以安全性考量的空間域浮水印策略

Watermarking approach with security in spatial mechanisms

楊政興
國立屏東教育大學資訊科學系
屏東市民生路 4-18 號
chyang@mail.npue.edu.tw

謝祥志
國立屏東教育大學資訊科學系
屏東市民生路 4-18 號
cm091121@mail.npue.edu.tw

翁麒耀
國立屏東教育大學資訊科學系
屏東市民生路 4-18 號
bm094108@mail.npue.edu.tw

摘要

Lin 學者於 2000 年提出新的浮水印嵌入方式，用以避免非法使用者將原圖以剪裁及資料壓縮的方式進行浮水印破壞；而在 2002 年，Chan 與 Cheng 兩位學者認為這樣的嵌入方式有其瑕疵，並提出影像攻擊方式。本論文我們將改善 Lin 學者所設計出的浮水印嵌入方式，加入 Random block、Random modulus 以及投票表決的觀念，進而增加其安全性；並以 Chan 與 Cheng 兩位學者的攻擊方式做測試，並分析模數 p 的適當範圍，最後以數據做結論，證實可以具有對抗影像壓縮的強韌度，並可減少此類攻擊所造成對藏入資訊的破壞。

Lin put forward the new method of watermark embedding, which was used to avoid that illegal users puncture data by cropping and making compression with the original image. However, in 2002, Chan and Cheng indicated that there existed weaknesses in Lin's embedding method and proposed attack method. In this paper, we add the ideas, random block, random modulus and vote scheme, into the blockwise scheme for the purpose of security. Also, we simulate the attack method designed by Chan and Cheng to our approach. The experimental results show that our approach is robust against the lossy compression and is strong against the attack of Chan and Cheng.

關鍵詞：Information Security (資訊安全); Watermark (浮水印); Lossy Compression(失真壓縮)

一、引言

由於近幾年來，網際網路的興起與資訊科技的蓬勃發展，以及網路傳輸的進步與技術成熟，促使資訊交流與存取更為快速與便捷，國與國之間的距離已經淡化，想藉由網路來傳遞大量的資料已非遙不可及的夢想。現今網際網路不但變得十分便利且內容豐富，使得現代人對網際網路的依賴性逐年升高。

一如現今在網際網路上的網頁，可以囊括敘述文字、多國語言、聲音、影像、影片等多媒體資訊。強大而廣闊的電腦網路脈絡與資訊數位化的世界潮流，造就了資訊的兩大特色：易於散佈與可變性。卻也因此，許多非法的複製、修改和散佈也正挑戰著數位化的道德觀念，當有心人士藉由網路挖取並竄改各種重要機密的時候，儲存在電腦內部的機密資訊該如何保護？我們又該如何避免讓非法的使用者輕易地更改重要資料呢？數位資訊的非法使用者，具有一別於傳統的非法手段，不僅難以追蹤，數位資料遭更改後，亦較難以判定著作權歸屬，因此，著作財產權的保障便顯得十分重要。

數位浮水印(Digital Watermarking)是保護數位資料財產權的方法之一，在浮水印技術的研究中，影像品質需求與結果之間有某些程度的衝突性。如強韌性(Robust)與隱蔽性(Imperceptibility)之間，便有著相當程度的衝突。而強韌的浮水印必需具備有強韌的抵抗破壞的能力，這些破壞包含失真壓縮(Lossy Compression)攻擊、雜訊(Noise)攻擊、剪裁(Cropping)攻擊等。

目前的數位影像存取方式可分成空間域(Spatial Domain)[10][11][12][18] 與頻率域(Frequency Domain)[6][7][9][15][17]兩種。空間域的浮水印嵌入方式主要分成 LSB(Least Significant Bit)[4]與 blockwize[8]兩種；而頻率域的浮水印嵌入方式，則是分成離散傅立葉轉換 DFT (Discrete Fourier Transform)[1] 、離散小波轉換 DWT (Discrete Wavelet Transform)[14][16]以及離散餘弦

轉換 DCT (Discrete Cosine Transform)[2][5][19]等。

空間域資訊以像素為基本的表示方式，藉由修改像素的灰階值達到嵌入浮水印的目的，雖然強韌性較頻率域來得不足，但嵌入量卻是較頻率域大。

本篇論文中，我們改善 Lin 在空間域提出的 blockwize 嵌入方式，加入 Random block、Random p 以及投票表決的觀念，並測試模數 p 的合理範圍；接著以 Chan 與 Cheng 兩位學者所提出的攻擊方式做測試，並加以分析。

