and HW codes were adopted as two spreading codes in the MC-CDMA system for comparison. Colluder weights in the collusion attack were generated randomly using a Gaussian distribution with zero mean, and a set of K colluders are randomly selected in a set of L users ($K \leq L$).

Simulation results are obtained from a total of 1000 simulation runs. For Examples 1–6, the length of spreading codes is chosen to be $N = 256$ as a basic unit. The length of the user message is set to $M = 32$. The total length of embedding codes is $T = NM = 8192$ without pilot symbols. If we add one pilot symbol, we need an additional 256 bits. From (14), the total number of users that can be supported is $L = 2^{31} \times 256$ without any shift (i.e., $P = 1$).

Example 1: Comparison of BEP Between Colluders and Innocent Users: One performance metric of the proposed MC-CDMA-based fingerprinting system is the BEP after colluder detection. In Fig. 9, we show the BEP histograms of colluders and innocent users under perfect CWI knowledge. We plot the performance of two detectors, MF and MRCPIC, in Fig. 9(a) and (b), respectively. For the MF detector, the BEPs of colluders and innocent users overlap with BEP equal to 0.2 and 0.3. Thus, they cannot be easily separately. In contrast, for the MRCPIC detector, we see a clear separation between BEPs of colluders and innocent users. (Specifically, BEPs of all colluders with the MRCPIC detector are equal to zero.) Thus, we can use a threshold to differentiate them easily.

The received user message may be different from all user messages embedded earlier due to bit errors resulting from the collusion attack and the colluder detection processes. Then, we can choose the user message that is closest to the detected one, and compute the BEP accordingly. As discussed in the end of Section IV-D, we can adjust the threshold value, η, to allow a trade-off between the false alarm rate and the miss rate. For example, we can choose a threshold η (e.g., $\eta = 0.1$) closer to the BEP of colluders to lower the false alarm rate at the cost of an increased miss rate. This could be more desirable since the penalty of a false alarm (accusing an innocent user as a colluder) is higher than that of a miss (missing a colluder in the detection). After decision level η is determined, we check the BEPs of all detected colluders. A detected colluder whose BEP is lower than η is confirmed to be a true colluder. Otherwise, we

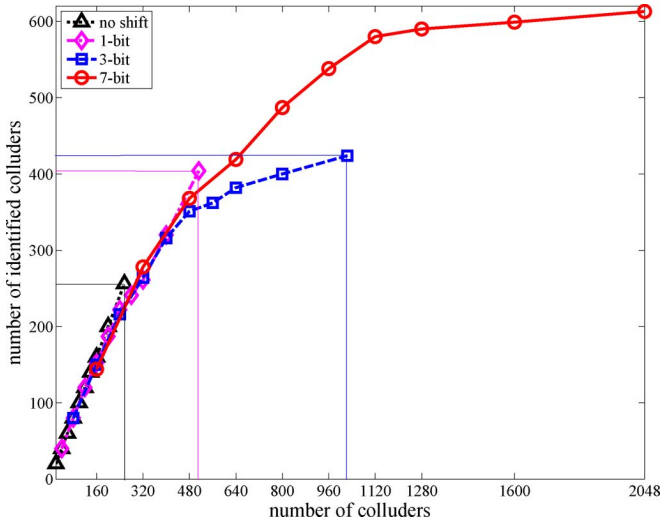

Fig. 13. Comparison of various shifts with the MRCPIC detector: no shift, 1-bit shift ($\Delta_l = 0, 1$), 3-bit ($\Delta_l = 0, 1, 2, 3$), and 7-bit shift ($\Delta_l = 0, 1, 2, 3, 4, 5, 6, 7$).

