淺談影像鑑別技術—以數位浮水印為例

作者/周兆龍 上尉・婁德權 上校

提要

一、資料完整性(Integrity)是資訊安全防護的主要核心，而鑑別(Authentication)技術是確保資料完整性的有效手段。

二、鑑別技術可以廣泛應用在文字、聲音、影像、視訊等各種型式的數位多媒體（Multimedia）資料，不同資料型態對於鑑別技術的需求亦不盡相同。以數位影像為例，因為影像是透過肉眼來檢視，因此不容易辨別影像內容的細微差異，這些差異可能只是一般影像處理的效果，也可能是遭有心人士的蓄意竄改或破壞的結果。

三、數位浮水印（Digital Watermarking）是應用於數位影像鑑別的有效方法。數位影像可以將代表鑑別資訊的數位浮水印隱藏在影像內容之中，降低被人察覺的機會，也可以結合數位簽章（Digital Signature），增加鑑別的正確性；另外數位浮水印也可以分散存在於影像平面中，藉而能有效追蹤影像資料內容的差異。

前言

自從網際網路逐漸普及之後，各種新興的電子商務應用開始蓬勃發展，隨之而來的網路詐騙案件層出不窮。以資訊安全的角度來看，網路上的資料傳輸都應具備有良好的鑑別（Authentication）機制，以確保資料的真實性及完整性。

現今各種常見的數位多媒體型態（例如文字、聲音、影像、視訊等）中，數位影像的應用範圍極為廣泛，例如提供個人或家庭的網頁設計與數位相片編輯等日常應用，或者提供醫學診斷、太空衛星遙測、工業生產品質檢測、犯罪偵察、建築裝潢輔助設計...等等的各種工商業應用。再加上各種數位相機、照相手機、掃瞄機等資訊設備不斷地推陳出新，數位影像的應用愈趨普及化，相對數位影像的安全性需求也隨之增加。

本文以數位影像為例，探討如何有效將鑑別技術應用在數位影像資料型態。文中除了介紹傳統資料鑑別的原理，也將介紹近年來被廣泛研究的數位浮水印技術，並深入探討數位影像的各種特性及相關數位浮水印方法，以供讀者研究參考。

壹、背景介紹

曾有一部改編自真實事件的電影，描述美軍一艘核子潛艦在例行的任務中，收

到指揮部要求提高戰備的緊急命令，但潛艦上的通信設備卻在接收過程中故障，艦長依據所收到的片段命令準備發射核子飛彈反擊，而潛艦內的軍官卻堅持一定要收到完整的命令才能行動，經過幾番對抗之後，才終於解讀出完整的命令，而避免了可能發生的災難。這部電影表達出資料完整性與真實性的重要，片段或不正確的訊息很可能會造成不可預期的後果。

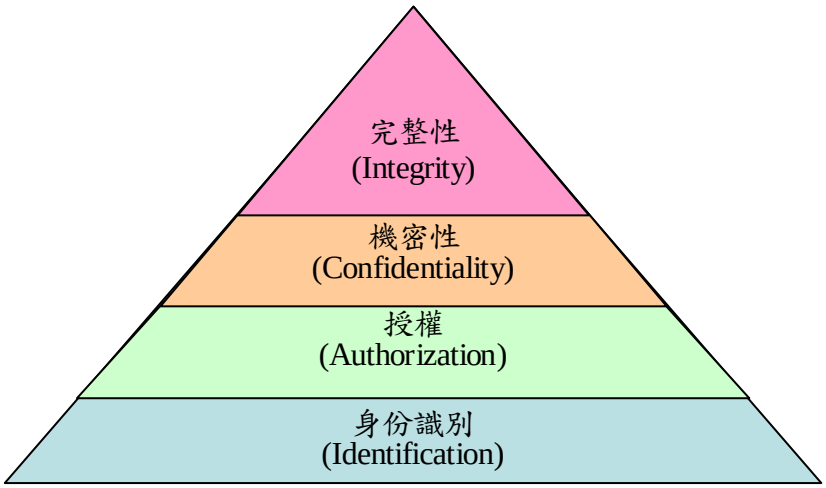
日常生活中我們也時常會遇到類似的情況，例如當我們購買商品時，會檢查檢驗合格商標或認證標籤，以避免買到仿冒品；在使用鈔票時，會留意鈔票上是否有防偽線或浮水印，以避免收到偽鈔；甚至當我們收到各種未知的電話或手機簡訊時，都必須再詳加查證對方的實際身份及其內容的真實性。以上這些日常常見的種種情況，簡單來說都是在分辨事物的真偽。

在電腦世界中同樣必須面對相同的安全問題，經過電腦數位化後的資料因為具有容易複製、修改、儲存與傳送的特性，使用十分方便，卻也容易遭受竄改或偽冒等惡意攻擊。因此為了能有效確保資料的完整性與真實性，電腦資訊系統必須具備足夠安全的防護機制。

一般常見的電腦資訊系統安全防護機制可以概分為下列幾種層次[1]，如圖一所示：

一、身份識別（Identification）

以電腦資訊系統而言，身份識別通常是進入系統的第一個關卡，主要功能是辨識進入系統的使用者是否合法。所謂身份識別係指確認使用者的身份在系統中是否合法，這裡所指的使用者可能不只是個人(human)，也可能代表某個系統程式（process）。



圖一 資訊系統安全架構示意圖

常見的身份識別作法是利用密碼（password）、憑證（certificate）或智慧卡（Smart

Card），在進入系統時提供相關的資訊供系統驗證。另外近年來利用人類生物特徵（biometrics）的身份識別方法也漸漸成為趨勢，例如利用人類的眼角膜、聲紋或指紋等等生物特徵，這種方式提供了更高的安全性，相對也需要較高的成本。

