JOURNAL OF KOREA MULTIMEDIA SOCIETY, VOL. 7, NO. 12, DECEMBER 2004(pp. 1708-1718)

Design of Digital Fingerprinting Scheme for Multi-purchase

JaeGwi Choi[†], KyungHyune Rhee[††]

ABSTRACT

In this paper, we are concerned with a digital fingerprinting scheme for multi-purchase where a buyer wants to buy more than a digital content. If we apply previous schemes to multi-purchase protocol, the number of execution of registration step and decryption key should be increased in proportion to that of digital contents to be purchased in order to keep unlinkability. More worse, most of fingerprinting schemes in the literature are based on either secure multi-party computation or general zero-knowledge proofs with very high computational complexity. These high complexities complicate materialization of fingerprinting protocol more and more. In this paper, we propose a multi-purchase fingerprinting scheme with lower computational complexity. In the proposed scheme, a buyer executes just one-time registration step regardless of the number of contents to be purchased. The number of decryption key is constant and independent of the number of contents to be purchased. We can also reduce the computational costs of buyers by introducing a concept of proxy-based fingerprinting protocol.

Keywords: Digital fingerprinting, multi-purchase, proxy signature, one-time registration

1. INTRODUCTION

Digital fingerprinting schemes are techniques applied to protect the copyright on digital contents. This is similar to digital watermarking, except that different information such as a user ID is embedded in each distributed contents. Thus it enables a seller to trace the owner(buyer) of an illegally distributed digital contents.

In this paper, we are concerned with multi-purchase fingerprinting scheme. In here, "multi-purchase" means that a buyer buys more than a digital content at a time. In general E-commerce, after a buyer looks up contents in the web site, she/he will order many contents at once. Thus it is necessary to propose an efficient multi-purchase digital fingerprinting. But most of previous works have focused on offering of new function or improvement of efficiency on one-purchase digital fingerprinting.

Let us suppose previous schemes applied to multi-purchase environments. What is important in anonymous fingerprinting scheme is to offer buyer's anonymity and unlinkability of digital contents. The unlinkability means that anyone cannot determine whether digital contents were purchased by the same buyer. Consider the case that the anonymity holds, and the unlinkability does not hold. Then, if a party can trace the buyer from a transcript by any other means, the party can also trace all transcripts of the buyer. In addition, it facilitates de-anonymization[1,2], that is, given the history of linkable transcripts of an anonymous buyer, a party may compare the history with the seller's information about when, what, and how many contents each real person

※ Corresponding Author : JaeGwi Choi, Address : (608-736) 314-79, Daeyeon-Dong, Nam-Gu, Busan, Korea, TEL : +82-51-620-6395, FAX : +82-51-626-4887
E-mail : jae@mail1.pknu.ac.kr
Receipt date : March 23, 2004, Approval date : Aug. 19, 2004
[†] Dept. of Information Security, Pukyong National Univ.
[††] Divison of Electronic, Computer and Telecommunication Engineering, Pukyong National Univ.
(E-mail : khrhee@pknu.ac.kr)
※ This work was supported by grant No.01-2002-000-00589-0 from the Basic Research Program of the Korea Science and Engineering Foundation (KOSEF).

purchase, and thus may trace the buyer. Because use of the same anonymous public key implies that the buyer's purchases are linkable, each digital contents must be purchased with each different pseudonym. In order to obtain several different pseudonyms, a buyer must go through the registration step several times in the previous schemes. The buyer must store secret keys corresponding with anonymous buyer's public keys for decryption, if the fingerprinted contents are encrypted with buyer's anonymous public key[3,4]. It is so inefficient.

In general, the watermarked contents can be made in off-line, because every sold copy is the same. On the contrary, buyers have to connect at the seller's server for buying digital contents in fingerprinting schemes, because every sold copy is slightly different from the original contents and unique to its buyer. But buyer's memory and computation power are very small relatively to ones of sellers. And it is certain that the computational cost of buyers in multi-purchase environment is larger than one-purchase environment. Thus we conclude that digital fingerprinting schemes that require much computation cost to the buyer are not suited to real applications. In fact, a step that requires the highest computation cost among steps (registration step, fingerprinting step, and identification step) is fingerprinting one. In the previous schemes, buyers must execute at least two steps: registration and fingerprinting with high computation complexity. It is not suited to the customer-centered commercial transaction.

In this paper, we the first suggest multi-purchase digital fingerprinting scheme. The purpose of this study is to propose a method whose computational cost is smaller than the typical method that an ordinary scheme is used repeatedly.

The followings are the notable features of our scheme.

- Buyers execute just one-time registration step.
- The number of necessary key to the buyer is constant independent of that of digital contents to be purchased. In our protocol, buyers can decrypt all encrypted contents with one decryption key even if each digital contents was encrypted with each different key.
- Anyone (except TTP) cannot determine whether any digital contents were purchased by the same buyer.
- Our scheme reduces the amount of buyers' computations to the minimum. In our protocol, buyers have to execute only the least step (registration and delegation step).

