抵抗列印掃描攻擊之彩色影像浮水印隱藏技術

陳伯岳
彰化師範大學 副教授
pychen@cc.ncue.edu.tw

林志龍
彰化師範大學 研究生
toyo2054@gmail.com

摘要

由於數位處理技術的快速進步，數位內容常輕易地被修改及重製，引發了許多數位內容的所有權或版權爭端。數位浮水印技術是應用於數位影像所有權認定的方法之一，其遭遇到的攻擊法很多，列印掃描則是當中較具挑戰性的一項。因為列印掃描攻擊不僅造成影像像素值的更改，也涉及影像的幾何轉換，使大多數的浮水印系統失效。本論文提出一個能抵抗列印掃描攻擊的浮水印技術，此技術將一彩色影像的三原色成分個別作離散餘弦轉換，再將浮水印分別嵌入轉換係數中。理由是三原色對於不同的攻擊方式具有不同的抵抗強度，取出浮水印時可利用三者適當的線性組合而排除大多數的攻擊效果。實驗結果顯示，提出的方法不僅保持一定的影像品質，同時也提供了浮水印的強韌性。

關鍵詞：數位浮水印、列印和掃描攻擊、離散餘弦轉換、BCH Code。

Abstract

Because of the fast development of digital processing techniques, it is convenient to modify and reproduce a digital content. As a result, many controversies over ownership and copyrights have arisen. In recent years, many watermarking schemes regarding the copyright issue have been proposed. However, there exist many attacks trying to break or remove the embedded watermark. Therefore, the embedded watermark should be robust against all kinds of attacks. Among various attacks, the print-and-scan (PS) attack is a challenging one because it not only alters the pixel values but also changes the positions of the original pixels. Most of the modern watermarking systems would fail under such an attack. In this paper, we propose a watermarking system operating in the discrete cosine transform (DCT) domain. Integrating the three components (Red, Green, and Blue) of a color image, the proposed system exhibits superior robustness over different attacks, including the PS attack. According to the simulation results, the system maintains an acceptable image quality while providing outstanding robustness against the PS attack.

Keywords: digital watermarking, print-and-scan attack, discrete cosine transform, BCH Code.

1. 前言

隨著數位影像攝影設備之流行，數位相片隨手可得，相關應用也因應而生。數位浮水印技術除了可用於保護智慧財產權外，亦可應用於資訊隱藏相關領域。因為數位資訊有著容易儲存、複製、修改、傳播的特性，所以網路上隨處可見各種未經授權的資料被不肖人士大量的複製與散佈，不僅對個人創作者的權益造成影響，也降低了其創作意願。因此，智慧財產權的保護措施便成了一

個非常重要的課題。數位影像浮水印技術必須能抵抗各種攻擊，換言之，當遭受到各種攻擊時尚必須能證明數位浮水印之存在性。而資訊隱藏技術要求則更嚴謹，必須能完整萃取及辨識出隱藏之資訊。對於數位影像的攻擊方法很多，其中的列印掃描(Print-and-scan, PS)攻擊是相當具有挑戰性。其攻擊後的影像不僅像素值遭修改，也使得像素位置有變動，使大多數的浮水印技術失效。抵抗列印掃描攻擊之主要重點有以下兩點：

(1) 將欲藏入的浮水印影像先經過 BCH Code 的錯誤更正編碼，即使影像遭受到破壞，可利用附加的資訊來還原正確之資訊。

(2) 將攻擊後的影像進行霍夫轉換(Hough Transform)以判斷該張影像是否在列印與掃描之間曾遭到幾何旋轉，若有則須先校正其角度再將資訊正確取出。

本論文之組織如下:第二節回顧近年之相關文獻所提出之各項技術，第三節清楚描述作者提出的方法，第四節則列出實驗結果並對相關數據進行討論分析，最後總結於第五節。

2. 文獻探討

本節首先討論列印掃描對於影像的影響，接著將針對抵抗 PS 攻擊的浮水印技術之文獻作回顧式的介紹，並加以分析討論。本論文將整合這些既有技術並提出新的解決方案，期望能充分利用數位影像之頻率域特性而開發出能抵抗列印掃描攻擊之浮水印技術。此外，鑑於現今數位影像多為彩色影像，有別於大多數文獻所提出之灰階影像嵌入技術，本論文也將利用光三原色之不同頻率域特性來嵌入強健型浮水印。

