基於 LSB 的適性高負載資訊隱藏法

冷輝世*[ab]、游孟霖[a]、曾顯文[b]
國立彰化師範大學數學系[a]
朝陽科技大學[b]

摘要－在資訊隱藏領域中，藏量與失真度是兩項重要的指標。本研究嘗試利用著名的邊緣檢測法（Median Edge Detection，以下簡稱 MED）判定平坦區與複雜區，並結合人類視覺系統的概念在平坦區嵌入較少的機密訊息，在複雜區嵌入較多的機密訊息以增加藏量。由於 MED 預測值的不準確性，本研究使用最低有效位元（Least Significant Bit，以下簡稱 LSB）藏匿法以及最佳化像素調整（Optimal Pixel Adjustment Process，以下簡稱 OPAP）的方法嵌入機密訊息以減少失真度。實驗結果顯示本研究可以得到高藏量與低失真的效果。

一、前言

在資訊隱藏領域中，藏量與失真度是兩項重要的指標。一般而言，人類視覺系統（Human Vision System，以下簡稱 HVS）對平坦區的變化較爲敏感，也就是周圍的像素值都很相近，那麼此像素點有小幅度的變化都很容易被察覺出來；相對的，對於複雜區，也就是周圍的像素值差異很大，那麼此像素點就算有大幅度的變化，也不容易被察覺。本研究利用邊緣檢測法（Median Edge Detection，以下簡稱 MED）判定平坦區與複雜區，並結合 HVS 的概念嵌入機密訊息，若是平滑區，則嵌入較少的訊息，若是複雜區則嵌入較多的訊息。實驗結果顯示本研究的方法可以得到高藏量與低失真的效果，並且可以避免針對 LSB 的僞寫分析的攻擊。

二、相關研究

以下分別介紹 LSB（Least Significant Bit，以下簡稱 LSB）藏匿法、OPAP（Optimal Pixel Adjustment Process，以下簡稱 OPAP）以及 MED（Median Edge Detection，以下簡稱 MED）。

2.1 LSB 藏匿法

Chan 等學者(2004)[2]所提出的 LSB 藏匿法是著名的不可逆式藏匿法，其優點是高藏量與低失真度。此法將機密訊息隱藏在圖像像素值的最後的 n 個位元，在藏匿的過程中，機密訊息與像素值皆以二進位表示。

例如：像素值 x=153=$(10011001)_2$，要藏入 3 位元的機密訊息爲$(110)_2$，將機密訊息藏入後得到新的像素值 y=$(10011\mathbf{110})_2$=158。

2.2 OPAP

LSB 藏匿法的缺點是當欲藏入的機密訊息長度越長，則隱藏後得到的新圖像品質就越差。Chan 等學者(2004)[2]另外提出了 OPAP 以改善僞裝影像的失真度。

假設 x 是圖像中某個像素值、y 是 x 經過 LSB 藏匿法得到的新像素值，z 是 y 經過 OPAP 得到的新像素值，假設 d=y-x，根據 LSB 藏匿法，在 x 藏入長度爲 n 位元的機密訊息可得到 y，因此，

$$d \in \left[2^{-n}, 2^{n}\right] \tag{1}$$

其中依照 d 值的範圍，有不同的處理方法：

$$\begin{aligned} &\text{方法一}: d \in \left(2^{n-1}, 2^{n}\right) \\ &If\ \ y \geq 2^{n}, then\ z = y - 2^{n}, otherwise\ z = y \\ &\text{方法二}: d \in \left[-2^{n-1}, 2^{n-1}\right] \\ &z = y \\ &\text{方法三}: d \in \left(-2^{n}, -2^{n-1}\right) \\ &If\ \ y < 256 - 2^{n}, then\ z = y + 2^{n}, otherwise\ z = y \end{aligned} \tag{2}$$

假設一：影像中某像素值 x=25=$(00011001)_2$，在像素值中藏入 3 位元（n=3）的機密訊息$(111)_2$，得到新的像素值 y=31=$(00011\mathbf{111})_2$，可算出兩像素的差值 d=y-x=31-25=6，依照 d 值判斷，由(2)此情況適用方法一，因爲 $y = 31 \geq 2^3$，所以得到新的像素值 z=y-2^3=31-8=23=$(0001\mathbf{0111})_2$，則誤差由 6 減少爲 2。