The paper is organized as follows. Section 2 describes previous schemes and requirements for multi-purchase digital fingerprinting protocols. Section 3, where our methodologies are shown. Then, the proposed multi-purchase fingerprinting scheme is described in Section 4. Security and efficiency of the proposed scheme are discussed in Section 5. Finally, we conclude in Section 6.

2. RELATED WORKS

2.1 Previous Schemes

Classical fingerprinting schemes are symmetrical in the sense that both the seller and the buyer know the fingerprinted copy. Thus, if another copy with the fingerprint turns up, the buyer can claim that the seller redistributed it. In order to solve the problem, an asymmetric fingerprinting[5] was proposed. Here, because only the buyer can obtain the exact fingerprinted copy, he/she cannot claim that an unauthorized copy may have originated from the seller. But the drawback of this solution is that the seller knows the buyer's identity even if the buyer is honest. Later, the concept of anonymous fingerprinting was introduced to protect buyer's anonymity[6]. The idea is that sellers can know neither the fingerprinted copy nor the buyer's identity. The problem with the constructions is

that, being based on secure multiparty computations needed much computation such as discrete logarithm problem or graph isomorphic problem[7]. Their complexity is much too high to be implementable in practice. Later, a scheme efficiently and completely specified from a computational point of view was proposed[8]. But it is insecure in the seller's dishonesty, and also has disadvantages that all buyers who bought a copy of digital contents have to participate in identification step to identify a traitor. Recently, two schemes[4,9] were suggested efficient methods without secure two party computations. But one[9] is also impractical because it used the Boneh's code[10] as a building block for collusion resistance. The code is so long that the overall system cannot be practical. The other scheme[4] used invisible watermarking algorithm[11] as a building block. The algorithm[11] uses normally distributed random values as watermarks, which are highly resistant to collusion attacks. The scheme[4] is a significant scheme in the sense that it provided possibility of efficient materialization.

2.2 Requirements of Digital Fingerprinting Schemes

Requirements of fingerprinting scheme are similar to the requirements of digital watermarking system, but there are a few different requirements. They can be listed as follows[4,6].

- **Anonymity**: A buyer should be able to purchase digital contents anonymously.
- **Unlinkability**: Given two digital contents, nobody can decide whether these two contents were purchased by the same buyer or not.
- **Traceability**: The buyer who has distributed digital contents illegally (traitor/copyright violator) can be traced.
- **No Framing**: An honest buyer should not be falsely accused by a malicious seller or other buyers.
- **No Repudiation**: The buyer accused of reselling an unauthorized copy should not be able to claim that the copy was created by the seller or a security breach of the seller's system.
- **Collusion tolerance**: Attacker should not be able to find, generate, or delete the fingerprint by comparing the copies, even if they have access to a certain number of copies.
- **Efficient materialization**: It is efficiently and completely specified from a computational point of view.
- **Efficient expansion of multi-purchase protocol**: It should be efficiently expanded to multi-purchases protocol. At least, it should be protocol whose computational cost is smaller than the typical method that an ordinary scheme is used repeatedly.

Note that we have added 7,8 requirements compared with the schemes[4,6].

3. OUR METHODOLOGY

3.1 Homomorphic Encryption

Our scheme is constructed based on a private watermarking scheme and a public key encryption scheme with homomorphic property defined as follows. We use these schemes in order to remove interaction between a buyer and a seller in the embedding step (fingerprinting step). Because security of our scheme relies on the one of the discrete logarithm problem, we can apply a homomorphic encryption[12] to our scheme.

A cryptosystems $E: G \rightarrow R$ defined on a group $(G, \cdot)$ is said to be homomorphic if f forms a (group) homomorphism. That is, given $E(x)$ and $E(y)$ for some unknown $x, y \in G$, anyone can compute $E(x, y)$ without any need for the private key. For instance, RSA cryptosystems has the property that $E(x) \cdot E(y) = E(x \cdot y)$. Besides RSA, several other homomorphic cryptosystems such as ElGamal[12] and Paillier cryptosystems[13] are

currently known. Others have proposed a number of other public key encryption schemes that have various useful homomorphic properties[14]. Somewhat surprisingly, this property has a wide range of applications, including secure voting protocols and multiparty computation.

3.2 Proxy Signature

The buyer has to connect at the seller's server for buying digital contents in fingerprinting schemes, because every sold copy is slightly different from the original contents and unique to its buyer. Besides buyers have a small memory and a little computation capability relatively to sellers. Thus, if it is extended to multi-purchase fingerprinting scheme, the burden of the buyers increases more. We propose a proxy signature-based model in order to reduce the amount of buyers' computations.

