

行政院國家科學委員會專題研究計畫期中報告

影像的快速分享與高容量隱藏、及它們在影像修復的應用(第二年期)

Fast sharing, high-capacity hiding, and their applications in images' recovery

計畫編號：NSC 97-2221-E-009-120-MY3

執行期限：98年8月1日~99年7月31日

主持人：林志青 交通大學資訊科學系所

計畫參與人員：陳李書滕、林憲正

交通大學資訊工程系所

一、 中文摘要

本計畫為期三年，其目的是提出快速影像分享與高容量資訊隱藏方法，及其在影像修復的應用。本年(第二年)的主題是高容量資訊隱藏方法與資訊隱藏量之上限研究。第二年第一個主題是以邊緣吻合向量量化為基礎的資訊隱藏。在本主題中，我們希望研究出一個機密資訊隱藏方法，可以藏入較高的資訊量，而仍然保有較佳的偽裝影像品質。第二年第二個主題是基於機密影像中相鄰像素間相似性而得的高容量資訊隱藏方法。在本主題中，我們希望藏入的機密影像大小可以與掩護影像同大小，並且方法還能兼顧欲保護的機密影像的隱匿性與影像品質。第二年第三個主題為資訊隱

藏量之上限研究。在本主題中，我們希望在給定任意 256 色灰階掩護影像，並在指定的影像品質之下，研究出該掩護影像的隱藏容量上限。第二年第四個主題為基於多維像素空間而得的影像隱藏方法。在本主題中，我們希望研究如何在高維像素空間做影像隱藏的研究，藉以提昇隱藏的容量。

關鍵詞：資訊隱藏；隱藏容量上限；高維像素，多維球體空間。

Abstract

This project is the second part of a three-year project. The goal of the three-year project is to provide fast secret image sharing methods,

high-capacity hiding schemes, and their applications in images' recovery. The second year is for the high-capacity data hiding and the upper bound estimate of the hiding capacity. There are four topics in the second year. The first topic is the data hiding technique based on side match vector quantization. The goal of this topic is to design a data hiding scheme that provides a high hiding capacity and good stego-image quality. The second topic is the high-capacity data hiding approach based on the correlation of the neighboring pixels of a secret image. The goal of this topic is to design an image hiding scheme that provides a high hiding capacity such that the embedded secret image can be as large as the cover image and the generated stego-image quality is acceptable. The third topic is the upper bound estimate of the hiding capacity. The goal of this topic is present a way to provide an upper bound estimate when a grayscale cover image and a PSNR value are given. The fourth topic is the

image hiding technique based on a multidimensional pixel space. The goal of this topic is to design an image hiding scheme in a multidimensional pixel space to increase hiding capacity.

二、計畫緣由與目的

本年度(第二年)的第一個主題是：以邊緣吻合向量量化為基礎的資訊隱藏方法。在資訊隱藏法中，藏入資訊量的多寡與偽裝影像的品質的好壞往往是一個取捨問題，也就是若藏入較高資訊量，則其偽裝影像的品質會較差；若藏入較低的資訊量，則其偽裝影像的品質會較佳。因此我們希望設計出一個以邊緣吻合向量量化為基礎的資訊隱藏方法，相較於前人所設計之邊緣吻合向量量化式的資訊隱藏法，此方法可以藏入較高的資訊量，而仍然保有較佳的偽裝影像品質。

本年度的第二個主題是：基於機密影像中相鄰像素間相似性的高容量資訊隱藏方法。一般來說，影像的資訊量都很大，因此若要將與掩護影像大小相同之機密影像藏入於該掩護影像，是有難度的。但由於人類的視覺

系統相對於電腦的量化數據而言較為遲鈍，亦即人眼是無法分辨影像本身的細微變化。因此我們利用此一現象配合影像鄰近周圍的像素具有極高的相似性，讓藏入至掩護影像的機密影像可以容忍有一點失真，但藏入的機密影像大小可以是掩護影像的大小。

