Ashwin Swaminathan, Min Wu, and K.J. Ray Liu

元件鑑識技術

理論，方法論及應用

© BRAND X PICTURES

視覺感測器技術在近幾十年中取得了巨大的發展，數位設備變得無處不在。由各種影像裝置擷取的數位影像被大量應用，從軍事和偵察到醫學診斷和消費類攝影產品。因此，在成像技術的快速發展和廣泛應用中，出現了一系列新鑑識問題。例如，不僅可以很容易地查出硬體和軟體元件是什麼類型，而且包括這些設備內部採用的參數嗎？某一幅特定數位圖像是用哪種成像感測器，或哪個品牌的感測器擷取的呢？該圖像是如何擷取的？使用的是數碼相機、拍照手機、圖像掃描器，還是經過圖像編輯軟體合成的呢？擷取此圖像後是否經過了一些操弄？是真實的呢，還是經過了某種方式的篡改？其中是否包含隱藏資訊或者加密資料？許多鑑識問題都與數位圖像的來源及其創建過程有關。得自於這種分析的證據可爲司法、治安和情報機構提供有用的鑑識資訊。瞭解圖像採集技術，也有助於解答關於圖像擷取後，可能經過的附加處理之特質等更爲深入的的鑑識問題。

當前有許多處理這些問題的方法。在本文中，我們將研究主流技術之一：基於*元件鑑識*的技術來解答這些鑑識問題。元件鑑識之目標是識別擷取資料時不同設備元件中之演算法和參數。元件鑑識分析的工作原理是：尋找數位圖像在一系列資訊處理中，經由不同處理塊時所留下的*固有指紋*痕跡，並使用這些痕跡估計元件參數。透過固有指紋的識別建置元件參數分析，元件鑑識爲許多鑑識問題之處理提供一個框架，例如發現設備技術侵權，保護智慧財產權和識別採集設備等等。

數位物件識別碼 10.1109/MSP.2008.931076

1053-5888/08/$25.00©2008IEEE

保護圖像設備的智慧財產權成爲近年來首要關心的事情，電子成像行業的激烈競爭導致法庭上提交侵權案例數量的增加。勝訴方獲取的賠償金額也急速增加，有時高達數十億美金。眾所周知，專利是保護智慧財產權的一種強大工具。然而，隨著現代尖端工具的發展，影像裝置產品的專利侵權變得易如反掌，察覺困難，甚至難以在法庭上舉證。實現侵權分析的一般方法是對產品的設計和實作進行調查，透過若干類型的反向工程尋找該產品與現有專利主張之間的相似性。然而，該方法非常繁瑣和低效，在許多案例中可能包含牽涉調查設備軟體模組中低階組合語言的逐條比對。元件鑑識藉由在一系列資訊處理中每個元件上進行演算法和參數之識別，爲侵權/授權鑑識提供一個系統性的方法論，由而保護智慧財產權。

元件鑑識還提供了用以確定圖像可信度和影像裝置的基礎。隨著操弄多媒體資料工具的快速發展，當圖像在新聞、偵察和司法應用上作爲決定性的證據時，內容和採集設備的完整性就愈形重要。例如，關於設備中硬體/軟體模組及其參數等資訊有助於建立設備的識別系統。這些系統可爲司法和情治機構提供關於採集圖像時所使用的是哪種設備或哪個商標/型號等有用的擷取鑑識資訊。另外，元件鑑識有助於確定一個實體模型，以確定直接從設備擷取之圖像特徵，相應地推動篡改鑑識，進而確定圖像離開設備後是否經過了任何的附加編輯和資料處理。

視可用的輸入之特質而定，元件鑑識主要可在三類情境下進行。在侵入式鑑識方面，鑑識分析者具有取用設備的許可，那麼他/她可拆解該設備，析出每個元件，並提出計算個別元件參數的方法。在半非侵入式鑑識情況時，分析仍然具有取用設備的許可，但不許拆解該設備，那麼他/她可以設計適當的輸入資料輸入設備，以便收集關於處理技術和個別元件參數等鑑識證據。在完全的非侵入式鑑識時，鑑識分析者僅可基於設備的樣本資料進行元件參數的估計。

本文中，我們將用視覺感測器和數碼相機擷取的圖像來論證元件鑑識，此時這些技術將進行適當修改和擴展爲其它類型的擷取模型和感測技術。我們評估了各種相機

元件的參數估計方法。我們展示所計算出的參數可用來估計相機技術的相似性，用來在侵權/授權中提供能說明問題之線索、識別捕捉所討論圖像之照相機類型和品牌/型號，並構建一個真實背景模型來說明對檢測圖像內容的操弄。

數位影像裝置的系統模型

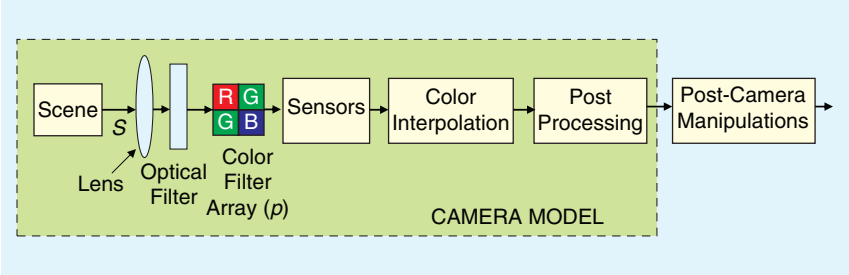
本章節中，我們評述一系列資訊處理中用以測試各種元件的數碼相機之圖像擷取模型。如圖 1 所示之圖像擷取模型，來自場景的光源傳過一個透鏡和光學濾鏡，最終由感測器陣列記錄下來。大多數相機採用彩色濾鏡陣列 (CFA) 捕捉來自真實世界場景的資訊。CFA 是感測器上的一個薄膜，選擇性地允許光源的某個特定成份通過薄膜，到達感測器 [1]。爲了便於討論，定義 S 爲被相機捕捉的真實世界場景，p 表示爲 CFA 模式矩陣。$S(x,y,c)$ 表示一個大小爲 $H\times W\times C$ 的像素值三維 (3D) 陣列，這裡 H 和 W 分別表示圖像的高度和寬度，$C=3$ 表示顏色元件的數目（紅、綠和藍）。CFA 採樣使真實世界的場景轉化爲一個 3D 矩陣 S_p 的形式

$$S_p(x,y,c)=\begin{cases}S(x,y,c) & if\ p(x,y)=c\\ 0 & otherwise\end{cases} \quad (1)$$

在記錄下從 CFA 獲得的資料後，式 (1) 中對應於點 $S_p(x,y,c)=0$ 的中間像素值透過一種眾所周知的處理運算——色彩插值或內插 [2]，利用其鄰域像素值進行插值並得到 $S_p^{(I)}$。插值後，對應於紅，綠，藍元件的三個圖像透過一個後處理階段。在該階段中，各種類型的相機處理運算例如白平衡，色彩校正，顏色矩陣化，伽瑪校正，位元深度縮減，和壓縮可以用來增強整個圖片品質和/或減少儲存空間，生成了最終的相機輸出 S_d。S_d 還可能經過軟體等附加的處理運算，例如，Adobe Photoshop 和 Google Picasa 可以用來進一步提高圖片品質及/或篡改圖像。在圖1所示之系統模型中，我們將攝後處理表示爲附加的操弄塊，如圖1所示。

元件鑑識方法論

正如我們在前一部分系統模型中該討論的那樣，當使用數位相機捕捉真實世界場景時，在最終的數位圖像生成前場景資訊經過了不同的設備元件。該系列資訊處理中的每個



[圖 1] 數碼相機中的資訊處理

元件透過採用特定參數集合的特殊演算法對輸入進行修改，在輸出時留下一些固有的指紋痕跡。在接下來的章節中，我們提出利用固有指紋痕跡的非侵入式技術估計各種相機元件之參數。

