There has been a wide-ranging discussion on the issue of content copyright protection in digital content distribution systems. Fiat and Tassa proposed the framework of dynamic traitor tracing. Their framework requires dynamic computation transactions according to the real-time responses of the pirate, and it presumes real-time observation of content redistribution. Therefore, it cannot be simply utilized in an application where such an assumption is not valid. In this paper, we propose a new scheme that provides the advantages of dynamic traitor tracing schemes and also overcomes their problems.

**key words:** dynamic traitor tracing, watermarking, digital rights management, content distribution

1. Introduction

There are a lot of approaches to protect content copyrights in content distribution services. Watermarking is one of the most important primitives of these approaches and a lot of methods employ it. The framework of dynamic traitor tracing proposed by Fiat and Tassa is one of these methods. It assigns each user to a certain subset in order to trace illegal redistributors (traitors) dynamically in real time according to the illegally redistributed content. Dynamic subset assignment enables tracers to obtain the most useful information to trace traitors according to the traitors’ strategy. However, it needs a real-time feedback channel, and thus a delayed attack, which redistributes content with some delay, is effective against it. As the above implies, dynamic traitor tracing is not a practical protection scheme. Our goal is to develop a new traitor tracing scheme that has the advantages of dynamic traitor tracing and fewer of its shortcomings.

1.1 Background

In recent years, the bandwidth available for Internet access has become wider, personal computers have become widespread, and high-density storage media such as DVDs and memory sticks have become inexpensive. As a result, audio and video content can now be easily distributed in digital form, but they can also be copied and redistributed illegally. For example, episodes of serial TV dramas can be illegally uploaded on Internet websites after they were broadcast. The users who did the uploading would face no penalty, since no tracing countermeasures are undertaken. Copyright holders such as broadcasting companies are becoming increasingly concerned about such violations of copyright. Copyright protection has become a major issue in content distribution services.

1.2 Related Works

**Traitor Tracing.** Traitor tracing is one of the major schemes for protecting copyrighted works. In a system, a content provider encrypts content and distributes it, and each user decrypts it with his/her decryption key, which is distributed prior to the service. Each user’s decryption key is unique, so if the user illegally redistributes the decryption key, it is possible to identify the decryption key’s owner [4], [5], [8], [13], [15]. However, these traitor tracing schemes cannot protect the decrypted content from illegal copying.

**Watermarking.** One sort of countermeasure is watermarking. A simple watermarking scheme works as follows [3], [21]. The content provider produces different contents and distributes them to users. These contents are generated from a single original, but their embedded information is different. Effectively then, each user gets content that is different from any other user’s content. Unfortunately, as part of a broadcasting service, this scheme requires a network capacity in proportion to the number of users and thus is not practical. Moreover, the scheme is ineffective against a collusion attack, whereby authorized users collude to make other content whose embedded information is not the same as any of the content they receive.

**C-secure Code.** There are approaches for creating code [6], [7], [20], called c-secure code. Using c-secure code as embedded information, one can specify at least one of up to c colluding attackers. Unfortunately, its code length is very long even if c is relatively small.

**Dynamic Traitor Tracing.** Fiat and Tassa assume that con-
tent is redistributed in real time and that it is possible to get the redistributed content in real time [10], [11]. Berkman, Parnas, and Sgall improved Fiat and Tassa’s scheme [1], [2]. In this case, the system must dynamically assign codes in real time soon after getting the redistributed content, and this enables one to identify traitors at a lower network cost compared with a static scheme such as c-secure code. Such schemes are called dynamic traitor tracing (DTT).

However, DTT has some shortcomings. One is that it must get redistributed content in real time. This means a real-time feedback channel is required. The other shortcoming is that a real-time dynamic watermark assignment is required, which implies that the CPU cost of the watermark assignment server is extremely high. Moreover, there is an effective attack whereby content is redistributed with some delay. That is, since the content provider gets redistributed content with some delay, it is hard for it to assign watermarks dynamically.

Sequential Traitor Tracing. Safavi-Naini and Wang proposed another approach to solve these problems, called sequential traitor tracing (STT) [18], [19]. In this scheme, even if there are no traitors, it is necessary to distribute multiple contents, and the number of contents is in proportion to the number of traitors whom the content provider assumes to be colluding and to redistribute content. Hence, the scheme’s network cost is high. However, a real-time dynamic watermark assignment is not required, which implies that the CPU cost of the watermark assignment server is low.

The above discussion illustrates that while DTT and STT are effective ways of tracing traitors, they do not meet all of the requirements for copyright protection.

1.3 Our Contribution

Our goal is to develop a new scheme that has the advantages of DTT but fewer of its shortcomings; we call it trade-off traitor tracing.

In our scheme, several segments are stored and the watermarks embedded into them are detected. Then, the subsequent pattern of watermarks embedded into several consecutive segments is determined after analyzing the detected watermarks pattern and with one dynamic computation. The determination must be made in a way that the information obtained from the watermarks detected in these consecutive segments works most effectively to identify traitors. This method is robust against delayed attacks [18], [19].

(1) Comparison with DTT

Consider a likely scenario in which attackers try to redistribute a serial drama episode the day after it was broadcast. The conventional scheme would not work in this case, but ours would. Say that an episode is broadcast every day. The attackers perform delayed attacks and illegally redistribute the $j$th episode the next day. The tracers, who would like to identify the attackers, determine the watermark patterns in the $j + 1$th episode broadcast once they notice that this episode has been illegally redistributed. In the case of DTT, only one new watermark pattern is determined for the next episode. On the other hand, in our scheme, one episode is divided into multiple segments (two segments in the following construction to make it easier to assess the performance of our scheme), and a distinct watermark pattern is assigned to each segment. This means one episode is considered to be one segment in DTT, but multiple (two) segments in our scheme. When the tracers find the next illegal redistribution of the $j + 1$th episode, they can decrease the set of users that includes the attackers to 1/2 in DTT and to 1/4 in our scheme. Hence, our scheme is more robust than DTT against delayed attacks.

Moreover, the computational cost (the number of dynamic watermark assignments needed to trace all traitors) of our proposal is less than that of DTT. Table 1 shows a comparison with the schemes of [1], [2], [10], [11], when the number of segments $t$ is two ($t = 2$) and the number of watermark variants to identify one traitor $\alpha$ is three ($\alpha = 3$). The comparison shows that our proposal can decrease the number of dynamic computations to about 79% ($= \log_3 3 = (p \log_4 n)/(p \log_3 n)$), where $p$ is the number of traitors and $n$ is the total number of users ($p \ll n$).

<table>
<thead>
<tr>
<th>Scheme</th>
<th>[10], [11]</th>
<th>[1], [2]</th>
<th>[18], [19]</th>
<th>Ours</th>
</tr>
</thead>
<tbody>
<tr>
<td>DA-security</td>
<td>-</td>
<td>-</td>
<td>$\sqrt{\text{Ours}}$</td>
<td>$\sqrt{\text{Ours}}$</td>
</tr>
<tr>
<td># DC</td>
<td>$p(\log_2 n + 1)$</td>
<td>$p(\log_3 n + 1)$</td>
<td>1†</td>
<td>$\max(p(\log_4 n/p + 4) - 3, p(\log_4 n + 1))$</td>
</tr>
<tr>
<td># Var†</td>
<td>$2p + 1$</td>
<td>$3p + 1$</td>
<td>$\max(1 + \sqrt{2n}, 2p^2 + 2p - 3)$</td>
<td>$3p + 1$</td>
</tr>
</tbody>
</table>

(2) Comparison with STT

Our scheme’s network cost is lower than STT’s [18], [19]. More precisely, even if there is only one traitor, STT always requires the tracer to distribute multiple contents, and the number of such contents $q_{STT}$ increases with the number of traitors $p'$ that the tracer assumes to be colluding. It remarks that $p' \geq p$, and roughly speaking, $q_{STT} = \max(1 + \sqrt{2n}, 2p^2 + 2p - 3)$. On the other hand, in our

—–

†Our scheme has intermediate performance between STT and DTT in terms of network and CPU costs, and that is why we call it “trade-off” traitor tracing.
scheme, if the number of contents to identify one traitor is $\alpha$ and if there is only one traitor, only $\alpha + 1$ contents are distributed. If two or more traitors exist, the number of distributed contents changes gradually and the maximum number is $q_{\text{ours}} = \alpha \cdot p + 1$. For $\alpha = 3$, $q_{\text{ours}} = 3p + 1$, and $\max(1 + \sqrt{2n}, 2p^2 + 2p - 3)$ is more than $3p + 1$ in almost all cases. Hence, STT’s network cost is almost always higher than ours.

STT does not employ any dynamic computations; it employs only one static computation. That is, once the distributed variants to each user are determined, the variants are not changed until all $p$ traitors are identified. Thus, STT has a small CPU cost for dynamic computations, and it needs only one static computation to identify all $p$ traitors. However, its large network cost offsets this saving. Table 1 also summarizes a comparison with the schemes of [18], [19].