Proxy signature is a signature scheme that an original signer delegates his/her signing capability to a proxy signer, and then the proxy signer creates a signature on behalf of the original signer. Many studies have been made on proxy signatures[15, 16]. Here we review one scheme[16] of them.

- p: A large prime
- q: A prime factor satisfying $q \mid p-1$.
- g: An element in Z_p^* whose order is q.

Assume that Alice (buyer), who is keeping a secret key x and has published the corresponding key $y = g^x \pmod p$, wants to delegate signing capability to Bob (proxy agent). The scheme is constructed as follows.

(1) Alice selects a random number $\overline{k}$ and computes $\overline{r} = g^{\overline{k}} \pmod p$, and sends to $\overline{r}$ to Bob.

(2) Bob randomly chooses $a \in Z_q$ and computes $r = g^a \cdot \overline{r} \pmod p$. Then he communicates r to Alice.

(3) Alice computes $\overline{s} = rx + \overline{k} \pmod q$ and forwards $\overline{s}$ to Bob.

(4) Bob computes $s = \overline{s} + a \pmod q$ and accepts s as a valid proxy signature key, if the following equation holds: $g^s = y^r r \pmod p$.

Hence, Bob can apply ElGamal type digital signature scheme to sign any given message using his secret key s. The verification algorithm however uses the public key $y' = y^r r \pmod p$.

4. A MULTI-PURCHASE FINGERPRINTING SCHEME

In this section, we describe the proposed anonymous fingerprinting scheme for multi-purchase. Our scheme is based on [4] scheme as fingerprints-embedding method and [11,17] schemes as building block for collusion resistance.

[Assumptions]

For ease of exposition we assume that the contents being sold is a still image, though in general the protocol is also applicable to audio and video data like [3,4] schemes. We also assume that all of the underlying primitives are secure and registration center and fingerprint certificate center do not collude with sellers and buyers.

[System Set-up]

Let $p \leq n(bits)$ be a large prime such that $q = (p-1)/2$ is also prime. Let G be a group of order $p-1$, and let g be a generator of G such that computing discrete logarithms to the base g is difficult.

[Notations]

The fingerprinting insertion step can be represented as $Ima^* = Image \oplus F$, where

- $Image$: Original image to be a vector of "features", $Image = \{ima_1, \cdots ima_m\}$.
- F: Fingerprints as a vector of "fingerprint elements", $F = \{f_1, \cdots, f_n\}$ with $m \geq n$.
- Ima^*, Ima^{**}: Fingerprinted image

- $\oplus$: Insertion operation, $Image \oplus F = \{ima_1 \oplus f_1, \cdots, ima_n \oplus f_n, ima_{n+1}, \cdots, ima_m\}$
- E/D: Encryption/Decryption scheme with homomorphic property.

[Roles of each entity]

The entities of our scheme consist of registration center (RC), fingerprint certificate center (FCC), a proxy agent, a buyer, and a seller. The role of each entity is as follows:

• Registration Center (RC)
- He generates buyers' anonymous public key and certifies it.
- He has private and public key, $x_R, y_R = g^{x_R} \pmod p$.

• Fingerprint Certificate Center (FCC)
- He generates random fingerprints in the required manner and issues them at user's (Proxy agent) request.
- He has private and public key, $x_F, y_F = g^{x_F} \pmod p$.

• Proxy Agent
- He carries out fingerprinting steps instead of buyers.
- He can sign messages about purchasing on behalf of the buyer after execution delegation protocol.
- He has private and public key, $x_P, y_P = g^{x_P} \pmod p$.

• Buyer
- He has private key and public key, $x_B, y_B = g^{x_B} \pmod p$.

• Seller
- She is an agent selling digital contents.

The proposed anonymous fingerprinting scheme for multi-purchase consists of the following 5 steps. The outline of our scheme appears in Fig. 1. Here, we assume that a buyer wants to buy $K(\geq 1)$ digital images.

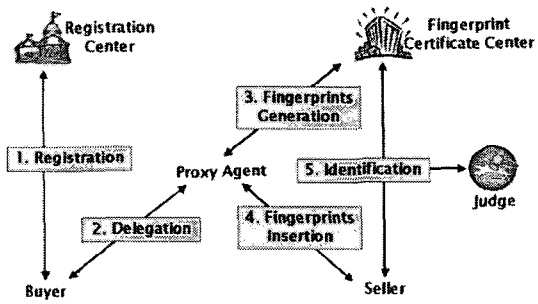


Fig. 1. Outline of Our Scheme.

4.1 One-time Registration Step

A buyer registers to RC as follows:

(1) A buyer chooses secret random x_{B1} and x_{B2} in Z_p such that $x_{B1} \cdot x_{B2} = x_B \in Z_p$. He sends $y_B^* = g^{x_{B1}} \pmod p$ and encrypting x_{B2} using RC's public key y_R such as $E_{y_R}(x_{B2})$ to RC. y_B^* is anonymous public key of the buyer. The buyer convinces the RC of zero-knowledge of possession of x_{B1}. The proof given in [18] scheme for showing possession of discrete logarithms may be used here.