二、授權（Authorization）

所謂授權係指使用者通過身份識別後，即可進入系統存取資源，惟所存取的系統資源必須要先經過授權，而且依據使用者不同等級應區分不同的權限。例如 UNIX 系統，將所有檔案目錄依擁有者（owner）、群組（group）、其他（others）分別設定讀取（read）、寫入（write）及執行（execute）的權限。這些授權規則在使用者帳號開放時一併訂定，以確保重要的系統檔案不被他人任意的讀取或執行。

三、機密性（Confidentiality）

所謂機密性係指確保資訊不被未授權者讀取，例如軍隊中常使用非機密、機密、極機密、絕對機密等區分資料的安全層級，未經授權者即無法讀取機密訊息。

機密性常見的作法是利用加密技術（encryption），包括對稱式（symmetric）與非對稱式（asymmetric）加密技術。資料經過加密處理之後，即由明文（plaintext）轉變成受保護形式的密文（ciphertext），即使資料不慎洩漏，也能確保機密資料不被輕易的破解。

四、完整性(Integrity)

所謂完整性係指資料在傳輸、儲存或使用過程中沒有任何一個位元（bit）遭受改變。影響資料完整性的因素包括網路封包遺失、雜訊干擾、或遭有心人士蓄意竄改、破壞...等等。資料完整性直接影響的就是資料內容的可信度，因此資料一旦受到完整性破壞，即使資料經過嚴密的加密防護也不足信賴，因此完整性是資料安全防護的主要核心。

貳、傳統鑑別技術

一、資料傳輸常見攻擊類型

網路是開放式的環境，資料在網路上傳輸有可能遭受各種類型的攻擊。常見的攻擊可概分為兩大類：主動式攻擊（Active Attacks）與被動式攻擊（Passive Attacks）。主動式攻擊通常以直接破壞使用者的資料、系統功能或網路連線為主，例如電腦病毒、偽冒資料、竄改資料、漏洞掃瞄、拒絕系統服務（Denial of Service, DoS）等等攻擊模式；而被動式攻擊通常不會直接破壞使用者的資料或系統功能，而是在使用者未察覺的情形下，將資料另行複製保存，例如竊聽程式、網路流量監控等等。

以資料傳輸（Data Communication）的角度來看，資料透由網路由傳送端傳送到接收端的傳輸過程中可能面臨的下列幾種危險（如圖二所示）[2]：

(一)中斷（Interruption）

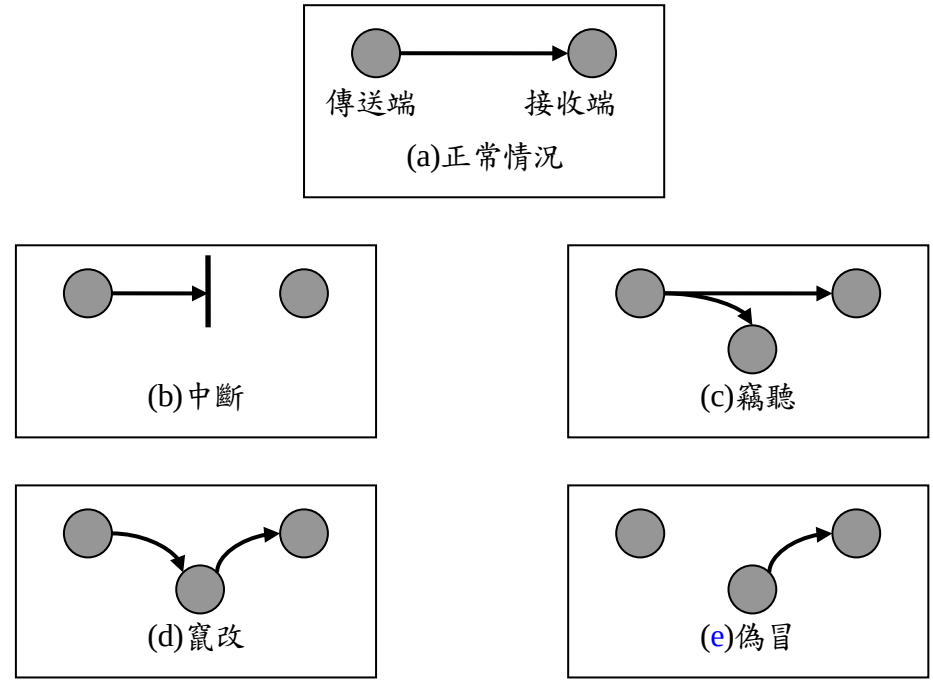
係指使接收端無法順利接收資料，例如實體中斷網路連線、拒絕系統服務（DoS）攻擊等方式，使接收端無法有效收取訊息，如圖二(b)所示。

(二)竊聽（Interception）

係指在傳送端與接收端雙方未知的情況下，第三者同步複製傳輸的資料，進行資料蒐集或流量分析，如圖二(c)所示。

(三)竄改（Modification）

係指第三者截取傳輸資料，並修改原始的資料內容後，才將已修改之資料傳送給接收端，使得接收者所接收的資料非原始的正確資料，如圖二(d)所示。



圖二 資料傳輸攻擊模式示意圖[2]

(四)偽冒（Fabrication）

係指第三者假冒傳送端的名義，偽造資料內容並逕行傳送給接收端，意圖欺騙接收端，如圖二(e)所示。

上述四種情況，前兩種傳輸資料本身並沒有被更動，而後兩種情況資料本身則分別遭到第三者修改及偽造。此時若使用鑑別技術，則不僅可以確認資料來源，亦可以確認資料的完整性，因此我們可以瞭解鑑別技術可以有效偵測出資料是否遭竄改與偽冒。

