Performance Study on Multimedia Fingerprinting Employing Traceability Codes *

Shan He and Min Wu

University of Maryland, College Park, U.S.A.

Abstract. Digital fingerprinting is a tool to protect multimedia content from illegal redistribution by uniquely marking copies of the content distributed to each user. Collusion attack is a powerful attack whereby several differently-fingerprinted copies of the same content are combined together to attenuate or even remove the fingerprint. Coded fingerprinting is one major category of fingerprinting techniques against collusion. Many fingerprinting codes are proposed with tracing capability and collusion resistance, such as Traceability (TA) codes and Identifiable Parent Property (IPP) codes. Most of these works treat the important embedding issue in terms of a set of simplified and abstract assumptions, and they do not examine the end-to-end performance of the coded multimedia fingerprinting. In this paper we jointly consider the coding and embedding issues and examine the collusion resistance of coded fingerprinting systems with various code parameters. Our results show that TA codes generally offer better collusion resistance than IPP codes, and a TA code with a larger alphabet size and a longer code length is preferred.

1 Introduction

Technology advancement has made multimedia content widely available and easy to process. These benefits also bring ease to unauthorized users who can duplicate and manipulate multimedia content, and re-distribute it to a large audience. The protection of multimedia content becomes increasingly important. Digital fingerprinting is an emerging technology to protect multimedia content from unauthorized dissemination, whereby each user's copy is identified by a unique ID embedded in his/her copy and the ID, which we call *fingerprint*, can be extracted to help identify culprits when a suspicious copy is found. A powerful, cost-effective attack from a group of users is collusion attack, where the users combine their copies of the same content to generate a new version. If designed improperly, the fingerprints can be weakened or removed by the collusion attacks.

A growing number of techniques have been proposed in the literature to provide collusion resistance in multimedia fingerprinting systems. Many of them fall in one of the two categories, namely, the non-coded fingerprinting and the coded fingerprinting. The orthogonal fingerprinting is a typical example of non-coded

* This work was supported in part by the U.S. Office of Naval Research under Young Investigator Award N000140510634 and the U.S. National Science Foundation under CAREER Award CCR-0133704. The authors can be contacted via email at {shanhe, minwu}@eng.umd.edu.

fingerprinting. It assigns each user a spread spectrum sequence as the fingerprint and the sequences among users are mutually orthogonal. The collusion resistance of orthogonal fingerprinting has been well studied by Wang et al. [1] and Ergun et al. [2]. Coded fingerprinting employs an explicit coding step to build the fingerprint sequences. One of the earliest works is by Boneh and Shaw [3], where a two-level code construction known as a c-secure code was proposed to resist up to c colluders with a high probability. This binary code was later used to modulate a direct spread spectrum sequence to embed the fingerprints in multimedia signals [4]. Following Boneh and Shaw's framework, many recent works consider the construction of fingerprinting codes for generic data that have tracing capability and are able to resist collusion. We collectively call these codes traceability codes, which include Identifiable Parent Property (IPP) codes and Traceability (TA) codes[1] [5]- [9]. In [10] and [11], TA codes are applied to multimedia fingerprinting and extended to deal with symbol erasures contributed by noise or cropping in multimedia signal domain. Fernandez and Soriano [12] employ TA codes constructed through algebraic-geometry codes for fingerprinting multimedia content. They define identifiable colluders and propose to employ the Guruswami-Sudan soft-decision list decoding algorithm for algebraic-geometry codes to find such users. Existing coded fingerprinting mainly focuses on the code layer and treat the embedding issues through an abstract model known as the *marking assumption* [3] [10]. It typically assumes that colluders can only change fingerprint symbols where they have different values, and the colluders assemble pieces of their codes to generate a colluded version. Although the marking assumption may work well with generic data, it alone is not always appropriate to model multimedia fingerprinting. Both coding and embedding issues need to be considered in multimedia fingerprinting. A recent work by Trappe et al. [13] has shown very promising results by this joint consideration. In their work, a code based on combinatorial design was proposed, and each code bit is embedded in an overlapped fashion by modulating a spreading sequence that covers the entire multimedia signal. The overlap spreading confines the types of manipulation from colluders, and colluders can be identified through the code bits shared by them.

In our recent work on coded fingerprinting [14] [15] [16], we jointly consider coding and embedding and have found that coded fingerprinting allows for a much more efficient detection than non-coded orthogonal fingerprinting [1], but it has rather limited collusion resistance. Based on this joint consideration, we propose a *Permuted Subsegment Embedding (PSE)* technique [16] which substantially improves the collusion resistance of coded fingerprinting. With this improvement, coded fingerprinting has a better trade-off between collusion resistance and detection efficiency than the non-coded fingerprinting. One question

[1] The term "traceability codes", in a broad sense, refers to the collection of fingerprinting codes with tracing capability, and in a narrow sense, refers to a specific type of traceability codes that will be discussed later. To avoid confusion, in this paper, we will use "TA codes" to represent the narrow-sense traceability codes.

that remains to be answered is the effect of the code parameters on the performance of the fingerprinting systems.

