眼見為憑？淺談數位影像偽冒偵知技術

陸軍少校　曾棨傑　空軍中校　周兆龍

提　要

一、隨著數位影像擷取設備及影像編輯軟體技術的快速發展，現今數位影像的使用率已經遠遠超過傳統相片，然而，伴隨著數位影像愈趨普及且應用廣泛而來的是其遭受竄改或偽冒的情況也日益頻繁。

二、對於一些重要的數位影像應用範疇，如軍事情報、衛星影像、醫學影像、犯罪偵察影像…等，影像內容的完整性至關重要。數位影像鑑識即是為了確保影像資料的真實性及完整性而發展出來資訊安全技術。

三、本文探討目前常見的各種影像偽冒方法與案例，並介紹數位影像鑑識中用以檢測影像是否曾遭竄改的影像偽冒偵知技術，提供讀者研究參考。

關鍵詞：數位影像鑑識、完整性、資訊安全、影像偽冒偵知。

前　　言

西方諺語曾說『一圖勝過千言萬語』、『To See is to Believe』，一張影像對於人所能產生的感受通常遠超過於文字描述。隨著各種數位相機、智慧型手機、網路攝影機(Webcam)、掃瞄機等資訊設備愈趨普及化，再加上如Photoshop等影像編輯軟體功能不斷地推陳出新，現今數位影像的使用率已經遠遠超過傳統的相機相片，應用的範疇包括個人或家庭常見的數位相片沖洗、社群網站存放的個人相片，更包括應用在網頁新聞、報章雜誌、醫學診斷、電腦繪圖、產品設計、衛星遙測、工業品管、裝潢設計、犯罪偵察、軍事情報…等。

數位影像是經由電腦產生的一種二維圖像，透過包含光亮與色彩資訊的數個像素(Pixel)所組成。這些二維圖像透過人的雙眼，並經由大腦感應這些光線及色彩資訊之後，便轉變成為我們所看到的影像。然而，人的眼睛的構造其實存在有許多的限制。例如人眼對於可見光範圍(波長380～780 nm)以外的光亮及色彩敏感對較低；人眼有所謂視覺暫留的現象，電影即是利用此特性，將靜止影像的在短時間內連續放映(通常為每秒24張影像以上)，即會讓人的視神經產生動畫的感覺；另外，人眼對於影像解析度也有極限，通常影像解析度以DPI(Dot Per Inch, DPI)

來代表每英吋所含之像素數量，DPI愈高表示解析度愈佳，而人眼對於300 DPI以上的影像即會覺得畫面細緻，而即使DPI增加很高，人眼也並不容易發覺影像中所呈現的細節。

一般人常說『有圖有真相』，但隨著數位影像的應用愈趨廣泛，數位影像遭受竄改或偽冒的情況日益頻繁。網路上的新聞照片是否可信？所接收到的軍事照片是否可靠？法庭上的數位影像是否足以作為犯罪事實的證據？這些對於數位影像真實性的疑慮，光靠一般人眼是不夠的，還必須仰賴影像鑑識技術(Image Forensics)與專業人士的輔助。

本文探討目前常見的各種影像偽冒方法與案例，並介紹數位影像鑑識中檢測影像是否曾遭竄改的影像偽冒偵知(Image Forgery Detection)技術。相關內容可提供國軍資訊單位發展或運用相關數位影像鑑識技術之參考。

數位影像鑑識

一、背景介紹

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(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)被改變，因此良好的完整性亦代表了資料內容的可信度與真實性。影響資料完整性的可能因素包括資料毀損、網路傳輸遺失、雜訊干擾、或遭有心人士蓄意竄改、破壞…等等。

目前常見的數位影像鑑識技術的應用範疇如下：

(一)身分辨識

運用個人生物特徵(如人臉、指紋、虹膜)以數位影像方式建立個人身分資料，運用影像處理與模式辨識(Pattern Recognition)技術，即可將其應用於個人安全管理、門禁安全管制、軍事安全、犯罪調查…等。

(二)智慧財產權保障

網路傳播資料十分迅速，具智慧財產權的數位影像亦容易遭到非法複製、修改或散播，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。如版權影像加上正版原廠商標Logo，或重要文件加註可視型(Visible)數位浮水印。

(三)醫學影像

例如X光影像、藥品等，可以影像方式建檔，加註病患身分、病歷記錄、藥品成分、醫師授權、藥品管理資訊…等，可用以保障病人隱私權、提供醫師追蹤病歷，並建立合法用藥的安全性。