本論文的組成如下：第二、三節分別介紹 Lin、Chan 與 Cheng 的方法，我們的方法在第四節提出，實驗結果在第五節展示，最後，在第六節提出結論。

二、文獻探討：Lin 的浮水印嵌入體制

該論文[13]選擇將資訊嵌入在影像中具有邊緣(Edge)特徵的鄰近區域，並且，為進一步加強對抗剪裁攻擊，可以集中將資訊嵌入在影像中具有重要特徵的地方。

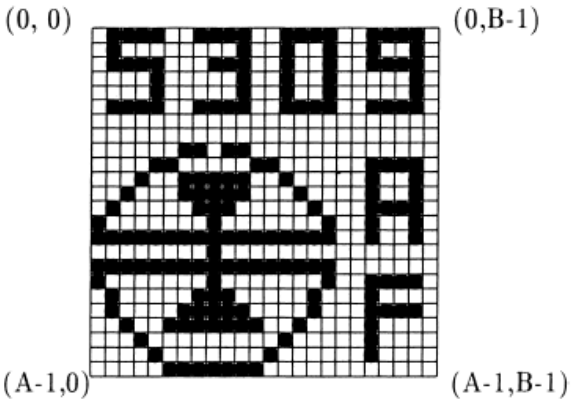


圖 1： 浮水印的範例

圖 1 為該論文所提供的浮水印範例，內含產品型號和序號等，大小為 A × B 之影像二元圖。該二元圖被轉換成位元字串(Binary bit string)，做為最後被嵌入的浮水印資料。另外，在嵌入過程中，選擇一個固定的數值 $2p$ ($0 < p < 10$)，用來做為浮水印嵌入(Embedding)和取出(Extraction)的模數。底下為其主要的演算法步驟：

1. 找出整個影像的所有邊緣像素。
2. 從邊緣像素中，依序選出嵌入的區域 $P_0, P_1, P_2, \cdots$，使得 P_i 和 P_j 的距離大於等於 7。
3. 在每個區域 P_i 中，利用下列方式藏入資訊：

(a) 分割 7 x 7 的區塊成四個 3 x 3 的區塊，將這些區塊稱為 b_k，$k = 4\,i + l$； $l = 0, 1, 2, 3$，每個 b_k 將會藏入一個浮水印位元。

(b) 由左而右，由上而下將區塊 b_k 中的九個元素標記為 P_{kj} ，$j = 1, 2, ..., 9$。如圖 2 所示 [13]。

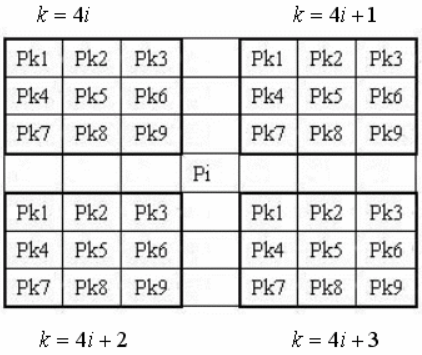


圖 2： 將 7 x 7 的區塊分割成 4 個 3 x 3 區塊

(c) 隨機重新排列像素 P_{kj}，j =1, 2, ..., 9，使之形成一個新順序 $P_{kj'}$; j'= 1, 2, ..., 9。

(d) 計算 $\mu_k = (\sum_{j'=1}^{9} v_{kj'}) / 9$ 和 $r_{\mu k} = \mu_k \pmod{2p}$，並根據以下的規則設定 $c_{\mu k}$：

$$
\begin{cases}
0 \le r_{uk} < \frac{p}{2} & \begin{cases} c_{uk} = \frac{p}{2} - r_{uk} & if \quad m_k = 0 \\ c_{uk} = -(\frac{p}{2} + r_{uk}) & if \quad m_k = 1 \end{cases} \\
\frac{p}{2} \le r_{uk} < \frac{3p}{2} & \begin{cases} c_{uk} = -(r_{uk} - \frac{p}{2}) & if \quad m_k = 0 \\ c_{uk} = (\frac{3p}{2} - r_{uk}) & if \quad m_k = 1 \end{cases} \\
\frac{3p}{2} \le r_{uk} < 2p & \begin{cases} c_{uk} = (\frac{3p}{2} - r_{uk}) & if \quad m_k = 0 \\ c_{uk} = -(r_{uk} - \frac{3p}{2}) & if \quad m_k = 1 \end{cases}
\end{cases}
\tag{1}
$$

