

使用最低位元替換法及特定量化區間的像素差值藏入法

冷輝世* 黃瑄惠
國立彰化師範大學數學系

lenghs@cc.ncue.edu.tw* s0522132@mail.ncue.edu.tw

摘要

Khodaei與Faez學者於2011年結合最低位元替換法與像素差值藏匿法以達成高藏入量與高偽裝影像品質的資訊隱藏技術。此法對量化區間做了不同的分類以決定藏入量的多寡。Leng學者於2017年針對像素差值藏匿法提出量化區間的最佳化策略。本研究將前者所使用的像素差值藏匿法中的量化區間改用後者的最佳化策略並選定一特定的量化區間以提高藏入量並保持良好的偽裝影像品質。

關鍵詞：資訊隱藏、最低位元替換法、像素差值藏匿法、量化區間、最佳化策略。

前言

Wu與Tsai學者(2003)提出像素差值藏匿法(Pixel-Value Differencing，以下簡稱PVD法)。PVD法中量化區間的定義是基於人類視覺敏感度的特徵，並由兩兩像素差值所屬的量化區間區決定可藏的機密訊息長度[2]

Leng學者 (2017)提出像素差值藏匿法的新策略，企圖找出最佳化的量化區間[4]。

Khodaei與Faez學者(2011)提出結合最低位元替換法與像素差值藏匿法[11]。此法對量化區間做了不同的分類以決定藏入藏入量的多寡。本研究延用[11]的方法，但是使用[4]選定特定的量化區間以達到高藏入量與良好的偽裝影像品質。

文獻探討

2.1 Khodaei與Faez的方法

2011年，Khodaei與Faze提出的方法是將三個連續像素分為一組，先對中央像素以LSB法(含OPAP法)藏入機密訊息再利用已藏入機密訊息的中央像素與其兩側的相鄰像素計算差值並以單向的PVD法(中央像素藏入機密訊息後不可移動)藏入機密訊息。

例如：像素組(g_1, g_2, g_3) = (140, 121, 196)，假設機密訊息為'110 1100 011001'。首先，先對中央像素121=(1111**1001**)₂使用LSB法藏入3個位元的機密訊息'110'，得到126=(1111**110**)₂，接下來使用OPAP法最佳化得到中央像素最後的偽裝像素值 $g_2' = 118$ =(1110**110**)₂。然後以此對兩側的像素計算差值 $d_1 = |118 - 140| = 22$ ， $d_2 = |118 - 196| = 78$ 。 $d_1 \in R_3 = [16, 31]$ 可藏入4位元的機密訊息'1100'， $d_2 \in R_5 = [64, 255]$ 可藏入6位元的機密訊息'011001'，所以 $d_1' = 16 + 12 = 28$ ， $d_2' = 64 + 25 = 89$ 。由於 g_2' 是不可移動的，我們取 $g_1' = g_2' - d_1'$ 或 $g_2' + d_1'$ ，利用公式(1)取其中失真較小者。同理，我們取 $g_3' = g_2' - d_2'$ 或 $g_2' + d_2'$ ，一樣利用公式(1)取其中失真較小者。最後可以求得最後的偽裝像素組(g_1', g_2', g_3') = (146, 118, 207)(如圖1)。

$$g_1' = \begin{cases} g_2' - d_1', & \text{if } |g_2' - d_1' - g_1| \leq |g_2' + d_1' - g_1| \\ g_2' + d_1' & \text{otherwise} \end{cases}$$
$$g_3' = \begin{cases} g_2' - d_2', & \text{if } |g_2' - d_2' - g_3| \leq |g_2' + d_2' - g_3| \\ g_2' + d_2' & \text{otherwise} \end{cases}$$

公式(1)

