COLLUSION-RESISTANT DYNAMIC FINGERPRINTING FOR MULTIMEDIA

Shan He and Min Wu

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

ABSTRACT

This paper considers protecting multimedia content from unauthorized redistribution in subscription based services, where adversaries work together to pirate multiple multimedia programs during a subscription period. Collusion-resistant fingerprinting is an emerging tool for traitor tracing. However, most of the existing fingerprinting works did not consider multiple rounds of interaction between collusion and detection. In this paper, we exploit the temporal dimension and propose a dynamic fingerprinting scheme that adjusts the fingerprint design based on the detection result of previously pirated signal. We also examine colluders' strategies to combat the tracing by dynamic fingerprinting. Both analytical and simulation results show that the proposed dynamic fingerprinting provides better collusion resistance than conventional static fingerprinting.

Index Terms– Multimedia fingerprinting, dynamic fingerprinting, collusion resistance, dynamic collusion strategy.

1. INTRODUCTION

Nowadays, subscription based content services have become very popular, such as cable TV or online downloading, where users can obtain multimedia content from the content provider during the subscription period. It is important to protect the content from unauthorized redistribution during the subscription period. Fingerprinting is an emerging tool to enable the content owner to trace the source of leak by embedding a unique ID into each user's copy. Collusion is a powerful, cost-effective attack from a group of users, whereby the users combine their copies of the same content to generate a new version.

Among the anti-collusion works in the literature, a simple and effective approach for a small scale of users and media data is orthogonal fingerprinting, which assigns each user a spread spectrum sequence as fingerprint and the sequence is mutually orthogonal to those for other users [1]. An early work by Boneh and Shaw focused on generic data and introduced a two-level code construction to resist a given number of colluders with high probability [2]. A sequential fingerprinting work was proposed by Safavi-Naini et al. [8], in which a code structure is determined beforehand to facilitate sequential detection. To fingerprinting multimedia signal, an anti-collusion code based on combinatorial design was embedded in multimedia through spread spectrum code modulation and can identify colluders through the code bits shared by them [3]. Another recent work on joint coding and embedding multimedia fingerprinting significantly improved the collusion resistance of coded fingerprinting while maintaining the efficiency in fingerprint construction and distribution [4]. This work is later applied to accommodate a large user group on the order of tens to hundreds of millions [5].

Authors' email: {shanhe, minwu}@eng.umd.edu

Most fingerprinting works address the anti-collusion problem for one signal in a static way, i.e. the fingerprint for each user is designed before-hand. One of the first several works considering dynamic traitor tracing is by Fiat et al [6] and was improved in [7]. In their work, the host signal is transmitted in segments, and the fingerprint in each segment is dynamically determined according to the detected fingerprints from previous segments. After collecting many segments, the detector makes a decision on the likely colluder. A major limitation of the work is the assumptions on real-time surveillance feedback and on dumb colluders, which may not always be realistic. Although it is possible to extend Fiat's dynamic fingerprinting to subscription scenarios of multiple programs by treating one movie as one segment, the detector has to collect tens of pirated movies for the algorithm to converge to catch ten colluders out of only 1000 users. If the total number of users scales up to millions, the detector has to collect nearly 100 pirated movies to catch colluders, which is impractical.

In this paper, we consider the time dimension of the subscription based services and exploit the dynamics between the content owner and the colluders to design fingerprint. Specifically, we adjust the fingerprint strength dynamically according to the colluders' information collected from previous pirated signals. To better understand the performance of the proposed scheme, we also examine possible strategies that colluders may take to combat dynamic fingerprinting. Results show that the proposed scheme has better collusion resistance than static ones and is robust to various collusion strategies.

