Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 3 / ISSUE 3 / DECEMBER 2008 / 103-118

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

The Use of Digital Watermarking for Intelligence Multimedia Document Distribution

Shing-Chi Cheung[1], Dickson K. W. Chiu[2] and Cedric Ho[3]

Department of Computer Science and Engineering, Hong Kong University of Science and Technology,
[1] scc@cs.ust.hk, [3] cedric.ho@gmail.com
[2] Dickson Computer Systems, Kowloon, Hong Kong dicksonchiu@ieee.org

Received 10 April 2008; received in revised form 6 September 2008; accepted 6 October 2008

Abstract

Digital watermarking is a promising technology to embed information as unperceivable signals in digital contents. Various watermarking techniques have been proposed to protect copyrights of multimedia digital contents over Internet trading so that ownership of the contents can be determined in subsequent copyrights disputes. However, their applications in preventing unauthorized distribution of intelligence document have not been studied. In this paper, we propose a watermark-based document distribution protocol, which complements conventional cryptography-based access control schemes, to address the problem of tracing unauthorized distribution of sensitive intelligence documents. The reinforcement of document distribution policies requires a concrete support of non-repudiation in the distribution process. The distribution protocol is adapted from our previous work on the watermarking infrastructure for enterprise document management. It makes use of intelligence user certificates to embed the identity of the users into the intelligence documents to whom are distributed. In particular, keeping the identity secrecy between document providers and users (but yet traceable upon disputes) is a key contribution of this protocol in order to support for intelligence applications. We also outline an implementation of the distribution protocol and watermarking scheme employed.

Key words: Intelligence content management, Multimedia content security, Digital watermarking, Document distribution protocol, Intelligence user certificate

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 3 / ISSUE 3 / DECEMBER 2008 / 103-118

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

1 Introduction

The enforcement of distribution policies for sensitive intelligence documents is important but difficult. Sensitive documents may be found left behind in conference rooms, common areas, printing rooms, or public folders. Access control based on cryptography alone cannot address this problem. Once after obtaining access to a sensitive document may a person make unnecessary copies or handle it without care. A major challenge in the reinforcement of distribution policies for sensitive documents is the support of *non-repudiation* in the underlying process so that unauthorized copies of intelligence documents can be identified and traced back to their users. The reinforcement should also be applicable to both hard copies and soft copies of the documents. Conventional cryptographic schemes that cover only soft copies are inadequate to handle this requirement.

Digital watermarking is a promising technology employed by various digital rights management (DRM) systems to achieve rights management. It supports copyright information (such as the owner's identity, transaction dates, and serial numbers) to be embedded as unperceivable signals into digital contents [1]. The signals embedded can be perceivable or unperceivable to humans. In this paper, we focus on the application of invisible watermarking techniques for documents that are based on the imperfection of the human vision system. While visible watermarks should be perceptible enough to discourage theft but not perceptible enough to decrease the utility or appreciation of the document, invisible watermarks should be imperceptible. Furthermore, robust watermarking techniques [12], [14], [15] have been designed to resist tampering and support later extraction and detection of these watermark signals. These signals recover the rights information originally embedded in the document.

In this paper, we apply digital watermarking techniques for the distribution intelligence multimedia documents such as images and audios. In particular, we present a novel distribution protocol for such documents. The protocol is adapted from two pieces of previous work (Cheung & Chiu [3]; Memon & Wong [17]), which describes an enterprise document management system and a watermarking protocol for purchasing digital contents over the Internet, respectively. It introduces the concepts of *intelligence user certificate*s and trusted authorities responsible to issue these certificates. Document users may use the *intelligence user certificate*s obtained from a trusted authority to identify themselves in acquisitions of intelligence documents. The same *intelligence user certificate* may be used in multiple acquisitions. These watermarks, once inserted, are difficult to be removed from their watermarked documents without knowing the exact *insertion* parameters [7]. Watermarks can be preserved across media. For instance, a watermark embedded in a text document in its digital form can be detected in the hard copies of the digital document. If multiple watermarks are applied to individual digital copies, watermarking may also be used to indicate the identity of the legitimate document user of each copy. This allows unauthorized copies to be traced back to the document user from which they originated and thereby deterring unauthorized distribution of sensitive documents. However, this alone cannot fulfill the non-repudiation requirement in document distribution because these unauthorized copies may also originate from the document providers. As such, the document distribution protocol should be able to distinguish the copies made by the document users from those made by *intelligence* document provider*s*. In other words, the distribution protocol should be able to prevent document providers from making copies on behalf of document users. Further, the use of intelligence user certificates together with intermediaries in our protocol enforces the identity secrecy between document suppliers and users (but yet traceable upon disputes). This is a key contribution in order to support for intelligence applications.

This paper is organized as follows. Section 2 gives an overview of the watermarking and document distribution infrastructure. Section 3 gives an account of our protocol, which is followed by an implementation framework in Section 4. Section 5 discusses the advantages of our scheme and Section 6 concludes our work.

2 Background and Related Work

In this section, we present the basic principles of watermarking schemes and the advantages of our watermarking protocols, by comparing related work.

2.1 Principle of Watermarking Schemes

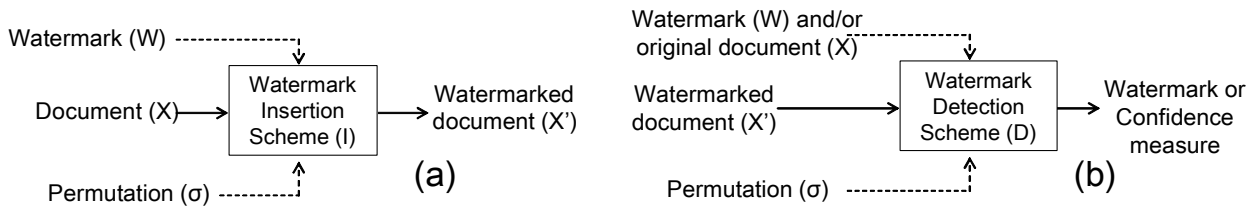

Figure 1: The Processes for (a) Watermark Insertion and (b) Watermark Detection

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 3 / ISSUE 3 / DECEMBER 2008 / 103-118

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

Watermarking schemes refer to the use of signal processing techniques to process watermarking signals in a piece of digital document. Existing watermarking schemes generally involve two stages: watermark insertion and watermark detection as shown in Figure 1. Suppose we have a digital document X, a watermark W, and a permutation function σ. A watermark insertion scheme I inserts a watermark W to the document X, where:

$$X' = I(X, W, \sigma)$$

For illustration, let us explain the principle of the insertion scheme based on a popular secure spread-spectrum watermarking technique proposed by Cox *et al.* [7]. The spread-spectrum technique assumes (i) the document is a vector of "features", i.e., $X = \{x_1, x_2, \ldots, x_n\}$ and (ii) the watermark signal is a vector of "watermark elements", i.e., $W = \{w_1, w_2, \ldots, w_m\}$ with $n \geq m$. Note that the number of features in a document must be much greater than the number of components in a watermark signal so that the signal is unperceivable in the watermarked document X'. The permutation function σ is a bijection that shuffles the watermark elements before inserting them to the document X. As such, the shuffled watermark is a vector of $\sigma(W) = \{w_1', w_2', \ldots, w_m'\}$, where $w_i' = \sigma(w_j)$ with $i, j \leq m$. The permutation function is used for protecting the secrecy of the watermark to be inserted to the document X. The shuffled watermark elements are then inserted to the document X by means of a linear insertion operation $\oplus$, such that X' in the insertion scheme I is given by:

$$X \oplus \sigma(W) = \{x_1 \oplus w_1', x_2 \oplus w_2', \ldots, x_n \oplus w_m'\}$$

Corresponding to the watermark insertion scheme I, there is a watermark detection scheme D, which returns a confidence measure of the existence of a watermark W exists in a piece of document X'. A watermarking technique is referred to as *non-blind watermarking* when its detection scheme D requires the knowledge of the original document X, i.e.,

$$\begin{cases} D(X, X', W, \sigma) = true & \text{if } W \text{ exists in } X' \\ D(X, X', W, \sigma) = false & \text{if } W \text{ does not exist in } X' \end{cases}$$

If D does not require the original document X, the scheme is called *oblivious watermarking* [13]. There are two main scenarios where watermarking techniques are used for rightful ownerships. In the first scenario, the provider inserts a unique watermark into the document. If a copy is later found, the provider can prove its ownership by detecting its unique watermark from the document. In the second scenario, since the provider can insert different watermarks to the origin document for identifying each of its users, each copy can be distinguished and therefore traced.

