JOURNAL OF KOREA MULTIMEDIA SOCIETY, VOL. 6, NO. 4, JULY 2003

An Anonymous Fingerprinting Scheme with a Robust Asymmetry

Jae-Gwi Choi, Ji-Hwan Park and Kouichi Sakurai

ABSTRACT

Fingerprinting schemes are techniques applied to protect the copyright on digital goods. These enable the merchants to identify the source of illegal redistribution. Let us assume the following situations connectedly happen: As a beginning, buyer who bought digital goods illegally distributed it, next the merchant who found it revealed identity of the buyer/traitor, then the goods is illegally distributed again. After this, we describe it as "*The second illegal redistribution*". In most of anonymous fingerprinting, upon finding a redistributed copy, a merchant extracts the buyer's secret information from the copy and identifies a traitor using it. Thus the merchant can know the traitor's secret information (digital fingerprints) after identification step. The problem of the second illegal distribution is that there is a possibility of the merchant's fraud and the buyer's abuse: that is a dishonest employee of the merchant might just as well have redistributed the copy as by the buyer, or the merchant as such may want to gain money by wrongly claiming that the buyer illegally distributed it once more. The buyer also can illegally redistribute the copy again. Thus if the copy turns up, one cannot really assign responsibility to one of them. In this paper, we suggest solution of this problem using two-level fingerprinting. As a result, our scheme protects the buyer and the merchant under any conditions in sense that (1) the merchant can obtain means to prove to a third party that the buyer redistributed the copy. (2) the buyer cannot worry about being branded with infamy as a traitor again later if he never distribute it.

Key words: Digital Fingerprinting, Multiple Fingerprinting, Second Illegal Redistribution, Robust Asymmetry, Anonymity.

1. INTRODUCTION

Protection of intellectual property in digital goods has been a subject of research for many years and led to the development of various techniques. A digital fingerprinting scheme is an important class of these techniques. This is similar to digital watermarking, except that different information such as the user ID is embedded in each distributed digital goods. It is the cryptographic method applied to deter people from redistributing a data item by enabling a merchant to trace a copy back to its original buyer.

*Jae-Gwi Choi and Ji-Hwan Park are with the Dept. of Information Security, Graduate School, Pukyong National Univ. Korea. E-mail: jae@mail.pknu.ac.kr and jpark@pknu.ac.kr

*Kouichi Sakural is with the Faculty of Information Science and Electrical Engineering, Kyushu Univ. Japan. E-mail : sakurai@csce.kyushu-u.ac.jp

1.1 Known Classes of Fingerprinting Sch

Classical fingerprinting schemes[11] are symmetrical in the sense that both the merchant and the buyer know the fingerprinted copy. Thus, if another copy with this fingerprint is found, one cannot really assign responsibility to one of them: because the merchant does not find anything in the redistributed copy that he could not have made up himself. In other words, the merchant does not obtain means to prove to a third party that the buyer redistributed the copy.

The problem is overcome by asymmetric scheme [2]. Here, only the buyer knows the fingerprinted copy: where the buyer also inputs secret information and the merchant does not see the fingerprinted copy that the buyer obtains. Only if

he finds this copy after, he can extract the proof. Hence the merchant can identify the buyer and prove to third parties that the buyer is a traitor (the buyer who was distributed the digital contents that she/he bought). However the drawback of this solution is that the merchant knows the buyer's identity even if the buyer is honest. To protect buyer's privacy, later anonymous fingerprinting schemes[1,3-5,9,10] were introduced: The idea is that the merchant can know neither the fingerprinted copy nor the buyer's identity. Nevertheless it enables the merchant to identify traitors later. The possibility of identification will only exist for traitors, whereas honest buyers will remain anonymous.

1.2 Related Works

A key issue in this paper is the distinction between *symmetric* fingerprinting and *Anonymous asymmetric* fingerprinting.

Description 1: *A symmetric fingerprinting* scheme consists of two algorithms, fingerprinting and identification. Since a merchant executes both algorithms, both the merchant and the buyer know the fingerprinted copy.