In this paper, building upon a cross-layer framework and employing our previously proposed PSE technique, we examine the effect of different codes on the collusion resistance of coded multimedia fingerprinting. The paper is organized as follows. Section 2 provides a general background on coded fingerprinting and reviews fingerprinting codes with emphasis on IPP code and TA code. We examine the collusion resistance of multimedia fingerprinting based on IPP codes and TA codes through analysis and simulations in Section 3. Finally the conclusions are drawn in Section 4.

2 Background on Coded Fingerprinting for Multimedia

2.1 System Framework

A typical framework for coded multimedia fingerprinting includes a code layer and a spread spectrum based embedding layer [14]. For anti-collusion purposes, the fingerprint code is constructed such that a colluded codeword by a coalition of c colluders can be traced back to one of the colluders. Each codeword is then assigned to one user as the fingerprint. To embed a codeword, we first partition the host signal into L non-overlapped segments with one segment corresponding to one symbol. Then we build q mutually orthogonal spread spectrum sequences $\{\mathbf{w}_j, j = 1, 2, ..., q\}$ with identical energy $||\mathbf{w}||^2$ to represent the q possible symbol values in the alphabet. Each user's fingerprint sequence is constructed by concatenating the spreading sequences corresponding to the symbols in his/her codeword. Before the embedding of the spreading sequence, we employ the *Permuted Subsegment Embedding (PSE)* technique proposed in our recent work [16] to get better collusion resistance. In PSE, each segment of the fingerprint sequence is partitioned into β subsegments and these subsegments are then randomly permuted according to a secret key. The permuted fingerprint sequence is added to the host signal with perceptual scaling to form the final fingerprinted signal.

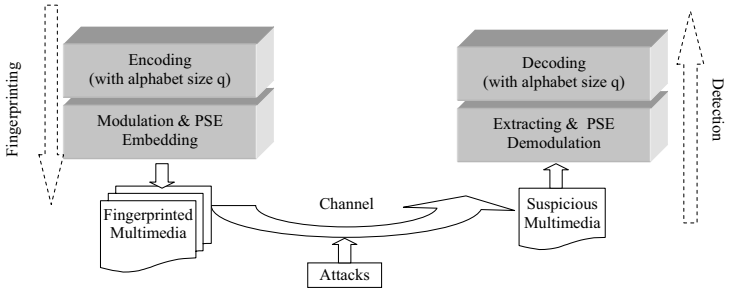

Fig. 1. Framework of traceability code based fingerprinting scheme

After the distribution of the fingerprinted copies, users may collaborate and mount cost-effective collusion attacks. The existing works on coded fingerprinting have primarily targeted code-level collusion resistance. The widely considered collusion model is the *interleaving collusion*, whereby each colluder contributes a non-overlapped set of segments (corresponding to symbols) and these segments are assembled to form a colluded copy. Additional distortion may be added to the multimedia signal during the collusion, which we model as additive noise. Since few colluders would be willing to take higher risk than others, they generally would make contributions of an approximately equal amount in the collusion. Another major type of collusion is done in the signal domain. A typical example is the *averaging collusion* [1], whereby colluders average the corresponding components in their copies to generate a colluded version. The averaging collusion can be modelled as follows:

$$\mathbf{z} = \frac{1}{c} \sum_{j \in S_c} \mathbf{s_j} + \mathbf{x} + \mathbf{d}, \tag{1}$$

where $\mathbf{z}$ is the colluded signal, $\mathbf{x}$ is the host signal, $\mathbf{d}$ is the noise term, $\mathbf{s}_j$ represents the fingerprint sequence for user j, S_c is the colluder set, and c is the number of colluders. For simplicity in analysis, we assume that the additional noise under both collusions follows *i.i.d.* Gaussian distribution.

At the detector side, our goal is to catch one colluder with a high probability. We first extract the fingerprint sequence and inversely permute it according to the secret key used in the PSE. We then determine the symbol that is most likely to be present in each multimedia segment using a correlation detector commonly used for spread spectrum embedding [17]. We search the codebook and identify the colluder to be the one whose codeword has the smallest Hamming distance to the extracted codeword. Alternatively, after the inverse permutation of the fingerprint sequence, we can employ a correlation detector to correlate the entire test signal directly with every user's fingerprint signal $\mathbf{s}_j$. In this case, the decision is based on the overall correlation and no intermediate hard decision needs to be made at the symbol level. The user whose fingerprint has the highest correlation with the test signal is identified as the colluder, i.e. $\hat{j} = arg\max_{j=1,2,...,N_u} T_N(j)$. Here, the detection statistic $T_N(j)$ is defined as:

$$T_N(j) = \frac{(\mathbf{z} - \mathbf{x})^T \mathbf{s}_j}{\sqrt{\|\mathbf{s}\|^2}} \quad j = 1, 2, ..., N_u, \tag{2}$$

where $\mathbf{z}$ is the colluded signal, $\mathbf{x}$ is the original signal which is often available in fingerprinting applications, and $\|\mathbf{s}\| = \|\mathbf{s}_j\|$ for all j based on the equal energy construction. Compared with the former 2-step hard-decision scheme, the latter scheme takes advantage of the soft information on the symbol level and provides a better performance.