2.2 Intelligence Document Distribution Infrastructure

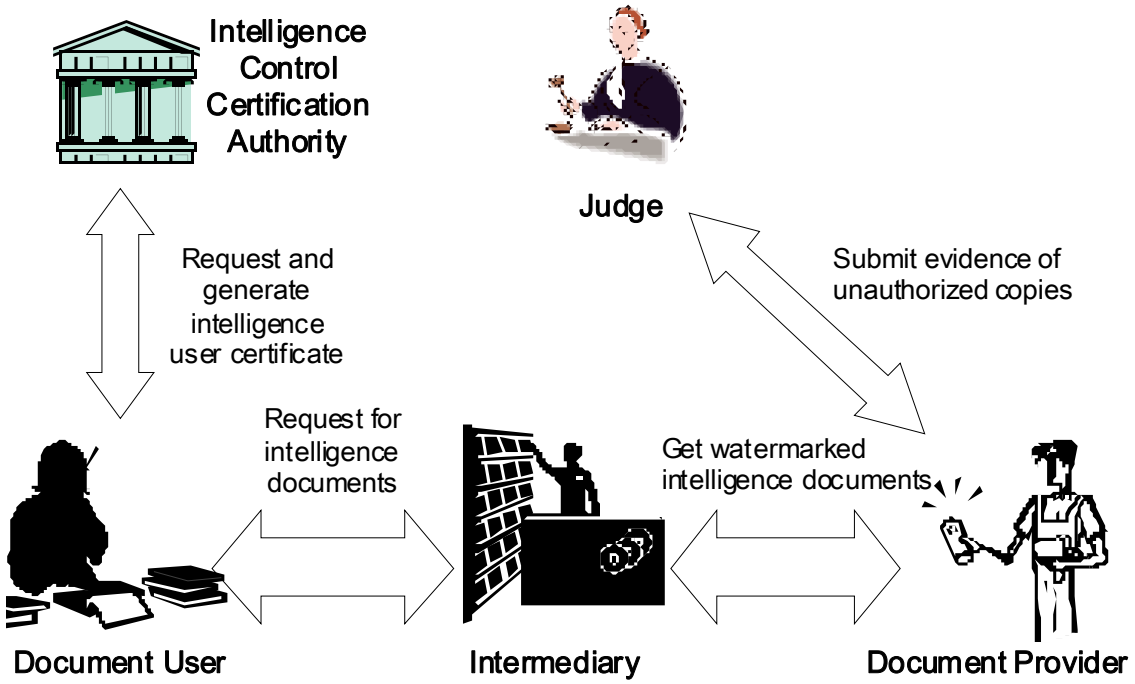

Figure 2: Overview of an intelligence document distribution infrastructure for intelligence document protection

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 3 / ISSUE 3 / DECEMBER 2008 / 103-118

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

We identify five distinguished roles in an intelligence document distribution infrastructure, namely, *Document user*, *Document provider*, *Intelligence control certification authority, Judge*, and *Intermediary*, as shown in Figure 2. Document users are the ones who want to acquire some intelligence documents. Each copy of the intelligence document can be individually watermarked to identify its authorized user. Document providers are producers of these intelligence documents. Document providers employ their own, possibly proprietary, watermarking techniques to encode watermarks into intelligence documents before distributing them to document users. *Intelligence control certification authorities* are trusted parties that generate *intelligence user certificate* identifying document users. *Judges* are trusted parties to resolve allegations filed by document providers against document users. Based on the evidence submitted by the document provider, a judge will decide whether the allegation is justified.

Intermediaries are third party agents between document users and providers; they know both the document providers and the users. Intermediates are only necessary in the cases where users and providers must remain anonymous to each other. Otherwise, if the user and provider know each other, the intermediaries can be bypassed. Intermediaries do not produce intelligence documents themselves and they do not need to be trusted.

In this paper, we are primarily interested in those intelligence documents with content values that can be preserved only by duplicating the source documents. Examples of these documents are often multimedia in nature such as films, maps, photographs, and so on. This is because documents with contents that can be wholly presented by texts (such as financial market news) can also be reproduced by retyping the original document or applying optical character recognition (OCR) without losing the content values.

Although various application of watermarking schemes for the trading of digital contents have been studied in the literature (such as [4], [10], [12], [14], [15], [17]), a comprehensive treatment of these five roles altogether in the proposed intelligence document distribution infrastructure has not been studied, in particular, regarding the issuance of *intelligence user certificate*s and their utilization in the control of intelligence documents.

2.3 Watermarking Protocols

In general, watermarking protocols govern the process of exchanging watermarks and watermarked digital contents between a user and a provider (traditionally a buyer and a merchant in contents trading over the Internet). Such watermarking protocols have been mainly deployed for complementing digital rights management. For example, Schneider & Cheng [21] illustrate how content-based digital signatures can be applied for image authentication, which relates to the tracking of the document provider. Wolf et al. [24] present a framework based on various digital watermarking technologies for marking, searching, and retrieving multimedia files over the Internet for the protection of digital rights. Hartung & Ramme [11] discuss how such DRM approaches can be applied to mobile commerce applications. Nair et al. [18] discuss some issues of DRM related to digital content redistribution and propose a scheme to address them after our initial attempt [4].

With the advancement of watermarking research and increasing adoptions, various problems of attacks to watermarking protocols are being discovered. A watermarking protocol generally comprises three major processes: watermark generation, watermark insertion & distribution, and dispute resolution. The watermark generation process concerns the creation of a legitimate watermark that can identify a buyer. The watermark insertion process concerns the insertion of watermarks to digital contents by a merchant and the distribution of watermarked contents reliably to buyers (some work separates watermark insertion and content distribution into two processes). The dispute resolution concerns the resolution of copyrights upon the detection of suspected copies. In connection to these three major processes, latest researches on watermarking protocol generally address the six issues as tabulated in Table 1. Regarding the issues (b) to (f), different work makes different assumptions on the degree of trusts.

Table 1: Research Issues of Watermarking Protocols

Process	Issues
Watermark Generation	(a) Protection of watermark secrecy
Watermark Insertion & Distribution	(b) Buyers cannot be trusted (c) Merchants cannot be trusted
Dispute Resolution	(d) Buyers cannot be trusted (e) Merchants cannot be trusted (f) Judges cannot be trusted

The technical research issues in the protection of watermark secrecy in the process of watermark generation are similar to those occur in the public key infrastructure. As such, most existing works on watermarking protocols do not explicitly address that issue. Memon & Wong [17] and Cheung & Curreem [4] address the issue by requiring the buyers to present a valid public key on requesting a trusted *certification authority* for a legitimate watermark. Issue (b) is addressed by most existing watermarking protocols in the way that buyers are not trusted to provide a legitimate watermark. To resolve this issue, most protocols require intermediaries to be responsible for the watermark generation, while our protocol does not require this.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 3 / ISSUE 3 / DECEMBER 2008 / 103-118

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

Several studies attempt the problem that content merchants may not be trusted in the process of watermark insertion, i.e., the issue (c) in Table 1. Qiao and Nahrstedt [19] suggest two ways to tackle the problem. One is to introduce a *trusted third party* (TTP). The merchant first sends the original content to the TTP, the content is encrypted with a symmetric key system. Then the watermark is generated at the TTP and inserted to the original content. Finally, the watermarked content is delivered to the buyer through a secured channel between the TTP and the buyer. Another alternative is to use cryptographic protocols between merchants and buyers. The merchant uses the buyer's unique identification certificate (a random bit sequence) to generate the watermark. This identification certificate is generated by the buyer using the standard DES (Data Encryption Standard) algorithm [22] and contains an encrypted copy of the *seed information* privately agreed between the buyer and the merchant. The encryption key of the identification certificate is known only to the buyer. This protocol prevents merchants to generate identification certificates without buyers' involvement. However, it still relies on the honesty of the merchants not to abuse the identification certificates and not to disseminate them to other parties. Jun et al. [12] propose another watermarking protocol for digital contents copyright protection. Like the approach by Qiao and Nahrstedt [19], it assumes a trusted third party called *monitoring service merchant* (MSP) to maintain all the inserted watermarks.