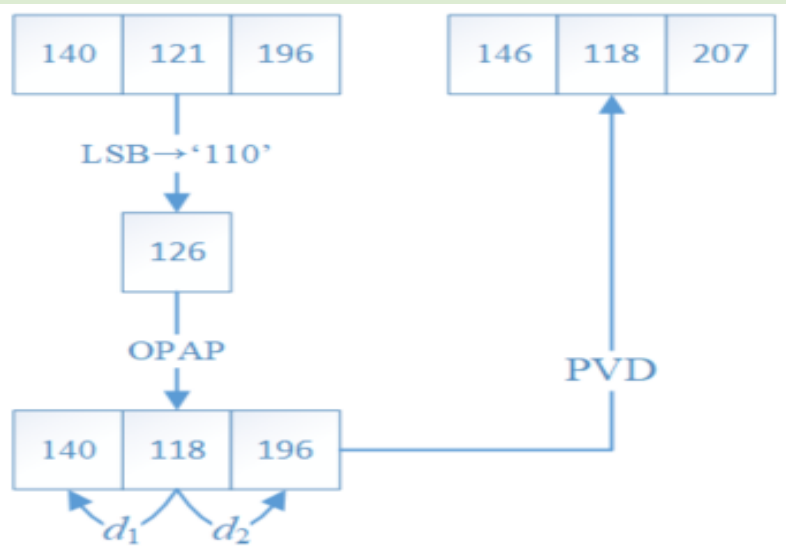


圖 1 Khodaei與Faze嵌入範例

2.2 Leng學者的像素差值藏匿法的新策略

2017年，Leng學者提出像素差值藏匿法的新策略。在其所設計的量化區間中，使用反向編碼的方式提高藏入量。以 $R_1 = [0, 14]$ 為例：

	R ₁ ⁻						
x	0	1	2	3	4	5	6
b ₃ b ₆ b ₇ b ₈	0000	0001	0010	0011	0100	0101	0110
s ₄ s ₃ s ₂ s ₁	0000	0001	0010	0011	0100	0101	0110
	R ₁ ⁺						
x	7						
b ₃ b ₆ b ₇ b ₈	0111						
s ₄ s ₃ s ₂ s ₁	111						
	R ₁ ⁺						
x	8	9	10	11	12	13	14
b ₃ b ₆ b ₇ b ₈	1000	1001	1010	1011	1100	1101	1110
s ₄ s ₃ s ₂ s ₁	1000	1001	1010	1011	1100	1101	1110

表 1 量化區間R₁ = [0,14]範例

在表1中 R_1 可分割成三部份， $R_1^- = [0, 6]$ 、 $R_1^* = [7]$ 和 $R_1^+ = [8, 14]$ 。其中 R_1^- 和 R_1^+ 的每一個(差)值相差為8，剛好是 b_8 的位置($b_3b_6b_7b_8$ 分別代表相對應 x 值的末四碼LSB)。若機密訊息為 $s_1s_2s_3s_4\dots$ ，則必須反序取出並找出所對應的 $b_3b_6b_7b_8$ 即為藏入後的偽裝(差)值。否則必存在 R_1^* 中的值其末三碼的LSB與反序的3位機密訊息相同。

研究方法

本研究利用Khodaei與Faez的方法，將原始影像分割成連續三個像素一組，先利用LSB法及OPAP法對中央像素嵌入3位元的機密訊息，再分別計算藏入機密訊息後的中央像素與兩側相鄰像素的差值。量化區間則採用Leng學者提出的像素差值藏匿法的新策略中長度全部都為15的設計。即 $R_i = [15 * (i - 1), 15 * i - 1]$ ，其中 $i = 1, 2, \dots, 17$ 。則每個 R_i 量化區間皆可藏入3或4位的機密訊息。而且若像素差值為255，則不做藏入動作。 R_i 如表1，另外舉例 R_2 如表3，其餘 $R_3 \sim R_{17}$ 依此類推。嵌入機密訊息後的新差值採用上述2.1節的單向PVD法利用公式(1)即可求得偽裝像素組的值。若單向PVD法造成溢位問題(像素值小於0或大於255)，則可以考慮使用[2]提供的檢測方法不做藏入動作或是將溢位像素組整組平移即可。

	R ₂ ⁻						
x	15	16	17	18	19	20	21
b ₃ b ₆ b ₇ b ₈	1111	0000	0001	0010	0011	0100	0101
s ₄ s ₃ s ₂ s ₁	1111	0000	0001	0010	0011	0100	0101
	R ₂ ⁺						
x	22						
b ₃ b ₆ b ₇ b ₈	0110						
s ₄ s ₃ s ₂ s ₁	110						
	R ₂ ⁺						
x	23	24	25	26	27	28	29
b ₃ b ₆ b ₇ b ₈	0111	1000	1001	1010	1011	1100	1101
s ₄ s ₃ s ₂ s ₁	0111	1000	1001	1010	1011	1100	1101