Description 2: *An asymmetric fingerprinting* scheme consists of four protocol, key generation, fingerprinting, identification and disputation. In here, fingerprinting protocol is a 2-party protocol between a merchant and a buyer. The buyer also inputs secret information and the merchant does not see the fingerprinted copy that the buyer obtains. Only if the merchant finds this copy after redistribution, he can extract the proof.

Description 3: *An anonymous fingerprinting* scheme mostly consists of five algorithms: key distribution, registration, fingerprinting, identification and trial. All anonymous fingerprinting schemes are asymmetric. The merchant and the buyer carry out it anonymously, nevertheless this scheme enables the merchant to identify traitors later.

It is easy for one to conclude that anonymous fingerprinting[1-5,9,10] is more secure and efficient than symmetric and asymmetric ones.

In previous scheme[3], they asserted that an anonymous fingerprinting scheme provided the security of the buyer and the merchant. The securities are:

(1) For the security of a buyer
  ① It does not leak information about *emb* (*emb* is the entire value to be embedded).
  ② If a buyer is honest, he will remain anonymous and should not find guilty by an arbiter.

(2) For the security of a merchant
  ① A merchant can also convince any third party that a particular person was a traitor.
  ② A merchant can identify the traitor if there are at most *coll_size* traitors (Let *coll_size* denotes the maximal size of a collusion of buyers against which the scheme is secure). In other words, extracting *emb* will recover the embedded value.

1.3 Motivation

Unfortunately, an anonymous asymmetric fingerprinting isn't a truly asymmetric technique.

Now, we start a study on the assumption that the second illegal redistribution occurred. Here we show a reason why most of fingerprinting schemes are symmetric under the second illegal redistribution*. When the first illegal redistribution occurred, a merchant who found a redistributed copy extracts the *emb* from the copy in order to identify a traitor. If cryptographic techniques are used to make it collusion tolerant, he can identify the dishonest buyer. Moreover he can know the

*As a beginning, buyer who bought digital goods illegally distributed it (we describe it as "***The first illegal redistribution***"), next the merchant who found it revealed identity of the buyer/traitor, then the goods is illegally distributed again. After this, we describe it as "***The second illegal redistribution***".

buyer's secret information *emb* too even if the buyer is a dishonest buyer. Here, we have to remind ourselves of the proposal background of asymmetric fingerprinting. i.e., after the first illegal redistribution*, it is possible that the merchant can embed the buyer's secret information to original contents and redistributes it for his gain. Thus, finally most of anonymous fingerprinting schemes become symmetric under the second illegal redistribution. That is, most of anonymous asymmetric fingerprinting schemes[1-5,9,10] cannot offer the securities as mentioned above.

Proposition 1: An anonymous asymmetric fingerprinting scheme doesn't offer security of the buyer and the merchant anymore under the second illegal redistribution.

Proof 1 (sketch): At least two kinds of fraud are possible:

(1) The merchant may obtain all the *emb* needed to impersonate the buyer. Since the merchant can know *emb* after execution of the identification step (of the first illegal redistribution), he can embed original contents into it and indicate the buyer as a traitor for his commercially gains.

(2) The buyer may claim that it was the result of fraud. i.e., he may stand that the merchant redistributed in spite of fact that he redistributed it illegally. Since the buyer knows that the merchant knew *emb*, he shall deny his/ her own guilty.

Thus the merchant doesn't obtain means to prove to a third party that the buyer redistributed the copy in anonymous asymmetric fingerprinting, too. Fig. 1. shows the possibility of a merchant's fraud in the second illegal redistribution.

