有效應用區間間隔之可逆式資訊隱藏技術

呂慈純
朝陽科技大學資訊管理系
e-mail：tlc@cyut.edu.tw

陳培倫
朝陽科技大學資訊管理系
e-mail：s9614601@cyut.edu.tw

摘要

可逆式資訊隱藏技術不但可以藏入訊息，而且可以還原原始影像，本項技術可應用於醫學影像、軍事方面，由於這兩個領域要求媒體不能有絲毫的誤差，所以它的實用性及重要性使其成為研究的一個重要議題。本篇論文提出一個有效應用區間間隔的可逆式資訊隱藏技術，利用像素值所設定的區間間隔將機密資訊藏入。接收方能夠有效的將藏入的資訊取回，並且能夠還原原始影像。

關鍵詞：可逆式資訊隱藏、區間量表、隱藏學、最低有效位元。

Abstract

Reversible information hiding techniques not only can embed secret message into a host image, but also can completely remove the concealed message and recover the original media. This technique can be used in medical and military areas. Because these two areas not allow any error and the reversible information hiding technique is suitable for the request. Its practicability and significant make the reversible information hiding technique to become an important research issue.

This paper proposes an efficiency reversible hiding scheme based on interval expansion. The proposed scheme expands the interval between pixels to embed information in an image. The receiver can extract the concealed message and restore the original image from the stego-image.

Keywords: Reversible information hiding, interval, steganography, least significant bit.

1. 前言

隨著數位資訊時代的來臨與資訊技術的進步，網際網路已經成為生活上不可或缺的工具。透過網路的傳送，雖然為生活上帶來了許多的便利性，但是其中潛在的安全性問題，卻成為一項不能忽略的重要議題。

常使用於保護資料安全的機制是資訊隱藏技術，其將重要的機密資訊(Secret Data)嵌入至數位媒體(包含圖像、聲音、文字、影像、執行檔、壓縮碼等)中。嵌入機密資訊後的數位媒體與原始資訊的差異不會太大，因此不會讓第三方察覺，進而有效保護隱藏的資訊。

依影像媒體所發展的隱藏技術可分為取代式系統(Substitution System)、頻率域(Frequency Domain)技術、展頻(Spread Spectrum)技術、統計方法、失真技術、隱蔽媒體產生技術等六大類[5]。一個好的資訊隱藏技術需滿足安全性、不可察覺性以及高負載量等需求[1]。

本篇論文所提出的資訊隱藏技術，主要是應用區間間隔藏入機密資訊，並且可還原原始影像。

2. 相關文獻探討

本節中將探討與本研究相關的研究與其相關的技術。在 2005 年 Lu 等學者提出一個量化導向式隱藏方法[1]，這個方法是將像素值域切割成好幾個區間，每一區間對應一個機密訊息，量化間距(Quantization Step Size, q)決定切割區間的大小。接著，以機密金鑰與機密訊息做 *XOR* 的動作，產生 S 序列為藏入的訊息。利用 S 序列對應像素值，使 S 序列的位元奇偶數與像素值相同，再將序列透過區間及公式，藏入到掩護影像中。

以下舉例說明，假設有一個灰階影像大小為3×3，如圖 1 所示，利用金鑰產生的序列為 (1,1,0,0,0,1,1,0,1)，假設機密資訊為 (1,1,0,1,1,0,0,1,0)，將金鑰產生的序列與機密資訊做 *XOR* 運算得到 S 序列 (0,0,0,1,1,1,1,1,1)。

5	11	20
40	27	17
37	85	15

圖 1、灰階影像，影像大小 3×3

接著以 S 序列修改像素的奇偶數，利用公式 1 對照 S 修改影像得到修改後的影像如圖 2 所示。

$$\hat{p}_i = \begin{cases} p_i + 1, \ if \ s_i \neq (p_i \bmod 2), \\ p_i, \quad otherwise。 \end{cases} \tag{1}$$

