Fingerprinting Protocol for On-Line Trade Using Information Gap between Buyer and Merchant

Kuribayashi, Minoru

Tanaka, Hatsukazu

(Citation)
IEICE transactions on fundamentals of electronics, communications and computer sciences,E89-A(4):1108-1115

(Issue Date)
2006-04-01

(Resource Type)
journal article

(Version)
Version of Record

(URL)
https://hdl.handle.net/20.500.14094/90001350

PAPER

Fingerprinting Protocol for On-Line Trade Using Information Gap between Buyer and Merchant

Minoru KURIBAYASHI[†a)], *Member and* Hatsukazu TANAKA[††b)], *Fellow*

SUMMARY The homomorphic property of the public key cryptosystem has been exploited in order to achieve asymmetric fingerprinting such that only a buyer can obtain fingerprinted content. However, this requires many computations and a wide-band network channel because the entire uncompressed content must be encrypted based on the public key cryptosystem. In this paper, instead of the homomorphic property, we introduce the management of the enciphering keys for the symmetric cryptosystem. Based on a buyer's identity, a trusted center issues the buyer a partial sequence which is one of the two elements in the entire sequence. Although a merchant shares the entire sequence with the center, he cannot extract the buyer's key sequence from it. Such an information gap enables our protocol to be asymmetric and efficient. For each packet of content, the merchant produces two marked packets that contains a "0" or "1" information bit, and they are enciphered using the two elements from the entire sequence. Subsequently, the buyer obtains the two ciphertexts (the encrypted marked packets) containing the information bits of his identity. Since the merchant does not know the ciphertext decrypted by the buyer, an asymmetric property is achieved. In our protocol, before trade between a buyer and a merchant, the merchant can produce and compress the marked packets; this enables the reduction of both the computational costs for the encryption and the amount of data for transmission. Since only the enciphering operation is performed by a merchant in the on-line protocol, real-time operation may be possible.

key words: *fingerprinting protocol, key management, asymmetric property, symmetric cryptosystem*

1. Introduction

Due to the rapid growth of the Internet, the transmission of multimedia content has become considerably easier and faster. It provides us numerous possibilities to produce applications and cultivate new business. However, it also increases the risk of unauthorized distribution of intellectual content such as music, images, movies, etc. Without copyright protection, a business may not be feasible. One of the candidates for copyright protection is the technique of watermarking [1] that enables the embedding of sub-information in digital content without causing serious degradation. In order to identify an illegal user of redistributed content, an author should embed a digital fingerprint in the content at the time of selling it. Such a technique is called fingerprinting.

Fingerprinting techniques are classified into two schemes. One is the method to produce the fingerprint itself, and the other is the protocol for embedding information in digital content. In the fingerprinting technique, each user purchases content containing his own fingerprint; hence, each content is slightly different. If users collect some content, they may attempt to find the difference and delete/change the embedded information. In order to withstand such an attack, one of the schemes generates specific codes such as c-secure code [2] and anti-collusion code (ACC) [3]. A cryptographic protocol for trade between a buyer and a merchant is considered in the second scheme. If both the buyer and the merchant obtain fingerprinted content in the protocol, the merchant cannot accuse the buyer of illegal distribution of the copy, even if the buyer's fingerprint is extracted. This is because the merchant may distribute it himself in order to frame an innocent buyer. Hence, it is desirable that only a buyer is able to obtain his own fingerprinted content in the protocol; such a protocol is called asymmetric fingerprinting protocol.

In [5]–[8], the asymmetric protocol is performed by exploiting the homomorphic property of the public key cryptosystem that enables a merchant to embed an encrypted fingerprint in an encrypted content. Since the ciphertext is computed using a buyer's encryption key, only the buyer can decrypt it; hence, only he can obtain the fingerprinted content. Although the homomorphic property is effective for constructing asymmetric fingerprinting, there are problems in its implementation. In general, multimedia content such as music, images, and movies should be compressed as they contain considerable redundancy. However conventional schemes cannot compress the content in order to embed an encrypted fingerprint by exploiting the homomorphic property. It also requires extremely high computational costs to encrypt an entire uncompressed content on the basis of public key cryptosystem. In addition, a merchant must perform the embedding and enciphering operations on each request from a buyer. Thus, from the point of view of data size and the computational costs, the conventional schemes are extremely inefficient. Balleste et al. [9] proposed asymmetric fingerprinting using a trusted third party (TTP) and symmetric fingerprinting to overcome the problem. However, most parts of the protocol in this system are performed by TTP, and a merchant functions as a sales agent of the TTP. Therefore, the amount of load on TTP is extremely large.

In this paper, we propose a new fingerprinting proto-

Manuscript received September 1, 2005.
Manuscript revised November 2, 2005.
Final manuscript received January 4, 2006.