二、鑑別特性

鑑別的英文是”Authentication”，常見的中文翻譯為”認證”或”鑑別”，不同中文

翻譯所代表的意義可能有所差異，例如認證通常指對使用者身份的認證；而鑑別則廣泛的包含身份識別與資料完整性的範疇。

根據國際電訊聯盟（ITU-T）X.800 文件中的定義 [3]，鑑別區分為兩種層次，一種是傳輸端鑑別（Peer Entity Authentication），而另一種是資料來源鑑別（Data-Origin Authentication）。傳輸端鑑別主要是針對”人”，亦即確認傳輸者的身份是否如其所宣稱；而資料來源鑑別主要是針對傳輸的”資料”本身，亦即確認所接收的資料內容是否正確。

在運作方式方面，傳輸端鑑別通常傳送與接收兩端是處於即時（Real-time）驗證的狀態，例如打電話時，雙方必須同時在電話線上，利用彼此講話的聲音語調即可確認對方是誰，又例如登入電腦系統，輸入帳號密碼之後，系統立即會回應使用者是否登入成功；而資料來源鑑別則通常毋需處於即時狀態，例如寄送電子郵件，雙方不需要同時在線上也能收到對方的郵件。表一為傳輸端鑑別與資料來源鑑別的差異比較。

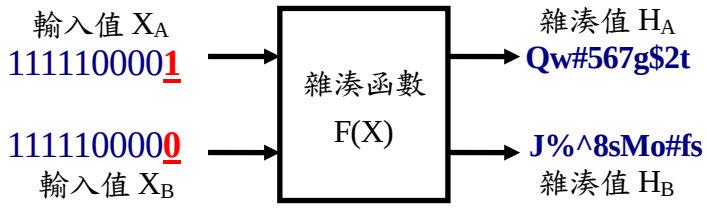
表一 傳輸端鑑別與資料來源鑑別的差異比較

區分	目標	驗證方式	主要功能	常見技術
傳輸端鑑別	人(entity)	即時 (real time)	身份識別 (identification)	密碼(password)、憑證(certificate)、 生物特徵(biometrics)
資料來源鑑別	資料 (data)	非即時	資料完整性驗證 (data integrity)	雜湊函數(hash function)、訊息鑑別碼 (MAC)、數位簽章(digital signature)

基本上傳輸端鑑別與資料來源鑑別在良好的電腦系統安全架構中是一體兩面，密不可分的。本文所提到鑑別技術，主要就資料來源鑑別作更進一步的研討。

三、雜湊函數（Hash Function）

雜湊函數（Hash Function）是一種多對一（Many-to-one）的函數，不同長度（Variable-length）的輸入經過雜湊函數的運算後會產生相同長度（Fixed-length）的輸出，稱作雜湊值（Hash-value）。雜湊函數的特性是計算快速，並且正向的計算很容易而反向的計算很困難，因此又常被稱為單向雜湊函數（One-Way Hash Function）。雜湊函數的另一項特性是輸入的資料只要有任何一個位元不同，經過雜湊函數運算後即會產生不同的雜湊值，如圖三所示。



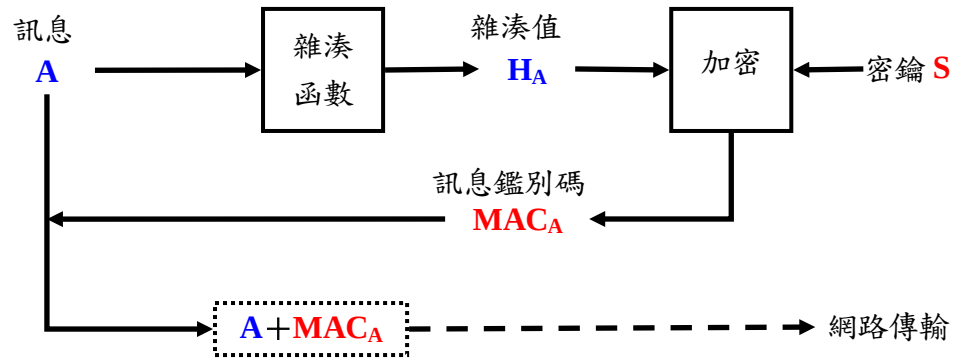
圖三 雜湊函數運算示意圖

只要資料位元經過新增（insertion）、刪除（deletion）或替換（substitution）等處理，所產生的雜湊值即會不同，因此只要利用比對雜湊值的方式，便可以用來驗證資料的完整性。

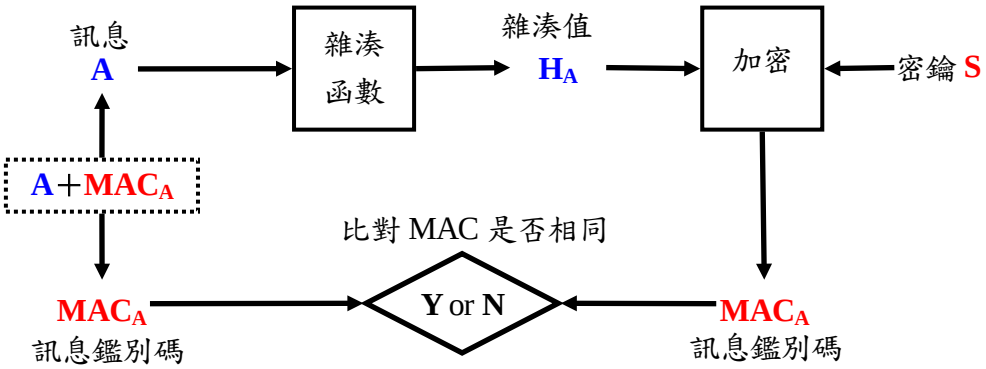
另一種常見的雜湊函數稱為單向暗門雜湊函數（Trapdoor One-Way Hash Function），單向暗門雜湊函數因為具有某種暗門，可以讓反向的計算變得很容易，因此常被應用在密碼加解密方面。密碼加解密的過程簡單來說就是將原始訊息（明文）透過演算法與金鑰（key）運算之後，輸出成為一串沒有意義的亂碼（密文），讓一般人很難從一堆亂碼中解讀原本的訊息，唯有掌握金鑰的人才能順利的解讀原始訊息。而單向暗門雜湊函數中的"暗門"即扮演了重要角色，成為金鑰提供的主要來源。