(2) The RC first decrypts $E_{y_R}(x_{B2})$ using his private key x_R and checks that $(y_B^*)^{x_{B2}} = y_B \pmod p$. If it is verified, RC returns to the buyer certificates $Cert(y_B^*)$ that state the correctness of y_B^*.

(3) RC keeps them, $(y_B, Cert(y_B^*), y_B^*)$, secretly in his secure user information database RC_DB.

4.2 Delegation Step

An anonymous buyer and a proxy agent execute a delegation step. Here, an anonymous buyer delegates the power of signing (purchase contents) to the proxy agent. After this step, the proxy agent is able to perform the rest of fingerprinting step on behalf of the buyer. The delegation step of our scheme appears in Fig. 2.

(1) An anonymous buyer chooses secret random $\overline{k}$ and computes $\overline{r} = g^{\overline{k}} \pmod p$. Then he sends to $\overline{r}$ to a proxy agent.

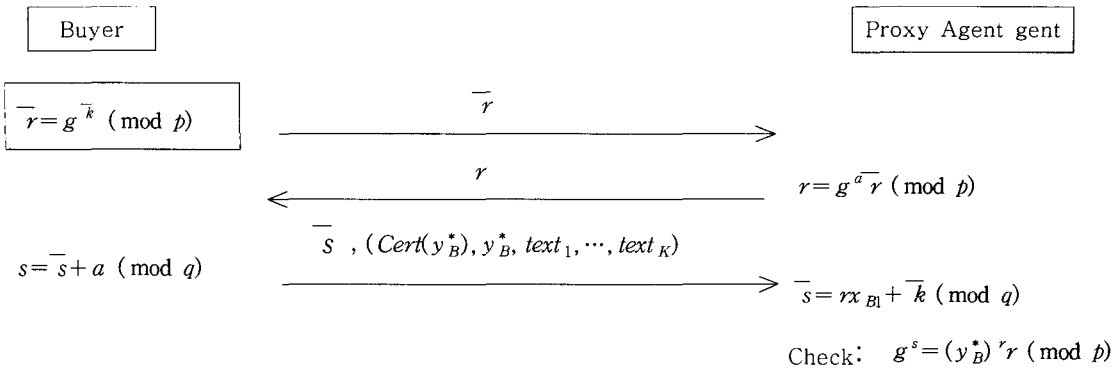


Fig. 2. Delegation Step.

(2) The proxy agent randomly chooses $a \in Z_q$ and computes $r=g^a \cdot \bar{r} \pmod p$.
Then he communicates r to the buyer.

(3) The buyer computes $\bar{s}=rx_{B1}+\bar{k} \pmod q$ and sends $\bar{s}$, and $(Cert(y_B^*), y_B^*, text_1, \cdots, text_K)$ to the proxy agent. Where $text_i$, $(1 \le i \le K)$ is a string identifying each purchase

(4) The proxy agent computes $s=\bar{s}+a \pmod q$. If $g^s=(y_B^*)^r r \pmod p$ is hold, he accepts s as a valid proxy signature key.

The proxy agent can apply ElGamal type digital signature schemes to sign any given messages using his secret key s. The verification algorithm uses the public key $y_P^*=(y_B^*)^r r \pmod p$.

4.3 Fingerprints Generation Step

This protocol is performed between FCC and the proxy agent. This step appears in Fig. 3.

4.3.1 Fingerprints generation

(1) The proxy agent sends $(Cert(y_B^*), y_B^*, K, y_P^*, Sign_P)$ to the FCC, where $Sign_P$ is a signature on $(Cert(y_B^*), y_B^*, K)$ made with proxy secret key s, K is the number of contents to be purchased.

(2) FCC first verifies $Sign_P$ by using $y_P^*, (y_B^*, r)$ and checks the certificate, $Cert(y_B^*)$ on y_B^*. If they are verified, FCC generates fingerprints $(F_1, \cdots, F_K)$ randomly as many as the number of contents that the proxy agent will buy. Note that $F_i = \{f_{i1}, \cdots, f_{in}\}$.

4.3.2 Contents Encryption keys generation

In our scheme, fingerprinted image is transmitted as encrypted with (anonymous) buyer's public key. Thus each fingerprinted image sold to a buyer must be encrypted with each different key for unlinkability of digital images.

(1) FCC chooses K keys $k_1, \cdots, k_K$ $(k_i \in Z_p^*)$ randomly and computes $(y_1, \cdots, y_K)$, where $y_i := [(y_B^*)^{k_i}, g^{k_i} \pmod p]$. FCC sends to the proxy agent $(y_1, \cdots, y_K)$ and the fingerprints encrypted with these keys $Fing_i = E_{y_i}(F_i)$ along with $Sign_{F_i} = Sign_{x_F}(Fing_i \| y_i)$, which certifies the validity of the fingerprints and also ensures that y_i was used to encrypt F_i. Here $\|$ denotes a concatenation and $E_{y_i}(F_i) = E_{y_i}(f_{i1}), \cdots, E_{y_i}(F_{in})$ as in [4,3]. FCC stores $y_P^*, y_i, Fing_i, Sign_{Fi}, y_B^*, Cert(y_B^*)$ in the buyer's record of his database FCC_DB.