2.1 列印掃描對於影像的影響

影像在經過列印與掃描之後，會導致像素值變化與幾何失真兩種情況[1][2][3]，進而造成影像浮水印的認證失敗，以下分別描述此二種情況。

2.1.1 像素值差異

影像經過列印和掃描後，其像素的對比、亮度和色度都會有所變化。Shi 等學者[1]使用直方圖均勻分佈的標準測試影像進行實驗，結果發現在列印掃描後，低灰階像素值個數稍微增加，而高灰階像素值個數則會下降，如圖 1 所示。要開發能抵抗 PS 攻擊的浮水印技術可充分利用此一特性。

2.1.2 幾何失真

影像經過列印和掃描後，可能因為人為的因素產生影像的縮放、旋轉或裁切等幾何失真，使得影像中的浮水印因遭受攻擊而改變，造成在萃取浮水印時因使用錯誤的浮水印位置，而產生取出的錯誤。

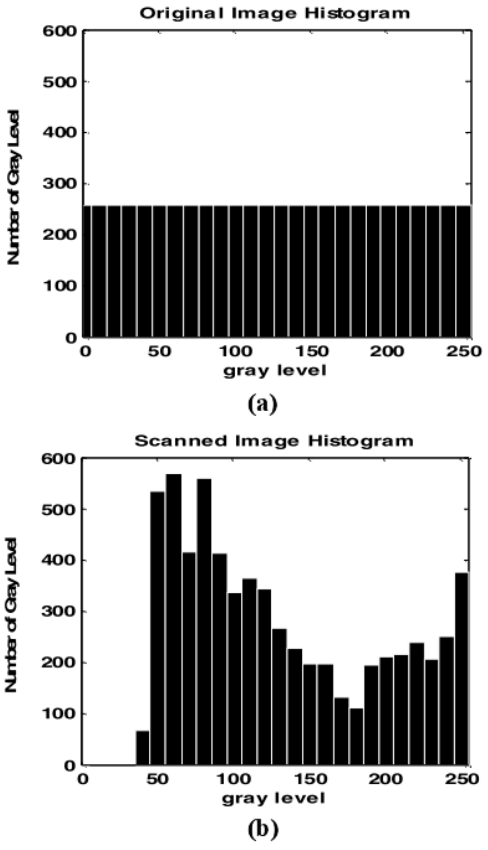

圖 1. (a)原始直方圖；(b)列印掃描後直方圖

2.2 抵抗列印掃描的浮水印相關文獻

Shi 等學者[4]將影像切割成相同大小的區塊分別進行 DCT 轉換，再選取各區塊的中頻帶做為浮水印的嵌入區域。浮水印嵌入法則是將區塊所有係數值改為相同符號方式嵌入。例如，欲嵌入位元 1，則將所有係數改為正值；反之，則將所有係數改為負值。此嵌入法由於可能更改大量係數的符號，對於影像品質有相當大的破壞。此外為解決影像畫質問題，該方法需記錄區塊正負值係數數量的大小關係，在浮水印嵌入時是將所有係數改為符號數量較多者(亦即，更動較少的係數正負號)。如此就必須儲存各區塊原始係數符號數量關係的額外資訊。因此，此法屬於知情浮水印系統（Informed watermarking system），而非較通用的盲水印系統（Blind watermarking system）。Jin 等學者[5]將影像切割成小區塊並作 DCT 轉換，取出絕對值大於門檻值之中頻係數，再透過設定區塊係數正負值數量來嵌入浮水印。然而此方法對於列印掃描抵抗的錯誤率偏高。Tang 等學者[6]將影像切割成多個區塊並作 DCT 轉換，再將區塊的係數內取中頻帶利用調變正負符號係數之比例以嵌入浮水印。此方法與[4]不同之處在於，將所有係數符號均改為相同，只要維持一個比例即可。 此方法在抵抗列印掃描之效果不錯，不過在抵抗 JPEG 之圖像壓縮的效果尚有改進的空間。Cheng 等學者[7]發現經由列印掃描後的影像係數的平均值幾乎不變，且絕大多數分佈在−1 ~ 1 間。再經由改變正負符號方式去嵌入浮水印，嵌入的強度由人眼視覺系統的可感覺差異(Just Noticeable Distance, JND) 模式決定以避免失真問題。此嵌入法所定義門檻值未將影像本身特性考慮進來，對於小尺寸影像的浮水印偵測錯誤偏高。Tang 等學者[8]首先計算嵌入影像的平均值的分佈範圍，取得調整係數的門檻值，用來增加浮水印的嵌入強度，再來更改嵌入區塊內的係數值，讓區塊內的係數及平均值變大，以提高此方法的強韌度。此方法相較於[7]在較小的列印尺寸之浮水印偵測的錯誤率有些許的改善。