Regarding the dispute resolution phase, most watermarking protocols require contents and sensitive information to be revealed to a third party, commonly referred to as a judge, for verification. If the judge cannot be trusted, problems will arise as a watermark can be removed easily when it is known. To address the issue (f) in Table 1, Gopalakrishnan *et al.* [10] suggested a protocol that need not reveal watermarks to a judge in the dispute resolution phase. But there is a disadvantage with this scheme. The verification procedure is expensive and complicated. Amongst all the watermarking protocols, the Buyer-Seller Watermarking Protocol (Memon & Wong [17]) offers the highest protection to buyers in the sense that it restricts a piece of watermarked content to be used only by its buyers. It addresses the issue (c) in Table 1 where unethical merchants can frame buyers. For instance, a merchant might reproduce a copy of watermarked content that was acquired by a buyer, distribute it illegally, and subsequently sue the buyer for compensation.

Although existing watermarking protocols for multimedia content trading may be deployed in the distribution of intelligence documents by mapping content buyers to document users and content merchants to document providers, such deployments either ignore the interests of document users (in particular, the secrecy of watermarks in the process of watermark insertion and distribution) or do not address the distinguished roles of intermediaries and document providers. Protocols in the former category are unappealing to document users since these document users may not trust intermediaries or document providers not to abuse their watermarks. Protocols in the latter category are unlikely to be adopted by document providers, which may not have full trusts in the intermediaries. This is because the issue that intermediaries may exploit document providers has not been addressed. For instance, the protocol proposed by Memon and Wong [17] has not addressed the scenario where a buyer may contact a merchant through an intermediary. Thus, a user could obtain an unauthorized copy of digital contents if an unethical intermediary agrees to cheat the provider with an encrypted watermark of another user. This problem can be prevented with the use of intelligence user certificates introduced in this paper.

3 A Distribution Protocol for Intelligence Documents

Our distribution protocol consists of three processes: (i) generation of watermarks and intelligence user certificates, (ii) acquisition of watermarked intelligence documents, and (iii) resolution of policy violation. The processes and the data relations involved will be diagrammatically specified in the Unified Modeling Language (UML) [16], which is a well defined modeling language widely used for specifying, constructing, and documenting software systems. To support flexible enterprise document management policies, our distribution protocol is designed to address the following two issues.

- **Maintenance of watermark secrecy**: The secrecy of document users' watermarks must be maintained because these watermarks identify document users. This issue is particularly important in the processes of document distribution where a party can be at the same time a document provider and a document user. Watermarks must not be released to document providers. In our protocol, a document user does *not* need to release his/her watermark to any parties after acquisition of the legitimate watermark.

- **Prevention of Trojan horse attacks**: A document user cannot use the intelligence user certificate of another user to obtain a watermarked document.

The document distribution protocol comprises three major processes: intelligence user certificate generation, intelligence document acquisition, policy violation resolution. The intelligence user certificate generation process concerns the creation of a registration certification, which embeds an encrypted version of a legitimate watermark that identifies a document user. The watermarked document creation process governs the creation of watermarked documents and their reliable distributions to document users. The policy violation resolution process focuses on the collection of evidence and justification of a policy violation allegation against a document user.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 3 / ISSUE 3 / DECEMBER 2008 / 103-118

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

3.1 Generation of an Intelligence User Certificate

Figure 3 and Figure 4 present the process of acquiring an intelligence user certificate and the associated data relations, respectively. Before applying for an intelligence user certificate, a document user should have obtained a valid Public Key Infrastructure (PKI) Certificate, which contains a public key to be used in the purchase of digital contents. A legitimate certificate must be issued by a trusted PKI Certification Authority.

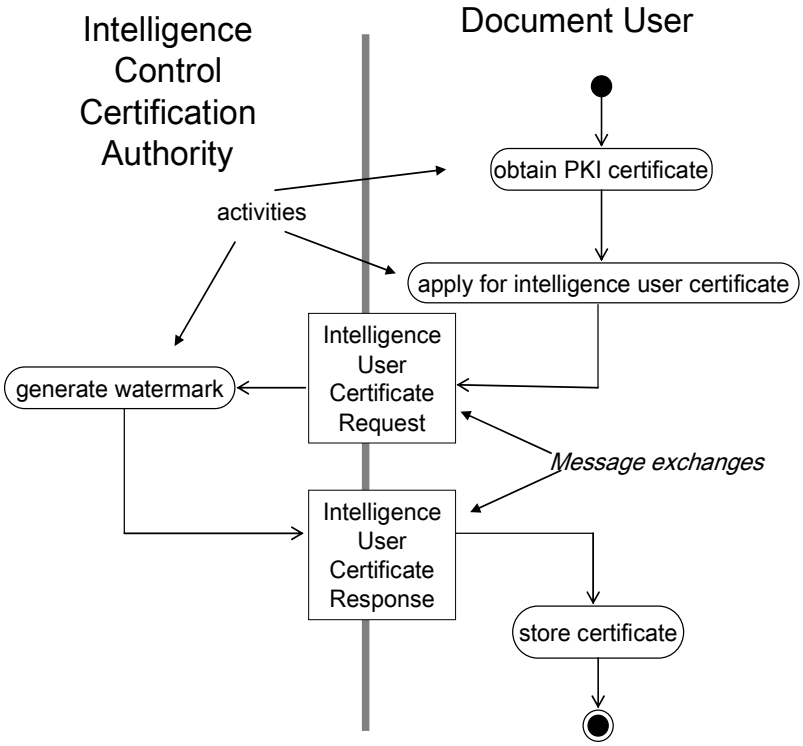

Figure 3: An UML Activity Diagram for the Acquisition of an *Intelligence user certificate*

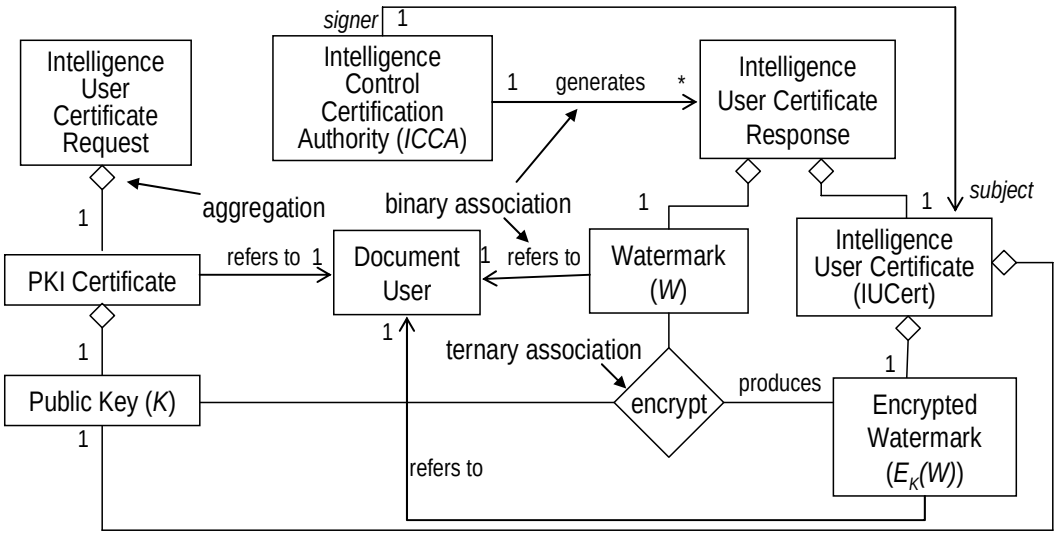

Figure 4: An UML Class Diagram of Data Relations for the Acquisition of *Intelligence user certificate*s

When the document user wants to acquire a watermark for accessing a document, he/she attaches his/her PKI certificate in an intelligence user certificate request and submits it to a trusted intelligence control certification authority. Like a PKI certification authority, an intelligence control certification authority is a third party trusted by document users, document producers, intermediaries, and judges. In response to the intelligence user certificate request, the intelligence control certification authority generates a legitimate watermark (*W*) and prepares an

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 3 / ISSUE 3 / DECEMBER 2008 / 103-118

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

intelligence user certificate containing an encrypted copy ($E_K(W)$) of W based on the document user's public key K. By $E_K(W)$, we mean:

$$E_K(W) = E_K(\{w_1, w_2, \ldots, w_m\}) = \{E_K(w_1), E_K(w_2), \ldots, E_K(w_m)\}.$$

The document user can verify the encrypted watermark, if necessary, using his/her private key and the received watermark. The watermark (W) uniquely identifies the document user. Like PKI private key, the watermark (W) is to be kept confidentially. Only the encrypted copy ($E_K(W)$) is used in the subsequent acquisition of intelligence documents in order to protect the secrecy of the user's watermark. The Intelligence control certification authority signs the intelligence user certificate to ensure the watermark validity of a document provider, while keeping the watermark private to the document user. In addition, this allows the document provider to verify the consistency between $E_K(W)$ and K.