(四)軍事管理

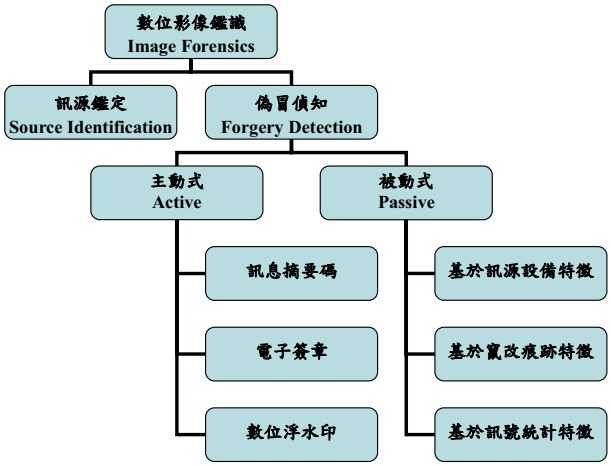
重要軍事影像資料傳遞，例如衛星照片、軍事地圖等，可以加入合法授權的認證，使接收方在確認資料來源同時也能確保資料的完整性，以確保軍事安全。另外如武器裝備或零附件之基本資料及庫儲資訊、電子公文…等一般軍事事務，亦可以數位影像的方式建檔，以利相關管理作業。

(五)犯罪調查

無論一般的民事糾紛或重大的刑事案

件，數位影像常作為法庭審理案件時的呈堂證供，因此影像內容的完整性十分重要。而影像的來源除了監視器外，也常來自於個人所持有的數位相機、手機、行車記錄器…等，為了避免影像真實性遭受質疑，在案件調查期間影像資料仍應透過具公信力與權力的機關部門進行專業的鑑識程序，以確保公正性。

數位影像鑑識一般包含兩個主要工作：訊源鑑定(Source Identification)及偽冒偵知。[1]其架構如圖一所示。



圖一　數位影像鑑識架構示意圖(資料來源：作者繪製)

●訊源鑑定

數位影像的來源十分廣泛，包括數位相機、智慧型手機、監視器、掃描器。不同類型的設備具備不同的特性，因此拍攝出來的照片品質均不相同；而即使相同的設備也會因為廠牌的不同而有差異，例如採用感光耦合元件 (Charged-Coupled Device, CCD)／互補氧化金屬半導體(Complementary Metal- Oxide-Semiconductor, CMOS)鏡頭出來的呈像效果不同，如何分辨這些細微的差異就是屬於訊源鑑定的工作。

●偽冒偵知

影像偽冒偵知的目的是要確認影像是否遭到任何的竄改，以確保其完整性。數位影像偽冒偵知依照使用的方式區分大致可以分成主動式(Active)及被動式(Passive)的兩大類。[2]所謂主動式是指數位影像在產生或使用之前，影像本身已經嵌入了用以認證用的特徵碼，例如訊息摘要碼(Message Digest)、電子簽章(Digital Signature)或數位浮水印(Digital Watermarking)…等，因此在進行鑑識時只需要用標準認證程序即可驗證出影像是否經過竄改；而被動式是指影像完全沒有嵌入可供認證參考的任何訊息，沒有特定的方法可以直接進行驗證，而必須嘗試各種方法來進行鑑識。本文所探討的重點即為被動式的影像偽冒偵知技術。

二、主動式影像偽冒偵知技術

主動式數位影像偽冒偵知技術最常見的有訊息摘要碼、電子簽章或數位浮水印等三種。

1 Z. Geradts and J. Bijhold "Pattern recognition and image processing in forensic science," Proceedings of the Irish Machine Vision and Image processing, 2000, pp. 15-33.

2 G. R. Elwin, T. S. Aditya, and M. S. Shankar "Survey on passive methods of image tampering detection," Proceedings of International Conference on Communication and Computational Intelligence, India, Dec. 2010, pp. 431-436.

(一)訊息摘要碼：

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)。雜湊函數主要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。因此只要任何一個資料位元經過新增(Insertion)、刪除(Deletion)或替換(Substitution)等處理，所產生的雜湊值即會不同，利用比對雜湊值的方式，便可以用來驗證資料的完整性。

訊息摘要碼簡單來說就是加了密鑰(Secret Key)的雜湊函數。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摘要碼。接收端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摘要碼，經過比對後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。

(二)電子簽章

訊息摘要碼具有計算快速的優點，但其缺點是若有第三者事先取得傳送端與接收端使用的相同密鑰，便可能利用這個密鑰偽造訊息。電子簽章可以解決訊息摘要碼的這個缺點，改以使用公鑰(Public Key)與私鑰(Private Key)的非對稱式加解密系統，事先特別選取了某種單向暗門雜湊函數(Trapdoor One-Way Hash Function)，單向暗門雜湊函數因為具有某種暗門，可以讓十分困難的反向雜湊函數計算變得很容易。電子簽章將訊息以公鑰進行加密，並利用私鑰進行解密，可以同時確保資料的完整性及不可否認性。