1.4 Our contributions

What we need is anonymous fingerprinting with a robust asymmetry: even if the merchant executes identification step of the first illegal redistribution,

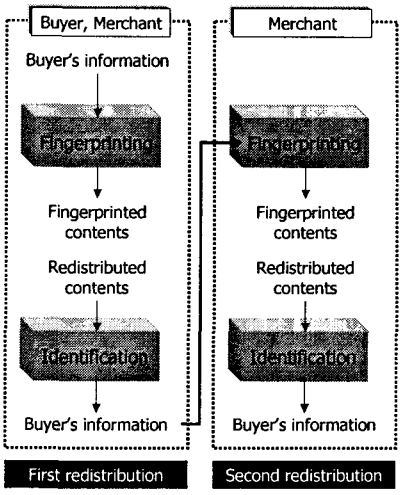


Fig. 1. Problem of Pervious Anonymous Fingerprinting under the second illegal redistribution

he cannot know all *emb* to be embedded. Only the buyer knows the contents with all fingerprints.

Definition 1: If it holds the following requirements, we call it "*Anonymous fingerprinting with a robust asymmetry*".

- *General requirements*:

(1) For the security of the buyer: buyers can buy digital contents anonymously and execute fingerprinting protocol with safety.

- *Special requirements*:

(1) For the security of the buyer: the buyer should be found guilty even if he was a traitor before.

(2) For the security of the merchant: the merchant can obtain means to prove to a third party that the buyer redistributed the copy, even if the buyer was a traitor before.

In this paper, we propose anonymous fingerprinting with a robust asymmetry satisfied above requirements.

The outline of this paper is as follows: Section 2 gives a short introduction of the model of our proposal. Then, in Section 3 presents 'Anonymous fingerprinting with a robust asymmetry' of our

goal. Section 4, we analysis its security and compare the proposed method with the previous scheme.

2. THE MODEL OF OUR SCHEME

In this section we briefly introduce the methodology and components of our scheme.

2.1 Methodology

To achieve our goal, we seek to find a solution from two angles. The first angle is that the merchant never can embed buyer's information by getting rid of the original contents after execution of fingerprinting protocol. Not to mention, it should premise the scheme that can extract embedding information without the original contents. Several studies have been made on it by terminology named "*public watermarking*"[8].

However if we apply it to our proposal, some doubt remains: the merchant can keep the original contents at discretion. There is no means of preventing that. So it cannot be a proper means to make our goal because there is still room for argument about responsibility of redistribution.

The second angle is that the merchant cannot know all information to be embedded. We will now find the means in the number of fingerprints to be embedded.

In previous anonymous fingerprinting, the *emb* are embedded and are extracted together as one group. Upon finding redistributed copy, the merchant have to extract all of the *emb* within the limits of the possible in order to exactly trace a traitor. Thus after identification step, all *emb* are revealed and at the same time the merchant also can know the buyer's secret information (digital fingerprints). After all, it also could be symmetric fingerprinting.

To overcome this problem, we increase the number of embedding information. In this paper, we increase in embedding information by two. One is information for tracing a traitor (emb_1), the other is information for the reliable evidence (evidence that a merchant can prove the traitor's guilty to the third party) (emb_2). Then these are embedded into content. For this, we introduce multiple *fingerprinting*[7,13]. A multiple *fingerprinting* is multi-level method that can embed numbers of different information to content. The Fig. 2 is a diagram of the simple multiple fingerprinting (2-level fingerprinting). After, upon finding a redistributed copy, the merchant should extract emb_1 to trace a traitor and the buyer should use emb_2 in order to prove his innocence. Two parties cannot extract all of this information alone. Of course the merchant can identify the dishonest buyer, but cannot do dishonest things such as framing the honest buyer as a traitor under not only the first illegal redistribution but also the second illegal redistribution.

In multiple fingerprinting, it must have orthogonality among keys to be used in embedding step for the right extraction of the embedding information[13]. In our scheme, we might desire to:

(1) Embedding key $Ortho(random\_key_1)$ is encrypted with the merchant's public key in order to identify a traitor
(2) Embedding key $Ortho(random\_key_2)$ is encrypted with the buyer and the merchant common public key in order to provide reliable evidence.