相機響應函數的估計

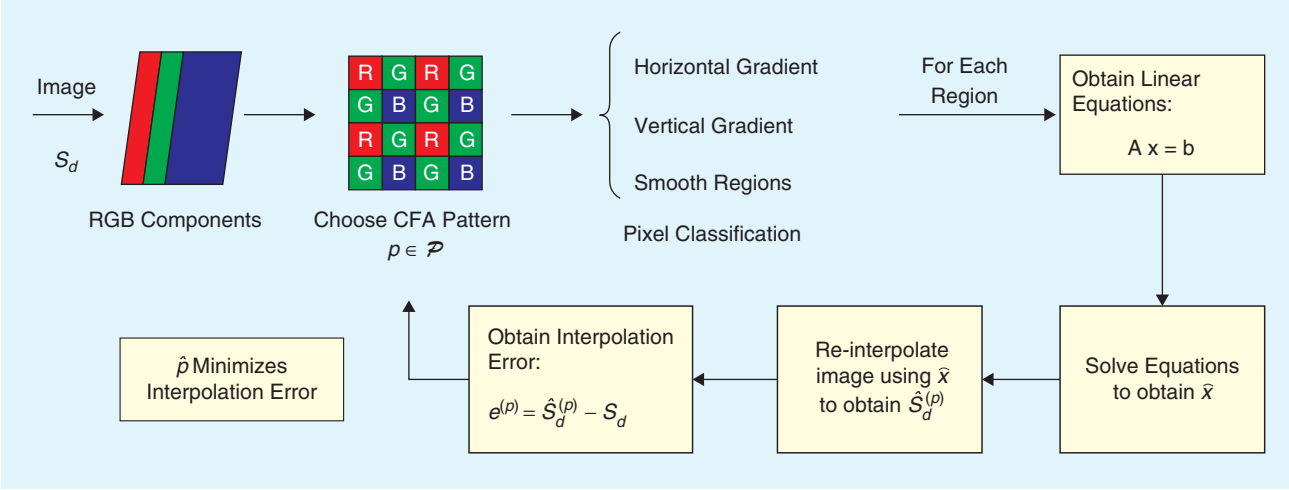
相機響應函數 (CRF) 將入射光能量映射爲圖像強度值 [3]。CRF 的知識對許多應用都非常有用，例如，利用陰影和光度立體進行銳化的電腦視覺演算法，另外在認證演算法中，可用 CRF 做自然浮水印。基於單個相機輸入的 CRF 估計是一個約束不足問題，因此大部分的前期工作是透過假設一個特定非線性模型估計 CRF。在文獻 [4] 中，Farid 假設 CRF 可以寫成 $f(r) = r^{\gamma}$ 的形式，其中 r 和 $f(r)$ 分別表示入射光能量和圖像強度值，γ 是轉換參數。Farid 提出，轉換形式 r^{γ} 在頻域中引入相關性，這可用相干分析計算（三階統計特性），無須瞭解影像裝置的詳情 [4]。儘管此相干分析方法能夠在 7.5% 的平均準確率內估計出 γ 值，該方法受到使用 γ-curve（γ 曲線）CRF 模型的限制，這對於真實世界的 CRF 遠遠不夠。

在文獻 [5] 中，透過測算圖像經邊緣色彩分佈後非線性響應效果，Lin 和 Zhang 提出了一種從單獨的紅綠藍 (RGB) 顏色圖像估計 CFR 的方法。作者假設邊緣像素是線性混合的，同時引入一種計算逆輻射響應的方法，將邊緣色彩的非線性分佈映射到線性分佈。實驗結果證明，估算的逆回應曲線的平均均方根誤差 (RMSE) 大約爲 10^{-2}。文獻 [6] 將該方法進一步推廣到灰階圖像中，藉由利用沿圖像邊緣的更高階分佈特徵，得到兩個相機裝置的 RMSE 接近 10^{-2}。Ng 等人在假設 CRF 函數服從一個一階廣義 Gamma 曲線模型 [3] 的條件下，研發了一類有約束方程以識別潛在的局部平面輻照度點，再利用這些點估計 CRF。作者將模擬擴展到五種相機型號，驗證估計演算法之良好性能，該方法用於單幅圖像時，CRF 估計得到的平均 RMSE 接近 10^{-2}，但 RMSE 隨著額外的相機輸出增加而降低。

彩色濾鏡陣列和色彩插值參數

對於 CFA 和色彩插值模組這些元件而言，元件輸出的知識提供關於輸入的完整資訊，因爲輸入和輸出分別對應著採樣和插值資料 [7]。Popescu 和 Farid 採用期望最大 (EM) 演算法來估計鑑識分析中的色彩插值係數。作者先假設圖像像素隸屬於以下兩個模型之一：1) 像素點與其鄰域線性相關，可由一個線性插值演算法獲取，或者 2) 像素點與鄰域不相關。基於此假設，作者提出了兩步 EM 演算法估計 CFA 係數[7]。在 E 步驟時，估計出每個樣本歸屬於兩個模型的機率，在 M 步驟找出相關性的確定形式。EM 演算法生成兩個輸出：表示像素歸屬於兩個模型可能性的二維機率分佈圖和加權係數。作者透過模擬結果表明，估算的機率分佈圖能有效用於檢測彩色圖像是否經過色彩插值的結果，色彩插值係數則有助於區分不同的插值演算法 [7]。

Swaminathan 等人提出了將估計彩色濾鏡陣列模式和色彩插值係數相結合的演算法 [8]。該方法原理如圖 2 所示。首先基於數碼相機設計中常見操弄確定一個關於 CFA 模式的搜索空間 $\mathcal{P}$，同時觀察到大部分採用 RGB 型 CFA 的商業相機所具有的固定週期爲 2x2。對於搜索空間 $\mathcal{P}$ 中的每一個 CFA 模式 p，在不同類型之紋理區域中，透過線性模型擬合獨立計算插值係數。具體而言，基於局部鄰域的梯度特徵，將圖像劃分成三類區域，位置爲（x, y）的圖像像素被



[圖 2] 彩色濾鏡陣列的估計演算法和色彩插值係數

歸類爲三個區域之一：區域 $\mathcal{R}_1$ 包含具有顯著水平梯度的圖像部分；區域 $\mathcal{R}_2$ 包含具有顯著垂直梯度的圖像部分，$\mathcal{R}_3$ 包含圖像的剩餘部分，主要包含光滑區域。

利用最終的相機輸出 S_d 和假定的樣本模式 p 直接從感測器陣列擷取的 S_d 中像素位置集合，和被插值之像素位置集合進行識別。對於色彩插值而言，在每個三類區域 $\mathcal{R}_m(m=1,2,3)$ 和圖像的三個彩色通道 (R, G, B) 上假定存在一個線性模型，插值的像素可以表示爲像素之加權平均，假定這些像素能直接從感測器擷取。由求解這些方程來獲得係數之權值。假設 N_e 方程組中對於一個特定區域 N_u 未知，色彩通道表示爲 **Ax=b**，其中 **A** 的大小是 $N_e \times N_u$，**b** 的大小是 $N_e \times 1$，分別指定可直接擷取的像素值和那些所插值的像素值。**x** 大小是 $N_u \times 1$，代表估算的插值係數。爲了處理由於插值後的其它機內運算(例如 JPEG 壓縮)而造成的 **A** 和 **b** 中可能存在的雜訊像素值，用奇異值分解 (SVD) 估計插值係數 [8][9]。得到係數後，用其對相機輸出 S_d 做二次插值，以得到 $\hat{S}_d^{(p)}$，並計算誤差項 $e^{(p)} = \hat{S}_d^{(p)} - S_d$。對於搜索空間 $\mathcal{P}$ 的所有模式 p，重複實施這些步驟，插值誤差最低的模式被選爲 CFA 的估計。在此過程中，同時獲得與估算的 CFA 模式相對應的插值係數。更多的細節請參閱文獻 [8]。

