第二十六章

電子檔案之安全技術

Security Techniques for Electronic Records

李正吉
Cheng-Chi Lee
國立中興大學資訊科學所博士班學生
Ph.D. Student, Department of Computer Science, National Chung Hsing University

林詠章
Iuon-Chang Lin
高雄應用科技大學資訊管理系助理教授
Assistant Professor, Department of Information Management, National Kaohsiung University of Applied Sciences

黃明祥
Min-Shiang Hwang
朝陽科技大學資訊管理系教授
Professor, Department of Management Information System, National Chung Hsing University

壹、前言

二十一世紀將是另外一次的資訊革命，而網際網路將是促成這場革命的先鋒，且在網路人口急劇遞增之際，網際網路的發展應用，勢將改變我們以往的生活模式。『秀才不出門，能知天下事』這句俗語不僅可以道出網路的特質，更可以反映出網際網路的便利性，例如網路銀行、網路購物、訂閱電子報、網路報稅、網路下單等。網際網路已經慢慢與我們的生活相結合，未來網際網路的商業應用，將引導我們邁向二十一世紀。

網際網路的盛行，帶動了各行各業紛紛投入這個商機，透過網際網路無遠弗屆的特性，把商機或是資訊傳送到任何一個地方。基於這個特性，目前政府正在

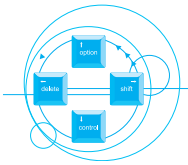
朝著電子化政府的目標邁進，希望透過網路的應用，提供民眾便利的服務，節省民眾到窗口辦理的時間。早期，各機關檔案資料均以紙張的方式儲存，不僅民眾調閱不便，頻繁的調閱頻率亦造成紙張的損壞，使得檔案紀錄的保存不易。

七十年代由於微縮技術成熟，許多機關採用微縮技術作爲檔案永久儲存的媒介，然而由於微縮片的保存環境要求嚴苛，且製作及翻印的成本昂貴，加上不利於線上調閱，在事事講究效率的社會中，微縮技術並不符合當前的社會需求，目前多用於重要檔案資料的永久保存之用。現今，電腦科技發達、網際網路的盛行、文件掃描及光碟技術的成熟，以電子化方式儲存的檔案資料，經過適當的整合管理，不但經濟、環保更有利於提供線上調閱服務，世界上許多先進國家已採用電子設備處理檔案，並以數位化的方式儲存。可預期的，未來以電子化儲存的檔案資料將與日遽增，如何有效保存並管理這些檔案資料將是目前重要的議題。

由於網路是開放式的，任何人都可以從網路中間攔截或修改資訊，所以網路安全就顯得特別重要，如何防止駭客從網路中間破壞，將是一個很重要的研究課題。而電子檔案在網路上傳送的安全考慮就亦顯重要，由於是以數位的方式儲存，使得檔案的複製、僞造及竄改就變的極爲容易，如何防止電子檔案被不法人士輕易的僞造、竄改檔案內容，將是電子檔案安全上極爲重要的議題。電子檔案在網路上傳送，雖然爲我們生活帶來許多便利，但也衍生出許多安全方面的問題值得我們深思，例如，訊息存放在資料庫系統中可能遭到非法的存取、訊息在網路上傳遞可能遭到竊取或竄改等，種種的攻擊方式都有賴於健全的安全機制來加以預防或偵測。

因此，國內外有許多學者紛紛投入此一領域進行研究，足見其重要性。相關的研究有：使用者驗證機制，以防止非法使用者的入侵電腦；存取控制機制，針對使用者的存取權限給予適當的限制，使其能在授權範圍內獲得合理的電腦資源；電子加密技術，可確保機密資訊的安全性；數位簽章技術可確認訊息來源的合法性及訊息內容的完整性。這些研究的目的，無非是要達到資訊系統的安全需求，確保資訊的私密性、完整性、以及鑑別性。

可預期的未來各機關會有越來越多以電子化方式儲存的檔案紀錄，爲因應此一趨勢，電子檔案安全之研究，刻不容緩。接下來，我們將會在第二節中，介紹



電子檔案在網路上傳送時，所可能面臨的威脅，另外，我們會說明爲了防止安全上的威脅，所需考量的一些基本安全性需求。第三節中，爲了達到這些安全性需求，我們將介紹一些可以應用的技術。最後在第四節中，我們將針對電子檔案安全之技術作一簡單的結論。