四、訊息鑑別碼（Message Authentication Code）

訊息鑑別碼(Message Authentication Code，MAC)簡單來說就是加了密鑰(Secret Key）的雜湊函數。其運作方式如圖四所示。



（a）加入訊息鑑別碼流程示意圖



（b）驗證訊息驗證碼流程示意圖

圖四 訊息鑑別碼運作流程示意圖

訊息經過雜湊函數計算產生雜湊值，接著雜湊值再利用密鑰進行加密運算後即

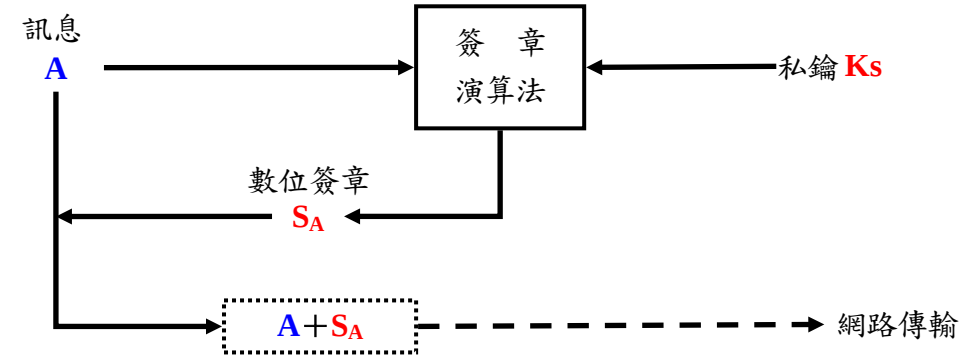
產生該訊息專屬之訊息鑑別碼。此訊息鑑別碼可以分開或直接附加在原訊息之中一起傳送，其流程如圖四(a)所示。

接收端在收到訊息及訊息鑑別碼之後，只需將原訊息利用相同之雜湊函數及密鑰運算出一個訊息鑑別碼，並與所收到的訊息鑑別碼作比對，訊息鑑別碼經過比對若相同則表示資料未經過修改；若不相同，則表示資料已遭到修改或破壞，其流程如圖四(b)所示。

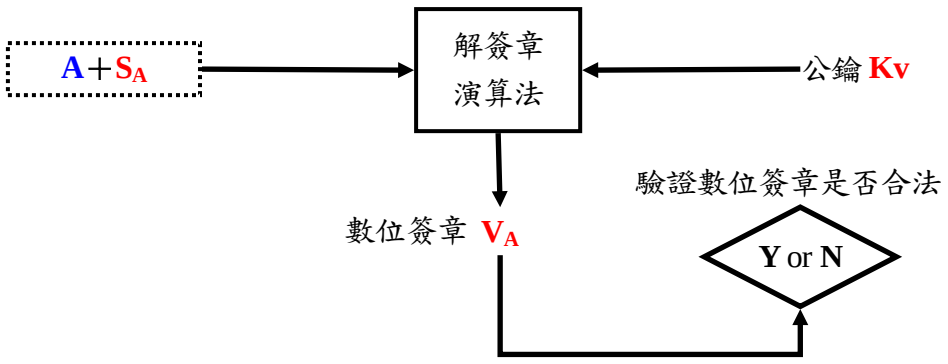
這種方式可以確保資料的完整性，有效判斷資料是否遭到竄改，但其缺點是無法提供不可否認性（Non-repudiation），由於傳送端與接收端均使用相同的密鑰，因此若有第三者事先取得同樣的密鑰，則仍可能發生偽冒的情形。

五、數位簽章（Digital Signature）

數位簽章可以解決訊息鑑別碼所無法具備的不可否認性。數位簽章改以公鑰（Public Key）與私鑰（Private Key）取代原本訊息鑑別碼所使用的密鑰。完整的數位簽章系統包含簽章加入及解簽章兩個部分：簽章加入係指傳送端將訊息與本身的私鑰進行簽章運算，運算所得之數位簽章與訊息一起傳送，其流程如圖五(a)所示。而解簽章係指當接收端收到包含數位簽章之訊息時，利用傳送端的公鑰進行解簽章運算，並驗證該數位簽章是否合法，其流程如圖五(b)所示。



（a）簽章加入流程示意圖



（b）解簽章流程示意圖

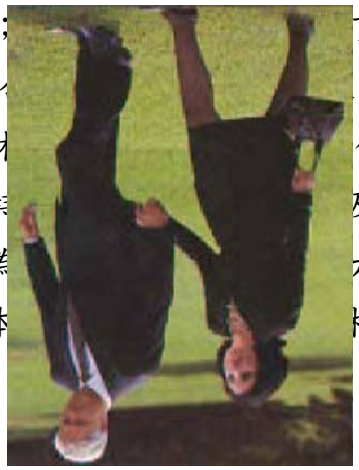
圖五 數位簽章流程示意圖

數位簽章由於使用非對稱式加、解密技術，除了確保資料完整性之外，還能確保資料來源的不可否認性（Non-repudiation），因此能有效的判斷竄改與偽冒攻擊。

參、影像鑑別

一、影像鑑別特性

無論是傳統的平面影像或數位影像（Digital Image），影像一直是傳達訊息非常直接又有效的方式。隨著資訊科技的發展，數位影像逐漸普遍於一般人的日常生活之中，應用範疇十分廣泛。數位影像依據不同的應用可以分成無失真型（loseless）及失真型（lossy）兩類。無失真型影像主要應用在需要高精密與高解析度的影像畫質，例如醫學影像、衛星照片與科學影像等；