假設二：影像中某像素值 x=26=$(00011010)_2$，在像素值中藏入 3 位元（n=3）的機密訊息$(101)_2$，得到新的像素值 y=29=$(00011\mathbf{101})_2$，可算出兩像素的差值 d=y-x=29-26=3，依照 d 值判斷，由(2)此情況適用方法二，因此得到新的像素值 z=y=29。

假設三：影像中某像素值 x=7=$(00000111)_2$，在像素值中藏入 3 位元（n=3）的機密訊息$(001)_2$，得到新的像素值 y=1=$(00000001)_2$，可算出兩像素的差值 d=y-x=1-7=-6，依照 d 值判斷，由(2)此情況適用方法三，因爲 $y = 1 < 256 - 2^3 = 248$，所以得到新的像素值 z=y+2^3=1+8=9=$(00001001)_2$，則誤差由 6 減少爲 2。

以上的各項假設經由 OPAP 可使誤差的絕對值小於 2^{n-1}（其中 n 爲欲嵌入的機密訊息位元長度）。

2.3 MED

Weinberger 等學者(2000)[3]提出的 MED 是著名的邊緣檢測法，除了預測是否有邊緣存在之外，並可預測目標像素的預測值。但是本研究發現，其預測誤差變動範圍非常大。換句話說，若是以一般的差值做爲藏入機密訊息長度的依據會造成高度失真。

MED 是用目標像素點 x 附近的三個像素點 a、b、c，

Corresponding author:lenghs@cc.ncue.edu.tw
DOI:10.6159/IJSE.2014.(4-1).58

來預測 x 的像素值 $\hat{x}$。

$$\hat{x}=\begin{cases}\min\{a,b\} & if\ \ c\geq\max\{a,b\}\\ \max\{a,b\} & if\ \ c\leq\min\{a,b\}\\ a+b-c & otherwise\end{cases} \quad (3)$$

c	b
a	x

圖一：目標素點 x 與鄰近像素示意圖

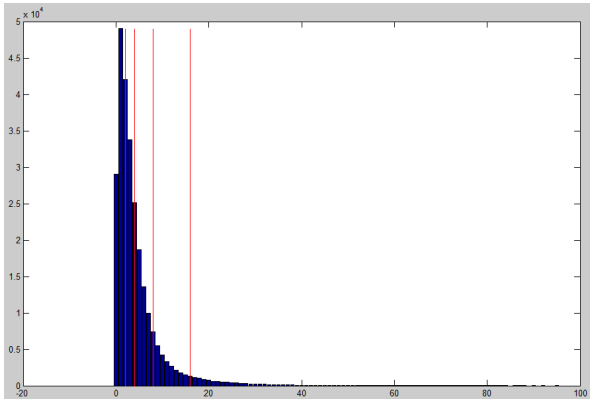
本研究僅利用其判斷是否存在邊緣的特性：若 $c\geq\max\{a,b\}$ 或 $c\leq\min\{a,b\}$，則表示存在邊緣，則稱之爲複雜區，否則不存在邊緣則稱之爲平坦區。

以下說明不使用 MED 的預測值來當作訊息藏匿主要依據的原因。以 SIPI 影像資料庫中的 Lena 圖與 Baboon 圖爲例（如圖二）。

(a)Lena (b)Baboon

圖二：SIPI 影像資料庫中的 Lena 圖與 Baboon 圖

圖三與表 I 爲 Lena 圖的誤差統計圖與誤差累計百分比，其 $n\leq16$ 的百分比達 95.84%。表示 MED 預測值還算精確。（紅線是相對於 LSB+OPAP 的 n 值）

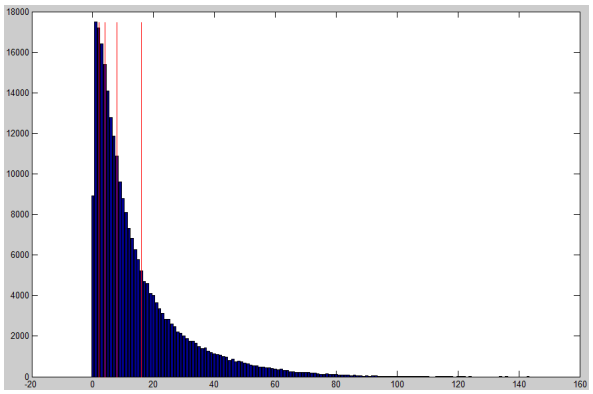


圖三：Lena 圖的誤差值統計圖

表 I
Lena 圖誤差累計百分比

n	$n\leq2$	$n\leq4$	$n\leq8$	$n\leq16$
累計百分比	45.85%	68.31%	87.25%	95.84%

圖四與表 II 爲 Baboon 圖的誤差統計圖與誤差累計百分比，由於 Baboon 圖是偏向於複雜的圖形其 $n\leq16$ 的百分比只有 69.78%。很明顯的，表示 MED 預測值並不準確。（紅線是相對於 LSB+OPAP 的 n 值）



