New Traceability Codes against a Generalized Collusion Attack for Digital Fingerprinting

Hideki Yagi[1], Toshiyasu Matsushima[2], and Shigeichi Hirasawa[2]

[1] Media Network Center, Waseda University
1-6-1, Nishi Waseda, Shinjuku-ku Tokyo 169-8050 Japan.
E-mail: yagi@hirasa.mgmt.waseda.ac.jp
[2] School of Science and Engineering, Waseda University
3-4-1 Ohkubo Shinjuku-ku, Tokyo, 169-8555 Japan.

Abstract. In this paper, we discuss collusion-secure traceability codes for digital fingerprinting which is a technique for copyright protection of digital contents. We first state a generalization of conventional collusion attacks where illicit users of a digital content collude to create an illegal digital content. Then we propose a collusion-secure traceability code which can detect at least one colluder against it. We show the rate and properties of the proposed traceability code.

1 Introduction

Digital fingerprinting is a technique to allow tracing illicit users of digital contents such as software, digital movies or audio files. When digital contents are distributed with fingerprinting technique, a unique codeword (**fingerprint**) to each user is embedded into the original contents by a watermarking technique. Fingerprinting techniques are devised to tackle the problem that some illicit users (**colluders**) collude to make pirated contents. When an illegally pirated content created by colluders is observed, the detector estimates the colluders' fingerprints. When the number of colluders is not greater than a positive integer T, a code which can detect at least one colluder is called a T-**traceability code**. A T-traceability code is a strong version of a frameproof code and an identifiable parent property (IPP) code [6, 8].

A well-discussed collusion attack is called the **interleaving attack** [3] where each symbol of the illegal fingerprint is selected among symbols of colluder's fingerprints [1, 2, 6–8]. Another well-known collusion attack is the **averaging attack** [9, 10] where symbols of colluders' fingerprints are averaged and set to the symbol of the illegal fingerprint. Although S. He and M. Wu have discussed the performance difference of fingerprinting codes against these attacks in [3], no T-traceability codes which can handle with the both attacks have been devised.

In this paper, we extend a collusion attack so that it includes both interleaving attack and averaging attack as a special case and we propose a collusion-secure T-traceability code against it. We devise a construction method of a T-traceability code by concatenation of a certain type of an integer set and an

error-correcting code. We discuss a method for increasing the rate of the T-traceability code by allowing some detection error of symbols of the inner code. We also derive a condition for detecting more than one colluders.

2 Preliminary

2.1 Digital Fingerprinting

Let $\Gamma = \{u_1, u_2, \ldots, u_M\}$ be the set of M users for a given digital content $\boldsymbol{w}$. Denote the fingerprint (codeword) of a user $u_i \in \Gamma$ by $\boldsymbol{c}_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,N}) \in \mathcal{I}(q)^N$ where $\mathcal{I}(q)$ denote a set of q integers. Then $\mathcal{C} = \{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_M\}$ is a set of fingerprints (fingerprinting code) for users of the digital content. The supplier of the digital content embeds each fingerprint $\boldsymbol{c}_i$ into the digital content by a watermarking technique so that users cannot detect their embedded fingerprints. We assume that the watermarked content for the user $u_i \in \Gamma$ is $\boldsymbol{v}_i = (v_{i,1}, v_{i,2}, \ldots, v_{i,N})$ such that

$$v_{i,j} = w_j + \alpha_j c_{i,j}, \quad 1 \leq j \leq N, \tag{1}$$

where α_j is just-noticeable-difference (JND) from human visual system models [11].

Some illicit users (**colluders**) might compare their watermarked contents to know where their imperceptible fingerprints are embedded. Then they attempt to create a pirated content with an illegal fingerprint and they use it for an illegal purpose. This procedure is called **collusion attack**. Throughout of this paper, we assume that the set of colluders is $\mathcal{S} = \{u_1, u_2, \ldots, u_{|\mathcal{S}|}\}$ where $|\mathcal{S}| \leq T$ for simplicity. We denote the illegal fingerprint obtained from the pirated content by $\boldsymbol{y} = (y_1, y_2, \ldots, y_N) \in \mathcal{R}^N$. We assume that the detector of the colluders knows the original digital content $\boldsymbol{w}$ and the JND coefficients $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_N)$. The detector of the colluders estimates the set of colluders $\mathcal{S}$ when it observes the illegal fingerprint $\boldsymbol{y}$. In the studies of digital fingerprinting, it is important to construct a fingerprinting code which can detect one or more colluders in $\mathcal{S}$ from the pirated content.

2.2 Collusion Attack

We describe collusion attacks in previous studies and the collusion attack considered in this paper. Most of previous studies have considered the interleaving attack and the averaging attack.