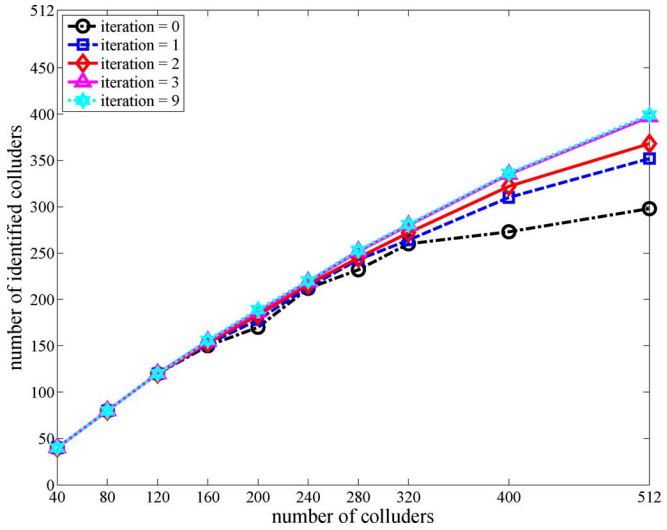

Fig. 14. The effect of the number of PIC iterations on the performance of the MRCPIC detector in the 1-bit shift case.

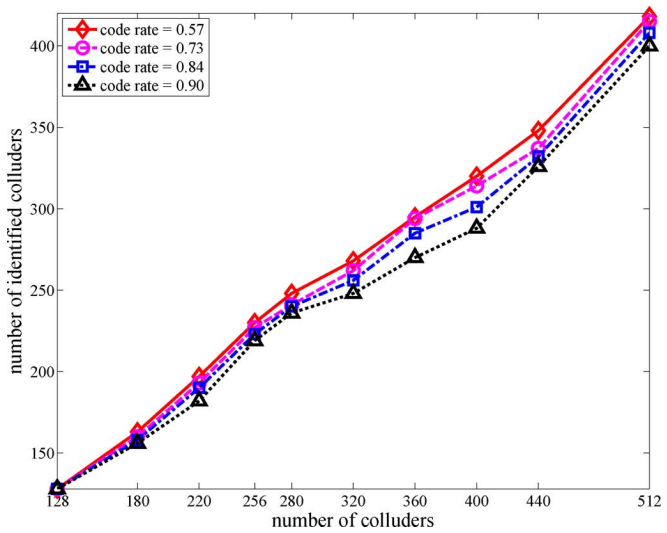

Fig. 15. The impact of the code rate on the number of identified colluders with the MRCPIC detector.

will reclassify it to an innocent user. If the BEP of a colluder is higher than η, a miss occurs.

Example 2: Colluder Identification Performance: We plot the number of identified colluders as a function of the total number of colluders participating in the collusion attack with the perfect CWI in Fig. 10 with no shift and 1-bit shift in codeword reuse. Again, we observe that MRCPIC gives the best performance while the MF detector gives the worst performance. In the case of no shift, MRC and MRC/PIC-MUD give the same performance since there is no colluder interference within the same codeword group. In the case of a 1-bit shift, the performance of MRC degrades when the number of colluders becomes large.

Example 3: Performance Comparison With Estimated CWI: We consider the estimation of CWI from pilot symbols in this example, where the length of pilot code is 256. The pilot codes for all users are embedded in the same position of the media file, and the power of pilot codes is kept at the same level as user spreading codes. The length of fingerprint codes should be properly extended depending on the codeword reuse scheme. That is, 256 for no shift and 512 for the 1-bit shift. The latter case needs twice the space to achieve IGI-free pilot-based estimation. The number of identified colluders is plotted as a function of the total number of participating colluders in Fig. 11. We see almost the same performance as that in Fig. 10(a) when there is no shift in codeword reuse. For the 1-bit shift case, the performance degrades due to the impairment of estimated CWI using pilot symbols in the presence of a multipath channel [32].

Example 4: Comparison of PN and HW Spreading Codes: We compare the performance of PN codes and HW codes with no shift and 1-bit shift in Fig. 12, where the MRCPIC detector was used. Clearly, HW achieves better identification performance than PN, which is even more obvious in the 1-bit shift case. Since PN codes have a cross-correlation term to achieve the high peak in correlation detection, they experience a strong IGI effect [29] when the collusion attack occurs between colluders from different colluder groups. The PN is a poor choice if interference cannot be properly handled for pilot-based estimation and MRCPIC detection in the receiver as observed in [48].

Example 5: Comparison of the Shift Effect in Codeword Reuse: We compare the shift effect on the colluder identification performance with HW codes and estimated CWI in Fig. 13. The system can support 256, 512, 1024, and 2048 users with zero, 1-bit, 3-bit, and 7-bit shifts, respectively. We see that the number of identified colluders is equal to 256, 410, 430, and 620 in the extreme case (that is, all users participate in the collusion attack). In other words, the ratio of identified colluders drops. More shifts degrade the colluder identification performance more, which is related to the multipath fading effect. The problem of detecting a large number of users in a multipath fading environment is difficult [24].