後插值處理估計

此處理運算是相機在色彩插值後完成的如白平衡和色彩校正等，確保場景中的白色物體在一幅照片中呈現白色。白平衡運算是典型的乘法運算，照片中的每種色彩都乘以一個在相機色彩空間中經適當選擇的常數。由於白平衡運算的乘法性質，非侵入而僅基於單個相機的輸出，無法精確地估計這種運算 [10]。然而，這種運算可以透過半非侵入式的兩步方法來估計，首先得到在不同內置白平衡設置下的兩個圖像，然後藉由求解一組方程，利用 Von-Kries 假設推導 [10]。

JPEG 壓縮是數碼相機中流行的另一種後插值處理元件。JPEG 壓縮被看做是在離散餘弦變換 (DCT) 域的量化。在這種情況下，元件輸出的知識不能提供對應於輸入之完整資訊；但有提供量化步長範圍內輸入之粗略估計。文獻 [11] 和 [12] 利用基於像素合併技術統計分析進行量化矩陣的非侵入式估計。已經過論證，這些演算法在圖像的低頻，水平和垂直方向的高頻子帶之量化步長估計方面具有較好的準確性，這些子帶中非零量化值相當多。在對角方向子帶上，量化爲零的係數個數眾多，則導致較大的估計誤差。

元件鑑識之應用

我們現在考慮元件鑑識的一些應用，留在數位圖像上的固有指紋痕跡提供解密線索，有助於解答關於數位圖像之原始性和真實性的許多問題。

相機識別鑑識

估算的相機元件參數將被用作相機識別鑑識的特徵，用來鑒別採集數位圖像的相機品牌和型號。Bayram 等人提出一種相機識別方法 [13]，該方法採用 EM 演算法中的加權係數 [7] 和機率分佈頻譜的尖峰之位置及數量作爲特徵。從輸入條件受約束的兩個相機中擷取的圖像，與從網際網路上隨機擷取的圖像一起用於實驗，作者提出三個品牌做實驗時準確率接近 84%，其中 20% 的圖像用於訓練，剩餘的 80% 用於測試 [13]。文獻 [14] 是該方法的進一步改進，分別考慮圖像之光滑和非光滑區域，對於三種相機品牌分類的準確率達到 96%。

Swaminathan 等人在文獻 [8] 中提出了一種結合 CFA 模式和插值演算法的估計技術，用於相機鑑識，針對 19 種不同相機型號，提出對更大資料庫所進行的大量相機識別結果。實驗中包含的相機型號目錄如表 1 所示。對於資料庫中 19 種相機型號的每一種，作者搜集大約 200 幅不同的 512x512 圖像，都是在無約束條件下的不同場景、不同照明環境和不同 JPEG 品質因數的壓縮。根據品牌或型號將資料庫中的這些圖像分爲不同的組別，每類區域和色彩通道（每幅圖像共有 441 個係數）所估算的 7x7 大小的濾鏡係數被用於相機識別。透過模擬，作者印證了九種不同相機品牌分類的平均識別準確率約爲 90%，對於來自九種不同品牌的不同圖像從19種相機型號之間區分的識別準確率則接近86%[8]。此外，作者論證了這些結果不受相機內的後插值處理運算的影響，比如 JPEG 壓縮，加性雜訊和非線性點運算諸如伽瑪 (Gamma) 校正 [8]。

在數量更大和種類更多的資料庫方面，相較於其它關於相機識別的研究，文中的元件鑑識技術具有更高的準確率

[表 1] 文獻[8]的實驗中採用的相機型號

NO.	CAMERA MODEL	NO.	CAMERA MODEL	NO.	CAMERA MODEL
1	CANON POWERSHOT A75	8	NIKON E5400	15	CASIO QV 2000UX
2	CANON POWERSHOT S400	9	SONY CYBERSHOT DSC P7	16	FUJIFILM FINEPIX S3000
3	CANON POWERSHOT S410	10	SONY CYBERSHOT DSC P72	17	FUJIFILM FINEPIX A500
4	CANON POWERSHOT S1 IS	11	OLYMPUS C3100Z/C3020Z	18	KODAK CX6330
5	CANON POWERSHOT G6	12	OLYMPUS C765UZ	19	EPSON PHOTOPC 650
6	CANON EOS DIGITAL REBEL	13	MINOLTA DIMAGE S304		
7	NIKON E4300	14	MINOLTA DIMAGE F100		

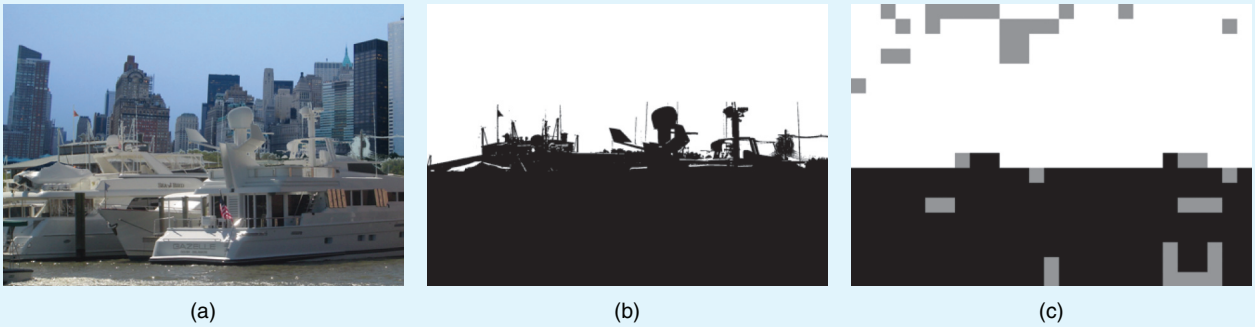
[15]–[17]；其後，該技術推廣到照相手機上，達到了 98% 的準確率 [35]。Kharrazi 等人在文獻 [15] 中關於相機識別提出了一組 34 個特徵的集合，目的是對數碼相機中的圖像擷取過程建模。特徵集包括：平均像素值、RGB 兩者間的相關性、鄰域分佈重心、RGB 能量比率、小波域統計量 [18]，以及圖像品質度量 [19]。作者採用支撐向量機 (SVM) 演算法進行分類，當測試圖像來自 3 種品牌的 5 種相機型號的有約束條件輸入下時，公佈其準確率接近 88%。在文獻 [16] 中也在相機識別中使用相同的特徵集，對於在受控輸入條件下來自兩種不同模型的四種相機型號，得到的準確率接近 95%。另一個關於相機識別的研究工作是估算像素之非均勻雜訊，這是圖像非均勻光電響應雜訊之主要分量，是圖像感測器所必然產生的，可用於區別兩個相同品牌，型號和裝置的相機。在演算法的訓練階段，採用一種基於小波去噪演算法取得像素非均勻雜訊估計，該雜訊的隨機分量可藉由平均許多圖像的估計予以消除。在測試階段，判斷某一幅特定圖像是否爲某一特定數碼相機所採集，要獲得圖像的雜訊頻譜，並與某特定數碼相機的平均雜訊頻譜（也叫做參考頻譜）求相關。相關值大於所預選的閾值表示某特定圖像是來自某特定數碼相機的。作者展示了當採用高品質圖像做測試時，該方法能以 100% 的準確率識別相機之來源。Dirik 等人提出了一種透過粉塵特性識別數碼單反相機 (SLR) 的方法 [20]，對三種不同品牌相機的準確率接近 92%。其針對相機識別的研究工作，重點在於典型特徵的提取，但無法對系列資訊處理的不同元件進行明確的估計。