貳、電子檔案之安全威脅及安全需求

由於網際網路的盛行，政府自民國八十年代開始陸續推動電子化政府，藉以提高政府的行政效率，縮短紙上作業的時間。因爲傳統上各機關要做電子公文交換時，必須要花費大量時間、成本及人力，相當浪費政府資源，自從網際網路的蓬勃發展後，更是希望將這些繁雜的電子公文交換應用到目前的網際網路上，藉以減少不必要的時間、成本及人力。然而，在開放的網路上進行電子公文交換時，電子檔案的資訊安全問題將是一大隱憂。以下歸納出幾個電子檔案系統所可能面臨的安全威脅：

一、訊息內容被竊知。

二、訊息內容被僞造。

三、訊息內容被竄改。

四、智慧財產權被侵占。

五、駭客的侵入。

六、發送者否認傳送或接收者否認接收。

七、被人冒名發文。

爲了能夠抵擋以上安全威脅，一個安全的電子檔案認證系統必須包含下列三大安全架構 ：

一、電子檔案的安全儲存及傳輸機制

電子檔案可透過網路來進行安全的傳遞，並以數位的方式儲存，因此，如何確保機密檔案的私密性，是檔案安全儲存上的一項重要議題。另外，電子檔案在網路上安全傳輸，需要加解密機制，安全的網路傳輸協定也是必

須考量，目前主要網際網路之安全網路傳輸協定有 SSL 及 S-HTTP 兩種。

二、 檔案來源的合法性認證

電子檔案的儲存雖然便利，但隨之衍生的安全問題卻不容我們忽視，試想當利用網路調閱檔案資料時，如何確信此檔案的確爲該機關所核發之檔案，而非有心人刻意僞造。因此，研究如何確認電子化檔案來源的合法性，亦是電子檔案認證研究所著重的重點之一。

三、 檔案內容的完整性認證

電子檔案內容完整性之認證，其主要目的爲確保檔案內容不會經有意或無意的修改或破壞，這類型的破壞包含有資料的修改、資料的加入、資料的修改等，造成資訊原意被扭曲、誤解，以達到特定的目的。因此，確保檔案資訊內容的完整性格外重要。

藉由考量以上的電子檔案潛在的安全威脅，系統管理者必須評估系統面臨這些安全威脅時所帶來的風險，並在三大安全架構下，進而了解電子檔案系統所需的安全需求，選擇最適當的安全技術。因此，若想透過網際網路作安全的電子檔案交換，設計出一套安全、有效率的電子檔案交換機制是刻不容緩。

爲了保護電子檔案在開放的網際網路上安全的傳遞，有幾項基本安全需求是必須達到的：

一、來源鑑別

來源鑑別主要目的是要驗證發文單位的合法性，因爲在公開的網路上傳遞電子檔案，可能會被非法人員假借發文單位僞造電子檔案，所以爲了防止電子檔案被不法人員僞造，進而確認電子檔案的來源合法性是很重要的一項安全需求。

二、機密性

爲了確保電子檔案內容在公開的網路傳送，不被非法人員竊取檔案內容，所以使用加密技術來保護電子檔案的機密性，防止不法人員得知電子檔案內容，加密過後的電子檔案，即使被攔截，也是亂七八糟的密文，非法人員無法從中得知正確的明文。

三、存取控制

除了保護電子檔案的機密性外，也要付予存取控制的權限，也就是只有合法的使用者才能存取電子檔案，從加密過後電子檔案，還原出原來的電子檔案，進而存取。

四、完整性

電子檔案在公開的網路上傳遞時，會遭到不法人員蓄意的竄改或變造電子檔案，致使電子檔案與原來的內容不符，以達到特定的目的。因此，爲了保護電子檔案不被破壞，確保電子檔案的完整性就顯得格外的重要。

五、不可否認性

電子檔案發送者或是接收者不能否認傳送或接收資料，對其來源做一證明以達權責歸屬與不可否認性。

參、電子檔案之安全技術

在充分了解電子檔案安全的重要性後，我們必須考慮有什麼安全技術可以抵擋整個電子檔案的安全威脅，以確保電子檔案能在開放的網際網路上安全的傳遞。本節中，我們將介紹一些安全技術，以防止電子檔案在網際網路上傳遞時，被不法人士更改，而這些技術可以達到上節中之安全需求。一般而言，檔案儲存格式依其類型可概分爲以下六大類型：