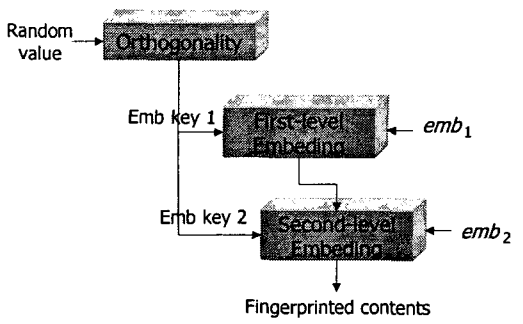


Fig. 2. Embedding procedure of multiple fingerprinting.

After each $Ortho(random\_key_i : i = \{1,2\})$ is used to embed and extract emb_i.

2.2. Components

In our scheme, the involved parties are a merchant M, a buyer B, registration center RC. The model requires buyers to register at the RC before they purchase fingerprinted contents. We assume that B can generate signatures under her "real" identity and that the corresponding public keys have already been distributed. Here RC only plays a role in offering buyer's anonymity. Our scheme consists of the following four procedures.

(1) ***Key Generation*** is a probabilistic key setup algorithm for the registration center. Its output is the center's secret key (x_R) and its public key (y_R), which is published authentically.

(2) ***Registration*** is a two-party protocol between a B and a RC. The common inputs are the B's a real identity (y_B), the RC's public key. The RC's secret input is its secret key. The output is B's anonymous identity ($y_B^* = y_1$) and RC's records about the B.

(3) ***Fingerprinting*** is a two-party protocol between a M and an anonymous B. The M secretly inputs the digital content (that the buyer wants to buy) ($item_0$) and his secret key (x_M), the B secretly input her registration records and signature on purchase, and both input a common *text* that describes what this purchase is about. In here we use two-level fingerprinting schemes[7,12-13]. First embedding information is $emb_1 = (text, sig_1, y_B^*, Cert_B)$. Second embedding information is $emb_2 = (text, sig_2, y_B^*, y_M, y_{BM})$. The output for the B is the multiple fingerprinted contents and the output for the M is a purchase record. The Fig. 3 shows the two-level fingerprinting of our proposal.

(4) ***Identification*** is two-level protocols. First level is an algorithm for the M and second level is a protocol between the M *and* B. The main input is a redistributed content ($item_{red}$) that is found by merchant. The output should be the guilty of the buyer or innocence of the buyer or failure (if more than *coll_size* buyers colluded to produce $item_{red}$, the output is failure).

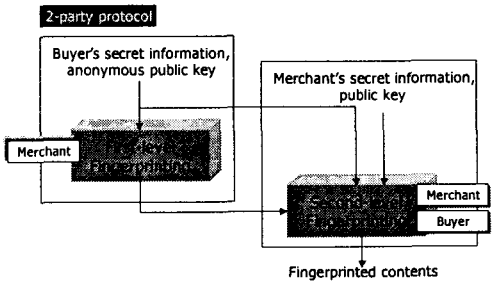


Fig. 3. Two-level fingerprinting process.

3. CONSTRUCTION

3.1 Preliminaries

Marking Assumption: Let *item* $\{0,1\}^*$ denote some digital content (bit-string) that is fingerprintable, i.e., some of its bits can be changed such that (1) the result remains "close" to *item* but (2) without knowing which particular bits where changed, altering "a good portion" of these bits is impossible without rendering the good useless. We refer to [5] for a formal definition of this "marking assumption", Finally, let $item^*$ demote the set of all "close copies" of *item* and l be a security parameter.

We also assume that only buyers and the merchants can distribute/redistribute digital contents (fingerprinted contents).

The trusted authority decides the following system parameters and publishes them:

p : A large prime.

q : A large prime satisfying $q|p-1$.

g : An element in Z_p^* whose order is q.

All users must decide the following parameters:

Registration center. RC

x_R : A secret key in Z_q^*.

y_R : A public key $y_R = g^{x_R}$.

Merchant. M

x_M : A secret key in Z_q^*.

y_M : A public key satisfying $y_M = g^{x_M}$.

Buyer. B

x_B : A Secret key in Z_q^*.

y_B : A public key satisfying $y_B = g^{x_B}$.

