A CONTENT-PROTECTION SCHEME FOR MULTI-LAYERED RESELLING STRUCTURES

Pei-Ling Yu, Pan-Lung Tsai, and Chin-Laung Lei
Department of Electrical Engineering, National Taiwan University

Abstract: Since the idea of digital watermarks was proposed, various watermarking schemes have been developed to protect digital contents in electronic transactions. However, most schemes limit themselves to the simplified buyer-seller model that can be applied to only a small number of cases rather than common scenarios in real life. In this paper, a more practical watermarking scheme is proposed to protect digital contents in real-world transactions using PKI (Public-Key Infrastructure). The proposed scheme is considered more practical in the sense that one or more reselling agents may exist between buyers and the original seller, and the seller can package the merchandise in advance without the involvement of buyers. The packaged merchandize can hence be made publicly accessible (e.g., on top of an open shelf) for the purpose of demonstration and circulates in the market. The proposed scheme also preserves the anonymity of the buyers while guaranteeing that the distributor of any illegal copy will be unambiguously identified.

Keywords: Digital watermark, Public-Key Infrastructure, content protection, anonymity, privacy protection

1. INTRODUCTION

In modern times, a wide variety of materials have been digitized to facilitate the processing of information. Unfortunately, the convenience of data manipulation encourages many kinds of software piracy in that the efforts of retrieving and duplicating contents have been greatly reduced as well. To alleviate the problem of piracy, various content-protection schemes have been proposed to restrict the access and use of digital contents to legitimate users only. Content-protection schemes in electronic commerce

Y. Deswarte et al. (eds.), *Security and Protection in Information Processing Systems*

generally consist of two important parts, one for ensuring that only those users who have paid are granted access to digital contents, and the other for tracking down the unauthorized content distributors who should be responsible for the pirated copies found in the market.

In the content-protection schemes [1, 2, 3, 4, 5] that make use of the digital watermarking technology [6, 7, 8, 9, 10], a watermark uniquely associated with each transaction is inserted into the copy of the digital content to be sold. In order to achieve the goals of secure and fairness, the seller and the buyer are required to perform the watermark insertion collaboratively using cryptographic techniques when carrying out the transaction. Such schemes guarantee that neither the seller nor the buyer alone is able to remove the watermark embedded in the copy of the digital content. When a pirated copy of the digital contents is found sometime later, the watermark can then be extracted and/or detected to identity a particular transaction and the corresponding buyer, who should now be responsible for the piracy.

Such watermark-enabled content-protection schemes have several major drawbacks. Firstly, these schemes are primarily designed to deal with purely electronic transactions where the entire digital content is going to be transferred across the Internet. This can be prohibitive or unreliable for large-volume digital contents such as digital videos. Secondly, the preparation of the merchandize requires the involvement of buyers so that buyer-specific information can be used to generate effective watermarks. This prevents the original seller of the digital content to pre-package the merchandize without knowing the actually buyers. Thirdly, most schemes focus on the direct-sale business model and consider only the interactions between the seller and the buyer in the transaction. In real-life scenarios, it is common to have intermediary reselling agents, and these schemes simply fail on such multi-layered reselling structures. To sum up, these schemes are not practical and can barely used in real-world transactions.

Taking ISO (International Organization for Standardization) Store [11], the on-line shopping services for ISO publications, as an example will make previous discussions more clear. In order to protect its copyright, ISO Store requires a buyer to register at first, and then dynamically inserts the buyer's name and affiliation into the documents sold in the transaction. Such approach is hardly applicable to merchandize that is high-volume or accompanied by non-digital materials, and can only be realized in purely electronic transactions. It works exclusively for direct-sale model and does not allow the merchandize to be pre-packaged. As a result, the circulation of the merchandize through reselling agents is prohibited.

Another important goal of a practical content-protection scheme is to preserve the privacy of buyers. Although the substantial objective of content-

protection schemes is to track down the unauthorized distributors, we cannot simply presume the guilt of buyers by treating them as potential distributors of pirated copies of digital contents and hence deprive buyers of their privacy. Besides, the rights to shopping anonymously are essential to current practice of commercial transactions.

In this paper, a practical content-protection scheme is proposed to achieve the goal of protecting digital contents in real-world transactions. The proposed scheme integrates the digital watermarking technology with Public-Key Infrastructure (PKI) [12] and allows the existence of intermediary reselling agents, in addition to the basic direct-sale business model. It also permits the original seller to pre-package the merchandize without the involvement of buyers (i.e., without knowing who the buyers are during merchandize preparation). The privacy of buyers and the rights of reselling agents are also considered. The rest of the paper is organized as follows. Section 2 describes the proposed scheme in detail, and section 3 presents the security analysis along with further discussions. Section 4 finally concludes the paper.