Definition 1 (Interleaving Attack [1, 6, 7]) For $j = 1, 2, \ldots, N$, let $\mathcal{C}_j(\mathcal{S}) = \{c_{1,j}, c_{2,j}, \ldots, c_{|\mathcal{S}|,j}\}$ be a set of the j-th symbol of the colluders' fingerprints in $\mathcal{S}$. The colluders create the j-th symbol of $\boldsymbol{y}$ by selecting one of the symbols in $\mathcal{C}_j(\mathcal{S})$. □

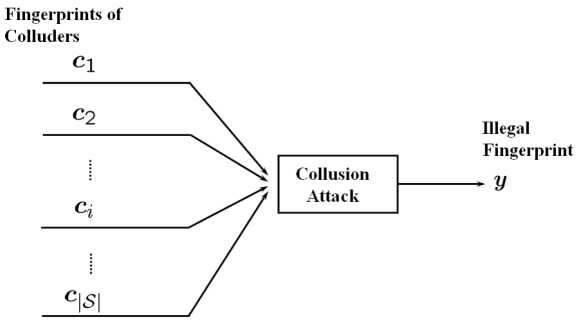

Fig. 1. Illustration of Collusion Attack

Definition 2 (Averaging Attack [9, 10]) The colluders create the j-th symbol of $\boldsymbol{y}$ by averaging all of the j-th symbols of the colluders' fingerprints. i.e.,

$$y_j = \frac{1}{|\mathcal{S}|} \sum_{i|u_i \in \mathcal{S}} c_{i,j}. \tag{2}$$

where $\boldsymbol{c}_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,N})$ and the addition is carried out in real numbers. □

Remark 1 Since the colluders cannot see their fingerprint symbols in the watermarked content, they actually select one of the j-th component of the watermarked content $\boldsymbol{v}_i, i \in \mathcal{S}$, in the interleaving attack. In this case, the detector of the fingerprint can obtain y_j by $y_j = (v_{i^*,j} - w_j)/\alpha_j$ where i^* denotes the user index of the selected symbol

When the colluders commit the averaging attack, the j-th symbol of the watermarked content $\boldsymbol{v}_i, i \in \mathcal{S}$ are averaged. In this case, since

$$v'_j = \frac{1}{|\mathcal{S}|} \sum_{i|u_i \in \mathcal{S}} v_{i,j} = w_j + \frac{\alpha_j}{|\mathcal{S}|} \sum_{i|u_i \in \mathcal{S}} c_{i,j}, \tag{3}$$

the detector of the fingerprint can obtain y_j by $y_j = (v'_j - w_j)/\alpha_j$.

Hereafter, to simplify the discussion, we only describe the illegal fingerprint without original content. Even in this case, the discussion is not essentially different. □

In conventional studies, these collusion attacks have been considered separately. In this paper, we assume the following collusion attack.

Definition 3 (Collusion Assumption)

When the colluders create the j-th symbol of $\boldsymbol{y}$, they select a subset of the j-th symbols of colluders' fingerprints. We denote the set of users' indexes of the

selected subset by $\mathcal{S}_j$. The all symbols in the selected subset $\mathcal{S}_j$ are averaged and the averaged value is set to the j-th symbol of $\boldsymbol{y}$. i.e., we have

$$y_j = \frac{1}{|\mathcal{S}_j|} \sum_{i|u_i \in \mathcal{S}_j} c_{i,j} \tag{4}$$

where the summation is carried out in real numbers. □

This collusion attack is reduced to the interleaving attack when $|\mathcal{S}_j| = 1$ for $j = 1, 2, \ldots, N$ and the averaging attack when $|\mathcal{S}_j| = |\mathcal{S}|$ for $j = 1, 2, \ldots, N$.

3 Proposed Code Construction against Generalized Collusion Attack

3.1 *T*-Traceability Code

We will discuss code construction against the new collusion attack. First, we define the Hamming distance between a symbol and a symbol set. We define the following sets:

$$\mathcal{Y}_j = \{c_{i,j} | \, u_i \in \mathcal{S}_j\}. \tag{5}$$

$$\mathcal{Y} = \{\boldsymbol{x} = (x_1, x_2, \ldots, x_N) | \, x_j \in \mathcal{Y}_j, 1 \leq j \leq N\}. \tag{6}$$

The set $\mathcal{Y}_j$ expresses a set of candidate symbols which may give the j-the symbol of the illegal fingerprint $\boldsymbol{y}$. We define the Hamming distance between a symbol x_j and the set $\mathcal{Y}_j$ as

$$\delta(x_j, \mathcal{Y}_j) = \begin{cases} 0, & \text{if } x_j \in \mathcal{Y}_j; \\ 1, & \text{otherwise.} \end{cases} \tag{7}$$

We define the Hamming distance between the sequence $\boldsymbol{x} = (x_1, x_2, \ldots, x_N)$ and the set $\mathcal{Y}$ as

$$d_H(\boldsymbol{x}, \mathcal{Y}) = \sum_{j=1}^{N} \delta(x_j, \mathcal{Y}_j). \tag{8}$$

We define a **T-traceability code** against the new collusion attack.

Definition 4 (T-Traceability Code) For a set of colluders $\mathcal{S}$ such that $|\mathcal{S}| \leq T$ and any $u_j \in \Gamma \setminus \mathcal{S}$, if there is at least one colluder $u_i \in \mathcal{S}$ satisfying

$$d_H(\boldsymbol{c}_i, \mathcal{Y}) < d_H(\boldsymbol{c}_j, \mathcal{Y}), \tag{9}$$

then the code $\mathcal{C}$ is called the **T-traceability (TA) code**. □

A T-TA code enables us to detect at least one colluder in $\mathcal{S}$ by simply calculating the Hamming distance if we obtain each symbol in $\mathcal{Y}_j$ for $j = 1, 2, \ldots, N$. This definition is analogous to T-TA codes against the interleaving attack [6, 7].

We will propose a T-TA code against the new collusion attack defined in Definition 3. The proposed T-TA code is constructed based on the following two

steps: (1) Each fingerprint is obtained from a codeword of a q-ary (N, K, D) linear error-correcting (EC) code of the length N, the number of information symbols K and the minimum distance D [5]. (2) The q symbols in each position of the q-ary (N, K, D) EC code are mapped into another integer set $\mathcal{I}(q)$. This code can be regarded as a **concatenated code** with a q-ary (N, K, D) outer code and an inner code of size q.

