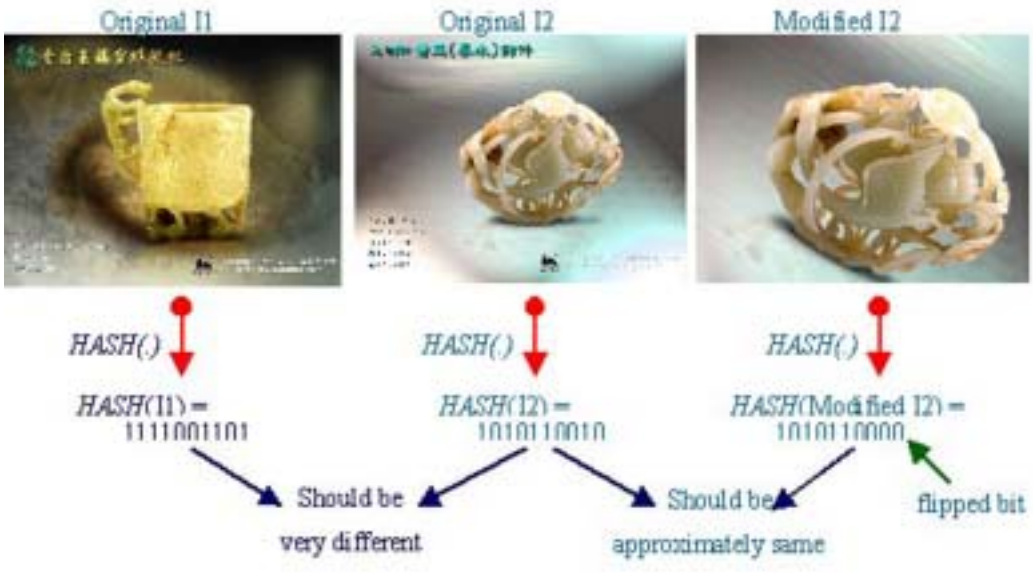
知識天地

多媒體的數位指紋

呂俊賢（資訊科學研究所副研究員）

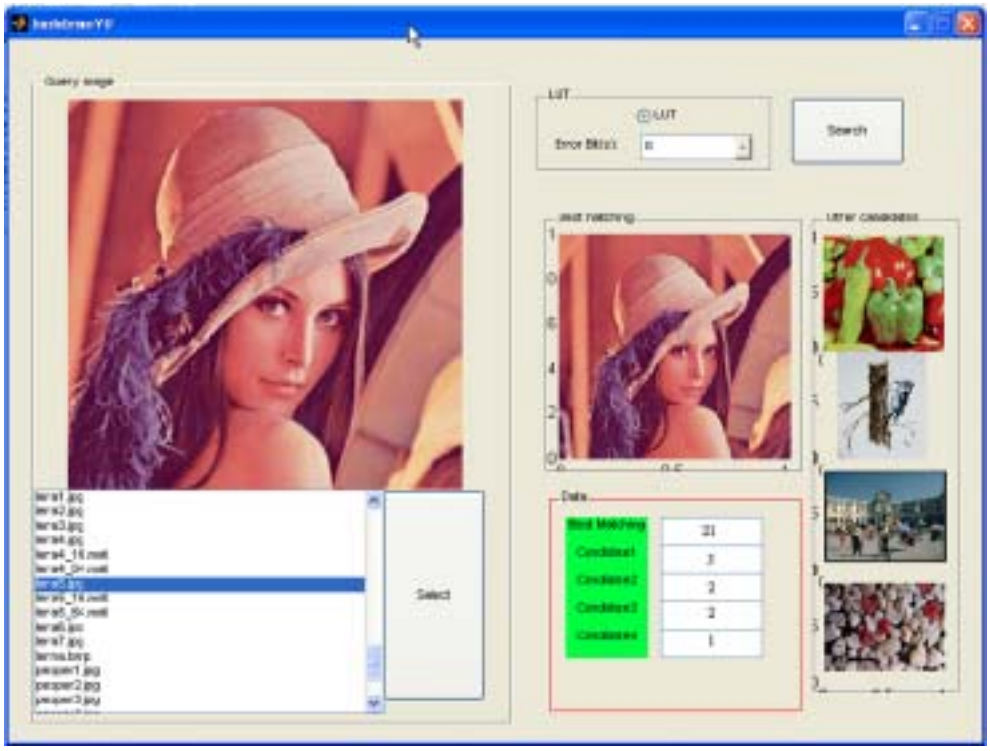
由於多媒體與網路技術快速的發展，使得多媒體資料如影像（image）、視訊（video）、與音訊（audio）等，完整無誤的複製（copy）變得相當容易，再加上網路使用便利的助長，促使非法複製的傳輸更爲快速。爲了追蹤數位內容的未經授權使用，以內容爲主之多媒體搜尋系統，若其目地在從資料庫找尋詢問資料（query content）經必要之非惡意處理（incidental manipulation）（如影像壓縮）或惡意竄改（malicious tampering）（如人臉等物件置換）前之原始版本（original version），則此搜尋系統必須滿足強韌性（robustness）。這就是近來新興的多媒體赫序技術（digital media hashing）或是稱爲多媒體指紋技術（digital media fingerprinting）[1][2][3]，它們在數位資料內容管理領域受到相當重視。多媒體赫序技術可使用於非法複製搜尋（illegal copy detection）、多媒體內容鑑定（content authentication），也可利用於輔助數位浮水印技術（digital watermarking）之著作權保護的互補功能，與使用於分散式視訊編碼（distributed video coding）等許多應用；是一相當重要的核心技術。

