IMPROVING COLLUSION RESISTANCE OF ERROR CORRECTING CODE BASED MULTIMEDIA FINGERPRINTING

Shan He and Min Wu

Electrical & Computer Engineering Department, University of Maryland, College Park

ABSTRACT

Digital fingerprinting protects multimedia content from illegal redistribution by uniquely marking copies of the content distributed to each user. Collusion is a powerful attack whereby several differently fingerprinted copies of the same content are combined together to attenuate or remove the fingerprints. Focusing on the error correction code (ECC) based fingerprinting, we explore in this paper new avenues that can substantially improve its collusion resistance, and in the mean time retain its advantages in detection complexity and fast distribution. Our analysis suggests a great need of jointly considering the coding, embedding, and detection issues, and inspires the proposed technique of permuted subsegment embedding that is able to substantially improve the collusion resistance of ECC based fingerprinting.

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. 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 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, 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 uncoded fingerprinting and the coded fingerprinting. The orthogonal fingerprinting is a typical example of uncoded fingerprinting. It assigns each user a spread spectrum sequence as the fingerprint and the sequences among users are mutually orthogonal [1][2]. An early work on coded fingerprinting focused on generic data and introduced a two-level construction in code domain to resist up to c colluders with high probability [3]. This binary code was later used to modulate a direct spread spectrum sequence to embed the fingerprints in multimedia signals [4]. A q-ary ECC code resisting c colluders, constructed as the c-traceability code or c-TA code in short, was employed and extended to deal with symbol erasures contributed by noise or cropping in multimedia signal domain [5]. A recent code based on combinatorial design was proposed in [6], where 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.

Multimedia data such as audio and video often consist of a sequence of naturally divided frames. Among the fingerprinting constructions reviewed above, the ECC-based fingerprinting provides an inherent support of the frame structure. Owing to a relatively small alphabet size q compared to the number of users N_u as well as one symbol being put in one non-overlapping media *segment* (which can be one frame or a group of frames), the ECC-based fingerprinting has the potential to generate and distribute fingerprinted media in an efficient way. For example, for each frame, a total of q copies carrying q different symbol values can be generated beforehand; a fingerprinted copy for any user can then be quickly obtained by assembling appropriate copies of the frames together according to the fingerprint code assigned to him/her. The small alphabet size also keeps the computational complexity of fingerprint detection lower than the orthogonal fingerprinting approach [7]. Despite all these attractive advantages, ECC-based fingerprinting has rather limited collusion resistance, which is about one magnitude lower than that of the orthogonal fingerprinting in the settings examined in our recent work [7]. The small alphabet size serves as a double-edge sword here as it substantially reduces the degrees of freedom in constructing fingerprint signals.

The focus of this paper is to explore avenues that can both retain the advantages provided by the ECC-based fingerprinting and improve the collusion resistance. We have observed that the existing ECC fingerprinting works put most of the attention on the code layer and few work has considered the interaction between coding and embedding. In the mean time, joint consideration of coding and embedding has shown promising results recently in [6] for non-segment based fingerprinting. This motivates us to examine the interplay between the ECC code layer and the embedding layer. As we shall see, by employing a strategic embedding mechanism referred to as the *permuted subsegment embedding* for putting the ECC fingerprint code into host media, we can benefit from the joint consideration of coding and embedding for ECC-based fingerprinting and substantially improve its collusion resistance.

2. ECC BASED FINGERPRINTING SYSTEMS

A typical framework of ECC based multimedia fingerprinting [7] includes an ECC based code layer and a spread spectrum based embedding layer. An ECC codeword is assigned to represent each user, and embedded into the multimedia document with one symbol per segment. After the distribution of the fingerprinted copies, users may collaborate and mount cost-effective collusion attacks. In this paper we focus on two types of collusions. One is the *interleaving collusion*, whereby each colluder contributes a non-overlapped set of segments and these segments are assembled to

Contact information: {shanhe, minwu}@eng.umd.edu

0-7803-8874-7/05/$20.00 ©2005 IEEE

form a colluded copy. The other type is the *averaging collusion*, whereby colluders average the corresponding components in their copies to generate a colluded version. Additional distortion may be added to the multimedia signal, which is typically modelled as an additive noise [6].