2. Model: Trade-off Traitor Tracing

In some content distribution systems, any user can become a traitor who illegally redistributes his/her received content. In addition, any countermeasure to trace the traitor is currently not undertaken as described in Sect. 1.1, so the traitor can freely redistribute the content. When some kinds of countermeasures will be undertaken, several traitors may collude and try to break the countermeasures, and such collusion is easy, since the traitors are connected through networks. Moreover, the traitors redistribute content during any time span, since they have storage to store the content. Trade-off traitor tracing scheme is one of countermeasures against such traitor’s illegal redistribution.

Our model is similar to that of DTT [10], [11] (we describe the model of DTT in Appendix A.1 and its construction and shortcomings in Appendices A.2 and A.3 briefly), but real-time content feedback is unnecessary. That is, the next watermark pattern is determined with adaptive and dynamic computations, depending on the watermark information extracted from illegally redistributed content, and we assume that the following traitors exist:

- Traitors redistribute content before a broadcaster (tracer) determines a pattern of watermarks embedded into the next content.

Actually, illegal redistribution of content often occurs soon after the content is broadcast, and there seems to be enough time to determine the next watermark pattern. For example, as mentioned in Sect. 1.1, an episode of a serial drama is illegally uploaded on Internet websites just after it was broadcast and the next episode will be broadcast tomorrow or one week later. One day or one week remains to determine the next pattern and it is enough time. Thus, the assumption holds in almost all cases.

Content providers distribute content, and then traitors redistribute it illegally. The providers can see the redistributed content through a feedback channel. One piece of content consists of multiple segments, and multiple variants are generated for each segment. Distinct information is embedded in each variant. In addition, the set of users is divided into subsets, and each variant is distributed to each subset. In this process, several current segments are stored and the watermark information is detected. Then, as shown in Fig. 1, the detected watermark pattern is used to determine the next pattern, which would be embedded in the subsequent segments. That is, users are dynamically assigned to distinct subsets for each segment at a particular timing. On the other hand, DTT assigns users to the same subsets for all segments.

With this modification, the computational cost can be decreased and delayed redistribution attacks can be thwarted. In the following sections, we describe the details of our model by using the notation in Table 2.

2.1 Content Structure

Figure 2 shows the content structure of our model. This structure is the same as in DTT. One piece of content is divided into several consecutive segments. In the case of video content, for example, one piece of video content is divided into minute-long segments. We assume that a watermarking scheme exists such that no detection error occurs for any attack (we call it an “ideal” watermarking scheme). Multiple
variants of one segment are generated with this watermarking scheme and the information embedded in each variant is different from the others. The following conditions are required for these variants:

- Fundamentally, all variants carry the same information to the extent that humans cannot easily distinguish between them.
- Given any set of variants of the jth segment (1 ≤ j ≤ m), \( v^j_1, \ldots, v^j_{\lambda(j)} \), it is impossible to generate another variant that can not be traced back to one of the original variants \( v^j_i \) (1 ≤ i ≤ \( \lambda(j) \)).

Clearly, assuming that there exists a watermarking scheme which meets the above requirements, it would be possible to identify at least one variant with illegally redistributed variants and prove that there is one traitor among the set of users who received the same variant with the identified variant.

2.2 Algorithms

Trade-off traitor tracing consists of two algorithms, WMK and TRC. WMK is the algorithm to embed watermarks. TRC is the algorithm to trace traitors who redistribute content illegally.

WMK: This is an algorithm which takes as inputs \( U \), \( t \) consecutive segments (from the \( j^\text{th} \) to \( j+t-1^\text{th} \) segments), and \( h \). It generates multiple variants \( v^j_k \) (1 ≤ k ≤ r) for all \( j \) segments (j ≤ i ≤ j+t-1). For all \( i \) and \( k \) (j ≤ i ≤ j+t-1, 1 ≤ k ≤ r), it determines the sets of users \( S^j_i \) and the variant \( v^j_k \) distributed to \( S^j_i \), updates the side information \( h \), and returns \( v^j_k, S^j_i \) and \( h \).

TRC: This is an algorithm which takes as inputs \( U \), the detected watermark information from \( t \) consecutive segments (from \( j^\text{th} \) to \( j+t-1^\text{th} \) segments), \( S^j_i \) (j ≤ i ≤ j+t-1, 1 ≤ k ≤ r), and \( h \), and returns the updated \( h \).

These two algorithms are used as follows. When the content is distributed, WMK generates multiple variants \( v^j_k \) (1 ≤ k ≤ r) for each segment \( i \) (j ≤ i ≤ j+t-1). If the content is subsequently found to have been illegally redistributed, the variants detected in the content, the user set information \( S^j_i \) (j ≤ i ≤ j+t−1, 1 ≤ k ≤ r), and information \( h \), which shows the relationship between the sets of users and the distributed variants, are inputted to TRC. TRC analyzes these data and reduces the number of suspicious users. It outputs \( h \), which includes information about new subsets from which to collect the most meaningful information. After that, WMK takes as inputs these new subsets and generates new variants \( v^j_k \) and sets \( S^j_k \) (1 ≤ k ≤ r) for the next \( t \) consecutive segments (j+1 ≤ i ≤ j+2t−1). This process is repeated until all traitors are identified.

3. Our Construction of Trade-off Traitor Tracing

Here, we show the construction of the trade-off traitor tracing scheme. Although the scheme is based on [10], [11], it is significantly different from these other schemes in regard to their strategy to identify traitors. That is, trade-off traitor tracing collects \( t \) consecutive segments and analyzes them simultaneously. Different user subsets are created for each segment, and this is the trick to get the most meaningful and most effective information.

On the other hand, direct use of the scheme described in [10], [11] is not effective, since the traitors can adaptively choose which segments to redistribute and thus the content provider (tracer) collects less information. That is, once a set of users is divided into subsets, the subsets are not changed until an illegal redistribution is found. One subset assignment is used for all segments, regardless of the number of segments. The traitors can thus follow a strategy in which they redistribute only the segments distributed to one subset.
This strategy is illustrated in Fig. 3. C denotes the set of users to which an illegal redistributed variant is distributed first, and \( C_\emptyset \) and \( \overline{C_\emptyset} \) denote subsets of C which are created by the tracer for the next distribution and to which different variants are distributed, e.g., two distinct variants \( \upsilon_1 \) and \( \upsilon_2 \) are distributed to \( C_\emptyset \) and \( \overline{C_\emptyset} \), respectively. At the time of the first content distribution, all of the traitors are in C, but at the time of the next distribution, traitors exist in both subsets \( C_\emptyset \) and \( \overline{C_\emptyset} \). Suppose that the traitors only in \( C_\emptyset \) redistribute the segments in that case. The traitors can select such segments, since they have storage and can analyze the segments. If the duration for storing content and analysis is less than the time that users can wait for, the illegal redistribution would become a viable service, and this attack would become effective since the tracer can only obtain information that the traitor is in one subset \( C_\emptyset \). That is, the traitors can choose segments such that the information that the tracer can collect from \( t \) consecutive redistributed segments is the same information obtained from one of the \( t \) segments.

### 3.1 Basic Strategy

The strategy to collect the most meaningful information to identify traitors from the variants of two segments is as follows. To simplify our explanation in the following, we set \( t \) to two \((t = 2)\) and the number of watermark variants to identify one traitor \( \alpha \) to three \((\alpha = 3)\), even though the larger these numbers are, the more effective our scheme becomes. Let C be the set of users who receive an illegal redistributed variant. Regarding the two segments that the content provider will distribute next, the provider makes four subsets of C, \( C_\emptyset, \overline{C_\emptyset}, C_\emptyset \) and \( \overline{C_\emptyset} \), where \( C_\emptyset \cup \overline{C_\emptyset} = C \), \( |C_\emptyset| = |\overline{C_\emptyset}| = |C_\emptyset| = |\overline{C_\emptyset}| = \frac{1}{4}|C| \), and \( |C_\emptyset \cap C_\emptyset| = |C_\emptyset \cap \overline{C_\emptyset}| = |\overline{C_\emptyset} \cap C_\emptyset| = |\overline{C_\emptyset} \cap \overline{C_\emptyset}| = \frac{1}{4}|C| \).

For the first segment, one variant is distributed to \( C_\emptyset \) and another variant to \( \overline{C_\emptyset} \). For the next segment, one is distributed to \( C_\emptyset \) and another to \( \overline{C_\emptyset} \). For example, two distinct variants of the first segment \( \upsilon_1 \) and \( \upsilon_2 \) are distributed to \( C_\emptyset \) and \( \overline{C_\emptyset} \), respectively, and two distinct variants of the second segment \( \upsilon_3 \) and \( \upsilon_4 \) are distributed to \( C_\emptyset \) and \( \overline{C_\emptyset} \), respectively. If, for example, the variants \( \upsilon_1 \) and \( \upsilon_2 \) assigned to \( C_\emptyset \) and \( C_\emptyset \) are found to be illegally redistributed, the following situations can be imagined:

(i) At least one traitor is in \( C_\emptyset \cap C_\emptyset \).