(2) The proxy agent verifies each $Sign_{Fi}$ with the FCC's public key.

4.4 Fingerprints Insertion Step

This is an interactive protocol between a seller

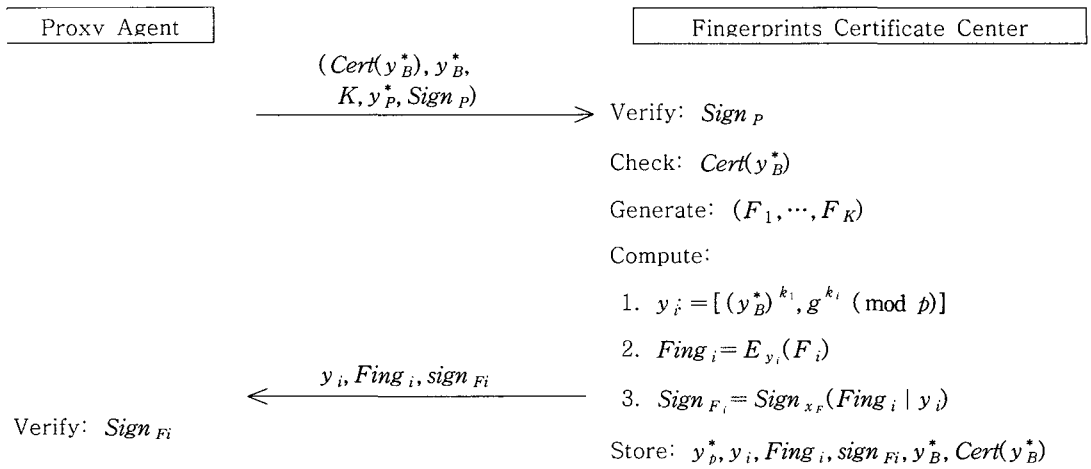


Fig. 3. Fingerprints Generation Step.

(sellers) and the proxy agent who must buy digital image instead of the buyer. This protocol depends on the underlying watermarking algorithm and homomorphic encryption techniques used. It appears in Fig. 4.

(1) A proxy agent sends $y_i, E_{y_i}(F_i), y_P^*, Sign_{Fi}, text_i$ $(1 \le i \le K)$ to a seller.

(2) A Seller verifies each $Sign_{Fi}$ with FCC's public key y_F. If the verification holds, the next step proceeds.

(3) Let $Image_i (Image_1, \cdots, Image_K)$ denote the original image that the buyer (the proxy agent) wants to purchase. The seller generates K unique $W_1, \cdots, W_K$ randomly and embeds a unique fingerprint into digital image $Image_i$. Let Ima_i^* be the fingerprinted image with W_i. When an unauthorized copy Ima_i^* is found, this unique fingerprint W_i is used for identifying the original buyer of Ima_i^*. To embed the second fingerprint F_i generated by the FCC into Ima_i^* without decrypting $E_{y_i}(F_i)$, the seller encrypts the watermarked contents Ima_i^* with y_i and finds the permutation σ_i satisfying $\sigma_i(E_{y_i}(\sigma_i(F))$. Because of the homomorphic property of the encryption algorithm E used by the FCC, the seller can compute fingerprinted contents $E_{y_i}(Ima_i^{**})$ by the following process. If input is T, then the output is $E_{y_i}(T) := (T, (y_B^*)^{k_i}, g^{k_i})$.

$$
\begin{aligned}
E_{y_i}(Ima_i^{**}) &= E_{y_i}(Ima_i^*) \oplus \sigma_i(E_{y_i}(F_i)) \\
&= E_{y_i}(Ima_i^*) \oplus E_{y_i}(\sigma_i(F_i)) \\
&= \{E_{y_i}(ima_{i1}^*), \cdots, E_{y_i}(ima_{im}^*) \oplus E_{y_i}(f_{i\sigma_i(1)}, \cdots, f_{i\sigma_i(n)})\} \\
&= \{E_{y_i}(ima_{i1}^* \oplus f_{i\sigma_i(1)}), \cdots, E_{y_i}(ima_{\in}^* \oplus f_{i\sigma_i(n)}), \cdots, \\
&\quad E_{y_i}(ima_{im}^*)\} \\
&= E_{y_i}(Image_i \oplus W_i \oplus \sigma_i(F_i)), m \ge n
\end{aligned}
$$

(4) The seller transmits $E_{y_i}(Ima_i^{**})$ to the proxy agent and stores $y_P^*, y_i, W_i, E_{y_i}(F_i), \sigma_i$, and $Sign_{F_i}$, $(1 \le i \le K)$ in his database Seller_DB. Seller_DB is a table of records maintained by seller herself for digital image $Image$ containing one entry for each copy of $Image$ that she sells.