3. 提出方法

本論文所提出的方法是基於 DCT 轉換至頻率域後將秘密資訊予以藏入，並且具強韌性之資訊隱藏方法。除了能抵抗常見的基本攻擊，最大特色在於能抵抗 PS 攻擊，且能萃取出隱藏之機密資訊。主要內容分為機密資訊嵌入以及機密資訊萃取二部份，茲分述如後。

3.1 浮水印嵌入流程

嵌入浮水印流程如圖 2 所示，首先讀取一張 $M \times M$ 的 RGB 彩色影像，取出紅色、綠色、藍色頻帶。之所以對三個頻帶區塊重覆作嵌入，主要原因是在遭受不同的攻擊方式後，三個頻帶具有不同的抵抗能力。例如遭受 PS 攻擊時，紅色頻帶的變化會比其他兩個頻帶來的小[6]；受到 JPEG 壓縮、裁切、雜訊等攻擊時，綠色頻帶的變化會比其他兩個頻帶來的小[9]；而藍色頻帶則是基於人眼視覺對藍光的變化較不敏感[10]的理由，可用於加強影像品質。

三個頻帶分別被切割成 32×32 之區塊，之後各自作 FDCT 轉換；同時，對一 $m \times m$ 的浮水印使用 Arnold 攪亂[11][12]，其目的有二，一是使秘密資訊均勻的散佈在原始影像上，二是增加安全性(攪亂需要一個密鑰與演算法，攻擊者即使有嵌入浮水印的圖像，沒有密鑰與演算法也無法將浮水印萃取出來)。

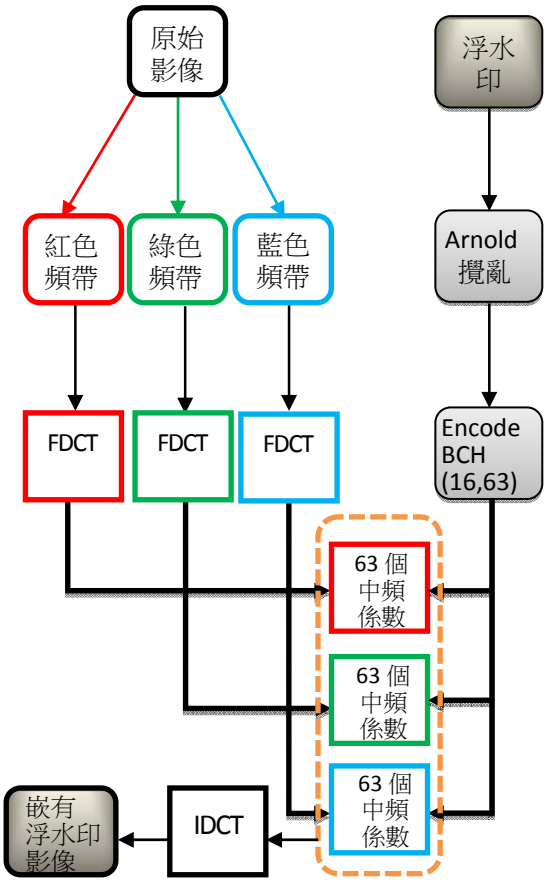

圖 2.嵌入浮水印之流程圖

接著由各區塊選取 63 個之中頻係數作嵌入的動作。嵌入方式如下:

嵌入浮水印

若 $w_i = 1$：

$$dct\_blockR_{x,y} = dct\_blockR_{x,y} + \alpha$$

$$dct\_blockG_{x,y} = dct\_blockG_{x,y} + \alpha$$

$$dct\_blockB_{x,y} = dct\_blockB_{x,y} + \alpha$$

若 $w_i = 0$ ：

$$dct\_blockR_{x,y} = dct\_blockR_{x,y} - \alpha$$

$$dct\_blockG_{x,y} = dct\_blockG_{x,y} - \alpha$$

$$dct\_blockB_{x,y} = dct\_blockB_{x,y} - \alpha$$

其中，w_i 是攪亂浮水印的第 i 個位元，α 稱為嵌入強度，是為了調整浮水印之穩定度而設的參數。三個頻帶都嵌入相同的浮水印，是為了能抵抗各式攻擊。

3.2 浮水印取出流程

浮水印之取出流程如圖 3 所示。若藏有浮水印的影像因曾遭攻擊而有角度改變，先作幾何校正再進行浮水印偵測。在影像經過列印掃描處理的過程中，常會因為人為操作疏失，導致影像的幾何失真，其中最常見者為旋轉。首先偵測影像的邊緣像素(Edge pixels)，其次利用霍夫轉換(Hough transform)偵測影像之直線邊界以校正影像。

萃取的動作與嵌入的動作類似，將幾何更正後的影像取出紅色、綠色、藍色頻帶，並給予相對的權重值 γ、ϑ、與 β，這三個參數之初始值皆設為 $\frac{1}{3}$。

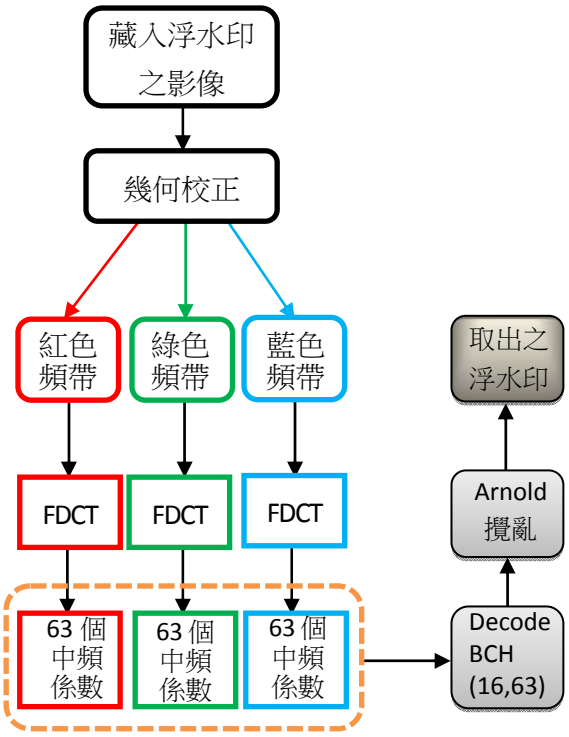

圖 3.萃取浮水印之流程圖

之後進行 FDCT 轉換並由每個區塊分別取出 63 個中頻係數，利用(1)式可得出浮水印 $w'' = \{w_i'' \mid i = 1, 2, \cdots, 16128\}$，之後再進行

$$\begin{cases} ((dct\_blockR \times \gamma) + (dct\_blockG \times \vartheta) + (dct\_blockB \times \beta)) > 0 & : w_i'' = 1, \\ ((dct\_blockR \times \gamma) + (dct\_blockG \times \vartheta) + (dct\_blockB \times \beta)) < 0 & : w_i'' = 0, \\ \gamma + \vartheta + \beta = 1 \end{cases} \quad (1)$$

BCH 解碼為 ，再以 Arnold 作攪亂，因為 Arnold 攪亂具有週期性，需根據原始的密鑰給予一定的次數攪亂即可還原成原始浮水印。

3.3 浮水印取出之完整性

本論文根據 NCC (Normalized Cross Correlation，定義如(2)式)來判斷取出之浮水印的完整性。如果 NCC 大於某個門檻值，則表示圖片藏有浮水印，也就是愈接近原始的浮水印，NCC=1 代表浮水印完全取出無誤；式中 w_{ij} 為原始浮水印像素值，w'_{ij} 是萃取出來浮水印的像素值，i 跟 j 分別代表橫向與縱向座標位置。

$$NCC = \frac{\sum_i \sum_j w_{ij} w'_{ij}}{\sum_i \sum_j (w_{ij})^2} \quad (2)$$