2.2 Fingerprinting Codes

At the code layer, a code with tracing capability is employed for the purpose of collusion resistance. In the literatures of fingerprint code design, codes such as

Identifiable Parent Property(IPP) codes and Traceability(TA) codes are widely studied [5]- [9]. We briefly review these two kinds of codes in the following.

***c*-TA Code** A c-TA code satisfies the condition that any colluded codeword by any c (or fewer) colluders has a smaller distance to at least one of these colluders' codewords than to the innocent users' [5]. We can construct a c-TA code using an established Error Correcting Code (ECC), provided that the minimum distance D is large enough and satisfies [5]

$$D > \left(1 - \frac{1}{c^2}\right) L. \tag{3}$$

Here L is the code length and c is the number of colluders that the code is intended to resist. With the minimum distance achieving the Singleton bound, a Reed-Solomon code is a natural choice for constructing a c-TA code. Then, the number of c-TA codewords over an alphabet of size q constructed through a Reed-Solomon code is $N_u = q^k$, where $k = \lceil L/c^2 \rceil$.

***c*-IPP Code** A c-IPP code satisfies the condition that any colluded codeword by a coalition of size at most c can be traced back to at least one member of the coalition [5]. A c-TA code is a c-IPP code, but a c-IPP code is not necessarily a c-TA code. Therefore, the set of c-TA codes is a subset of c-IPP codes. In terms of the traceability, the c-TA codes are stronger than those c-IPP codes that are not c-TA codes, which we call proper c-IPP codes. Van Trung et al. propose a method that can be used to construct a proper c-IPP code as follows [9]:

> Let A be an (L_2, N_2, q_2) c-IPP code with code length L_2, codeword number N_2 and alphabet size q_2. Let B be an (L_1, q_2, q_1) c-IPP code with code length L_1, codeword number q_2 and alphabet size q_1. Then the concatenated code C of A and B is an (L_1L_2, N_2, q_1) c-IPP code with code length L_1L_2, codeword number N_2 and alphabet size q_1.

The concatenation of code A and code B is done by replacing each symbol in the alphabet of code A by a codeword in code B. Since a c-TA code is also a c-IPP code, the construction of a proper c-IPP code can be done by concatenating two c-TA codes.

In this paper, we are interested in the comparison of c-TA codes with proper c-IPP codes. From this point on, for the sake of brevity we use the term c-IPP codes to refer to proper c-IPP codes.

3 Performance Evaluation

In this section, we compare the collusion resistance of fingerprinting systems employing different codes. We try to answer the questions: what kind of code is better for collusion resistance and what parameter settings of the codes are favorable for building the fingerprint sequences? We provide analysis on the relationship between collusion resistance and code parameters. Simulations are then used to validate the analysis and conjectures.

3.1 Analysis of Collusion Resistance

We measure the collusion resistance of a fingerprinting system in terms of the probability of catching one colluder, denoted as P_d. To get the analytic approximation, first consider an ideal fingerprinting system whose fingerprint sequences have a constant pairwise correlation denoted as ρ. Without loss of generality, we assume that the first c users perform averaging collusion. (Notice that with the PSE technique, the interleaving collusion has similar effect to the averaging collusion. [16]) The vector of detection statistics T_N's defined in (2) follows a N_u-dimensional Gaussian distribution:

$$\mathbf{T} = [T_N(1), ..., T_N(N_u)]^T \sim N([\mathbf{m}_1, \mathbf{m}_2]^T, \sigma_d^2 \Sigma) \tag{4}$$
$$\text{with} \quad \mathbf{m}_1 = \|\mathbf{s}\| \left(\frac{1}{c} + \left(1 - \frac{1}{c} \right) \rho \right) \mathbf{1}_c, \quad \mathbf{m}_2 = \|\mathbf{s}\| \rho \mathbf{1}_{n-c},$$

where $\mathbf{1}_k$ is an all one vector with dimension k-by-1, and Σ is an n-by-n matrix whose diagonal elements are 1's and off-diagonal elements are ρ's, σ_d^2 is the variance of the noise, $\mathbf{m}_1$ is the mean vector for colluders, and $\mathbf{m}_2$ is the mean vector for innocent users. Given the same colluder number c and fingerprint strength $\|\mathbf{s}\|$, the mean correlation values with colluders and with innocents are separated more widely for a smaller ρ. This suggests that in the absence of any prior knowledge on collusion patterns, a smaller ρ leads to a higher colluder detection probability P_d. Therefore, we prefer fingerprint sequences with a small pairwise correlation ρ in the system design.