Example 6: The PIC Iteration Effect: The PIC module is used to cancel interference from other colluders in the collusion attack. Intuitively, a larger PIC iteration number tends to improve

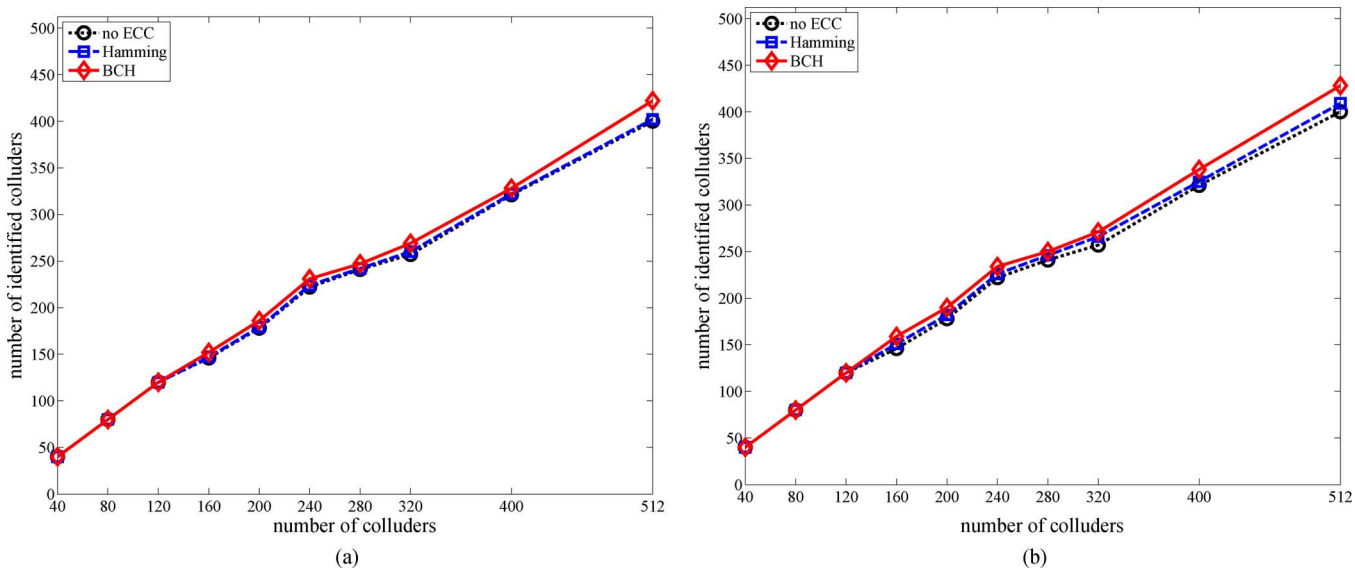

Fig. 16. Comparison of ECCs (no ECCs, the Hamming codes and the BCH codes) with the MRCPIC detector under two code rates: (a) $\rho = 0.73$ and (b) $\rho = 0.57$.

the colluder detection performance. To see the effect of the PIC iteration number, we plot the number of identified colluders as a function of the total number of participating colluders parameterized by the PIC iteration number in Fig. 14. Five cases were compared: no PIC, one, two, three, and nine PIC iterations. We see that the performance improves up to three iterations. After that, the performance remains about the same with more iteration numbers. The gap between no and one PIC iteration is significant when the number of participating colluders is larger.

Example 7: Impact of the Code Rate: Recall that the code rate is the ratio of the number of user message bits over the full message length with error correction coding as defined in (7). We plot the number of identified colluders as a function of the total number of participating colluders parameterized by the code rate, where the Hamming code was adopted as the ECCs in Fig. 15. We see that, as ρ increases, the performance is poorer. This is because a larger ρ value leads to a higher BEP, and it is more difficult to separate colluders and innocent users.

Example 8: Comparison of ECCs: We compare the effect of different ECCs with the MRCPIC detector in Fig. 16. They are the (15, 11) and (7, 4) codes for both Hamming and BCH [31]. We also show the performance of no ECC as the performance benchmark, where bits reserved for error correction were set to one default pattern (say, all 0's or 1's). The following two cases were examined.