圖四：Baboon 圖的誤差統計圖

表 II
Baboon 誤差累計百分比

n	$n\leq2$	$n\leq4$	$n\leq8$	$n\leq16$
累計百分比	16.64%	28.77%	47.69%	69.78%

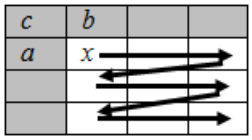
因此，本研究不選擇 MED 的預測值來做爲藏匿訊息的依據，而是使用 LSB+OPAP，當嵌入 n 個位元時，誤差的絕對值小於 2^{n-1}。

三、研究方法

以下分別說明機密訊息的藏匿方法與取出方法。

3.1 藏匿方法

藏匿過程分成兩個階段進行，首先針對第一行與第一列中的每個像素點，均使用 LSB+OPAP 藏入(n-1)個位元的機密訊息，如圖五的灰色部份。



圖五：第一階段嵌入

接著將圖五中其它白色部份，依 zig-zag 方式，利用(3)判別是否存在邊緣。若是，則藏入 n 個機密訊息；若否，則藏入(n-1)個機密訊息以符合 HVS。

舉例說明如下：假設 n=3，目標像素 x=55=(110**111**)$_2$，其附近的像素點 a=28、b=47、c=20，首先利用(3)進行預測。因爲 $c\leq\min\{a,b\}$，可知存在邊緣，假設要藏入的機密訊息爲(000)$_2$，先經過 LSB 藏匿得到 y=48=(110**000**)$_2$，在經過 OPAP 調整，可得 d=-7，由(2)，此情況適用方法一，藏匿後得到新的像素點 z=56=(111**000**)$_2$。依此類推，可對整張影像做藏入的處理，最後得到藏有機密訊息的僞裝影像。

3.2 取出方法

首先要取出圖五中灰色區域的機密訊息，直接將像素值 x 以二進位表示後，取出最後(n-1)個位元爲爲機密訊息。其次要取出圖五中白色區域的機密訊息，以 zig-zag 的方式依次對像素值 x 進行 MED 預測，判別是否存在邊緣。若是則將像素值 x 以二進位表示後，取出最後 n 個位元；若否，則取出最後(n-1)個位元。

例如：n=3，目標像素 x=56 爲圖五中白色區域的像素點，其鄰近像素 a=28、b=47、c=20，則進行 MED 預測。由(2)，因爲 $c \le \min\{a,b\}$，可知存在邊緣，將 x=56 表示成二進位$(111000)_2$，取出最後三位元$(000)_2$，即可取出藏匿在目標像素的機密訊息。

四、實驗結果

本研究採用 SIPI 影像資料庫中的 Lena、Tiffany、Baboon、F16、Scene 和 Peppers 這六張影像做爲實驗對象，並以 LSB 藏匿法、OPAP 與本研究的方法做比較（如圖六）。

(a) Lena (b) Peppers

(c) Tiffany (d)F16

(e) Scene (f) Baboon

圖六：SIPI 影像資料庫的六張實驗影像

表Ⅲ至表Ⅷ中的 n 值，對於 LSB 與 OPAP 是指嵌入機密訊息的長度，對本研究方法則是有兩種不同的意義，若是該目標像素被判定爲有邊緣存在，表示此像素位於複雜區，則嵌入 n 個位元；若否，表示此像素位爲平坦區，則嵌入(n-1)個位元。

一般而言，自然影像中的平坦區會遠多於複雜區，所以表Ⅲ至表Ⅷ比較使用平坦區的 n 值作爲對照。以表Ⅲ爲例，n=4 時，OPAP 方法的 Payload 爲 4bpp，PSNR 值爲 34.80dB，對照於本研究方法應採用 n=5，Payload 爲 4.68bpp，PSNR 值爲 30.02dB。表示本研究在符合 HVS 的情況下具有高藏量。