侵權和授權鑑識分析

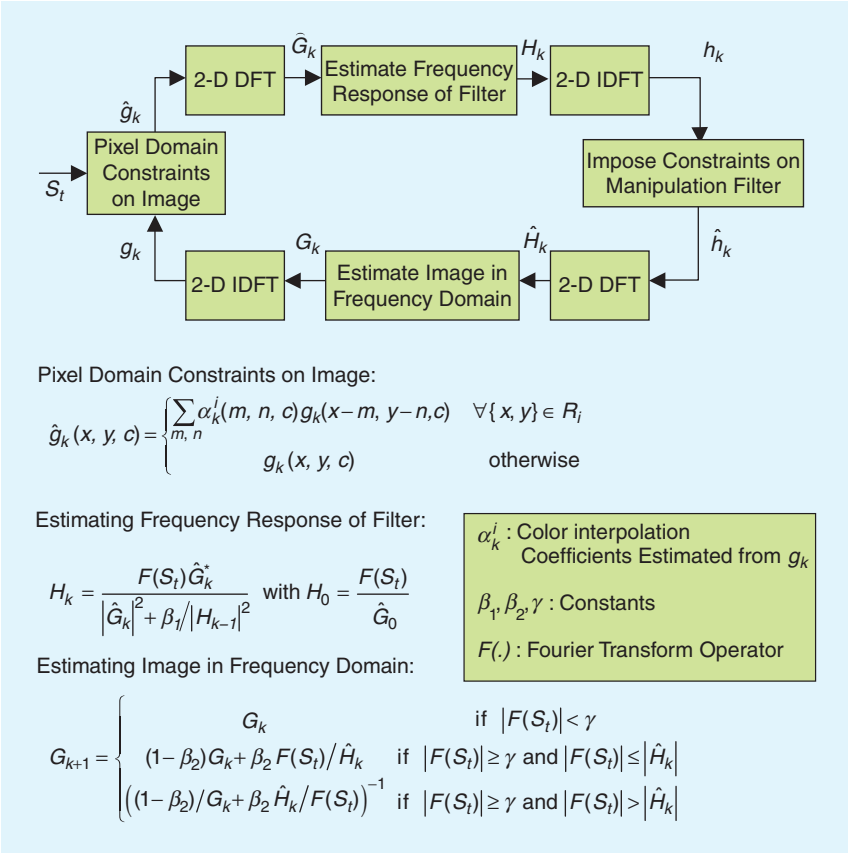
元件鑑識分析可用來做與影像裝置關聯的共同特徵識別，適合應用於設備元件侵權和授權識別。在文獻 [8] 中，將一種基於分類的方法用於不同相機所使用的插值演算法之間之相似性研究。作者首先透過從資料中刪掉一種相機型號來訓練分類器，再用刪掉的相機係數對其測試，以找出色彩插值係數空間上的最近鄰域。文章的實驗結果表示，當 SVM 採用來自 18 個相機的 200 幅圖像做訓練(其中不包括Canon Powershot S410)，再使用來自 Canon Powershot S410 的 200 幅圖像做測試時，Canon Powershot S400 圖像的分類準確率爲 66%。此外，剩餘圖像的 28% 被分類爲 Canon 型號的一種；這意味著不同型號但品牌相同在的相機使用這類插值演算法時，存在極大相似性。文獻 [8] 中的結果表明 Minolta DiMage S304 和 Nikon E4300 之間存在相似性，在分類測試時，約爲 53% 的 Minolta DiMage S304 圖片被認爲是 Nikon E4300 型號。基於這些結果，可定義一種新度量標準來研究兩個相機品牌/型號之間的相似性 [8]。該分析可在估算相機元件參數中的識別相似性方面有所應用，用於確定潛在的侵權或授權。

基於元件參數中不一致性的剪貼鑑識檢測

用剪貼僞造建立的篡改圖像常包含從不同相機擷取的圖片中選取圖像的不同部分，這些相機的內部元件可能採用不同的演算法/參數集合。從不同圖像區域獲得的、估計出來的感測器模式雜訊之間的不一致性 [17]，或者估計出來的相機元件之固有指紋痕跡間的不一致性（例如色彩插值係數 [21] 或 CRFs [22]），可用於識別如剪貼這類的數碼僞造操弄。在本文中，我們以文獻 [21] 所提出的研究實例來做論證。在文獻 [21] 中，作者建立一幅大小爲 2048×2036 的篡改圖片，這是由使用兩種不同相機所獲得的兩幅圖像經部分組合而得到的。圖 3(a) 和 (b) 分別提出該幅篡改圖像並標記了不同色彩的個別部分。圖 3(b) 中呈現在白色的區域取自於 Canon Powershot S410 數碼相機所拍攝的圖像，黑色部分是 Sony Cybershot DSC P72 型相機所攝的圖片裁



[圖 3] 來源鑒定之應用 (a) 篡改的圖像樣本，(b) 從兩個相機擷取的區域 (c) CFA插值識別結果(黑色：Sony Cybershot DSC P72；白色：Canon Powershot S410；灰色：分類為其它相機的區域)



[圖 4] 用以估算操弄濾波器係數的反覆運算約束增強演算法 [24]

剪和粘貼而成。合成的圖像經過了品質因數爲 80% 的 JPEG 壓縮。

爲了在圖片的不同部分上識別其固有的相機指紋，利用一個步階爲 64x64，大小爲 256x256 的滑窗進行圖像測試，估計每一個 256x256 塊內的色彩插值係數 [21]。19 個相機型號分類器的檢測結果如圖 3(c) 所示。圖中標記爲黑色的區域表示那些被分類爲 Sony Cybershot DSC P72 機型，而白色區域則相對應來那些被正確分類爲 Canon Poweshot S410 機型的部分。用灰色表示的剩餘區域對應於那些被錯誤分類爲剩下 17 個機型中一種的圖塊。正如圖 3(c) 所示，結果表明在篡改圖像的大部分區域內，利用 256x256 大小的巨集區塊擷取的資料可以識別出正確的相機，並且具有較高可信度。

在上述特例中，被操弄圖像具有來自兩個不同相機的明顯痕跡，因此是被篡改的。

用作篡改檢測中真值建模的元件鑑識

攝後處理運算包括內容保留和內容修改操弄，例如篡改。攝後處理通常難以檢測和估計，由於缺乏關於操弄種類的知識，這導致對模型的不當選擇。爲了避免此問題，一些關於篡改檢測的早期文獻試圖透過從經歷的失真這種形式來定義操弄後的圖像特性以檢測篡改，利用該分析提出了用於檢測操弄後的圖像和識別操弄種類及其參數。在文獻 [18] 和 [23] 中，採用基於變異數分析方法 [23] 和高階小波統計量 [18]的特徵檢測圖像的操弄是否存在，但沒有關注於識別操弄種類和/或其係數等方面。這些方法用於分類時需要篡改後的圖像樣本(針對每種操弄)，從真正的相機採集圖像中區分這些操弄過的圖像。另外，這些圖像並不能有效識別操弄的種類，因爲構建分類器時並沒有對其建模或直接考慮在內。