1) the user ID length was $U = 55$, the message length was $M = 75$, and the code rate was $\rho = 11/15 = 0.73$;
2) the user ID length was $U = 40$, the message length was $M = 70$, and the code rate was $\rho = 4/7 = 0.57$.

The total length of embedding codes was $T = NM = 256 \times 75 = 19200$ for $\rho = 0.73$ and $T = NM = 256 \times 70 = 17920$ for $\rho = 0.57$. The 1-bit shift was used for codeword reuse. We see from the figure that the number of identified colluders increases when the BCH and the Hamming codes are applied. The performance of ECC codes decreases as the code rate increases (i.e., less protection). The BCH codes outperform the Hamming codes at the same code rate.

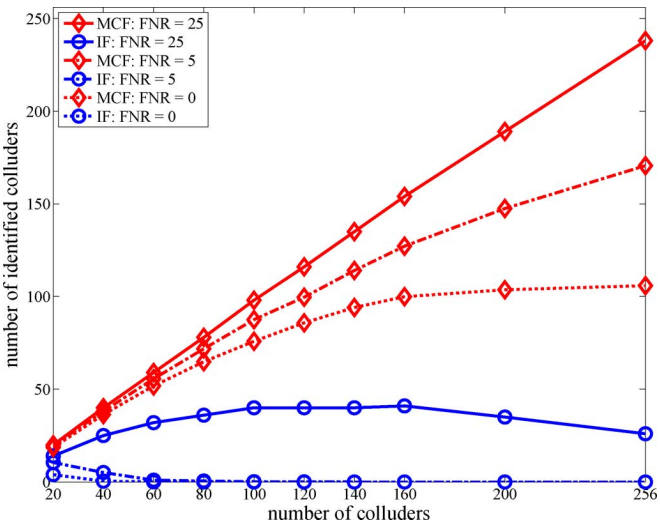

Fig. 17. Comparison of the colluder identification performance between the MC-CDMA-based and the independent fingerprinting schemes, which are labelled by MCF and IF, respectively, for three FNR values.

Example 9: Comparison With Independent Fingerprinting Under Noise: We compare the colluder identification performance of the proposed MC-CDMA-based and the independent fingerprinting [7], [49] schemes in Fig. 17 with three FNR values (i.e., 0, 5, and 25 dB). We see that the MC-CDMA-based fingerprinting outperforms the independent fingerprinting clearly with the same codeword length and power in all FNR values. To improve the colluder detection performance in the low FNR range, we may apply more robust estimation schemes such as the minimum mean square error estimator [29], [45], which will be explored in the future.

Example 10: Impact of Noise and Quantization: A 16-bit audio signal sampled at 44.1 KHz and a video signal with 256