(ii) At least one of them is in \( C_\emptyset \cap \overline{C_\emptyset} \) and at least one of them is in \( \overline{C_\emptyset} \cap C_\emptyset \).

In particular, when only one traitor exists in C, (i) is true, and hence, one dynamic computation enables tracers to decrease the number of suspicious users to \( \frac{1}{4} \). Figure 4 illustrates the strategy. In contrast, the conventional traitor tracing scheme [10], [11] requires two dynamic computations to decrease the number to \( \frac{1}{4} \).

Realistically (and especially at the beginning of tracing), it is natural to suppose that multiple traitors exist in C. A decision such that (i) or (ii) is true may make it so that traitors can not be identified in the subsequent tracing process. Hence, a decision made from one piece of collected information is not likely to be effective, and we need another strategy to identify the true traitors.

The correct strategy is one in which the tracers set a high probability on (i) and they utilize a scheme (scheme-i) to identify traitors in \( C_\emptyset \cap C_\emptyset \). Simultaneously, for the case that (ii) is true, the tracers utilize another scheme (scheme-i) to identify traitors in \( (C_\emptyset \cap \overline{C_\emptyset}) \cup (\overline{C_\emptyset} \cap C_\emptyset) \). Concretely, scheme-i and scheme-ii are as follows:

**Scheme-i.** To investigate \( C_\emptyset \cap C_\emptyset \) in more detail when the next two segments are distributed, \( C_\emptyset \cap C_\emptyset \) is divided into
for example, suppose that three different variants $v^3_1$, $v^3_2$ and $v^3_3$ of the first segment of the next content are distributed to the subsets $C_{t_1}$, $C_{t_2}$ and $L'$, respectively, and three different variants $v^3_1$, $v^3_2$ and $v^3_3$ of the second segment of the next content are distributed to the subsets $C_{t_1}$, $C_{t_2}$ and $L'$, respectively. That is, $C_{t_1} \cap C_{t_2}$ is intensively investigated, since there is a strong chance that at least one traitor is in $C_{t_1} \cap C_{t_2}$. On the other hand, $(C_{t_1} \cap C_{t_2}) \cup (C_{t_3} \cap C_{t_4})$ is not intensively investigated, since there is not much of a chance of finding traitors in it. Moreover, $(C_{t_1} \cap C_{t_2})$ is checked off the list of suspects, since there is no chance of finding traitors in it, and it is added to the innocent subgroup $I$.

If (ii) is true, the scheme-ii works effectively and the tracers can get more information about the traitors than in the scheme-i. Concretely, if $v^3_2$ or $v^3_3$ is redistributed, the tracer can know at least two traitors exist. This information cannot be obtained by using only scheme-i. As a result, traitors cannot help but perform in the way in which (i) is true.

### 3.2 State Transitions of User Subsets

Our scheme has four states, State0 to State3, and seven transitions, Case1 to Case7. Figure 5 shows the state transition diagram. In the figure, the subsets for two segments are expressed in one object. $State_i-j$ denotes a Statei with an index $j$, where $j$ is only used to make a distinction from another Statei. In addition, we use the following variables:

- $\omega$: The fewest number of traitors who inevitably exist. $1 \leq \omega \leq p$.
- $I$: The set of users in which traitors have not been found.
- $C_l$ ($1 \leq l \leq \omega$): This is a set of users, in which a traitor is known to exist $l$th.
- $C_{t_1}, C_{t_2}, C_{t_3}, C_{t_4}, C_{t_5}, C_{t_6}, C_{t_7}$ (1 $\leq l \leq \omega$): These are sets of users such that $C_{t_1} \cup C_{t_2} = C_{t_3} \cup C_{t_4}$ and at least one traitor exists in $C_l$.
- $C_{t_1}', C_{t_2}', C_{t_3}', C_{t_4}', C_{t_5}', C_{t_6}', C_{t_7}'$ (1 $\leq l \leq \omega$): These are sets of users such that $C_{t_1}' \cup C_{t_2}' = C_{t_3}' \cup C_{t_4}'$ and $C_{t_1}'$ includes at least one traitor or $L_i$ includes at least two traitors.
- $C_{t_1}''$, $C_{t_2}''$, $C_{t_3}''$, $C_{t_4}''$ ($1 \leq l \leq \omega$): These are sets of users such that two sets among $C_{t_1}''$, $L_i''$, and $R_i''$ include at least one traitor.
- $\emptyset$: This is an empty set of users.

Roughly speaking, the subsets $C_l, C_{t_1}, C_{t_2}, C_{t_3}, C_{t_4}, C_{t_5}, C_{t_6}, C_{t_7}, C_{t_1}', C_{t_2}', C_{t_3}', C_{t_4}', C_{t_5}', C_{t_6}', C_{t_7}'$ are sets in which traitors seem likely to exist. The subset $L'$ is the set in which traitors seem not so likely to exist, but the probability is not 0. Tracers set the same probability in subsets $C_l''$, $L_i''$, $R_i''$.

We define State0 to State3 as follows:

- **State0**: The state in which there is only one subset $I$ or $C_l$.
- **State1**: The state in which there are four subsets $C_{t_1}, C_{t_2}, C_{t_3}, C_{t_4}, C_{t_5}, C_{t_6}, C_{t_7}$.
- **State2**: The state in which there are seven subsets $I, C_{t_1}, C_{t_2}, C_{t_3}, C_{t_4}, C_{t_5}, C_{t_6}, C_{t_7}$.
- **State3**: The state in which there are four subsets $I, C_{t_1}, C_{t_2}, C_{t_3}, C_{t_4}, C_{t_5}, C_{t_6}, C_{t_7}$.

Diagram. We define the transitions, Case1 to Case7, shown in the diagram. In the following, the pair $(A, B)$ denotes two subsets $A$ and $B$ that received the same variants with the illegally redistributed variants, where $A$ received the variant distributed with the first segment (the first segment of two consecutive segments) and $B$ received the variant distributed with the second segment (the second segment of two consecutive segments).

- **State0** is the state in which the set is $I$ or $C_l$. When illegal redistribution is detected in State0, the state changes into State1. This is **Case1** transition.
- When illegal redistribution is detected in State1, the state changes into State2. This is **Case2** transition.
- If illegal redistribution is detected in State2 and the detected subsets’ pair is one of $(C_{t_1}, C_{t_2}), (C_{t_3}, C_{t_4}), (C_{t_5}, C_{t_6}), (C_{t_7}, C_{t_8})$, the state changes into another State2. This is **Case3** transition. This state is different from the previous State2, in that the number of $|I|$ increases and the numbers of $|C_{t_1}'|$, $|C_{t_2}'|$, $|C_{t_3}'|$, $|C_{t_4}'|$, $|C_{t_5}'|$, $|C_{t_6}'|$, $|C_{t_7}'|$ decrease to $1/4$.
- If illegal redistribution is detected in State2 and the detected subsets’ pair is $(L_i, L_j)$, the state changes into State3. This is **Case4** transition.
- If illegal redistribution is detected in State2 and one of the detected subsets is $(C_{t_1}, C_{t_2}, C_{t_3}, C_{t_4}, C_{t_5}, C_{t_6}, C_{t_7})$ and the other is $L_i$, the state changes into one State0 and two State1s (State1-1 and State1-2). This is **Case5** transition. In this case, there are at least two traitors, and hence, $\omega$ is updated to $\omega = \omega + 1$. At least one of the traitors is in a subset $(C_{t_1} \cup C_{t_2} \cup C_{t_3} \cup C_{t_4} \cup C_{t_5} \cup C_{t_6} \cup C_{t_7})$ among $(C_{t_1}, C_{t_2}, C_{t_3}, C_{t_4}, C_{t_5}, C_{t_6}, C_{t_7})$, and at least one of them is in $L_i$. $C_{t_1}$ can be treated as $C_l$ in State0, and $L_i$ can be treated as $C_{t_1}$ in State0, where $\omega$ is the maximum number of $l$. Each of these states changes into State1.
- If illegal redistribution is detected in State3 and the detected subsets’ pair is one of $(C_{t_1}', C_{t_2}')$, $(L_i', L_j')$, $(R_i', R_j')$, the state changes into one State0 and two State1s (State1-1 and State1-2). This is **Case6** transition. In this case, there are at least two traitors, and hence, $\omega$ is updated to $\omega = \omega + 1$. At least one of the traitors is included in a subset $(L_i')$ among $(C_{t_1}', L_i', R_i')$, and at least one of them is included in a combined subset $(C_{t_1}' \cup R_i')$ in Fig. 5, which is generated.
by excluding the detected subset ($L''_i$ in Fig. 5) from the subset ($C''_i \cup L''_i \cup R''_i$). The detected subset ($L''_i$ in Fig. 5) can be treated as $C''_i$ in State0, where $\omega$ is the maximum number of $I$, the other subset ($C''_i \cup R''_i$ in Fig. 5) can be treated as $C_i$ in State0. Each of these states changes into State1.