The existing works on ECC fingerprinting have primarily targeted at code-level collusion, which is equivalent to segment-by-segment interleaving. We take the c-TA code [5] as an example. A c-TA code satisfies the condition that any colluded version of the codewords by any c colluders have closer distance to at least one of these colluders' codewords than to the innocents'. We can construct a c-TA code using established ECC over an alphabet of size q, provided the minimum distance D is large enough and satisfies

$$D > (1 - \frac{1}{c^2})L, \qquad (1)$$

where L is the code length and c is the number of colluders that the code is intended to resist under interleaving collusion [5]. With the minimum distance achieving the Singleton bound, Reed-Solomon code is a natural choice in ECC based fingerprinting. The number of c-TA codewords over an alphabet of size q using Reed-Solomon code is $N_u = q^t$, where $t = \lceil L/c^2 \rceil$. To embed a code, the host signal is first partitioned into L non-overlapped segments. In each segment, we use q mutually orthogonal spread spectrum sequences $\{\mathbf{u}_j, j = 1...q\}$ with identical energy $||\mathbf{u}||^2$ to represent the q possible symbol values, and add one of these sequences into the segment (with perceptual scaling) according to the symbol value in the fingerprint code. The concatenation of all fingerprinted segments forms the ultimate fingerprinted signal.

A common goal considered in the fingerprinting literature is to catch one colluder with high probability. One approach is to first determine which symbol is most likely present in each multimedia segment using a correlation detector commonly used for spread spectrum embedding [2, 8]. We then search the codebook and identify the colluder as the one whose codeword has the smallest Hamming distance to the extracted codeword, or run the ECC decoder if an efficient decoding algorithm is available. Alternatively, we can employ a correlation detector to correlate the entire signal in question directly with every user's fingerprint signal $\mathbf{s}_j$, which is the concatenation of the orthogonal sequences corresponding to the symbols in the user's codeword. 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. $\hat{j} = arg \max_{j=1}^{N_u} T_N(j)$. Here, the detection statistic $T_N(j)$ is defined as:

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

where $\mathbf{z}$ is the colluded signal, $\mathbf{x}$ is the original signal which is often available in fingerprinting application, and $||\mathbf{s}|| = ||\mathbf{s}_j||$ for all j based on the equal energy construction. Compared with the former 2-step scheme, the latter scheme takes advantage of the soft information on the symbol level and provides a better performance. Eq. (2) is also consistent with the detector used for orthogonal fingerprinting, which can be treated as a special case of ECC fingerprinting with $q = N_u$, code length L = 1 and segment size of N. We shall use the whole-signal correlator in our discussions.

3. IMPROVED ECC BASED FINGERPRINTING

In this section, we first examine the collusion resistance of conventional ECC based fingerprinting and compare it with orthogonal fingerprinting. We discover a gap between the performance of ECC based fingerprinting under the interleaving collusion and the averaging collusion. The inspiring analysis on this gap suggests the need of jointly considering the coding, embedding, and detection issues, and leads to our proposed technique that can substantially improve the collusion resistance of ECC based fingerprinting.

3.1. Resistance Against Averaging vs Interleaving Collusion

Consider first an ideal fingerprinting system whose fingerprint sequences have a constant pairwise correlation denoted as ρ. Without loss of generality, we assume the first c users out of n users perform averaging collusion. The vector of detection statistics T_N's defined in (2) follows a n-dimensional Gaussian distribution:

$$\mathbf{T} = [T_N(1), ..., T_N(n)]^T \sim N([\mathbf{m}_1, \mathbf{m}_2]^T, \Sigma) \qquad (3)$$

$$\text{with} \quad \mathbf{m}_1 = \|\mathbf{s}\|(\frac{1}{c} + (1 - \frac{1}{c})\rho)\mathbf{1}_c, \quad \mathbf{m}_2 = \|\mathbf{s}\|\rho\mathbf{1}_{n-c},$$