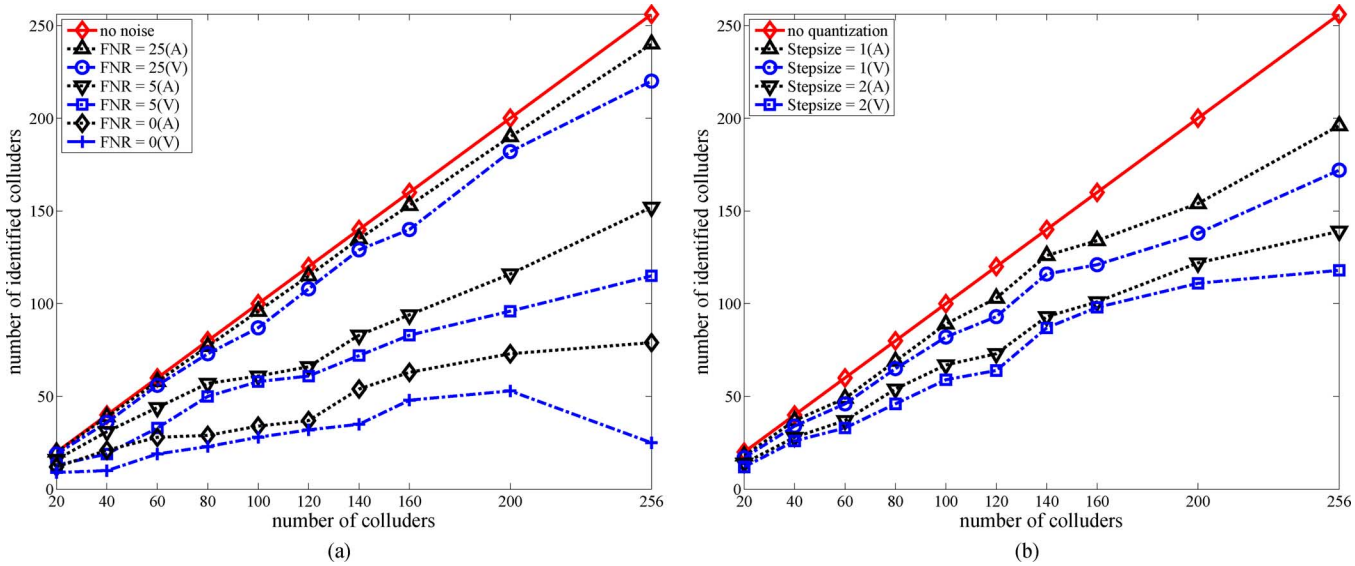

Fig. 18. Performance of the MC-CDMA-based fingerprinting system on audio (A) and video (V) data under the impact of (a) noise and (b) quantization.

gray levels of size 760×480 were used as the host signal. The embedded code strength $\alpha(i)$ was chosen according to the JND criterion as discussed in Section III. There was no bit shift in codeword generation. The frequency-domain (i.e., FFT domain or wavelet domain) code embedding was implemented.

Information loss could be resulted from additive noise and signal quantization and, consequently, the performance degrades. To see this, we compare the performance of the MC-CDMA-based fingerprinting system with three FNR values (i.e., 0, 5, and 25 dB) in Fig. 18(a) and with two quantization levels (i.e., step sizes 1 and 2) in Fig. 18(b). When there is no noise or quantization effect, the performance is the same as shown earlier. However, when there exists noise or quantization, the colluder detection performance degrades due to the impairment of user codes and pilot codes. Clearly, the performance is related to the power of embedded fingerprint codes. The higher the fingerprint power, the better the detection performance.

VIII. Summary of Main Concepts and Research Contributions

In this work, we have shown a strong analogy between MC-CDMA-based fingerprinting and MC-CDMA communication systems. Several main concepts are summarized in Table II. Concepts shared by both systems are given in the top half of the table. Some concepts unique to the fingerprinting system are presented in the bottom half of the table.

We have made the following contributions in this research.

- To the best of our knowledge, this is the first attempt to deal with time-varying collusion attacks, where the constant collusion attacks studied in the literature becomes a special case. The latter case can be easily solved with the proposed MC-CDMA-based fingerprint solution.
- We explain the different roles of user IDs, user messages, and user spreading codes in the fingerprint code generation in Section IV-B. In the proposed scheme, we adopt user message as well as spreading codes to form a unique user ID. In contrast, the SSM [7] only uses the spreading codes as the user ID. The proposed bit assignment framework can accommodate much more users for a fixed length of fingerprint codes.
- We present a new approach to design fingerprint codes based on the multicarrier construction [3], [4] and their detection via advanced detection techniques [6], [14].
- We introduce the concept of delayed embedding and relate it to multipath fading. As a result, the number of users can be greatly increased.
- Due to the strong analogy between MC-CDMA-based fingerprinting and MC-CDMA communication, many existing MC-CDMA communication techniques can be leveraged to solve the fingerprinting problem. For example, we can apply channel estimation techniques to collusion weight estimation and advanced symbol detection techniques to colluders' fingerprint detection.
- We propose a new performance metric in comparing the performance of various fingerprinting techniques and systems.