6	12	20
41	27	17
37	85	15

圖 2、修改後影像

其中 p_i 為第 i 個像素，$\hat{p}_i$ 為修改後像素。假設量化間距為 8，即 q=8，產生的區間量表如圖 3 所示。圖 3 中每個區間會對應一個機密訊息位元。最後利用公式 2 計算出偽裝像素(p')及偽裝像素如圖 4 所示。

$$p_i' = \begin{cases} \hat{p}_i + \left\lfloor \dfrac{\alpha(\hat{p}_i)\times q - \hat{p}_i}{2} \right\rfloor, if \ \beta(\hat{p}_i) = s_i, \\ \hat{p}_i + \left\lfloor \dfrac{(\alpha(\hat{p}_i)+1)\times q - \hat{p}_i}{2} \right\rfloor, otherwise。 \end{cases} \tag{2}$$

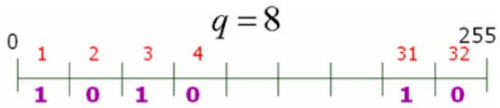


圖 3、間距為 8 的區間

11	14	28
48	33	20
38	86	19

圖 4、偽裝影像

$\beta(x)$ 函式會回傳 x 像素所屬區間其相對應的機密訊息位元。

Mielikainen 於 2006 年提出一個最低位元匹配(LSB Matching)隱藏方法[4]，其藏入方法是以兩個像素為單位，每一次藏入兩個機密訊息。藏入過程中利用一個二元函式(Binary Function)，如公式 3，判斷修改的像素值為何。藏入過程可以一個二元樹來表示，如圖 5 所示。其中 A 和 B 分別為兩個像素，m_1 為要藏入 A 的機密訊息，m_2 則為要藏入 B 的機密訊息，C 和 D 表示 A 和 B 藏入訊息後的像素。

$$F(A,B) = LSB(\left\lfloor \frac{A}{2} \right\rfloor + B)。 \tag{3}$$

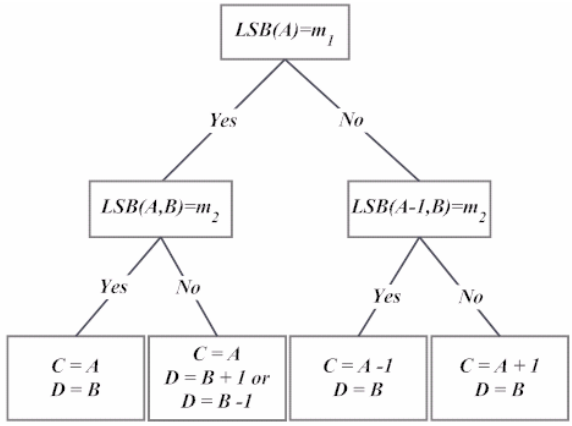


圖 5、最低位元匹配法示意圖

假設 $A=43$ 和 $B=38$，要藏入的機密資訊為 $m_1=1$ 和 $m_2=0$，則 $LSB(A)=1=m_1=1$，而且 $F(A,B)=1\neq m_2=0$，所以修改後的偽裝像素值為 $C=43$ 和 $D=37$ 或 39，由圖 5 可知當遇到機密資訊和原始像素的 LSB 不同時，只需要更改其中一個像素值，因此可以減少像素被更改的機率以達成失真較少的目的。

Celik 等學者在 2002 年提出一個廣義最低位元藏入法(Generalized Least Significant Bit, G-LSB)[3]，這個方法是先將原始圖形 S，如圖 6，經過量化得到量化圖形 $Q(S)$，如圖 7，量化的公式如公式 4 所示。

20	15	33	8
30	37	21	14
27	30	6	27
14	15	24	33

圖 6、原始影像 S

20	15	30	5
30	35	20	10
25	30	5	25
10	15	20	30

圖 7、量化後影像 $Q(S)$

$$\tilde{p} = \left\lfloor \frac{p}{q} \right\rfloor \times q \ , \tag{4}$$

其中 p 為原始像素值，q 為量化值，接著再將機密資訊藏入 $Q(S)$ 中，藏入公式如公式 5，

$$S' = Q(S) + W' \text{。} \quad (5)$$

機密訊息 W 表示為小數位數，再轉換成十進制，即可得到 W'。假設機密資訊為 $W = 1001$，W 以小數位數表示為 0.1001，轉換成十進制則表示 $W' = (0.1001)_2 = (0.5625)_{10}$。

然後將 0 到 1 之間的數值平均分成 q 等份，以 $q = 5$ 來舉例，我們將 0 到 1 之間的數值分成 5 等份，得到一個比例區間圖，如圖 8 所示，第一個區間稱為 R_0，由下往上遞增。