(三)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)的一種，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。數位浮水印早期常被應用作為著作權保障(Copyright Protection)，例如電視新聞畫面常見的Logo或者DVD影碟中的產品追蹤碼。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(Embed)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(Extract)回來。嵌入浮水印時可以視情況加入金鑰，以增加系統安全性，並確保不可否認性；在浮水印萃取階段，則通常參考原始影像或金鑰來進行浮水印的比對。

數位浮水印依特性可以區分為強固型(Robust)與脆弱型(Fragile)兩大類。其中脆弱型數位浮水印主要就是針對影像資料完整性作設計。最常見的脆弱型數位浮水印作法是將整張影像細分成同等大小的區塊，每個影像區塊再分別計算其訊息摘要碼，接著將整張影像進行無失真(Lossless)壓縮，並將壓縮後的影像資料與各影像區塊的訊息摘要碼合併成為一個影像檔案。這種作法除了可以判斷影像是否經過修改之外，還可以分別驗證每個不同影像區塊的訊息摘要碼，以判斷出來影像哪個部分遭到修改。

上述幾種方法的共同特徵是在進行鑑識時通常需要原始影像、演算法或金鑰等參考資訊以供比對，無論是加密與解密或浮水

印的嵌入與萃取，一旦缺少其中任何一項參考資訊，便可能無法順利的完成影像鑑識工作。然而，一般在數位影像偽冒偵知的實務上，更多的情況是所蒐集到的數位影像證據並沒有其他的參考資訊，此時即需要採用被動式影像偽冒偵知方法。

三、被動式影像偽冒偵知技術

近年來隨著數位相機的普及以及社群網路的發達，許多的數位影像是由個人或家庭所產生，例如網路個人相簿、部落格、網路討論區…等。而這類的影像通常無法由特定的主動式影像偽冒偵知技術來鑑定其真實性，因此需要被動式影像偽冒偵知技術。

被動式數位影像偽冒偵知技術因為需要較專業複雜的技術，因此大部分仍是應用在特定的領域，例如政府機關、軍事單位、企業組織…等。在實務上數位影像為了方便使用或或儲存在電腦上，通常會經過壓縮、模糊、銳化、格式轉換、影像增強、色彩修正、雜訊消除…等處理，這類的訊號處理應該將其視為合法的使用範疇。然而，有些加工程序例如裁切、刪除物件、置換物件、增加物件、影像合成…等，則可能是有心人士試圖竄改影像的結果。因此，被動式數位影像偽冒偵知可以概分為兩個層次：第一個層次是確認影像是否經過加工處理，這些大部分均可仰賴電腦技術來完成；第二個層次則是判斷這些加工是否為惡意的竄改或偽冒，這部分除了電腦技術，還需要仰賴專業的判斷。

目前針對被動式數位影像偽冒偵知還沒有完整具體的系統方法和理論，大多還是需要針對不同的影像竄改方式中，去嘗試出相對應的鑑識方法。數位影像偽冒偵知仰賴許多專業技術的結合，包括資料探勘(Data Mining) 、模式辨識、機器學習(Machine Learning)、訊號處理(Signal Processing)、影像處理(Image Processing)、機率統計…等。一般而言，被動式數位影像鑑識依據影像竄改類型及所參考的不同特徵，可以區分為以下幾種類型：