For the coded fingerprinting, the pairwise correlation can be calculated by examining the code construction. Codes with a larger minimum distance have a smaller upper bound on the correlation and thus are preferable. This is consistent with the principle indicated in (3) to employ codes with large minimum distance. Under the code construction with large minimum distance, the largest pairwise correlation between the fingerprinting sequences ρ_0 will be close to 0 and we can use the above equal pairwise correlation model with $\rho = \rho_0$ to approximate the performance of the coded fingerprinting under averaging collusion.

Taking a Reed-Solomon code based fingerprinting as an example, we calculate its pairwise correlation. We denote the alphabet size as q, dimension k, and code length L. The total number of codewords is $N_u = q^k$ and the minimum distance is $D = L - k + 1$. We use $\mathbf{s}_i$ and $\mathbf{s}_j$ to represent the fingerprint sequences for user i and user j, respectively, and $\mathbf{w}_{im}$ as the orthogonal sequence representing the symbol in user i's codeword at position m with $\|\mathbf{w}_{im}\| = \|\mathbf{w}\|$. The normalized correlation between $\mathbf{s}_i$ and $\mathbf{s}_j$ is

$$\begin{aligned} \frac{< \mathbf{s}_i, \mathbf{s}_j >}{\|\mathbf{s}\|^2} &= \frac{< [\mathbf{w}_{i1}\mathbf{w}_{i2}\cdots\mathbf{w}_{iL}], [\mathbf{w}_{j1}\mathbf{w}_{j2}\cdots\mathbf{w}_{jL}] >}{L\|\mathbf{w}\|^2} \\ &= \frac{\sum_{m=1}^{L} \mathbf{w}_{im}\mathbf{w}_{jm}^T}{L\|\mathbf{w}\|^2} \leq \frac{L-D}{L} = \frac{k-1}{L} \triangleq \rho_0. \end{aligned} \tag{5}$$

We can choose k and L to make ρ_0 close to 0 to achieve better collusion resistance.

3.2 Comparisons on Collusion Resistance

***c*-IPP codes versus *c*-TA codes** Inequality (3) shows the sufficient condition for a code to be a c-TA code, and it does not hold for a c-IPP code. Rewriting inequality (3) as

$$\frac{L-D}{L} < \frac{1}{c^2},$$

and combining it with Eqn.(5), we can see that a c-TA code has pairwise correlation $\rho_0 < 1/c^2$, while c-IPP code has pairwise correlation $\rho_0 > 1/c^2$. According to the analysis in Section 3.1, the fingerprinting system constructed on c-TA code should have better performance than the fingerprinting system employing c-IPP code.

To validate the analysis, we examine the performance of a c-IPP code based fingerprinting system and a c-TA code based fingerprinting system through simulation. For a host signal with length $N = 40,000$, we design two systems that are capable of holding $N_u = 256$ users as follows:

- System 1 is built upon a 2-IPP code (40,256,4) with code length L=40, codeword number $N_u = 256$ and alphabet size q=4. This 2-IPP code is constructed through the concatenation of two 2-TA Reed-Solomon codes (8,256,16) and (5,16,4) following the method proposed in [9]. The pairwise correlation of the fingerprint sequences ρ_0 is 0.3 according to Eqn. (5).
- System 2 is built upon a 2-TA Reed-Solomon code (8,256,16) with code length L=8, codeword number $N_u = 256$ and alphabet size q=16. The pairwise correlation ρ_0 is 0.14.

In both systems, we employ our previously proposed PSE technique and choose the same subsegment size 200 for permutation. We examine the probability of catching one colluder P_d of both systems against interleaving collusion and averaging collusion with colluder number c ranging from 2 to 30 and Watermark-to-Noise-Ratio(WNR) ranging from -20dB to 0dB. The simulation results are shown in Fig. 2. For ease of comparison, we show the case of WNR=$-$12dB in Fig. 2(e) and (f). From the results, we can see that under averaging collusion (Fig. 2(b), (d) and (f)) 2-TA code based System 1 has 8% gain in the probability of detection P_d. Under interleaving collusion (Fig. 2(a), (c) and (e)), the performance gain can be up to 30%. The results are consistent with our analysis that due to the low pairwise correlation among the fingerprint sequences, 2-TA code based system outperforms 2-IPP code based system in all the cases we examined.

***c*-TA codes with different parameters** From the above comparison results, we can see that the fingerprint sequences constructed based on a c-TA code have lower correlation than the sequences constructed based on a c-IPP code. This low correlation helps defending against collusion attacks. A TA code is thus preferred in designing the fingerprint sequences. A natural question is, that given a host signal and the number of users the system needs to hold, how should we choose the parameters of TA codes to achieve good collusion resistance.