2. THE PROPOSED SCHEME

In this section, a content-protection scheme using digital watermarks and PKI is presented with each phase in an individual subsection. The goals to be achieved are:

a) Full access to a single copy of the digital content to be sold is granted only after the buyer successfully registers himself to the original seller for that copy. On the other hand, reselling agents may decide to present samples with lower quality (e.g., thumbnails, movie trailers, etc.) or in non-digital forms (e.g., posters) to attract potential buyers, as in real-world commercial transactions.
b) When a pirated copy is found in the market, the original seller can always track down the real identity of the responsible distributor, who must be a buyer in certain transaction happened previously.
c) The privacy of buyers is well protected. As long as a buyer does not commit piracy, he is guaranteed to remain anonymous during transactions and arbitrations.

The proposed scheme is based on the following assumptions:

1. At least one robust watermarking insertion, extraction, and/or detection algorithm exists for the digital content to be sold. Watermarking schemes

for certain types of digital contents have been well studied, as mentioned in section 4, while others may still need more research efforts. Nevertheless, as more and more researchers devote themselves to this area, this assumption will definitely hold for more and more types of digital contents.

2. A PKI implementation has been deployed to provide adequate authentication and non-repudiation services.
3. The original seller does not intentionally frame a buyer by distributing illegal copies herself and then accusing the buyer of piracy. In subsection 3.3, a possible extension to the proposed scheme dealing with malicious sellers will be described and hence further relax this assumption.

Several roles are used when explaining the details of the proposed scheme. They are listed and briefly described as follows.

S: The seller, who is the rightful owner of the original digital content and wants to make a profit on the sales of it.

B: The buyer, who wants to purchase a copy of the digital content from **S** via intermediary reselling agents.

CA: A trusted certification authority, who is responsible for issuing anonymous certificates.

ARB: A decent arbiter, who will make righteous judgments on disputes according to the evidences presented.

Some notations used throughout the rest of the paper are defined as:

$U \oplus V$: The watermarked/fingerprinted copy of digital content U. The binary operator $\oplus$ denotes the operation of watermark insertion, and V is the chosen watermark to be inserted.

$Priv_{\mathbf{I}}$: The private key of identity **I**.

$Pub_{\mathbf{I}}$: The public key of identity **I**.

$Cert_{\mathbf{I}}$: The digital certificate issued to subject **I** by **CA**. By using X.509-compliant digital certificates, $Priv_{\mathbf{I}}$ and $Pub_{\mathbf{I}}$ can be derived from $Cert_{\mathbf{I}}$.

$Sign_{Priv\mathbf{I}}(M)$: The signature of message M signed by **I** with $Priv_{\mathbf{I}}$.

$E_{Pub\mathbf{I}}(M)$: The ciphertext of message M encrypted with $Pub_{\mathbf{I}}$. The encryption can be performed by anyone.

$D_{Priv\mathbf{I}}(C)$: The original message (plaintext) of ciphertext C decrypted by **I** using $Priv_{\mathbf{I}}$.

$Enc_J(M)$: The ciphertext of message M encrypted with symmetric key J. The encryption can be performed by anyone that knows J.

$Dec_J(C)$: The original message of ciphertext C decrypted with symmetric key J. The decryption can be performed by anyone that knows J.

2.1 Initialization

In order to remain anonymous during transactions and (possibly) unsolicited arbitrations, **B** first applies to **CA** for an anonymous certificate. An anonymous certificate is a special type of digital certificates with the corresponding subject field being a pseudonym rather than the real identity of the applicant. Let **P** denote the pseudonym used by **B**. The information of binding the issued anonymous certificate, $Cert_{\mathbf{P}}$, to **B** will then be kept safely by **CA**. Upon receiving the anonymous certification, **B** saves it in his personal computer, and stores another copy in a specialized smart card so that the anonymous certificate can be easily used whenever needed.

B may use a single anonymous certificate in multiple transactions, or he may request a distinct anonymous certificate for each individual transaction. Using the same anonymous certificate in many transactions to the same seller may allow the seller to gain extra knowledge about the purchasing behavior of **B**. However, it is undoubtedly more convenient and more efficient for **B** to reuse his anonymous certificates. The issue of reusing anonymous certificates will be revisited in subsection 3.2.