其中 $v_{kj'}$ 代表像素 $P_{kj'}$的值(Intensity)，m_k 代表正要嵌入的浮水印位元。

(e) 根據以下的原則，變更區塊中每個像素值 $v_{kj'}$ ，來代表嵌入的浮水印位元 m_k：

$$
\begin{aligned}
v_{kj'} &= v_{kj'} + c_{\mu_k} - 2, \quad j' = 1 \\
v_{kj'} &= v_{kj'} + c_{\mu_k} - 1, \quad j' = 2, 3 \\
v_{kj'} &= v_{kj'} + c_{\mu_k}, \quad j' = 4, 5, 6 \\
v_{kj'} &= v_{kj'} + c_{\mu_k} + 1, \quad j' = 7, 8 \\
v_{kj'} &= v_{kj'} + c_{\mu_k} + 2. \quad j' = 9
\end{aligned} \tag{2}
$$

在上述的嵌入方式中，b_k 中的九個像素值被修正來滿足下列規範：平均像素值 $\mu_k \bmod 2p$，其值若為 $p/2$ 代表藏入位元 0，其值若為 $3p/2$，代表藏入位元 1。

浮水印萃取過程，可以利用上述規範來判斷被取出的位元為 0 或是 1。

三、文獻探討：Chan 與 Cheng 的攻擊方式

該論文[3]針對上一節所述 Lin 的浮水印技術，提出安全上的攻擊。在上述浮水印的萃取過程中，可以知道被萃取的浮水印位元 m'_k 是依賴區塊 b_k 中的平均像素值 μ'_k，這表示，如果區段 b_k 的平均像素值被改變，例如：

$$\mu''_k = \mu'_k + \alpha \tag{3}$$

被萃取的浮水印位元會因 α 值的大小而改變。例如：將 α 值的大小設定成滿足下列條件：

$$
\begin{aligned}
&0 \le \mu''_k \pmod{2p} < p \\
&\text{if} \quad p \le \mu''_k \pmod{2p} < 2p
\end{aligned}
$$

$$
\begin{aligned}
&p \le \mu''_k \pmod{2p} < 2p \\
&\text{if} \quad 0 \le \mu''_k \pmod{2p} < p
\end{aligned} \tag{4}
$$

則被萃取的浮水印位元會與最初的版本呈反白狀態。

再者，由於 b_k 的平均像素值 $\mu_k \bmod 2p$，其值為 $p/2$ 代表位元為 0，若為 $3p/2$ 代表位元為 1，所以只要將 α 設成滿足 $p/2 \le \alpha < 3p/2$，被萃取的浮水印就會被反白。例如：假設以 Lin 的方法來嵌入浮水印，且令 $p = 7$，接著加上 $\alpha = 5$ 作攻擊，則萃取出來的浮水印如圖 3(b)[3]。另外，若只針對部分區塊的平均像素值增加 α，則所取出的浮水印將難以辨別，如圖 3(d)[3]。

(a) **(b)**

(c) **(d)**

圖 3：(a) 將 α = 5 加入四個 3 x 3 的區塊中的所有像素後之影像(PSNR=37.41 dB)。(b)從(a)圖中所萃取出的浮水印(正確率 = 0%)。(c) 把 α = 5 加入四個 3 x 3 的區塊中的兩個後的影像 (PSNR=39.25 dB)。(d)從(c)圖中所萃取出來的浮水印(正確率 = 56.78%)

四、改良方式

為了克服 Chan 與 Cheng 的攻擊方式，我們提出新的浮水印技術，該技術藉由下列三個方法，來改善 Lin 的方法：

(一) Random block

為了避免用來藏入浮水印位元的區塊(Block)，其位置與組成像素輕易的就被確認，我們提出 Block 是由亂數隨機選取的像素所組成，稱為 Random block。為了不增加演算法的複雜度，我們採取固定大小的區塊，例如 3 x 3。當然，不同的區塊其取得之像素不應重複，我們只須額外記錄產生亂數的種子(Seed)，該亂數所產生的數值不應重複。例如，使用 $f(x) = (k_0 + k_1 \times x) \bmod s$，其中 x 是像素的位置，k_0 和 k_1 是亂數種子(Seed)，且 $\gcd(k_1, s) = 1$，s 則為浮水印的大小 。