- If illegal redistribution is detected in State3 and the detected subsets’ pair is one of ($('C'_i, 'R'_i)$, ($('C''_i, 'R''_i)$, ($('C''_i, 'R''_i)$, ($('C'_i, 'R'_i)$, ($('C''_i, 'R''_i)$, ($('C''_i, 'R''_i)$, ($('C''_i, 'R''_i)$, ($('C''_i, 'R''_i)$), the state changes into one State0 and two State1s (State1-1 and State1-2). This is Case7 transition. In this case, there are at least two traitors, and hence, $\omega$ is updated to $\omega = \omega + 1$.

As described above, the number of subsets for any segment of any state is less than or equal to three. For example, the number of subsets for the first segment of State1 is two ($C''_i$ and $C''_i$), the other subset ($C''_i \cup R''_i$ in Fig. 5) can be treated as $C_i$ in State0, where $\omega$ is the maximum number of $I$, and the other one ($C''_i$ in Fig. 5) can be treated as $C_i$ in State0. Each of these states changes into State1.

3.3 Full Description of Our Trade-off Traitor Tracing

Our scheme uses the following basic function $\text{Sub}$, and its basic strategy is to decrease the number of users in a set, which includes traitors, to 1/4.

$\text{Sub}$: It takes as inputs a set of users $X$, and returns four subsets of $X$: $X_o, \overline{X_o}, X_{\bar{o}},$ and $\overline{X_{\bar{o}}}$, where $X_o \cup \overline{X_o} = X_o \cup \overline{X_o} = X$, $|X_o| \approx |\overline{X_o}| \approx |X_{\bar{o}}| \approx |\overline{X_{\bar{o}}}| \approx \frac{1}{4}|X|$, $|X_o \cap X_{\bar{o}}| \approx |X_o \cap \overline{X_o}| \approx |X_{\bar{o}} \cap X_{\bar{o}}| \approx |X_{\bar{o}} \cap \overline{X_{\bar{o}}}| \approx \frac{1}{8}|X|$, and $X_o \cap \overline{X_o} = X_o \cap X_{\bar{o}} = X_{\bar{o}} \cap \overline{X_o} = \emptyset$.

In addition, the function $\text{Div2}$ is used, which is used in DTT [10], [11].

$\text{Div2}$: It takes as inputs a set of users $X$, and returns two subsets $L$ and $R$, where $L \cup R = X$, $|L| \approx |R| \approx \frac{1}{2}|X|$, and $L \cap R = \emptyset$.

Our scheme also uses the side information $h$ to identify traitors.
If \( (l, C_{\text{dir}}, C_{\text{sub}}) \) means that the set of all users is divided into three sets, \( I, C_{\text{dir}}, \) and \( C_{\text{sub}} \) and that each set of \( I, C_{\text{dir}}, \) and \( C_{\text{sub}} \) is set to one of different variants of a segment is distributed. \( P_0 \) denotes the \( P \) that includes only the following subsets, \( I, C_{\text{dir}}, C_{\text{sub}}, C_{\text{dir}}, C_{\text{sub}}, L'_1, C'_1, L'_2, R'_2 \) (1 \( \leq l \leq p \)). Similarly, \( P_0 \) denotes the \( P \) that includes only the following subsets, \( I, C_{\text{dir}}, C_{\text{sub}}, C_{\text{dir}}, C_{\text{sub}}, L'_1, C'_1, L'_2, R'_2 \) (1 \( \leq l \leq p \)). If \( \omega \) and \( P \) are given, the watermark information that is used to generate each variant of a segment is assigned to each subset of \( P \), and the variants that are to be distributed to each user are determined. Hence, we shall focus on how a content provider (tracer) updates \( P \). In our scheme, \( P_0 \) and \( P_\omega \) show the relationship between the variants of two consecutive segments and subsets of users. \( h \) includes \( \omega, P_0, P_\omega \) and the information about the relationship between the subset patterns and watermarks embedded into the variants.

**Our Construction.** Trade-off traitor tracing is performed with the algorithms WMK and TRC. WMK generates multiple variants of each segment and updates \( h \). TRC has seven cases. In each case, new subsets patterns for the next distribution are determined, the current subsets patterns are erased from \( P_0 \) and \( P_\omega \), and the new subset patterns are added to \( P_0 \) and \( P_\omega \). Basically, the idea is that the new subsets taken from the most suspicious subset are smaller than the current most suspicious subset, and new attributes are added to the other subsets without eliminating the possibility of them including traits. In Case2, for example, \( (L'_1 \in \bigcup (C_{\text{dir}} \cap C_{\text{sub}})) \) is processes for determining the new subsets, \( (C_{\text{dir}} \cap C_{\text{sub}}) \) and \( I \in \bigcup (C_{\text{dir}} \cap C_{\text{sub}}) \) are processes for adding new attributes, and \( P_0 \) is \( P_0 \) (\( I \in \bigcup (C_{\text{dir}} \cap C_{\text{sub}}) \)) for a given \( l \) (1 \( \leq l \leq p \)).

**WMK:** It takes as inputs \( U \), two consecutive segments (\( j \)th and \( j+1 \)th segments), and \( h \). It divides \( U \) into multiple subsets and chooses different watermarks for each subset. It generates multiple variants \( v_j \) (\( i = j, j+1, 1 \leq k \leq r \)) and updates \( h \) depending on the relationship between the subsets and the watermarks. It returns \( v_j, S_j \) (\( i = j, j+1, 1 \leq k \leq r \)), and the updated \( h \).

**TRC:** It takes as inputs \( U, \sigma \), and \( S_j \) (1 \( \leq k \leq r \)) and \( h \), and performs the following.

**Case1.** If \((S_j, S_j) = (I, I)\), it performs

\[
\omega \leftarrow \omega + 1
\]

\[
C_{\text{dir}}, C_{\text{dir}}, C_{\text{sub}}, C_{\text{sub}} \leftarrow \text{Sub}(I)
\]

and also performs

\[
P_0 \leftarrow (P_0 \setminus \{I\}) \cup \{C_{\text{dir}}, C_{\text{dir}}\}
\]

\[
P_\omega \leftarrow (P_\omega \setminus \{I\}) \cup \{C_{\text{dir}}, C_{\text{dir}}\}
\]

**Case2.** If \((S_j, S_j) = (C_{\text{dir}}, C_{\text{dir}})\) for a given \( l \) (1 \( \leq l \leq \omega \)), it performs

\[
C_{\text{dir}}, C_{\text{dir}} \leftarrow \text{Sub}(C_{\text{dir}} \cap C_{\text{dir}})
\]

It also performs

\[
I \leftarrow I \cup \{C_{\text{dir}} \cap C_{\text{dir}}\}
\]

\[
L'_1 \leftarrow (C_{\text{dir}} \cap C_{\text{dir}}) \cup (C_{\text{dir}} \cap C_{\text{dir}})
\]

and

\[
P_0 \leftarrow (P_0 \setminus \{C_{\text{dir}}, C_{\text{dir}}\}) \cup \{C_{\text{dir}}, C_{\text{dir}}\}
\]

**Case3.** If \((S_j, S_j) = (C_{\text{dir}}, C'_{\text{dir}})\) for a given \( l \) (1 \( \leq l \leq \omega \)), it performs

\[
I \leftarrow I \cup \{C_{\text{dir}}, C_{\text{dir}}\} \cup \{C_{\text{dir}}, C'_{\text{dir}}\}
\]

\[
L'_1 \leftarrow (C_{\text{dir}} \cap C'_{\text{dir}}) \cup (C_{\text{dir}} \cap C'_{\text{dir}})
\]

\[
C'_{\text{dir}}, C'_{\text{dir}} \leftarrow \text{Sub}(C'_{\text{dir}} \cap C'_{\text{dir}})
\]

A similar computation is performed for the other subsets pairs such that \((S_j, S_j) = (C_{\text{dir}}, C_{\text{dir}}), (C_{\text{dir}}, C_{\text{dir}}), \) or \((C_{\text{dir}}, C_{\text{dir}}), \).

**Case4.** If \((S_j, S_j) = (C'_{\text{dir}}, C'_{\text{dir}})\) for a given \( l \) (1 \( \leq l \leq \omega \)), it performs

\[
C'_{\text{dir}} \leftarrow C'_{\text{dir}} \cup C'_{\text{dir}} \cup C'_{\text{dir}}
\]

\[
L'_1, R'_1 \leftarrow \text{Div2}(L'_1)
\]

A similar computation is performed for the other subsets pairs such that \((S_j, S_j) = (C_{\text{dir}}, C_{\text{dir}}), (C_{\text{dir}}, C_{\text{dir}}), \) or \((C_{\text{dir}}, C_{\text{dir}}), \).

