行政院國家科學委員會專題研究計畫　期中進度報告

數位權限管理系統(1/3)

計畫類別：個別型計畫
計畫編號：NSC92-2213-E-002-080-
執行期間：92 年 08 月 01 日至 93 年 07 月 31 日
執行單位：國立臺灣大學資訊工程學系暨研究所

計畫主持人：賴飛羆

計畫參與人員：賴飛羆、胡裕華

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 93 年 6 月 1 日

行政院國家科學委員會專題研究計畫期中報告

數位權限管理系統

Digital Right Management System

計畫編號：NSC92-2213-E-002-080
執行期限：92 年 8 月 1 日至 93 年 7 月 31 日

主持人：賴飛羆　國立台灣大學資訊工程系
計畫參與人員：胡裕華　國立台灣大學資訊工程系

一、中文摘要

由於科技的進步與電子設備的普及，以及近幾年網際網路的快速發展，人們的生活已與數位化的資訊有不可分割的密切關係，數位化資訊本身有著儲存成本低廉，複製容易，並且可以傳播快速，即時等優勢，但是如何保護這些數位化資訊，以及規範其使用的方式，則成為一個相當重要的需求。在數位權限管理系統中，有一個重要的問題是如何將數位化的資料，有效且安全地送給訂購者，而且能限制訂購者無法肆意的散布所收到的數位資料。在這篇報告中，我們由目前所提出了一些方法中，分析如何達成追蹤數位化資料是否被散布。

關鍵詞：數位權限管理系統

Abstract

Due to the advance of technology, the generalization of the electronic devices, and the rapid development of the Internet in recent years, the style of human living has the indivisibility with the digital information. The digital information has the advantages of low-cost to store, easy to duplicate, fast to spread, and real-time. But how to protect the digital information and regulate the usage becomes a critical issue. In Digital Rights Management system, one important issue is that how to efficiently and securely deliver the digital content to the consumers, and restrain the consumers from distributing the digital content arbitrarily. In this report, we based on the proposed schemes to analyze how to identify whether digital content is distributed or not.

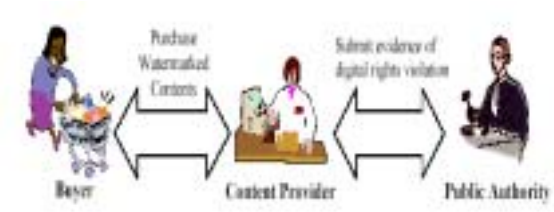
Keyword: DRM

二、緣由與目的

資訊的保密是在通訊上的重要課題。但當資訊安全地送給訂購者之後，訂購者若沒有妥善地保存這些資訊，而將這些資訊任意的散布，對原來的資訊所有權人將會造成相當的傷害；這也是另一個可能洩漏資訊的方式，所以如何能追蹤出資訊是從何流出，便成為現今保護數位內容的研究重點。而在這類課題中，如何同時保護資訊所有權人及訂購者的權益是最主要的研究重點，此外，如何增強訂購者的隱私權也是另一個研究方向。

為達成上述的目的，需要使用到一些技術：浮水印(Watermarking)、基礎公鑰建設(PKI)中的數位簽章(Digital Signature)及公鑰系統(Public Key System)、憑證管理中心(CA)等。而每一個項目均扮演相當重要的角色。浮水印能讓我們追蹤數位資訊是從何處散布？基礎公鑰建設可以使資訊所有權人及散布者在發生爭執時，做為判斷的依據。而憑證管理中心負責產生合法的金鑰及浮水印。

三、研究方法與演算法

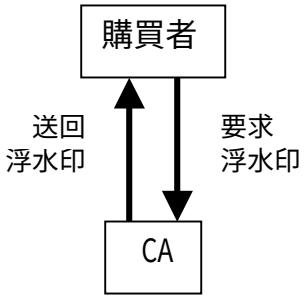


圖一、資訊交易協定的三個體

在多數的數位資訊交易協定中，可以分成三個主要的個體如圖一及分為三個階段：

(1) 產生浮水印階段：

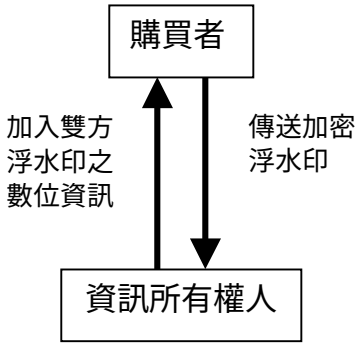
為了確保訂購者的權益, 訂購者所附加於數位資訊的浮水印不能讓資訊所有權人或是資訊銷售人員知道, 否則可能會被陷害；而又為確保資訊所有權人的權益浮水印又不能由訂購者任意產生後, 沒有留下任何証明的資訊, 否則在日後舉証上會造成問題。