2. PROBLEM DESCRIPTION AND BASIC FINGERPRINTING SCHEME

A dynamic fingerprinting scheme consists of several rounds. Each round i employs a basic fingerprinting system $\mathcal{F}_i$. The content owner distributes a signal $\mathbf{x}_i$ with fingerprint embedded to all users in the system. After receiving the fingerprinted signals, the colluders collectively generate a copy $\mathbf{z}_i$ and redistribute it. When a detector obtains a colluded copy $\mathbf{z}_i$, detection is performed on $\mathbf{z}_i$ to identify colluder(s). According to the detection results, the content owner redesign the fingerprint for round $i+1$ to increase the chances for colluders being caught. As a result, the fingerprinting scheme for round $i+1$, $\mathcal{F}_{i+1}$, is a function of $\mathcal{F}_i$ and the collusion strategy $\mathcal{K}_i$, i.e. $\mathcal{F}_{i+1} = f(\mathcal{F}_i, \mathcal{K}_i)$, where $f()$ is the dynamic fingerprinting strategy. The same process will continue in round $i+1$.

In this paper, we employ orthogonal fingerprinting [1] as the basic fingerprinting scheme for each round and this basic fingerprinting scheme can be replaced by other fingerprinting systems [4] according to the application requirements. In orthogonal fingerprinting, mutually orthogonal spreading sequences $\{\mathbf{u}_j, j = 1...N_u\}$ with identical energy $||\mathbf{u}||^2$ are assigned to N_u users as the fingerprints. User j's fingerprinted copy is obtained as $\mathbf{y}_j =$

$\mathbf{x} + \mathbf{u}_j$. After the distribution of the fingerprinted copies, the adversaries may employ various attacks $\mathcal{K}$. In this paper we focus on averaging collusion [1], where colluders take the average of the corresponding signal in their copies to generate a colluded version. The colluded version $\mathbf{z}$ follows:

$$\mathbf{z} = \frac{1}{K}\sum_{j\in S_c}\mathbf{y}_j + \mathbf{d} = \frac{1}{K}\sum_{j\in S_c}\mathbf{u}_j + \mathbf{x} + \mathbf{d}, \quad (1)$$

where S_c is the colluder set with size K. The additional distortion is modelled as an $i.i.d.$ additive Gaussian noise $\mathbf{d}$ with zero-mean and variance σ_d^2.

To identify colluders who have contributed to a suspicious copy of multimedia content, we employ a correlation detector commonly used for spread spectrum embedding. In this paper, we focus on catching one colluder with high probability, for which the maximum detector [1] is employed. The user with the highest correlation with the test signal is identified as the colluder: $\hat{j} = arg\max_{j=1}^{N_u} T_j$, where

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

The colluder set in each round can be the same or different. In this paper, we first consider the case of static colluder set, in which colluders remain the same for each round. In Section 4, we will discuss the dynamic strategies that colluders can employ in different rounds.

3. THE PROPOSED DYNAMIC FINGERPRINTING

3.1. Dynamic Fingerprinting Scheme

For simplicity, we start with a two-round system, and assumes the content owner initially does not have information about the colluders. In the first round, the content owner assumes every user has equal probability to collude, and the orthogonal fingerprinting with equal strength is employed. When a pirated copy is leaked, the correlation based detector in Eqn. (2) is employed to identify colluder.

We design the fingerprints of the second round based on the detection statistic $T^{(1)}$ from the first round. Given the statistic $\{T_i^{(1)}\}$ for each user, a threshold h is chosen such that the users whose detection statistic is higher than h are put into the suspicious user set U_s. The fingerprint strength of the users in U_s will be increased by a small amount β in the second round to increase the probability of catching colluder(s). That is, for users in U_s, the fingerprinted copy is obtained as $\mathbf{y} = \mathbf{x} + (1+\beta)\mathbf{u}$. Other users' fingerprint strength remains as $\|\mathbf{u}\|$. The strategy of increasing only suspicious users' fingerprint energy instead of all the users is important in the applications where it is crucial to guarantee innocent users to get high-fidelity content. The parameters h and β in the proposed scheme enable the designer to achieve a trade-off between the detection performance and the received perceptual quality according to various applications' requirements.

After finding out a suspicious copy in the second round, the content owner employs the correlation detector in Eqn. (2) to identify colluder. As will be seen from Section 3.2, the increased fingerprint strength will increase the colluders' probability of being caught while the probability of false alarm remains unchanged. The detection statistic from second round $T_i^{(2)}$ can also be combined with $T_i^{(1)}$ as $T_i = (T_i^{(1)} + T_i^{(2)})/\sqrt{2}$ to facilitate the final decision, where we pick the user with highest T as the colluder.