3.2 Inner Code Construction

In this subsection, we describe the methods for constructing an inner code of the concatenated fingerprinted code. First, we define the following set of integers.

Definition 5 Let $\mathcal{D}(q, t_1, t_2)$ be a set of q integers such that all sums of any t_1 or fewer distinct elements (allowing for each element to be repeated at most t_2 times) are distinct. If we take repeated elements into account, the maximum number of chosen elements is $t_1 t_2$. We call this set $\mathcal{D}(q, t_1, t_2)$ the (q, t_1, t_2)**-sum distinct (SD) set**. □

This definition for the (q, t_1, t_2)-SD set differs from that in [4], where the repetitions of an element are not allowed.

Definition 6 Let $\mathcal{A}(q, t_1, t_2)$ be a set of q integers such that all averages of any t_1 or fewer elements (allowing for each element to be repeated at most t_2 times) are distinct. If we take repeated elements into account, the maximum number of chosen elements is t_1. We call this set $\mathcal{A}(q, t_1, t_2)$ the (q, t_1, t_2)**-average distinct (AD) set**. □

The average of t_1 or fewer elements (allowing each element be repeated at most t_2 times) in a (q, t_1, t_2)-AD set is equal to that of other t_1 or fewer distinct elements (allowing each element be repeated at most t_2 times) in the (q, t_1, t_2)-AD set if and only if two subsets of the (q, t_1, t_2)-AD set are equal. For example, for a set $\{v_1, v_2, \ldots, v_\tau\}, \tau \leq t_1/2$, the set in which each element of $\{v_1, v_2, \ldots, v_\tau\}$ is chosen exactly twice gives the same average value. We regard that these sets are essentially equal.

[Construction 1]

We here propose a method for constructing (q, t_1, t_2)-AD. We call this method **Construction 1**. We show the following lemma and proposition.

Lemma 1 Define $\mathcal{E}(q, t) = \{t^j | j = 0, 1, \ldots, q-1\}$ and $b = t^{q-1} - 1$. Let $\mathcal{B}(q, t) = \{b\} \cup \{b - x | x \in \mathcal{E}(q-1, t)\}$. Then the set $\mathcal{B}(q, t)$ is a $(q, t-1, t-1)$-SD set.

(**Proof**) We first show that the set $\mathcal{E}(q, t)$ is a $(q, t-1, t-1)$-SD set. It is straightforward to show

$$a_0 + a_1 t + a_2 t^2 + \cdots + a_{j-1} t^{j-1} < t^j \tag{10}$$

where integers a_i satisfy $0 \leq a_i < t$ for $i = 0, 1, \ldots, j-1$. Therefore, all sums of any $t-1$ or fewer distinct elements from $\{1, t, t^2, \ldots, t^{j-1}\}$ (allowing for each element to be repeated at most $t-1$ times) are less than t^j.

Assume that a sum of μ elements $\{t^{i_1}, t^{i_2}, \ldots, t^{i_\mu}\}$ is equal to that of ν elements $\{t^{j_1}, t^{j_2}, \ldots, t^{j_\nu}\}$ such that $\mu < t, \nu < t$. i.e., we have

$$a_1 t^{i_1} + a_2 t^{i_2} + \cdots + a_\mu t^{i_\mu} = b_1 t^{j_1} + b_2 t^{j_2} + \cdots + b_\nu t^{j_\nu}$$

where a_i and b_j are integers such that $0 \leq a_i < t$ and $0 \leq b_j < t$ for all i and j. Therefore, if $i_\mu > j_\nu$, then the left-hand side is greater than the right-hand side from eq. (10). Otherwise, the right hand side is greater than the left-hand side. Hence, the set $\mathcal{E}(q,t)$ is a $(q, t-1, t-1)$-SD set.

From the fact that $\mathcal{E}(q,t)$ is a $(q, t-1, t-1)$-SD set, we can readily show that the set $\mathcal{B}(q,t)$ is also a $(q, t-1, t-1)$-SD set. □

The (q,t,t)-SD set by Lemma 1 is similar to a $(q,t,1)$-SD set by D. B. Jevtić [4] which does not allow repetitions of elements.

Proposition 1 A $(q, t_1, t_1 t_2)$-SD set is a (q, t_1, t_2)-AD set.

(**Proof**) See Appendix A. □

From Proposition 1, the following result is immediate.

Corollary 1 A $(q, t_1 t_2, t_1 t_2)$-SD set is a (q, t_1, t_2)-AD set. □

As we will see in Sect. 3.3, we want to obtain the inner code from a (q, T, T)-AD set to construct a concatenated T-TA code. By Corollary 1, the (q, T, T)-AD set is equal to (q, T^2, T^2)-SD set if we use Construction 1. The rate of an inner code given by Construction 1 is

$$R_{in}^{(1)} = \frac{\log_{T^2+1} q}{q-1} \tag{11}$$

(Note that the (q, T^2, T^2)-SD set by Construction 1 is a Q-ary integer set of the size q such that $Q = (T^2+1)^{q-1}$).