3.2 Acquisition of Intelligence Documents

Figure 5 and Figure 6 present the process of acquiring an intelligence document and the associated data relations, respectively. In this process, a document user places a request containing his/her intelligence user certificate (*IUCert*) to an intermediary that knows where to find a provider of the requested document. The intermediary then forwards the *IUCert* to the corresponding document provider. The provider retrieves the encrypted watermark ($E_K(W)$) and the user's public key (K) from the *IUCert* and verifies their consistency based on the digital signature $Sign_{ICCA}(IUCert)$ by the intelligence control certification authority. If the verification succeeds, the document provider generates a unique identifier (V) and prepares a hashed value $H(\sigma)$ of a selected *permutation function* σ using an one way hash function, such as MD5 (RSA **¡Error! No se encuentra el origen de la referencia.**). The permutation is to increase the watermark robustness so that the watermarked intelligence documents can better resist tampering. Further details of the permutation function will be discussed in Section 4.

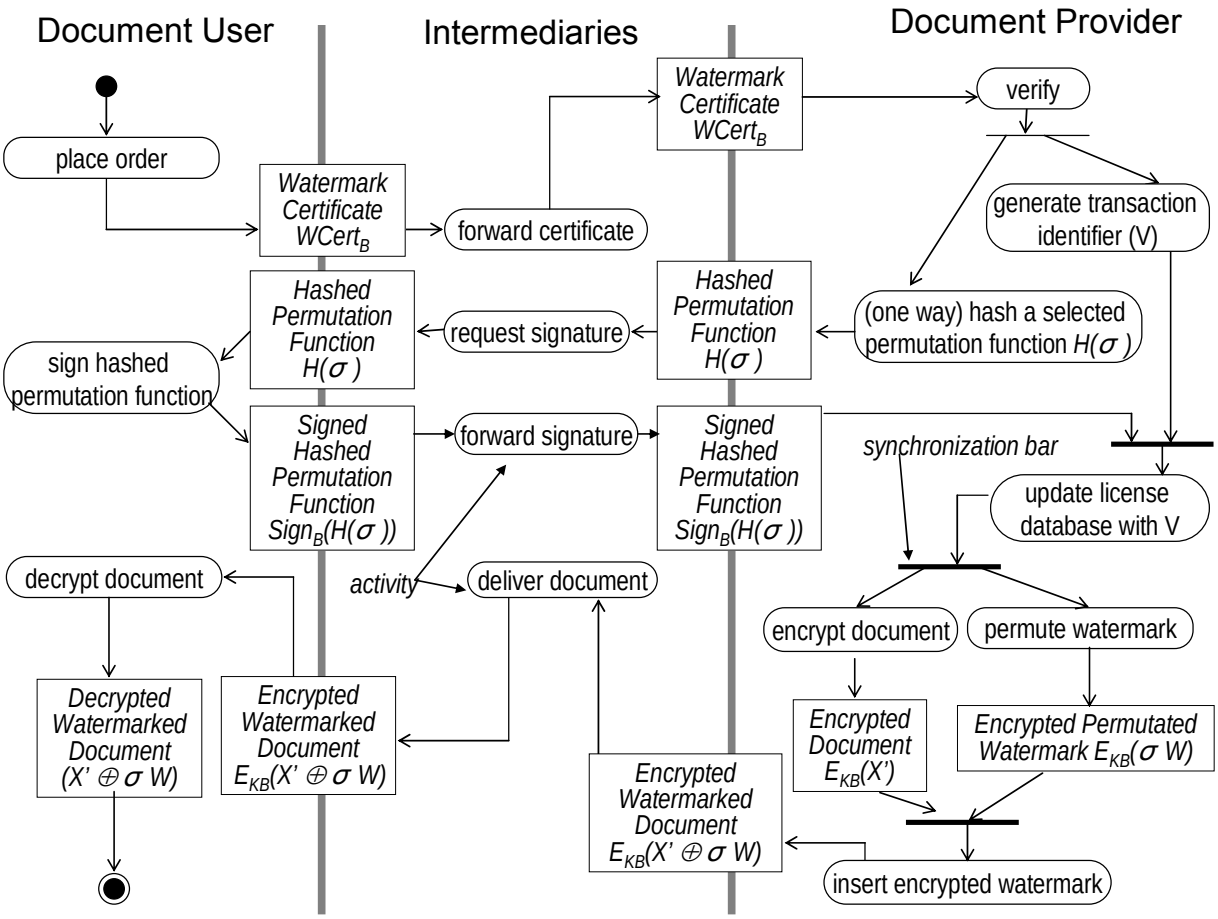

Figure 5: An UML Activity Diagram for the Acquisition of an Intelligence Document

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 3 / ISSUE 3 / DECEMBER 2008 / 103-118

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

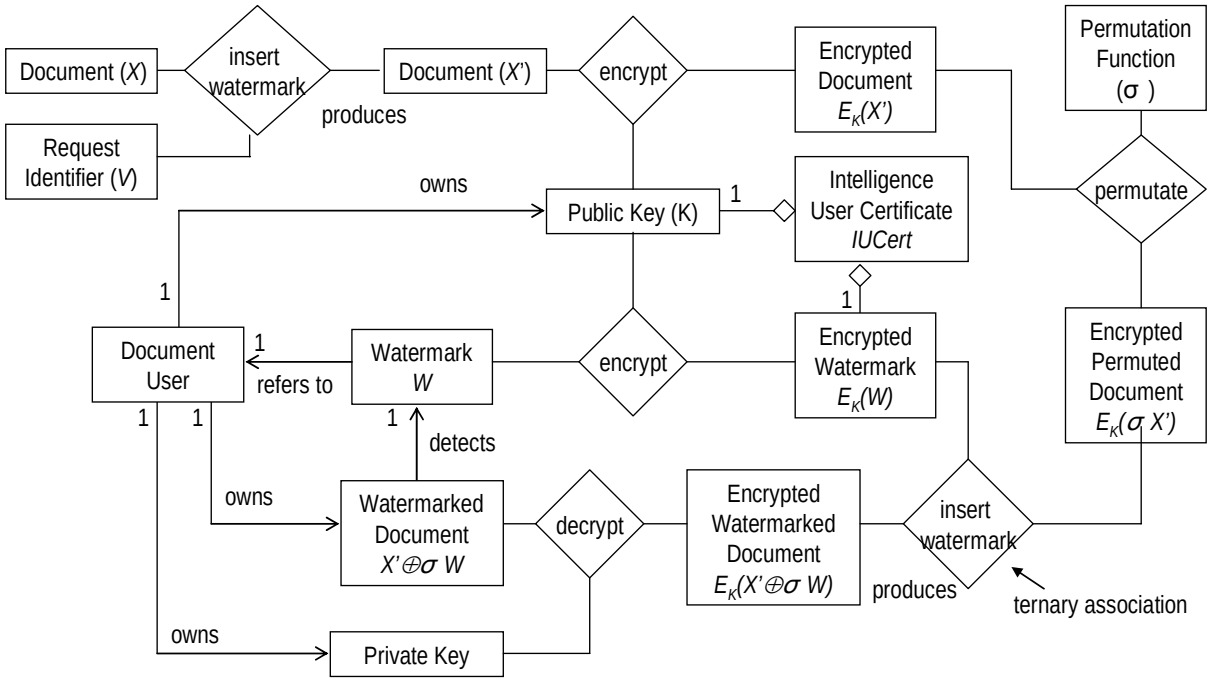

Figure 6: An UML Class Diagram of the Data Relations for the Acquisition of an Intelligence Watermarked Document