另外[6][8]則是以錯誤率(error rate) E (定義如(3)式，m 為浮水印大小)將取出的浮水印 w' 與由金鑰所產生的浮水印 w 進行驗證，通常 E 值若低於 10%，則表示浮水印成功取出。

$$E = \frac{1}{m \times m} \sum_{ij} \left| w_{ij} - w'_{ij} \right| \quad (3)$$

4. 實驗結果

實驗使用的影像如圖 4。圖 4(a)為原始影像，大小為 512×512 的彩色影像；4(b)為浮水印圖像，大小為 64×64 的二值化影像。

表 1 為針對不同的嵌入強度去作測試，兩者比較結果，使用 $\alpha = 10$ 是較佳的選擇，原因是 PSNR 接近 40 時，人的肉眼很難看出兩張影像的差異度，而較大的嵌入強度將會使浮水印更加強韌。實驗乃採用 Fuji Xerox DocuCentre Color a450 雷射印表機，及 Epson AcuLaser MX14 複合機之掃描功能。表 2 為 $\alpha = 10$ 之影像經過列印掃描後(掃描解析度為 600dpi)取出之結果。

Lena **Peppers** **Tiffany**

(a)原始影像

(b)浮水印圖像

圖 4. 實驗影像

表 1.不同嵌入強度之影像品質(以 Lena 為例)

嵌入強度	**PSNR**
$\alpha = 7.5$	42.20 dB
$\alpha = 10$	39.75 dB

表 2.列印掃描後取出結果

Lena		**NCC** 0.9204 **E** 6.59%
Peppers		**NCC** 0.9293 **E** 5.71%
Tiffany		**NCC** 0.9107 **E** 7.98%

最後再透過常見之影像處理攻擊來測

試本方法的強韌性，包含旋轉、模糊化、裁切及銳利化等。實驗結果如表 3 所示。結果顯示浮水印的平均錯誤率都在 10%以下，也證明本研究所提出方法具備極佳的強韌性。

表 3. 幾何攻擊之浮水印錯誤率

攻擊種類	Lena		Peppers		Tiffany	
	NCC	E	NCC	E	NCC	E
Gaussian Blur (Radius:1 pixels)	0.9805	2.49%	0.9929	0.88%	0.9903	1.25%
Gaussian Blur (Radius:2 pixels)	0.9316	6.01%	0.9412	7.28%	0.9216	9.38%
Sharpening (Radius:3 pixels)	0.9991	0.12%	1	0.00%	0.9991	0.12%
Sharpening (Radius:5 pixels)	0.9986	0.17%	1	0.00%	0.9989	0.12%
Gaussian Noise 5%	0.9883	0.88%	0.9923	0.95%	0.9747	3.13%
Cropping 50%	0.9403	5.32%	0.9409	5.06%	0.9409	5.10%
Cropping 75%	0.9152	8.13%	0.9152	8.18%	0.9141	8.25%
JPEG Compression 90%	0.9988	0.15%	1	0.00%	0.9954	0.54%
JPEG Compression 70%	0.9569	3.86%	0.9405	4.30%	0.9084	8.86%
restore size after the scale 0.75	0.9732	2.61%	0.9833	2.22%	0.9655	4.17%
Rotation 15°	0.9766	2.91%	0.9915	0.95%	0.9650	3.91%
Rotation 45°	0.9515	5.13%	0.9674	4.03%	0.9348	6.88%

表 4. 幾何攻擊之比較 (原始影像為 Lena)

攻擊種類	攻擊參數	NCC	
		本方法	Bei[13]
Gaussian Blur	Radius:2 pixels	0.9316	0.9193
Gaussian Noise	3%	0.9968	0.9315
	8.50%	0.9069	0.9026
Cropping	from the center (1/4)	0.9651	0.8994
	from the surround (1/4)	0.9689	0.9213
Rotation	65°	0.9406	0.8927
JPEG compression	80%	0.9982	0.9816
	50%	0.9071	0.8912
Sharpening	USM sharpening (number=20,radius=1)	0.9995	0.9562