[Construction 2]

We propose another construction method of a (q, t_1, t_2)-AD set. We call this method **Construction 2**. We use the parity check matrix of a binary linear EC code. Consider a (n, k, d) linear code $\mathcal{C}_{in}$ with the parity check matrix H. The parity check matrix H of size $(n-k) \times n$ has the following property [5]: Let $t = \lfloor \frac{d-1}{2} \rfloor$, then any $2t$ columns of H are linearly independent over $GF(2)^{n-k}$. Letting $\boldsymbol{h}_i = (h_{i,1}, h_{i,2}, \ldots, h_{i,n-k})^{\mathrm{T}} \in \{0,1\}^{n-k}$ denote the i-th column of H where T denotes the transpose of a vector. sets of any t columns $\{\boldsymbol{h}_{i_1}, \boldsymbol{h}_{i_2}, \ldots, \boldsymbol{h}_{i_t}\}$ and $\{\boldsymbol{h}_{j_1}, \boldsymbol{h}_{j_2}, \ldots, \boldsymbol{h}_{j_t}\}$ satisfy

$$\boldsymbol{h}_{i_1} \oplus \boldsymbol{h}_{i_2} \oplus \cdots \oplus \boldsymbol{h}_{i_t} \neq \boldsymbol{h}_{j_1} \oplus \boldsymbol{h}_{j_2} \oplus \cdots \oplus \boldsymbol{h}_{j_t} \tag{12}$$

where $\oplus$ denotes the exclusive OR operation.

We show the following theorem.

Lemma 2 Consider the mapping $w_{t,p}$ $(p \leq 1)$ such that

$$w_{t,p} : GF(2)^{n-k} \to \left\{0, 1, 2, \ldots, (tp+1)^{n-k-1} - 1\right\} \tag{13}$$

defined as

$$w_{t,p}(\boldsymbol{h}_i) = \sum_{j=1}^{n-k} (tp+1)^{j-1} h_{i,j} \tag{14}$$

where $\boldsymbol{h}_i$ is the i-th column of the parity check matrix H of a binary (n, k, d) EC code. Then the set $\mathcal{W} = \{w_{t,p}(\boldsymbol{h}_1), w_{t,p}(\boldsymbol{h}_2), \ldots, w_{t,p}(\boldsymbol{h}_n)\}$ is a (n, t, p)-SD set if $p \geq 1$.

(**Proof**) We first show that if eq. (12) holds, then

$$\sum_{\nu=1}^{t} \boldsymbol{h}_{i_\nu} \neq \sum_{\nu=1}^{t} \boldsymbol{h}_{j_\nu} \tag{15}$$

where the summation is carried out in real numbers. Assume that $\sum_{\nu=1}^{t} \boldsymbol{h}_{i_\nu} = \sum_{\nu=1}^{t} \boldsymbol{h}_{j_\nu}$. Then if we take module 2 operation for the both sides, we have $\sum_{\nu=1}^{t} \boldsymbol{h}_{i_\nu} (\mathrm{mod}\ 2) \equiv \sum_{\nu=1}^{t} \boldsymbol{h}_{j_\nu} (\mathrm{mod}\ 2)$ and this contradicts that any $2t$ or fewer columns of H are linearly independent over $GF(2)^{n-k}$. Hence, eq. (15) holds.

Obviously, the mapping $w_{t,p}$ is isomorphism for $p \geq 1$. If any sum of t or fewer columns of H is not equal to that of other t or fewer columns of H, any sum of t or fewer elements of $\mathcal{W}$ is not equal to that of other t or fewer elements of $\mathcal{W}$. Even if an element is repeatedly chosen less than p times and the total number of elements (allowing repetition) is less than $tp + 1$, we can show all sums are distinct. This indicates that the set $\mathcal{W}$ is a (n, t, p)-SD set. □

Note that we can construct a (n, t, p)-AD set from a (n, t, tp)-SD set by Proposition 1.

As we will see in Sect. 3.3, we want to obtain the inner code from a (q, T, T)-AD set to construct a concatenated T-TA code. By Proposition 1, the (q, T, T)-AD set is given by a (q, T, T^2)-SD set if we use Construction 2. If we use the parity check matrix of a T-error correcting (n, k, d) BCH code as H, then $n = 2^m - 1$ and $n - k = Tm$ for a given m [5]. In this case, the rate of the inner code is given by

$$R_{in}^{(2)} = \frac{\log_{T^3+1}(2^m - 1)}{Tm} = \frac{\log_2(2^m - 1)}{Tm(\log_2 T^3 + 1)}. \tag{16}$$

This rate satisfies

$$\frac{m-1}{Tm \log_2(T^3+1)} < R_{in}^{(2)} < \frac{1}{T \log_2(T^3+1)}. \tag{17}$$

Therefore,

$$R_{in}^{(2)} \to \frac{1}{T \log_2(T^3+1)}, \quad \text{as } m \to \infty. \tag{18}$$

We may use combinatorial methods for constructing (q, t_1, t_2)-AD sets. For example, block designs, Latin squares or orthogonal arrays are used for the parity-check matrix of a low-density parity check codes which are instances of linear EC codes.

3.3 Concatenated Fingerprinting Code

As mentioned in Sect. 3.1, we use a q-ary (N, K, D) EC code as an outer code. We first let each codeword of the q-ary (N, K, D) outer code correspond to each user in Γ. Then we uniquely map q symbols of the outer code into each element of a (q, T, T)-AD set and this gives the q-ary concatenated fingerprinting code $\mathcal{C}$.

