

以 DCT 係數符號轉換為基礎之抵抗列印掃描浮水印技術

唐元亮*, 曾盛宥

朝陽科技大學資訊管理系

*yltang@cyut.edu.tw

摘要

目前數位影像的著作權保護大多利用數位浮水印技術在影像中嵌入相關資訊，而所嵌入的浮水印應該具備強韌性，以避免遭到破壞或移除。數位浮水印的攻擊法很多，其中列印掃描是一項極具挑戰的攻擊，因為列印與掃描攻擊不僅包含對於影像像素本身的修改，也會改變像素位置，這使大多數的浮水印系統失效。在本論文中，我們將提出能夠抵抗列印與掃描攻擊的浮水印技術，利用離散餘弦轉換係數經過列印掃描後所產生的特性來設計，不僅可以保護影像品質不因嵌入浮水印而過度破壞，同時也保持浮水印的強韌性。

關鍵詞：數位浮水印、列印和掃描攻擊、離散餘弦轉換。

Digital watermarking techniques have been used to protect the ownerships of digital images. That is, related information is embedded to an image as a watermark such that its ownership can be identified. However, there are also many attacks trying to break or remove the embedded watermark. Therefore, the embedded watermark should be very robust against all kinds of attacks. Among various attacks, the print-and-scan (PS) attack is very challenging 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 which is PS resistant. By considering the properties of DCT coefficients under the PS attack, the system is able to maintain the image quality and the embedded watermark is very robust against the PS attack as well.

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

1. 前言

隨著多媒體科技不斷的發展，數位影像的複製、修改、及傳輸變得非常容易。然而，科技的發展也帶來許多問題，例如，未經授權的複製導致許多著作權的爭議。目前數位影像的著作權保護大多利用數位浮水印技術，亦即在影像中嵌入相關資訊藉以宣告著作權，而所嵌入的資訊應該具備強韌性，避免遭到破壞或移除。數位浮水印的攻擊方法很多，其中列印與掃描(Print-and-scan, PS)是一項極具挑戰的攻擊，因為列印與掃描攻擊不僅包含對於影像像素的修改，也會改變像素位置，這使大多數的浮水印功能失效。在本論文中，我們將提出能夠抵抗列印與掃描攻擊的彩色影像浮水印技術。此法利用離散餘弦轉換(Discrete Cosine Transform, DCT)係數經過列印掃描後所產生的特性來設計，主要重點有三：首先，探討列印掃描對於影像或 DCT 係數所產生的影響。其次，分析影像在經過離散餘弦轉換之後，其係數所產生的變化，並利用其係數關係為基

礎，設計出一套浮水印嵌入法。第三，基於人類視覺特性找出不易失真，且具強韌性的資訊嵌入位置及強度。

2. 相關文獻探討

本節將介紹相關的技術與文獻。首先，討論列印掃描對於影像的影響。其次，介紹抵抗列印掃描的浮水印相關文獻。

2.1 列印掃描對於影像的影響

影像在經過列印和掃描之後，會產生像素值差異與幾何失真。

2.1.1 像素值差異

像素值差異來自於列印和掃描後像素的對比、亮度、或色度變化。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，結果發現原始影像的像素值和列印掃描之後像素值主要的不同點在於灰階範圍縮小以及部份集中在低灰階部份，如圖 1 所示。