(二) Random modulus

為了讓攻擊者無法藉由將像素值加上固定大小的 α 值，就輕易的將內藏的浮水印破壞，用來嵌入浮水印的模數 $2p$ 並不採用固定數值，而是由亂數產生，稱為 Random modulus。每個區塊所使用的模數值都不盡相同，我們只須額外記錄產生亂數的種子，並使得所產生的亂數值 $2p$ 在合理的範圍內，有關 $2p$ 數值的合理範圍，我們將於下一節中加以闡述。

(三) 投票表決機制

為了增加浮水印的強韌性，可以就區塊大小、模數大小以及嵌入浮水印次數來做調整。由於前兩項參數已定，所以我們利用嵌入多次浮水印與投票表決機制來增進強韌性。雖然此方法會降低整體資訊嵌入量，但一般而言，浮水印通常不會有太多的嵌入量，很少會有隱藏大量的浮水印的情形。

我們將每個要嵌入的位元，分別嵌入 3 個不同的區塊中。在萃取出來的時候，若是該浮水印位元為 1 的次數為 2 或 3，則認定此浮水印位元為 1；反之，若是浮水印位元為 0 的次數為 2 或 3，則認定此浮水印位元為 0。

嵌入策略的整體演算法描述如下：

針對每個欲藏入的浮水印位元 m_k，完成下面步驟：

1. 建立三個大小為 3 x 3 的 Random block b_{k1}, b_{k2}, b_{k3}。

2. 產生三個 Random modulus $2p_{k1}$, $2p_{k2}$, $2p_{k3}$。

3. 參考 Lin 學者的方法，分別調整 b_{k1}, b_{k2} 和 b_{k3} 內的像素值，使調整後的平均像素值 μ_{k1}, μ_{k2}, μ_{k3} 滿足下列條件：

若 m_k 為 0，則

$$\begin{aligned} \mu_{k1} \bmod 2p_{k1} &= 1/2\ p_{k1} \\ \mu_{k2} \bmod 2p_{k2} &= 1/2\ p_{k2} \\ \mu_{k3} \bmod 2p_{k3} &= 1/2\ p_{k3} \end{aligned}$$

若 m_k 為 1，則

$$\begin{aligned} \mu_{k1} \bmod 2p_{k1} &= 3/2\ p_{k1} \\ \mu_{k2} \bmod 2p_{k2} &= 3/2\ p_{k2} \\ \mu_{k3} \bmod 2p_{k3} &= 3/2\ p_{k3} \end{aligned} \qquad (5)$$

五、結果分析

我們以自製、大小為 64 x 64 的浮水印二元圖作實驗，浮水印如圖 4(a)，嵌入於圖 4(b)的 512 x 512 Lena 灰階原圖；以 Random block、Random modulus 嵌入後的圖如圖 4(c)，加入投票機制，則嵌入後的 Lena 圖則是圖 4 (d)。

(一) 抗壓縮實驗

(a) 使用 Random block 與 Random modulus

由於模數 $2p$ 的值越大，則藏入浮水印後的影像圖，其相對於原圖的的 PSNR 值會越小，但是其浮水印的強韌性會越高。因此必須定出 $2p$ 的合理範圍，以作為演算法中 Random modulus 選取之用。表 1 列出不同的 $2p$ 值，其藏入浮水印後之 PSNR 值，以及針對 1:10 和 1:20 壓縮比後，其所萃取出的浮水印位元正確率。由表 1 的數據中可分析出，當 $2p$ 值的範圍大於 37 以後，其嵌入之 PSNR 值將小於 30，所以，$2p$ 值介於 5~37 之間是可接受的範圍。表 1 之最後一列為 $2p$ 值介於 5~37 之間的亂數時，所獲得之結果。圖 5 (a)和(b)顯示其所萃取出的浮水印。

(a)

(b)

(c)

(d)

圖 4： (a)自製的 64 x 64 pixels 浮水印二元圖。(b)512 x 512 pixels Lena 原圖。 (c)以 Random block 與 Random modulus 嵌入後的 Lena 圖(PSNR=37.83(dB))。 (d)以 Random block 與 Random modulus 及投票表決機制嵌入後的 Lena 圖(PSNR=32.69(dB))。

表 1：將浮水印以 Random block、Random modulus 以及投票機制的方式嵌入，針對影像作 1:10 和 1:20 的壓縮後，所萃取出的浮水印位元正確率