[†] The author is with the Faculty of Engineering, Kobe University, Kobe-shi, 657-8501 Japan.
[††] The author is with the Kobe Institute of Computing, Kobe-shi, 650-0001 Japan.
a) E-mail: kminoru@kobe-u.ac.jp
b) E-mail: tanaka@kic.ac.jp

DOI: 10.1093/ietfec/e89–a.4.1108

col based on the key management by a trusted center. The objective of our scheme is to reduce the computational costs required for both the buyer and the merchant and also reduce the volume of communication. Without using the homomorphic property, a trusted center manages the enciphering keys for the cipher communication between a buyer and a merchant; however, it does not participate in the protocol. A buyer who registers at the center is assigned a partial key sequence that has been entrusted by a merchant. Here, the key sequence is designed to indicate the buyer's fingerprint. Hence, a buyer distributing the sequence may be traced. An excellent feature of our fingerprinting is the maintenance of an information gap between a buyer and a merchant by the generation of the key sequence in order to achieve the asymmetric property. In our protocol, content is partitioned into small packets and two kinds of watermarked packets for each packet are calculated. Subsequently, every set of two watermarked packets is encrypted using different keys selected from the key sequence. When a buyer receives the encrypted packets, he can decrypt one of them because the assigned key sequence is one of the selected keys. Since the buyer's key sequence indicates the buyer's fingerprint, the decompressed content from the decrypted packets also contains it. In this case, it is remarkable that a merchant cannot know which of the ciphertexts is decrypted by the buyer. Such a feature completes the asymmetric property in a fingerprinting protocol.

This paper is organized as follows. In the next section, we review the conventional fingerprinting schemes and highlight the problems. The proposed fingerprinting protocol is introduced in Sect. 3, and security is discussed in Sect. 4. The efficiency of the protocol is considered in Sect. 5. Finally, Sect. 6 concludes.

2. Overview of the Fingerprinting Protocol

The fingerprinting technique can prevent people from illegally redistributing digital content by enabling a merchant to identify the original buyer of the redistributed copy. In this paper, we consider the cryptographic protocol for fingerprinting. In the protocol, a merchant embeds a buyer's identity (fingerprint) in his content using a watermarking technique. Here, the protocol is classified into three schemes.

Symmetric Scheme: A merchant embeds a buyer's fingerprint in his content, and he knows the fingerprinted content after completion of the protocol. Thus, if the copy is found to be redistributed, the buyer can claim that it was done by the merchant. Further, a malicious merchant may try to frame an innocent buyer by illegally distributing the fingerprinted content.

Asymmetric Scheme: In order to solve the drawback in the symmetric scheme, a public key cryptosystem is applied to the fingerprinting protocol. Although both the merchant and the buyer can perform the encrypting operation using the buyer's public key, only the buyer can decrypt the ciphertext. Therefore, only the buyer obtains the fingerprinted content in the protocol.

Anonymous Scheme: To protect the buyer's privacy, neither the fingerprinted content nor the buyer's identity is revealed to a merchant. However, a buyer redistributing the content can be identified by the merchant by referring to the registration log at a trusted center.

In the asymmetric fingerprinting scheme [5]–[8], a buyer and a merchant jointly embed a fingerprint. First, the buyer encrypts a fingerprint and sends it to the merchant. The merchant verifies that the received ciphertext is made from the buyer's fingerprint and embeds it in his encrypted content by multiplying these ciphertexts based on the homomorphic property of the applied public key cryptosystem. If an operation on a ciphertext space results in an operation on the message space, the cryptosystem is homomorphic; principally, the former operation is multiplication and the latter is one of the three operations, *addition, multiplication,* and *exclusive or*, in public key cryptosystems. For example, RSA [10] and ElGamal [11] retain multiplicative properties, Okamoto-Uchiyama [12] and Paillier [13] retain additive property, and exclusive or operation is retained for quadratic residues [14]. Adaptive exploitation of such a property can help achieving asymmetric fingerprinting.

Let $E(m)$ be a ciphertext of a message m. The homomorphic property satisfies the following equation:

$$E(m_1) \cdot E(m_2) = E(f(m_1, m_2)), \tag{1}$$

where $f(\cdot)$ is one of the three above mentioned operations. If m_1 is regarded as digital content and m_2 as a fingerprint, the encrypted information can be embedded in the encrypted content by multiplying those ciphertexts. Only the buyer has the decryption key of the ciphertexts as these are calculated using buyer's public encryption key. Since the fingerprinted content is decrypted only by the buyer, the asymmetric property is satisfied. The embedding operation based on the homomorphic property is basically performed for each fingerprinting information bit; therefore, each bit is embedded in a corresponding position. Thus, m_1 is not the entire content, but one of the components, like the frequency elements to be fingerprinted by a watermarking technique. In order to maintain the secrecy of the embedding position, every component should be encrypted and sent to a buyer after embedding, thus encrypting the entire content.

Before beginning the protocol, a buyer must register at a trusted center to join the system. If a buyer redistributes an illegal copy, a merchant can trace the buyer from the registration log. The buyer then obtains the proof of registration like the digital signature from the center in order to convince the merchant that he is a legitimate user. The fingerprinting protocol begins with the sending of the proof by the buyer to the merchant.