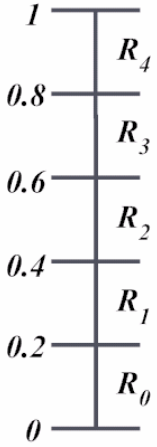


圖 8、比例區間圖

接著，我們將 W' 映射到比例區間圖中，看 W' 位於哪一個區間。在上述的例子中，$W' = 0.5625$ 位於 R_2 區間中，而 R_2 區間的上限為 0.6，下限為 0.4。將量化後的像素值加上區間號碼即可得到偽裝像素值。上述例子中圖 7，量化後的第一個像素值為 20，加上 W' 位於 R_2 區間，所以 $p' = 20 + 2 = 22$。

以 R_2 區間為中心，再分成 5 等份，如圖 9 所示。將 W' 映射到新的比例區間中，由於 W' 位於 R_4 區間中，所以第二個像素值等於 $p' = 15 + 4 = 19$。依此類推，由於 W 只有四個位元，所以當嵌入至第四個位元後，即可將 W 的資訊都藏入掩護影像中，圖 10 為藏入機密資訊後的偽裝影像。

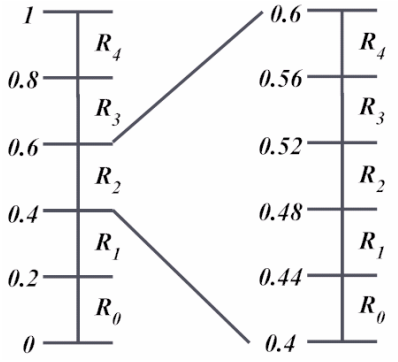


圖 9、R_2 區間圖再分割

22	19	30	6
30	35	20	10
25	30	5	25
10	15	20	30

圖 10、偽裝影像 S'

在機密資訊取出的過程中，接收方收到偽裝影像 S'，如圖 10 所示，先執行量化的動作，得到 $Q(S')$，如圖 11 所示，之後將 S' 減掉 $Q(S')$ 就可以取得藏入的機密資訊，如圖 12 所示。

20	15	30	5
30	35	20	10
25	30	5	25
10	15	20	30

圖 11、量化後偽裝影像 $Q(S')$

2	4	0	1
0	0	0	0
0	0	0	0
0	0	0	0

圖 12、S' 與 $Q(S')$ 的差異值

雖然 G-LSB 資訊隱藏方法能夠有效的將機密資訊藏入到掩護影像中，但是會造成較大的失真，而且是不可逆的資訊隱藏技術。為了改善這些缺點，Celik 等學者在 2005 年提出無失真廣義最低位元藏入法(Lossless G-LSB)的方法[2]，將因為量化所造成的失真資訊保留起來，以還原原始影像。

為了保留因為量化而形成的失真，所以在資訊藏入前先計算出原始影像 S 與量化後影像 $Q(S)$ 之間的差異，如公式 6，

$$R = S - Q(S) \text{。} \quad (6)$$

得到的差異值，我們稱為 R 表，如圖 13。將 R 表利用算術編碼壓縮法進行壓縮得到

$Comp(R)$，壓縮的結果會和機密訊息W一起藏入原始影像S之中，以達到無失真還原影像的目的。

0	0	3	3
0	2	1	4
2	0	1	2
4	0	4	3

圖 13、差異值(R 表)

接下來說明如何利用算術編碼壓縮法將R表壓縮成$Comp(R)$。算術編碼是一種無失真的壓縮方法，其輸出結果為 0 和 1 的實數，解碼端可利用此實數解碼回原來的訊息。壓縮前先求出R表中每個數字出現的機率，再利用機率進行編碼的動作，如表 1 所示。

表 1、R 表比例分析

數字	出現次數	機率
0	5	0.31
1	2	0.12
2	3	0.19
3	3	0.19
4	3	0.19

接著，以每個數字出現的機率做成比例區間圖，分成 5 等份，如圖 14 所示，以最接近 0 的第一個區間稱為R_0，由下往上遞增。

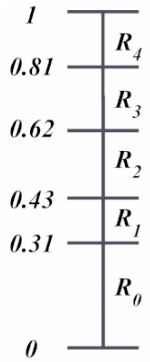


圖 14、比例區間示意圖

然後再將圖 13 以比例區間示意圖做壓縮，由於圖 13 第一個值為 0，對應至圖 14 的R_0區間，然後再將R_0分成 5 等份，上限為 0.31 下限為 0；由於第二個值也是 0，故將R_0再分成 5 等份找出R_0區間，依此類推。從最後得到的區間中任意取一實數轉成二進級，其值則為壓縮過後的$Comp(R)$值。