(一)基於不同影像訊源設備所產生的特徵來進行鑑識。

(二)基於各種影像竄改痕跡所產生的特徵進行鑑識。

(三)基於數位影像訊號的統計特徵來進行鑑識。

數位影像竄改類型

一、影像竄改案例

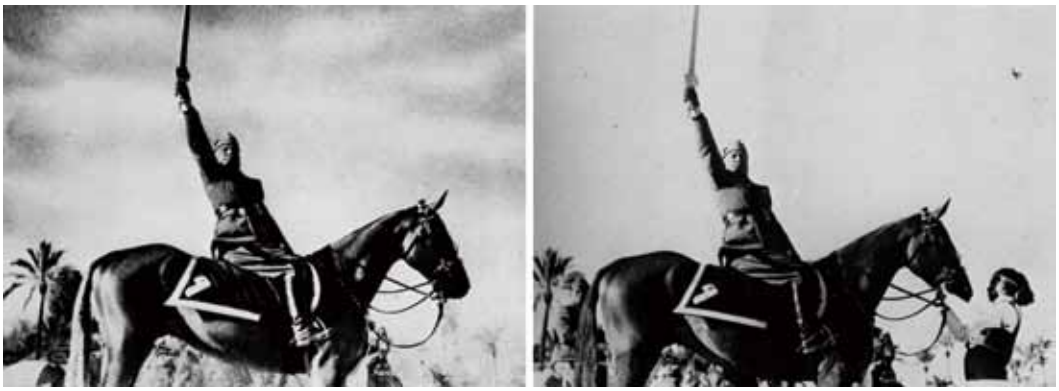
影像竄改的事件不是只有發生在現代，許多歷史上的名人都曾出現過相片遭到修改的痕跡。例如義大利的墨索里尼(如圖二)、蘇聯的史達林(如圖三)、德國的希特勒(如圖四)都曾出現過經過變造後的照片。歷史上這些著名的影像修改案例，姑且不論背後的目的為何，在當時要修改一張照片可能需要數個小時，經過各種複雜的程序，才能完成一張看似真實的偽裝照片。

隨著現代數位化程度的提昇，數位影像可以輕易透過各種影像擷取設備產生，再加上各種先進的影像處理軟體輔助，便可以輕易的製作出幾可亂真的影像。本節將介紹一些現今的數位影像竄改案例，並將這些方法

加以分類，以期讀者瞭解常見的數位影像竄改類型。

●時代雜誌辛普森封面照案例[3]

1994年，美國著名的辛普森殺妻案，成為美國及世界的頭條新聞，當時美國時代雜誌(Times Magazine)及新聞週刊(Newsweek)不約而同的將辛普森的警局檔案照當作雜誌的封面片。然而，將兩本雜誌封面互相比對之下，可以明顯的發現時代雜誌所刊登的辛普森整個人色調變的昏暗，彷彿給人一種邪惡、黑暗的感覺(如圖五(a)所示)。時代雜誌承認將辛普森的照片經過修改，但否認與種族意識有關。在美國民眾強烈譴責的壓力下，時代雜誌最終不得不對修改辛普森照片一事進行公開道歉。



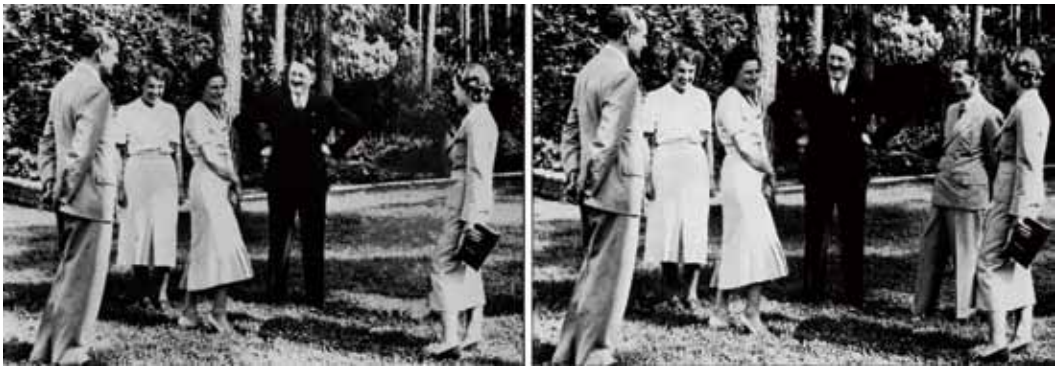
(a) (b)

圖二　墨索里尼的變造照片(a)馬伕遭到移除，(b)原始照片(資料來源：H. Farid, Digital image forensics, 2011, pp. 5-6.)

(a) (b)

圖三　史達林的變造照片(a)身旁人遭移除，(b)原始照片(資料來源：H. Farid, Digital image forensics, 2011, pp. 5-6.)

3 〈Photo Tampering throughout History〉，http://www.fourandsix.com/photo-tampering-history/category/1950-1999?currentPage=2



(a) (b)

圖四　希特勒的變造照片(a)身旁人遭移除，(b)原始照片(資料來源：H. Farid, Digital image forensics, 2011, pp. 5-6.)