Random block and Random modulus			加入投票表決機制		
	1：10 壓縮	1：20 壓縮		1：10 壓縮	1：20 壓縮
$5 \le 2p \le 10$ PSNR=44.73	96.09%	90.97%	$5 \le 2p \le 10$ PSNR=43.87	96.82%	94.10%
$10 < 2p \le 15$ PSNR=43.83	96.83%	92.19%	$10 < 2p \le 15$ PSNR=42.79	97.24%	94.94%
$15 < 2p \le 20$ PSNR=39.49	97.07%	93.65%	$15 < 2p \le 20$ PSNR=38.63	97.65%	95.76%
$20 < 2p \le 25$ PSNR=37.43	97.56%	94.38%	$20 < 2p \le 25$ PSNR=36.46	98.16%	96.17%
$25 < 2p \le 30$ PSNR=34.69	98.05%	95.61%	$25 < 2p \le 30$ PSNR=33.83	98.75%	96.17%
$30 < 2p \le 35$ PSNR=31.83	98.29%	96.34%	$30 < 2p \le 35$ PSNR=30.69	99.03%	97.65%
$35 < 2p \le 40$ PSNR=29.25	99.02%	97.56%	$35 < 2p \le 40$ PSNR=28.76	99.76%	98.13%
$35 < 2p \le 37$ PSNR=30.26	98.78%	97.35%	$35 < 2p \le 37$ PSNR=29.83	99.58%	98.87%
$5 \le 2p \le 37$ PSNR=37.83	97.36%	94.03%	$5 \le 2p \le 37$ PSNR=34.67	98.67%	96.49%

(a) **(b)**

(c) **(d)**

圖 5： 以 $5 \le 2p \le 37$ 做測試。(a)1:10 壓縮萃取出來的浮水印二元圖(正確率=97.36%)。(b)1:20 壓縮萃取出來的浮水印二元圖。(正確率=94.03%) (c)加入投票表決機制，1:10 壓縮萃取出來的浮水印二元圖。(正確率=98.67%) (d)加入投票表決機制，1:20 壓縮萃取出來的浮水印二元圖(正確率=96.49%)。

(b) 加入投票表決機制

表 1 之右半部顯示加入投票表決機制後之實驗結果。雖然使用投票表決機制，使得浮水印嵌入之 PSNR 值降低，但圖像壓縮後再萃取出來的正確性卻提高了。當加入投票機制時，2*p* 值的適切範圍則是落在 5~35 之間。為利比較，表 1 之最後一列右半部，仍然呈現 2*p* 值介於 5~37 之間的亂數時，所獲得之結果。圖 5 (c)和(d)顯示其所萃取出的浮水印。

由上述結果可知，我們的方法可以有效對抗壓縮處理。

(二) 對抗 Chan 與 Cheng 的攻擊

針對 Chan 與 Cheng[3]攻擊的方式，我們模擬出下列三種攻擊策略：

(a) 對所有區塊之像素值都加上固定 *p* 值

(b) 對任意區塊之像素值隨意加上固定 *p* 值或不加 *p* 值

(c) 對所有區塊之像素值都加上隨意 *p* 值

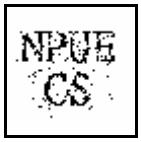
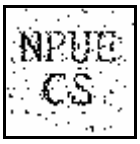
由於攻擊者無法確知區塊是由哪些像素所組成，我們假設其將整個影像以棋盤方式分割成大小為 3 x 3 之不重疊區塊。表 2 分別列出受到各種攻擊後之結果，其中固定 *p* 值，我們選取合理 *p* 值範圍之中間值，即令 $p = 10$。由表 2 所呈現出的數據得知，我們的方法可以有效對抗此類攻擊策略。所有浮水印位元的正確率都在八成以上，且都可以利用肉眼輕易判斷出浮水印。

六、結論

我們以 2000 年 Lin [13]提出的浮水印嵌入方式，加入 Random block、Random modulus 以及投票表決機制三個方法加以改良，再使用 Chan 與 Cheng[3]所設計的攻擊方法實驗，發現這樣的浮水印嵌入方式，由於 Random block 與 Random modulus 是亂數產生，且 *p* 值的範圍是由實驗結果合理訂定，使得失真壓縮與隨意增加 *p* 值的攻擊方法，都無法有效的破壞浮水印；若是加入投票表決機制，則位元正確率會相對的提高。

由數據分析可得：單純使用 Random block 與 Random modulus 的方式嵌入浮水印，2*p* 的值域介於 5~37 之間，則 PSNR 可大於 30 的臨界值；若為了提高浮水印位元正確率，加入投票表決機制後，則 2*p* 的值域介於 5~35 之間較為理想。