最後再將W與$Comp(R)$做串接的動作，並以 G-LSB 的方式藏入掩護影像中，即為 Lossless G-LSB 的藏入方式。取回過程與 G-LSB 相似，當接收方收到偽裝影像後，先進行量化得到$Q(S')$，再將S'減掉$Q(S')$則得到藏入的機密資訊。因為藏入的資訊包含了機密資訊W和$Comp(R)$，所以再利用算術編碼法將$Comp(R)$解壓縮取得R表，再把$Q(S')$加上R表即可還原原始影像S。

3. 有效應用區間間隔之可逆式資訊隱藏技術

為了能夠有效應用區間間隔，本研究提出一個能夠輕易的將機密資訊取回，也能將掩護影像(Cover-Image)還原的資訊隱藏機制。所提出的方法先建立一個以 4 為倍數的區間間隔(例如：0、4、8…等)，如表 2 所示，將掩護影像像素值除以 4 取餘數，以決定像素值需乘上幾倍去取得符合區間所代表的值，稱為擴張值。接著計算像素值與擴張值間的距離，將機密訊息以最低位元取代方式加入後形成偽裝像素值。

表 2、區間間隔表

0	4	8	12	16	20	24	…

由於偽裝像素值與掩護像素值差異不大，一般人類視覺是無法察覺出來的，所以偽裝過後的影像在網路上傳輸時，較不容易被不法的第三者所察覺，詳細的嵌入過程、取出及還原掩護影像過程詳述於 3.1 節及 3.2 節。

3.1 嵌入過程

利用區間量表及函式$f(x)$進行資訊隱藏，$f(x)$函式會回傳最靠近且不大於x的區間值，其計算式為，

$$f(x)=\left\lfloor \frac{x}{4} \right\rfloor \times 4 \text{。} \qquad (7)$$

例如$f(110)=108$，區間值108為最靠近且不大於數值110的區間值。

機密資訊的嵌入過程如下：

步驟 1：令像素為A，藏入資訊為w。

步驟 2：計算A除以4的餘數，稱為索引值I，利用索引值對應倍數Y，對應表如表 3 所示。

表 3、索引值對應倍數表

I	0	1	2	3
Y	2	4	6	2

步驟 3：計算 $\hat{A}$，計算式如下：

$$\hat{A} = Y \times A \text{。} \quad (8)$$

步驟 4：計算 $\hat{A}$ 與 $f(\hat{A})$ 的差距 d，

$$d = \hat{A} - f(\hat{A}) \text{。} \quad (9)$$

步驟 5：計算藏入後像素 A'，計算式如下：

$$A' = f(A) + d + w \text{。} \quad (10)$$

步驟 6：重覆步驟 1 到步驟 5 直到所有資訊皆藏入為止。

步驟 7：將索引值 I 轉成 2 進制，並利用算術編碼(Arithmetic Coding)進行壓縮[5]。壓縮結果為還原原始像素的重要資訊，送方可直接送給收方，或將其視為機密訊息的一部分，依據嵌入過程藏入掩蔽影像中。若欲將索引值藏入影像中，送方可先分析掩蔽影像，將像素值除以 4 取餘數，求得每個像素的索引值。再將所有的索引值以算數編碼壓縮法進行壓縮，壓縮結果再與機密資訊串接在一起，一併藏入掩蔽影像中。