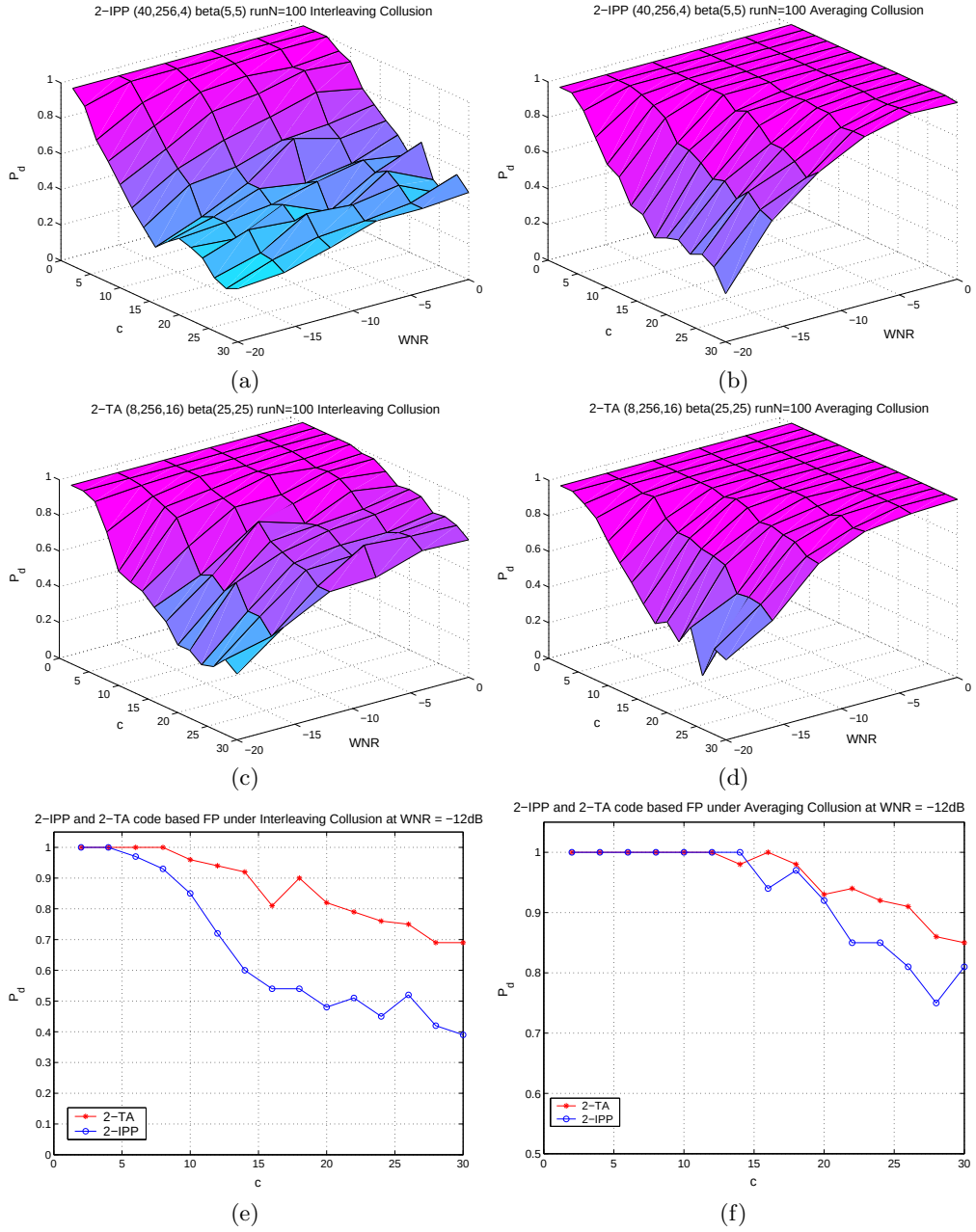

Fig. 2. Simulation results for IPP codes and TA codes based fingerprinting systems: the performance of 2-IPP code based system under (a) interleaving collusion and (b) averaging collusion; the performance of 2-TA code based system under (c) interleaving collusion and (d) averaging collusion. The performance of both systems under (e) interleaving collusion and (f) averaging collusion with WNR=−12dB.

In the following, we consider TA codes constructed on Reed-Solomon codes over alphabet size of q with dimension k. Examining Eqn. (5) we find that in order to get a small ρ_0, we can decrease k and increase L. In order to meet the desired number of users N_u and reduce the dimension k, larger q is preferred. Moreover, for Reed-Solomon code (including extended Reed-Solomon code), $L \leq q+1$. In order to get larger L, a larger q is also preferred. Therefore, our conjecture is that the fingerprinting system constructed on a TA code with a larger alphabet size q and a longer code length L should have better collusion resistance.

To validate our analysis, we examine the collusion resistance of the systems with various parameters through simulations. We construct three fingerprinting systems as follows:

- System 3 is built upon a TA code (15, 4096, 16) with code length $L = 15$, codeword number $N_u = 4096$ and alphabet size $q = 16$. According to Eqn. (5), the pairwise correlation ρ_0 is 0.13.
- System 4 is built upon a TA code (14, 4096, 64) with code length L =14, codeword number N_u=4096 and alphabet size q =64. The pairwise correlation ρ_0 is 0.07.
- System 5 is built upon a TA code (62, 4096, 64) with code length L =62, codeword number N_u=4096 and alphabet size q =64. The pairwise correlation ρ_0 is 0.016.