We here mention the decoding process for the illegal fingerprint $\boldsymbol{y}$. We first calculate the sets $\mathcal{Y}_j$ for $j = 1, 2, \ldots, N$ where this procedure corresponds to decoding of the inner code. We can correctly detect the sets $\mathcal{Y}_j$ such that $|\mathcal{Y}_i| \leq T$ since the inner code is constructed from a (q, T, T)-AD set. After decoding of the inner code, we perform decoding of the outer code. This procedure is carried out by calculating the Hamming distance for any $\boldsymbol{c}_i \in \Gamma$ and the set $\mathcal{Y}$. If the concatenated fingerprinting code is a T-TA code, we can correctly detect at least one colluder $u_i \in \mathcal{S}$ which has the nearest codeword from the set $\mathcal{Y}$.

We show a condition for the outer (N, K, D) code to give a T-TA code as follows.

Theorem 1 Assume that we use a (q, T, T)-AD set as the inner code and a q-ary (N, K, D) code such that

$$D \geq N\left(1 - \frac{1}{T^2}\right) \tag{19}$$

as the outer code. Then, the fingerprinting code is a T-TA code.

(**Proof**) The proof is analogous to the case of the codes against the interleaving attack [6, 8]. □

The condition $D \geq N(1 - \frac{1}{T^2})$ is simply derived from a T-TA code against the interleaving attack. Actually this condition is identical to that for the T-TA codes against the interleaving attack [6, 8].

From Theorem 1, if a fingerprint $\boldsymbol{c}_i$ satisfies

$$d_H(\boldsymbol{c}_i, \mathcal{Y}) \leq N - T(N - D), \tag{20}$$

then the user u_i is a one of colluders. Eq. (20) is a criterion for user u_i to be judged as a colluder.

Note that by Singleton's bounds, the minimum distance of a linear code satisfies $D \leq N - K + 1$. Since it is desirable for the minimum distance D to be as large as possible, we use the Reed-Solomon code (an instance of the maximum distance separable (MDS) codes) [5] satisfying $D = N - K + 1$ and $N = q - 1$ as an outer code by letting q be a prime power.

The total rate of the proposed code is given by

$$R^{(1)} = \frac{K}{N} R_{in}^{(1)} = \frac{K \log_{T^2+1}(N+1)}{N^2} \tag{21}$$

from eq. (11) for Construction 1 of the inner code, and

$$R^{(2)} = \frac{K}{N} R_{in}^{(2)} = \frac{K \log_{T^3+1}(N+1)}{NTm} \tag{22}$$

from eq. (16) for Construction 2 of the inner code.

4 Discussion

4.1 Method for Increasing Rate

Note that the total code rate of the proposed T-TA code strongly depends on the rate of an inner code which might be very low. We can increase the code rate if we permit detection error of some symbols of an inner code. Assume that we use a (q, T, s)-AD set such that $1 \leq s \leq T$ as the inner code. In this case, if there are some symbol positions in which a certain symbol is averaged more than s times, then symbols of these positions are not correctly detected in decoding of the inner code.

Theorem 2 Assume that we use a (q, T, s)-AD set such that $1 \leq s \leq T$ as the inner code and a q-ary (N, K, D) code such that

$$D \geq N \left(1 - \frac{1}{T^2 + \beta(s)T + \beta(s)}\right) \tag{23}$$

as the outer code where we define $\beta(s) = \lceil \frac{T-s}{s} \rceil$. Then, the fingerprinting code is a T-TA code. In this case, the total rate of the proposed T-TA code can achieve

$$R^{(1)}(s) = \frac{K \log_{Ts+1}(N+1)}{N^2} = \frac{\log_T(T^2+1)}{\log_T(Ts+1)} R^{(1)} \tag{24}$$

for Construction 1 of the inner code, and

$$R^{(2)}(s) = \frac{K \log_{T^2 s+1}(N+1)}{NTm} = \frac{\log_T(T^3+1)}{\log_T(T^2 s+1)} R^{(2)} \tag{25}$$

for Construction 2 of the inner code.

(**Proof**) See appendix B. □

It is obvious that the function $R^{(1)}(s)$ decreases as s increases within the range $1 < s < T$ since

$$R^{(1)}(s+1) - R^{(1)}(s) < 0. \tag{26}$$

for $1 < s < T$. Therefore, $R^{(1)}(T) = R^{(1)}$ and $R^{(1)}(s) > R^{(1)}$ for $1 \leq s < T$. In terms of the code rate, it is desirable for s to be as small as possible. i.e., the case $s = 1$ might be the optimal one. On the other hand, the condition on the minimum distance of the outer code becomes strict as s decreases (See Appendix C). As for the case with Construction 2, we can discuss in the same way and we have $R^{(2)}(T) = R^{(2)}$ and $R^{(2)}(s) > R^{(2)}$ for $1 \leq s < T$.

Corollary 2 Assume that we use a $(q, T, 1)$-AD set as the inner code and a q-ary (N, K, D) code such that

$$D \geq N\left(1 - \frac{1}{2T^2}\right) \tag{27}$$

as the outer code. Then, the fingerprinting code is a T-TA code. In this case, the total rate of the concatenated code is

$$R^{(1)}(1) = \frac{\log_T(T^2+1)}{\log_T(T+1)} R^{(1)} \tag{28}$$

from eq. (24) for Construction 1 of the inner code, and

$$R^{(2)}(1) = \frac{\log_T(T^3+1)}{\log_T(T^2+1)} R^{(2)} \tag{29}$$

from eq. (25) for Construction 2 of the inner code. □

4.2 Capability for Detecting More Colluders

We here discuss that a condition for detecting more than one colluders. For the case that the cardinalities $|\mathcal{S}_j|$ for $1 \leq j \leq N$ are greater than or equal to a certain constant (say, τ), we have the following result.