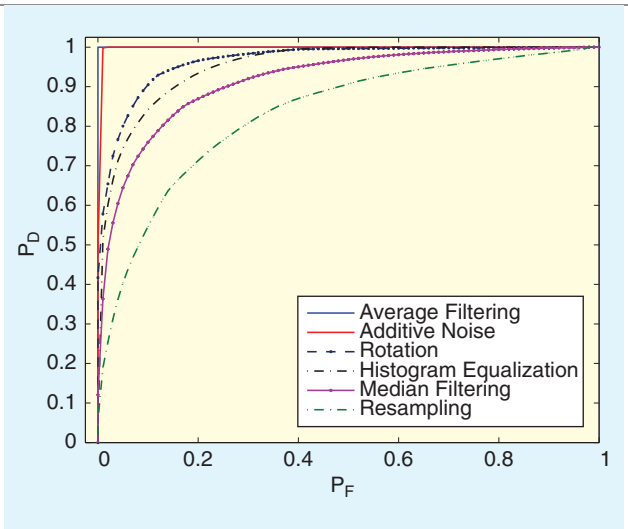
在文獻 [24] 中，作者透過把所有攝後處理作爲一個操弄塊進行建模，將元件鑑識方法推廣到用於識別圖像操弄的存在與否 [24]。該演算法首先假設某特定測試圖像，S_t 是操弄過的相機輸出，由實際的相機出 S_d 經過一種操弄運算得到。任何應用在 S_d 上的後相處理這時都可作爲某種線性濾波器進行建模，其係數可用反覆運算的約束增強演算法估計 [24]。圖 4 提出了文獻 [24] 中用來估計操弄濾波器的係數之演算法原理圖。測試圖像 S_t 則用於反覆運算過程的初始化。對每一反覆運算，對圖像和濾波器在像素域及傅立葉域中反覆地運用已知的約束條件，以更新所估計的相機輸出 g 和濾波係數 h [25] [26]。在第 k 次反覆運算時，對圖像 g_k 施加像素域約束條件以得到 $\hat{g}_k$；像素域約束條件代表相機約束條件，這裡相機元件參數 α_k^i 可以透過章節“彩色濾鏡陣列和色彩插值參數的估計”中的元件鑑識技術估計。在獲得圖像 $\hat{g}_k$ 後，對其做

[表 2] 實驗中包含的篡改運算

MANIPULATION OPERATION	PARAMETERS OF OPERATION	THE NUMBER OF IMAGES
SPATIAL AVERAGING	FILTER ORDERS 3-11 IN STEPS OF TWO	5
MEDIAN FILTERING	FILTER ORDERS {3, 5, 7}	3
ROTATION	DEGREES {5, 10, 15, 20}	4
RESAMPLING	SCALE FACTORS {0.5, 0.7, 0.85, 1.15, 1.3, 1.5}	6
ADDITIVE NOISE	PSNR 5 DB AND 10 DB	2
HISTOGRAM EQUALIZATION		1
TOTAL		21

離散傅立葉變換 (DFT) 以得到 G_k。所估計的操弄濾波器之頻率回應可由 $\hat{G}_k$ 和測試圖像的傅立葉變換 $\mathcal{F}(S_t)$ 而得，記爲 H_k，如圖 4 所示。所估計的回應 H_k 進行反傅立葉變換可得到 h_k，爲獲得 $\hat{h}_k$ 而施加給 h_k 的濾波器約束條件是 h_k 的實部存在。最終獲得的 G_{k+1} 值是一個雙變數估計的函數形式：a) 當前的 G_k 值和 b) $\mathcal{F}(S_t)/\hat{H}_k$，其中 $\hat{H}_k = \mathcal{F}(\hat{h}_k)$。該演算法的完整細節及其性質參見文獻 [24]。來自恒等變換估計的操弄濾波器參數偏差可以透過相似性值衡量，這表明在相機擷取後測試圖像已經過某些的操弄。

在文獻 [24] 中，作者採用來自 9 種不同相機型號的資料（對應的機型編號是表 1 中的 1-7、10 和 16）用於測試反覆運算的約束增強演算法。這裡提出了在相機圖像庫中 900 種不同的 512×512 圖像，每個相機型號具有 100 個圖像。這些圖像經過處理加工，每個圖像生成 21 種篡改版本，共獲得 18,900 幅操弄過的圖像。表 2 中列出了考察的操弄種類及其參數設置。對於每一種直接的相機輸出及其操弄過的版本，計算估計的操弄濾波器的頻域係數 H_t，與選擇的參考型號 H_{ref} 之間的相似度，使用一種相似性值來定義。真實的相機輸出的參考型號 H_{ref}，在訓練階段可利用同樣的反覆運算約束增強演算法優先獲得，有助於抵消相機內的後插值處理產生的較小誤差。爲了計算相似性值，得到的測試圖像頻

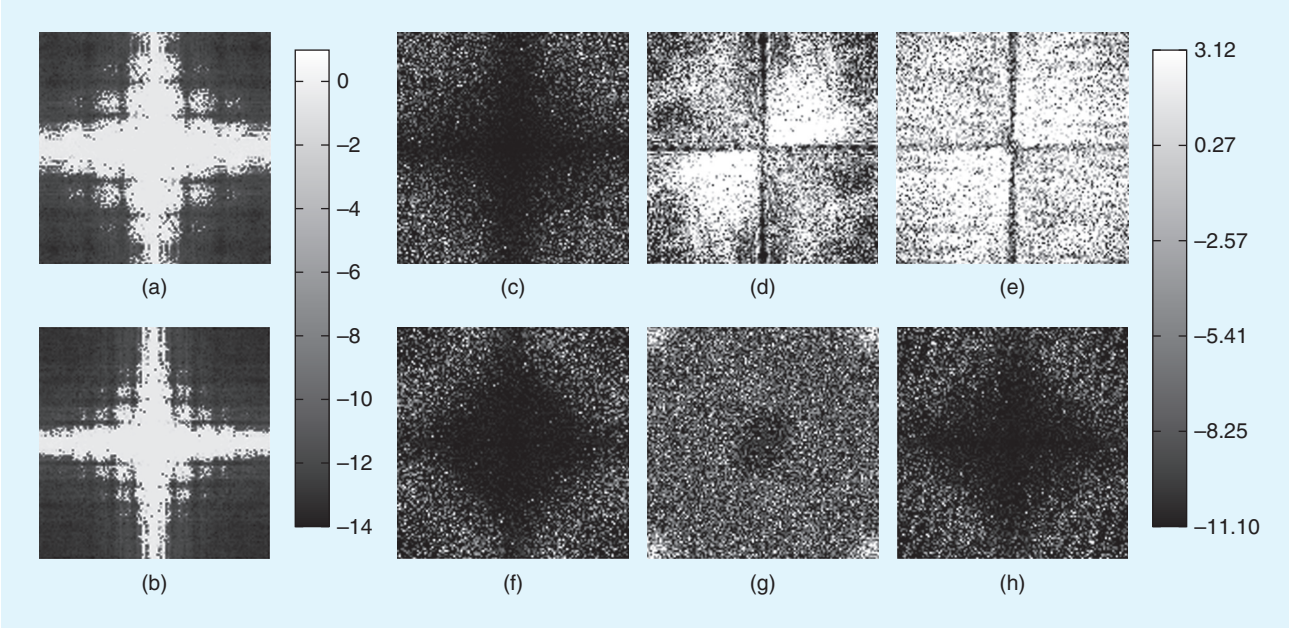


[圖 5] 關於篡改檢測的接受者操作特徵 (ROC)，這時測試物件是資料庫中所有圖像，其中 200 幅圖像用來訓練。

率回應幅值的對數函數 $\Theta_t = \log_{10}(|H_t|)$，與參考圖像的對數幅度係數之間相似性計算如下：

$$s(\Theta_t, \Theta_{ref}) = \sum_{m,n} (\Theta_t(m,n) - \mu_t) \times (\Theta_{ref}(m,n) - \mu_{ref})$$