(a) (b)

圖五　美國辛普森案新聞雜誌封面 (a)時代雜誌 (b)新聞週刊(資料來源：http://www.fourandsix.com/storage/photo-tampering-history/Jun1994-ojsimpson.jpg)

●小布希總統競選照遭竄改案例[4]

2004年，美國小布希總統競選時所用的宣傳照片(如圖六(b)所示)，後來被人發現某個小布希總統在現場的演說畫面被移除了。這張照片將一群背景的美軍士兵複製之後，再將原本小布希的畫面加以覆蓋，刻意讓小布希總統消失在畫面之中。經過專業的檢驗之後，發現這張影像中有三個區塊疑似遭到竄改(如圖六(a)所示)，因為相同的士兵面貌很明顯的重複出現。

●青藏鐵路攝影作品案例[5]

2006年，由大陸攝影師劉為強所拍攝的一張西藏野生羚羊在青藏鐵路附近奔跑的一張照片，獲選為當年中央電視臺的年度10大新聞圖片銅獎(如圖七所示)。然而，此照之後被證實為合成照片，原因是被大陸網友發現鐵路橋墩及照片下緣有明顯的影像拼接痕跡；此外，羚羊天性機靈敏感，因此若真如照片中有火車從上方經過，應該會四處逃竄，而非像照片中一般的筆直行進。

4 〈Photo Tampering throughout History〉，http://www.fourandsix.com/photo-tampering-history/category/2004.
5 〈造假趕羚羊 新聞銅牌獎〉，http://blog.roodo.com/gamy543/archives/5553589.html.

(a) (b)

圖六　小布希總統選舉宣傳照 (a)遭竄改之照片 (b)原始照片(資料來源： http://www.fourandsix.com/photo-tampering-history/category/2004.)

圖七　青藏鐵路攝影作品 (資料來源：http://www.flickr.com/photos/maybird/2273407652/)

●教宗新聞照案例[6]

2007年，天主教教宗本篤十六世於梵蒂岡接見臺灣商業代表團，新聞媒體刊登了一幅教宗正在參觀法藍瓷的照片(如圖八(b)所示)，其中自由時報所刊登的新聞照片中，聯合報發行人王曉蘭女士的影像被抹去了(如圖八(a)所示)。自由時報的解釋是直接採用法藍瓷公司所提供經過修改過的照片，而在不知情之情況下刊登。

●美軍首位女四星上將宣傳照[7]

2008年，美國陸軍軍官Ann Dunwoody被授與四星上將軍階，成為美國歷史上第一位女性四星上將。然而，美軍國防部發給媒體的新聞照片，卻被質疑遭到修改(如圖九所示)。修改的部分包括照片背景被美國國旗取代、胸前原本的三星軍階被切掉，還有臉部經過修飾，使其看起來更為年輕。

●國軍巴紐陣亡將士迎靈照案例[8]

2009年，國防部派員到巴布亞紐幾內亞，接迎二次大戰期間遭日軍俘擄後在巴紐當地身亡的大批國軍官兵忠魂回台，並在大直忠烈祠舉行暫祀安靈儀式。然而，中國大

6 〈Photo Tampering throughout History〉，http://www.fourandsix.com/photo-tampering-history/category/2008.
7 〈Row over altered US Army photo〉Nov. 19 2008，http://news.bbc.co.uk/2/hi/americas/7738342.stm.
8 〈「中華民國」不見了牌位照遭大陸竄改〉，http://mag.udn.com/mag/world/storypage.jsp?f_ART_ID=182335.

(a) (b)

圖八　教宗接見台灣代表團新聞照(a)自由時報刊登之照片 (b)原始照片(資料來源：http://www.fourandsix.com/storage/photo-tampering-history/Jan2008-LibertyTimes.jpg)

(a) (b)

圖九　美軍首位女四星上將照片(a)官方照片(b)原始照片(資料來源：The Fake General Dunwoody，http://www.museumofhoaxes.com/hoax/photo_database/image/the_fake_general_dunwoody.)

陸新浪網網路新聞所刊登的照片中，原本迎靈牌位的字樣被竄改為「巴紐陣亡將士」，原本的「中華民國國軍」等字樣遭到刪除(如圖十所示)。而這張遭到竄改的照片之後也被大陸其他媒體錯誤引用。

●桐花節攝影比賽案例[9]

2012年，客委會主辦桐花攝影比賽，首獎作品「山中傳奇」(如圖十一(a)所示)遭眼尖的網友發現，照片下方的男女腳部相當奇怪，且身上的色溫與整體光源不同，疑似經過影像合成。經過網友熱心比對後，發現照片中的男女早已出現在該作者2011年由台北醫學大學所主辦的攝影比賽佳作作品「誰與爭鋒」之中(如圖十一(b)所示)，除了方向相反之外，其餘外觀一模一樣，經專業評審審查後確定影像經過合成。作者事後承認此事並親自道歉，而主辦單位也取消他的首獎資格。

二、影像竄改類型

依照數位影像竄改的方式，大致可以將其區分為以下幾種類型：

(一)合成照片(Composite)

係指利用兩張以上不同的照片，合成

9〈桐花攝影　陳炳－桐花攝影首獎「山中傳奇」確定經後製　攝影師陳炳道歉(圖＋影片)〉，http://mape99.pixnet.net/blog/post/92681301-桐花攝影　陳炳－桐花攝影首獎「山中傳奇」。