The homomorphic property of public key cryptosystems enables achieving the asymmetric property of the fingerprinting protocol. Such a system can work in theory, but is extremely difficult to implement in a real network because it needs many computations and considerable network capacity. Generally, public key cryptosystems are used to share a common key for the symmetric cryptosystem that requires significantly fewer computations. However, in the above protocol, the entire content is encrypted based on public key cryptosystems. Unfortunately, the content cannot be compressed because of the following reason: The compression of the ciphertext is impossible because the value of the ciphertext acts like a random number. The content that is compressed before the enciphering operation must have a fingerprint embedded in it. However, it is desirable to embed a fingerprint in uncompressed content considering an attack that changes the format of the content [1]. Therefore, for robustness against the attack, the content should not be compressed in the conventional schemes. As a result, the amount of data being encrypted based on public key cryptosystems becomes very large, and hence the protocol becomes inefficient.

3. Proposed Fingerprinting Protocol

In this section, we propose a new fingerprinting protocol based on key management. In order to improve the computational costs and the amount of the transmission data, the symmetric cryptosystem is applied to the fingerprinted data after compression. Subsequently, the asymmetric property of the fingerprinting protocol is achieved by managing the key.

3.1 Initialization

There are three parties in our fingerprinting protocol buyer, merchant, and trusted center. Before beginning the transaction between a buyer and a merchant, both of them must register at a trusted center in order to set up the system.

First, a merchant prepares an initial key table such that each index $i, (1 \leq i \leq n)$ and its corresponding key k_i are listed, and defines a function $g(\cdot)$ to generate the extension key sequence. The size n implies the permissible number of users in our system. When a merchant joins the system, he registers the initial key table and $g(\cdot)$ with a trusted center. The initial key table is like a code book assigned for buyers. *Note:* The only security requirement for the initial key table is that no party other than the merchant and the center can access the table. Thus, the merchant can randomly produce the key table. In this case, the size of the table becomes large if the number of buyers is increased. However, it can be produced efficiently by following an encoding procedure like the cyclic code; in such an event, only the generator of the code is required.

Next, each buyer registers at the center. The center assigns a key to a buyer from the initial key table and produces the extended key sequence using a function $g(\cdot)$. The buyer's key sequence is selected from a part of the sequence based on the buyer's identity information.

Let k_i and its index i be the assigned key for the i-th buyer, then the extended key sequence is generated as

$$g(k_i) = \{k_{i,t} | 0 \leq t \leq 2L - 1\}. \qquad (2)$$

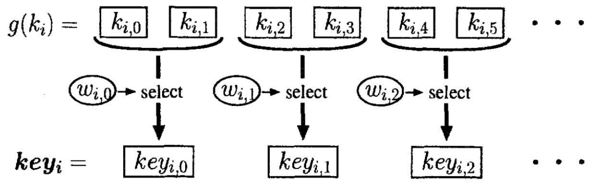


Fig. 1 Generation of a buyer's key.

The requirements for the function $g(\cdot)$ are enumerated as follows:

- For a given $k_{i,t}$, no information about $k_{i,t'}, (t \neq t')$ is leaked.
- For a given $g(k_i)$, no information about $g(k'_i), (i \neq i')$ is leaked.

The buyer's fingerprint is calculated from his identity information ID_i using an invertible function $h(\cdot)$ and a random number r_i

$$\boldsymbol{w}_i = h(ID_i \| r_i) \qquad (3)$$
$$= \{w_{i,j} | w_{i,j} \in \{0,1\}, 0 \leq j \leq L-1\}, \qquad (4)$$

where $\|$ implies concatenation. Following this, the center produces the buyer's key sequence

$$\boldsymbol{key}_i = \{key_{i,j} | 0 \leq j \leq L-1\}, \qquad (5)$$

where

$$key_{i,j} = \begin{cases} k_{i,2j} & (w_{i,j} = 0) \\ k_{i,2j+1} & (w_{i,j} = 1). \end{cases} \qquad (6)$$

Figure 1 briefly illustrates the procedure for generating the key sequence $\boldsymbol{key}_i$. When a buyer registers at the center, he receives his own key sequence $\boldsymbol{key}_i$ and its index i. The center also issues a registration proof reg_i like a signature so that the buyer can trade with a merchant. Here, $h(\cdot)$ is kept secret by the center and the information (ID_i, r_i, i, reg_i) is stored in the registration log. Note that the triplet $(\boldsymbol{key}_i, i, reg_i)$ is valid for one purchase from a merchant. If a buyer uses it more than twice, the anonymity of the buyer is not maintained and his security may be threatened.