以下舉一個例子說明，圖 15 為一張掩護影像大小為 3×3，藏入步驟如下。

110	100	109
145	150	98
133	99	90

圖 15、掩護影像

步驟 1：像素為 $A=110$，利用函式 $f(A)$ 計算得知 $f(A)=108$，假設欲藏入資訊為 $w=1$。

步驟 2：計算 A 除以 4 的餘數求得索引值，$I=110 \bmod 4=2$。

步驟 3：計算 $\hat{A}=6\times110=660$ 及 $f(660)=660$。

步驟 4：計算 $\hat{A}$ 與 $f(\hat{A})$ 的差距，$d=660-660=0$。

步驟 5：求得偽裝像素 $A'=108+0+1=109$，故藏入資訊後的偽裝像素值為 109。

步驟 6：重覆 1 至 5 的步驟藏入剩餘資訊，圖 16 為偽裝影像。

109	100	109
145	150	98
133	99	90

圖 16、偽裝影像

步驟 7：將索引值轉成 2 進制，利用算術編碼進行壓縮，圖 17 為索引值。

2	0	1
1	2	2
1	3	2

圖 17、索引值(Index)

3.2 取出及還原掩護影像過程

接收方收到偽裝影像後，從中取得藏入資訊，並且可將偽裝影像還原成掩護影像。取出及還原掩護影像過程如下，令偽裝像素為 A'：

步驟 1：取出藏入訊息 $w=LSB(A')$。

步驟 2：取出索引值壓縮結果，利用算數編碼解碼出索引值及找出索引值的對應倍數 Y。並對應倍數表，如表 3 求得 Y。

步驟 3：計算 A' 與 $f(A')$ 的差距，計算式如下：

$$d' = A' - f(A') \text{。} \quad (11)$$

步驟 4：計算 $\hat{A}$，計算式如下：

$$\hat{A} = f(Y \times A') + d' \text{。} \quad (12)$$

步驟 5：利用樹狀結構，如圖 18，還原原始像素。

步驟 6：重覆步驟 1 至步驟 5 取出及還原掩護影像。

我們以圖 16 為例說明如何取出及還原掩護影像，其過程如下：

步驟 1：第一個偽裝像素 $A'=109$ 其藏入資訊為 $LSB(A')=LSB(109)=1$。

步驟 2：由索引值壓縮結果可值索引值為 $I=2$，其對應倍數為 $Y=6$。

步驟 3：求得 $f(A')=f(109)=108$，並計算 A' 與 $f(A')$ 的差距 $d'=109-108=1$。

步驟 4：計算 $\hat{A}=f(6\times109)+1=653$。

步驟 5：由於 $Y=6$，根據圖 18 可知 A 的還

原公式為 $A=\left\lfloor \frac{\hat{A}}{6} \right\rfloor +2$，因此 $A=\left\lfloor \frac{653}{6} \right\rfloor +2=110$。