表 2 本研究採用的量化區間

i	R _i	Width	Payload
1	[0,14]	15	3 or 4
2	[15,29]	15	3 or 4
3	[30,44]	15	3 or 4
4	[45,59]	15	3 or 4
5	[60,74]	15	3 or 4
6	[75,89]	15	3 or 4
7	[90,104]	15	3 or 4
8	[105,119]	15	3 or 4
9	[120,134]	15	3 or 4
10	[135,149]	15	3 or 4
11	[150,164]	15	3 or 4
12	[165,179]	15	3 or 4
13	[180,194]	15	3 or 4
14	[195,209]	15	3 or 4
15	[210,224]	15	3 or 4
16	[225,239]	15	3 or 4
17	[240,254]	15	3 or 4

表 3 量化區間R₂ = [15,29]範例

實驗結果

實驗結果的偽裝影像的品質評估採用常見的峰值信噪比(Peak Signal-to-Noise Ratio，以下簡稱PSNR)，其中PNSR定義如下：

$$PSNR = 10 \times \log_{10} \left(\frac{255^2}{\frac{1}{mn} \sum_{i=1}^m \sum_{j=1}^n (x'_{ij} - x_{ij})^2} \right)$$

公式(2)

其中 m 、 n 為原始影像的長跟寬， x'_{ij} 、 x_{ij} 分別代表位於 i 、 j 位置的偽裝像素與原始像素的值。實驗測試圖形採用SIPI影像資料庫中六張大小為512*512的標準測試圖形‘Tiffany’、‘Baboon’、‘Lena’、‘Jet’、‘Scene’與‘Peppers’(如圖2)並取隨機亂數做為機密訊息。實驗結果與[11]比較如下，其中藏入量以位元(bit)為單位，影像品質以PSNR(dB)值為單位：

	本研究		[11]	
	dB	bit(s)	dB	bit(s)
Tiffany	33.8995	928759	38.3300	790253
Baboon	34.0719	928525	36.7200	810126
Lena	33.9240	928816	38.1800	791253
Jet	33.7258	928629	38.0500	792617
Scene	34.0568	928543	38.1000	795456
Peppers	34.0643	928145	38.3500	789989
平均	33.9571	929837	37.9550	794949

表 4 實驗結果與[11]的比較

由表4，本研究的平均藏入量約為929837個位元，相較於[11]的平均藏入量794949個位元多出了134888個位元 bits(提昇17%)。其主因應該是在差值較小的區間中本研究幾乎都藏入4個位元的機密 訊息而[11]只藏入3個位元的機密訊息。且本研究的量化區間設計對於特徵不同的六張測試影像藏入量皆相似。換句話說，本研究方法不受影像特徵的影響。

本研究與[11]的偽裝影像的品質比較(如圖2)：

標準測試圖						
	(a)Tiffany	(b)Baboon	(c)Lena	(d)Jet	(e)Scene	(f)Peppers
本研究						
	(a)Tiffany	(b)Baboon	(c)Lena	(d)Jet	(e)Scene	(f)Peppers
[11]						
	(a)Tiffany	(b)Baboon	(c)Lena	(d)Jet	(e)Scene	(f)Peppers

圖 2 測試圖形及偽裝影像的比較

由圖2，兩者偽裝影像並無顯著差異。由於本研究使用特定量化區間且長度相等(15)，每組差值皆有14/15的機率可以藏入4個位元的機密訊息，另外1/15的機率則藏入3個位元的機密訊息。相較於[11]的量化區間，可藏入的機密訊息長度則是分佈在3~6之間。因此，在理論上，本研究在差值大的像素組中會有較小的失真，但是由於自然影像中相鄰像素差值的分佈集中於較小的一端，所以本研究方法的偽裝影像品質略遜於[11]。

結論

本研究將Khodaei與Faez的方法中使用像素差值藏匿法中的部份改用Leng學者提出的像素差值藏匿法的新策略中的最佳化量化區間設計(且區間長度皆為15)與反向編碼藏入機密訊息以提昇藏入量。實驗結果顯示，本研究的平均藏入量提昇了17%，並保持良好的偽裝影像品質(平均33.9571dB)。