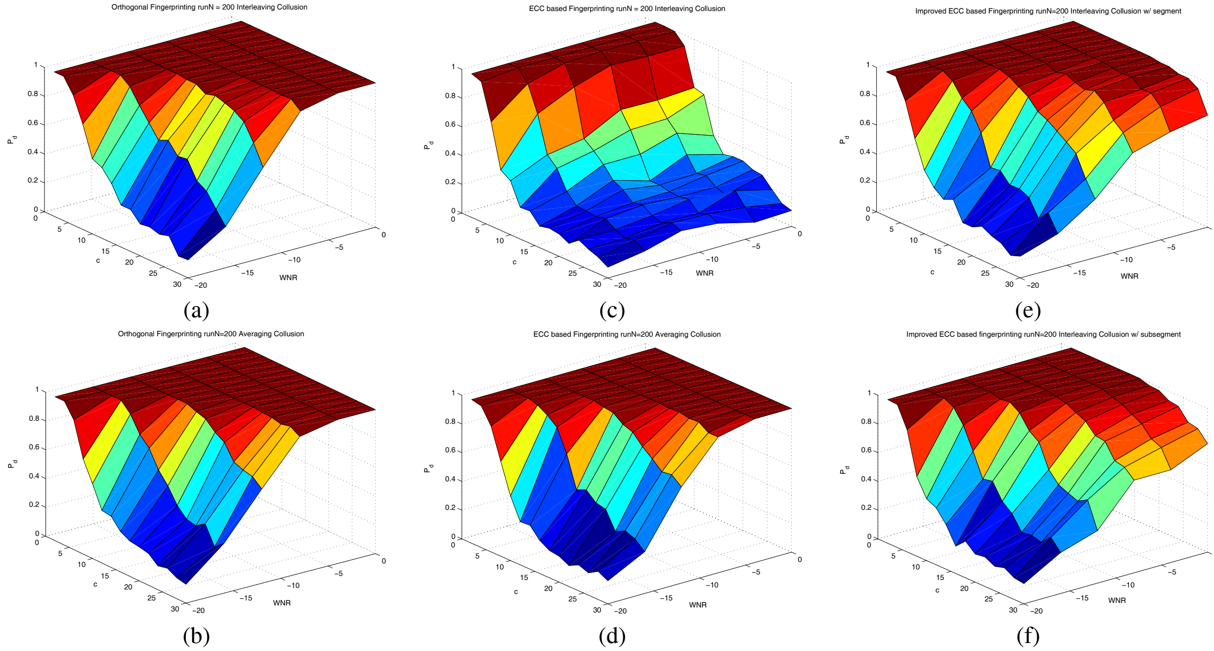
where $\mathbf{1}_k$ is an all-1 vector with dimension k-by-1, and Σ is an n-by-n matrix whose diagonal elements are 1's and off-diagonal elements are ρ's. Given the same colluder number c and fingerprint strength $\|\mathbf{s}\|$, the mean correlation values with colluders $\mathbf{m}_1$ and with innocents $\mathbf{m}_2$ are separated more widely for a smaller ρ. Thus in absence of any prior knowledge on collusion pattern, a smaller ρ leads to a larger colluder detection probability P_d. Therefore, we prefer fingerprint sequences with a small pairwise correlation ρ in designing a fingerprinting system. For ECC 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 more preferable.

Consider an ECC based fingerprinting constructed on Reed-Solomon code with alphabet size q, dimension t, and code length L. Its total number of codewords is $N_u = q^t$ and the minimum distance $D = L - t + 1$. We use $\mathbf{s}_i$ and $\mathbf{s}_j$ to represent the fingerprint sequences for user i and user j, respectively, and $\mathbf{w}_{ik}$ as the orthogonal sequence representing the symbol in user i's codeword at position k with $\|\mathbf{w}_{ik}\| = \|\mathbf{w}\|$. The normalized correlation between $\mathbf{s}_i$ and $\mathbf{s}_j$ is

$$\frac{< \mathbf{s}_i, \mathbf{s}_j >}{\|\mathbf{s}\|^2} = \frac{\sum_{k=1}^{L} \mathbf{w}_{ik}\mathbf{w}_{jk}^T}{L\|\mathbf{w}\|^2} \leq \frac{L - D}{L} = \frac{t - 1}{L} \triangleq \rho_0. \qquad (4)$$

We can choose t and L such that ρ_0 is close to 0. By doing so, the ECC based fingerprinting and orthogonal fingerprinting systems should have comparable resistance against averaging collusion.

We use simulation to verify this conjecture. We choose a Reed-Solomon code with $q = 32$, $t = 2$, $L = 30$, which leads to the number of users $N_u = 1024$. According to the conditions in (1), the code level alone can only assure resisting up to five users' interleaving collusion; on the other hand, the correlation between fingerprint sequences is only 0.03 according to (4). For comparison purpose, we build orthogonal fingerprinting with the same N_u. Both systems are applied to a host signal that is modelled as i.i.d. Gaussian distribution with length $N = 3 \times 10^4$. This simple assumption suits the fingerprinting applications well as the host signal is known to the detector. The corresponding segment size for ECC based fingerprinting is 1000. The detector in (2) is employed for both fingerprinting systems. We measure the probability of correctly catching a colluder (P_d) for different values of colluder number c with Watermark-to-Noise-Ratio (WNR)



(a) (c) (e)

(b) (d) (f)

Fig. 1. Collusion resistance of (a) orthogonal fingerprinting under interleaving collusion; (b) orthogonal fingerprinting under averaging collusion; (c) ECC based fingerprinting under interleaving collusion; (d) ECC based fingerprinting under averaging collusion; (e) Improved ECC fingerprinting under segment-wise interleaving collusion; (f) Improved ECC fingerprinting under subsegment-wise interleaving.

ranging from -20dB to 0dB. The settings of WNR include the scenarios from severe distortion to mild distortion. The simulation results of both systems under interleaving and averaging collusion are shown in Fig. 1(a)-(d).