[1]For orthogonal fingerprinting with Gaussian distributed fingerprints, a number of non-linear collusions employing order statistics, such as minimum collusion attack, have been shown [9] to be well approximated by the averaging collusion plus additive noise.

3.2. Analyzing Colluder Detection Performance

In this section, we analyze the probability of catching one colluder for the proposed dynamic fingerprinting. For comparison purpose, we also analyze two other alternatives: (1) repeatedly employing equal-energy orthogonal fingerprinting with the same fingerprint energy for both rounds, which we call *static fingerprinting*, and (2) employing equal-energy orthogonal fingerprinting for the first round and increasing the energy by β for all the users in the second round, called *blind dynamic fingerprinting* since it does not utilize the detection results from the first round.

For all three schemes, the first step is to determine the distribution of $T^{(1)}$ and $T^{(2)}$ so as to derive the distribution of the final detection statistic $T_i = (T_i^{(1)} + T_i^{(2)})/\sqrt{2}$ for each user. After obtaining the distribution of T_i's, we are able to calculate the probability of detection as

$$P_d = Pr(T_{M1} > T_{M2}) = \int Pr(T_{M1} > t) f_{T_{M2}}(t)dt \quad (3)$$

where $T_{M1} = \max_{i\in S_c} T_i, T_{M2} = \max_{i\notin S_c} T_i$, and $f_{T_{M2}}(t)$ is the $p.d.f.$ of T_{M2}. For all three schemes, T_i for innocent users are the same and follow Gaussian distributions $N \sim (0, \sigma_d^2)$. Thus we have

$$f_{T_{M2}}(t) = \frac{N_u - K}{\sigma_d}\Phi\left(\frac{t}{\sigma_d}\right)^{N_u-K-1} \times \phi\left(\frac{t}{\sigma_d}\right), \quad (4)$$

where N_u is the total number of users, and $\Phi()$ and $\phi()$ are the $c.d.f.$ and $p.d.f.$ of standard Gaussian distribution, respectively.

The detection statistic T for static fingerprinting and blind dynamic fingerprinting can be shown to follow

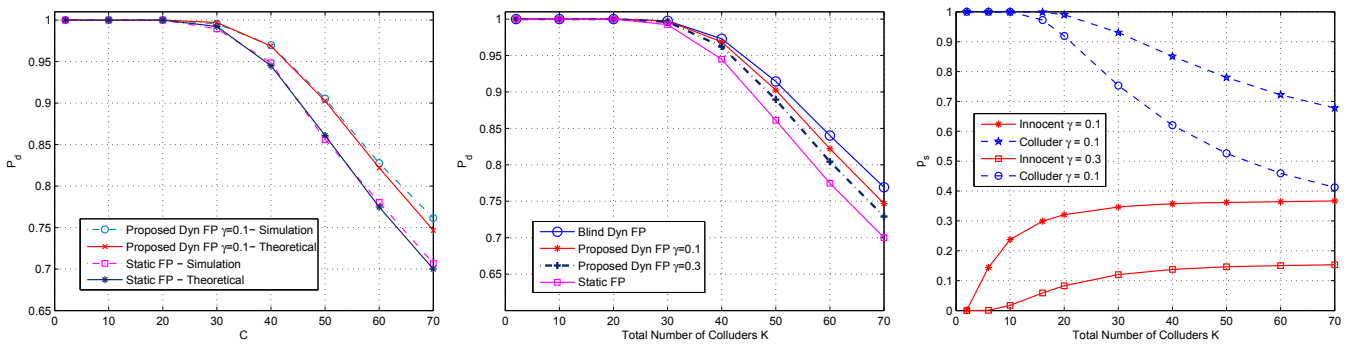
$$T_i \sim \begin{cases} N(0, \sigma_d^2), & i \notin S_c, \\ N(\mu_C, \sigma_d^2), & i \in S_c, \end{cases} \quad (5)$$

where μ_C takes value of $\sqrt{2}\|\mathbf{u}\|/K \triangleq \mu_{C1}$ for static fingerprinting and $(2+\beta)\|\mathbf{u}\|/(\sqrt{2}K) \triangleq \mu_{C2}$ for blind dynamic fingerprinting.