E : Encryption algorithm

D : Decryption algorithm

$Ortho$: Orthogonal algorithm

3.2 Protocol 1: Registration

(1) B chooses the random numbers x_{B_1}, $x_{B_2} \in Z_p$ such that $x_{B_1} x_{B_2} = x_B$. And she computes $y_1 = g^{x_{B_1}}$, $E_{y_R}(x_{B_2})$, by using y_R. B sends $[y_1, E_{y_R}(x_{B_2})]$ to RC. After B convinces RC in zero-knowledge of possession of x_{B_1} and x_{B_2}.

(2) RC decrypt x_{B_2} and by using it, she checks that $y_1^{x_{B_2}} = y_B$. If it holds, the registration center sends $[Cert(y_1)]$ to B.

(3) B checks equation (1). If it holds, B obtains a certification.

$$y_1 = g^{x_1}, \quad y_B = y_1^{x_2} \bmod p \qquad (1)$$

3.3 Protocol 2: Fingerprinting

This is a two-party protocol between the merchant and the buyer. In here, we use secure multi-party protocol (SMPC)[6] and multiple fingerprinting[13]. SMPC protocol offers a function that they don't know each other's inputs, however they convinced that the inputs are right. Also this offers another function that secretly sends each output to them.

1 STEP : Authentication

(1) B sends $[y_1, Cert(y_1), text]$ to the merchant M, where $text$ is a string identifying the purchase $item$. B signs $text$ by computing $sig_1 := (x_{B_1}, text)$. The signature sig_1 is not sent to M.

(2) M verifies the certificate on y_1 using the registration centers' public key.

2 STEP : First-level Fingerprinting

If authentication-step holds, B and M enter a secure two-party computation [7]. Input of M are $[y_1, Cert(y_1), item, x_M, y_{BM}, text]$, where $item$ is the original digital content to be fingerprinted, B's inputs are $[sig_1, y_1, x_{B_1}, y_{BM}]$. Where $y_{BM} = y_1^{x_M} = y_M^{x_{B_1}}$. The computations performed are:

(1) $ver_1 = equal(y_{BM}, y_{BM})$. It checks whether the first y_{BM} (buyer's input) is equal to the second y_{BM} (merchant's input). The output ver_1 is a Boolean variable seen by M, and B which is true if and only if the thing checks succeed.

(2) $ver_2 = verify(y_1, sig_1)$. sig_1 is verified by using y_1 verified in advance. The output ver_2 is a Boolean variable only seen by M, which is true if and only if the thing checks succeed

(3) If above two steps were successful, it executes the embedding procedure. A multiple fingerprinting algorithm is used to embed emb_1 into the original content $item$. $item_1^*$:

$= Fing(item, emb_1)$. is obtained as output of the first-level fingerprinting step.

$$emb_1 := (text, sig_1, y_1, Cert(y_1))$$

3 STEP : Second-level Fingerprinting

If above first-level fingerprinting step is executed succeeds, computations of second-level fingerprinting step are performed are:

(1) It produces their common signature $sig_2 := (text, x_{B_1}, x_M)$.

(2) It executes the embedding procedure:. $item_2^* = Fing(item_1^*, emb_2)$. A multiple fingerprinting algorithm is used to embed emb_2 into the $item_1^*$. The second fingerprinted

content $item^*_2$ are obtained as output of the second-level fingerprinting-step

$$emb_2 := text \| sig_2 \| y_1 \| y_{BM} \| y_M$$

The last fingerprinted information $item^*$ is obtained as output of two-level fingerprinting protocol and is only seen by B.

$$item^* = item^*_2 = Fing(item, emb_1, emb_2)$$

In the above two-party computation, M obtains his outputs (ver_1, ver_2) first. Unless (ver_1, ver_2) are all true, B does not get her output $item^*$.

In this protocol, embedding keys of each fingerprinting-step are as follows:

(1) $Ortho(random\_key_1)$ is used in the first level fingerprinting. Then the key is encrypted using the merchant's public key $[E_{y_M}(Ortho(random\_key_1))]$.