The simulation results in Fig. 1(b)(d) show that under averaging collusion, the orthogonal and ECC fingerprinting systems constructed above have similar performance as expected. They both can resist at least a few dozens colluders' averaging attack under high WNR and about half dozen's under low WNR. Thus from colluders' point of view, averaging collusion for an ECC fingerprinting system is not a very effective strategy. However, when applying interleaving collusion, we observe from Fig. 1(a)(c) a huge gap on the collusion resistance between the two systems. For orthogonal fingerprinting, the probability of colluder detection under interleaving collusion is comparable to that under averaging collusion owing to the orthogonal spreading [6]. On the other hand, the detection probability of the ECC fingerprinting drops sharply when more than five colluders come to create an interleaved copy, even when WNR is high. Thus from colluders' point of view, interleaving collusion is an effective strategy to circumvent the protection. The drastic difference in collusion resistance of averaging and interleaving collusions on ECC fingerprinting inspires us to look for an improved fingerprinting method for which the interleaving collusion would have a similar effect to averaging collusion. This will lead to a substantial improvement in resisting interleaving collusion, which has been shown as a weak link.

3.2. Joint Consideration of Coding and Embedding

Careful examination on the two types of collusions shows that the difference in the resistance against them comes from the amount of role given to the embedding layer to play. The segment-wise interleaving collusion is equivalent to the symbol-wise interleaving collusion on the code level since each colluded segment comes from just one user. The collusion resilience primarily relies on what is provided by the code layer and bypasses the embedding layer. Because of the limited alphabet size, the chance of the colluders to interleave their symbols and create a colluded fingerprint close to the fingerprint of an innocent user is so high that if to handle this on the code level alone, it would require a large minimum distance in the code design. This means that either a code representing some given number of users can resist only a small number of colluders, or a code can represent only a small total number of users. On the other hand, for averaging collusion, every colluder contributes his/her share in every segment. Through a correlation detector, the collection of such contribution over the entire test signal leads to high expected correlation values when correlating with the fingerprints from the true colluders, and to low expected correlation when with the fingerprints from innocent users. In other words, the embedding layer contributes to defending the collusion. This suggests that more closely considering the relation between fingerprint encoding, embedding, and detection is helpful to improve the collusion resistance against interleaving collusion.

The basic idea of our improved algorithm is to prevent the colluders from exploiting the code-level limitation of using the whole segment that carries one symbol as an interleaving unit, and to make each colluded segment contain multiple colluders' contribution. Our solution builds upon the existing code construction and performs two important additional steps that we collectively refer to as *permuted subsegment embedding*. Consider as before a fingerprint signal generated by concatenating the appropriate sequences corresponding to the symbols in a user's codeword. We first partition each original segment of the fingerprint signal into β subsegments, giving a total of βL subsegments. We then randomly permute the subsegments according to a secret key to obtain the final fingerprint sequence to represent the user. In detection, the extracted fingerprint sequence is first inverse permuted and then

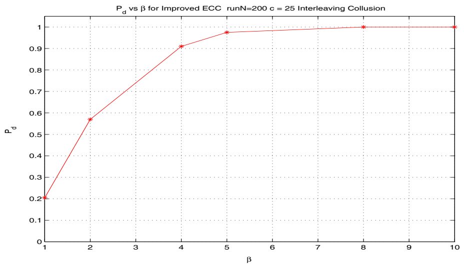


Fig. 2. P_d vs β for $c = 25$ and WNR = 0dB of the proposed scheme.

the whole-signal correlator is applied to identify the colluder.

With segment partitioning and permutation, each colluded segment after inverse permutation most likely contains subsegments from multiple users when the colluders employ interleaving collusion. To correlation-based detectors (including both hard and soft detection on the symbol level), this would have a similar effect to what averaging collusion brings. Since averaging collusion is far less effective from the colluder's point of view, the permuted subsegment embedding can greatly improve the collusion resistance of ECC based fingerprinting under interleaving collusion. Even if the colluders know the actual size of a segment or a subsegment, the permutation unknown to them prevents them from creating a colluded signal with the equivalent effect of symbol interleaving in the code domain.