The hashed value is then signed with the private key of the user to produce $Sign(H(\sigma))$. The private key used must match the public key (K) in the intelligence user certificate. It can be readily checked by using the user's public key after receiving $Sign(H(\sigma))$. This procedure allows the user to acknowledge the permutation function to be used in the subsequent watermark insertion process. After receiving the signed hashed value $Sign(H(\sigma))$, the document provider validates the signature using K. If the validation succeeds, the request details and the signed hashed value are recorded to a database; otherwise the request is aborted. To facilitate the detection of access right violation, the document X' is watermarked with the unique identifier V. The document X' is then encrypted to $E_K(X')$ using the public key K. The provider also permutes the encrypted watermark $E_K(W)$ with the function σ, resulting in $\sigma(E_K(W))$. Since $E_K(W)$ is a vector in the form of $\{E_K(w_1), E_K(w_2), \ldots, E_K(w_m)\}$, the resultant value gives the encrypted permutated watermark $E_K(\sigma W)$. The provider then inserts the permutated watermark $E_K(\sigma W)$ into the encrypted document $E_K(X')$ using a non-invertible watermarking technique, resulting in $E_K(X' \oplus \sigma W)$. Here, we make use of a public key cryptosystem that exhibits *privacy homomorphism* with respect to the watermark insertion operator $\oplus$, that means,

For two pieces of document a and b,

$E_k(a \oplus b) = E_k(a) \oplus E_k(b)$*, where* $E_k(\ )$ *is the encryption function and k is the public key*

For example, the well known RSA **¡Error! No se encuentra el origen de la referencia.** public key cryptosystem is one of those that exhibit privacy homomorphism with respect to an addition operator.

The document provider delivers the encrypted watermarked document $E_K(X' \oplus \sigma W)$ to the intermediary. Alternatively, the document provider may deliver an URL at which the document user may retrieve the encrypted watermarked document $E_K(X' \oplus \sigma W)$; this saves the communication overhead of delivering the document through the intermediate intermediary. Now, only the document user can recover the plain document $(X' \oplus \sigma W)$ using his/her private key. As such, the document user is liable to unauthorized distribution of the document $(X' \oplus \sigma W)$. The mechanism ensures only the document user to whom the watermark identifies can recover the document. As the intermediary does not know the document user's watermark and the recovered watermarked document, both the interests of document users and providers can be protected.

The assumption for a watermark generation algorithm that supports an insertion function $X'=I(X,W,\sigma)$, a detection function $D(X',X,W,\sigma)$, and a privacy homomorphism are commonly supported by most watermark generation algorithms. The specific implementation of I and D does not affect the applicability of our protocol and therefore is not the focus of this paper. As such, the protocol can be used with most existing watermark generation algorithms.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 3 / ISSUE 3 / DECEMBER 2008 / 103-118

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

3.3 Resolution of Policy Violation

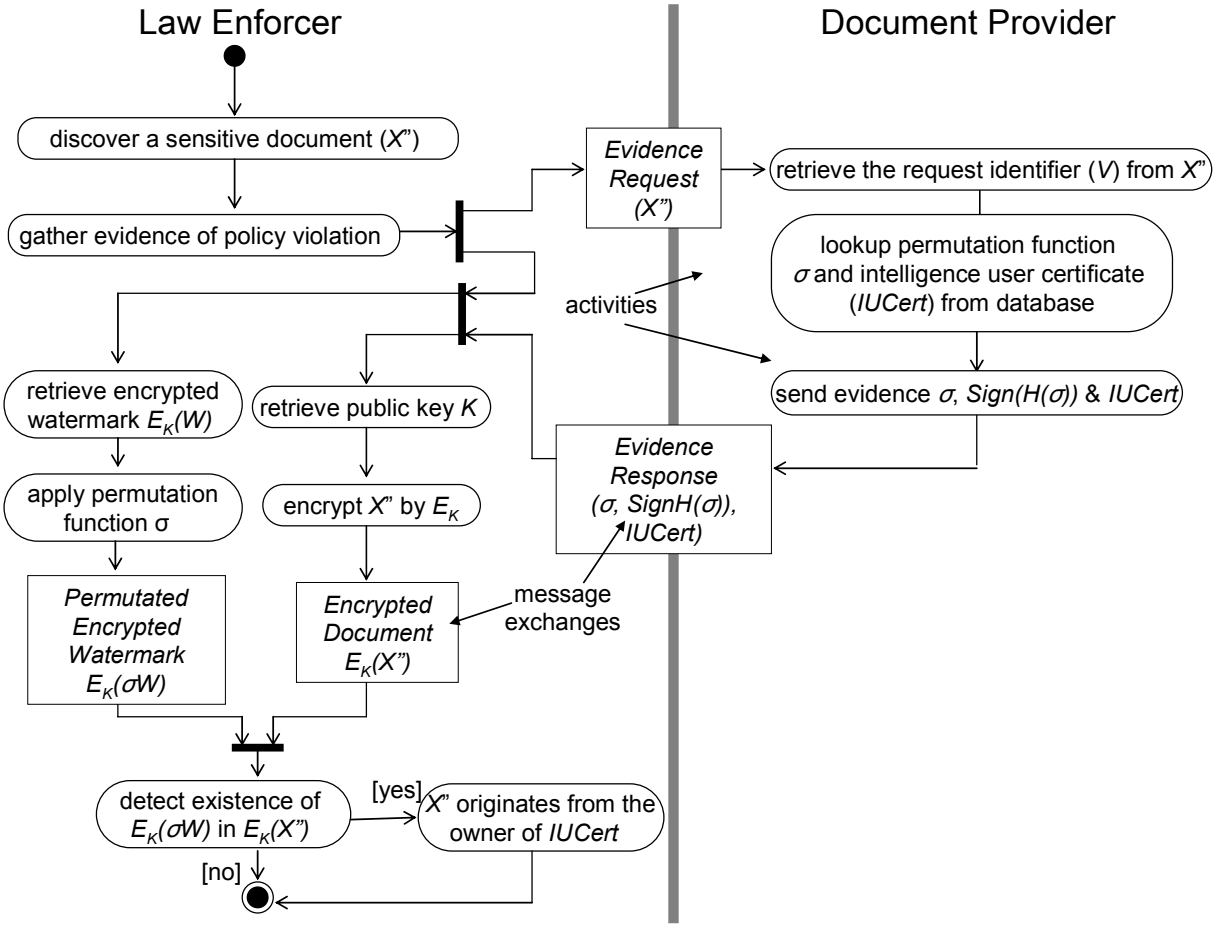

Figure 7: An UML Activity Diagram for the resolution of policy violation

Figure 7 presents the protocol for the policy violation resolution process. When an unauthorized copy of document, say *X"*, is found, the affected document provider can extract the unique request identifier *V* encoded in *X"*. Based on the corresponding request record in its authorization database, the document provider retrieves the permutation function σ, its signed hashed value $Sign(H(\sigma))$, and the intelligence user certificate containing $E_K(W)$ and K. The document provider submits these evidences to a judge for an allegation made against a user. In our approach, the judge can carry out the verification directly without the need of approaching the suspected document user for the watermark. This is a desirable feature because the document user might either provide a wrong watermark or have lost the watermark upon the allegation. In our protocol, if the watermark $E_K(\sigma W)$ can be detected in the encrypted version of unauthorized copy $E_K(X")$, the suspected document user is concluded guilty; otherwise innocent.

4 Implementation Framework

In this section, we present a case study based on our implementation framework to demonstrate the functionality and practicability.

4.1 System Architecture

Figure 8 outlines the system architecture of an intelligence document distribution infrastructure centered on intermediaries. An intermediary needs to have a full-scale intelligence document management system, while document users or providers may rely on that of an intermediary. The main components of the management system are as follows.

1. The *front end application* is tightly coupled with an *access control layer* for authentication and control of document users and providers.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 3 / ISSUE 3 / DECEMBER 2008 / 103-118

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

2. The *agencies / role manager* maintains the information of the document users and providers in strict confidentiality. The roles captured the capability and authorization about which kind of documents they can use or provide.

3. The *document tracker* keeps track of all the document request and provision, validating the authorization.

4. The *watermark engine* processes watermark insertion and extraction. In case a document provider cannot process watermark, it may fall back to use the facility provided by the intermediary.