(2) $Ortho(random\_key_2)$ is used in the second level fingerprinting. Then the key is encrypted using merchant and buyer's common public key $[E_{y_{BM}}(Ortho(random\_key_2))]$.

After each $Ortho(random\_key_i)$ is used to embed and extract emb_i.

3.4 Protocol 3 : Identification

In the identification protocol, keys to be used are the same as follows.

$$ext_{key_1} = D_{x_M}(E_{y_M}(Ortho(random_{key_1})))$$
$$ext_{key_2} = D_{x_M x_{B_1}}(E_{y_{BM}}(Ortho(random_{key_2})))$$

1 STEP : First-level identification

The first-level identification step is not a protocol but an algorithm. When redistribution of $item_{red}$ is detected, identification is based on the information (emb_1) extracted from the $item_{red}$. Under the marking assumption [5], a collusion tolerant fingerprinting algorithm is need. Upon finding a redistributed copy, M extracts emb_1 by using own secret key. The extracted information contains the values specified by emb_1 to construct a redistribution proof. The merchant sends $proof := (text, sig_1, y_1)$, which proves that the owner of this pseudonym (y_1) has redistributed the content corresponding to *text*, to the registration center and asks for the real identity (y_B) of the traitor. If the registration center refuses, the merchant shows *proof* to an arbiter, together with $Cert(y_1)$ to prove that the registration center can know the corresponding identity. The dishonest buyer (traitor) B has been identified.

2 STEP : Second-level identification

When the accused buyer doubts merchant's decision, he extracts emb_2 to a redistributed contents with the help of the merchant. For convenience sake, we describe emb_2 as the information extracting from the redistributed content ($item_{red}$).

The merchant and the accused buyer extract emb_2 to the redistributed copy. If the buyer illegally distributed copy, the extracted information contains the followings.

$$emb_2' := text \| sig_2 \| y_1 \| y_{BM} \| y_M$$

(1) The signature sig_2 on the *text* is verified by using y_{BM}.

(2) If the result *text* and the *text* of the first-level identification are the same, it proves the accused buyer to be a traitor. Otherwise, if other person (merchant or another person) redistributes the content, a correct value cannot be extracted. Since they can't extract and embed emb_2 without help of the buyer.

4. ANALYSES AND COMPARISON

4.1 Analyses of Security

In this section, we prove security of our scheme by showing that it satisfies the definition 4.

4.1.1 Registration security

Proposition 2 : Protocol 1 provides buyer authentication without compromising the private x_B key of the buyer.

Proof 2 (sketch) : In registration protocol, the registration center knows y_1, x_{B_2} and a zero-knowledge proof. The latter leaks no information. The registration center needs no knowledge of x_{B1} to find values y_1, which is related in the same way as y_1. Now we consider the zero-knowledge proofs. An attacker who does not know x_B can compute y_1, y_2 such that he can demonstrate possession of $\log_g^{x_{B_1}}$, $\log_g^{x_{B_2}}$ and $y_1^{x_{B_2}} = y_B$ holds. Then the attacker can compute the discrete logarithm x_B. Even if the attackers are a collusion of merchant and registration center and the buyer securely can execute our construction. Since registration center and merchant cannot know secret key x_{B1}, they can neither produce valid signature of the buyer nor get certifications of anonymous *ID* from another registration center to disguise as the buyer.

4.1.2 Buyer anonymity

Proposition 3 : An honest buyer who follows Protocol 2 will not be identified if computing discrete logarithms is hard and secure two-part computation is feasible.

Proof 3 (sketch) : In the fingerprinting protocol, the merchant knows a pseudonym y_1. Since x_{B_2} is encrypted as registration center's secret key, it is unknown to the merchant. Thus if merchant can not compute discrete logarithms, buyer's anonymity is provided.

4.1.3 Reliable evidence about redistribution

Proposition 4 : Protocol 2,3 provides that (1) the merchant obtains means to prove to a third party that the buyer redistributed the copy, (2) the buyer is not branded with infamy as a traitor on the content that she does not redistributed.