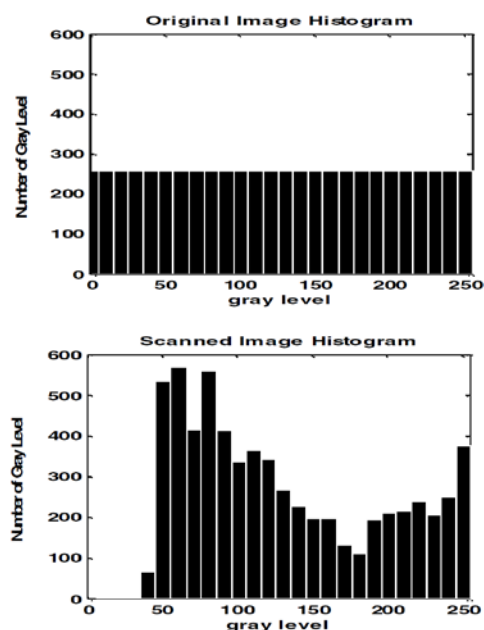


圖1：(a)原始直方圖，(b)列印掃描後直方圖

2.1.2 幾何失真

影像在經過列印掃描後會產生縮放、旋轉、裁切、及解析度不同等變化，這些大多數是因人為操作所導致。幾何失真對於浮水印的攻擊在於破壞浮水印的同步性，亦即資訊嵌入的位置因為幾何攻擊而改變，造成在資訊取出時使用錯誤的位置，使浮水印偵測失敗。

2.2 抵抗列印掃描的浮水印相關文獻

Guo 等學者[2]將影像紋理較複雜之區塊做離散傅立葉轉換(DFT)，並在這些區塊的中頻區域將某些係數放大以嵌入浮水印。由於紋理複雜之區塊經過列印掃描後，容易被模糊，浮水印易隨之消失，故此法只適用於高品質的列印影像。Kaushal 等學者[3]利用低頻 DFT 係數在經過列印掃描後變化幅度較小的特性，將訊息藏入於變化較不顯著的區域。他們首先利用不同影像品質的索引方法設定門檻值，再利用選擇嵌入低頻方法將低頻區域依角度判斷是否通過門檻值來藏入浮水印，此法雖然可保護影像品質不被破壞，但取出浮水印的檢測需要原始的影像與資訊。Jin 等學者[4]將影像切割成區塊並作 DCT 轉換，取絕對值大於某個門檻之係數，再利用設定區塊係數正負號數量的關係來嵌入浮水印，此法對於列印掃描的抵抗的錯誤率偏高。

Shi 等學者[1]將影像切割為區塊並做 DCT 轉換，再取中頻係數做為浮水印嵌入的區域，如圖 4 灰色區域所示。浮水印則是透過將某區域所有係數均改為相同符號方式嵌入。例如，欲嵌入 1，則將所有係數改為正號；反之，欲嵌入 0，則將所有係數改為負號。此嵌入法對於影像畫質有相當大的衝擊，例如，若某區域的正係數數量極大於負係數，將所有係數均改為負值，影像畫質必定遭受重大衝擊。為解決此問題，Shi 等學者先行記錄該區域正負係數數量的關係，然後浮水印的嵌入則永遠是將所有係數改為符號數量較大者。但此解決方案有兩個問題：第一、此嵌入法變得毫無意義，因

為是永遠將所有係數符號改為符號數量大者。第二、必須儲存額外資訊，亦即原始係數符號關係。除了將浮水印系統變成知情水印系統(Informed watermarking system)，而非盲水印系統(Blind watermarking system)，且系統效能較差之外，儲存符號關係資訊其實等於儲存浮水印本身，浮水印嵌入沒有意義。

1	2	6	7	15	16	28	29	45	46	66	67	91	92	120	121	153	154
3	5	8	14	17	27	30	44	47	65	68	90	93	119	122	152	155	188
4	9	13	18	26	31	43	48	64	69	89	94	118	123	151	156	187	189
10	12	19	25	32	42	49	63	70	88	95	117	124	150	157	186	190	219
11	20	24	33	41	50	62	71	87	96	116	125	149	158	185	191	218	220
21	23	34	40	51	61	72	86	97	115	126	148	159	184	192	217	221	246
22	35	39	52	60	73	85	98	114	127	147	160	183	193	216	222	245	247
36	38	53	59	74	84	99	113	128	146	161	182	194	215	223	244	248	269
37	54	58	75	83	100	112	129	145	162	181	195	214	224	243	249	268	270
55	57	76	82	101	111	130	144	163	180	196	213	225	242	250	267	271	288
56	77	81	102	110	131	143	164	179	197	212	226	241	251	266	272	287	289
78	80	103	109	132	142	165	178	198	211	227	240	252	265	273	286	290	303
79	104	108	133	141	166	177	199	210	228	239	253	264	274	285	291	302	304
105	107	134	140	167	176	200	209	229	238	254	263	275	284	292	301	305	314
106	135	139	168	175	201	208	230	237	255	262	276	283	293	300	306	313	315
136	138	169	174	202	207	231	236	256	261	277	282	294	299	307	312	316	321
137	170	173	203	206	232	235	257	260	278	281	295	298	308	311	317	320	322
171	172	204	205	233	234	258	259	279	280	296	297	309	310	318	319	323	324