這裡 μ_t 表示 Θ_t 的像素級均值，μ_{ref} 表示 Θ_{ref} 的像素級均值。假如與參考型號的相似性大於適當選定的閾值，則測試的輸入則被分類爲未經操弄的。另一方面，假如輸入圖像經過了篡改或加密寫入運算，估算的操弄濾波器係數應包含這些操弄的影響，因此與參考型號(從一個未經操弄的相機輸出得到)之間的相似度會減少，這樣會導致相似性



[圖 6] 對相機輸出的操弄濾波器頻率回應 (a) 7×7 均值濾波器，(b) 11×11 均值濾波器,，(c) 7X7 中值濾波器，(d) 20 度旋轉，(e) 70% 重採樣，(f) 130% 重採樣，(g) 雜訊加至 PSNR20dB，(h) 長條圖均衡化。頻率回應在 log 尺度上展示和移動，以便 DC 分量處於中心。

值將低於選定的閾值。圖 5 以接受者操作特徵 (ROC) 的形式提出了反覆運算條件增強演算法的性能。圖中顯示，在 P_F 接近 10% 的情況下，對於諸如空域求平均和加性雜訊等操弄，P_D 接近 100%，對於中值濾波，長條圖均衡化和旋轉則約為 70%~80%。

在文獻 [24] 中，作者利用估算的操弄濾波係數識別攝後處理運算的種類和係數。圖 6 提出了對於表 2 中不同種類的操弄，所估計的操弄濾波係數之頻率回應。仔細觀察頻域中的操弄濾波器係數，可看出不同類型的篡改操弄間有明顯區別。對於一些如均值濾波的操弄，可在頻譜上觀察到明顯的空白，這些空白的間隙可以用來估計均值濾波的階數及其參數。例如加性雜訊這樣的圖像操弄會導致在操弄濾波器中具有一個雜訊譜如圖 6(g) 所示，雜訊強度可由濾波係數計算而來。旋轉和向下採樣可以由操弄濾波器頻譜 LH 和 HL 子帶上較小的值識別。近年來，Chuang 等人 [27] 在文獻 [24] 基礎上提出了許多種類的線性移不變 (LSI) 和非 LSI 影像處理運算，例如重採樣，JPEG 壓縮，和非線性濾波，在它們的經驗頻率回應 (EFR) 中展現了一致和獨特的圖譜。在用做六類操弄分類時，對基於 EFR 的操弄種類，識別性能大約為 93%。

通用隱藏分析和圖像擷取鑑識之應用

就通用隱藏分析和圖像擷取鑑識分析而言，其共同挑戰就是如何對真實的原始圖像資料進行建模。使用一個相機型號及其元件分析，元件鑑識可以提供一個框架來區分相機擷取圖像和具有加密隱藏資訊的圖像或其它方式擷取的圖像 [24]。圖像插值，例如浮水印和加密，可被建模為一種後處理操弄並應用於相機輸出，由反覆運算約束增強演算法估計出的操弄係數可用來將其與真實資料做區分。由其它類型之擷取來源生成的圖像會導致操弄濾波器與期待得到相機輸出的理想 delta 函數明顯不同，該圖像可藉由對比操弄濾波器係數和從相機輸出直接得到的參考型號來區分。其它細節請見文獻 [24]。

元件鑑識的理論分析

正如先前章節所述，經過影像裝置的不同元件後，其固有指紋痕跡留在最終的數碼照片上，可用作證據來估計元件參數並提供線索，以解答關於數位資料之原始性和真實性等鑑識問題。然而，由於固有指紋痕跡經過系列資訊處理之不同部分，因此其中的一些可能已經改變或者損毀，而另外一些又重新生成。這引發了許多基本問題，例如什麼元件痕跡丟失或者改變了？哪些元件在系列資訊處理中可識別而哪些又不是？一個元件的可識別性會如何影響另一個的估計？關於元件鑑識之理論框架在文獻 [28] 和 [29] 中提出，它們關注於解答此類問題及測試元件參數能被識別或者精確分類之條件。下面，我們將總結該工作的主要結果。

理論概念和框架

在文獻 [28] 和 [29] 中，作者定義了元件做為系列資訊處理之基本單元，將設備表示為 N_c 個元件的串聯，寫成 $\{C_1, C_2, \ldots, C_{N_c}\}$ 的形式。作者將系統的第 k 個元件 C_k 所採用的參數集合記為 θ^k，元件鑑識分析之目標即根據元件參數 θ^k 的可識別性或者可分類來定量。關於 θ^k 作者考慮了兩種可能情境。在第一種情況下，作者假定演算法空間關於 θ^k 之可能集合為事前已知，也就是說 $\theta^k \in \Theta^k = \{\theta_1^k, \theta_2^k, \ldots\}$。在這種情況下，此問題轉化為一個分類問題，可以用模式分類方法分析該情境 [28]。在第二種情境下，假設關於可能演算法空間的知識並非事前已知，或者不是假定的事前機率，作者提出了一個基於估計理論和 Fisher 資訊的框架分析此情況 [29]。

若 θ^k 取機率有限的值，這樣 $\theta^k \in \Theta^k$，對於該情境，作者定義元件 C_k 為侵入可分類 (i-classifiable) 的條件為：對所有輸入，利用正確演算法進行分類可侵入分類或者說是 i-classifiable，把元件分類到利用正確演算法，在某特定輸入和輸出的情況下，其機率大於或等於將其錯分到其它類別之機率。此外，對於至少一個輸入 x^* 及其相應輸出，正確分類之機率完全大於錯分機率[28][30]。在這種情境下，參數識別演算法的優勢是在作出正確判斷時可以根據置信度衡量，可被定義為做出正確判斷之可能性和做出錯誤判斷相應之最大可能性之差。如此這般，對於正確判斷 θ^k 的置信度 $\gamma_i^k(x)$ 可以寫為：

$$\gamma_i^k(x) = f(\theta_i^k \mid y, x) - \max_{\theta \in \Theta^k \setminus \theta_i^k} f(\theta \mid y, x)$$

這裡 $f(\theta \mid y, x)$ 表示元件在輸入為 x，相應的輸出為 y 之條件下，元件採用參數 θ 的機率

置信度 $\gamma_i^k(x)$ 是一個輸入為 x 的函數，可以透過選擇合適的輸入將其提升。例如，考慮一個具有參數 $\{\xi_0, \xi_1\}$ 的元件做例子，其輸入和輸出由以下關係提出：

$$y(n) = \xi_0 x(n) + \xi_1 x(n-1)$$

設 $x^{(1)} = [\ldots, 1, 1, 1, \ldots]$，$x^{(2)} = [\ldots, 0, 1, 2, \ldots]$ 是系統的兩個可能輸入。相應對的輸出分別是 $y^{(1)} = [\ldots, \xi_0 + \xi_1, \xi_0 + \xi_1, \xi_0 + \xi_1, \ldots]$ 和 $y^{(2)} = [\ldots, -\xi_1, \xi_0, 2\xi_0 + \xi_1, \ldots]$。請注意，$y^{(1)}$ 是

一個常數序列，每個元素都是等於 $\xi_0 + \xi_1$ 的，該和式不能提供關於參數 ξ_0 或 ξ_1 的任何提示。因此，對於元件值的估計而言，$x^{(1)}$ 並不是較好的輸入。另一個方面，觀察系統的輸出 $y^{(2)}$，可以表示爲一個線性方程的系統以計算 ξ_0 或 ξ_1 值，因此，$x^{(2)}$ 是可以得到元件參數值的較好輸入。本例說明了參數估計中的置信度可以透過輸入的選擇來提高，將該結論推廣，文獻 [28] 定義了使置信度達到最高的最佳輸入。