Proof 4 (sketch) : (1) Since the merchant can extract only the value emb_1, he can't know the other embedding information emb_2 by himself. Thus even if the merchant embeds emb_1 to original content for his gains, he can't cheat the buyer. i.e., he can't make correct fingerprinted contents. Thus the proof obtained from the redistributed content can be reliable evidence that the buyer redistributed the copy ($item_{red}$). Besides the buyer cannot extract the value emb_2 alone even if she colludes the registration center. Since this is needed the merchant's secret information. (2) A certain individuals can't embed and extract both of information emb_1, emb_2. In two-level multiple fingerprinting scheme, though there is a correlation between key and key, it is very difficult that it derives another key from a certain key[15]. i.e., as the merchant knows neither a random number nor orthogonal number of the buyer, he can't derive emb_1, emb_2 from his own key. Thus the buyer cannot worry about being branded with infamy as a traitor again later even if she was a traitor before. Besides the merchant cannot extract the value emb_2 alone even if he colludes the registration center. Since this is needed the buyers secret information x_{B_1}. In other words, protocol 2,3 plays an important role in achieving "Anonymous fingerprinting with a robust asymmetry".

4.2 Comparison with Previous works

We compare our proposal with previous works. Table 1 shows the comparison between our method and the asymmetric and anonymous fingerprinting.

In here, property of asymmetric is means that the merchant can means to prove to a third party that the buyer illegally distributed the copy. In anonymous fingerprinting scheme, since the merchant who found a redistributed copy, can extract the buyer's secret information from it, he can embed the buyer's secret information into original contents for his commercial gain. Thus in the second illegal redistribution, he cannot prove the buyer's guilty even if the buyer illegally distributed it. On the other hand, a merchant can obtain the means that the buyer is a traitor under the second illegal redistribution in our proposal [refer 4.1]. Thus our scheme is *an asymmetric anonymous fingerprinting scheme under any conditions*.

Table 1. Comparison our proposal with previous works fingerprinting[1,3-5,9,10].

	Function	Asy*1	Anony*2	Our scheme
1st redistribution*3	Asymmetric	O	O	O
	Anonymity	×	O	O
2nd redistribution*4	Asymmetric	×	×	O

(*1 Asymmetric fingerprinting scheme)
(*2 Anonymous fingerprinting scheme)
(*3 The first illegal redistribution)
(*4 The second illegal redistribution)

5. CONCLUSION

In this paper, we pointed out a serious problem of the previous schemes: that is the responsibility problem of redistribution after tracing a traitor. In order to solve this problem, we introduced the notion of anonymous fingerprinting with a robust asymmetry and suggest it by using two-level multiple fingerprinting. Our scheme gives (1) reliable evidence about responsibility of redistribution: the merchant can obtain means to prove to a third party that the buyer redistributed the copy after execution identification step, (2) anonymity of buyer: the buyer can buy contents anonymously. We expect the proposed scheme to be much utility value of digital contents copyright protection in real-life.

But our scheme cannot prevent redistribution by a third person who received copies (fingerprinted copy that is embedded specific buyer's information) from the buyer. A further direction of this study will be to solve this drawback.

6. ACKNOWLEDGEMENTS

The first and second authors was partly supported by grant No.01-2002-000-00589-0 from the Basic Research Program of the Korea Science & Engineering Foundation. It was done while the first author visits in Kyushu University, Japan with the support of Association of International Education, Japan.

7. REFERENCES

[1] B.Pfitzmann and Ahmad-Reza Sadeghi, "Anonymous Fingerprinting with Direct Non-Repudiation", Asiacrypt 2000, *LNCS 1976, Springer-Verlag,* 2000. pp.150-164.

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

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

[4] Chanjoo.Jung, et al., "Efficient anonymous fingerprinting of electronic information with improved automatic identification of redistributors", ICICS 2000, LNCS 2015, *Springer-Verlag,* 2001. pp. 221-234.

[5] D.Boneh and J.Shaw, "Collusion-secure Fingerprinting for Digital Data", Crypto'95, *LNCS.963, Springer-Verlag,*1995. pp.452-465.