圖二、產生浮水印階段

(2) 浮水印加入數位資訊階段：

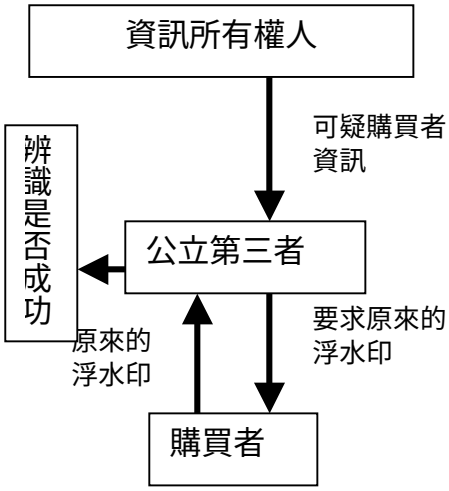
除了上述訂購者的浮水印外, 資訊所有權人或是資訊銷售人員也會加入自己的浮水印以便追蹤是從哪位訂購者所散布出去. 又因為最後的數位資訊將傳送給訂購者, 若直接把訂購者的浮水印加到數位資訊中, 可能會使訂購者把浮水印移除, 所以在加入訂購者的浮水印時, 會先把訂購者的浮水印排序後再加入數位資訊中, 使得訂購者無法任意移除含有訂購者相關訊息的浮水印, 以免造成舉証的問題。



圖三、浮水印加入數位資訊階段

(3) 違法散布辨別階段：

主要的目的為辨別當資訊所有權人或是資訊銷售人員得到相關訊息, 某個數位資訊是從某人非法散布時, 藉由在此數位資訊中的浮水印來判斷是從哪位購買者之處所流散出來, 之後再把該位訂購者的保留的浮水印的憑証、排序規則、資訊所有權人或是資訊銷售人員的浮水印交給中立的仲裁者來判斷。



圖四、違法散布辨別階段

若可以成功的判斷是從某位惡意的訂購者所散布，則為成功的協定；若無法完全的判斷，則為失敗的協定。

四、成果與討論

在目前的數位資訊交易協定中，常見的攻擊方式有下幾種：

(1)浮水印技術攻擊：
在這類的協定中，需要把浮水印放入數位資訊中，而又不能讓人可以任意的把浮水印拿掉。而目前在浮水印技術還沒有可以完全的達成此一目的[1]。

(2)基礎公鑰建設攻擊：
主要為公鑰系統(Public Key System)無法滿足數位資訊交易協定需求的問題。因為訂購者的浮水印在加入數位資訊時，不能讓資訊所有權人得知，而又要資訊所有權人把浮水印加到數位資訊中，所以使用的密碼系統要滿足交換性，即 $E(K_1,E(K_2,DD))=E(K_2,E(K_1,DD))$ $E(K,A)$表示使用金鑰 K 把 A 的內容加密。而非所有的密碼系統都有交換性，在為了滿足交換性的要求下對密碼系統所做的修改動作[2]可能會洩漏一些資訊，反而造成修改後的密碼系統不安全。

(3)共謀攻擊：
原本 CA 的目的是為了當公正的第三者，但是在[1] [2]的方法中，提供了一個漏洞，也就是當 CA 和資訊所有權人共謀時，會使得訂購者的資訊曝光，除了匿名性不存在之外，更會使得訂購者的浮水印被得知；在[2] [4]提到為了避免這種情形，就沒有產生浮水印的 CA 存在。

(4)訂購者的浮水印被資訊所有權人得知：
在[1] [2] [4]的方法中，只要資訊所有權人能得知最終訂購者手上的數位資訊，加上原有的數位資訊，就可以拿到經過排序的訂購者的浮水印，而資訊所有權人又擁有原來的排序方法，於是就可以得到原來訂購者的浮水印，如此就無法達到保護原來不要讓資訊所有權人拿到訂購者的浮水印的目的。

(5)訂購者給假的浮水印：
在浮水印加入數位資訊階段，訂購者需提供加密後的浮水印給資訊所有權人，因為此時無法得知浮水印的正確性；[4]中所提出的方法，若提供假的浮水印，資訊所有權人也無法得知，最後訂購者散布含有假的浮水印的數位資訊，就無法進行違法散布辨別階段。

(6)資訊所有權人惡意栽贓：
若資訊所有權人可以得知訂購者的浮水印，之後就任意的產生有訂購者浮水印的數位資訊，再嫁禍給訂購者。

目前我們已經了解這些攻擊的方法，及一些應對之道，我們將從既有的協定中，衍生新的協定以避免上述的攻擊。

由上述的攻擊方式可以得知數位資訊交易協定中有幾項重點：

(1) 浮水印的技術
在此交易上需要有兩個浮水印方法，一個用於資訊所有權人的浮水印，用於辨別是哪一位購買者？另一個用於購買者的浮水印，作為當發現數位內容含有浮水印時的不可否認性；這些浮水印需確保不會讓資訊所有權人、購買者或其他的惡意的攻擊者任意的移除。