IX. Conclusion and Future Work

The MC-CDMA-based fingerprinting system was introduced to protect continuous media such as audio and video, and its colluder detection performance against time-varying colluder weights was studied. We formulated this problem as an MUD problem in a wireless communication system. We constructed embedding codes with code spreading followed by multicarrier modulation. The weights were estimated by inserting pilot signals in the embedded fingerprint. As to advanced message symbol detection, we replaced the traditional correlation-based detector with the MRC detector and the PIC multiuser detector. The superior performance of the proposed MC-CDMA-based fingerprinting system was demonstrated in the presence of time-varying collusion attacks. In the near future, it is worthwhile to investigate the impact of various parameters of the proposed fingerprinting scheme on the overall traitor-tracing performance

TABLE II
TERMS AND MEANINGS

Terms	Meanings
User messages	User messages (in bits) containing user IDs and error correction codes.
Spreading code	Orthogonal codes used to spread user messages.
Inter-group interference	Analogous to multi-access interference.
Colluder weight	Analogous to the impulse response of a wireless communication channel.
Colluder weight estimation	Analogous to pilot-based channel estimation.
Advanced colluder detection	Analogous to diversity schemes and multiuser detectors.
MC-CDMA ngerprint codes	Cascade of the FFT of spreading and pilot codes.
Circular shift	Used to increase the number of users.
User ID	A sequence of bits used to represent an user uniquely.
Group index	Users with the same spreading code having the same group index.
Subgroup index	Users in the same group with the same shift amount having the same subgroup index.
Colluder identi cation	Binary decision between the colluder and the innocent user sets.

and quality degradation of the colluded media. These parameters include the amount of redundant bits for user ID protection, the shift amount within one group, the length and energy of user IDs and pilot signals, etc.

REFERENCES

[1] G. B. Giannakis and E. Serpedin, "Linear multichannel blind equalizers of nonlinear FIR volterra channels," *IEEE Trans. Signal Process.*, vol. 45, no. 1, pp. 67–81, Jan. 1997.

[2] J. K. Tugnait, L. Tong, and Z. Ding, "Single-user channel estimation and equalization," *IEEE Signal Process. Mag.*, vol. 17, no. 3, pp. 16–28, May 2000.

[3] B.-H. Cha and C.-C. J. Kuo, "Design of collusion-free codes based on MAI-free principle," in *Proc. IEEE Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing*, Pasadena, CA, Dec. 2006, pp. 639–642.

[4] B.-H. Cha and C.-C. J. Kuo, "Design of collusion-free hiding codes using MAI-free principle," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, Honolulu, HI, Apr. 2007, pp. 145–148.

[5] B.-H. Cha and C.-C. J. Kuo, "Design of multiuser collusion-free hiding codes with delayed embedding," in *Proc. IEEE Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing*, Kaohsiung, Taiwan, Nov. 2007, pp. 379–382.

[6] B.-H. Cha and C.-C. J. Kuo, "Advanced colluder detection techniques for OSIFT-based hiding codes," in *Proc. IEEE Int. Symp. Circuits and Systems*, Seattle, WA, May 2008, pp. 2961–2964.

[7] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[8] Z. J. Wang, M. Wu, H. V. Zhao, and K. J. R. Liu, "Anti-collusion forensics of multimedia fingerprinting using orthogonal mudulation," *IEEE Trans. Image Process.*, vol. 14, no. 6, pp. 804–821, Jun. 2005.

[9] H. V. Zhao, M. Wu, Z. J. Wang, and K. J. R. Liu, "Forensic analysis of nonlinear collusion attacks for multimedia fingerpinting," *IEEE Trans. Image Process.*, vol. 14, no. 5, pp. 646–661, May 2005.

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

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

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

[13] S. He and M. Wu, "Joint coding and embedding techniques for multimedia fingerprinting," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 231–247, Jun. 2006.

[14] B.-H. Cha and C.-C. J. Kuo, "Design and analysis of high-capacity anticollusion hiding codes," *J. Circuits, Syst., Signal Process.*, vol. 27, pp. 195–211, Mar. 2008.

[15] S.-H. Tsai, Y.-P. Lin, and C.-C. J. Kuo, "MAI-free MC-CDMA systems based on Hadamard–Walsh codes," *IEEE Trans. Signal Process.*, vol. 54, no. 8, pp. 3166–3179, Aug. 2006.

[16] Y. Yacobi, "Improved Boneh–Shaw content fingerprinting," in *Proc. RSA Conf.*, San Francisco, CA, Apr. 2001.

[17] N. Kiyavash and P. Moulin, "A framework for optimizing nonlinear collusion attack on fingerprinting systems," in *Proc. Conf. Infromation Sciences and Systems*, Princeton, NJ, 2006.