所謂多媒體資料（在此以後將以數位影像爲例）的赫序（hash），其定義是把資料量較大（或維度大）的影像應對至資料量較小（或維度小）的特徵向量，此特徵向量須滿足若是相似的兩張影像其赫序需相似，反之亦然。換句話說，影像的赫序代表其內容扼要的本質（condensed essence），具備永久性與唯一性，就好比人類的指紋，可用來達到辨識的功能。更重要的是，一張影像的赫序必須滿足幾何不變性（geometric-distortion invariance）[4]。這是因爲幾何處理並不改變影像內容，這議題也是數位赫序技術研究的高難度問題之一[1]。如圖一所示，圖左與圖中是不同的兩張圖，其所取出的赫序差異越大越好，而圖右是圖中的幾何變形但內容仍維持不變，因此它們的赫序差異越小越好。爲了取出數位影像的赫序，傳統的密碼學赫序函數並不適用，理由是兩張幾乎一樣的影像，即使是僅一個像素（pixel）的灰階度不同，所產生出的赫序也會截然不同。由於密碼學赫序函數的高脆弱性（fragility）不適用於多媒體，我們需依照多媒體資料可接受一定程度的變形與失眞（distortion）這一獨特性質，進而發展多媒體專屬之強韌性赫序（robust media hashing）。



圖一、多媒體赫序之視覺相似性（perceptual similarity）

然而，現有多媒體赫序技術的共同缺點是它們抵抗幾何處理攻擊的能力非常不足，有鑑於此，我們提出一個強韌性影像赫序技術與系統[4]。與現有方法比較，我們的方法是第一個能抵抗知名的攻擊軟體（Stirmark）[5]，展現最強強韌性。圖二是我們的系統從一詢問影像（圖左）搜尋其對應之原始影像（圖中）的結果。



圖二、數位指紋影像搜尋系統[4]

上述所提的是一種利用多媒體的數位指紋達成「以內容追尋內容」的多媒體搜尋技術。另一方面，我們要繼續探討的是，是否可能從數位影像內容去追尋其相機型號，這就好比經由子彈特徵做槍枝識別達成「以彈追槍」。這種數位相機識別技術特別在數位僞造偵測（digital forgery detection）等鑑識科學方面相當有用，並且成爲近年來新興研究的題材[6][7]。尤其，需要把數位圖片在法庭當證物時，資料內容可信度的驗證，與僞造內容的偵測變得相當重要。