第二年計畫的第三個主題是資訊隱藏量之上限研究。在許多的應用上，如何去評估一張影像的資訊隱藏量是重要的課題。因為我們可以在做隱藏之前便可以大略評估一下到底機密資訊是否可以隱藏進去，進而省去許多無謂的嘗試時間。一般而言，一個好的影像隱藏方法可以在差不多的影像品質之下，達到較高的資訊隱藏量；但是，我們知道不管是如何優秀的資訊隱藏法，總會有一個理論上的極限（例如，一張 256×256 大小的 8 位元灰階影像不可能放進 512×512 byte 大小且不壓縮的機密資訊）。有些人可能在評估一張偽裝影像的隱藏容量大小時，指定一個特定的影像隱藏方法（例如，在 LSB 的方法之下），但是這種資訊隱藏量的評估方法會受到所使用的影像隱藏方法影響，所估計出來的數字並無法代表該影像真正的資訊隱藏量的極限。而本題目便是希望可以研究出一套測量的方法以量度

每張影像的容量上限。這個上限值所表示的是一個天然障礙（亦即不存在可以突破此上限的資訊隱藏法）。我們也希望這個計算方法可以簡單的計算出來（而不是利用大量的模擬來估計出解答）。

第二年計畫的第四個主題是基於多維像素空間而得的影像隱藏方法。過去的研究觀察到，當我們想要對影像做向量量化壓縮的時候，向量量化的效果總是會比純量量化的效果好上一些。而我們也發現到，這樣的特性也存在於影像隱藏的領域之中。因此本題目主要便是將目前的影像隱藏方法以高維度像素空間的角度觀察，並分析出如何設計出更高隱藏率的影像隱藏演算法。

三、 結果與討論

在第一主題：邊緣吻合向量量化為基礎的資訊隱藏方法，首先將一張掩護影像切割成多個不重疊的 4×4 像素大小的區塊。該張掩護影像的第一列或第一行的區塊不用來藏任何機密資訊，故這些區塊經由向量量化壓縮後再即刻解壓縮，而這些解壓縮的區

塊資訊便成為偽裝影像相對位置的區塊內容。剩下的每個區塊（即不是掩護影像的第一列或第一行的區塊），則利用其相鄰區塊的解碼資訊來產生一本子編碼簿，再從此編碼簿找出一個離此區塊距離最近的 16 維碼向量 X ，與離 X 最近的 16 維碼向量 Y ，然後根據 X 與 Y ，定義一個以 X 為球心，半徑為 $\lceil \|X - Y\|/2 \rceil - 1$ 的球體。為了可以將機密資料藏到 16 維碼向量 X 的每一個分量中，必需先算出每一個分量的隱藏量。一般來說，若要將 v ($1 \leq v \leq 4$) 個位元的機密資訊，利用 v -LSB 替換法藏入到 16 維碼向量 $X = (x_0, x_1, \dots, x_{15})$ ，得到偽裝碼向量 $Z = (z_0, z_1, \dots, z_{15})$ ，則 z_i 與 x_i ($0 \leq i \leq 15$) 的差值最多為 $2^v - 1$ ，因此

$$\sum_{i=0}^{15} (z_i - x_i)^2 \leq 16(2^v - 1)^2。$$

另一方面，我們要求 X 與 Z 的距離不能超過球體的半徑，因此

$$\sum_{i=0}^{15} (z_i - x_i)^2 \leq (\lceil \|X - Y\|/2 \rceil - 1)^2。$$

為了算出 v ，只要要求

$$16(2^v - 1)^2 \leq (\lceil \|X - Y\|/2 \rceil - 1)^2$$

就可。因此，

$$v = \left\lfloor \log_2 [(\lceil \|X - Y\|/2 \rceil - 1)/4 + 1] \right\rfloor。$$

在算出 v 值之後，16 維碼向量 X 的某幾個分量有可能可以再多藏一個位元的機密資訊（假設有 w 個分量）。此時，為了仍然可以滿足 X 與 Z 的距離不能超過球體的半徑的條件，則

$$w[(2^{v+1} - 1)^2 - (2^v - 1)^2] \leq (\lceil \|X - Y\|/2 \rceil - 1)^2 - 16(2^v - 1)^2。$$