To determine the distribution of T for the proposed dynamic fingerprinting, we need to first calculate the probability of $T_i^{(1)}$ having higher value than the threshold after the first round. This probability, denoted as p_{si}, is the probability for each user to be put into a suspicious user set. In this paper, we set the threshold h adaptively as $h = \gamma \max_i T_i^{(1)}$. Then, the p_{si} is calculated as

$$p_{si} = \int \prod_{j\neq i} Pr(T_j^{(1)} < t/\gamma) f_{T_i}(t)dt. \quad (6)$$

Due to the equal energy and orthogonal fingerprint construction in the first round, p_{si} for all the innocent users are the same. We denote it as p_{s0}. Similarly, p_{si} for all the colluders would be the same under fair collusion, and we denote it as p_{s1}. We can show



(a) (b) (c)

Fig. 1. Performance of three schemes: (a) Simulation results vs. analytical results; (b) Analytical results for all three schemes (c) Portion of users having higher fingerprint strength in the second round.

that T of the proposed scheme has the distribution of

$$T_i = \begin{cases} N(0,\sigma_d^2), & i \notin S_c, \\ N(\mu_{C2},\sigma_d^2), & \text{with prob. } p_{s1} \quad i \in S_c \\ N(\mu_{C1},\sigma_d^2), & \text{with prob. } 1-p_{s1} \quad i \in S_c, \end{cases} \tag{7}$$

$$\text{and} \quad Pr(T_{M1} > t) = 1 - \sum_{i=0}^{K} \Phi^i\left(\frac{t-\mu_{C2}}{\sigma_d}\right) \times \Phi^{K-i}\left(\frac{t-\mu_{C1}}{\sigma_d}\right)\binom{K}{i} p_{s1}^i (1-p_{s1})^{K-i}. \tag{8}$$

Plugging in the obtained results into Eqn. (3), we can obtain the probability of catching one colluder for all three schemes.

We validate the analysis through simulations with 5000 iterations. The examined system holds 1000 users, and the fingerprint length is 10^4, which is roughly the number of embeddable components in a 256×256 natural image. The first round of all three systems employs orthogonal fingerprinting with equal strength. In the second round, the static fingerprinting keeps the same fingerprint strength; the two dynamic fingerprinting schemes employ $\beta = 0.2$ to introduce a small amount of extra distortion, which is equivalent to 1.6dB loss in PSNR. Fig. 1(a) shows the simulation results on probability of detection P_d along with the numerical evaluation of Eqn. (3), where we select the results of static fingerprinting and the proposed dynamic fingerprinting as representatives. We can see that the analytical results match well with simulation results.

3.3. Comparison of Fingerprinting Schemes

In this section, we evaluate the performance of the proposed dynamic fingerprinting in comparison with the other two alternatives. The experimental settings are the same as that in Section 3.2. The adaptive threshold γ for the proposed dynamic fingerprinting is set at 0.1 and 0.3, respectively. Fig. 1 (b) shows the analytical results of P_d versus the colluder number K at a Fingerprint-to-Noise Ratio of -5dB for all three schemes. We can see that the collusion resistance of the blind dynamic fingerprinting is better than that of static fingerprinting due to higher fingerprint strength in the second round. With the same detection probability, e.g. P_d=0.85, the static fingerprinting can only resist 51 colluders, while the blind dynamic fingerprinting can resist 59 colluders giving a 16% improvement in collusion resistance. The performance of the proposed dynamic fingerprinting lies in between and is close to blind dynamic fingerprinting scheme. For example, with $\gamma = 0.1$, the proposed dynamic fingerprinting can catch $6 \sim 7$ more colluders than static fingerprinting. As the threshold γ decreases, the collusion resistance of the proposed scheme gets closer to that of blind dynamic fingerprinting.