Proposition 2 Assume that we use a (q, T, s)-AD set such that $1 \leq s \leq T$ as the inner code and a q-ary (N, K, D) code satisfying eq. (23) as the outer code. If $|\mathcal{S}_j| \geq \tau$ such that $1 \leq \tau \leq T$ for all j, then there are at least τ colluders $u_i \in \mathcal{S}$ satisfying eq. (9). □

Proposition 2 indicates that we can detect at least τ colluders correctly when $|\mathcal{S}_j| \geq \tau$ for $j = 1, 2, \ldots, N$. Even in this case, we do not falsely detect innocent users' fingerprints. Since the case $|\mathcal{S}_j| = 1$ for $j = 1, 2, \ldots, N$ corresponds to the interleaving attack, the proposed code can guarantee at least one colluder against the interleaving attack. The case that $|\mathcal{S}_j| = |\mathcal{S}|$ for $j = 1, 2, \ldots, N$, corresponds to the averaging attack, and we can detect all colluders in this case.

Even if the cardinalities of the sets $\mathcal{S}_j$ in some symbol positions are less than τ, it is desirable to capture more than or equal to τ colluders. We show the following theorem.

Theorem 3 Assume that at least $N-\eta$ symbol positions satisfy $|\mathcal{S}_j| \geq \tau$. If the T-TA code is obtained from a (q,T,T)-AD set as the inner code and a q-ary (N,K,D) code such that

$$D \geq N\left(1-\frac{1}{T^2}\right)+\frac{\eta}{T^2}, \tag{30}$$

as the outer code, we can detect more than τ colluders correctly.

(**Proof**) Fingerprints of at least τ colluders $u_i \in \mathcal{S}$ share more than $(N-\eta)/T$ symbols with $\mathcal{Y}$. On the other hand, fingerprints of any $u_j \in \Gamma \setminus \mathcal{S}$ share at most $T(N-d)$ symbols with the set $\mathcal{Y}$ because they share at most $(N-d)$ symbols with each fingerprint $\boldsymbol{c}_i$, $u_i \in \mathcal{S}$. Therefore, we have

$$d_H(\boldsymbol{c}_i,\mathcal{Y})-d_H(\boldsymbol{c}_j,\mathcal{Y}) = \frac{(N-\eta)}{T}-T(N-d) \tag{31}$$

$$= \frac{(N-\eta)-T^2(N-d)}{T} \tag{32}$$

$$> \frac{(N-\eta)-T^2N+T^2N(1-\frac{1}{T^2})+\eta}{T}=0. \tag{33}$$

Therefore, we have at least τ colluders $u_i \in \mathcal{S}$ satisfying $d_H(\boldsymbol{c}_i,\mathcal{Y}) < d_H(\boldsymbol{c}_j,\mathcal{Y})$ for any $u_j \in \Gamma \setminus \mathcal{S}$. By calculating the Hamming distance $d_H(\boldsymbol{c}_i,\mathcal{Y})$, we can correctly detect at least τ colluders. □

5 *T*-TA Code against Segment-by-Segment Collusion Attack

In [3], He and Wu consider the interleaving attack segment by segment. In this section, we consider a segment-by-segment collusion attack.

Consider the case that we map each symbol of the outer code to a binary sequence $\boldsymbol{b}=(b_1,b_2,\ldots,b_\gamma)$ of the length γ uniquely. This fingerprinting code is a binary code of the length $N\gamma$. We regard this binary sequence of the length γ as a **segment**. For a codeword $\boldsymbol{c}_i=(c_{i,1},c_{i,2},\ldots,c_{i,N})$, we assume a symbol $c_{i,j}$ represents a j-th symbol segment of $\boldsymbol{c}_i$ (i.e., $c_{i,j}$ is a binary vector of length γ). Also, for an illegal fingerprint $\boldsymbol{y}$, a symbol y_j represents a j-th symbol segment of $\boldsymbol{y}$.

In this section, we assume the following collusion attack.

Definition 7 (Collusion Assumption)

When the colluders create the j-th symbol segment of $\boldsymbol{y}$, they select a subset of the j-th symbols segment of colluders' fingerprints. The all segments in the selected subset are averaged and the averaged value is set to the j-th symbol of $\boldsymbol{y}$. i.e., denoting the set of selected users' indexes by $\mathcal{S}'_j$, we have

$$y_j = \frac{1}{|\mathcal{S}'_j|}\sum_{u_i \in \mathcal{S}'_j} \boldsymbol{c}_{i,j} \tag{34}$$

where the summation is carried out in real numbers. □

In the case of the segment-by-segment collusion attack, we have a different result about the rate of an inner code from symbol-by-symbol collusion attack.

The binary inner code is obtained from the AD set by Construction 1. If each element of $\mathcal{B}(q,t)$ is represented by t-ary representation, each element is expressed as a binary vector of the length $\gamma = q-1$. We denote this set by $\mathcal{B}_{\rm b}(q,t)$. We can show this set of binary vectors $\mathcal{B}_{\rm b}(q,t)$ is a (q,t,t)-SD set of vectors. Therefore, the (q,t,t)-AD set of vectors is constructed from the (q,t^2,t^2)-SD set of vectors.