(2) 具有交換性的密碼系統
在浮水印加入數位資訊階段中，需要確保訂購者的浮水印不被知道，這就可以利用有交換性的密碼系統來完成這些任務。

(3) 訂購者浮水印的保護
要保護訂購者浮水印的原因是為了避免資訊所有權人或是資訊銷售人員可以任意的產生有訂購者資訊內容的數位資訊，且散布出去的問題；在[1]中所提的方法中，資訊所有權人或資訊銷售人員擁有大多的資訊，除了訂購者浮水印，如果再得到最後購買者手上的數位資訊，則可以得到原來訂購者的浮水印；所以可以把一些資訊，例如對訂購者的浮水印的排列，交給 CA 來決定，如此可以使得資訊所有權人或資訊銷售人員即使得

知購買者手上的數位資訊仍無法得知訂購者原來的浮水印。

(4) 訂購者浮水印的完整性

在有匿名性的數位資訊交易協定中，常常不需要 CA 的存在，所以由訂購者自行產生浮水印, 也因此造成浮水印無法驗証是否是有效的，[4]所提出的改善的方式，就會有這個問題, 所以為了確保資訊所有權人的權益, 就要保存訂購者浮水印的憑証。

此外在傳統的資訊交易上，存在所謂的"二手書"，也就是當第一次購買者覺得不再需要這些資訊時，可以把這些資訊轉賣出去；在數位的世界上，第一手和第二手的資訊內容可能是一模一樣。若第二手資訊比較便宜，則會衝擊到原來的資訊所有權人的權宜；又若可以轉賣資訊的話，可以轉賣幾份?如經銷商可能拿一份母帶，拷貝多份賣出，而非直接向資訊所有權人拿多份資訊。這些問題，目前還待研究。

結論

這篇報告中，我們提出了一些在數位資訊交易協定中常見的攻擊方式，讓我們可以去評斷所設計的數位資訊交易協定的缺失，也同時知道在設計一個協定時所要考慮的項目。因為數位資訊交易協定中，把一些識別資訊放入數位資訊中，所以購買者無法肆意的傳遞這些資訊，進而達到管理數位資訊的目的。

五、成果發表

1. J.C. Lin, C.H. Tzeng, F. Lai, H.C Lee. Optimizing Centralized Secure Group Communications with Binary Key Tree Recomposition, AINA 2004

參考資料

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

[2] J.G.Choi,K.Sakurai,J.H.Park, Does it Need Trusted Third Party? Design of Buyer-Seller Watermarking Protocol without Trusted Third Party, Proc. Applied Cryptography and Network Security'03, LNCS 2846, p.265-279, 2003.

[3] S.C. Cheung, H.F. Leung, C. Wang, A Commutative Encrypted Protocol for the Privacy Protection of Watermarks in Digital Contents, Proc. 37th Hawaii International Conference on System Sciences, Hawaii, p. 40094a, 2004.

[4] B.M Goi et al, Cryptanalysis if Two Anonymous Buyer-Seller Watermarking Protocols and an Improvement for True Anonymity,Proc. Applied Cryptography and Network Security'04, LNCS 3089, p.369-382, 2004.

[5] P. W. Wong, and N. Memon. Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verfication. In *IEEE Transactions on Image Processing*, vol. 10, no. 10, pages 1593-1600, October 2001.

[6] S. C. Cheung, and H. Curreem. Rights Protection for Digital Contents Redistribution Over the Internet. In Proceedings of the 26th Annual International Computer Software and Applications Conference (COMPSAC'02) , 2002 IEEE

[7] W. Stallings. Cryptography and Network Security: Principles and Practice, 2nd edition. Prentice-Hall Inc., 1999.

[8] P. Biddle, P. England, M. Peinado, and B. Willman. The darknet and the future of content distribution. In 2002 ACM Workshop on Digital Rights Management.

[9] B. P.tzman, W. Waidner, Anonymous Fingerprinting, Eurocrypt'97, LNCS 1233, pp. 88-102, 1997.

[10] Hak-Soo Ju, Hyung-Jeong Kim, Dong-Hoon Lee and Jong-In Lim., An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control¨, ICISC2002, LNCS 2587, p. 421-432, 2003

[11] Asokan, N., Shoup, V. and Waidner, M. (1998), "Optimistic fair exchange of digital signatures, In Advances in

Cryptology-EUROCRYPT’98, LNCS 1403, p 591-606, 1998

行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※ ※
※ 數位權限管理系統 ※
※ ※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：☑個別型計畫 □整合型計畫

計畫編號：NSC92-2213-E-002-080

執行期間：2003 年 8 月 1 日至 2004 年 7 月 31 日

計畫主持人： 賴 飛 羆 教授

共同主持人：

計畫參與人員： 胡裕華 （博士班研究生）
曾建華 （碩士班研究生）
鄭世揚 （碩士班研究生）

本成果報告包括以下應繳交之附件：

□赴國外出差或研習心得報告一份

□赴大陸地區出差或研習心得報告一份

□出席國際學術會議心得報告及發表之論文各一份

□國際合作研究計畫國外研究報告書一份

執行單位：國立台灣大學資訊工程系

中 華 民 國 2004 年 5 月 31 日