了降低網路傳輸與儲存的成本，會在不破壞影像品質的

資料進行壓縮（compression）處理，例如網頁影像、數位

像等等。

數位影像因為具有一般數位資料共同的特

及修改，因此數位影像遭到竄改或偽冒的機率很高。以圖六為

六(b)同時比較，可以很明顯的看出與圖六(b)曾遭到竄改，原本

柯林頓夫人希拉蕊的頭部被置換成李文斯基。

(a)　　(b)

圖六 影像竄改範例一[4]

再看圖七例子，若同樣將圖七(a)與圖七(b)同時比較，應該可以明顯看出影像中汽車車牌的差異，但卻不容易靠肉眼直接分辨出兩張影像的真假[5]。

(a) (b)

圖七 影像竄改範例二[5]

由此可知，因為數位影像是以二維（2-dimension）形式展現，而經由人類肉眼感知，影像內容（content）是否完整是影像鑑別時的重點；其次則是考慮數位影像在實務應用上常需經過壓縮或格式轉換等一般影像處理，影像鑑別應要能辨識出合理範圍內的影像處理。

傳統鑑別方法可以有效確保資料完整性，但卻因為不允許影像資料遭受任何壓縮或正常處理，也無法進一步指出影像資料究竟何處遭到修改，因此傳統的鑑別方法無法滿足影像鑑別的需求。

一般數位影像鑑別具有下列幾項需求特性：

(一)能有效判斷出影像是否經過修改。

(二)能有效判斷出影像是正常使用或遭非法破壞。

(三)能有效將鑑別資訊整合於影像資料之中。

(四)能有效指出影像遭修改的位置。

影像鑑別必須包含傳統鑑別方法的基本功能，也就是只要資料有任何變動就能被偵測出來，以確保資料的完整性；若影像曾經過修改，還必須要能分辨出是合理的影像處理還是惡意的竄改；另外鑑別資訊最好能隱藏於影像資料中，不被人輕易察覺，以增加安全性；更進一步還必須能夠指出影像資料中被修改的部位，以符合實務上的需求。

二、影像鑑別應用

影像鑑別常見的應用範疇如下[6]：

(一)醫學影像

例如病人 X 光影像，可加入病患身份、就診日期等鑑別資料，用以保障病人隱

私權，並提供醫師追蹤病歷。另外藥品亦可以影像方式建檔，配合領藥病患、醫師授權等鑑別資料，建立合法用藥的安全性。

(二)犯罪調查

數位影像作為法庭案件佐證資料時，影像資料的正當性十分重要，加入具公正權威的鑑別資料，可以避免影像真實性的質疑，亦可建立公權力的威信。另外個人指紋特徵以數位影像建檔，可以用於案件調查時的重要證據。

(三)智慧財產權保障

網路傳播資料十分迅速，具智慧財產權的影像資料亦容易遭到非法複製、修改，加入所有權宣告的鑑別資料可以確保智慧財產權不輕易遭受損害。

(四)身份辨識

個人生物特徵（臉、指紋、眼球）均可以數位影像方式建立個人身份資料，應用於門禁安全管制。另外車輛牌照亦可以數位影像方式建檔，應用於停車場管理。

(五)軍事情報

重要軍事影像資料傳遞，例如衛星照片、地圖等，可以加入合法授權的認證，使接收方在確認資料來源同時也能確保資料的完整性，以確保軍事安全。

三、影像鑑別類型

數位影像鑑別技術依據嵌入方式的不同可以概分為標籤型技術（Label-based Techniques）與數位浮水印型技術（Watermarking-based Techniques）兩種主要類型[7,8]。標籤型技術指的就是數位簽章等傳統鑑別技術，是將鑑別資訊存於影像資料的檔頭或另存於其他檔案；而數位浮水印型技術則是直接將鑑別資訊存於影像資料之內。

標籤型技術的主要優點是不會變更影像資料內容，因此能嚴格確保影像的完整性與影像品質，並且可以儲存較高容量的鑑別資訊，其缺點是無法有效偵測出影像內容何處被改變，另外也無法滿足一般網路應用常見的影像壓縮等使用需求。而數位浮水印型技術可以用來克服標籤型技術的上述缺點。

數位浮水印型影像鑑別技術具有以下幾項優點：

(一)可指出影像遭修改的位置

數位浮水印可以對整張影像做處理，因此只要影像任何部位有變動都可以輕易的被紀錄下來。

(二)更為精良

數位浮水印是直接嵌入（embed）於影像之中，而不是另外增加檔案於檔頭或其他位置，因此不用擔心影像格式轉換或檔頭資訊被修改等問題。除非整個影像完全被破壞，否則浮水印一定存在。

(三)更有彈性

數位浮水印技術可以允許合理範圍內的一般訊號處理，因此適合於一般網路應用，此外數位浮水印技術同樣可以嚴格確保影像完整性，因此依據不同的應用需求，浮水印技術具有更佳的彈性。