**Case5.** If \((S_j, S_j) = (C'_{\text{dir}}, L'_1)\) for a given \( l \) (1 \( \leq l \leq \omega \),
it performs
\[ \omega \leftarrow \omega + 1 \]
\[ C_{\omega,0}, \overline{C_{\omega,0}}, C_{\omega,0}, \overline{C_{\omega,0}} \rightarrow \text{Sub}(\ell_i) \]
\[ C_{\omega,0}, \overline{C_{\omega,0}}, C_{\omega,0}, \overline{C_{\omega,0}} \rightarrow \text{Sub}(\ell_i) \]
\[ I \leftarrow I \cup \overline{C_{\omega,0}} \]

and
\[ P_\oplus \leftarrow (P_\oplus \setminus \{C_{\omega,0}, \overline{C_{\omega,0}}, L_i^j, R_i^j\}) \cup \{C_{\omega,0}, \overline{C_{\omega,0}}, C_{\omega,0}, \overline{C_{\omega,0}}\} \]
\[ P_\oplus \leftarrow (P_\oplus \setminus \{C_{\omega,0}, \overline{C_{\omega,0}}, L_i^j, R_i^j\}) \cup \{C_{\omega,0}, \overline{C_{\omega,0}}, C_{\omega,0}, \overline{C_{\omega,0}}\} . \]

A similar computation is performed for the other subsets pairs, \((S_{k,j}^i, S_{k,j}^{\pi_1}) = (C_{\omega,0}, L_i^j, R_i^j)\).

**Case 6.** If \((S_{k,j}^i, S_{k,j}^{\pi_1}) = (L_i^j, L_i^j)\) for a given \(1 \leq l \leq \omega\), it performs
\[ \omega \leftarrow \omega + 1 \]
\[ C_{\omega,0}, \overline{C_{\omega,0}}, C_{\omega,0}, \overline{C_{\omega,0}} \rightarrow \text{Sub}(L_i^j) \]
\[ C_{\omega,0}, \overline{C_{\omega,0}}, C_{\omega,0}, \overline{C_{\omega,0}} \rightarrow \text{Sub}(L_i^j) \]
\[ I \leftarrow I \cup \overline{R_i^j} \]

and
\[ P_\oplus \leftarrow (P_\oplus \setminus \{C_{\omega,0}, \overline{C_{\omega,0}}, L_i^j, R_i^j\}) \cup \{C_{\omega,0}, \overline{C_{\omega,0}}, C_{\omega,0}, \overline{C_{\omega,0}}\} \]
\[ P_\oplus \leftarrow (P_\oplus \setminus \{C_{\omega,0}, \overline{C_{\omega,0}}, L_i^j, R_i^j\}) \cup \{C_{\omega,0}, \overline{C_{\omega,0}}, C_{\omega,0}, \overline{C_{\omega,0}}\} . \]

A similar computation is performed for the other subsets pairs, \((S_{k,j}^i, S_{k,j}^{\pi_1}) = (C_{\omega,0}, L_i^j, \overline{R_i^j})\) or \((L_i^j, \overline{R_i^j})\).

**Case 7.** If \((S_{k,j}^i, S_{k,j}^{\pi_1}) = (L_i^j, C_i^j)\) for a given \(1 \leq l \leq \omega\), it performs
\[ \omega \leftarrow \omega + 1 \]
\[ C_{\omega,0}, \overline{C_{\omega,0}}, C_{\omega,0}, \overline{C_{\omega,0}} \rightarrow \text{Sub}(L_i^j) \]
\[ C_{\omega,0}, \overline{C_{\omega,0}}, C_{\omega,0}, \overline{C_{\omega,0}} \rightarrow \text{Sub}(C_i^j) \]
\[ I \leftarrow I \cup \overline{R_i^j} \]

and
\[ P_\oplus \leftarrow (P_\oplus \setminus \{C_{\omega,0}, \overline{C_{\omega,0}}, L_i^j, R_i^j\}) \cup \{C_{\omega,0}, \overline{C_{\omega,0}}, C_{\omega,0}, \overline{C_{\omega,0}}\} \]
\[ P_\oplus \leftarrow (P_\oplus \setminus \{C_{\omega,0}, \overline{C_{\omega,0}}, L_i^j, R_i^j\}) \cup \{C_{\omega,0}, \overline{C_{\omega,0}}, C_{\omega,0}, \overline{C_{\omega,0}}\} . \]

A similar computation is performed for the other subsets pairs, \((S_{k,j}^i, S_{k,j}^{\pi_1}) = (C_i^j, R_i^j)\) or \((L_i^j, R_i^j)\).

The existence of multiple traitors is confirmed in Case 4, Case 5, Case 6 and Case 7 transitions, whereas the existence of more than one traitor can not be confirmed in Case 1, Case 2 and Case 3 transitions.

**Remark 1:** Although this scheme looks complex, it is based on simple strategy we described in Sect. 3.1. The strategy is to decrease the number of suspicious users to 1/4 with the basic function Sub, and when the traitors are not included in the subset that the tracer suspected, the tracer can detect this fact and can continue the tracing in other subsets. For example, let us consider a situation in which the traitors are not included in the set that the tracer suspects. When the tracer finds variants \(S_{k,j}^i = C_{\omega,0}\) and \(S_{k,j}^{\pi_1} = C_{\omega,0}\), it tries to decrease the number of suspicious users to 1/4 and sets \(\{C_{\omega,0} \cap C_{\omega,1}\}\) as the main target and divides the main target to four subsets, \(\{C_{\omega,0}, C_{\omega,1}\}\) and \(\{C_{\omega,0}, C_{\omega,1}\}\). If one traitor is in \(\{C_{\omega,0} \cap C_{\omega,1}\}\), this process works effectively. However, it is also possible that multiple traitors exist and that one of them belongs to \(\{C_{\omega,0} \cap C_{\omega,1}\}\) and one of them belongs to \(\{C_{\omega,0} \cap C_{\omega,1}\}\), and that they collude to make illegal content for redistribution. In this case, new attributes are given to the sets, \(\{C_{\omega,0} \cap C_{\omega,1}\}\) and \(\{C_{\omega,0} \cap C_{\omega,1}\}\), and even if the traitors are not included in the main target set \(\{C_{\omega,0} \cap C_{\omega,1}\}\), the tracer can learn this and can take measures without having to worry about being misled. If traitors employ such a collusion strategy, the tracer can learn that there are at least two traitors. That is, the tracer can identify two traitors at once. The most adequate strategy for traitors is one in which the tracer gets as little information as possible, for example, information revealing the existence of only one traitor. Nonetheless, employing such a strategy results in the tracer’s main target being correct.

### 4. Evaluation

A similar discussion to the one in [10],[11] on security proves that the following attack is the strongest. Traitors select the variants to be redistributed such that if \(p < 0,6\), the state moves as \(S_1 \rightarrow (S_2 \rightarrow S_4 \rightarrow S_6 \text{ or } S_7) \rightarrow (S_2 \rightarrow S_4 \rightarrow S_6 \text{ or } S_7) \rightarrow \cdots\), and otherwise \(S_1 \rightarrow S_2 \rightarrow S_2 \rightarrow S_2 \rightarrow \cdots\), where \(S_1, \cdots, S_7\) denote the states after Case 1, Case 7 transitions and A → B denotes the transition from state A to state B. We thus shall address the traceability of the tracing scheme and evaluate it with regard to the number of dynamic computations in comparison with DTT [1], [2],[10],[11]. In addition, we shall evaluate our scheme’s effectiveness against delayed attacks. Moreover, we shall evaluate it with regard to the network costs in comparison with STT [18],[19].

#### 4.1 Security Analysis

We discuss two kinds of security: “traceability” and “delayed attack resilience”.

#### 4.1.1 Traceability

We show that our tracing algorithm can trace at most \(p (1 \leq p < [r/3])\) traitors perfectly, where \([x]\) denotes a function which outputs a maximum integer less than or equal to \(x\). Formally, we prove the following theorem.

**Theorem 1:** If the number of traitors \(p\) is less than \([r/3]\), the tracing algorithm can trace all \(p\) traitors.

For the proof of this theorem, we utilize the following two claims under the condition of \(p < [r/3]\). These claims and their proofs use the notation \(\Pi_i\), where \(\Pi_i \in \{C_i, C_{\omega,0}, C_{\omega,1}\}\).
Upon discovery of il-

traitors (We show that the two traitors can be traced in all cases.

Π and the traitors in

every process are repeated until the number of users included in 
vj

Similarly, if u1 and u2 belong to two distinct subsets Π1 and Π2, the tracer performs

Case 2 transition and the state moves to S2. In the S2, u1 and u2 belong to L1, u1 and u2 receive variants v2j

Π when there are multiple traitors in a subset

Π placed into two distinct subsets

Π

Π in S0 (Πl = C), the tracer performs

Case 1 transition and the state of Πl moves to S1. When the variants that only u1 receives are repeatedly redistributed, the state moves as follows: S2 → S2 → ... → S2 (Case 3 transition) until the number of users in Πl becomes one, since the other traitors cannot receive the same variants. Even if the variant vj

Π (l ≠ i) is redistributed on the way, the side information related to Πi is held and that of Πl is updated. The state of Πl moves as follows: S2 → ... → S2 until the number of users in Πl becomes one. These processes are repeated until the number of users included in every p subset becomes one, and finally, all p traitors can be traced.