It is remarkable that a buyer can be traced from the key sequence $\boldsymbol{key}_i$. Since in our setting, $key_{i,j}$ is selected from one of $k_{i,2j}$ and $k_{i,2j+1}$ based on $w_{i,j}$, the sequence $\boldsymbol{key}_i$ semantically indicates the hashed value of the buyer's identity. When a merchant finds a key sequence $\boldsymbol{key}_i$ and its index i, he can obtain the corresponding fingerprint $\boldsymbol{w}_i$ as follows: First, the merchant finds a key k_i by referring to his key table using the index i and generates the key sequence $g(k_i)$. By comparing the illegally distributed key sequence $\boldsymbol{key}_i$ with the generated sequence, each bit of $\boldsymbol{w}_i$ is easily identified. As a consequence, a buyer illegally distributing the sequence will be traced.

In our scheme, the secret information preserved by a trusted center is $(h(\cdot), r_i, \boldsymbol{w}_i)$, and the public information is $g(\cdot)$. The center does not reveal the fingerprint $\boldsymbol{w}_i$ to the merchant and the buyer. For anonymity, a buyer's identity ID_i

and his key sequence $\boldsymbol{key}_i$ are kept secret from a merchant. On the other hand, the merchant retains initial key table and the generated key sequence $g(k_i)$. As a result, an information gap is created between the buyer and the merchant.

3.2 Protocol

We now describe the fingerprinting protocol between a buyer and a merchant. The protocol begins by sending an index i and the registration proof reg_i from the buyer to the merchant. After verifying the proof, the merchant generates a key sequence $\boldsymbol{key}_i$ using a key k_i that can be identified from a key table by the index i. Using the generated key sequence $g(k_i)$, a requested content is encrypted based on the symmetric cryptosystem.

Let $X = \{X_j | 0 \le j \le L-1\}$ be the digital content of the merchant. The fingerprinting protocol is performed as follows:

Step. 1 A buyer sends his index i and registration proof reg_i to a merchant to begin a fingerprinting protocol.

Step. 2 The merchant verifies the validity of reg_i.

Step. 3 The merchant prepares the key k_i corresponding to the index i from a key table and generates the key sequence $g(k_i)$.

Step. 4 For each packet $X_j, (0 \le j \le L-1)$, the merchant performs the following operations (see Fig. 2).

4.1 Two kinds of packets $X_j^{(0)}$ and $X_j^{(1)}$ are calculated for one packet X_j by embedding information bit "0" and "1", respectively.

4.2 Both the packets $X_j^{(0)}$ and $X_j^{(1)}$ are compressed.

4.3 An information string that guarantees the success of the decryption is attached to each compressed packet.

4.4 The compressed packets with information strings are encrypted based on the symmetric cryptosystem. Following this, $k_{i,2j}$ is used for the compressed packet of $X_j^{(0)}$ and $k_{i,2j+1}$ is used for that of $X_j^{(1)}$. The produced ciphertexts are denoted by $c_j^{(0)}$ and $c_j^{(1)}$, respectively.

4.5 The order of the two ciphertexts is rearranged by a permutation function $\sigma_j\left(c_j^{(0)}, c_j^{(1)}\right)$.

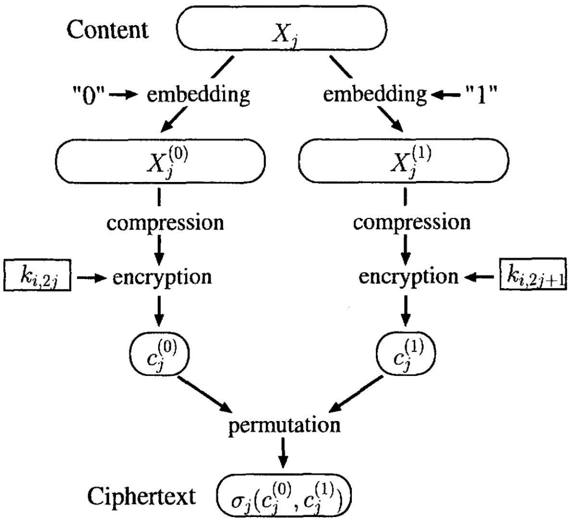


Fig. 2 Enciphering operation in the fingerprinting protocol.

Step. 5 The ciphertexts $\sigma_j\left(c_j^{(0)}, c_j^{(1)}\right), (0 \le j \le L-1)$ are sent to the buyer from the merchant.

Step. 6 The buyer decrypts parts of the ciphertexts using his key sequence $\boldsymbol{key}_i$ and decompresses the compressed files. Finally, the fingerprinted content can be obtained.

$$X^{(w_i)} = \{X_j^{(w_{i,j})} | w_{i,j} \in \{0,1\}, 0 \le j \le L-1\} \quad (7)$$

When enciphering operations are performed, $k_{i,2j}$ is used to encipher the compressed packet in which an information bit "0" is embedded. It is remarkable that $k_{i,2j}$ is selected for $key_{i,j}$ if the fingerprinting information bit $w_{i,j}$ is "0" in Eq. (6), otherwise $k_{i,2j+1}$ is selected. When the buyer tries to decrypt a received ciphertext $\sigma_j\left(c_j^{(0)}, c_j^{(1)}\right), (0 \le j \le L-1)$, he obtains two bit strings. One is a properly compressed packet that contains $w_{i,j}$, and the other is a random number that implies decryption failure. The buyer easily finds the proper bit string using the attached information string. Therefore, what the buyer obtains from the ciphertext $\sigma_j\left(c_j^{(0)}, c_j^{(1)}\right)$ is $X^{(w_{i,j})}$ in Step 6. Consequently, the buyer can obtain the fingerprinted content $X^{(w_i)}$. In our protocol, the merchant can embed a signal in his digital content; however, he cannot know which ciphertext of $(c_j^{(0)}, c_j^{(1)})$ is decrypted by the buyer.