一、文字檔，其檔案格式有 XML、DOC、PDF 等。

二、圖片檔，其檔案格式有 JPEG、BMP、GIF 等。

三、聲音檔，其檔案格式有 MP3、WAV 等。

四、視訊檔，其檔案格式有 MP2、AVI 等。

五、文字影像檔，其檔案格式有 JPEG、TIFF 等。

六、工程圖檔，其檔案格式有 IGES、DXF、STEP 等。

有了這些標準的檔案格式，資訊得以在不同電腦系統間流通，達到資訊共享的目的。但針對不同的檔案儲存格式來進行加解密、數位簽章或數位浮水印等安全機制，其技術上卻有些許的差異。一般而言，電子檔案不論其儲存格式爲何，

對電腦來說都只是一連串 0 與 1 的位元而已，因此一般的加解密或電子簽章技術均可應用於這些不同的檔案格式。但由於圖片檔、聲音檔或視訊檔，其檔案資料量一般都比文字檔要大許多。以一張 1024 × 1024 像素(Pixels)的彩色圖片來說，其檔案大小約爲 3MB 左右，直接利用 DES 或 RSA 密碼技術來做加解密及數位簽章是非常沒有效率的。不僅如此，檔案的資料量越大在網路上傳輸所需的時間也越多。因此，在人類視覺、聽覺難以察覺的前提下，若能允許圖片、聲音、視訊等檔案做某些程度的失真，則通常可以大幅地降低檔案的資料量，這種技術稱之爲壓縮。而 JPEG、GIF、TIFF、MP3、MP2 等檔案格式都是常見的檔案壓縮格式，以 JPEG 格式爲例，壓縮率最高可達到十六分之一，也就是壓縮後的檔案大小爲原始檔案的十六分之一，可大幅地縮小檔案的資料量。因此，在對圖片、聲音、視訊等檔案作加解密或數位簽章前，通常我們會先對其做壓縮。

除了加解密及數位簽章等安全機制外，針對影像檔案因其可容許些許的失真，因此我們還可以加入數位浮水印來保障創作者的智慧財產權。另外數位簽章只能提供驗證者來確認圖形內容是否有被經過竄改，卻無法偵測出竄改的部位，因此圖形竄改偵測技術正可以彌補數位簽章這一方面的不足。

以下我們將詳細地介紹檔案儲存格式的加解密技術、數位簽章技術、圖形檔案的竄改偵測技術及數位浮水印技術。

一、加解密技術

不論何種檔案格式，在電腦運算上其實都是一連串 0 與 1 的位元，因此其加解密機制都可使用 RSA 或 DES 等密碼系統，但 RSA 密碼系統爲一種公開金鑰的密碼系統，使用者有一把公開金鑰及一把私密金鑰，配合憑證管理中心可有效地解決金鑰管理的問題，但在加解密的過程中，RSA 密碼系統需要做模指數運算，這種運算需要大量的運算時間，因此執行效率較差。相對的，DES 密碼系統爲一種對稱式的密碼系統，加密者與解密者需握有相同的一把秘密金鑰，雖然有秘密金鑰管理及協議上的困難，但其運算速度卻比 RSA 快了近 1000 倍。

因此，利用 RSA 密碼系統來協議一把 DES 密碼系統所需的秘密金鑰，再利用 DES 來對訊息做加密，是一種有效率且安全的方式。目前政府正積極推動公開金鑰基礎建設，透過政府憑證管理中心，使用者可申請一組經過合法認證的 RSA 公開金鑰，當一人員或機關透過網路要調閱機密資料時（包括各種電子檔案格式的資料），在網路的傳送過程中必須對這些電子檔案進行加密。其加密過程描述如下：