圖2：18×18 區塊呈鋸齒型排列

因此，本論文改善他們所提出的方法，不僅可以保護影像品質不被過度破壞、保持嵌入資訊的強韌性、也不必儲存額外資訊，維持盲水印系統之特性。

3. 提出方法

本論文所提出的方法是利用 DCT 係數在經過列印掃描後所產生的特性，將訊息嵌入影像的適當頻率域內。

3.1 浮水印嵌入流程

浮水印嵌入的流程如圖 4 所示，首先讀取一張 $M \times M$ 的 RGB 彩色影像，取出紅色頻帶並切割成大小為 $N \times N$ 之區塊。其次，由於列印掃描常對於影像外側造成失真，因此我們排除外緣區塊，僅取內部 $R = (M/N - 2) \times (M/N - 2)$ 區塊，並將所有區塊重疊排列成為三維陣列： $N \times N \times R$ 。最後，將每個區塊進行離散餘弦轉換，鋸齒狀掃描係數後選擇 m 個中頻係數以嵌入浮水印(m 個位元)，每 R 個係數嵌入一個浮

水印位元。接著，透過一個私密金鑰，產生一組浮水印 $W = \{w_i \mid w_i = 0, 1; i = 1..m\}$ ，然後依照浮水印位元來更改 R 個係數中的正負號比例藉以嵌入浮水印。

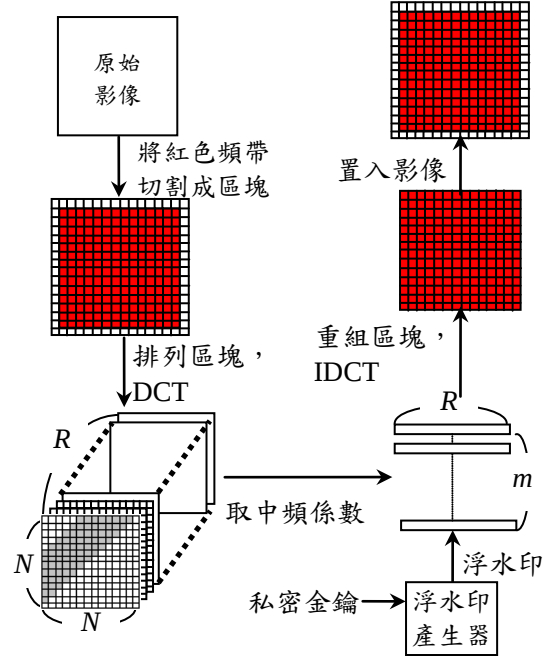


圖3：嵌入流程

為了避免 DCT 係數在嵌入浮水印時受到過度修改而導致影像品質不佳，我們利用係數值大者不易受到列印掃描影響的特性，來決定浮水印嵌入之強度。在上述三維陣列中，取相同位置的 R 個係數進行實驗分析，經過列印掃描之後，在中頻區域係數改變符號的數量比例低於 $1/3$ ，如圖 5 所示。再加上係數絕對值之因素，係數絕對值大小在前 $1/3$ 者，經過列印掃描攻擊後符號改變的比率非常小，亦即絕對值在前 $1/3$ 之係數平均有高達 99.34% 之係數維持原符號，如表 1 所示。