(5) The proxy agent sends $E_{y_i}(Ima_i^{**})$ to the buyer.

(6) The buyer decrypts the encrypted image $E_{y_i}(Ima_i^{**})$ and obtains K fingerprinted image Ima_i^{**}. The buyer can decrypt the fingerprinted image encrypted with each different key y_i with one key in our proposal. The decryption process is as follows.

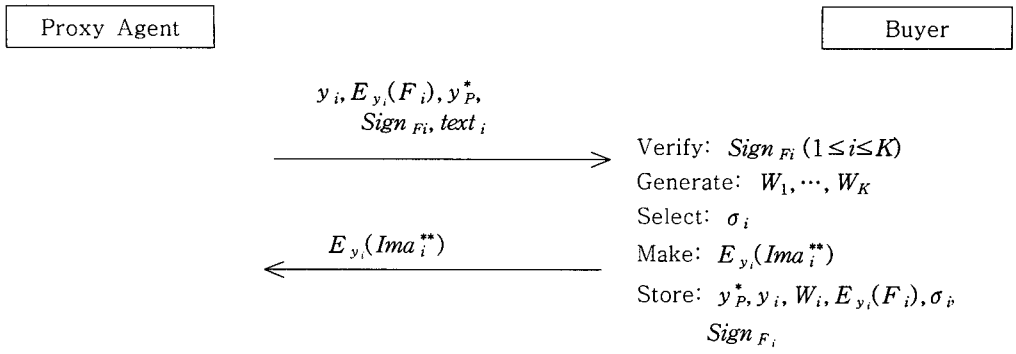


Fig. 4. Fingerprints Insertion Step.

$$E_{y_i}(T) := (T, (y_B^*)^{k_i}, g^{k_i})$$

$$D_{x_{B1}}(E_{y_i}(T)) := \frac{T \cdot (y_B^*)^{k_i}}{(g^{k_i})^{x_{B1}}} = \frac{T \cdot (y_B^*)^{k_i}}{(y_B^*)^{k_i}} = T$$

4.5 Identification Step

When an illegal copy Y of an original image $Image_i$ is discovered,

(1) The seller extracts the unique watermark U in Y using detection algorithm. Then, he finds the buyer's information $y_P^*, y_i, W_i, E_{y_i}(F_i), \sigma_i, Sign_{F_i}$ stored with W_i by examining the correlations of extracted watermark U and all W_i's in Seller_DB. And the seller sends them with $Image_i$, Y to an arbiter.

(2) The arbiter verifies $Sign_{F_i}$ with the FCC's public key y_F. If the verification holds, the arbiter performs the next step.

(3) The arbiter sends y_P^*, y_i to FCC. Then the FCC sends $y_B^*, Cert(y_B^*), y_i, F_i$ back to the arbiter.

(4) The arbiter computes $\sigma_i(F_i)$ and checks the existence of $\sigma_i(F_i)$ in Y by extracting the fingerprint from Y and estimating its correlations with $\sigma_i(F_i)$.

(5) If there exists $\sigma_i(F_i)$, the arbiter sends $y_B^*, Cert(y_B^*)$ to RC and reveals the buyer's real identity with the help of RC. The owner of y_B^* is found guilty. If $\sigma_i(F_i)$ is not found in Y, he is innocent.

5. FEATURES AND SECURITY ANALYSIS

We discuss various features of the proposed scheme according to the list of requirements in the section 2.

▫ **Anonymity**: We assumed that the registration center does not reveal the buyer's real identity if he/she is honest. Even if the seller and the proxy agent know a pseudonym y_B^*, they cannot know y_B, because x_{B2} is encrypted with RC's public key. Thus buyer's anonymity is provided if the seller and the proxy agent cannot compute discrete logarithms.

▫ **Unlinkability**: In our protocol, not y_B^* but K different keys $y_1, \cdots, y_K$ are transmitted to the seller. And each fingerprinted image sold to a buyer must be encrypted with each different key for unlinkability of digital contents. Thus given two digital contents, nobody can decide whether these two images (contents) were purchased by the same buyer or not.

▫ **Traceability**: Due to the properties of the underlying encryption and digital signature techniques, we can assume that a malicious buyer cannot change or substitute a fingerprint generated by the fingerprint certificate center. The security of traceability is the same as that of [3,4] schemes. Sellers should insert two fingerprints W_i and $\sigma_i(F_i)$ in the right manner for his own interest.