Proof of Claim 2. Suppose that there are multiple traitors in a subset C_l and that the variants distributed to two of these traitors (u1 and u2) are redistributed.

We consider the following cases: S1 → S2 → S2 → S2 → ... , S1 → (S2 → S4 → S6 or S7) → ... , and other cases. We show that the two traitors can be traced in all cases.

Case of S1 → S2 → S2 → S2 → ... . Upon discovery of illegally distributed content, the tracer performs Case 1 transition and the state of C_l moves to S1. Then, if both traitors are included in the same subsets at the times of continuous two segments distribution, e.g. u1, u2 ∈ C_{0,l} ∩ C_{0,l}, the tracer performs Case 2 transition and the state moves to S2. Similarly, if u1 and u2 are in the same subsets in S2, e.g. u1, u2 ∈ C_{0,l} ∩ C_{0,l}, the tracer performs Case 2 transition and the state moves to another S2. Naturally, the number of users included in subset l increases, but the number of users included in C_{α,l} ∩ C_{α,l} decreases. Consequently, these two traitors are assigned to distinct two subsets at some time, e.g. u1 ∈ C_{α,l} and u2 ∈ C_{α,l} \cap C_{α,l}.

Case of S1 → (S2 → S4 → S6 or S7) → ... . If u1 and u2 receive different variants such that v_{2j}^{C_{α,l}} and v_{2j}^{C_{α,l}} are distributed to u1 and that v_{2j}^{C_{α,l}} and v_{2j}^{C_{α,l}} are distributed to u2, it means that u1 and u2 are in two distinct subsets, u1 ∈ C_{0,l} ∩ C_{0,l} and u2 ∈ C_{0,l} ∩ C_{0,l}. u1 and u2 can then use both variants for redistribution, e.g. v_{2j}^{C_{α,l}} and v_{2j}^{C_{α,l}}. The tracer then performs Case 2 transition and the state moves to S2. In the S2, u1 and u2 belong to L1, u1 and u2 receive variants v_{2j}^{L1} and v_{2j}^{L2}, and redistributes them. The tracer performs Case 4 transition and the state moves to S4. u1 then receives v_{2j}^{L1} and v_{2j}^{L2}, and u2 receives v_{2j}^{L3} and v_{2j}^{L4}. u1 and u2 then redistribute v_{2j}^{L3} and v_{2j}^{L4}, or v_{2j}^{L4} and v_{2j}^{L5}. Consequently, the tracer performs Case 7 transition, the state moves to S7, and u1 and u2 are assigned to two distinct subsets Π1 and Π2. If u1 and u2 select a variant pair (v_{2j}^{L1} and v_{2j}^{L2}), or (v_{2j}^{L3} and v_{2j}^{L4}), the tracer performs Case 6 transition, the state moves to S6, and u1 and u2 are assigned to two distinct subsets Π1 and Π2.

Other cases. We have to consider other cases such that the same variant of a certain segment is distributed to both u1 and u2, and that two different variants of the next segment are distributed to them, e.g. v_{2j}^{C_{α,l}} and v_{2j}^{C_{α,l}} are distributed to u1 and v_{2j}^{C_{α,l}} and v_{2j}^{C_{α,l}} are distributed to u2, i.e., u1 ∈ C_{0,l} ∩ C_{0,l} and u2 ∈ C_{0,l} ∩ C_{0,l}. u1 and u2 redistribute v_{2j}^{C_{α,l}} and v_{2j}^{C_{α,l}}, or v_{2j}^{C_{α,l}} and v_{2j}^{C_{α,l}}. The tracer then performs Case 2 transition.

The result is u1 ∈ C_{α,l} ∪ C_{α,l} and u2 ∈ L, and receive different variants at the time of the next consequent two segments distribution, u1 receives v_{2j}^{C_{α,l}} and v_{2j}^{C_{α,l}}, and u2 receives v_{2j}^{C_{α,l}} and v_{2j}^{C_{α,l}}. Accordingly, the tracer performs Case 5 transition, and it can place u1 and u2 into two distinct subsets Π1 and Π2.

It remarks that, when α variants are necessary to trace one traitor, it is almost impossible to trace traitors if p ≥ \ceil{r/|α|}, since the number of variants is insufficient. On the other hand, in the case of p < \ceil{r/|α|}, the number of variants is sufficient to trace all traitors. In the above scheme, α = 3 and p < \ceil{r/3}. Hence, the above always holds true under the condition that the consecutively redistributed variants are the ones that distinct two traitors received, who are in two distinct subsets Π1 and Π2, whose indices are the same, e.g. Π1 = C_{α,l} and Π2 = C_{α,l}, and the two traitors can be assigned to two distinct subsets Π1 and Π2 (l ≠ α). As a result, when there are multiple traitors in a subset Πl, they can be placed into two distinct subsets Π1 and Π2 (l ≠ α), each of which includes at least one traitor.

Proof of Theorem 1 (Sketch). Suppose that there are p (1 ≤ p < \ceil{r/3}) traitors and that multiple traitors belong to one subset Πl. The tracing algorithm can lead to the situa-
Discussion: It is important to consider the gap between ideal watermark and non-ideal (real) one since there is actually no ideal watermarking scheme.

In our scheme, a tracer must perform the following processes:

(1) The tracer gets illegally redistributed content through a feedback channel and detects the watermark embedded into the content.

(2) The tracer assigns users into subgroups for the next subsequent segments according to the result of the process (1).

(3) The tracer embeds watermarks into the next subsequent segments of the content.

When some detection errors occur in the process (1), the new user assignment does not work effectively. That is, the subgroup, which includes a true traitor and should be investigated intensively, is not investigated intensively. For example, suppose that a traitor is in a subset $C_{\oplus}$ and that a variant of a certain segment $v_{\oplus}$, into which information $t_{\oplus}$ is embedded, and $v_{\ominus}$, into which information $t_{\ominus}$ is embedded, were distributed to $C_{\oplus}$ and $C_{\ominus}$, respectively. The traitor redistributes a variant $v_{\oplus}$ and the tracer obtains it. However, watermark detection error occurs and the detected information is $t_{\ominus}$. Consequently, the tracer will investigate intensively $C_{\ominus}$ which does not include the traitor and an innocent user would be identified as a traitor. However, some practically available watermark embedding and detecting systems exist [12], [14], [16] and there has been no error report on them at the moment. Therefore, these real watermarking systems can be regarded as close to the ideal one and can be used practically.

Moreover, when considering traitors’ behavior (attack), algorithms of the watermarking scheme should be closed. If the entity who embeds watermarks can be the same with the one who detects watermarks, the algorithms can be highly concealed. Consequently, it is possible to protect embedded information from modifying and to protect the information from detection error caused by the attacks. Such a management makes real watermarking schemes closer to the ideal one. However, even if such a management method is employed, there remains low possibility to trace innocent users. We hope that a watermarking scheme that does not have this problem will be developed in the future.

We also have to consider the time span between certain illegal redistribution and the next content distribution that the tracer requires. The tracer has to perform the above (1), (2) and (3) processes in the span. Actually, the watermarking systems [12], [14], [16] have a real-time property. That is, it takes only the same amount of time with the length of content to perform the process (1) or (3). Furthermore, the required time for process (2) is extremely less than those of the processes (1) and (3). Consequently, the required total time for all processes (1), (2) and (3) is only about twice as long as length of the content. When considering actual illegal redistribution described before, there is enough time for the tracer to perform above all processes since content is redistributed soon after it was broadcast and since a watermark assignment is performed once a day or once a week before the next version of the same program will be broadcast. As a result, our scheme can be practically used.

4.1.2 Delayed Attack Resilience

Our scheme is robust against delayed attacks. The subset assignment for each segment is determined before the next consecutive segments are distributed, and the assignment is recorded in the side information in order to trace traitors. In the worst case, the traitors wait for the distribution to be completed and then start redistribution. However, since distinct subsets are assigned to users for each segment, not one piece but multiple pieces of the information to be used for tracing can be obtained and can be used for the next dynamic computation. This is in contrast to DTT, which is completely insecure against a delayed attack.

In addition, both DTT and our scheme require the feedbacks from traitors. However, DTT requires real-time feedback channels, whereas our scheme does not necessarily require them. Therefore, our scheme is more robust against delayed attacks than DTT.

4.2 Costs for Dynamic Computations

We show that our scheme uses fewer dynamic computations than [10], [11].

Number of Dynamic Computations of Our Scheme.

Regarding the number of dynamic computations to trace all $p$ traitors, the following claim is true and we prove it here.

Claim 3: The largest number of dynamic computations of our scheme to trace all $p$ traitors is $p \times (\log_4 n - \log_4 p) + 4 p^3$ if $p < 60$, otherwise $p \times (\log_4 n + 1)$.