因此，

$$w = \left\lfloor \frac{t^2 - 16(2^v - 1)^2}{(2^{v+1} - 1)^2 - (2^v - 1)^2} \right\rfloor。$$

故 16 維碼向量 X 的每一個分量的隱藏量為

$$C(x_0) = C(x_1) = \dots = C(x_{w-1}) = v+1;$$

$$C(x_w) = C(x_{w+1}) = \dots = C(x_{16}) = v。$$

最後，分別取出機密資訊的 x_i 位元，再利用 x_i -LSB 替換法將 x_i 位元藏入到分量 x_i ，便會得到偽裝碼向量 Z 。如圖一，(a) 為 512×512 的邊緣吻合向量量化影像（未藏入任何機密資訊），(b) 為利用本主題方法所產生的 512×512 偽裝影像，(c) 為將圖(a)的鼻子與嘴巴放大的影像，(d) 為將圖(b)的鼻子與嘴巴放大的影像。本方法與邊緣吻合向量量化法比較，具有較佳的影像品質。另外，

表一比較本方法與隱藏方法[1]的隱藏量與偽裝影像品質。由表一得知，本方法的隱藏量與偽裝影像品質皆優於[1]。

在第二個主題：基於機密影像中相鄰像素間相似性的高容量資訊隱藏方法，首先將機密影像利用向量量化技術壓縮，再利用 Thien and Lin's 的方法[2]，將壓縮檔藏入到掩護影像的像素值。如圖二，(a)-(b)分別為本實驗用的 512×512 機密影像與 512×512 掩護影像，(c)為利用本方法將(a)藏入(b)所產生的 512×512 偽裝影像，(d)為從(c)擷取出的 512×512 機密影像。另外，表二比較本方法與其它隱藏方法[3,4]的影像品質。由表二得知，採用本方法所得的偽裝影像品質遠遠優於[3,4]，而且，經由偽裝影像擷取之機密影像的品質與[3,4]的差距不大。

在第三主題：資訊隱藏量之上限研究，我們利用多維球體的公式來計算出 PSNR 上限值。首先，對於一張 $w \times h$ 的影像 H ，其 PSNR 公式為

$$PSNR = 10 \log \frac{255^2}{MSE}, \text{ 其中}$$

$$MSE = \frac{1}{wh} \sum_{i=0}^{w-1} \sum_{j=0}^{h-1} (H(i, j) - H'(i, j))^2。$$

由公式可知，將 PSNR 最大化即是將 MSE 最小化，而 MSE 代表的是多維空間下的歐氏距離。假設

1. 掩護影像 H 是均勻分布。
2. 機密資料是均勻分布。
3. 掩護影像與機密資料是互相獨立。

由以上三個假設，我們可以畫出如圖三的模式。其中圓心代表在多維空間中一個表示影像 H 的點，而 x 點代表影像 H 藏入一種機密資料後可能的位置 (即為偽裝影像)。因為一個 x 點代表一種機密資料，所以 x 點的數量代表隱藏量， x 點越多，代表隱藏量越大。假設我們要隱藏 s 位元至影像 H 之中，則 x 點的個數為 2^s 。另一方面，為了最小化 MSE，這些 x 點將會以影像 H 為圓心分布在一個半徑為 R 的多維球體內，而球體積為 2^s 。代入多維球體的公式後，我們可計算出

$$R = \left[\frac{(wh/2)! 2^s}{\pi^{wh/2}} \right]^{1/wh}。$$

將 R 代回 MSE 公式後，可得

$$MSE_{worst} = \left(\frac{wh}{2\pi} \right)^{-0.5} \left[(wh/2)! 2^s \right]^{1/wh}。$$