在文獻 [28] 中，半非侵入式可分和完全非侵入式可分元件的定義相似，這些定義有利於確立一些理論成果。例如，作者已證明假如一個元件是非侵入式可分的，然而其參數可以被半非侵入式識別，假如一個系統是半非侵入式可分的，那麼其每個元件也是侵入式可分的。另外，利用半非侵入式分析得到的平均置信度值都高於或等於那些透過完全非侵入式分析得到的結果，低於那些透過侵入式分析所得的結果。此結果是因爲半非侵入鑑識對鑑識分析提供更多的控制，因此可以設計更好的輸入以提高整體性能，侵入分析在實驗裝置上提供最高的控制。理論上的結果也已驗證當且僅當系統的所有元件都一致時，侵入式，半非侵入式和完全非侵入式鑑識可以提供相同的置信度，這意味著輸入的知識可以提供關於輸出的全部資訊，反之亦然[28]。

圖像採集技術的知識同樣有助於進一步解答鑑識問題，此問題是關於圖像擷取後可能經過的附加處理的性質

在第二個情境下，如果關於可能演算法空間的先備知識不存在，那麼元件鑑識問題就變成一個估計問題，估計偏差和估計變異數作爲理論上的分析度量，這部分內容在文獻 [29] 中有所討論。對於這類情況，透過半非侵入式分析得到的元件參數估計誤差小於透過完全非侵入式分析所得的結果，而大於侵入式分析所得結果，對於一致元件，這些分析技術是等價的。定義和原理的細節及證明示意圖如文獻 [29] 所示。

數碼相機之實例研究

我們現在考察一些實例研究以論證理論框架的實用性

- 彩色濾鏡陣列和色彩內插模組：在存在雜訊或者附加的處理時，對於諸如 *CFA* 和色彩內插模組這類元件，元件輸出的知識提出了關於對應輸入的完整資訊，因爲輸入和輸出分別對應著經過採樣和插值的資料。因此，在該情境下，*CFA* 和色彩內插模組皆爲一致的元件。早先提出的理論分析已經證明半非侵入式鑑識可以提供與完全非侵入式鑑識同樣的準確率，也就是說，即使在輸入條件受約束，以及輸入需精心設計的情況下，元件估計的準確率不能提高到與非侵入式分析相提並論。

  然而，存在附加的後插值處理運算時，元件就不再一致，半非侵入式鑑識可以提供優於完全非侵入式鑑識的準確性[28][29]。該情況下，爲半非侵入式鑑識設計基於這些元件共同知識的良好的測試條件和啓發式模式[10]，這些將被進一步優化[28][29] 以便於爲參數估計提供更佳置信度和準確性。
- 後插值處理模組：諸如白平衡和色彩修正等運算，實際上都是典型的乘法運算。由於其乘法特性，皆不是非侵入式可分的 *[10]*，例如某個特定兩項乘積形式的輸出，那麼不能把單個的項式分別地明確解析。在該情境下，作者提出了相機輸入的知識，有助於處理該問題，半非侵入式分析被用以參數估計並具有良好的準確性 *[10]*。
- 後-相機處理模組：許多後-相機處理模組可以透過理論框架進行類似地分析。爲了實施非侵入式估計，一些文獻提出了這種後-處理運算的方法，例如重採樣 *[31]*，不規則雜訊頻譜 *[32]*，亮度或照明方向 *[33]*，色差*[34]*，非線性點運算，和伽瑪 *(Gamma)* 校正 *[4]*。例如，當圖像上採樣時，一些像素點值從較小的圖像直接獲得，留下的像素則藉由插值擷取，因此與其鄰域高度相關。這樣，重採樣參數可以由對特定範圍內重採樣像素值引入的相關性研究來識別 *[31]*。諸如對比度變化，伽瑪 *(Gamma)* 校正和其它圖像非線性化等影像處理可以被建模，更高階的統計例如雙頻譜可以被用於識別其元件參數 *[32]*。其中的一部分方法假定關於可能演算法空間的先備知識，需要對所有機率進行徹底搜索。

本章節考察的理論分析框架可以提供系統方法論用於解答系列資訊處理中哪些元件和處理運算是可識別的或者是不可識別的，這將有助於量化估計之準確性。這些框架被推廣到一系列廣義資訊處理中對不同元件間交互作用的研究上。

結論

本文考慮了元件鑑識問題，提出關於視覺感知之多媒體元件鑑識的當前文獻資料調查。本文安排爲三個部分。在第一部分中討論了許多數碼相機元件鑑識之方法論，這些方法可以用於估計相機內元件，例如相機響應函數，彩色濾鏡陣列和色彩內插參數，另外也討論了後插值處理演算

法，例如白平衡和 JPEG 壓縮。第二部分展示了可以用於多種不同應用之估計參數，包括設備品牌和型號識別，侵權/認證鑑識分析，建立真值模型以檢測全域和局部的篡改，包括加密寫入，對圖像採集鑑識進行不同擷取來源圖像的區分。第三部分提出了關於元件鑑識之理論分析框架，主要關注在得到關於元件鑑識的具體理解，和解答許多關於何種處理運算可以或不可以將其識別，以及在什麼條件下可以識別這類基本問題。概括地說，我們認爲元件鑑識分析對於專利侵權案例，智慧財產權管理和數位傳媒之技術進化研究等，可以提供一個資訊的主要來源，並且推動多媒體鑑識發展，以便深入理解資訊處理鏈。

作者簡介

Ashwin Swaminathan (sashwin@qualcomm.com) received the B.Tech degree in electrical engineering from the Indian Institute of Technology, Madras, India in 2003, and the Ph.D. degree in electrical and computer engineering from the University of Maryland, College Park in 2008. He is currently a senior engineer at Qualcomm Incorporated in San Diego, California. He was a research intern with Hewlett-Packard Labs in 2006 and Microsoft Research in 2007. His research interests include multimedia forensics, information security, authentication, and information discovery. He was the winner of the Student Paper Contest at the 2005 IEEE International Conference on Acoustic, Speech and Signal Processing and received the ECE Distinguished Dissertation Fellowship Award in 2008. He is a Member of the IEEE.

Min Wu (minwu@eng.umd.edu) received the Ph.D. degree in electrical engineering from Princeton University in 2001. She is an associate professor at the University of Maryland, College Park. Dr. Wu leads the Media and Security Team at the University of Maryland, with main research interests on information security and forensics and multimedia signal processing. She is a corecipient of two Best Paper Awards from the IEEE Signal Processing Society and EURASIP, respectively. She also received an U.S. NSF CAREER award, a TR100 Young Innovator Award from the *MIT Technology Review Magazine*, a U.S. ONR Young Investigator Award, and a Computer World "40 Under 40" IT Innovator Award. She is currently the area editor of *IEEE Signal Processing Magazine* for its "Inside Signal Processing E-Newsletter" and is the associate editor of the *IEEE Transactions on Information Forensics and Security*.

K.J. Ray Liu (kjrliu@eng.umd.edu) is a Distinguished Scholar-Teacher of University of Maryland, College Park, where he received university-level Invention of the Year Award; and both Poole and Kent Senior Faculty Teaching Award and Outstanding Faculty Research Award from A. James Clark School of Engineering Faculty. Dr. Liu is the recipient of numerous best paper awards and was an IEEE Signal Processing Society Distinguished Lecturer. He was Vice President- Publications, the Editor-in-Chief of *IEEE Signal Processing Magazine*, and the founding Editor-in-Chief of *EURASIP Journal on Applied Signal Processing*.