表 4 為本論文的方法與 Bei 等學者[13]的方法比較，因選用的嵌入影像大小與浮水印大小為相同，相互比較較為公平。其結果顯示本方法在每一種攻擊情況下，浮水印的取出完整性皆優於[13]。

5. 結論

本論文提出一個具抵抗列印與掃描攻擊之彩色影像資訊隱藏方法。利用三元色對各式攻擊具有不同抵抗能力的事實，採取適當的線性組合來抵抗不同的攻擊。同樣透過 DCT 轉換再將浮水印予以藏入後，經過不同的攻擊再取出其浮水印之流程，本文所提方法明顯優於[13]。由實驗分析證明本論文所提之方法在影像遭受幾何攻擊後，取出的浮水印之 NCC 值較高，且能抵抗列印與掃描之攻擊。

本論文的影像攻擊中，列印與掃描攻擊對影像的破壞算是較嚴重的。在未來會嘗試列印與照相攻擊，此攻擊我們認為比列印掃描攻擊破壞程度更大，因為列印之後再利用數位相機翻拍時，相機的參數(如：ISO 值、曝光值)，亦或是相機的鏡頭、光圈的不同，所呈現的結果即不一樣，因此這種方式的攻擊更具挑戰性。

參考文獻

[1] Ante Poljicak, Lidija Mandic, Darko Agic, “Discrete Fourier transform - based watermarking method with an optimal implementation radius,” Journal of Electronic Imaging 20(3), 2011. pp 033008-1-033008-8.

[2] Longjiang Yu, Xiamu Niu, Shenghe Sun, “Print-and-scan model and the watermarking countermeasure, ” Image and Vision Computing, 23 (9) (2005), pp. 807–814

[3] Chunlin Song, Sud Sudirman, Madjid Merabti and David Llewellyn-Jones, “Analysis of Digital Image Watermark Attacks, ” Consumer Communications and Networking Conference (CCNC), 2010, pp. 1-5 .

[4] Shi Dongcheng, Wang Qi, and Liang Chao, “Digital Watermarking Algorithm for Print-and-Scan Process used for Printed matter Anti-Counterfeit,” Congress on Image and Signal Processing, Vol. 5, 2008, pp. 697–701.

[5] Jin Jamming, Xiong Yuhong, and Hou Huiman, “A Practical DCT Based Blind Image Watermarking Scheme for Print-and-Scan Process,” HP Laboratories Technical Reports, Vol. 7538, 2010.

[6] Yuan-Liang Tang, Sheng-Yu Tseng, “Print-and-scan resilient watermarking through polarizing DCT coefficients, ” Computing, Communications and Applications Conference, 2012, pp. 411-414.

[7] D. Cheng, X. Li, W. Qi, and B. Yang, “A Statistics-Based Watermarking Scheme Robust to Print-and-Scan,” Proceedings of Electronic Commerce and Security, pp. 894-898, 2008.

[8] Yuan-Liang Tang, Chia-Jung Yang, “Print-and-Scan Resilient Watermarking Based on Modulating the Averages of DCT Coefficients, ” Computing, Biometrics and Security Technologies (ISBAST), 2012 International Symposium, pp. 113-117.

[9] Liu Lianshan, Li Renhou,Gao Qi, “Method of Embedding Digital Watermark into the Green Component of Color Image, ” Journal of Xian Jiaotong University,

Vol.38 No.12, 2004, pp. 1256-1259.

[10] GAO Pi-lian, HOU De-wen, LI Peng, “Dual watermarking algorithm of colored images based on wavelet transform ,“ Computer Engineering and Design, Vol.29 No.1, 2008, pp. 31-33.

[11] Gabriel Peterson, “Arnold's cat Map, ” http://online.redwoods.cc.ca.us/instruct/darnold/laproj/Fall97/Gabe/catmap.pdf.

[12] Ding Wei, Yan Weiqi, Qi Dongxu, “Digital image scram-bling technology based on Arnold transformation, ” Journal of Computer-Aided Design and Computer Graphics, 2011, 13(4), pp. 338-341.

[13] Yi-lin Bei, De-yun Yang, Ming-xia Liu, Li-li Zhu, “A Milti-channel Watermarking Scheme Based on HVS and DCT-DWT, ” Computer Science and Automation Engineering (CSAE) 2011, Vol. 4, pp. 305-308.