Although blind dynamic fingerprinting has the highest detection probability in all three schemes, everyone in the system, including innocent users, suffers a larger distortion in the second round of content distribution because of the increased fingerprint strength. This is unfair for the innocent users. In comparison, the proposed dynamic fingerprinting only increases the fingerprint strength for the suspicious users. Fig. 1(c) shows the portion of the innocent users' and colluders' fingerprint to be increased. From the results, we can see that with $\gamma = 0.1$, only 37% of the innocent users receive content with larger distortion in the second round and 68% of the colluders have their fingerprint energy increased, and we are able to achieve almost the same detection performance as the blind dynamic fingerprinting where all users have larger distortion. As we increase γ, fewer innocent users and colluders receive low quality signal, which leads a lower P_d. We can see that γ is a parameter used to achieve a trade-off between the collusion resistance performance and user satisfaction. Overall, the proposed dynamic fingerprinting has a better trade-off than the other two schemes.

4. DYNAMIC COLLUSION STRATEGIES

The results shown in the last section are based on the assumptions that the colluders remain the same in both rounds. However, knowing the dynamic fingerprinting is employed, colluders may take different strategies in each round to circumvent the proposed fingerprinting. In this section, we examine the possible strategies that the colluders may take, and study the performance of the proposed dynamic fingerprinting against those collusion strategies. Here we assume that each of the colluders is honest to the coalition, and issues regarding selfish colluder can be studied following the framework in [10].

The effectiveness of the proposed scheme comes from the fact that the colluders participate the collusion in both rounds so that (1) the colluders may be detected as suspicious user in the first round and get fingerprint of increased strength for second round; (2) after participating the collusion in the second round, his/her probability of being detected is higher than before due to the increased fingerprint energy. Observing this, colluders may form different collusion sets for each round to circumvent the dynamic

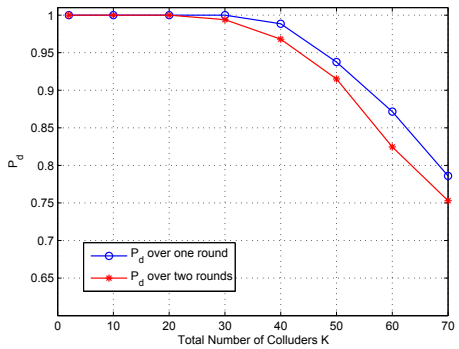


Fig. 2. P_d of the proposed scheme against distinct colluder set.

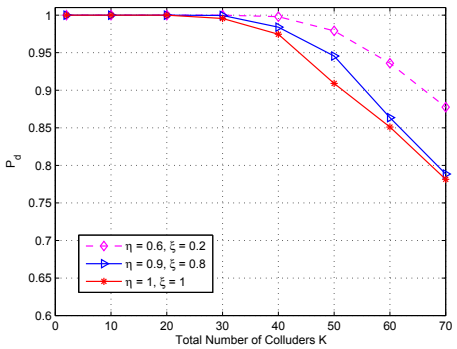


Fig. 3. P_d of the proposed scheme against overlapped colluder set.

fingerprinting.

Suppose there are totally K colluders, denoted as S_c. The colluders decide to choose a subset of the colluders to collude in the first round and use a different subset of colluders for the second round. We denote the colluder set in the first round as S_{c1} with K_1 colluders, in the second round as S_{c2} with K_2 colluders, and $S_c = S_{c1} \cup S_{c2}$. The ratio of the colluders in the first round over the entire colluder group is denoted as $K_1/K = \eta$. We define an overlap ratio as $\xi = |S_{C1} \cap S_{C2}|/K$. It is obvious that $K_2 + K_1 = (1+\xi)K$. The parameters η and ξ feature the strategy employed by the colluders. For simplicity, we consider the colluder set for both rounds to have the same colluder number, which imposes one more constraint of $\eta = 1 + \xi - \eta$. Under this model, the collusion strategy with repeated colluder set we have examined in Section 3 is a special case with $\eta = \xi = 1$. Now we examine other two cases, namely, disjoint colluder set and overlapped colluder set.

Disjoint Colluder Set In this strategy, the colluders divide themselves into two disjoint groups and each group performs collusion attack in one round, i.e. $\eta = 0.5$, $\xi = 0$. As a result, every colluder participates the collusion only in one round. Under this case, the detection statistic T based on both rounds has distribution close to that of the static fingerprinting as in Eqn. (5), and thus the detection performance would be similar to that of the static fingerprinting. However, due to the smaller colluder group in each round, the basic fingerprinting system in each round has a higher probability of detection as shown in Fig. 2. In this case, at each round, the detector is able to make decision without aggregating the detection statistics from multiple rounds, and the colluders actually have higher risk of being caught than before.