Consider we construct the inner code from the (q,T,T)-AD set by Construction 1. The rate of the inner codes is given by $R^{(1)}_{{\rm b},in} = (\log_2 q)/(q-1)$ since the code length is $q-1$ and the number of codewords is q. Remark that the rate is independent of T. The total rate of the concatenated code is

$$R^{(1)}_{\rm b} = \frac{K}{N} R^{(1)}_{{\rm b},in} = \frac{K \log_2 q}{N(q-1)}. \tag{35}$$

As in the previous sections, if we use a q-ary (N,K,D) Reed-Solomon code, $N = q-1$ and the rate $R^{(1)}_{\rm b}$ is expressed as

$$R^{(1)}_{\rm b} = \frac{K \log_2 (N+1)}{N^2}. \tag{36}$$

Next, we consider constructing a binary inner code from the AD set by Construction 2. We can show a (n,t,p)-AD set of binary vectors is given by a (n,t,tp)-SD set of binary vectors.

Consider we construct the inner code from the (q,T,T)-AD set by Construction 2. Since the (n,T,T^2)-SD set is constructed by the parity check matrix of a T-error correcting (n,k,d) EC code, the rate of the inner codes by Construction 2 is given by $R^{(2)}_{{\rm b},in} = (\log_2 n)/(n-k)$. If we use the BCH code, $n = 2^m - 1$ for some $m \geq 1$ and $n - k = Tm$. Then $R^{(2)}_{{\rm b},in} = (\log_2 2^m - 1)/Tm$. If we also use a q-ary (N,K,D) Reed-Solomon code, $N = q-1$ and the rate $R^{(2)}_{\rm b}$ is expressed as

$$R^{(2)}_{\rm b} = \frac{K}{N} R^{(2)}_{{\rm b},in} = \frac{K \log_2 (N+1)}{NTm}. \tag{37}$$

6 Conclusion and Future Works

In this paper, we discussed a new collusion attack model that includes well-known conventional collusion attacks for digital fingerprinting as a special case. We proposed a construction method of a T-TA code, which can detect at least one colluder, against the new collusion attack when the number of colluders is smaller than or equal to T. We discussed a method for increasing the rate of the T-TA code by allowing some detection error of symbols of the inner code. We also derived a condition for detecting more than one colluders.

As future works, we need to analyze properties of the proposed T-TA code in detail. We also need to derive upper-bounds of the number of codewords for given the code length N and the maximum size of the colluders T.

References

1. D. Boneh and J. Shaw: Collusion-secure fingerprinting for digital data. IEEE Trans. Inform. Theory **44** (1998) 1897–1905
2. B. Chor, A. Fiat, M. Naor, and B. Pinkas: Tracing traitors. IEEE Trans. Inform. Theory **46** (2000) 893–910
3. S. He and M. Wu: Improving collusion resistance of error correcting code based multimedia fingerprinting. Proc. of 2005 IEEE Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP'05) **2** (2005) 1029–1032
4. D. B. Jevtić: Disjoint uniquely decodable codebooks for noiseless synchronized multiple-access adder channels generated by integer sets. IEEE Trans. Inform. Theory **38** (1992) 1142–1146.
5. F. J. MacWilliams and N. J. A. Sloane: The Theory of Error-Correcting Codes. Amsterdam, The Netherlands: North-Holland (1977)
6. J. N. Staddon, D. R. Stinson, and R. Wei: Combinatorial properties of frameproof and traceability codes. IEEE Trans. Inform. Theory **47** (2001) 1042–1049
7. R. Safavi-Naini and Y. Wang: New results on frame-proof codes and traceability schemes. IEEE Trans Inform. Theory **47** (2001) 3029–3033
8. R. Safavi-Naini and Y. Wang: Sequential Traitor Tracing. IEEE Trans. Inform. Theory **49** (2003) 1319–1326
9. W. Trappe, M. Wu, Z. J. Wang, and K. J. R. Liu: Anti-collusion fingerprinting for multimedia. IEEE Trans. Signal Process. **51** (2003) 1069–1087
10. Z. J. Wang, M. Wu, H. V. Zhao, W. Trappe, and K. J. R. Liu: Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation. IEEE Trans. Image Process. **14** (2005) 804–821
11. C. Podilchuk and W. Zeng: Image adaptive watermarking using visual models. IEEE J. Select. Areas Commun. **16** (1998) 525–540

A Proof of Proposition 1

For $\nu \leq t_1$ and $\mu \leq t_1$, consider choosing ν elements $\{v_{i_1}, v_{i_2}, \ldots, v_{i_\nu}\}$ from a $(q, t_1, t_1 t_2)$-SD set and μ elements $\{v_{j_1}, v_{j_2}, \ldots, v_{j_\mu}\}$ from it by allowing any element is repeatedly chosen at most t_2 times. In this case, we restrict the total number of choices to at most t_1. We assume that the average of all elements of $\{v_{i_1}, v_{i_2}, \ldots, v_{i_\nu}\}$ is equal to that of all elements of $\{v_{j_1}, v_{j_2}, \ldots, v_{j_\mu}\}$. i.e., we have

$$\frac{1}{\nu}(v_{i_1} + v_{i_2} + \cdots + v_{i_\nu}) = \frac{1}{\mu}(v_{j_1} + v_{j_2} + \cdots + v_{j_\mu}) \tag{38}$$

and this is equivalent to

$$(\mu v_{i_1} + \mu v_{i_2} + \cdots + \mu v_{i_\nu}) = (\nu v_{j_1} + \nu v_{j_2} + \cdots + \nu v_{j_\mu}). \tag{39}$$

This equation indicates the sum of ν elements of $\{v_{i_1}, v_{i_2}, \ldots, v_{i_\nu}\}$ in which an element is repeatedly chosen at most $\mu \times t_2$ times is equal to that of μ elements of

$\{v_{j_1}, v_{j_2}, \ldots, v_{j_\mu}\}$ in which an element is repeatedly chosen at most $\nu \times t_2$ times. Since $\nu \leq t_1$ and $\mu \leq t_1$, this contradicts the assumption that the ν elements $\{v_{i_1}, v_{i_2}, \ldots, v_{i_\nu}\}$ and μ elements $\{v_{j_1}, v_{j_2}, \ldots, v_{j_\mu}\}$ are from a (q, t_1, t_1t_2)-SD set. Therefore, eq. (38) does not hold and this indicates that the (q, t_1, t_1t_2)-SD set is a (q, t_1, t_2)-AD set.