(1) 檔案主機伺服器隨機選擇一把長度爲 168 bits 的 Triple-DES 秘密金鑰。

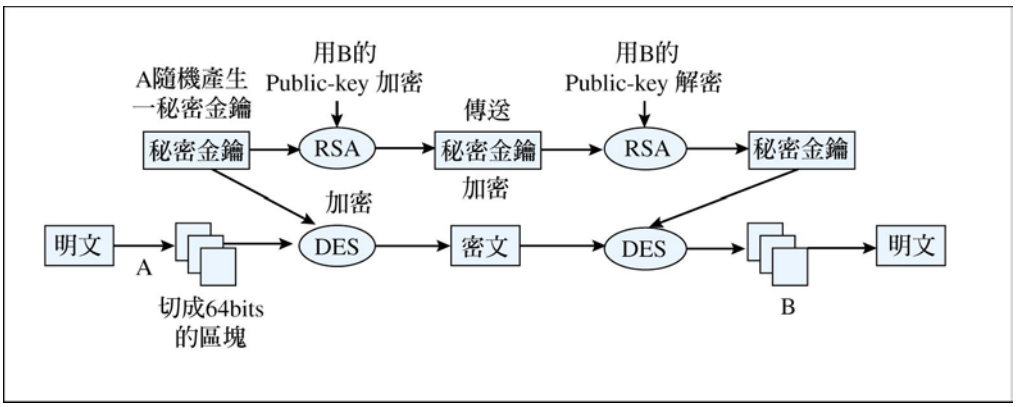
(2) 透過合法憑證管理中心所核發的電子憑證來驗證此申請者的公開金鑰是否正確。

(3) 若正確，則利用 RSA 密碼機制以申請者的公開金鑰來對 Triple-DES 的秘密金鑰進行加密，加密後將此密文送給申請者。

(4) 申請者收到密文後，可利用其私密金鑰來解密，解密後所得到的明文即爲 Triple-DES 密碼機制所需的一把 168 bits 的秘密金鑰。

(5) Triple-DES 的加密機制中所使用的金鑰長度爲 168 bits，將 64 bits 的明文轉換爲 64 bits 的密文。因此若所要傳送的機密資料若其長度大於 64 bits，必須以 64 bits 爲單位分成數個區段，分別加密後再依序傳送給申請者。

(6) 申請者收到後，用相同一把秘密金鑰對各區段的密文進行解密，解密後再將之結合在一起，便可得知此訊息內容。



圖一 加解密機制

圖一爲此加解密過程的描述。因爲 Triple-DES 所用的秘密金鑰爲 168 bits，故只需用 RSA 做一次加解密即可，而所要傳送的訊息其長度通常較長，以一 256 KB 的檔案爲例，就必須被切成 2^{15} 個 64 bits 的區段，再用 Triple-DES 來對個區段做加解密。因此，檔案主機伺服器僅需要 1 個 RSA 的加密運算及 2^{15} 個 Triple-DES 的加密運算；而申請者方面同樣需要 1 個 RSA 的解密運算及 2^{15} 個 Triple-DES 的解密運算。若使用硬體來做 RSA 及 Triple-DES 的運算，RSA 的運算速度較 Triple-DES 慢了近 1000 倍，若使用軟體來做 RSA 及 Triple-DES 的運算，RSA 亦較 Triple-DES 慢了近 100 倍，故用此方式來做加密要比全部使用 RSA 來做加密要有效率的多。

除此之外，檔案的大小亦直接影響加解密所需的時間，檔案越大所切割的區

段亦越多，也就需要較多的 Triple-DES 運算，所耗費的時間也就越多。例如視訊檔或聲音檔其檔案資料量動輒數百萬 bits 其加解密所需的時間也就越多。

二、數位簽章技術

與加解密技術相似，RSA 數位簽章機制亦可適用於各種電子檔案格式，但爲增進簽章及驗證的效率，我們可以利用單向雜湊函數(one-way hash function)的技術，在做簽章之前先對訊息做單向雜湊函數的運算後，得到長度較短的訊息摘要(message digest)後，再對此訊息摘要做簽章。以 SHA-1 的單向雜湊函數爲例，輸入至多 2^{64}-1 位元長度的訊息其輸出爲 160 bits 的訊息摘要，故可大量的縮短訊息的長度。以下是我們建議採用的簽章機制：

（一） 簽章者將所要簽署的電子文件先經過 SHA-1 的算後得到一訊息摘要，若訊息長度大於 2^{64} bits 則需切割成數個 2^{64} bits 的區段，再分別來做 SHA-1 的運算。