System 3 and System 4 have approximately the same code length but different alphabet size. System 4 and System 5 have the same alphabet size but different code lengths. All the systems are designed to protect a host signal with length $N = 15,000$ and to accommodate $N_u = 4096$ users. We employ the PSE technique for the fingerprint embedding, and a subsegment size of 50 is chosen for the permutation. We examine the probability of catching one colluder P_d of all three systems against interleaving collusion and averaging collusion, with colluder number c ranging from 2 to 20 and WNR ranging from -20dB to 0dB. We show the simulation results in Fig. 3, where the results for WNR = 0dB and -8dB cases are shown separately in Fig. 4 for better illustration. Comparing System 3 and System 4, we observe that under averaging collusion (Fig. 4(b) and (d)) System 4 with a larger alphabet size has 8% gain in the probability of detection P_d. The performance gain under interleaving collusion (Fig. 4(a) and (c)) can be as high as 40%. The comparison of System 3 and System 4 shows that with the same code length and the same subsegment permutation, the system with a larger alphabet size has better performance. Comparing System 4 and System 5, we can see that under both averaging and interleaving collusions, System 5 has about a 5% performance gain due to a longer code length. This small performance gain is because in this particular experimental settings, the pairwise correlations of both System 4 and 5 are very small and close to 0. There is little room for the improvement brought about by the smaller pairwise correlation of System 5. The simulation results of all three systems are consistent with our analysis in Section 3.1 in that TA codes with larger alphabet size q and longer code length L result in fingerprint sequences with smaller pairwise correlation, and thus better collusion resistance.