[18] N. Kiyavash and P. Moulin, "On optimal collusion strategies for fingerprinting," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, Toulouse, France, May 2006, pp. 405–408.

[19] K. J. L. Ray, W. Trappe, Z. W. Jane, M. Wu, and H. Zhao, *Multimedia Fingerprinting Forensics for Traitor Tracing*. New York: Hindawi, 2005, EURASIP on Signal Processing and Communications.

[20] H. V. Zhao and K. J. R. Liu, "Tritor-within-traitor behavior forensics: Strategy and risk minimization," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 4, pp. 440–456, Dec. 2006.

[21] H. S. Stone, Analysis of Attacks on Image Watermarks With Randomized Coefficients NEC Res. Inst. Tech., Princeton, NJ, Tech. Rep. 96-045, 1996.

[22] P. A. Bello, "Characterization of randomly time-variant linear channels," *IEEE Trans. Commun.*, vol. 11, no. 4, pp. 360–393, Dec. 1963.

[23] B. Sklar, "Rayleigh fading channels in mobile digital communications systems part I: Characterization," *IEEE Commun. Mag.*, vol. 35, no. 7, pp. 90–100, Jul. 1997.

[24] D. N. C. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[25] N. Jayant, J. Johnston, and R. Safranek, "Signal compression based on models of human perception," *Proc. IEEE*, vol. 81, pp. 1385–1422, Oct. 1993.

[26] W. Liu, L. Dong, and W. Zeng, "Optimum detection for spread-spectrum watermarking that employs self-masking," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 645–654, Dec. 2007.

[27] Y.-W. Liu and J. O. Smith, "Audio watermarking through deterministic plus stochastic signal decomposition," *EURASIP J. Inf. Security*, vol. 2007, pp. 1–12, 2007.

[28] C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 525–539, May 1998.

[29] L. Hanzo, M. Munster, B. J. Choi, and T. Keller, *OFDM and MC-CDMA for Broadband Multi-User Communications, WLANs and Broadcasting*. West Sussex, U.K.: Wiley, 2004.

[30] H. V. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1994.

[31] S. Lin and D. J. Costello, *Error Control Coding*. Upper Saddle River, NJ: Prentice-Hall, 2004.

[32] J. G. Proakis, *Digital Communication*. New York: McGraw-Hill, 1995.

[33] B. Natarajan, C. R. Nassar, S. Shattil, M. Michelini, and Z. Wu, "High-performance MC-CDMA via carrier interferometry codes," *IEEE Trans. Veh. Technol.*, vol. 50, no. 6, pp. 1344–1353, Nov. 2001.
[34] M. K. Simon, J. K. Omura, R. A. Sholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*, Electronic ed. New York: McGraw-Hill, 2002.
[35] S. Hara and R. Prasad, "Overview of multicarrier CDMA," *IEEE Commun. Mag.*, vol. 35, no. 12, pp. 126–133, Dec. 1997.
[36] D. Kirovski and H. S. Malvar, "Spread-spectrum watermarking of audio signals," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 1020–1033, Apr. 2003.
[37] M. D. Swanson, B. Zhu, A. H. Tewfik, and L. Boney, "Robust audio watermarking using perceptual masking," *Signal Process.*, vol. 66, pp. 337–355, May 1998.
[38] H.-J. M. Wang, P.-C. Su, and C.-C. J. Kuo, "Wavelet-based digital image watermarking," *Opt. Express*, vol. 3, pp. 525–528, 1998.
[39] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 776–786, Aug. 2003.
[40] M. Morelli, C.-C. J. Kuo, and M.-O. Pun, "Synchronization techniques for orthogonal frequency division multiple access (OFDMA): A tutorial review," *Proc. IEEE*, vol. 95, no. 7, pp. 1394–1427, Jul. 2007.
[41] U. Tureli, D. Kivanc, and H. Liu, "Channel estimation for multicarrier CDMA," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, Istanbul, Turkey, Jun. 2000, pp. 2909–2912.
[42] Y. Li, "Pilot-symbol-aided channel estimation for OFDM in wireless systems," *IEEE Trans. Veh. Technol.*, vol. 49, no. 4, pp. 1207–1215, Jul. 2000.
[43] S. Caoleri, M. Ergen, and A. Bahai, "Channel estimation techniques based on pilot arrangements in OFDM systems," *IEEE Trans. Broadcasting*, vol. 48, no. 3, pp. 223–229, Sep. 2002.
[44] M.-O. Pun, M. Morelli, and C.-C. J. Kuo, "Maximum-likelihood synchronization and channel estimation for OFDMA uplink transmissions," *IEEE Trans. Commun.*, vol. 54, no. 4, pp. 726–736, Apr. 2006.
[45] M. Morelli and U. Mengali, "A comparison of pilot-aided channel estimation methods for OFDM systems," *IEEE Trans. Signal Process.*, vol. 49, no. 12, pp. 3065–3073, Dec. 2001.
[46] S. Verdu, *Multiuser Detection*. Cambridge, U.K.: Cambridge Univ. Press, 1998.
[47] D. Divsalar, M. K. Simon, and D. Raphaeli, "Improved parallel interference cancellation for CDMA," *IEEE Trans. Commun.*, vol. 46, no. 2, pp. 258–268, Feb. 1998.
[48] J. G. Andrews, "Interference cancellation for cellular systems: A contemporary overview," *IEEE Commun. Mag.*, vol. 12, no. 2, pp. 19–29, Apr. 2005.
[49] M. Wu, W. Trappe, Z. J. Wang, and K. J. R. Liu, "Collusion-resistant fingerprinting for multimedia," *IEEE Signal Process. Mag.*, vol. 21, no. 2, pp. 15–27, Mar. 2004.