表 2：將浮水印以 Random block、Random modulus 以及投票機制的方式嵌入後，利用 Chan 與 Cheng 的方式攻擊，其所對應攻擊後之影像和萃取出的浮水印。

	Random block 與 Random modulus	加入投票表決機制
(a) 全部加 *p*	  浮水印位元正確率=84.63% PSNR=33.43	  浮水印位元正確率=88.46% PSNR=32.31
(b) 對任意 block 加 *p* 或不加 *p*	  浮水印位元正確率=86.97% PSNR=33.27	  浮水印位元正確率=94.63% PSNR=31.93
(c) 加任意 *p*	  浮水印位元正確率=76.05% PSNR=31.83	  浮水印位元正確率=84.20% PSNR=30.19

七、參考文獻

[1] F. Alturki, R. Mersereau, “Secure blind image steganographic technique using discrete Fourier transformation” , in: Proceedings of 2001 International Conference on Image Processing, Thessaloniki, Greece, pp. 542-545, 2001.

[2] A.G. Bor, I. Pitas, “Image watermarking using DCT domain constraints”, Proceedings of 1996 IEEE International Conference on Image Processing (ICIP’96), vol. 3, pp. 231-234, 1996.

[3] C.K. Chan, L.M. Cheng, “Security of Lin’s

image watermarking system", The Journal of System and Software, vol. 62, pp. 211-215, 2002.

[4] C.K. Chan, L.M. Chen, "Hiding data in images by simple LSB substitution", Pattern Recognition, vol. 37, no. 3, 4 pp. 69-474, 2004.

[5] C.C. Chang, T.S. Chen, L.Z. Chung, "A steganographic based upon JPEG and quantization table modification", Inform.Sci., vol. 141, no. 1-2, pp. 1579-1587, 2002.

[6] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997.

[7] F. Hartung, B. Girod, "Watermarking of MPEG-2 encoded video without decoding and re-encoding", Signal Processing, vol. 66, pp. 283-301, May 1998.

[8] M. Holliman and N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes", IEEE Transactions. Image Processing, vol. 3, pp. 432-441, Mar. 1997.

[9] C.T. Hsu, J.L. Wu, "Hidden digital watermarks in images", IEEE Transactions on Images Processing, vol. 8, pp. 58-68, Jan. 1999.

[10] M.S. Hwang, C.C. Chang, K.F. Hwang, "A watermarking technique based on one-way hash functions", IEEE Transactions on Consumer Electronics, vol.45, no.2, pp. 286-294, 1999.

[11] M. Kutter, F. Jodran, F. Bossen, "Digital watermarking of color image using amplitude modulation", Journal of Electronic Imaging, vol. 7, no. 2, pp. 326-332, 1998.

[12] G.C. Langelaar, J.C.A. van der Lubbe, R.L. Lagendijk, "Robust labeling methods for copy protection of images", Proceedings of SPIE Electronic Imaging' 97,Storage and Retrieval for Image and Video Database V, San Jose(CA), pp. 298-309, Feb. 1997.

[13] P.L. Lin, "Robust transparent image watermarking system with spatial mechanisms", The Journal of Systems and Software, vol. 50, pp. 107-116, 2000.

[14] H. Noda, J. Spaulding, M.N. Shirazi, E. Kawaguchi, "Application of bit-plane decomposition steganography to JPEG2000 encoded images", Signal Proc. Lett., vol. 9, no. 12, pp. 410-413, 2002.

[15] C.I. Podilchuk, W. Zeng, "Image -adaptive watermarking using visual models",IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 525-539, May 1998.

[16] J. Spaulding, H. Noda, M.N. Shirazi, E.Kawaguchi, "BPCS steganography using EZW lossy compressed images", Pattern Recognition Lett., vol. 23, no. 13, pp. 1579-1587, 2003.

[17] P.C. Su, C.C.J. Kuo, H.J.M. Wang, "Blind digital watermarking for cartoon and map images", Proceedings of SPIE Security and Watermarking of Multimedia Contents, vol. 3657, pp. 296-306, Jan. 1999.

[18] C.C. Thien, J.C. Lin, "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function", Pattern Recognition, vol. 36, pp. 2875-2881, 2003.

[19] H.W. Wong, C. Au, W.C. Wang, "Data hiding and watermarking in JPEG compressed domain by DC coefficient modification", Proceedings of SPIE Symposium of Security and Watermarking of Multimedia Contents 2000, San Jose, vol. 3971, pp. 237-244, January 2000.