3.3 Tracing

When a buyer distributes an illegal copy, he must be identified by extracting the embedded fingerprint. We discuss the tracing method and the requirement for our system.

When a merchant finds an illegal copy, he tries to extract a fingerprint. If he succeeds, he sends the extracted fingerprint $\hat{w}_i$ to a trusted center in order to find out the corresponding buyer. As the center knows the invertible operation $h^{-1}(\cdot)$, the identity of the illegal buyer is specified. Since only the buyer has the fingerprinted content that contains his fingerprint, he cannot repudiate the allegations of illegal distribution of the content.

Step. 1 A merchant sends a fingerprint $\hat{w}_i$ to a trusted center.

Step. 2 The center decodes the buyer's identity,

$$ID_i \| r_i = h^{-1}(\hat{w}_i), \quad (8)$$

and checks the relationship between ID_i and r_i by referring to the registration logs.

Step. 3 Before revealing the identity ID_i to the merchant, the center requests proof that guarantees the transaction between the buyer and the merchant.

3.1 The center sends an index i.

3.2 The merchant returns the corresponding registration proof reg_i received from a buyer.

3.3 The buyer is regarded a traitor if reg_i is valid, otherwise the merchant is guilty.

3.4 Features

In a generic watermarking technique, an attacker cannot modify/delete the embedded information without a secret key to embed information. The same key is also required for the extraction of a watermark. If a different key is used to produce marked packets $X_j^{(0)}$ and $X_j^{(1)}$ for each buyer, a merchant may not be able to identify the secret key uniquely to extract a fingerprint from an illegal copy because he does not know which key is used to embed a fingerprint. Therefore, we give the following definition.

Definition 1: The ciphertexts $\sigma_j\left(c_j^{(0)}, c_j^{(1)}\right)$ are calculated from the same marked packets $X_j^{(0)}$ and $X_j^{(1)}$ for every buyer, although the enciphering keys are different.

From definition 1, the marked packets $X_j^{(0)}$ and $X_j^{(1)}$ can be calculated before trade with a buyer. Therefore, operations 4.1 and 4.2 in the protocol should be performed before trade.

In a market, varied content is displayed and sold to multiple buyers. In our scheme, the required computations during trade with buyers reduce if the marked and compressed packets have been previously prepared by a merchant. For example, assume that a merchant possesses α contents $X_s, (1 \leq s \leq \alpha)$. Before selling those contents, he pre-processes them and stores the marked and compressed ones $\boldsymbol{x}_s^{(0)}$ and $\boldsymbol{x}_s^{(1)}$. In each request from buyers for the content X_s, the merchant encrypts only $\boldsymbol{x}_s^{(0)}$ and $\boldsymbol{x}_s^{(1)}$ using the key sequence generated from k_i that is determined by the buyer's index i. Since the symmetric cryptosystem is applied in our scheme, the enciphering operation can be performed in real-time. Streaming of the fingerprinted contents may be possible if one selects a streaming cipher for the symmetric cryptosystem.

For the realization of our scheme, robustness against compression must be satisfied for the applied watermark technique. In our scheme, compression is performed merely to reduce of the redundancy in content and not to eliminate the embedded information as an attack. Therefore, it is rather easy to satisfy the requirement for the existing watermarking schemes. However, considering the attacks from malicious buyers, a robust watermarking technique should be applied. Since the embedding operation can be performed independent of the buyer's identity, any watermarking technique can be applied.

4. Security Analysis

4.1 Security for the Buyer

In a fingerprinting protocol, information pertaining to an innocent buyer should not be leaked to a merchant. Therefore, we should consider the anonymity of the buyer and the secrecy of his key sequence. Here, we assume that a merchant never colludes with a trusted center. Thus, the center is absolutely trusted in our protocol. It is clear that if a buyer distributes his key sequence, he can be traced as discussed in the previous section. The following discussion pertains to the merchant with regard to whether he can obtain some information about the buyer during the protocol.

- *Anonymity of a buyer*

  In the protocol, a buyer only reveals an index i assigned to him from a trusted center. Hence a merchant can not know the relationship between the index i and the buyer without referring to the registration log of the center.

A merchant can generate every key sequence as he has the initial key table and the function $g(\cdot)$. However, the merchant cannot obtain information on the buyer's key sequence $\boldsymbol{key}_i$ from the generated ones $g(k_i)$, even if the index i of the key is revealed.