(a) (b)

圖十　國軍巴紐陣亡將士迎靈照(a)官方照片(b)原始照片(資料來源：http://www.fourandsix.com/storage/photo-tampering-history/Mar2009-Sina.jpg)

(a) (b)

圖十一　(a) 2012年客委會桐花攝影比賽首獎作品「山中傳奇」(b) 2011年由台北醫學大學所主辦的攝影比賽佳作作品「誰與爭鋒」(資料來源： http://mape99.pixnet.net/blog/post/92681301-桐花攝影　陳炳一桐花攝影首獎「山中傳奇」)

為一張偽裝照。為了讓人難以發覺，通常這種方式會有一張正常的背景，而在這張背景影像中找尋要合成的位置加以處理。例如、『青藏鐵路攝影作品』及『美軍首位女四星上將宣傳照』、『桐花節攝影比賽』均屬之。

(二)複製－貼上(Copy-Move)

係指在同一張照片中，對某個部分進行修改或破壞，通常這種方式會將影像中的某個部分加以複製後，貼上要修改的位置，掩蓋原始的影像內容。例如『小布希總統競選照遭竄改』、『國軍巴紐陣亡將士迎靈照』均屬之。

(三)裁切(Cut)

係指直接將影像的某個部分加以裁切去除，再將其他部分加以拼接，這種方式與

『複製-貼上』不同之處是影像經過裁切後會比原始影像還小。例如『教宗新聞照』屬之。

(四) 影像修整(Retouching)

常見在各種電影海報、平面宣傳廣告、婚紗照、雜誌封面照…等，係指不改變影像的內容，但針對影像的色彩、亮度、解析度、對比度…等影像特性進行調整，而改變影像原始特性。例如『時代雜誌辛普森封面照』及『美軍首位女四星上將宣傳照』均屬之。

本文將上述各項影像竄改案例與其竄改類型相互對照(如表一所示)，可以發現遭竄改之數位影像並不侷限單一類型之竄改方法，例如『美軍首位女四星上將宣傳照』即同時遭合成及影像修整兩種竄改方式。

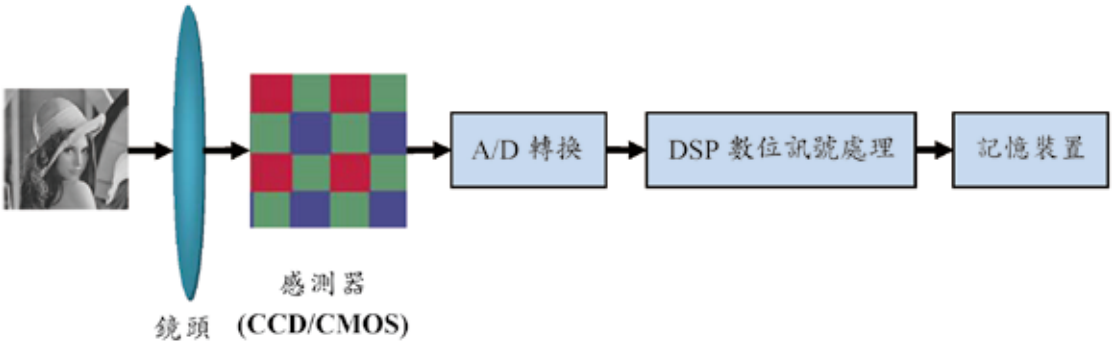
數位影像偽冒偵知技術

一、基於影像訊源的特徵

一般數位相機包含了鏡頭、濾鏡、影像感測器、色彩解析、記憶儲存裝置等各部分。數位影像的成像需依序經過鏡頭、濾鏡、影像感測器、A/D轉換、數位訊號處理(如曝光補償、白平衡、伽瑪校正、降低雜訊、銳化…等)及檔案儲存等步驟(如圖十二所示)。其中光學鏡頭和彩色濾鏡因為不同的

表一　影像竄改案例及其竄改類型對應表(資料來源：作者繪製)

類型＼案例	時代雜誌辛普森封面照	小布希總統競選照	青藏鐵路攝影作品	教宗新聞照	美軍女四星上將宣傳照	巴紐陣亡將士迎靈照	桐花節攝影比賽
合　　成			V		V		V
複製－貼上		V				V	
裁　　切				V			
影像修整	V				V		