[6] D.Chaum et al., "Multiparty Computation Ensuring Privacy of Each Party's Input and Correctness of the Result", Crypto'87, *LNCS 293, Springer-Verlag,* 1987. pp. 86-119.

[7] F. Mintser and G.W. Braudaway, "If one Watermark is Good, Are more Better?", IEEE Int'l Conf. On Acoustics, *Speech and Signal Processing,* 1999.

[8] Gang Qu, "Keyless Public Watermarking for Intellectual Property Authentication", Information Hiding 2001, *LNCS 2137, Springer- Verlag,* 2001. pp. 96-111.

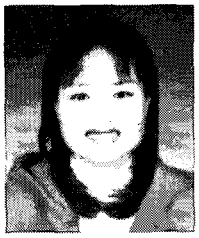
[9] Jan Camenisch, "Efficient Anonymous Fingerprinting with Group Signatures", Asiacrypt 2000, *LNCS 1976, Springer-Verlag,* 2000. pp. 415-428.

[10] J.Domingo-Ferrer, "Anonymous Fingerprinting of Electronic Information with Automatic Identification of Redistributors", *Electronics Letters* 34/13. 1998. pp.1303-1304.

[11] Neal R.Wagner, "Fingerprinting", *IEEE Symposium on Security and Privacy,* 1983.

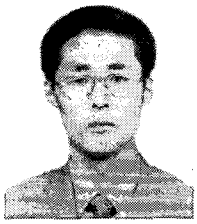
[12] Thomas S.Shore. "Applied Linear Algebra and Matrix Analysis", *McGraw-Hill Primis Publishing*, 1999.

[13] Y.H.Oh, H.H.Kang, J.H.Park, "Multiple Watermarking Using Gram-Schmidt Orthogonal Processing", *Journal of Korea Information Processing Society*, Vol.8-C. No.6, 2001. pp. 703-710.



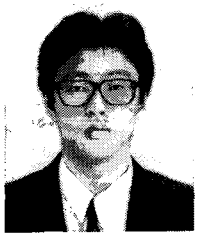
Jae-Gwi Choi

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 is currently working toward her Ph. D. degree in information security at Pukyong National University, and studying in Kyushu University, Japan as a exchange student (Oct,2002-Aug,2003). Her research interests include information security and cryptography.



Ji-Hwan Park

He received the B.S degree in electronic engineering from Kyunghee University, Seoul, Korea in 1984 and the M. E. degree and D. E degree from the University of Electro-Communications and Yokoha ma National University, Tokyo and Yokohama, Japan in 1987 and 1990, respectively. He is currently a full professor of the Division of Electronic Computer and Telecom. Eng. PuKyong National University, Busan, Korea. From 1990 to 1996 he was an assistant professor of the department of computer science, National Fisheries University of Pusan, Korea. He was a guest researcher at the institute of industry science, university of Tokyo in 1994-1995. His primary research interests include information theory and its applications, cryptography and its applications, image processing. He is a member of IEEE, Society of Information Theory and its Applications, Korean Institute of Communication Sciences, Korean Institute of Information Security and Cryptology, Korea Information Processing Society and Korean Multimedia Society.



Kouichi Sakurai

He received the B.S. degree in mathematics from Faculty of Science, Kyushu University and the M.S. degree in applied science from Faculty of Engineering, Kyushu University in 1986 and 1988, respectively. He had been engaged in the research and development on cryptography and information security at Computer & Information Systems Laboratory at Mitsubishi Electric Corporation from 1988 to 1994. He received the Dr. degree in engineering from Faculty of Engineering, Kyushu University in 1993. Since 1994 he has been working for Department of Computer Science of Kyushu University as an associate professor, and now he is a full professor. His current research interests are in cryptography and information security. Dr. Sakurai is a member of the Information Processing Society of Japan, the Mathematical Society of Japan, ACM and the International Association for Cryptologic Research.

For information of this article, please send e-mail to: jpark@pknu.ac.kr(Ji-Hwan Park)