近來，有些實例顯示數位內容眞僞的鑑定是相當重要的。例如美國美式足球明星 O. J. Simpson 刑事案件的一張照片，被警方故意加工，把其膚色變黑，並刊登在媒體雜誌上，加深大眾對黑人的偏見。另一近來實例是，美國總統布希在對其軍隊講話的一張照片，被發現某些士兵重覆地出現在照片中，後來也被證實是經由同一照片其它處剪貼複製得到。爲了能驗證數位相片可信度，已有相機國際大廠（如 Kodak 與 Epson）在相機製程當中加入數位浮水印功能。雖然，數位浮水印技術已可達成資料內容可信度的驗證，但由於隱藏浮水印等同事先修改影像內容，這種侵入性性質在法庭上的認同仍有疑義。在此，我們將從數位指紋技術（具非侵入性性質）探討此一問題。我們利用相機在生產過程與拍攝過程所引進的特殊雜訊（noise）當成其特有的「指紋」，而此指紋會伴隨著所拍攝的照片來提供數位內容眞僞鑑定的證據。

目前，已存在一些追蹤數位影像攝影來源的方法，其中最簡單的方式是檢視電子檔本身或其檔頭（header）或者其它附屬資訊，這些通常記錄著照相機型號與當時拍攝條件（如曝光時間等）。然而，這種簡易方法本身存在著資訊易被篡改等可靠性存疑的問題。另一有趣的方法是，利用所謂的「有缺陷的像素」（defective pixel）如 hot pixel 或 dead pixel 做相機辨識。然而，這方法也未必完全可行，尤其，一些相機已使用影像後處理機制去消除有缺陷的像素。

最近，有些研究開始利用相機本身感應器（charge-coupled device （CCD）與 CMOS）所產生的「pattern noise」特性，處理數位相機辨識問題。相機的 pattern noise 是由一些因素產生，如像素的不一致性與光學元件干擾等，且每台相機即使是同一型號，在生產過程中所引進的 pattern noise（或稱爲指紋）也有差異。在這方面，一個共通的做法是，利用數位影像處理的雜訊濾波器，將 pattern noise 擷取出來，再利用圖形識別領域理的分類器（classifier）做相機辨識（當然也對應著照片內容辨識）[8]。

[1] T. Kalker, “Applications and Challenges for Audio Fingerprinting,’’ Proc. 111th AES Convention, in the “`Watermarking versus Fingerprinting” Workshop, December 3, 2001.

[2] *IEEE Int. Workshop on Multimedia Signal Processing (MMSP)*, special session on Media Recognition, T. Kalker and I. Cox (co-organizers), Virgin Islands, USA, 2002.

[3] *IEEE Int. Conf. on Multimedia and Expo*, special session on Media Identification, J. Oostveen, C. S. Lu, and Q. Sun (co-organizers), June 2004.

[4] C. S. Lu and C. Y. Hsu, “Geometric Distortion-Resilient Image Hashing Scheme and Its Applications on Copy Detection and Authentication,’’ *ACM Multimedia Systems Journal, special issue on Multimedia and Security*, Vol. 11, No. 2, pp. 159-173, 2005.(peer-reviewed invited paper)

[5] F. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Attacks on Copyright Marking Systems,’’ *Proc. Int. Workshop on Information Hiding*, LNCS 1575, pp. 219-239, 1998.

[6] P. Blythe and J. Fridrich, “Secure Digital Cameras,’’ *Digital Forensic Research Workshop*, 2004.

[7] M. Kharrazi, H. T. Sencar, and N. Memon, “Blind Source Camera Identification,’’ *Proc. ICIP*, 2004.

[8] J. Lukas, J. Fridrich, and M. Goljan, “Determining Digital Image Origin Using Sensor Imperfections,’’ *Proc. SPIE Electronic Imaging, Image and Video Communication and Processing*, 2005.