5. The *document repository and database* collectively serve as a backend to store all the above information, documents, and logs for non-repudiation purposes.

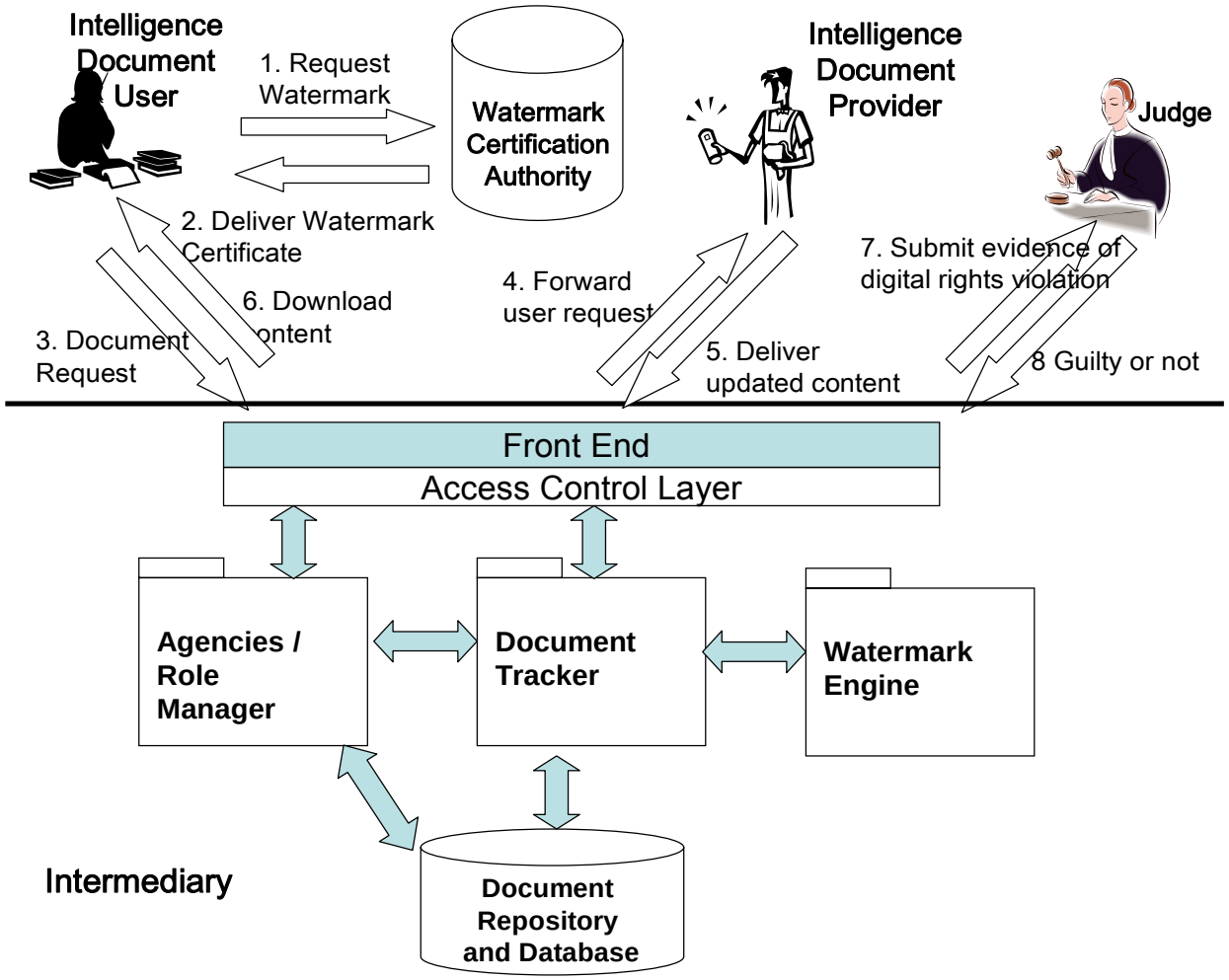

Figure 8: System Architecture Centered on Intermediaries

Furthermore, this architecture supports multiple tiers of intermediaries in an intelligence distribution network, which is an additional advantage. Instead of directly obtaining a document from a document provider, an intermediary can indirectly contact another capable intermediary for intelligence documents.

4.2 Structure of Intelligence User Certificate

Figure 9 depicts the structure of an intelligence user certificate. To support future extensions, each certificate carries a *version* number indicating its format. The *intelligence user certificate serial number*, assigned by the *intelligence control certification authority*, uniquely identifies each certificate. The *signature algorithm* identifier denotes the algorithm (say, md5RSA) used by the authority to sign this certificate. Fields are also contained in a certificate to indicate its issuer, owner, and effective period. The issuer of a certificate must be a trusted intelligence control certification authority. The *role* field specifies the role to be played by the owner of this certificate. Examples of role are individual, organization, and group. The role is used by document providers to define various policies. Each

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 3 / ISSUE 3 / DECEMBER 2008 / 103-118

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

certificate carries the public key of its owner, with which the certification authority encrypt the watermarks embedded in a certificate. This facilitates the verification of subject's identity against an encrypted watermark. Note that a document provider will permute the encrypted watermark before inserting it to a piece of digital content. The *watermarking scheme identifier* specifies the scheme to which the watermark is applicable. The *encrypted watermark* contains an encrypted value of each component of the watermark that the certification authority has issued to the owner of this certificate.

Version (of Intelligence user certificate Format)
Intelligence user certificate Serial Number
Signature Algorithm Identifier (for Intelligence Control Certification Authority's Signature)
Name of Intelligence Control Certification Authority
Validity Period (Start and Expiry Dates/Times)
Role
Owner's Public Key information (Algorithm Identifier & Public Key Value)
Watermarking Scheme Identifier
Encrypted Watermark

Digital Signature of a Trusted Intelligence Control Certification Authority

Figure 9: Format of an *intelligence user certificate* owned by a document user

4.3 Watermark Generation Algorithm

Our prototype uses a Spread-Spectrum watermarking scheme based on the one proposed by Cox *et al*. [7]. Other linear watermarking scheme can be used in the protocol as long as the watermark can be inserted in the encrypted domain, where digital documents are encrypted by public keys. The watermark consists of a set of 1,000 independent real numbers $W = \{w_1, w_2, \ldots, w_{1000}\}$. The choice of the value 1,000 is arbitrary; we may use a smaller number for watermark generation. Each of these real numbers is drawn from a Gaussian distribution using a pseudorandom number generator with a zero mean and a variance of 1.

The watermark is then inserted to the largest *1000* Discrete Cosine Transformation (DCT) coefficients of the digital document. For example, if a digital document X with the largest *1000* DCT coefficients $\{x_1, x_2, \ldots, x_{1000}\}$ is inserted with a watermark $W = \{w_1, w_2, \ldots, w_{1000}\}$, then the largest 1000 DCT coefficients of the watermarked document X' take the form of $\{x_1', x_2', \ldots, x_{1000}'\}$ where

$$x_i' = x_i(1+\alpha w_i), \quad 0 \le i \le 1000$$

and α is a small constant (*0.1* is used). After the insertion process, we use an inverse DCT operation to obtain the watermarked document X'. This completes the watermark insertion process. In order to detect the presence of a watermark in a digital document Y, we first use the DCT on Y to obtain the *1000* largest DCT coefficient of $Y=\{y_1,y_2,\ldots,y_{1000}\}$. Then we subtract each coefficient with x_i to obtain a set $T=\{t_1,t_2,\ldots,t_{1000}\}$, where

$$t_i = \frac{y_i - x_i}{\alpha x_i}$$

If the watermark $W = \{w_1,w_2,\ldots,w_{1000}\}$ is indeed present in Y, then there should be a high correlation between T and W. The formula for calculating the correlation is:

$$Corr(T, Y) = \frac{T \cdot W}{\sqrt{T \cdot T * W \cdot W}}$$

where • and * denotes the dot product operator and real number multiplication operator, respectively.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 3 / ISSUE 3 / DECEMBER 2008 / 103-118

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

Figure 10 shows our correlation result when the original watermark is compared with other 999 randomly generated watermarks. The spike in the graph represents the correlation of the original's watermark. We set our correlation threshold to 0.4 (tested out by experiment) to distinguish between a genuine watermark from a fake one.