B Proof of Theorem 2

Since we use a (q, T, s)-AD set as the inner code, the detection errors occur at the positions in which a symbol is repeatedly chosen more than s times. Denoting the maximum number of blocks (of length $N - D$ symbols) which contains more than s repetitions by a, this a satisfies

$$0 < T - a(s + 1) + a \leq s. \tag{40}$$

Then we have $a = \lceil \frac{T-s}{s} \rceil = \beta(s)$ since the foregoing inequality leads to

$$\frac{T - s}{s} \leq a < \frac{T}{s}. \tag{41}$$

Therefore, if $T > s \geq 1$, we can correctly decode all symbols in at least $N - (N - D)\beta(s)$ symbol positions. Note that if $T = s$, we can correctly decode all symbols in N symbol positions. We have at least one colluder $u_i \in \mathcal{S}$ such that

$$d_H(\boldsymbol{c}_i, \mathcal{Y}) < N - \frac{N - (N - D)\beta(s)}{T} \tag{42}$$

since at least one colluder's fingerprint shares more than $\{N - (N - D)\beta(s)\}/T$ symbols with the set $\mathcal{Y}$. On the other hand, any user $u_j \in \Gamma \setminus \mathcal{S}$ satisfies

$$d_H(\boldsymbol{c}_j, \mathcal{Y}) \geq N - (N - D)T - (N - D)\beta(s) \tag{43}$$

$$= N - (N - D)(T + \beta(s)) \tag{44}$$

since it has at most $(N - D)$ symbols in common with each fingerprint in $\mathcal{S}$.

Assume that all colluders' fingerprints $\boldsymbol{c}_i$ satisfy $d_H(\boldsymbol{c}_i, \mathcal{Y}) \geq d_H(\boldsymbol{c}_j, \mathcal{Y})$ for a $u_j \in \Gamma \setminus \mathcal{S}$. Then this inequality is expanded as

$$N - \frac{N - (N - D)\beta(s)}{T} > N - (N - D)(T + \beta(s)). \tag{45}$$

Arranging this inequality, we have

$$N\left(1 - \frac{1}{T^2 + \beta(s)T + \beta(s)}\right) > D. \tag{46}$$

This contradicts the assumption of the theorem. Therefore, we have at least one colluder $\boldsymbol{c}_i \in \mathcal{S}$ satisfying eq. (9).

From the argument about the inner code, the code from a (q, T, s)-AD set has the rate $R_{in}^{(1)}(s) = (\log_{Ts+1} q)/(q-1)$ if the code is constructed by Construction 1. Since the rate of the outer code is $R_{out} = K/N$, we have

$$R^{(1)}(s) = R_{in}^{(1)}(s) R_{out} = \frac{K \log_{Ts+1} q}{N(q-1)} \tag{47}$$

Note that we can set $N = q - 1$, if we use the Reed-Solomon code which is an instance of the MDS codes. Therefore,

$$R^{(1)}(s) = \frac{K \log_{Ts+1}(N+1)}{N^2} \tag{48}$$

$$= \frac{K \log_T (N+1)}{N^2 \log_T (Ts+1)}. \tag{49}$$

Since the rate $R^{(1)}$ is given by eq. (21), we obtain eq. (24).

As for $R^{(2)}(s)$, we can derive the rate in the same way.

C Monotonicity of the Condition eq. (23)

On the condition eq. (23), we show the following proposition.

Proposition 3 Define $A(s) = T^2 + (T+1)\beta(s)$. Using $A(s)$, the right hand side of eq. (23) is expressed as $N(1 - 1/A(s))$. Then we have

$$N\left(1 - \frac{1}{A(s)}\right) \geq N\left(1 - \frac{1}{A(s+1)}\right) \quad \text{for } 1 \leq s < T. \tag{50}$$

i.e., the right hand side of eq. (23) is the greatest when $s = 1$.

(**Proof**) Obviously, eq. (50) holds if and only if

$$A(s) \geq A(s+1) \quad \text{for } 1 \leq s < T. \tag{51}$$

Arranging eq. (51), we obtain

$$A(s) - A(s+1) = (T+1)(\beta(s) - \beta(s+1)) \geq 0. \tag{52}$$

$\beta(s) - \beta(s+1) \geq 0$ holds if

$$\frac{T-s}{s} - \frac{T-(s+1)}{s+1} > 0, \quad \text{for } 1 \leq s < T. \tag{53}$$

Therefore, it suffices to show that eq. (53) holds. Actually, eq. (53) holds since

$$\frac{T-s}{s} - \frac{T-(s+1)}{s+1} = \frac{T}{s(s+1)} \tag{54}$$

and $1 \leq s < T$. It follows that eq. (50) holds. □

Proposition 3 indicates, the condition on the minimum distance of the outer code (eq. (23)) becomes strict as s decreases.