此為 MSE 最佳解的下界。另一方面，我們可以用積分法求 MSE 的平均解為

$$MSE_{avg} = ((wh + 2)\pi)^{-0.5} [(wh/2)2^s]^{1/wh}$$

。平均解代表當我們實驗次數夠多，我們可以獲得的平均值（在此為最佳解的平均值）。

在第四主題：基於多維像素空間而得的影像隱藏方法，我們先將掩護影像 H 切成每個大小為 n 像素 (p_0, p_1, \dots, p_{n-1}) 的區塊，且每個區塊藏入一 m 位元的機密資料 B_m 。我們使用的公式為

$$f(p'_0, p'_1, \dots, p'_{n-1}) = 1p'_0 + c_1p'_1 + \dots + c_{n-1}p'_{n-1} = B_m \pmod{2^m}$$

其中 ($1, 2, \dots, c_{n-1}$) 是 n 個給予的正整數， $p'_i = p_i + \Delta p_i$ 代表隱藏資料後獲得的掩護像素，而 Δp_i 代表其差值。將上式轉換後，我們可以獲得以下結果

$$1\Delta p_0 + c_1\Delta p_1 + \dots + c_{n-1}\Delta p_{n-1} = B_m - (1p_0 + c_1p_1 + \dots + c_{n-1}p_{n-1}) \pmod{2^m}$$

其中公式的右半邊是可以計算出來的，令其結果等於 R_m ，而公式的左半邊是必須解決的問題。對於不同的 R_m 值，我們可以利用動態規劃演算法去求解 ($\Delta p_0, \Delta p_1, \dots, \Delta p_{n-1}$)，並將其記錄於表格中以利隱藏時的速度。當資料全部隱藏完後，解碼端只需要計算

$f(p'_0, p'_1, \dots, p'_{n-1})$ 便可解出機密資料 B_m 。然而，如何獲得好的 ($1, 2, \dots, c_{n-1}$) 是另一個問題，我們提供了表三，使用者可以依照不同的隱藏率選擇不同的 ($1, 2, \dots, c_{n-1}$)。表三亦提供預測的 PSNR，也就是說，使用者可以在不進行隱藏過程之前便可以預知做完後大致上的 PSNR 數值。表四則列出本方法與其他隱藏方法 [2,5-12] 的偽裝影像品質比較。由表四可看出，在不同的隱藏率下，本方法可獲得較佳的 PSNR 值。

四、計畫成果與自評

第二年的第一、二、三、四主題，我們均成功的達成預期目標與成果。第一主題已被 Optical Engineering 期刊 (SCI) 接受；第二主題已被 IJPRAI 期刊 (SCI) 接受；第三、第四主題也合併投稿至 Information Science (SCI) 期刊，目前在 revise。本計劃第二年之申請經費為 327,750 元 (核定為 442,000 元，因加列主持人費用)。第二年之成果大概會發表 3 篇國際期刊論文。這樣的經費成果比，應該還算可以。

五、 參考文獻

- [1] C. C. Chang, W. L. Tai, and C. C. Lin, A reversible data hiding scheme based on side match vector quantization, *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 16, No. 10, 1301-1308, 2006.
- [2] C. C. Thien and 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, No. 12, pp. 2875-2881, 2003.
- [3] K. L. Chung, C. H. Shen, and L. C. Chang, A novel SVD- and VQ-based image hiding scheme, *Pattern Recognition Letters*, Vol. 22, No. 9, pp. 1051-1058, 2001.
- [4] Y. C. Hu and M. H. Lin, Secure image hiding scheme based upon vector quantization, *International Journal of Pattern Recognition and Artificial Intelligence*, Vol. 18, No. 6, pp. 1111-1130, 2004.
- [5] I. C. Lin, Y. B. Lin, C. M. Wang, Hiding data in spatial domain images with distortion tolerance, *Computer Standards & Interfaces*, Vol. 31, No. 2, pp. 458-64, 2009
- [6] J. Mielikainen, LSB Matching Revisited, *IEEE Signal Processing Letters*, Vol. 13, No. 5, pp. 285-287, 2006.
- [7] X. Li, B. Yang, D. Cheng, T. Zeng, A generalization of LSB matching, *IEEE Signal Processing Letters*, Vol. 16, No. 2, pp. 69-72, 2009.
- [8] X. Zhang, S. Wang, Efficient Steganographic Embedding by Exploiting Modification Direction, *IEEE Communications Letters*, Vol. 10, No. 11, pp. 781-783, 2006.
- [9] D. C. Wu and W. H. Tsai, A steganographic method for images by pixel-value differencing, *Pattern Recognition Letter*, Vol. 24, No. 9-10, pp. 1613-1626, 2003.
- [10] C. M. Wang, N. I. Wu, C. S. Tsai, M.S. Hwang, A high quality steganographic method with pixel-value differencing and