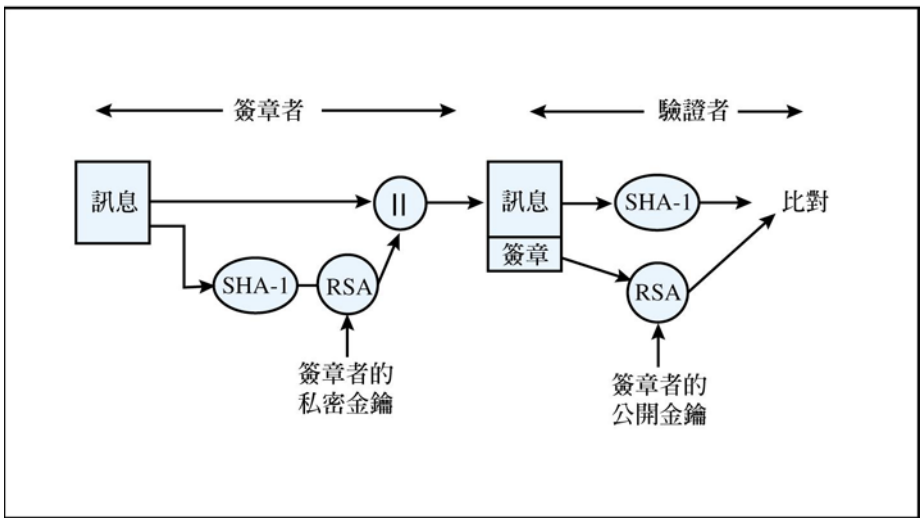
（二） 簽章者用其經政府憑證管理中心所簽發的合法私密金鑰來對此訊息摘要做 RSA 簽章，然後連同訊息、簽章及公開金鑰憑證一同送給接收端。

（三） 接收端收到後先驗證簽章者的公開金鑰是否正確，若正確則用此公開金鑰將訊息的數位簽章還原成訊息摘要。

（四） 接收端再將所接收到的訊息明文同樣透過 SHA-1 單向雜湊函數運算過得到一訊息摘要。

（五） 比對還原的訊息摘要與所計算的訊息摘要是否相同，若相同，則通過驗證。反之則失敗。

圖二爲數位簽章的運作過程。



圖二 電子檔案的數位簽章機制

因用 SHA-1 的單向雜湊函數，能將 2^{64}-1 位元長度的訊息轉爲 160 bits 的訊息摘要，大量的縮短訊息長度，並且 SHA-1 的運算速度極快比 RSA 運算要快上 10000 倍。此外，若採用與 GCA 相同的 RSA 密碼機制，其金鑰長度爲 1024 bits，最多一次能對 1024 bits 的明文做數位簽章，因此若以一 1MB 大小的電子檔案，若直接對其做 RSA 數位簽章，大約要做 1000 次的 RSA 簽章運算，但若先經 SHA-1 運算，因 1MB < 2^{64} bits，故簽章者只需做一次 SHA-1 運算便可得一 160 bits 的訊息摘要，因此再經一次 RSA 簽章運算便可得到此訊息的數位簽章，而驗證者亦只需做一次 SHA-1 運算及一次 RSA 驗證運算即可。由此可看出此方法是較有效率的方式。

三、電子影像檔案的竄改偵測技術

由於數位簽章只能驗證檔案內容是否招到竄改，但並不能找出被竄改的位置，在許多情況下這項技術是非常重要的，例如一張交通違規的照片，我們如何能確定照片中的違規車輛的車牌號碼沒有經過竄改，電子影像的竄改偵測技術恰可滿足這項需求。在電子影像的檔案中，在人類視覺難以察覺的情況下是可以容許些許的失真的。例如，一張灰階的電子圖片，每一個像素值都以 8 bits (0-255) 的資料量來表示其黑白濃淡的差異，其中每個像素值的前 5 個 bits 稱爲 MST (Most Significant Bits)，後 3 個 bits 稱爲 LST (Least Significant Bits)，因爲 MST 已大致決定了此像素的像素值，LSB 改變最多像素值也只差 7 而已，對整個影像改變不大，人類用肉眼很難察覺出來。因此我們可利用電子影像的此一特性來做影像的竄改

偵測。然而一般的文字檔案，或工程圖檔並不適用此項技術。因爲文字檔案一經變動內容將是完全不同的面貌，而工程圖檔需要相當的精細，不容許任何的失真。

在影像偵測技術方面我們建議採用 Straightforward 的方法，它是一種應用 RSA 數位簽章來做影像竄改偵測的技術，不但具有 RSA 數位簽章的功能同時還可以偵測出圖形被竄改的所在位置，底下我們來說明此技術的作法：

（一）圖形影像中每 342 個像素(pixels)分爲一個區塊(block)。

（二）然後將區塊中所有像素值的 MSB 拿出來　做 SHA-1 的雜湊函數運算後得一 160 bits 的訊息摘要。

（三）再將此訊息摘要用簽章者的私密金鑰做 RSA 的數位簽章，此 RSA 密碼機制與 GCA 所簽發的公開金鑰相同爲 1024 bits，因此簽章後會得一 1024 bits 的數位簽章。