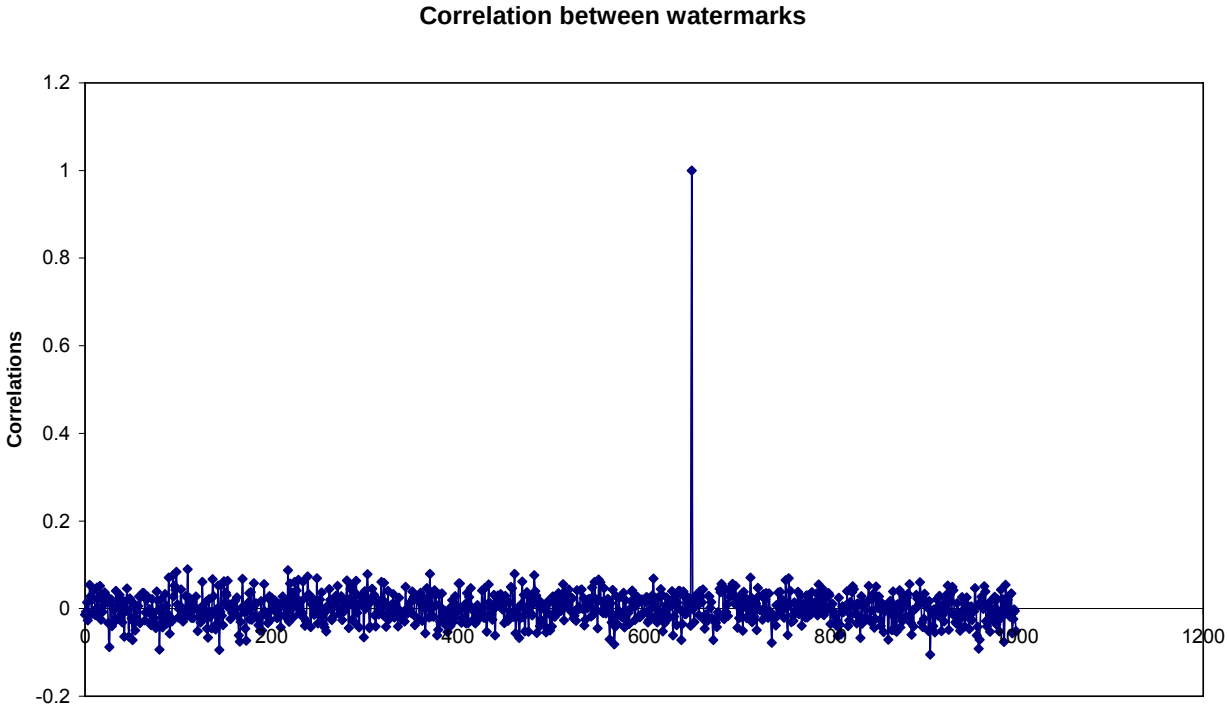

Figure 10: Correlation between watermarks

Next, we demonstrate our application of the RSA cryptosystem [51] for encryption in our protocol. In the encryption process, for a datum x and a public key a, the encrypted datum y is computed as:

$$y = E_a(x) = x^a \bmod n$$

where n is a product of two very large primes p and q. As for the decryption process, we use the private key b and compute:

$$x = D_b(y) = y^b \bmod n$$

If we have a watermark $W = \{(1+\alpha w_1), (1+\alpha w_2), \ldots, (1+\alpha w_{1000})\}$, then the process $X \oplus W$ can be considered as a watermark insertion operation because:

$$X \oplus W = \{x_1(1+\alpha w_1), x_2(1+\alpha w_2), \ldots, x_m(1+\alpha w_{1000})\}$$

By using the RSA cryptosystem property $(E(x) \oplus E(y)) = E(x \oplus y)$, watermarks can be inserted in the encrypted domain. For example, in our proposed protocol, we have X' as a watermarked music of X (where W is the watermark). An encrypted version of watermarked document $E_K(X' \oplus \sigma(W))$ can thus be generated through the computation $E_K(X') \oplus \sigma(E_K(W))$. This enables the document user to recover the watermarked document $X' \oplus \sigma(W)$ with his/her private key.

4.4 Permutation function

During the watermark insertion phrase, the provider has to permute the document user's encrypted watermark. We implemented this function (σ) by randomly swapping the 1000 watermark coefficient. The following code snippet illustrates how this can be done in the C programming language:

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 3 / ISSUE 3 / DECEMBER 2008 / 103-118

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

```
void permutefunc(VLONG wmark[], int size, int seed)
{
        int i, index1, index2;
        srand(seed);
        for (i=0; i < rand() % 100 + 50) // min. 50 times, max 150 times
        {
              VLONG tmp;
              index1=rand()%size;
              index2=rand()%size;

              // swap the two watermark coefficient
              tmp = wmark[index1];
              wmark[index1]=wmark[index2];
              wmark[index2]=tmp;
        }
}
```

The `VLONG` structure can hold an integer of any size and `seed` represents the seed number used for random number generator. The provider will compile this code into an object code. Together with the random seed used, the provider will applied SHA-1 [22] to the object code to generate a message digest $H(\sigma)$. This message digest is put on the provider's site and must be downloaded by the document user beforehand. Then, the document user can sign this message digest $Sign(H(\sigma))$.

5 Discussions

Watermark robustness is a key topic studied in the discipline of signal processing. Robustness refers to the ability to detect the watermark from a watermarked copy after common signal processing operations that do not destruct the contents. Various robust watermarking schemes (see section 2.3) have recently been proposed to survive different kinds of attacks, such as the insertion of malicious watermarks, spatial filtering, band-pass filtering, lossy compression, printing and scanning, re-sampling and noise addition, etc.

The scheme described in this paper supports watermark privacy so that one need not release the watermark obtained from an intelligence control certification authority. This is analogous to the privacy of private key in the Public Key Infrastructure. In the proposed scheme, each page of the textual documents is treated as an image in order to leverage on the existing robust watermarking techniques for images.

The proposed scheme is primarily aimed at improving privacy and confidentiality of the originators, namely the document providers. It allows a document provider to release its documents only to users who agree to be liable to the distribution of the acquired copies. If a user wishes to legitimately pass the document to another one, the approval from the original document providers must be sought so that another watermarked copy can then generated by the document providers and distributed to the target users. Note that this watermarked copy is encrypted using the target user's public key and therefore could only be opened by the target user. The issue of the providers' privacy has been further enforced throughout the distribution process because of the separation between the intermediary and the document provider. The scheme can complement conventional access control policy by providing traceability to the distribution to both hard and soft copies of documents.

5.1 Access Policy Model

We employ a role-based [3] access policy model augmented with an access management mechanism similar to that of the Structured Query Language (SQL) [9] in databases, as depicted in Figure 11.

A work unit may consist of multiple member work units down to the level a document user. A work unit, being a document user, may play one or more roles depending on its job function, seniority, group memberships, affiliations, etc. Access rights acquired by a work unit are automatically inherited by its members.

Note that a work unit may, at the same time, be a document provider of some documents and a document user of other documents. The document provider sets an initial access policy by granting access rights to roles, which are played by document users. A grantor who grants an access right may revoke it. Access rights may have the following attributes: *expiry time* and *grant option*. When an expiry time is specified, the affected document users will no longer have access rights to them after expiry. The artifact of *grant option* allows a document user of a document to be its access rights grantor. A document user, who is granted with a grant option, has the privilege in granting it further to other roles. If this happens, the system informs the provider of the document and its document users in the granting chain, so that the involved grantors in the chain may revise the access policy in case of undesirable access. The privilege of grant option expires upon the expiry or revocation of the granted access rights. We employ cascade

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 3 / ISSUE 3 / DECEMBER 2008 / 103-118

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

semantics on access rights revocation (as in SQL). Suppose a grantor *A* grants rights to *B* with grant option and *B* grants it further to *C*. The revocation of the rights by *A* from *B* will force the revocation of the corresponding rights acquired by *C* from *B*.