(四)安全性高

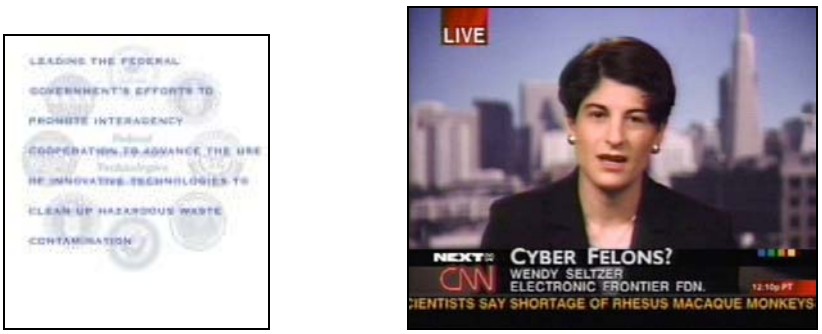
浮水印可以分散隱藏於影像之中，不容易被肉眼所發覺，因此有較佳的安全性。

數位浮水印的缺點是會對影像品質造成某種程度的破壞，因為一般數位浮水印技術會直接改變影像中的像素值（pixels），因此會造成影出現失真的情形。目前改善這種缺點的方法可以搭配轉換域（Transform Domain）方法，不直接處理影像像素值，而改以處理影像轉換後的係數（coefficients）；另外也可以搭配人眼視覺系統（Human Visual System, HVS）的特性，將浮水印嵌入在肉眼較不敏感的位置，如此即能保持影像較佳的視覺品質。

數位浮水印技術

一、數位浮水印

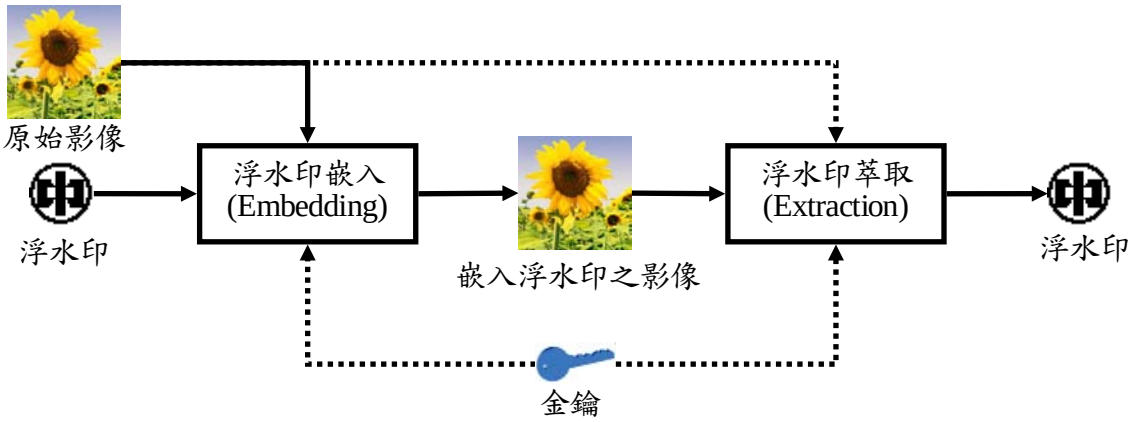
數位浮水印技術實際上是屬於資訊隱藏技術（Information Hiding Techniques）的一種[9]，其主要的概念就是將秘密訊息藏匿於某種不起眼的資料之中，可以進行秘密的通訊而不被外人發現。數位浮水印最早常被應用作所有權證明（Proof of Owner），例如在出版的文件紙張上浮刻著代表單位全銜的浮水印標記（如圖八(a)所示[10]），又或者如新聞電視台在播放的新聞畫面上加註公司商標logo（如圖八(b)所示[11]）…等等。而隨著多媒體數位資料的普及，為了避免資料的濫用問題，數位浮水印技術開始被廣泛應用在智慧財產權保障（Copyright Protection）。例如行政院國家科學委員會在民國91年發展的「數位典藏國家型科技計畫」中[12]，部分計畫內容即專門研究將數位浮水印技術應用於博物館文物數位化保障。



(a) (b)

圖八 浮水印範例[10,11]

簡單來說，數位浮水印就是利用某種演算法，將具有特殊意義的浮水印資料嵌入（embedding）於多媒體資料中，之後利用反向的演算法將浮水印資料萃取（extraction）回來。完整的數位浮水印系統，包括嵌入與萃取兩個階段（如圖九所示），嵌入的浮水印可以使用文字、數字或商標logo，並可以視情況加入金鑰，以增加系統安全性；在浮水印萃取階段，則參考原始影像或金鑰來萃取浮水印。



圖九 數位浮水印嵌入與萃取流程示意圖

一般數位浮水印依據不同的應用大致可以分成以下幾類，如表二所示[13]。

表二 數位浮水印分類表

分類方式	說明
依媒體種類區分	文字、影像、聲音、視訊
依視覺區分	可見型、不可見型
依強固性區分	脆弱型、半脆弱型、強固型
依嵌入方式區分	空間域、頻率域

數位浮水印依據肉眼可視程度可以分成可見型與不可見型兩大類，其中可見型浮水印因為會對影像造成明顯的破壞，同時也容易遭受攻擊，因此較不適合高安全性需求的應用。而不可見型浮水印可以維持較好的影像品質，也可以避免浮水印被直接破壞，因此較為大多數影像鑑別採用。