2.2 Merchandize Preparation

For each copy of digital content X, **S** randomly generates a watermark W and a one-time key K for symmetric encryption. **S** then performs watermark insertion to get the watermarked/fingerprinted copy Y:

$$Y = X \oplus W \tag{1}$$

Then **S** encrypts Y with K to get the ready-to-ship form Z:

$$Z = Enc_K(Y) \tag{2}$$

S also derives a product key, PK, from K:

$$PK = Hash(K) \tag{3}$$

Note that *Hash* is a public one-way hash function. It has the following property that everyone who knows K can easily calculate PK, while it is considered impossible to do the reverse (i.e., figuring out K from PK).

Finally, **S** computes the digital signature SIG:

$$SIG = Sign_{Priv_S}(PK, Z) \tag{4}$$

After the computation, the merchandize is packaged as (PK, Z, SIG). **S** then stores the tuple (PK, K, W) in her sales records and distributes (PK, Z, SIG), along with any accompanied materials (e.g., posters, free gifts, etc.), to one of the reselling agents.

Note that **S** does not need to know the actual buyers in the phase of merchandize preparation, and the merchandize is allowed to freely circulate in the market once it is packaged. This is exactly how most real-world commercial transactions proceed, in contrast to the common approach used in purely electronic transactions, which usually asks a buyer to authenticate himself beforehand so that buyer-specific information can be blended into the merchandize during preparation.

2.3 Merchandize Sale

The reselling agent who obtains sets of packaged merchandize from **S** may decide to resell them to next-level reselling agents, or directly to the real customers. If a reselling agent does not trust whom he gets the merchandize from, he may verifies the digital signature, SIG, included in the merchandize to ensure that the content has not been altered after the initial packaging. Subsequently, the agent may make the merchandize publicly accessible for the purpose of demonstration, as how he does to other non-digital merchandize. Once a buyer purchases a set of packaged merchandize, he then follows the registration and activation processes stated in the next two subsections, respectively.

2.4 Merchandize Registration

When **B** decides to buy a set of packaged merchandize, he performs the registration of the merchandize to **S** as part of the transaction. First **B** opens the package and extracts the product key, PK, of the merchandize. Then he inserts the smart card holding his anonymous certificate, $Cert_P$, into the card reader provided by the reselling agent, and types PK in the input device associated with the card reader. Upon receiving $Cert_P$ and PK, the program

stored in the smart card is instructed to run in "registration mode" and begins to compute:

$$PKS = Sign_{Priv\mathbf{P}}(PK) \tag{5}$$

Recall that $Priv_{\mathbf{P}}$ is the private key of pseudonym **P** and can be obtained directly from $Cert_{\mathbf{P}}$. Then the program sends ($Cert_{\mathbf{P}}$, *PK*, *PKS*) to **S**. When **S** gets ($Cert_{\mathbf{P}}$, *PK*, *PKS*), she verifies the signature, *PKS*, and rejects the request if it is invalid. If the request contains a valid signature, **S** then searches her sales records for an entry associated with *PK*. If no such entry is found, **S** rejects the request. Otherwise, **S** further checks the status of the merchandize associated with *PK*, and also rejects the request if the merchandize turns out to have been registered. If everything goes fine, **S** extracts the corresponding *K* from the entry and computes:

$$AK = E_{Pub\mathbf{I}}(K) \tag{6}$$

Then **S** adds ($Cert_{\mathbf{p}}$, *PK*, *PKS*) to the entry so that the merchandize is marked as registered, and sends the encrypted activation key, *AK*, back to the program. When the program running on the smart card successfully receives *AK* from **S**, it stores *AK* in the smart card and completes the transaction. If the request is rejected by **S** in the middle way, the program notifies **B** and aborts the transaction.

2.5 Merchandize Activation

After a successful transaction, **B** takes his merchandize and smart card home. Before **B** can make use of the digital content he just bought, he has to carry out one last action, activating the digital content. **B** starts by inserting the digital media (contained in the packaged merchandize) and his smart card into the corresponding readers. Then the program stored in the smart card is instructed to run in "activation mode" and invokes an auxiliary program running on **B**'s personal computer associated with the readers. The first thing the auxiliary program does is to verify that *SIG* is a valid signature of (*PK*, *Z*), followed by computing:

$$K = D_{Priv\mathbf{I}}(AK) \tag{7}$$

The auxiliary program proceeds to check the validity of *K* by evaluating equation (3) stated above. Finally **B** gets the watermarked/fingerprinted copy of the digital content by calculating:

$$Y = Dec_K(Z) \quad (8)$$

Note that an auxiliary program is needed here for the sake of computation efficiency. Although it is possible to perform the cryptographic operations mentioned in this subsection totally on the smart card, the restricted computation power of the smart card will result in intolerably long processing time when dealing with high-volume digital contents.