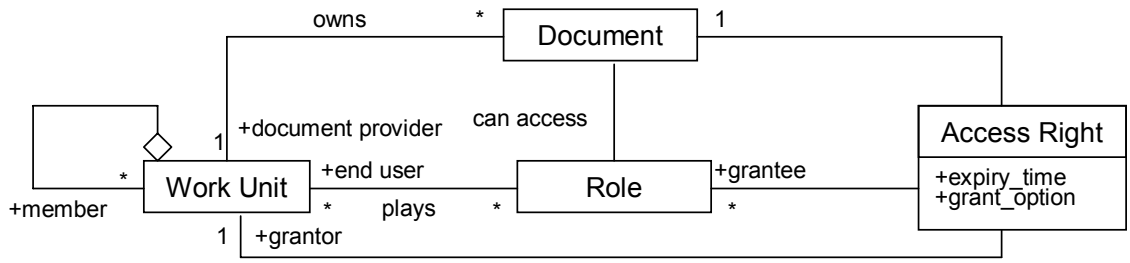

Figure 11: Access Policy Model in UML

5.2 Tracing of Source of Document Leakage

This is one of the most important applications of the proposed distribution protocol, where the document providers cannot trust the distribution channel of their intelligence documents. The watermark inserted at an intelligence document can identify the user responsible for the document. Thus, a document user must take uttermost care of the confidentiality of the document. Otherwise, a betraying or careless user leaking the document to an unauthorized party can also be traced by means of the watermark attached in the leaked document and be subsequently made responsible for policy violation. If the users are warned beforehand about the watermark, this keeps them alert to the enforcement of document confidentiality. Intelligence documents in this category may also be extended to other application such as inspection films prepared by film producers, audio clips used in public examinations, headline TV news, and so on.

On the other hand, another usage of documents with hidden watermarked carrying personal identification is to trace the route of unauthorized leakage or spies. In this case, the documents users, of course, are not told about this fact in order to be effective.

5.3 The Role of an Intermediary in our Infrastructure

Since each watermarked document is encrypted using its user's public key, the document may not be decrypted by parties other than the document user itself. Similarly, a document provider only needs to trust the *intelligence user certificate* issued by a trusted *intelligence control certification authority*. Since the certificate is digitally signed by the certification authority, integrity of the certificate is guaranteed. Note that, an intermediary cannot imitate a user to successfully request an intelligence document. The proposed protocol mandates the document provider to ask the user to digitally sign the message digest of a permutation function before document distribution. This assures that the request is made by the document user.

An important role of an intermediary in our infrastructure is to decouple document users from document providers. This allows both parties remain highly anonymous to each other. Here, the PKI certification authority concerned is trusted not to reveal the owner's identity of public keys. As such, document providers could not identify the owners from their public keys in the intelligence user certificates. To strengthen protection of intelligence agents, the protocol is so designed that document users cannot tell if their contact parties are intermediaries or document providers. Similarly, document providers cannot differentiate document users from intermediaries. There can also be multiple tiers of intermediaries. In other words, an intermediary may acquire an *intelligence document* through another intermediary.

With the support of contemporary and upcoming mobile technologies, document users and providers can have ubiquitous support from intermediaries, which is especially invaluable in this kind of applications. On the other hand, if the document user and provider know each other, the intermediaries can be bypassed. This becomes a special case of the protocol and the does not affect its integrity.

6 Conclusions

In this paper, a novel document distribution protocol has been proposed to address a problem in an intelligence distribution network so that document management policies can be properly reinforced. The protocol provides a concrete support for non-repudiation in the document distribution processes. It allows the document user, who has made each document copy, to be uniquely identified and accountable, and thus the route of document leakages can be identified. The support of non-repudiation in fact reduced to the requirement of the absence of mutual trusts between document users and document providers. To realize the protocol, we have also outlined a possible

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

implementation centered on intermediaries, which can isolate document users and providers. Further, we have discussed how the protocol is designed to address two important issues: the maintenance of watermark secrecy and the prevention of Trojan horse attacks. In particular, the use of intelligence user certificates together with intermediaries in our protocol help maintain the identity secrecy between document suppliers and users (but yet traceable upon disputes). This is a key contribution to support for intelligence applications.

Besides implementing a prototype for this infrastructure, we are looking into issues of integrating this watermarking protocol into our ADOME workflow management system [6] for intelligence document workflow applications. On the other hand, we are investigating various types of security policies that can be integrated to our document watermarking protocol.

Acknowledgments

We thank Hanif Curreem for his assistance in the prototype implementation of the proposed document distribution protocol. The research work is partially supported by the Hong Kong Research Grant Council (Grant ref. DAG03/04.EG27).

References

[1] H. Berghel, Watermarking Cyberspace, Communications of the ACM, vol. 40, no. 11, pp. 19-24, 1997.
[2] J. Bustos and K. Watson, Beginning .Net Web Services using C#, Birmingham, UK: Wrox Press Ltd., 2002.
[3] S. C. Cheung and D. K. W. Chiu, A watermarking infrastructure for enterprise document management, in Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS-36), CDROM, IEEE Press, Big Island, Hawaii, 2003, 10 pages.
[4] S. C. Cheung and H. Currem, Rights protection for digital contents redistribution over the Internet, in Proceedings of the 26th Annual International Computer and Applications Conference (COMPSAC 2002), Oxford, August 2002, pp. 105-110.
[5] D. K. W. Chiu, Q. Li, and K. Karlapalem, A meta modeling approach for process management system supporting exception handling, Information Systems, vol. 24, no. 2, pp. 159-184.
[6] D. K. W. Chiu, Q. Li. and K. Karlapalem, Web interface-driven cooperative exception handling in ADOME process management system, Information Systems, vol. 26, no. 2, pp. 93-120.
[7] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997.
[8] S. Craver, N. Memon, B. L . Yeo, and M. M. Yeung, Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks and implications, IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 573-586, 1998.
[9] R. A. Elmasri and S. B. Navathe, Fundamentals of Database Systems, Boston: Addison-Wesley, 5th edition, 2007.
[10] K. Gopalakrishnan, N. D. Memon, and P. Vora, Protocols for watermark verification, IEEE Multimedia, vol. 8, no. 4, pp. 66-70.
[11] F. Hartung and F. Ramme, Digital rights management and watermarking of multimedia content for m-commerce applications, IEEE Communications Magazine, vol. 38, no. 11, pp. 78-84, 2000.
[12] J. M. Jun, B. M. Lee, K. K. Kim, and D. H. Won, Digital watermarking and practical distribution protocol for digital contents copyright protection, in Proceedings of the WISA'2000, Seoul, Korea, 2000, pp. 251-264.
[13] S. Katzenbeisser and F. A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital watermarking, Norwood, MA: Artech House, 2000.
[14] D. Kirovski and H. Malvar, Robust Spread-spectrum audio watermarking, in Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing, Salt Lake City, UT., 2001, pp. 1345-1348.
[15] J. S. H. Kwok, S. C. Cheung, K. C. Wong, K. F. Tsang, S. M. Lui, and K. Y. Tam, Integration of Digital Rights Management into Internet Open Trading Protocol (IOTP), Decision Support Systems, vol. 34, no. 4, pp. 413-425, 2003.
[16] C. Larman, Applying UML and Patterns, Upper River Saddle, NJ: Prentice Hall, 1997.
[17] N. Memon and P. W. Wong, A document user-seller watermarking protocol, IEEE Transactions on Image Processing, vol. 10, no. 4, pp. 643-649, 2001.
[18] S. K. Nair, B. C. Popescu, C. Gamage, B. Crispo, and A. S. Tanenbaum, Enabling DRM-preserving digital content redistribution, in Proceedings of the Seventh IEEE International Conference on E-Commerce Technology (CEC'05), Munich, Germany, 2005, pp. 151-158.
[19] 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, 1998.
[20] R. A. Mollin, RSA and Public-Key Cryptography, Boca Raton: Chapman & Hall/CRC, 2002.
[21] M. Schneider and S.-F. Chang, A robust content based digital signature for image authentication, in Proceedings of the International Conference on Image Processing 1996, vol. 3, pp. 227-230, 1996.
[22] W. Stallings, Cryptography and Network Security, Principles and Practice, 4th edition, Upper River Saddle, NJ: Prentice Hall, 2006.
[23] J. Su, F. Hartung, and B. Girod, Digital watermarking of text, image and video documents, computers and

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762008000200008

graphics, vol. 22, no. 6, pp. 687-695, 1998.
[24] P. Wolf, M. Steinebach, and K. Diener, Complementing DRM with digital watermarking: mark, search, retrieve, Online Information Review, vol. 31, no. 1, pp. 10-21, 2007.