In the proposed scheme, the parameter β controls the "approximation" level of the effect of interleaving collusion to that of averaging collusion. Larger β provides a finer granularity in permutation. Thus each segment may contain subsegments from more colluders, leading to better approximation and better collusion resistance. We verify this relation by building an improved ECC fingerprinting system with different β upon the experiment setup in Sec.3.1. Fig. 2 shows the results when a total of $c = 25$ colluders perform segment-wise interleaving with WNR = 0dB. We can see that higher β indeed gives higher detection probability P_d. On the other hand, a larger β may incur higher computational complexity in permutation. Thus a tradeoff should be made according to the requirements by a specific application.

We evaluate the performance of the improved system with $\beta = 5$ under various WNRs, and show the results in Fig. 1(e) for segment-based interleaving collusion. We can see that the detection probability of the proposed system is substantially improved over the original ECC fingerprinting system under the same interleaving collusion shown in Fig. 1(c). The performance gap between the proposed system (Fig. 1(e)) and that of the orthogonal fingerprinting (Fig. 1(a)(b)) is very small. We also observe from Fig. 1 (e) and (f) that the detection performance under interleaving collusion using a subsegment as a unit and using a segment as a unit have similar performance and give a high detection probability for up to two dozens colluders at moderate to high WNR. Overall, the proposed system based on the joint consideration of the fingerprint coding and embedding has effectively improved the collusion resistance.

4. DISCUSSIONS AND CONCLUSIONS

The Role of Permutation Random permutation is a useful technique that has found quite a few applications in data embedding. It was used in image watermarking to equalize the uneven embedding capacity [9], and applied to a simple staircase construction of binary fingerprint code to prevent the framing of innocent users [3]. In our proposed work, we employ the random permutation to make each segment after interleaving collusion contain multiple colluders' information, thus mimicking the effect of averaging collusion and improve the collusion resistance against interleaving collusion.

Efficiency in Detection and Distribution The detection of the improved ECC based fingerprinting consists of three main stages. The computational complexity of the inverse permutation is $O(\beta L)$. Since the fingerprint sequences for each segment only have q different versions (corresponding to q symbols), we need $qL(N/L)$ multiplications plus $qL(N/L-1)$ summations to obtain correlation values with N_u users. The computational complexity of this stage is $O(qN)$. The last stage of finding maximum correlation needs at most $N_u - 1$ comparisons. Since normally $\beta L \leq N$ and $N_u << N$, the total computational complexity of the proposed system is $O(qN)$. When Reed-Solomon code is employed, the detection computational complexity becomes $O(\sqrt[t]{N_u}N)$ as $N_u = q^t$. This is basically the same as the complexity of the conventional ECC based fingerprinting and remains considerably lower than $O(N_u N)$ complexity of the orthogonal fingerprinting.

Similarly, we can show that the improved ECC based fingerprinting inherits the advantage from coded fingerprinting to allow the efficient generation and distribution of the fingerprinted signal discussed in Sec. 1.

Conclusions In this paper, we focus on improving the collusion resistance of the ECC based fingerprinting while retaining its advantages in detection complexity and fast distribution. We have discovered a gap in the collusion resistance of ECC based fingerprinting between the averaging and interleaving collusions. Our analysis on the gap suggests a great need of jointly considering the coding, embedding, and detection issues, and inspires to the proposed technique of permuted subsegment embedding. Experimental results demonstrate that the proposed technique can substantially improve the collusion resistance of ECC based fingerprinting, while inheriting the advantage in detection complexity and efficient distribution.

5. REFERENCES

[1] F.Ergun, J.Kilian and R.Kumar, "A Note on the limits of Collusion-Resistant Watermarks", *Eurocrypt '99*, 1999.

[2] 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.

[3] D. Boneh and J. Shaw, "Collusion-secure Fingerprinting for Digital Data," *IEEE Tran. on Info. Theory*, 44(5), 1998.

[4] Y. Yacobi, "Improved Boneh-Shaw Content Fingerprinting", *CT-RSA 2001, LNCS 2020*, pp. 378-391, 2001.

[5] 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.

[6] W. Trappe, M. Wu, Z.J. Wang, and K.J.R. Liu, "Anti-collusion Fingerprinting for Multimedia", *IEEE Trans. Sig. Proc.*, 2003.

[7] S. He and M. Wu, "Performance Study of ECC-based Collusion-resistant Multimedia Fingerprinting," in *Proceedings of the 38th CISS*, March 2004, pp. 827–832.

[8] 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.

[9] M. Wu and B. Liu, "Data Hiding in Binary Image for Authentication and Annotation", *IEEE Trans. Multimedia*, 2004.