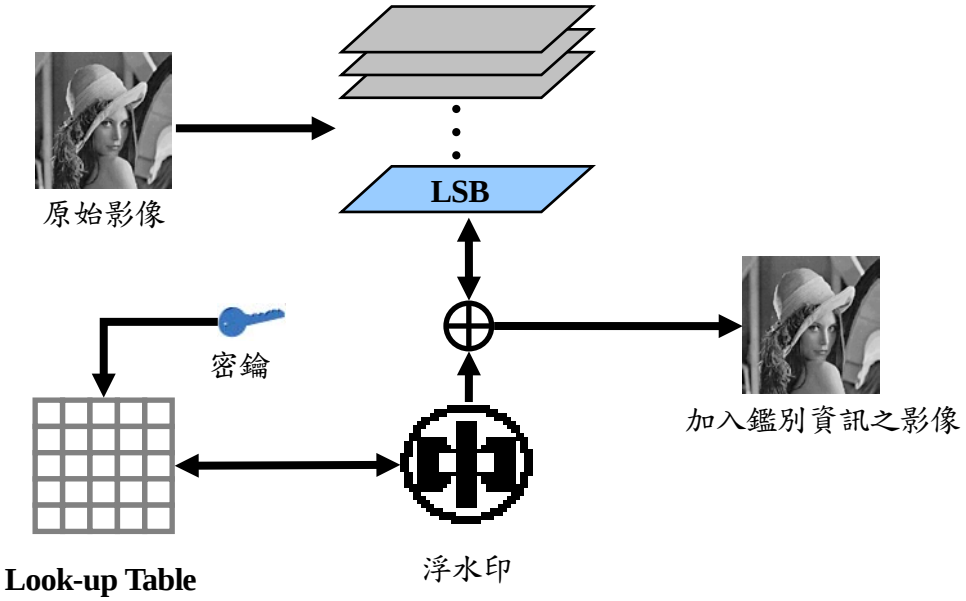
另外，依據浮水印的強固性又可將數位浮水印技術可以分成強固型（robust）、脆弱型（fragile）與半脆弱型（semi-fragile）三類。強固型浮水印是指對於一般影像處理的容忍程度很高，例如影像經過壓縮、放大、縮小、雜訊、格式轉換之後，浮水印資料還能有效的辨識，常被應用於智慧財產權保障；脆弱型浮水印是指影像資料只要有些微改變，浮水印資料便會被破壞；半脆弱型則是對於指可以辨識出影

像資料的變更是屬於正常處理或遭惡意的攻擊。其中影像鑑別常用的方法有脆弱型與半脆弱型兩類[14]，本文將進一步介紹這兩類的影像鑑別技術。

二、脆弱型數位浮水印方法

早期的數位影像鑑別方法主要是針對影像資料完整性作設計，因此所使用的演算法大多對影像的空間域（Spatial Domain）處理，亦即直接處理影像的像素。其中最常見的方法是利用最低位元（Least Significant Bit, LSB）的觀念，在影像每個像素的最後一個位元放入浮水印，因此只要影像有任何變動，便能馬上測試出來。

1997 年 Yeung 及 Mintzer 學者[15]，利用密鑰產生一個二元參照表（Binary Look-up Table），並選擇與原圖一樣大小的黑白商標作為浮水印，浮水印嵌入時是將每個像素值（0 或 1）分別去比對參照表的值，相同的則保留原圖的最低位元值，若相異則將其最低位元值改為與浮水印相同，其流程如圖十所示。驗證時，只要將依照原先的參照表順序，將影像每個像素的最低位元取出，便可以還原出商標的圖像，用以驗證影像資料的完整性，同時因為浮水印的大小與原圖相同，因此若影像有任何位置曾經變動，都能被偵測出來。



圖十 LSB影像鑑別系統示意圖

1998 年 Wong 學者[16]，同樣利用最低位元的觀念，先將原圖每個像素的最低位元設為”0”，原圖被細分成與浮水印大小相同的區塊（block），每個區塊分別使用 MD5 雜湊函數運算，再將與浮水印互斥運算（XOR operation）的結果以 RSA 公開金鑰系統進行加密，加密後的結果即儲存於影像區塊的最低位元。驗證時，將每個

影像區塊的最低位元解密，同樣將原圖區塊的最低位元以 MD5 作雜湊運算並作互斥運算比對，以驗證其影像資料的完整性。

三、半脆弱型數位浮水印方法

脆弱型浮水印對於影像資料的任何變動都能偵測出來，除了能確保其完整性之外，也能指出影像資料中遭修改的位置，但對於一般常見的影像壓縮或格式轉換等處理則不適用。因此考慮實際應用時數位影像常常會再經過某種影像處理或壓縮等情形，一般多採用半脆弱型浮水印技術，以期在防範惡意攻擊的原則下，也能允許某些常見的影像處理。

半脆弱型浮水印方法的設計通常只能針對某種特殊的影像處理才有較佳效果，目前沒有一個方法能有效的辨識所有的正常影像處理與惡意攻擊。同時半脆弱型浮水印為了避免讓影像資料太過敏感，通常不直接對影像空間域作處理，而改對影像轉換域作處理，常見的影像轉換方法包括離散餘弦轉換（Discrete Cosine Transform, DCT）與離散小波轉換（Discrete Wavelet Transform, DWT）等。

2000 年 Lin 與 Delp 等學者提出一種可以允許影像經過正常 JPEG 壓縮的影像鑑別技術[17]，其方法主要是利用 JPEG 壓縮的標準流程中，影像會先被分成許多 8×8 的區塊，經過離散餘弦函數轉換後，每個區塊共有 64 個係數，而作者選擇影像低頻（Low Frequency）的係數嵌入浮水印，雖然會使影像產生部分失真的現象，但卻能讓浮水印資料在經過 JPEG 壓縮時順利的保留下來，如此一來便能讓影像經過 JPEG 壓縮後再行傳送。