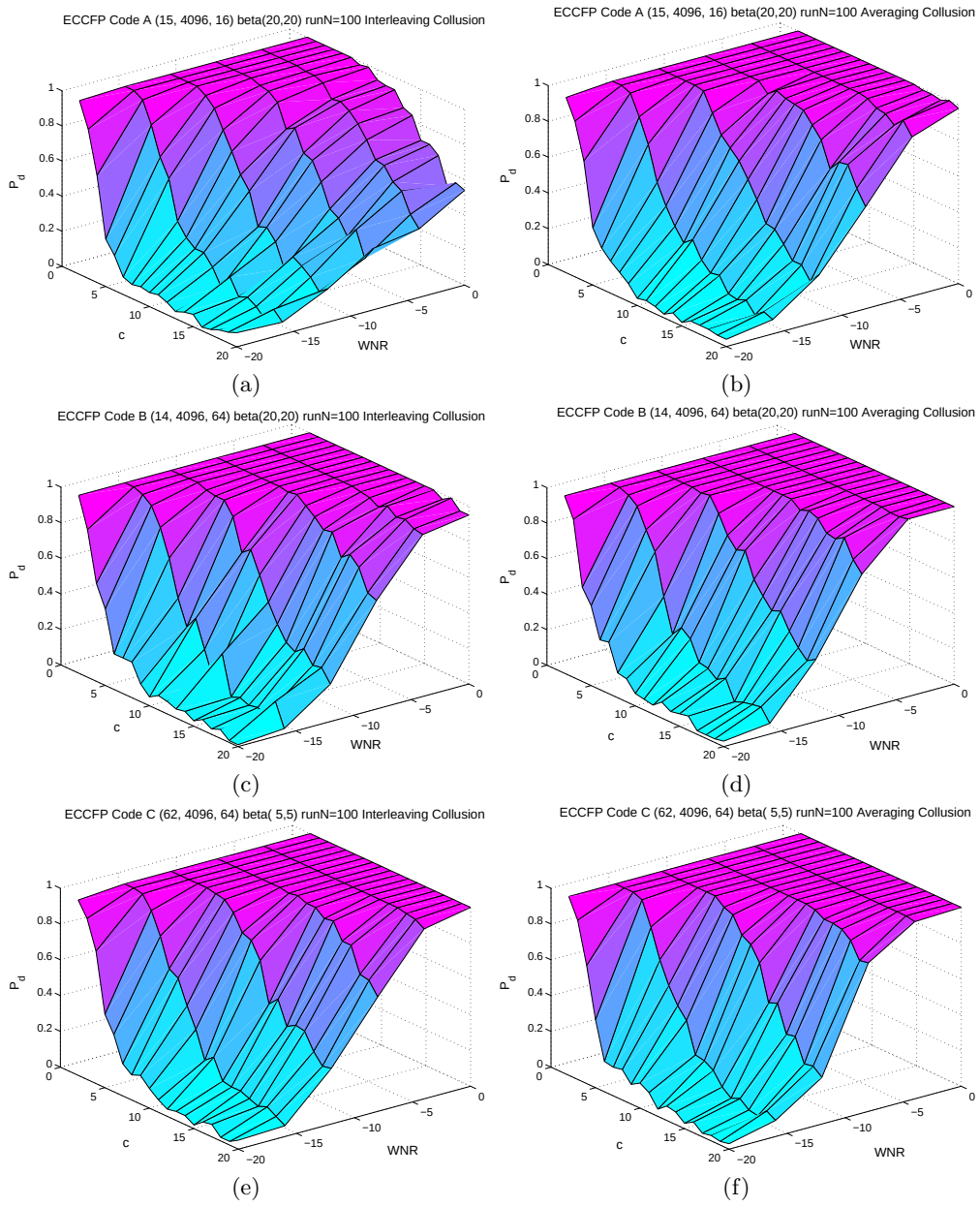

Fig. 3. Simulation results for systems with different code parameters under collusion attacks: System 3 under (a) Interleaving Collusion and (b) Averaging Collusion; System 4 under (c) Interleaving Collusion and (d) Averaging Collusion; System 5 under (e) Interleaving Collusion and (f) Averaging Collusion.

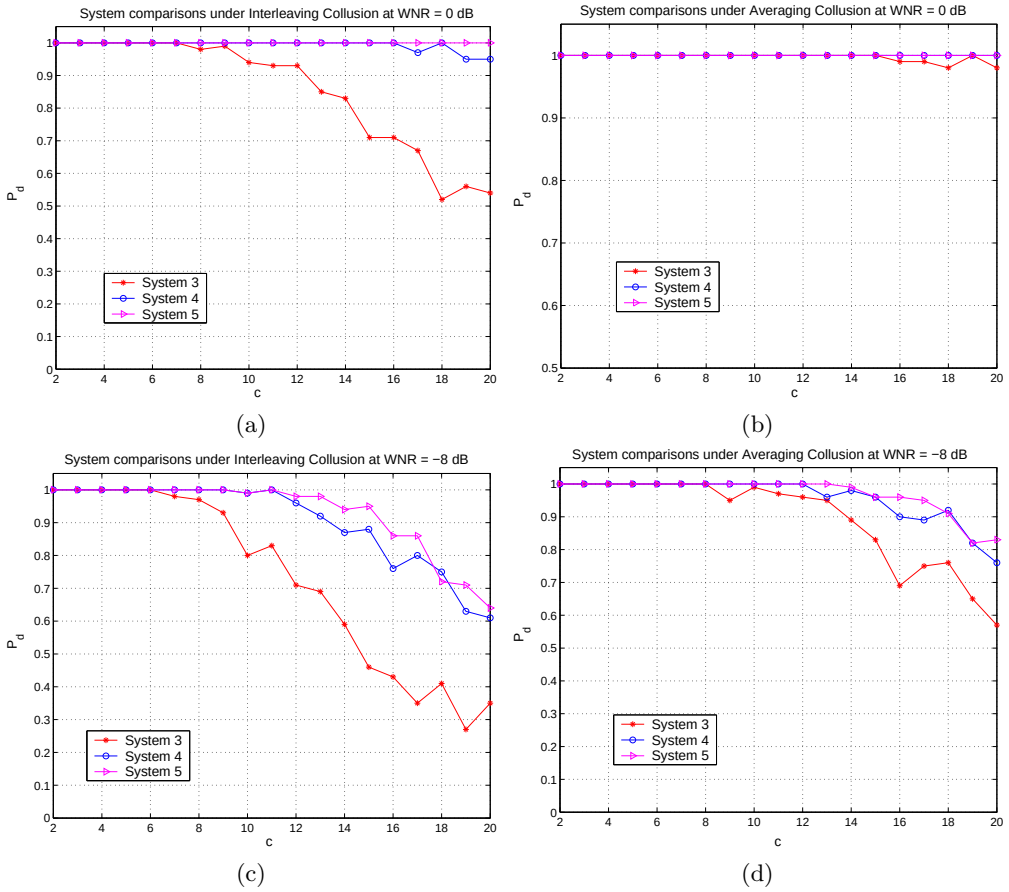

Fig. 4. Simulation results for systems with different code parameters under interleaving and averaging collusion at WNR = 0dB and -8dB. (a) Interleaving Collusion with WNR = 0dB; (b) Averaging Collusion with WNR = 0dB; (c) Interleaving Collusion with WNR = -8dB and (d) Averaging Collusion with WNR = -8dB

3.3 Discussions

The above results show that larger q and L values are preferred in code construction. However, q and L cannot be chosen arbitrarily. There are several constraints on them depending on the code constructions. Specifically, for the Reed-Solomon code construction, we have following constraints:

$$\text{System requirement on the total user number:} \quad q = \sqrt[k]{N_u}; \tag{6}$$

$$\text{Reed-Solomon code construction constraint:} \quad L \leq q + 1; \tag{7}$$

$$\text{Orthogonality of the FP sequences for each segment:} \quad q \leq \frac{N}{L}. \tag{8}$$

where N is the host signal length, N_u is the total number of users, q is the alphabet size and L is the code length. Taking L as the maximum value $q + 1$, we get from (8) that

$$q(q + 1) \leq N; \tag{9}$$

which means the upper bound of q value is roughly on the order of $\sqrt{N}$. Usually, in multimedia fingerprinting the host signal length $N >> N_u$ and $k \geq 2$ for Reed-Solomon codes. Therefore, Eqn. (6) is a more stringent requirement on q. In Eqn. (6), the dimension k can be used to achieve the desired trade-off between the collusion resistance and the computational complexity in detection which is $O(qN)$ according to our previous study [16]. Notice that the extreme case of $k = 1$ reduces to orthogonal fingerprinting which has better collusion resistance but high computational complexity in detection [16].