If he does not correctly insert W_i or $\sigma_i(F_i)$, he would not be able to identify the original buyer of an illegal copy. A detecting function in the fingerprint detection guarantees that the seller can extract the unique watermark (fingerprint) W_i that belongs to a traitor. Besides, the buyer cannot remove $\sigma_i(W_i)$ from Ima_i^{**}, even though he and the proxy agent know F_i because he does not know σ_i. Thus the buyer who has distributed digital contents illegally (traitor/copyright violator) can be traced in our scheme.

- **No Framing**: Since, to forge Y with the special watermark F_i, the seller must know either the buyer's private key x_{B1} or the buyer's unique watermark F_i. In our proposal, only the buyer knows his private key x_{B1} and his unique water mark if computing discrete logarithm is hard and used encryption algorithm (underlying primitives) is secure. Thus an honest buyer should not be wrongly identified as a copyright violator, because the seller cannot recreate the buyer's copy with specific watermark.

- **No Repudiation**: The others cannot recreate the buyer's copy, because only the buyer can decrypt encrypted fingerprinted contents (only the buyer knows his own secret key x_{B1}). Thus the buyer accused of reselling an unauthorized copy should not be able to claim that the copy was created by the seller or a security breach of the seller's system.

- **Collusion tolerance**: Our scheme used one of two schemes[11,17] as a building block. One[11] is a private key watermarking protocol needed original image in watermark detection step, whereas the other[17] is a public key watermarking protocol not needed it. We assumed that these algorithms are secure. And these algorithms are estimated to be highly resistant at collusion attacks[19]. Our protocol is secure only as much as the underlying watermarking techniques are secure and robust.

- **Efficient materialization**: In previous scheme [4,6,9], the buyer has to carry out the registration step and fingerprinting step. On the contrary, the buyer executes the one-time registration step and delegation step in our scheme. It is clear that computational cost of fingerprinting step[6,9] is higher than that of delegation one. Because fingerprinting step is based on multi-party protocols with very high complexity. Thus, it is enough to prove that our protocol is more efficient than the others previous scheme[6,9] from the view of buyers. Our scheme reduces the amounts of buyers' computations to minimum. We briefly show the comparison between our method and the previous methods about participators of each step in the Table 1.

- **Efficient expansion of multi-purchase protocol**: In our scheme, the buyer executes the one-time registration step regardless of the number of digital contents purchased, because the certificate on y_B^* can be re-used, keeping unlinkability. Besides, buyers can decrypt ciphertext with one decryption key even if each plaintext (fingerprinted image) is encrypted with each different key. We briefly show the comparison between our scheme and the scheme that use the previous

Table 1. Comparison between our method and previous methods

	[PS99][PW97][6,9]	[JK02][4]	Our method
Registration	**Buyer**-RC	**Buyer** -RC	**Buyer** - RC
Delegation	.	.	**Buyer** - Proxy agent
Fingerprints generation	**Buyer**-Seller	**Buyer** - FCC	Proxy agent-FCC
Fingerprints insertion		**Buyer**-Seller	Proxy agent-Seller
Identification	Seller,RC	Seller, RC, FCC	Seller, RC, FCC

Table 2. Comparison between our method and method I

	Method I	Our scheme
The number of Registration Execution	n*[1]	1
The number of Encryption Key	n	n
The number of Decryption Key	n	1

*1: The number of digital contents that buyers buy.

scheme[4] repeatedly (we mark the scheme to method I) in the Table 2.

6. CONCLUDING REMARKS

To our best knowledge, we have presented the first construction scheme of digital fingerprinting for multi-purchase. The proposed scheme is quite efficient for the buyer who wants to purchase multi-contents on executing only one-time registration. Only one decryption key is necessary for a buyer and the number of key is also independent of that of digital contents to be purchased. We also showed the possibility of materialization of multi-purchase digital fingerprinting by introducing proxy-based protocol. Our proposal reduced the amount of buyers' computations to the minimum. Even though Proxy-based methods are very useful tools in the fingerprinting schemes, under the distributed environment like the internet, it is very difficult to assume the trust of the buyer, proxy signer and the proxy key issuing protocol between them. Hence, for the practical and real situations, the fingerprinting schemes with the proxy signature should be designed carefully since the delegation of singing capability to others can be risky. And we must also consider the possibility of dishonesty of the TTP such as fingerprint certification center.

7. REFERENCES

[1] T. Nakanish, N. Haruna, and Y. Sugiyama, "Unlinkable Electronic Coupon Protocol with Anonymity Control", *ISW99, LNCS 1729, Springer-Verlag*, pp.37-46, 1999.

[2] B. Pfitzmann, and M. Waidner, "How to Break and Repair a "Provably secure" Untraceable Payment System", *Crypto'91, LNCS 576, Springer-Verlag*, pp.338-350, 1991.

[3] N.Memon and P.W.Wong, "A Buyer-Seller Watermarking Protocol", *IEEE Transactions on Image Processing*, vol.10, no. 4, pp.643-649, 2001.