參考文獻

[1] J. Adams, K. Parulski, and K. Spaulding, "Color processing in digital cameras," *IEEE Micro*, vol. 18, no. 6, pp. 20–30, Nov./Dec. 1998.

[2] J. E. Adams, "Interaction between color plane interpolation and other image processing functions in electronic photography," in *Proc. SPIE Cameras and Systems for Electronic Photography & Scientific Imaging*, San Jose, CA, Feb. 1995, vol. 2416, pp. 144–151.

[3] T.-T. Ng, S.-F. Chang, and M.-P. Tsui, "Using geometric invariants for camera response function estimation," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, Minneapolis, MN, June 2007, pp. 1–8.

[4] H. Farid, "Blind inverse gamma correction," *IEEE Trans. Image Processing*, vol. 10, no. 10, pp. 1428–1433, Oct. 2001.

[5] S. Lin, J. Gu, S. Yamazaki, and H.-Y. Shum, "Radiometric calibration from a single image," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, Washington, D.C., June 2004, vol. 2, pp. 938–945.

[6] S. Lin and L. Zhang, "Determining the radiometric response function from a single grayscale image," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, San Diego, CA, June 2005, vol. 2, pp. 66–73.

[7] A. C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," *IEEE Trans. Signal Processing*, vol. 53, no. 10, part 2, pp. 3948–3959, Oct. 2005.

[8] A. Swaminathan, M. Wu, and K. J. R. Liu, "Non-intrusive component forensics of visual sensors using output images," *IEEE Trans. Inform. Forensics Sec.*, vol. 2, no. 1, pp. 91–106, Mar. 2007.

[9] C. F. van Loan, *Introduction to Scientific Computing: A Matrix-vector Approach Using MATLAB*. Englewood Cliffs, NJ: Prentice-Hall, 1999.

[10] A. Swaminathan, M. Wu, and K. J. R. Liu, "Optimization of input pattern for semi non-intrusive component forensics of digital cameras," in *Proc. IEEE Int. Conf. Acoustic, Speech, and Signal Processing*, Honolulu, HI, Apr. 2007, vol. 2, pp. 225–228.

[11] J. Lukas and J. Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images," in *Proc. Digital Forensics Research Workshop*, Cleveland, OH, Aug. 2003.

[12] Z. Fan and R. L. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," *IEEE Trans. Image Processing*, vol. 12, no. 2, pp. 230–235, Feb. 2003.

[13] S. Bayram, H. T. Sencar, N. Memon, and I. Avcibas, "Source camera identification based on CFA interpolation," in *Proc. IEEE Int. Conf. Image Processing*, Genoa, Italy, Sept. 2005, vol. 3, pp. 69–72.

[14] S. Bayram, H. T. Sencar, and N. Memon, "Improvements on source camera-model identification based on CFA interpolation," in *Proc. WG 11.9 Int. Conf. Digital Forensics*, Orlando, FL, Jan. 2006.

[15] M. Kharrazi, H. T. Sencar, and N. Memon, "Blind source camera identification," in *Proc. Int. Conf. Image Processing*, Singapore, Oct. 2004, vol. 1, pp. 709–712.

[16] M.-J. Tsai and G.-H. Wu, "Using image features to identify camera sources," in *Proc. IEEE Int. Conf. Acoustic, Speech, and Signal Processing*, Toulouse, France, May 2006, vol. 2, pp. 297–300.

[17] M. Chen, J. Fridrich, M. Goljan, and J. Lukas, "Determining image origin and integrity using sensor pattern noise," *IEEE Trans. Inform. Forensics Sec.*, vol. 3, no. 1, pp. 74–90, Mar. 2008.

[18] H. Farid and S. Lyu, "Higher-order wavelet statistics and their application to digital forensics," in *IEEE Workshop on Statistical Analysis in Computer Vision*, Madison, WI, June 2003, vol. 8., pp. 94–101.

[19] I. Avcibas, B. Sankur, and K. Sayood, "Statistical evaluation of image quality metrics," *J. Electron. Imag.*, vol. 11, no. 2, pp. 206–223, Apr. 2002.

[20] E. A. Dirik, H. T. Sencar, and N. Memon, "Source camera identification based on sensor dust characteristics," in *Proc. IEEE Workshop Signal Processing Applications for Public Security and Forensics*, Brooklyn, NY, Apr. 2007, pp. 1–6.

[21] A. Swaminathan, M. Wu, and K. J. R. Liu, "Component forensics of digital cameras: A non-intrusive approach," in *Proc. Conf. Information Sciences and Systems*, Princeton, NJ, Mar. 2006, pp. 1194–1199.

[22] Y.-F. Hsu and S.-F. Chang, "Image splicing detection using camera response function consistency and automatic segmentation," in *Proc. IEEE Int. Conf. Multimedia and Expo*, Beijing, China, July 2007, pp. 28–31.

[23] I. Avcibas, S. Bayram, N. Memon, M. Ramkumar, and B. Sankur, "A classifier design for detecting image manipulations," in *Proc. Int. Conf. Image Processing*, Singapore, Oct. 2004, vol. 4, pp. 2645–2648.

[24] A. Swaminathan, M. Wu, and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," *IEEE Trans. Inform. Forensics Sec.*, vol. 3, no. 1, pp. 101–117, Mar. 2008.

[25] D. Kundur and D. Hatzinakos, "Blind image deconvolution," *IEEE Signal Processing Mag.*, vol. 13, no. 3, pp. 43–64, May 1996.

[26] G. R. Ayers and J. C. Dainty, "Iterative blind deconvolution method and its applications," *Opt. Lett.*, vol. 13, no. 7, pp. 547–549, July 1988.

[27] W.-H. Chuang, A. Swaminathan, and M. Wu, "Tampering identification using empirical frequency response," in *Proc. IEEE Int. Conf. Acoustic, Speech, and Signal Processing*, Taipei, Taiwan, Apr. 2009.

[28] A. Swaminathan, M. Wu, and K. J. R. Liu, "A pattern classification framework for theoretical analysis of component forensics," in *Proc. IEEE Int. Conf. Acoustic, Speech, and Signal Processing*, Las Vegas, NV, Apr. 2008, pp. 1665–1668.

[29] A. Swaminathan, M. Wu, and K. J. R. Liu, "A component estimation framework for information forensics," in *IEEE Workshop on Multimedia Signal Processing*, Crete, Greece, Oct. 2007, pp. 397–400.

[30] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification*, 2nd ed. New York: Wiley-Interscience, 2000.

[31] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," *IEEE Trans. Signal Processing*, vol. 53, no. 2, pp. 758–767, Feb. 2005.

[32] A. C. Popescu and H. Farid, "Statistical tools for digital forensics," in *Proc. 6th Int. Workshop Information Hiding & Lecture Notes in Computer Science*, Toronto, Canada, May 2004, vol. 3200, pp. 128–147.

[33] M. K. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments," *IEEE Trans. Inform. Forensics Sec.*, vol. 2, no. 3, part 1, pp. 450–461, Sept. 2007.

[34] M. K. Johnson and H. Farid, "Exposing digital forgeries through chromatic aberration," in *Proc. ACM Multimedia and Security Workshop*, Geneva, Switzerland, Sept. 2006, pp. 48–55.

[35] C. E. McKay, A. Swaminathan, H. Gou, and M. Wu, "Image acquisition forensics: Forensic analysis to indentify imaging source," in *Proc. IEEE Conf. Acoustic, Speech, and Signal Processing*, Las Vegas, NV, Apr. 2008, pp. 1657–1660.

[SP]