（四）再將此數位簽章分散藏入每個像素的 LSB 中，因每個區塊中恰好有 342 個像素，每個像素的 LSB 有 3 個 bits 故可剛好放的下此 1024 bits 的數位簽章，最後將藏入數位簽章的影像傳送給接收者。

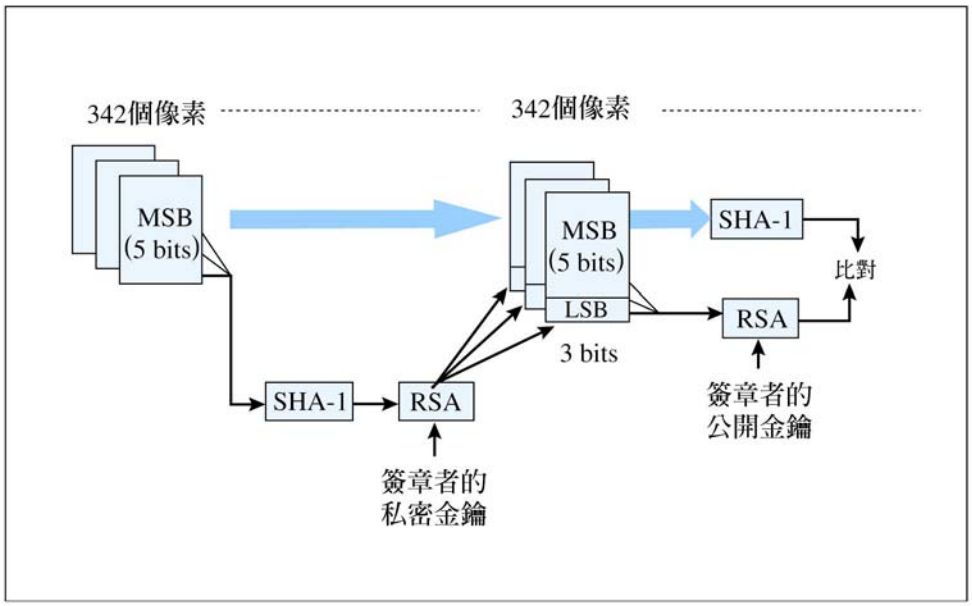
（五）接收者收到後可驗證此圖形是否有遭到竄改，首先將圖形影像每 342 個像素分爲一個區塊，然後將每個區塊中所有像素的 LSB 取出，去掉最後兩個 bits 後便得到此區塊的數位簽章(1024 bits)。

（六）取出區塊中所有像素的 MSB，將之組合後經過 SHA-1 運算，得一訊息摘要。

（七）驗證簽章者的公開金鑰是否正確，然後用此公開金鑰去運算得一訊息摘要。

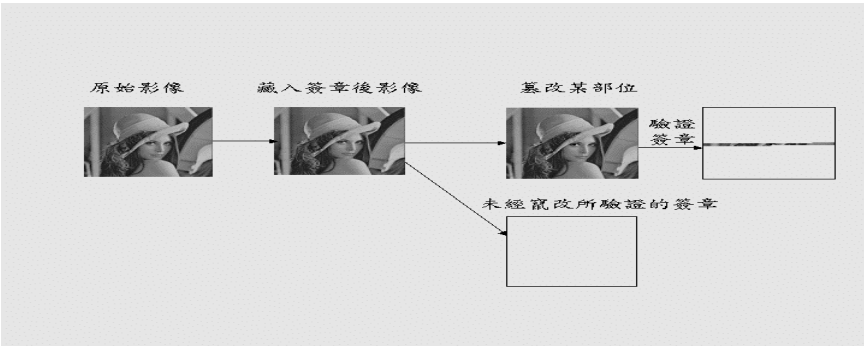
（八）最後比對兩訊息摘要是否相同，若相同則此區塊爲正確，沒有經過竄改；若比對不相同，則我們可以得知此區塊被竄改過。

圖三爲此方法的運作流程，圖四爲最後的實驗結果。



圖三 影像竄改偵測機制

在這個方法中，因數位簽章已藏入影像像素的 LSB 中，故所傳送的影像資料量與原始影像大小相同。但相較於一般的簽章方法，其需要做較多次的 RSA 簽章及 SHA-1 的運算，其次數視影像的大小而定。



圖四 實驗結果

四、影像的數位浮水印技術

在電子化的環境中，資訊可以透過網路廣泛的流通，因此對於著作財產權的保護就顯得相當重要，而數位浮水印技術便是保障著作財產權的一個有效方法。數位浮水印技術是在不嚴重影響媒體頻值的前提下，將代表創作者的圖騰藏入所創作的作品中，並且在藏入演算法爲公開的前提下，仍能抵抗竊取者的攻擊。目