- *Secrecy of a buyer's sequence*

  The buyer's key sequence $\boldsymbol{key}_i$ is generated by selecting a part of the key sequence $g(k_i)$. The selection depends on the buyer's fingerprint $\boldsymbol{w}_i$ that is generated from the buyer's identity ID_i using a function $h(\cdot)$. Therefore, without $\boldsymbol{w}_i$, it is impossible to know which of the two sequences $k_{i,2j}$ and $k_{i,2j+1}$ is selected for $key_{i,j}$. Since the identity of a buyer and $h(\cdot)$ are kept secret by a trusted center, a merchant cannot obtain the fingerprint $\boldsymbol{w}_i$ and, hence, cannot obtain $\boldsymbol{key}_i$.

In our fingerprinting protocol, both a buyer and a merchant cannot know the fingerprint $\boldsymbol{w}_i$ itself. They only exchange related information such as the index i and ciphertexts. Even if the merchant is able to send the ciphertexts that the buyer obtains with a specified fingerprinted content, the probability that the merchant can frame an innocent buyer is equal to the probability of guessing $\boldsymbol{w}_i$.

In a tracing protocol, a merchant may try to frame an innocent buyer by generating a binary sequence randomly. Here, if the function $h(\cdot)$ is assumed to be an encoder such that ID_i is encoded to a binary code, the success probability of such an attack can be decreased by designing a low coding rate. This seems to make the system inefficient, but only a few expansion of the rate is adequate. The merchant may be suspected by the center as a hostile party depending on the number of trials of the attack. For example, if a merchant submits wrong fingerprints (that have not been assigned to buyers) many times, the center can detect the illegal action of the merchant.

If a merchant colludes with a hostile buyer, the center can obtain the buyer's fingerprint and attempt to analyze the encoding function $h(\cdot)$. However, no innocent buyer will be framed even if the attack succeeds because of the following reason. Each fingerprint $\boldsymbol{w}_i$ is generated from each user's identity ID_i and each random number r_i. Hence, the random number makes it difficult to produce a valid fingerprint. Furthermore, the merchant must present the valid registration proof in the tracing protocol, which is equivalent to break the digital signature scheme applied at the trusted center.

Since the triplet $(\boldsymbol{key}_i, i, reg_i)$ is issued for each fingerprint $\boldsymbol{w}_i$ and is used only once, an illegal buyer is accused only for the corresponding illegal distribution. Even if a merchant finds one fingerprint $\boldsymbol{w}_i$, he cannot abuse it to frame a buyer for the redistribution of other content. Therefore, the one-time triplet guarantees the security of the buyer.

4.2 Security for the Merchant

A fingerprint should be extracted correctly from an illegal copy. It should not be modified or deleted by attacks. In this subsection, we discuss the security with regard to the merchant in the proposed fingerprinting protocol.

First, we consider the information that a buyer can obtain during the protocol. It is clear that a buyer can obtain his key sequence $\boldsymbol{key}_i$, its index i and the registration proof reg_i from a trusted center. However, he cannot obtain further information for the following reason. When a buyer registers at a trusted center, a key sequence $\boldsymbol{key}_i$ and its index i are issued. The key sequence is generated from the functions $g(\cdot)$ and $h(\cdot)$ using the original key k_i, but these parameters are not revealed to the buyer. Since the function $g(\cdot)$ satisfies two requirements, the buyer can obtain no information on the other keys $k_{i,j}$ and the key sequence $g(k_i')$ from $\boldsymbol{key}_i$. One candidate for such a function is a chaotic sequence generator [15], [16]. It is composed of a deterministic equation, but the generated sequence is randomly distributed and is unpredictable. If the parameters of the function are controlled by the key k_i, the analysis of the function becomes difficult and, hence, a buyer can obtain no useful information on the other keys. The registration proof reg_i is merely the signature that guarantees the legitimacy of the buyer. Hence, he cannot know the procedure to generate his key sequence due to the lack of information.

For each packet X_j, a buyer receives two ciphertexts $c_j^{(0)}$ and $c_j^{(1)}$ containing the information bits "0" and "1", respectively. However, a buyer has only one of the decryption keys of the ciphertexts. A merchant encrypts the marked packets $X_j^{(0)}$ and $X_j^{(1)}$ using $k_{i,2j}$ and $k_{i,2j+1}$, respectively. However, a buyer's key $key_{i,j}$ is selected from one of these two keys, and the selection is governed by a trusted center. Because of the secrecy of the operation, a buyer cannot know the other key; hence, both the ciphertexts $c_j^{(0)}$ and $c_j^{(1)}$ are not decrypted by the buyer. What the buyer obtains from the ciphertexts is $X_j^{(w_{i,j})}$, and the original packet is withheld from him. If the order of the ciphertexts is known, a buyer can know the embedded information bit from the decrypted packet. However, the random permutation $\sigma_j\left(c_j^{(0)}, c_j^{(1)}\right)$ makes it difficult to determine the order. As a consequence, a buyer cannot obtain the embedded information bit.