Other c-TA code constructions can be analyzed in a similar way. It is worth mentioning that the TA code proposed in [8] can be regarded as a TA code with dimension k lying between 1 and 2, which offers a fine adjustment on the trade-off between the collusion resistance and detection efficiency.

4 Conclusions

In this paper, we examine the collusion resistance of the coded fingerprinting through jointly considering fingerprint encoding, embedding, and detection. The results show that for a given host signal the pairwise correlation among fingerprint sequences is a key indicator of the collusion resistance, the lower the correlation the higher the collusion resistance. According to this principle, c-TA codes can be used to introduce a lower correlation among fingerprint sequences and thus is preferred over c-IPP codes in fingerprint design. Furthermore, a TA code with a larger alphabet size and a longer code length can provide better collusion resistance. The fingerprinting code construction provides a systematic way to introduce the correlation and to achieve a desired trade-off between the collusion resistance and detection efficiency.

References

1. Z.J. Wang, M. Wu, H. Zhao, W. Trappe, and K.J.R. Liu, "Resistance of Orthogonal Gaussian Fingerprints to Collusion Attacks," *Proc. of ICASSP*, pp. 724-727, Apr. 2003.
2. F.Ergun, J.Kilian and R.Kumar, "A Note on the limits of Collusion-Resistant Watermarks", *Eurocrypt '99*, 1999.
3. D. Boneh and J. Shaw, "Collusion-secure Fingerprinting for Digital Data," *IEEE Tran. on Info. Theory*, 44(5), pp. 1897-1905, 1998.
4. Y. Yacobi, "Improved Boneh-Shaw Content Fingerprinting", *CT-RSA 2001, LNCS 2020*, pp. 378-391, 2001.
5. J.N. Staddon, D. R. Stinson, and R. Wei, "Combinatorial Properties of Frameproof and Traceability Codes", *IEEE Trans. on Information Theory*, vol. 47, no. 3, pp 1042-1049, March 2001.
6. D. To, R. Safavi-Naini and Y. Wang, "A 2-secure code with efficient tracing algorithm", *Progress in Cryptology - INDOCRYPT'02, Lecture Notes in Computer Science*, Vol. 2551, Springer-Verlag, pp. 149-162, 2002.
7. A. Barg, G.R. Blakley and G. Kabatiansky "Digital fingerprinting codes: Problem statements, constructions, identification of traitors" *IEEE Trans. Information Theory*, 49(4), pp. 852-865, April 2003.
8. T. van Trung and S. Martirosyan, "On a Class of Traceability Codes", *Designs, Codes and Cryptography*, 2004.
9. T. van Trung and S. Martirosyan, "New Constructions for IPP Codes", *IEEE International Symposium on Information Theory*, 2003.
10. R. Safavi-Naini and Y. Wang, "Collusion Secure q-ary Fingerprinting for Perceptual Content," *Security and Privacy in Digital Rights Management (SPDRM'01)*, pp. 57-75, 2002.
11. R. Safavi-Naini and Y. Wang, "Traitor Tracing for Shortened and Corrupted Fingerprints" *Proc. of Digital Right Management (DRM'02)*, pp. 81-100, 2003.
12. M. Fernandez, and M. Soriano, "Soft-Decision Tracing in Fingerprinted Multimedia Content", *IEEE Multimedia*, Vol.11 No.2, pp38-46, April-June 2004.
13. W. Trappe, M. Wu, Z.J. Wang, and K.J.R. Liu, "Anti-collusion Fingerprinting for Multimedia", *IEEE Trans. on Sig. Proc.*, 51(4), pp. 1069-1087, 2003.
14. S. He and M. Wu, "Performance Study of ECC-based Collusion-resistant Multimedia Fingerprinting," in *Proceedings of the 38th CISS*, pp. 827-832, March 2004.
15. S. He and M. Wu, "Group-Oriented Joint Coding and Embedding Technique for Multimedia Fingerprinting," SPIE Conference on Security, Watermarking and Stegonography, pp.96-105, January 2005.
16. S. He and M. Wu, "Improving Collusion Resistance of Error Correcting Code Based Multimedia Fingerprinting," in *Proceedings of ICASSP 2005*, pp. 1029-1032, March 2005.
17. I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Trans. on Image Processing*, 6(12), pp.1673-1687, 1997.