Proof of Claim 3. We assume that the attack method is the best for the traitors such that the traitors can redistribute content as long as possible. When traitors find the best attack method, they repeat it, and the same state appears repeatedly. The states $S_2$, $S_5$, $S_6$ and $S_7$ become their candidates. We then calculate the largest number of dynamic computation among the cases in which the states $S_2$, $S_5$, $S_6$ or $S_7$ are appeared repeatedly. Consequently, we derive the conditions for traitors to select one candidate. The number is the maximum number of dynamic computations of our scheme. In the following, we calculate the number of dynamic computations and compare them.
Case of S2. One of the traitors redistributes content repeatedly until he/she is identified. The traitors, then, change the members and repeat the same things. Thus, the number of dynamic computations to identify all p traitors is \( N_{2,all} := p (\log_4 n + 1) \).

Cases of S5, S6 and S7. These three states are similar, since they all have two State1s and one State0. We thus can show only the number of dynamic computations of S6 as a representative.

Before the state becomes S6, three dynamic computations are performed and the existence of at least two traitors is detected. The traitors can then select one attack method out of two. One is that they select State0 for their redistribution; the other is that they select State1-1 or State1-2.

When the traitors select State0, the tracer confirms the existence of new two traitors with four subsequent dynamic computations. When the traitors repeat the same attack, \( 3 + (p-2)/2 \times 4 = 2p - 1 \) dynamic computations put \( p \) traitors into \( p \) distinct subsets, and all subsets move to State2. The average number of users in one subset is \( n/p \), when \( p \) traitors are put into distinct subsets. This average number means that the number of users in each subset is the same and that the number of dynamic computations necessary to identify all the traitors is the largest. That is, this is the most optimal attack. The number of dynamic computations is then \( p \times (\log_4 (n/p) + 1) \). Thus the total number of dynamic computations is \( N_{6,all} := 2p - 1 + p \times (\log_4 (n/p) + 1) = p \times (\log_4 n - \log_4 p) + 3p - 1 \).

When the traitors select State1-1 or State1-2, the tracer can confirm the existence of one more traitor with less than or equal to three dynamic computations, and \( 3 + 3 \times (p-2) = 3p - 3 \) dynamic computations are necessary to put \( p \) traitors into \( p \) distinct subsets. Then, all the subsets move to State2 and \( p \times (\log_4 (n/p) + 1) \) dynamic computations identify \( p \) traitors. The total number of dynamic computations is \( N_{6,all} := 3p - 3 + p \times (\log_4 (n/p) + 1) = p \times (\log_4 n - \log_4 p) + 4p - 3 \).

Comparing \( N_{6,all} \) with \( N_{6,all} \), we see that \( N_{6,all} \) is larger than \( N_{6,all} \) if \( p \geq 2 \). The number of traitors in this case is more than two, and hence, \( N_{6,all} \), the largest number of dynamic computations in the case of S6, is \( N_{6,all} \).

Similarly, in the case of S7, \( N_{7,all} = N_{6,all} = p \times (\log_4 n - \log_4 p) + 4p - 3 \), and in the case of S5, \( N_{5,all} = p \times (\log_4 n - \log_4 p) + 2p - 2 \).

Comparison. We compare \( N_{2,all} \), \( N_{5,all} \), \( N_{6,all} \) and \( N_{7,all} \). Comparing \( N_{5,all} \) with \( N_{6,all} (\equiv N_{7,all}) \), we see that \( N_{6,all} \) is larger than \( N_{5,all} \). Comparing \( N_{2,all} \) with \( N_{6,all} \), we see that

\[
N_{6,all} - N_{2,all} = (p \times (\log_4 n - \log_4 p) + 4p - 3) - (p \times (\log_4 n + 1)) = 3p - 3 - p \log_4 p.
\]

This value changes with \( p \). In fact, we can get the border value \( p = 60 \) from a computer calculation, and hence, when \( p < 60 \), \( 3p - 3 - p \log_4 p > 0 \) and when \( p \geq 60 \), \( 3p - 3 - p \log_4 p < 0 \). That is, when \( p < 60 \), then \( N_{6,all} > N_{2,all} \); otherwise \( N_{6,all} < N_{2,all} \). Consequently, the largest number of dynamic computations \( \max(N_{2,all}, N_{5,all}, N_{6,all}, N_{7,all}) = \max(N_{2,all}, N_{6,all}, N_{7,all}) \) is \( \max(p \times (\log_4 n - \log_4 p) + 4p - 3, p \times (\log_4 n + 1)) \), and it is \( p \times (\log_4 n - \log_4 p) + 4p - 3 \) if \( p < 60 \); otherwise \( p \times (\log_4 n + 1) \).

**Comparing Our Scheme with the Schemes of [10], [11].** Our scheme can decrease the number of suspicious users to 1/4 with one dynamic computation, whereas the conventional scheme [10], [11] can decrease the number only to 1/2 (see Fig. 6). Thus, our scheme can identify all traitors by using only half the number of dynamic computations. However, while our scheme uses up to three variants to identify one traitor, compared with the conventional scheme’s two variants, our scheme does not always use three variants.

To evaluate these schemes, a conventional scheme us-
We proposed the trade-off traitor tracing scheme. This scheme requires fewer dynamic computations than the conventional scheme does, and it does not need to make a dynamic computation in real time, since the computation is performed after several segments have been stored. Moreover, our scheme is more resilient against delayed attacks than the conventional scheme.

To reduce network costs, our scheme needs a lot of edge routers to control the distribution of watermark variants, but it is difficult to add the new function to all edge routers on the Internet. However, an overlay network, such as a P2P network, enables a user’s terminal to play a the role of a “pseudo-router”. In this case, an application software must be installed on each terminal, but that could be done more easily than on each edge router. Therefore, our scheme is practical.

DTT and our scheme require the feedbacks from traitors. However, there is no method for retrieving all pirate copies efficiently. Actually, many broadcast contents are illegally uploaded on the Internet websites, so right holders must look over uploaded contents carefully and check whether they are illegal or not. Therefore, it takes a long time to retrieve a pirate copy. However, real-time feedbacks from traitors are realized on some specific websites. DTT requires real-time feedbacks from traitors, so delayed attacks is effective. On the other hand, our scheme does not necessarily require real-time feedbacks from traitors. Therefore, our scheme is more robust against delayed attacks than DTT.

Finally, in this paper, we discussed only the case in which the maximum number of watermark variants is \(3p+1\) and the number of segments is two \((t=2)\). In fact, we can enlarge the number of segments and the number of variants, but in doing so, it becomes very difficult to evaluate the performance. In future, we will evaluate the performance of an enhanced scheme and develop an optimal construction for any parameter setting.

Acknowledgments

We would like to thank the anonymous reviewers for their useful comments.

References

Appendix A: Brief Review of Dynamic Traitor Tracing [10, 11]

A.1 Model of Dynamic Traitor Tracing

In the model of DTT, the next watermark pattern is determined with adaptive and dynamic computations in real time, depending on the watermark information detected from illegally redistributed content. Content providers distribute content and then traitors illegally redistribute it. The providers have real-time feedback channels and can see the content currently being redistributed. One piece of content consists of multiple segments and is possible to generate multiple variants of each segment. Distinct information is embedded in each variant. In addition, users are assigned to multiple subsets, and each subset receives a unique variant. The subsets are dynamically determined after information embedded in an illegally redistributed segment is analyzed, and the new subset is used in the next distribution. Figure A-1 shows the model.

A.2 Fiat and Tassa’s Construction

We show their construction of DTT. The basic strategy is to decrease the number of users in a set, which includes traitors, to 1/2 by using a function Div2.

Div2: It takes as inputs a set of users $X$, and returns two subsets $L$ and $R$, where $L \cup R = X$, $|L| = |R| \approx \frac{1}{2}|X|$, and $L \cap R = \emptyset$.

Construction: The set of users $U$ is partitioned into $2\omega + 1$ subsets $U = \cup_{S \in P} S$, where $P = \{L_1, R_1, \ldots, L_\omega, R_\omega, I\}$, and each of those sets receives a distinct variant. $I$ is the subset of users that is not known to include a traitor. These $I$, $\omega$, and $P$ are initialized to $U$, 0, and $\{I\}$. Then, a distinct variant for every nonempty set of users $S \in P$ is transmitted, and the traitor transmits a variant $v$.