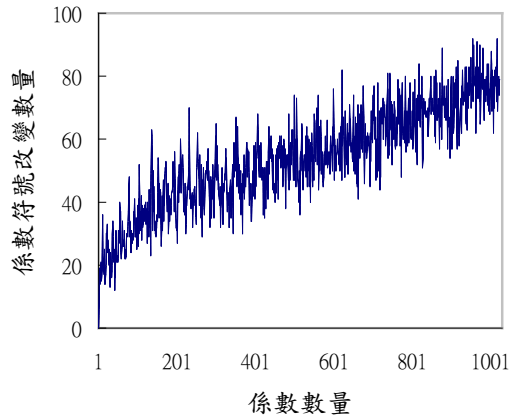


圖 4: Lena 影像係數的變化量

表 1: 列印掃描後 DCT 係數維持原符號之比率

	前 1/3	前 2/3
Lena	99.01%	93.87%
Baboon	99.95%	97.80%
Peppers	99.07%	96.92%
平均	99.34%	96.19%

假設 R 個 DCT 係數中分別有 p 及 n 個正及負係數，依照先前的分析結果，不需要如 Shi 等學者方法一般，將所有係數符號均改為相同，只要維持一定比例即可，假設此比例為 k 。由於改變係數絕對值較大者之符號會影響影像品質，因此係數絕對值在前 10% 者不會更動。此外為使嵌入之浮水印更為強韌，再將 R 個係數乘以嵌入強度 α ，使浮水印強韌度更高，嵌入法摘要如下：

- (1) 嵌入浮水印：
 - 若 $w_i = 1$ ：
 - 若 $p < kn$ ，更改某些負係數之符號，使 $p' = kn'$
 - 若 $w_i = 0$ ：
 - 若 $n < kp$ ，更改某些正係數之符號，使 $n' = kp'$
- (2) 將 R 個係數乘以 α

其中 p' 及 n' 分別為修改符號後正負號係數的數量。完成以上的嵌入步驟後，將區塊重組、反離散餘弦轉換、再合併紅藍綠三頻帶後產生嵌入浮水印之影像。

3.2 浮水印取出流程

浮水印取出包括兩個步驟：幾何更正及浮水印偵測。

3.2.1 幾何更正

在影像經過列印掃描處理的過程中，常會因為人為操作，導致影像的幾何失真，最常見者為旋轉。我們利用霍夫轉換(Hough Transform)偵測影像邊界以便校正影像。首先，偵測邊緣像素(Edge pixels)。其次，由於霍夫轉換計算量非常高，如果旋轉角度在一定的範圍內(例如： $\pm 10^\circ$)，則影像邊界也會在一定的區域範圍內。我們可以将影像中央部份的邊緣像素去除以大量減少計算量，系統的效率會更好。透過霍夫轉換偵測到四條影像邊界直線後，最後再依直線的斜率將影像校正，如圖 6 所示。

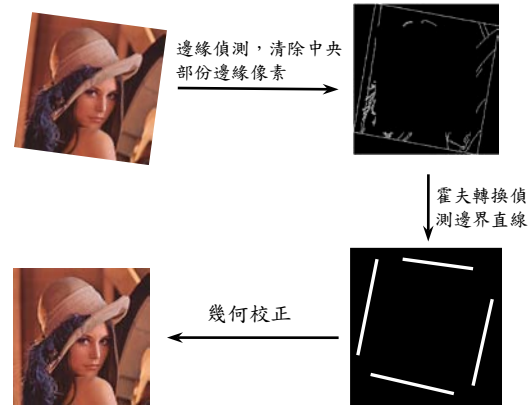


圖 5：幾何更正

3.2.2 浮水印偵測

將幾何更正後的影像取出紅色頻帶，進行區塊切割與離散餘弦轉換。再取出中頻係數並計算區塊係數的正負號的數量以得出浮水印 W' ：

$$\begin{cases} p' \geq n', w'_i = 1, i = 1, 2, \dots, m \\ p' < n', w'_i = 0, i = 1, 2, \dots, m \end{cases}$$