前的數位浮水印技術被廣泛地應用於數位影像中，在此我們採用失真補償法的數位浮水印技術。試想，若我們將浮水印圖騰藏入像素值的 LSB 中，雖然不致大幅影響影像品質，但竊取者只要將所有像素的 LSB 毀損即可破壞數位浮水印，針對此一缺點，此方法的設計精神是將浮水印圖騰亦藏入像素值的 MSB 中，卻又不對影像品質造成很大的影響。假設創作影像爲一灰階影像，而所要藏入的圖騰影像爲一較小的黑白影像，其作法如下：

一、 創作者先選定一具安全性的亂數產生器，並選擇一亂數作爲亂數產生器的種子(seed)，將此種子帶入亂數產生器(pseudo random number generator)運算會得到一連串的亂數值（x, y, z），其中（x, y）代表所要藏入的像素座標位置，z 是代表所要藏入在像素中的位置（由左至右爲 0、1、…、7），此外所選擇的種子必須保持妥善保存，不可洩漏。此外，若所計算出來的藏入座標點有重複的話，必須捨棄不用。

二、浮水印影像爲一較小的影像，且爲一黑白兩色的二元影像，故每個像素只需 1 bits 來表示即可。因此將浮水印影像的第一個像素藏到（x, y）座標像素的第 z 個位置中。

三、接下來要做失真補償，將此像數的 z-1 位置的 bit 改爲 1，z+1 至最後位置的 bit 都改爲 0，然後計算此像素值 p1 並和將此像數 z+1 至最後位置的 bit 都改爲 1 所得到的像數值 p2 做比較，若 p 與 p1 的誤差較 p 與 p2 的誤差要小，p 則將替換爲 p1，否則將 p 替換爲 p2，其中 p 爲原始的像素值。

四、重複步驟 2、3，直至藏完所有浮水印影像爲止。

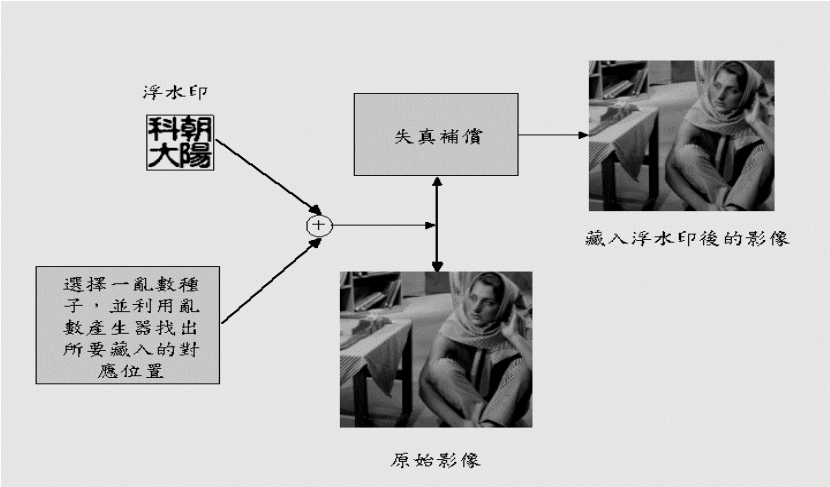
五、當要驗證此作品確爲其所創作，只需提出此亂數產生種子，透過亂數產生器產生一連串的亂數值（x, y, z）。