Case 1. If $v$ is associated with $I$, tracers (content providers) increment $\omega$ by one, split $I$ into two subsets $L_\omega$ and $R_\omega$, add those sets to $P$, and set $I = \emptyset$. Namely,

$$
\begin{align*}
\omega & \leftarrow \omega + 1 \\
L_\omega, R_\omega & \leftarrow \text{Div2}(I) \\
P & \leftarrow P \cup \{L_\omega, R_\omega\} \\
I & \leftarrow \emptyset.
\end{align*}
$$

Case 2. If $v$ is associated with one of the sets $L_i$, $1 \leq i \leq \omega$, then tracers add $R_i$ to $I$ and split $L_i$ into new subsets $L_i$ and $R_i$. Namely,

$$
\begin{align*}
I & \leftarrow I \cup R_i \\
L_i, R_i & \leftarrow \text{Div2}(L_i)
\end{align*}
$$

If $L_i$ is a singleton set, content providers suspend distribution to the user included in $L_i$, add $R_i$ to $I$, and remove $R_i$ from $P$. Namely,

$$
\begin{align*}
I & \leftarrow I \cup R_i \\
P & \leftarrow P \setminus R_i
\end{align*}
$$

If $v$ is associated with $R_i$, tracers do as above while switching the roles of $R_i$ and $L_i$.

A.3 Major Shortcoming of Dynamic Traitor Tracing: Delayed Attack

The major shortcoming of DTT is that the regrouping of users and assignment of watermarks to users in each interval depend on the rebroadcast content, also called feedback...
Suppose we want to provide protection for up to 16 (n = 16) users against up to 2 colluders (p = 2), and the user identities are \( u_1, \ldots, u_{16} \) and the colluders are \( u_3 \) and \( u_4 \). In addition, assume that the colluders select variant 1 for the first segment and variant 3 for the second segment, and thus \( u_3 \) and \( u_4 \) are in \( L_1 \). Hence, \( u_3 \) and \( u_4 \) receive variant 3 for the first segment and variant 3 for the second segment of the second content. Accordingly, the colluders can only select variant 3 for the first segment and variant 3 for the second when they redistribute the second content (variant 3 for the first segment and variant 3 for the second).

When the tracer gets the redistributed second content, it learns that the variants are 3 and 3 for the first and second segments. From this analysis, the tracer learns that at least one traitor is in \( L_1 \). However, the conclusion that there is only one traitor and he or she is in \( L_1 \) is contradictory to the analysis of the first content distribution. Thus, the tracer knows that at least two traitors exist. It then assigns users to new subsets for the next two segments according to Case4 transition. That is, for the first and second segments, \( C'_{\odot,1} = \{u_3, u_4\}, C'_{\odot,1} = \{u_3, u_4, u_5, u_6, u_9, u_{10}, \ldots, u_{14}\} \) and \( I = \{u_{11}, u_{12}, u_{15}, u_{16}\} \), and thus \( u_3 \) and \( u_{14} \) receive variant 3 for both segments and \( u_{14} \) receives variant 3 for both segments. The colluders select variant 2 that was distributed to \( u_3 \) in the first segment and variant 3 that was distributed to \( u_{14} \) in the second, and they redistribute the third content (variant 2 for the first segment and variant 3 for the second).

When the tracer gets the redistributed third content, it learns that the variants are 2 and 3 for the first and second segments, respectively. From this analysis, it learns that at least one traitor is in \( L_1' \) and at least one traitor is in \( L_1' \). It then assigns users to new subsets for the next two segments according to Case7 transition. That is, for the first segment, \( C'_{\odot,1} = \{u_3, u_4\}, C'_{\odot,1} = \{u_7, u_8, u_9, u_{10}, \ldots, u_{14}\}, C'_{\odot,1} = \{u_3, u_4, u_5, u_6, u_9, u_{10}, \ldots, u_{14}\}, C'_{\odot,2} = \{u_3, u_4, u_5, u_6, u_9, u_{10}, \ldots, u_{14}\} \) and \( I = \{u_1, u_2, u_5, u_6, u_9, u_{10}, \ldots, u_{14}\} \), and thus \( u_3 \) and \( u_{14} \) receive variant 1 for both segments, and \( u_3 \) receives variant 1 for both segments, and \( u_{14} \) receives variant 5 for both segments. The colluders select variant 1 that was distributed to \( u_3 \) in the first segment and variant 5 that was distributed to \( u_{14} \) in the second, and they redistribute the fourth content (variant 1 for the first segment and variant 5 for the second).

When the tracer gets the redistributed fourth content, it learns that the variants are 1 and 5 for the first and second segments, respectively. From this analysis, it learns that at least one traitor is in \( C'_{\odot,1} \) and at least one traitor is in \( C'_{\odot,2} \). It then assigns users to new subsets for the next two segments according to Case3 transition. That is, for the first segment, \( C'_{\odot,1} = \{u_5\}, C'_{\odot,1} = \{u_4\}, C'_{\odot,2} = \{u_{10}\}, C'_{\odot,2} = \{u_{14}\} \) and \( I = \{u_1, u_2, u_5, u_6, u_9, u_{10}, \ldots, u_{14}\} \), and thus \( u_3 \) is in \( C'_{\odot,1} \) and \( u_{14} \) is in \( C'_{\odot,2} \). Accordingly, \( u_3 \) receives variant 1 for both segments, and \( u_{14} \) receives variant 5 for both segments. The colluders select variant 1 that was distributed to \( u_3 \) in the first segment and variant 5 that was distributed to \( u_{14} \) in the second, and they redistribute the fourth content (variant 1 for the first segment and variant 5 for the second).
When the tracer gets the redistributed fifth content, it learns that the variants are 1 and 5 for the first and second segments, respectively. From this analysis, it learns that at least one traitor is in $C'_{\oplus,1}$ and at least one traitor is in $C'_{\oplus,2}$. Consequently, the tracer can identify the traitors as being $u_3$ and $u_{14}$, since each subset of $C'_{\oplus,1}$ and $C'_{\oplus,2}$ has only one user ($u_3$ or $u_{14}$).

In this case, each assignment of users is performed before each content is distributed, and hence, the total number
of dynamic computations is five. The number is less than the maximum number \( p(\log_4(n/p) + 4) - 3 = 8 \) shown in Table 1. This attack method is not the best one for the colluders.

The network cost is proportional to the number of necessary variants, and we can evaluate it by using the number of variants. In this case, the maximum number of variants is five, and it is less than the number \( 3p + 1 \) shown in Table 1. The network cost is low, since the total number of users is small and the attack method is not the best one for the colluders.

---

**Go Ohtake** received the B.E. and M.E. degrees from Tokyo Institute of Technology in 1999 and 2001, respectively. He is a research engineer of NHK Science and Technical Research Laboratories, and he is also a student of Institute of Information Security. His research interests include copyright protection technology, content distribution system, and digital signature.

**Kazuto Ogawa** received the B.E. and Ph.D. degrees from the University of Tokyo, Tokyo, Japan in 1987 and 2008, respectively. He joined NHK (Japan Broadcasting Corporation) in 1987. He has mainly engaged in the research and development on video image processing systems and digital content rights management systems. He is currently a senior research engineer of NHK Science and Technical Research Laboratories.

**Goichiro Hanaoka** received his bachelor's degree in Electronic engineering from the University of Tokyo in 1997, and received his master's and Ph.D. degrees in information and communication engineering from the University of Tokyo in 1999 and 2002, respectively. From 2002 to 2005 he was a Research Fellow of Japan Society for the Promotion of Science (JSPS). Since 2005 he has been with the National Institute of Advanced Industrial Science and Technology, Japan. He received the Wilkes Award from the British Computer Society in 2007.

**Hideki Imai** was born in Shimane, Japan on May 31, 1943. He received the B.E., M.E., and Ph.D. degrees in electrical engineering from the University of Tokyo in 1966, 1968, and 1971, respectively. From 1971 to 1992 he was on the faculty of Yokohama National University. From 1992 to 2006 he was a Professor in the Institute of Industrial Science, the University of Tokyo. In 2006 he was appointed as an Emeritus Professor of the University of Tokyo and a Professor of Chuo University. Concurrently he serves as the Director of Research Center for Information Security, National Institute of Advanced Industrial Science and Technology. His current research interests include information theory, coding theory, cryptography, and information security. From IEICE Dr. Imai received Best Book Awards in 1976 and 1991, Best Paper Awards in 1992, 2003 and 2004, Yonezawa Memorial Paper Award in 1992, Achievement Award in 1995, Inose Award in 2003, and Distinguished Achievement and Contributions Award in 2004. He also received Golden Jubilee Paper Award from the IEEE Information Theory Society in 1998, Wilkes Award from the British Computer Society in 2007, and Official Commendations from the Minister of Internal Affairs and Communications in June 2002 and from the Minister of Economy, Trade and Industry in October 2002. He was awarded Honor Doctor Degree by Soochunhyang University, Korea in 1999 and Docteur Honoris Causa by the University of Toulon Var, France in 2002. He is also the recipient of the Ericsson Telecommunications Award 2005. Dr. Imai is a member of the Science Council of Japan. He was elected a Fellow of IEEE, IEICE, and IACR in 1992, 2001, and 2007, respectively. He has chaired many committees of scientific societies and organized a number of international conferences. He served as the President of the Society of Information Theory and its Applications in 1997, of the IEICE Engineering Sciences Society in 1998, and of the IEEE Information Theory Society in 2004. He is currently the Chair of CRYPTREC (Cryptography Techniques Research and Evaluation Committee of Japan).