2002 年 Sun 與 Suto 等學者提出一種可以允許影像經過 JPEG2000 壓縮的影像鑑別技術[18]，其方法利用 JPEG2000 壓縮標準流程中最佳化區塊編碼演算法（Embedded Block Coding with Optimal Truncation, EBCOT）的特性，選出各個影像編碼區塊的特徵值（feature），並利用錯誤更正碼（Error Correction Code）將浮水印資料嵌入影像之中，同時亦採用同位元檢查（Parity Check）機制產生數位簽章。在驗證時，除了可以透過錯誤更正碼來判斷影像是否經過 JPEG2000 壓縮之外，還可以利用數位簽章來做進一步的驗證，因此具有較高的安全性。

未來發展

一、結合數位浮水印與數位簽章

數位簽章具有不可否認性，但卻需要將其附加於檔頭或其他位置傳送，增加簽章可能遭移除的機會。而數位浮水印直接將資料嵌入於影像之中，雖然可以避免簽章管理的問題，但由於影像資料在受到正常處理或遭惡意破壞的情況下，浮水印資料無法完整的提供不可否認性，因此具有數位簽章功能的半脆弱型數位浮水印方法

將是未來主要的發展方向。

二、結合影像復原技術

數位影像因為使用方便，常會經過各種處理，若沒有事先保留原圖，影像可能經過多次處理之後，便無法確切得知究竟原始影像為何。例如影像資料內容極為重要的醫學或軍事影像，若因為傳輸過程中的雜訊干擾而導致影像資料失真，可能會造成嚴重的後果。因此結合影像復原的影像鑑別技術，例如利用錯誤更正碼或重複嵌入浮水印等技術，將是未來研究發展的重點。

三、增強影像品質

數位浮水印因為直接嵌入於影像之中，會對影像內容造成一定程度的破壞，一般而言嵌入的浮水印資料量愈高，影像品質愈差。改善的方法便是利用人眼視覺模式，將浮水印資料隱藏在肉眼較無法發覺的部位，未來的挑戰將是如何發展更為精準的人眼視覺模式，以確保在不同條件下能保持良好的影像視覺品質。

四、增加準確性

影像鑑別技術的準確性在刑事犯罪調查等應用方面顯得十分重要，未來若每個人的指紋或臉型都以影像格式建檔時，每個人便都可以保有自己專屬的生物特徵值，當警調單位進行偵察時，便可以快速的利用影像進行調查。因此為了確保政府單位的公信力，未來仍須克服的重要問題是如何仍能在這些影像中準確並有效的進行鑑別，以確保人民的權益。

結論

隨著電腦硬體技術及資料編碼技術的進步，數位影像資料在網路上的使用更加便利，如何有效確保數位影像資料在傳輸使用時的真實性與完整性，是未來電腦安全防護中的重要議題。

對國軍而言，資訊化是未來的趨勢，國軍除了現有的各種衛星照片、地圖以外，包括各種公文、資料、圖表未來也都將朝數位化形式保存，數位影像資料的比例亦將逐漸增加。因此為了掌握資訊化潮流，也為了增進國軍電腦安全防護技術，數位影像鑑別技術值得我們更深入研究。

註釋

1.楊松諺，上官飛鳳譯，Java Security 全方位解決方案，(台北：碁峰資訊，2004)。
2.Y.. Zhao, “Dual domain semi-fragile watermarking for image authentication,” Master Thesis, (2003).
3.W. Stalling, Cryptography and Network Security – Principles and Practices,

Prentice-Hall, 3rd Edition, (2002).
4.http://www.ctr.columbia.edu/~cylin/auth/auth.html.
5.C. Fei, “Semi-Fragile Multimedia Content Authentication,” Presentation slides in SCG Seminar 2004.
6.C.-T. Li, and Y. Yuan, “Digital Watermarking Schemes for Multimedia Authentication,” Digital Watermarking for Digital Media, Idea Group Publishing, (2005), pp.30-51.
7.D.-C. Lou, J.-L. Liu and C.-T. Li, “Digital Signature-based Image Authentication,” Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellecutal Property, Idea Group Publishing, (2004), pp. 207-230.
8.D. Skraparlis, “Design of an Efficient Authentication Method for Modern Image and Video,” IEEE Transactions on Consumer Electronics, Vol. 49, (2003), pp. 417-426.
9.F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information Hiding – A Survey,” Proceedings of the IEEE, Vol. 87, No. 7, (July 1999), pp.1062-1078.
10.http://www.frtr.gov/watermark.jpg .
11.http://www.lisarein.com/.../ 8-09-03-cnn-wendy-eff.jpg .
12.http://www.ndap.org.tw .
13.周兆龍,「容忍失真性壓縮之資訊隱藏技術」,國防大學中正理工學院電子工程研究所碩士論文，(桃園，2004)。
14.C. Rey, and J.-L. Dugelay, “A Survey of Watermarking for Image Authentication,” *EURASIP Journal on Applied Signal Processing*, Vol. 6, (2002), pp. 613-621.
15.M. Yeung, and C. Mintzer, “An invisible watermarking technique for image verification,” Proceedings of ICIP, (1997), pp. 680-683.
16.P. W. Wong, “A watermark for image integrity and ownership verification,” Proceedings of IS&T PIC Conference, Portland, (1998).
17.E. T. Lin, C. I. Podilchuck, and E. J. Delp, “Detection of image alterations using semi-fragile watermarks,” Proceedings of SPIE Security and Watermarking of Multimedia Contents , Vol. 3971, (2000), pp. 152-163.
18.Q. Sun, S.-F. Chang, M. Kurato, and M. Suto, “A Quantitive Semi-Fragile JPEG2000 Image Authentication System,” Proceedings of ICIP, (2002).