此外，本研究是基於影像本身的邊緣特性，對於不同的目標像素藏入不同長度的機密訊息，。所以可避免針對 LSB 的僞寫分析的攻擊[1]。

表Ⅲ
Lena 圖的實驗結果

Lena		LSB	OPAP	本研究方法
n=2	Payload	2.00	2.00	1.70
	PSNR	44.15	46.37	47.36
n=3	Payload	3.00	3.00	2.69
	PSNR	37.92	40.72	41.83
n=4	Payload	**4.00**	**4.00**	3.68
	PSNR	**31.78**	**34.80**	35.97
n=5	Payload	5.00	5.00	**4.68**
	PSNR	25.86	28.81	**30.02**

表Ⅳ
Tiffany 圖的實驗結果

Tiffany		LSB	OPAP	本研究方法
n=2	Payload	2.00	2.00	1.71
	PSNR	44.16	46.34	47.27
n=3	Payload	3.00	3.00	2.70
	PSNR	37.91	40.65	41.73
n=4	Payload	**4.00**	**4.00**	3.69
	PSNR	**31.82**	**34.67**	35.82
n=5	Payload	5.00	5.00	**4.68**
	PSNR	26.10	28.36	**29.57**

表Ⅴ
Baboon 圖的實驗結果

Baboon		LSB	OPAP	本研究方法
n=2	Payload	2.00	2.00	1.63
	PSNR	44.15	46.37	47.61
n=3	Payload	3.00	3.00	2.63
	PSNR	37.92	40.74	42.08
n=4	Payload	**4.00**	**4.00**	3.63
	PSNR	**31.86**	**34.81**	36.19
n=5	Payload	5.00	5.00	**4.64**
	PSNR	25.81	28.81	**30.19**

表Ⅵ
F16 圖的實驗結果

F16		LSB	OPAP	本研究方法
n=2	Payload	2.00	2.00	1.69
	PSNR	44.16	46.37	47.40
n=3	Payload	3.00	3.00	2.68
	PSNR	37.98	40.73	41.89
n=4	Payload	**4.00**	**4.00**	3.67
	PSNR	**31.84**	**34.82**	36.04
n=5	Payload	5.00	5.00	**4.67**
	PSNR	26.07	28.82	**30.07**

表Ⅶ
Scene 圖的實驗結果

Scene		LSB	OPAP	本研究方法
n=2	Payload	2.00	2.00	1.68
	PSNR	44.16	46.37	47.40
n=3	Payload	3.00	3.00	2.68
	PSNR	37.91	40.73	41.89
n=4	Payload	**4.00**	**4.00**	3.66
	PSNR	**31.86**	**34.82**	36.05
n=5	Payload	5.00	5.00	**4.66**
	PSNR	25.78	28.80	**30.10**

表Ⅷ
Peppers 圖的實驗結果

Peppers		LSB	OPAP	本研究方法
n=2	Payload	2.00	2.00	1.73
	PSNR	44.16	46.38	47.26
n=3	Payload	3.00	3.00	2.72
	PSNR	37.92	40.72	41.70
n=4	Payload	**4.00**	**4.00**	3.70
	PSNR	**31.81**	**34.81**	35.90
n=5	Payload	5.00	5.00	**4.68**
	PSNR	25.75	28.82	**29.98**

五、結論

本研究是基於影像本身的邊緣特性，利用著名的 MED 邊緣檢測法判定平坦區與複雜區，結合 HVS 的概念，在平滑區嵌入(*n*-1)個位元，複雜區嵌入 *n* 個位元。實驗結果顯示本研究的方法可以得到高藏量與低失真的效果。此外，由於本研究對於不同的目標像素藏入不同長度的機密訊息，所以可避免針對 LSB 的偽寫分析的攻擊。

參考文獻

[1] W. J. Chen, C. C. Chang, T. Le. “High payload steganography mechanism using hybrid edge detector,” *Expert Systems with Applications*, 2010, pp. 3292-3301.

[2] C. K. Chan, L. M. Cheng. “Hiding data in images by simple LSB substitution, ” *Pattern recognition* , 2004, pp. 469-474.

[3] M. L. Weinberger, Seroussi G, “The LOCO-I lossless image compression algorithm:principles and standardization into JPEG-LS, ” *IEEE Trans. Image Process*, 2000, pp. 1309-1324.