Byung-Ho Cha (S'06) received the B.S. degree (*summa cum laude*) in Electronic Engineering from Sogang University, Seoul, South Korea, in 2004. He received the M.S. degree from Signal and Image Processing Institute, Ming Hsieh Department of Electrical Engineering, Viterbi School of Engineering, University of Southern California (USC), Los Angeles, in 2006. He is currently working toward the Ph.D. degree at USC.

He is a Research Assistant in the Media Communications Laboratory (MCL) at USC, advised by Prof. C.-C. Jay Kuo since 2005. He belongs to the Audio/Music Signal Processing (AMSP) subgroup in MCL. His research interests include multimedia security emphasis on watermarking, fingerprinting, steganography, and forensic analysis, multimedia communications, multimedia signal processing, multimedia quality assessment, wireless communication, and networking.

Mr. Cha received the Best Student Paper Award from the Eighth IEEE International Symposium on Multimedia, San Diego, CA, in 2006.

C.-C. Jay Kuo (S'83–M'86–SM'92–F'99) received the B.S. degree in electrical engineering from the National Taiwan University, Taipei, Taiwan, R.O.C., in 1980 and the M.S. and Ph.D. degrees in electrical engineering from the Massachusetts Institute of Technology, Cambridge, in 1985 and 1987, respectively.

He is the Director of the Signal and Image Processing Institute and a Professor of electrical engineering, computer science, and mathematics with the University of Southern California (USC), Los Angeles. He has guided about 94 students with their Ph.D. degrees and supervised 20 postdoctoral research fellows. His research group at USC currently consists of around 30 Ph.D. students. He is the coauthor of about 150 journal papers, 780 conference proceedings, and nine books. He has delivered more than 400 invited lectures at conferences, research institutes, universities, and companies. His research interests are in the areas of digital image/video analysis and modeling, multimedia data compression, communication and networking, and biological signal/image processing.

Dr. Kuo is a Fellow of The International Society for Optical Engineers and a member of Association for Computing Machinery. He was an IEEE Signal Processing Society Distinguished Lecturer in 2006. He is the Editor-in-Chief of the *Journal of Visual Communication and Image Representation* (an Elsevier journal) and has been the Editor for about ten international journals. He received the National Science Foundation Young Investigator Award and the Presidential Faculty Fellow Award in 1992 and 1993, respectively. He received the Northrop Junior Faculty Research Award from the USC Viterbi School of Engineering in 1994. He received the Best Paper Award from the Multimedia Communication Technical Committee of the IEEE Communication Society in 2005, the Best Student Paper Award from the IEEE Vehicular Technology Fall Conference in 2006, and the Best Paper Award from the IEEE Conference on Intelligent Information Hiding and Multimedia Signal Processing in 2006.