modulus function, *Journal of Systems and Software*, Vol. 81 No. 1, pp. 150-158, 2008.

[11] C. H. Yang, C. Y. Weng, S. J. Wang, H. M. Sun, Adaptive data hiding in edge areas of images with spatial LSB domain systems, *IEEE Transactions on Information*

Forensics and Security, Vol. 3, No. 3, pp. 488-497, 2008.

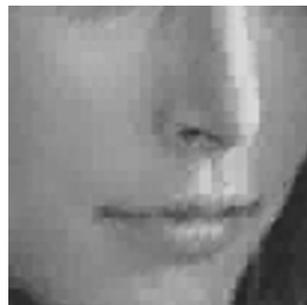
[12] H. Yang, X. Sun, G. Sun, High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution, *Radio-engineering*, Vol. 18, No. 4, pp. 509-516, 2009.



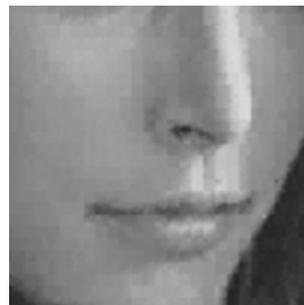
(a)



(b)



(c)



(d)

圖一. 第一主題(以邊緣吻合向量量化為基礎的資訊隱藏方法)的實驗結果。(a)為 512×512 的邊緣吻合向量量化影像(未藏入任何資訊); (b)為利用本主題方法產生的 512×512 偽裝影像; (c)為將圖(a)的鼻子與嘴巴放大的影像; (d)為將圖(b)的鼻子與嘴巴放大的影像

表一. 第一主題與前人的隱藏方法[1]之隱藏量與偽裝影像品質比較。

掩護影像	Chang et al. [1]		Ours	
	隱藏量 (bits)	偽裝影像品質 (dB)	隱藏量 (bits)	偽裝影像品質 (dB)
Lena	16,129	32.45	413,667	33.86
Jet	16,129	31.09	433,881	32.53
Boat	16,129	29.93	467,367	31.39
Peppers	16,129	29.19	413,322	33.94
Baboon	16,129	23.66	675,226	26.52



(a)



(b)



(c)

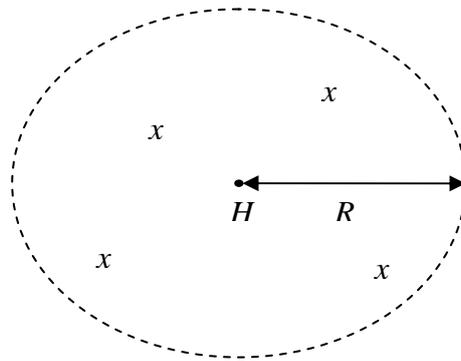


(d)

圖二. 第二主題(基於機密影像中相鄰像素間相似性的高容量資訊隱藏方法)的實驗結果。(a)為輸入的 512×512 機密影像; (b)為輸入的 512×512 掩護影像; (c)為將(a)藏入(b)所得的 512×512 偽裝影像; (d)為從(c)擷取出的 512×512 機密影像。