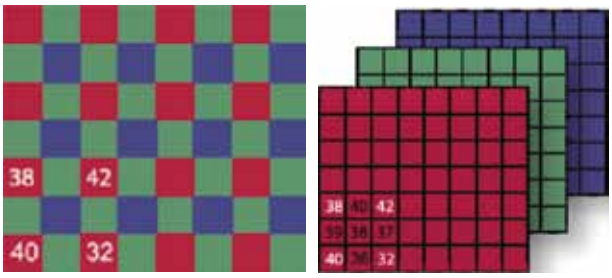


圖十二　數位影像成像流程示意圖(資料來源：作者繪製)

設備採用不同廠牌、材質及技術，因此具有獨特的特徵，可以被應用在數位影像竄改偵測。

以光學鏡頭為例，鏡頭通常用來控制光線、曝光、對焦等工作，但由於鏡頭不可能完美的聚焦各種波長的光線，因此不同的鏡頭會出現不同程度的失真(Distortion)情況，這種失真稱之為色差(Chromatic Aberration)。當影像遭受竄改時，色差會被破壞，而導致整張影像的色差不一致，利用橫向色差或縱向色差可以來檢測影像是否遭受竄改。

以彩色濾鏡為例，當光線進入鏡頭之後會先投射到影像感測器(通常為CCD或CMOS)，而這些影像感測器為了要捕捉彩色畫面必須要使用所謂的彩色濾光陣列(Color Filter Array；CFA)，彩色濾光陣列中每個位置只負責感測特定波長的光線。例如常用的拜爾陣列(Bayer Array)是以紅、藍、綠間隔的方式排列(如圖十三(a)所示)。當影像即將成像時，為了符合標準彩色三原色(紅、藍、綠)的方式，彩色濾光陣列在未感測到光線的位置會以內插(Interpolation)的方式計算出其像素值，而加以補足缺少的像素值(如圖十三(b)所示)。使用類似這種方式的數位相機，在影像最終成像的結果，每個鄰近的像素位置其像素值一定保有此種關連性。[10]若某張影像宣稱是由某台相機所拍攝，但卻又不符合這台數位相機應有的鄰近像素關連性，那麼這張影像應該已經被動過手腳了。



(a) (b)

圖十三　拜爾陣列濾光器(a)實際排列方式 (b)運用內插法計算鄰近像素值(資料來源：H. Farid, Digital Doctoring: can we trust photographs?, 2009, pp. 6.)

二、基於影像竄改痕跡的特徵

影像竄改的方式有合成、複製－貼上、裁切及影像調整等各種方法，無論哪一種方法，都可能在影像上留下蛛絲馬跡。本節針對這些不同竄改方法所產生的特徵介紹幾種常見的檢測方法。

(一) 暴力搜尋法

這種方法可以被應用在檢測影像複製-貼上竄改。通常複製-貼上的影像竄改方法會將影像背景中的部分區域加以複製，並貼在同一張圖上。這種方式很直覺的會讓影像中重複出現相同區域，採用暴力搜尋法即可能找出相同的區域，但是這種方式計算費時，並且可能容易產生誤判的情形發生。另一種選擇是可以將影像細分成小區塊之後，再分別進行頻率域轉換(如DCT轉換)，計算每個區塊的特徵值。出現相似的特徵值的區塊經過排列後，即可再經過人眼進行判斷，以確定該影像區域是否已遭到竄改。

10 A. C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," IEEE Transactions on Signal Processing, vol. 53, no. 10, pp. 3948-3959, 2005.

(二)JPEG雙重壓縮法：[11]

這種方法可以被應用在檢測影像合成竄改。一般數位影像常因為要節省儲存容量或傳輸時間，會將影像在合理的品質範圍進行壓縮處理。而合成照片大多來自於不同的照片，在進行偽造合成之前可能照片事先已經過了不同程度的壓縮處理。若這張合成照再經過一次壓縮，便會出現不同的特徵可以用以檢測影像是否經過竄改。以常見的JPEG壓縮為例，偽造影像經過JPEG雙重壓縮之後，不同壓縮比的區域會在影像DCT轉換係數中出現不同的週期性。

(三) 影像重取樣法(Resample)[12]

影像重取樣是指影像經放大、縮小、旋轉、平移等處理，而影像重取樣常會進行內插法運算，也就是會在鄰近像素之間造成相關性的變化。經過重取樣的影像因為影像訊號及週期性訊號的疊加，因此大多會在傅立葉轉換(Fourier Transform)之後出現規則性的亮點，而未經重取樣的影像則不會。透過影像重取樣偵測動作可以判斷影像是否遭到過重取樣的修改。

(四) 光源檢測法[13]

這種方法可以被應用在檢測影像合成竄改。合成影像是透過兩張以上的影像所合併而成，每張影像可能有各自不同的光源。當合併在同一張影像上時，會產生物件光源不一致的情況。以圖十四為例，針對影像中的人物進行光源檢測，其中黃色箭頭即代表光源，可以發現圖十四(a)中的人物光源一致，而圖十四(b)中的人物光源不一致。因此可以判斷圖十四(b) 中的人物是經過影像合成的結果。