From the above discussion, it is evident that no information on a buyer's fingerprint is leaked from the transmitted ciphertexts to the buyer. It is difficult for a buyer to analyze the fingerprint by himself from the fingerprinted content. However, some buyers may collude and try to find the embedded fingerprint by comparing their fingerprinted contents. Considering a collusion of hostile buyers, it may be effective to apply a collusion resistant code such as c-secure code [2] and ACC [3]. Such codes can be generated by a function $h(\cdot)$ when a buyer's key sequence is produced at a trusted center.

5. Considerations

5.1 Asymmetric Property

In order to convince a third party that a buyer has redistributed an illegal copy, a merchant must not obtain the fingerprinted content in the protocol. As mentioned in the previous section, a merchant cannot know a buyer's key sequence $\boldsymbol{key}_i$ which is a partial sequence of the key sequence $g(k_i)$. Hence, he cannot know which of the transmitted ciphertexts $c_j^{(0)}$ and $c_j^{(1)}$ is decrypted by a buyer. Therefore, a merchant cannot obtain the fingerprinted content until a buyer redistributes it. As a consequence, our fingerprinting protocol has an asymmetric property.

5.2 Efficiency

In general, multimedia content such as music, images, and movies must be compressed because they contain a lot of redundancy that can be reduced efficiently without serious degradation of their quality. However, in order to achieve an asymmetric property by applying the homomorphic property of public key cryptosystems, the digital content cannot be compressed in the conventional fingerprinting protocols. The message space of the ciphertext is not utilized efficiently in several schemes [5], [6], [8]. In [7], although the entire message space is used, the enciphering rate of the cryptosystem is 1/3 when the Okamoto-Uchiyama encryption scheme [12] is applied (1/2 for the Paillier scheme [13]). The enciphering rate of our scheme is 1/2 as two types of marked packets are produced from one packet. However, the total amount of the transmission data is reduced by compressing the marked packets before the encryption. Since there is considerable redundancy in multimedia content, the compression rate may become very high. Therefore, the amount of transmitted data is much smaller than the conventional schemes. It is unrealistic to encipher uncompressed content and to transmit the expanded ciphertext.

With regard to the estimation of the total amount of computation, accurate numerical comparison may be difficult because it depends on the applied cryptosystems, embedding operation, and compression algorithm. Nevertheless, our scheme has such an attractive property that the watermarked and compressed content are produced while off line. It enables our fingerprinting protocol to be performed

Table 1 Comparison of efficiency.

	Conventional	Proposed
cryptosystem	public key	secret key
enciphering rate	3(2)	2
compression	impossible	possible
off-line protocol	impossible	possible

on the fly because only the enciphering operation like stream cipher is required during the on-line protocol. Furthermore, the off-line operations which are mainly compression and embedding, are performed only once for each content in our scheme. For a merchant, once the sale of the content is completed, the transactions with the buyers are not a time-consuming task as compared with the conventional scheme that must perform enciphering and embedding operations for each order from each buyer. The comparisons are summarized in Table 1. A drawback of our scheme is the size of the user key sequence that is issued by a trusted center. If the size of each secret key applied for the enciphering of each packet is 128 bits and the number of packets is L, then the total size of the user key sequence becomes $128L$. Achieving a reduction in the size of the user key sequence will constitute our future work.

5.3 Comparison with Related Works

Although the distribution of fingerprinted content is achieved by a symmetric scheme in [9], almost all computations required for the protocol are performed by a trusted third party; such an operation is performed when a buyer places orders with a merchant. In our scheme, the trusted center only issues key sequences for users, and the distribution of the fingerprinted content is performed between a buyer and a merchant in a real-time operation because of the off-line computations. Hence, the protocol in our scheme is more suitable for realization.

From the viewpoint of distributing several variants of each packet, our scheme is similar to a dynamic traitor tracing scheme [17]. A data supplier distributes a variant to each user in order to trace an illegal user once the variant is redistributed. The scheme introduces a dynamic setting in which on-line feedback from illegal users may be detected by the data supplier. This enables the supplier to find the traitors by adaptively distributing a variant to each user. However, the dynamic setting is applicable only for the symmetric tracing system because the dynamical selection of the variants is managed by the supplier. If the management is performed by a trusted center in order to achieve the asymmetric property, the characteristic of the dynamic setting does not function. Furthermore, the dynamic setting requires real-time feedback from illegal users, which can be easily avoided. As opposed to the dynamic setting, our scheme is a static setting that can activate the tracing operation whenever illegal copies are found. In such a scenario, tracing a traitor from illegally distributed media such as CD, DVD, USB storage devices, etc. is possible.

6. Conclusion

We have proposed a new fingerprinting protocol based on key management by a trusted center. The center only issues key sequences for users during registration, and the fingerprinting protocol is performed between a buyer and a merchant. Since symmetric cryptosystems can be applied in our scheme, the required computation is considerably lesser than the conventional schemes that exploit the homomorphic property of public key cryptosystem. By assigning a proper key sequence to each buyer, only a part of the transmitted ciphertexts is decrypted, which is the fingerprinted content. With the assistance of a compression algorithm, our scheme can reduce both the computational costs and the amount of transmission data.