表二. 第二主題與其它隱藏方法[3-4]的擷取機密影像與偽裝影像品質之比較。

掩護影像	方法	機密影像	偽裝影像品質 (dB)	由偽裝影像擷取之機密影像的品質 (dB)
512×512 Lena	Chung et al. [3]	512×512 Jet	32.50	30.01
	Hu and Lin [4]	512×512 Tiffany	44.42	32.02
	Ours	512×512 Tiffany	51.68	32.02
		512×512 Jet	51.69	31.43



圖例三. 第三主題(資訊隱藏量之上限研究)的概念圖。其中圓心代表影像 H , x 代表 H 隱藏資料後可能的位置, 而這些位置 x 距離 H 不會超過 R 。

表三. 第四主題對於不同的隱藏率所建議的 $(1, c_1, \dots, c_{n-1})$ 。

隱藏率(bpp)	m, n	PSNR 預測值(dB)	$1, c_1, \dots, c_{n-1}$
0.500	4, 8	57.44	1, 2, 3, 4, 5, 6, 7, 8
0.571	4, 7	56.58	1, 2, 3, 4, 5, 6, 7
0.667	4, 6	55.40	1, 2, 3, 4, 5, 6
0.750	6, 8	54.81	1, 2, 3, 4, 5, 6, 13, 26
0.875	7, 8	54.25	1, 2, 8, 12, 24, 29, 47, 62
1.000	6, 6	53.33	1, 2, 5, 12, 20, 28
1.167	7, 6	52.26	1, 3, 8, 18, 42, 54
1.200	6, 5	52.04	1, 6, 10, 18, 31

1.250	5, 4	51.64	1, 2, 6, 11
1.333	8, 6	51.40	1, 3, 9, 27, 50, 93
1.400	7, 5	50.97	1, 3, 9, 28, 52
1.500	6, 4	50.34	1, 3, 8, 22
1.600	8, 5	49.75	1, 3, 58, 87, 124
1.667	5, 3	49.09	1, 4, 10
1.750	7, 4	48.65	1, 4, 40, 58
1.800	9, 5	48.46	1, 36, 86, 146, 215
2.000	10, 5	47.31	1, 9, 23, 243, 324
2.250	9, 4	45.73	1, 13, 149, 232
2.500	10, 4	44.23	1, 26, 33, 221
2.750	11, 4	42.72	1, 364, 559, 986
3.000	12, 4	41.22	1, 9, 350, 491
3.333	10, 3	39.10	1, 20, 195
3.500	7, 2	38.00	1, 12
3.667	11, 3	37.10	1, 61, 597
4.000	12, 3	35.10	1, 1210, 2026

表四. 比較第四主題與其它隱藏方法[2,5-12]的偽裝影像品質。其中掩護影像是512×512 大小的 Lena，且隱藏資料是亂數資料。

隱藏率(bpp)	方法	PSNR (dB)
0.50	[2,5]	54.14
0.50	ours	57.44
0.75	[2,5]	52.38
0.75	ours	54.82
1.00	[21]	51.14
1.00	[2,5]	51.14
1.00	[6] <small>(n=2)</small>	52.39
1.00	[7] <small>(n=6)</small>	53.33
1.00	ours <small>(m=n=6)</small>	53.33
1.16	[8]	52.11
1.17	ours	52.26
1.50	[5]	48.12
1.50	[2] <small>(mod 3)</small>	49.89
1.50	ours	50.34
1.56	[9]	41.79

1.56	[10]	44.10
1.99	[12]	45.14
2.00	[2,5]	46.37
2.00	ours	47.30
2.19	[11]	43.95
2.25	ours	45.73
2.39	[11]	36.96
2.50	[5]	42.69
2.50	$[2]_{(\text{mod } 6)}$	43.12
2.50	ours	44.23
2.89	[12]	39.31
3.00	[2,5]	40.73
3.00	ours	41.22
3.19	[11]	36.28
3.33	ours	39.11
3.50	[5]	36.82
3.50	$[2]_{(\text{mod } 12)}$	37.29
3.50	ours	38.00
3.53	[12]	34.54
3.67	ours	37.10
4.00	[2,5]	34.80
4.00	ours	35.10