最後，將取出的浮水印 W' 與由金鑰所產生的浮水印 W 進行驗證，其錯誤率計算如下，若

其值低於某個門檻值，則浮水印偵測成功。

$$E = \frac{1}{m} \sum_i |w_i - w'_i|$$

4. 實驗結果

我們以三張彩色影像 (Lena, Baboon, Peppers) 進行實驗，以驗證此方法的可行性。影像尺寸 $M \times M$ 為 512×512 ，區塊尺寸 $N \times N$ 為 32×32 ，影像共分割為 $16 \times 16 = 256$ 個區塊。為了避免列印掃描對於影像外側造成失真，我們忽略邊界區塊，將 $R = 14 \times 14 = 196$ 個區塊作離散餘弦轉換並將區塊重疊排列成為三維陣列： $32 \times 32 \times 196$ 。然後，鋸齒狀掃描每個區塊的係數並選擇 195 個中頻係數以嵌入浮水印 (195 個位元)，每 196 個係數嵌入一個浮水印位元。

我們使用 HP Color Laser Jet 380_dn 雷射印表機，以及 EPSON 1640_Su 掃描機，並以 600dpi 解析度列印影像，再以 600dpi 解析度掃描，實驗數據如表 2 所示，影像品質如表 3 所示，浮水印嵌入強度分別為 1.5 和 2。

表 2：機密訊息的驗證錯誤率

	嵌入強度	錯誤率
Lena	1.5	0.5%
	2.0	0.0%
Baboon	1.5	0.5%
	2.0	0.0%
Pepper	1.5	3.5%
	2.0	0.0%

表 3：嵌入浮水印影像品質 (PSNR)

嵌入強度	1.5	2
Lena	39.88	38.23
Baboon	39.46	37.05
Peppers	44.14	41.61

由以上實驗數據可見，嵌入強度設為 2.0 時，浮水印可完整取出，而且影像 PSNR 數值亦相當高。本實驗數據亦與 Shi 等學者之方法比較，該方法之錯誤率平均約為 5.5%，本論文之方法則為 0.0%。本論文之方法在影像品質方面亦表現較好，如表 4 所示。因此本論文所提出的方法不僅對於列印掃描攻擊有更好的強韌度，影像品質也較高。

表 4：影像品質比較 (PSNR)

	Shi 方法	本論文所提出的方法		
		$\alpha = 0$	$\alpha = 1.5$	$\alpha = 2$
Lena	33.59	42.17	39.88	38.23
Baboon	32.51	40.46	39.46	37.05
Peppers	33.61	47.07	44.14	41.61

5. 結論

本論文提出改善 Shi 等學者的方法，首先將影像切割成區塊再做 DCT 轉換，藉由調整係數正負號數量的關係來嵌入浮水印。本研究進行大量實驗，不僅探討 DCT 係數受到列印掃描攻擊的影響，亦分析修改係數對於影像畫質之衝擊。實驗數據證明，本論文所提出之浮水印嵌入法不僅可抵抗列印與掃描攻擊，浮水印的強韌度極高，而且影像亦可維持高畫質。

6. 參考文獻

- [1] 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.
- [2] Chengqing GUO, GuoaiX U, Xinxin NIU, Yixian YANG, and YangU, "A Color Image Watermarking Algorithm Resistant to

- Print-Scan,” *Wireless Communications, Networking and Information Security*, 2010, pp. 518–521.
- [3] K. Solanki, U. Madhow, B.S. Manjunath, S. Chandrasekaran, and I. El-Khalil, “Print and Scan Resilient Data Hiding in Images,” *Information Forensics and Security*, Vol. 4, 2006, pp. 464–478.
- [4] 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.
- [5] Yen-Chung Chiu and Wen-Hsiang Tsai, “Copyright Protection against Print-and-Scan Operations by Watermarking for Color Images,” *Journal of Information Science and Engineering*, Vol. 22, 2006, pp. 483–496.
- [6] Longjiang Yu, Xiamu Niu and Shenghe Sun, “Print-and-scan model and the watermarking countermeasure,” *Journal Image and Vision Computing archive*, Vol. 23, 2005, pp. 807–814.
- [7] Di Wu, Xuebing Zhou and Xiamu Niu, “A novel image hash algorithm resistant to print–scan,” *Special Section: Visual Information Analysis for Security*, Vol. 89, 2009, pp. 2311-2698.