Acknowledgment

A part of this research was supported by The Asahi Glass foundation—Research Assistance for Encouraging Themes. The authors would like to thank deeply for the great contribution.

References

[1] S. Katzenbeisser and F.A.P. Petitcolas, Information hiding techniques for steganography and digital watermarking, Artech House Publishers, Jan. 2000.

[2] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," IEEE Trans. Inf. Theory, vol.44, no.5, pp.1897–1905, 1998.

[3] W. Trappe, M. Wu, Z.J. Wong, and K.J.R. Liu, "Anti-collusion fingerprinting for multimedia," IEEE Trans. Signal Process., vol.51, no.4, pp.804–821, 2003.

[4] B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting," Proc. EUROCRYPT'96, LNCS 1070, pp.84–95, Springer-Verlag, 1996.

[5] N. Memon and P.W. Wong, "A buyer-seller watermarking protocol," IEEE Trans. Image Process., vol.10, no.4, pp.643–649, 2001.

[6] B. Pfitzmann and A. Sadeghi, "Coin-based anonymous fingerprinting," Proc. EUROCRYPT'99, LNCS 1592, pp.150–164, Springer-Verlag, 1999.

[7] M. Kuribayashi and H. Tanaka, "A new anonymous fingerprinting with high enciphering rate," Proc. INDOCRYPT2001, LNCS 2247, pp.30–39, Springer-Verlag, 2001.

[8] J.G. Choi, K. Sakurai, and J.H. Park, "Does it need trusted third party? Design of buyer-seller watermarking protocol without trusted third party," Proc. ACNS2003, LNCS 2846, pp.265–279, Springer-Verlag, 2003.

[9] A.M. Balleste, F. Sebe, J.D. Ferrer, and M. Soriano, "Practical asymmetric fingerprinting with a TTP," Proc. DEXA'03, pp.352–356, 2003.

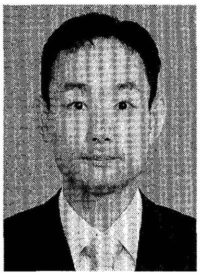
[10] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Commun. ACM, vol.21, no.2, pp.120–126, 1978.

[11] T. Elgamal, "A public key cryptosystem and a signature based on discrete logarithms," IEEE Trans. Inf. Theory, vol.IT-31, no.4, pp.469–472, 1985.

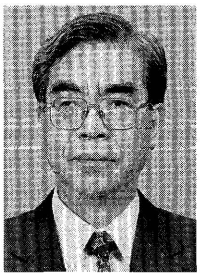
[12] T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring," Proc. EUROCRYPT'98, LNCS 1403, pp.308–318, Springer-Verlag, 1998.

[13] P. Paillier, "Public key cryptosystems based on degree residuosity classes," Proc. Eurocrypt'99, LNCS 1592, pp.223–238, Springer-Verlag, 1999.

[14] G. Brassard, D. Chaum, and C. Crepeau, "Minimum disclosure proofs of knowledge," J. Comput. Syst. Sci., vol.37, no.2, pp.156–189, 1988.
[15] C.E. Shannon, "Communication theory of secrecy systems," Bell Sys. Tech. J., vol.28, no.4, pp.656–715, 1949.
[16] S.C. Phatak and S.S. Rao, "Logistic map: A possible random-number generator," Phys. Rev. E, vol.51, no.4, pp.3670–3678, 1995.
[17] A. Fiat and T. Tassa, "Dynamic traitor tracing," J. Cryptology, vol.14, pp.211–223, 2001.



Minoru Kuribayashi received the B.E., M.E., and D.E. degrees from Kobe University in 1999, 2001, and 2004 respectively. Since 2002, he has been a Research Associate in the Department of Electrical and Electronics Engineering, Kobe University. His research interests are in digital watermark, information security and cryptography.



Hatsukazu Tanaka received the B.E. degree from Kobe University, Kobe, Japan in 1964, the M.E. degree in 1966, and the D.E. degree in 1969, both from Osaka University, Osaka, Japan. He joined the Faculty of Engineering, University of Osaka Prefecture as a Research Associate in 1969. In 1973 he was appointed as an Associate Professor in the Department of Electrical Engineering, Kobe University. From 1988 through 2004 he was a Professor in the Department of Electrical and Electronics Engineering, Kobe University. Since 2005 he has been a Professor Emeritus of Kobe University and a President of Kobe Institute of Computing (Graduate School of Information Technology). From 1980 through 1981 he was a member of the Communication Group of the University of Toronto, Toronto, Ontario, Canada, as a Visiting Scientist. His main work is on the basic theory of Information Engineering such as Information Theory, Coding Theory, Cryptography and Information Security, Image Processing, etc. Dr. Tanaka is a Fellow of IEEE, and a member of IACR.