If anything goes wrong during activation, **B** may simply return the broken merchandize and ask for refunding. The proposed scheme ensures that **B** will be able to present concrete evidences to show that the merchandize is broken and he does not have to be responsible for it.

2.6 Arbitration

Disputes may arise when a pirated copy is found in the market. The arbitration proceeds as follows. By running an appropriate watermark extraction and/or detection algorithm on the pirated copy, **S** can easily find out the distributor, who must be a buyer in some previous transaction, from her sales records. **S** then presents corresponding ($Cert_P$, *PK*, *PKS*, *W*) to **ARB**. Upon receiving the request from **S**, **ARB** checks whether *PKS* is a valid signature of *PK* signed by **P** and *W* actually exists in the pirated copy. If both conditions are true, **ARB** sends $Cert_P$ to **CA** and asks **CA** to reveal the real identity of pseudonym **P**. Once knowing who the buyer is, **ARB** makes the final judgment.

3. DISCUSSIONS

In this section, we first present the security analysis of the proposed scheme, followed by pointing out the issue that arises from reusing anonymous certificates. In the last subsection, we describe a possible extension to the proposed scheme so that buyers can be further protected from malicious sellers, and hence the assumption that there is no ill-intentioned seller can be relaxed.

3.1 Security Analysis

The security of the proposed scheme primarily comes from the underlying watermarking scheme and PKI. As long as the watermarking scheme adopted is robust, the watermark embedded in a watermarked/ fingerprinted copy can always be extracted and/or detected. In addition, the

authentication and non-repudiation services provided by PKI guarantee that nobody can lay his sins on others.

Based on the properties stated above, the proposed scheme is able to successfully protect the copyright of digital contents. Once a pirated copy is found in the market, **S** can unambiguously identify the anonymous certificate, $Cert_{\mathbf{P}}$, based on the watermark embedded in that copy. Besides, the evidences supplied by **S** during the arbitration are able to prove that **P** was indeed involved in certain previous transaction because nobody except **P** would be able to generate signature *PKS*.

The rights of **B** are also protected. On one hand, his real identity remains unexposed unless he is proven to have committed piracy. On the other hand, it is not possible for some malicious agents to sell an already-registered copy to **B** because **B** will be aware of the failure on his registration during the transaction. Furthermore, there is no chance for any reselling agent to peek into or alter the content of the merchandize since the merchandize is packaged in its encrypted form, *Z*, and has a digital signature, *SIG*, on it.

The digital signature, *SIG*, also contributes to the preservation of reselling agents' rights. It helps a reselling agent to ensure that the packaged merchandize has not been altered by his predecessors. Moreover, an honest reselling agent does not have to worry about having purchased already-registered copies because once a copy is found to have been registered, it is guarantee that the guilty one will always be unambiguously identified.

3.2 Reusing Anonymous Certificates

The anonymity of the proposed scheme basically relies on the introduction of a trusted third party, **CA**. Under such circumstances, if **B** uses a different anonymous certificate for each individual transaction, his real identity will never get exposed as long as **CA** is not compromised. However, this is both inconvenient and inefficient because **B** will then have to manage a large number of his certificates and **CA** will need tremendous storage for even more certificates of all buyers. An intuitive solution will be allowing **B** to reuse his anonymous certificate.

However, reusing a single anonymous certificate in many transactions to the same seller will make these transactions linkable and allow that particular seller to infer personal information about **B** via data-mining techniques. It is a potential threat because the seller may become able to take advantage of **B** without knowing **B**'s real identity. A simple way for **B** to alleviate the risk is to apply for several anonymous certificates and randomly choose one before a transaction takes place because doing so will increase the efforts for seller to infer useful information. As a matter of fact, the policy for reusing anonymous certificates depends on how **B** concerns his

privacy. There is a tradeoff between the complication of certificate management and the degree of privacy preserved.

3.3 Protecting Buyers from Malicious Sellers

In the proposed scheme, **S** is assumed to have no bad intentions. This is necessary because **S** has direct access to every watermarked/fingerprinted copy that is going to be sold, and hence she can easily frame **B** by waiting for **B**'s registration and then distributes the registered copy herself. Following the arbitration process, **S** can successfully charge **B** with piracy, which in fact he never did, and make him be mistakenly judged as the guilty one, who should be responsible for the illegal distribution.