六、到所對應的像素和位元中取出浮水印的像素值，重組後若可回復一代表創作者的浮水印，則可證明此作品爲此創作者所創作。

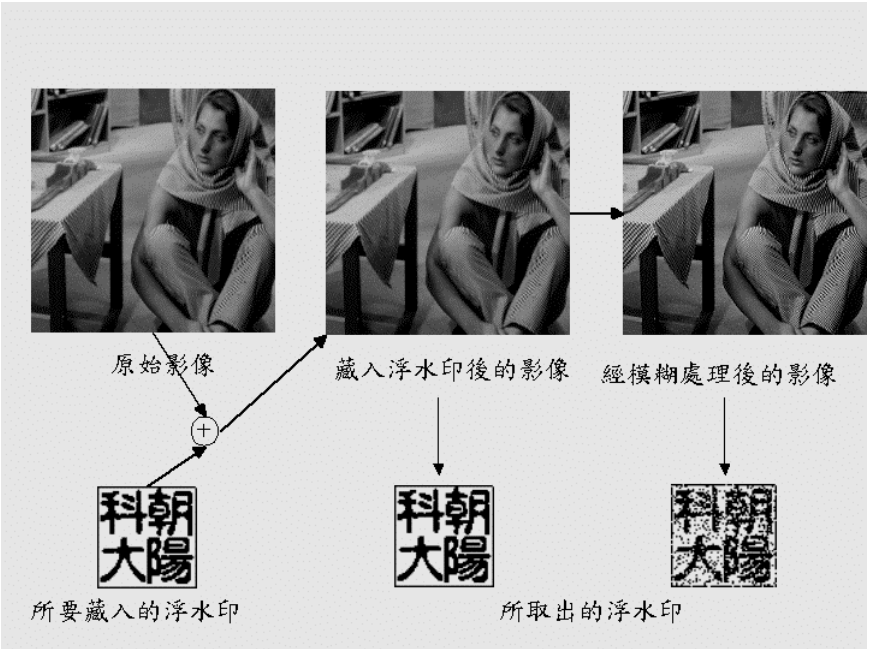
以下我們舉一例子來具體說明以上的運作流程。首先，若此亂數產生器所產生的第一個亂數爲(24，71，1)，假設在影像中座標（4，7）的原始像素值爲 p=170（10101010），而浮水印第一個像素值爲 1，於是將原始像素值位置爲 1 的 bit 由 0 改爲 1，而藏入後的像素值爲 234 (11101010)。接著計算 p1＝192（11000000），p2

＝127（01111111），我們可以發現 p1 與 p 的誤差較 p2 與 p 的誤差小，我們變將位置（24、71）的像素值改爲 p1（192）。

圖五爲此方法的運作流程，圖六爲實驗結果，我們可以發現藏入浮水印後的影像品質與原始影像相去不遠，肉眼很難辨識出來。此外，若此圖片經過模糊化的處理後，所取出的浮水印雖然會有雜訊，但我們依然可以清楚的辨識出其內容，此一特性我們便稱之爲強韌性(robustness)。另外在運算的成本方面，此浮水印技術因沒有使用到任何複雜的計算，故其執行速度相當快，所花費的成本也相對較低。



圖五 失真補償法之浮水印技術



圖六 實驗結果

貳、 結論

隨著網際網路的蓬勃發展及廣泛應用，電子檔案的安全性也隨之重要，人們將可透過網際網路傳送交換電子檔案，但隨之而來的安全性問題，是不可忽視的，在本文中，我們已經說明在網際網路上，傳送電子檔案時，可能所遭遇到的攻擊，並且提出一些安全技術，以抵擋在網際網路上傳送電子檔案時，所遭遇到安全威脅。除此之外，針對不同的電子檔案格式，我們也已提出其所適用的安全機制，除了一般的加解密及數位簽章等安全機制外，針對影像檔案因其可容許些許的失真，因此我們還可以加入數位浮水印來保障創作者的智慧財產權。另外數位簽章只能提供驗證者來確認圖形內容是否有被經過竄改，卻無法偵測出竄改的部位，因此圖形竄改偵測技術正可以彌補數位簽章這一方面的不足。藉著以上我們所提之電子檔案安全技術，希望可以提供一個實用、安全、及有效率的電子檔案安全之環境，透過此安全環境，將電子檔案透過網際網路來進行安全的傳遞與交換。

【原刊載於檔案管理局出版之檔案季刊（九十一年六月）第一卷第二期】

參考資料：

[1] 張真誠。電腦密碼學與資訊安全。台北：松崗，民國 78 年。

[2] 張真誠、黃國峰、陳同孝。電子影像技術。台北：松崗，民國 89 年。

[3] 賴溪松、韓亮、張真誠。近代密碼學及其應用。台北：松崗，民國 84 年。

[4] 國家檔案局籌備處。全國檔案資訊系統計畫構想。民國 89 年。

[5] 國家檔案局籌備處。檔案電子儲存管理辦法之研究。民國 89 年。

[6] 國家檔案局籌備處。檔案微縮等方法儲存紀綠及其複製品確認作業準則研究。民國 89 年。

[7] 國家檔案局籌備處。電子文件檔案管理與應用之研究。民國 90 年。

[8] 工業技術研究院。政府機關電子公文交換作業安全協定。民國 86 年。

[9] Willian, S.. Cryptography and network security (Second Edition). 1999, Prentice Hall International, Inc.