三、基於影像統計特性

影像竄改的方式日新月異，若有任何新式的影像竄改方式被提出，那麼現有的基於訊源特徵或基於影像竄改痕跡特徵的偵測方法將可能失效。因此，基於影像統計特性的偵測方法，不再只針對特定的影像竄改模式分析，而是改以分析影像本身的統計特徵，再判斷影像是否遭受過竄改。這種方式的好處是可以偵測到未知的影像竄改行為，但缺點是準確率通常較低。[14]

基於影像統計特性的方法採用了許多機器學習與模式辨識的技巧，將已知的影像竄改特徵建立資料庫，並不斷的重複偵測的程序，讓系統依據影像特徵學習分類、判斷並改進效能，可以具備偵測未知影像竄改的能

11 A. C. Popescu and H. Farid, "Statistical tools for digital forensics," Proceedings of 6th Intertional Workshop on Information Hiding, Toronto, Canada, 2004, pp. 128-147.

12 A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of re-sampling," IEEE Transactions on Signal Processing, vol. 53, no. 2, pp. 758-767, 2005.

13 M. K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," Proceedings of ACM Multimedia and Security Workshop, New York, USA, 2005, pp. 1-10.

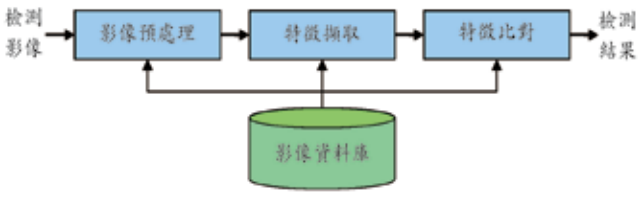
14 H. Farid, "A survey of image forgery detection," IEEE Signal Processing Magazine, vol. 2, no.26, pp. 16-25, 2009.

(a) (b)

圖十四　光源檢測影像(a)人物光源一致 (b) 人物光源不一致(資料來源：M. K. Johnson, Lighting and Optical Tools for Image Forensics, Ph.D. Dissertation, Dartmouth College, 2007, pp. 17-23.)

力，因此更能符合實務上的需求。

基於統計特性的影像偽冒偵知流程如圖十五所示。通常在進行影像偵知之前，會先將訊號強化的預處理(Pre-processing)，接著擷取影像特徵，影像統計特徵包括與直方圖(Histogram)有關的平均值(Mean)、變異數(Variance)、偏移率(Skewness)、峰態(Kurtosis)、共生矩陣(Co-occurrence)、轉換域係數(Transform Coefficients)、熵(Entropy)…等，各種不同的影像統計特性還可以依照影像竄改特性互相關連並增加，以提高辨識率。最後再與特徵資料庫進行比對，特徵比對通常是採用與模式辨識或機器學習有關的



圖十五　基於統計特性的影像偽冒偵知流程 (資料來源：作者繪製)

統計理論，以使檢測結果更為精準。

結　　論

隨著數位科技的不斷進步，數位影像的產生、編輯、儲存、傳輸…等相關技術將更為先進，數位影像的運用也將愈來愈廣泛。在可預見的未來，影像遭竄改或偽冒等濫用的情況將會愈來愈頻繁，而這些偽冒的影像將更難以被偵測出來。面對醫學、軍事、犯罪偵察…等重要的應用領域，具可靠度與公信力的數位影像鑑識技術發展刻不容緩。

數位影像偽冒偵知技術於軍事的相關應用亦十分廣泛，除了資訊安全管理之外，還可能應用在營區門禁管制、文書管理、後勤管理、庫儲管理、戰場地理影像資訊、敵情偵搜、情報傳遞、衛照判讀…等。因應未來國軍朝向軍隊數位化之方向持續發展，本文所介紹之數位影像偽冒偵知技術，將可提供各單位發展或應用相關技術之參考。

作者簡介

曾棋傑少校，國防管理學院資管系89年班、國防大學管理學院資訊管理研究所碩士99年班。曾任電腦硬體工程官、程式設計官 、資訊參謀官。現任職於國防部參謀本部後勤參謀次長室少校資參官。

周兆龍中校，中正理工學院資訊科學系87年班、國防大學理工學院電子工程研究所碩士93年班、國防大學理工學院國防科學研究所電子組博士101年班。曾任電腦系統工程官、程式設計官、後勤參謀官 、資訊參謀官。現任職於國防部參謀本部後勤參謀次長室中校資參官。