Overlapped Colluder Set In this case, some colluders only participate in one round of collusion and some participate in both rounds. The two parameters η and ξ are within the range of $0.5 < \eta < 1, 0 < \xi < 1$. In Fig. 3, we show the probability of detection under this collusion strategy, where we examined two settings: $\eta = 0.6$, $\xi = 0.2$ and $\eta = 0.9$, $\xi = 0.8$. Comparing the results with that of Section 3, we can see that the overlapped colluder set brings the detector up to 10% increase in probability of detection. As ξ and η approach 1, the performance approaches to the case with the same colluder set in both rounds. The strategy with overlapped colluder set does not bring benefit to the colluders. Fairness issues inside the colluders would also arise, which will be addressed in our future work.

In summary, if we look at only one round, both strategies with distinct and overlapped colluder set reduce the colluder number in each round and increase the colluders' risk of being caught; if we collectively examine two rounds, the overlapped strategy also increase the probability of detection. Therefore, the best strategy for colluders would be to try to collect as many colluders as possible in each round and launch the collusion attack altogether, which is the case that we have examined in Section 3.

5. CONCLUSIONS

In this paper, we have studied the problem of anti-collusion fingerprinting for applications with long-term subscription, where a group of pirates may launch several rounds of collusions. We propose a dynamic fingerprinting strategy to adjust the fingerprint strength in each round according to the detection results from previous round. Both analytical and simulation results show that the proposed scheme performs better, in terms of detection probability, than static fingerprinting and close to blind dynamic fingerprinting without having as many users suffering from reduced visual quality. Dynamic collusion strategies are also examined, where the results indicate that the best strategy for colluders is to gather as many colluders as possible in each round of the collusion.

6. REFERENCES

[1] Z.J. Wang, M. Wu, H. Zhao, W. Trappe, and K.J.R. Liu, "Anti-Collusion Forensics of Multimedia Fingerprinting Using Orthogonal Modulation," *IEEE Trans. on Image Proc.*, pp. 804–821, June 2005,

[2] D. Boneh and J. Shaw, "Collusion-secure Fingerprinting for Digital Data," *IEEE Tran. on Info. Theory*, 44(5), pp. 1897–1905, 1998.

[3] W. Trappe, M. Wu, Z.J. Wang, and K.J.R. Liu, "Anti-collusion Fingerprinting for Multimedia," *IEEE Trans. on Sig. Proc.*, 51(4), 2003.

[4] S. He and M. Wu, "Joint Coding and Embedding Techniques for Multimedia Fingerprinting," *IEEE Trans. on Info. Forensics and Security*, Vol.1, No.2, pp.231–247, June 2006.

[5] S. He and M. Wu, "Collusion Resistant Multimedia Fingerprinting for Large User Group," *IEEE Int'l Conf. on Image Proc.*, Oct. 2006.

[6] A. Fiat and T. Tassa, "Dynamic Traitor Tracing," *J. of Crypto., Vol. 14, No. 3, pp.211–223, 2001*

[7] T. Tassa, "Low Bandwidth Dynamic Traitor Tracing Schemes," *J. of Crypto., Vol. 18, No. 2, pp.167–183, 2005*

[8] R. Safavi-Naini and Y. Wang, "Sequential Traitor Tracing," *IEEE Trans. on Info. Theory*, Vol.49, No.5, pp.1319–1326, May 2003.

[9] H. V. Zhao, M. Wu, Z. J. Wang and K. J. R. Liu, "Forensic Analysis of Nonlinear Collusion Attacks for Multimedia Fingerprinting," *IEEE Trans. on Image Proc.*, vol. 14, no. 5, pp. 646–661, May 2005.

[10] H. V. Zhao and K. J. R. Liu, "Risk Minimization in Traitors Within Traitors in Multimedia Forensics," *IEEE Int. Conf. on Image Processing (ICIP'05)*, Genova, Italy, Sept. 2005