[4] H.S. Ju, H.J. Kim, D.H. Lee and J.I. Lim,, "An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control", *ICISC2002, LNCS 2587, Springer-Verlag*, pp.421-432, 2002.

[5] B.Pfitzmann and M.Schunter, "Asymmetric Fingerprinting", *Eurocrypt'96, LNCS 1070, Springer-Verlag*, pp.84-95, 1996.

[6] B. Pfitzmann and M. Waidner, "Anonymous Fingerprinting", *Eurocrypt'97, LNCS 1233, Springer-Verlag*, pp.88-102, 1997.

[7] D. Chaum, I.B. Damgard and J. Graaf, "Multiparty Computation Ensuring Privacy of Each Party's Input and Correctness of the Result", *Crypto'87, LNCS 293, Springer-Verlag*, pp.87-119,1987.

[8] J. Domingo-Ferrer, "Anonymous Fingerprinting Based on Committed Oblivious Transfer", *PKC'99, LNCS 1560, Springer-Verlag*, pp.43-52, 1999.

[9] B.Pfitzman and A.R.Sadeghi, "Coin-Based Anonymous Fingerprinting", *Eurocrypt'99, LNCS 1592, Springer-Verlag*, pp.150-164. 2000.

[10] D.Boneh and J.Shaw, "Collusion-secure Fingerprinting for Digital Data", *Crypto'95, LNCS*

963, Springer-Verlag, pp.452-465, 1995.

[11] I.J. Cox, J.Kilian, T.Leighton, and T.Shamnon, "Secure Spread Spectrum Watermarking for Image, Audio and Video", *IEEE Transactions on Image Processing*, vol.6, no 12, pp.1673-1678, 1997.

[12] R. Crammer, R.Gennaro, and B.Schoenmakers. "A Secure and Optimally Efficient Multi-authority Election Scheme". *Eurocrypt'97, LNCS 1233, Springer-Verlag*, pp.113-118, 1997.

[13] P Paillier. "Public-key Cryptosystems Based on Composite Degree Residuosity Classes". *Eurocrypt'99, LNCS 1592, Springer-Verlag*, pp.223-238, 1999.

[14] D. Naccache and J.Stern. "A New Public Key Cryptosystem Based on Higher Residues". *Proceedings of the 5th ACM Symposium on Computer and Communications Security*, pp.59-66, 1998.

[15] T.Okamoto, M.Tada and E.Okamoto, "Extended Proxy Signatures for Smart Cards", *ISW99, LNCS 1729, Springer-Verlag*, pp.247-258, 1999.

[16] K.Zhang, "Threshold Proxy Signature Schemes", *ISW97, LNCS 1396, Springer-Verlag*, pp.282-290, 1997.

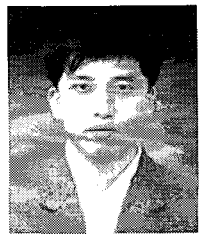
[17] M.Barni, F.Bartolini, V.Cappellini and A. Piva, "Robust Watermarking of Still Images For Copyright Protection", *Proceedings of 13th International Conf. Digital Signal Processing*, Vol 2, pp.499-502, 1997.

[18] D. Chaum, JH Evertse, and J. van de Graaf, "An Improved Protocol for Demonstrating Possession of Discrete Logarithms and Some Generalization", *Eurocrypt'87, LNCS 304, Springer-Verlag*, pp.127-141, 1987.

[19] J.Killian, F.T.Leighton, L.R. Matheson, G. Talal. Shannon, E.Robert. Tarjan, and Z. Francis, "Resistance of Digital Watermarks to Collusive Attacks", *IEEE International Symposium on Information Theory*, pp.271, 1998.

JaeGwi Choi

She received the B.S. degree in computer science from Pukyong National University and the M.E. degree in computer science education from Pukyong National University in 1998 and 2001, respectively. She was an exchange student in Kyushu University, Japan in 2002-2003 and studied at the institute of industry science of Tokyo University, Japan as a visiting researcher with the support of KOSEF in 2004. She is currently working toward her Ph.D. degree in information security at Pukyong National University. Her current research interests are in copyright protection technology and cryptography.



KyungHyune Rhee

He received his M.S. and Ph.D. degrees from Korea Advanced Institute of Science and Technology (KAIST), Daejon Korea in 1985 and 1992, respectively. He worked as a senior researcher in Electronic and Telecommunications Research Institute (ETRI), Daejon Korea from 1985 to 1993. He also worked as a visiting scholar in the University of Adelaide, the University of Tokyo, and the University of California, Irvine. He has served as a Chairman of Division of Information and Communication Technology, Colombo Plan Staff College for Technician Education in Manila, the Philippines. He is currently a professor in the Division of Electronic, Computer and Telecommunication Engineering of Pukyong National University, Busan Korea. His research interests center on key management and its applications, mobile communication security and security evaluation of cryptographic algorithms.