This issue is known as *customer's right problem* [4]. Some schemes [2, 5] have been developed to deal with this particular issue as follows. In order to prevent **S** from framing **B**, a watermark certification authority (**WCA**) is introduced to perform watermark generation in the encrypted domain. By encrypting the generated watermark with **B**'s public key, WCA inhibits **S** from knowing the actual watermark. **S** is still responsible for inserting the watermark to the digital content, but the insertion operation is performed in the encrypted domain and hence **S** has no access to the (decrypted) watermarked/fingerprinted copy that **B** will finally get.

Here we describe general guidelines about how the proposed scheme can be extended to overcome *customer's right problem* by following the spirits of the schemes mentioned above. We also introduce the existence of **WCA** for watermark generation, but, since we don't want the involvement of buyers in the phase of merchandize preparation, the schemes mentioned above cannot be applied directly. Instead, **WCA** generates an extra key pair for each request from **S**, and uses the public key of the key pair to encrypt the watermark. During the transaction, **B** is required to make an additional contact to **WCA** to get the corresponding private key so that he has enough information to activate the watermarked/fingerprinted copy later. As a result, this extended scheme successfully achieves the goal of protecting buyers from malicious sellers.

4. CONCLUSIONS

In this paper, a practical watermarking scheme is proposed to protect digital contents in real-world transactions using PKI (Public-Key Infrastructure). The proposed scheme enables the original seller to pre-package the merchandize without the involvement of buyers, and permits the circulation of packaged merchandize in the market by allowing one or more

reselling agents to exist between the original seller and buyers. The digital watermarking technology is seamlessly integrated with PKI to make the proposed scheme easily applicable to real-world transactions.

In the proposed scheme, the copyright of the digital content belonging to the original seller is well protected, as the distributor of any pirated copy is guaranteed to be unambiguously identified. On the other hand, the privacy of buyers is preserved since a buyer can always stay anonymous unless he is proven to have committed piracy. The rights of reselling agents are not forgotten. Mechanisms are provided to detect broken merchandize during resale, and the seller's traceable records of registration also entitle reselling agents the immunity of accusations.

REFERENCES

1. J. Doming-Ferrer and J. Herrera-Joancomarti, "Efficient Smart-Card Based Anonymous Fingerprinting," Proceedings of International Conference on Smart Card Research and Applications (CARDIS '98), LNCS 1820, pp. 221-228, September 1998.
2. N. Memon and P. W. Wong, "A Buyer-Seller Watermarking Protocol," IEEE Transactions on Image Processing, Vol. 10, No. 4, pp. 643-649. April 2001.
3. B. Pfitzmann and A.-R. Sadeghi, "Coin-Based Anonymous Fingerprinting," Proceedings of 17th Annual IACR Eurocrypt Conference (EUROCRYPT '99), LNCS 1592, pp. 150-164, May 1999.
4. L.Qiao and K. Nahrstedt, "Watermarking Schemes and Protocols for Protecting Rightful Ownership and Customer's Rights," Journal of Visual Communication and Image Representation, Vol. 9, No. 3, pp. 194-210, September 1998.
5. C.-L. Lei and M.-H. Chan, "An Efficient Anonymous Buyer-Seller Watermarking Protocol," 2002 International Computer Symposium, Workshop on Cryptology and Information Security, December 2002.
6. G. Depovere, T. Kalker, and J.-P. Linnartz, "Improved Watermark Detection Reliability Using Filtering Before Correlation," Proceedings of IEEE International Conference on Image Processing (ICIP '98), Vol. 1, pp. 430-434, October 1998.
7. I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Mulimedia," IEEE Transactions on Image Processing, Vol. 6, No. 12, pp. 1673-1687, December 1997.
8. J. R. Hernandez, F. Perez-Gonzalez, J. M. Rodriguez, and G. Nieto, "Performance Analysis of a 2-D-Multipulse Amplitude Modulation Scheme for Data Hiding and Watermarking of Still Images," IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, pp. 510-524, May 1998.
9. A. Herrigel, J. O. Ruanaidh, H. Petersen, S. Pereira, and T. Pun, "Secure Copyright Protection Techniques for Digital Images," Proceedings of Second International Workshop on Information Hiding (IH '98), LNCS 1525, pp. 169-190, April 1998.
10. N. Memon and P. W. Wong, "Protecting Digital Media Content," Communications of the ACM, Vol. 41, No. 7, pp. 35-43, July 1998.
11. ISO Store, http://www.iso.org/iso/en/prods-services/ISOstore/store.html.
12. IETF Public-Key Infrastructure (X.509) Working Group. http://www.ietf.org/html.charters/pkix-charter.html