步驟 6： 重覆步驟 1 至步驟 5 取出及還原掩護影像。

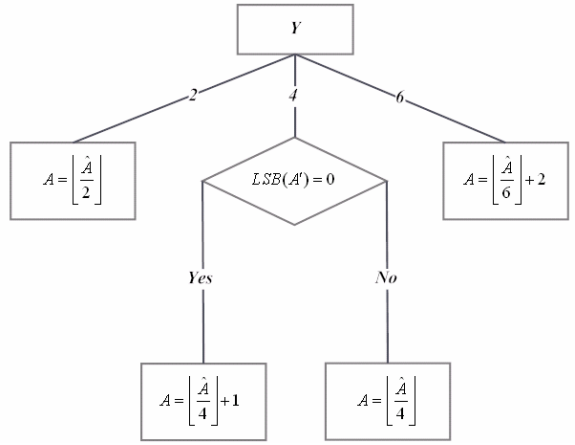


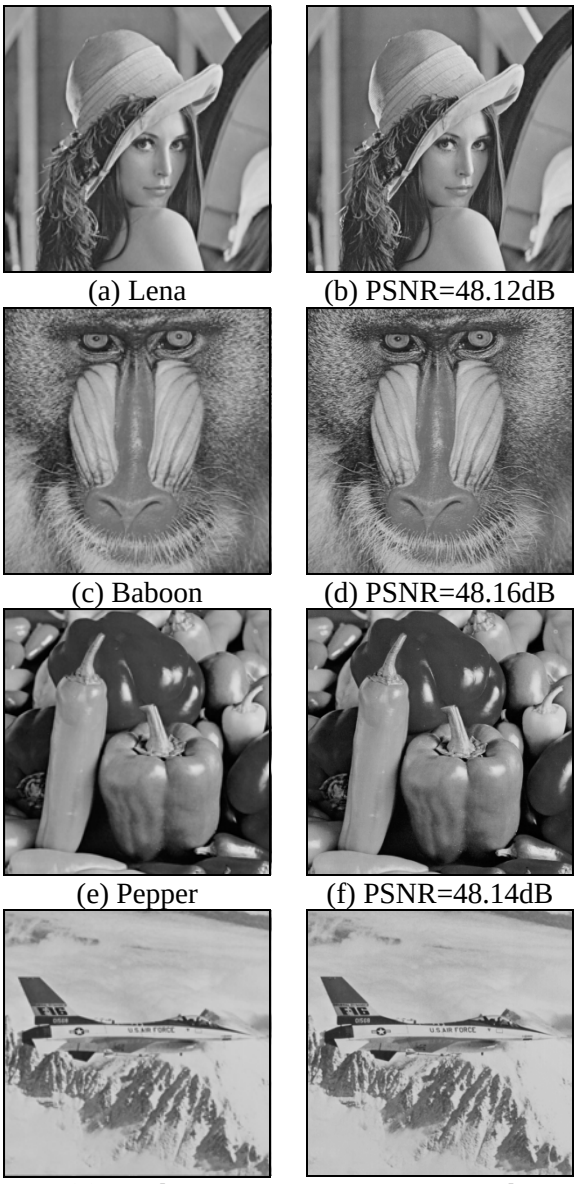
圖 18、取出及還原掩護影像示意圖

4. 實驗結果

本篇論文以 Lena、Baboon、Pepper 和 Airplane 四張 512×512 大小的影像做實驗，以亂數產生器產生機密訊息，而後利用提出方法將機密訊息藏入，並將索引值經由算術編碼壓縮與機密資訊一併嵌入影像中。我們採用影像信號雜訊比(Peak Signal to Noise Ratios, PSNR)、機密訊息藏入量及平均藏入位元數做為衡量所提方法之評量依據，實驗結果如表 4 所示。實驗之原始影像與嵌入機密資訊後影像顯示於圖 19。

表 4、實驗結果

衡量 / 影像	藏入量 (bits)	平均藏入位元 (bpp)	PSNR (dB)
Lena	213,432	0.814	48.12
Baboon	213,240	0.813	48.16
Pepper	213,408	0.814	48.14
Airplane	213,248	0.813	48.12



(a) Lena (b) PSNR=48.12dB
(c) Baboon (d) PSNR=48.16dB
(e) Pepper (f) PSNR=48.14dB
(g) Airplane PSNR=48.12dB

圖 19、原始影像與嵌入後的影像

由圖 19 可看出，偽裝影像與原始影像的差異不大，較不容易被第三方發覺出異常。接收方可從偽裝影像中取出像素的最低有效位元，即可將隱藏的資訊取出，而後利用算術編碼將壓縮的索引值取回，得以還原掩護影像。

5. 結論

本篇論文所提方法能讓傳送方輕易的將機密資訊藏入，並且將索引值經過壓縮與要藏入的資訊一起嵌入，偽裝影像的影像品質較高，不容易讓第三方輕易發現有所異常。接收方能夠取得藏入的資訊，並且能夠還原掩護影像。未來，我們將試圖增加藏入量，並且透過加密方式以增加強韌性。

參考文獻

[1] 呂慈純、陸哲明、張真誠，***多媒體安全技術***，全華圖書股份有限公司，2007。

[2] Celik, M. U., Sharma, G., Tekalp, A. M., and Saber, E., "Lossless Generalized-LSB Data Embedding," ***IEEE Transactions on Image Processing***, Vol. 14, No. 2, pp. 253-266, 2005.

[3] Celik, M. U., Sharma, G., Tekalp, A. M., and Saber, E., "Reversible Data Hiding," ***Proceedings of IEEE International Conference on Image Processing***, Vol. 2, pp. 157-160, 2002.

[4] Mielikainen, J., "LSB Matching Revisited," ***IEEE Signal Processing Letters***, Vol. 13, No. 5, pp. 285-287, 2006.

[5] Witten, I. H., Radford, M., and Cleary, J.G., "Arithmetic Coding for Data Compression," ***Communications on ACM***, Vol. 30, No. 6, pp. 520-540, 1987.

[6] Katzenbeisser, S. and Petitcolas, F. A. P., ***Information Hiding Techniques for Image Steganography and Digital Watermarking***, Boston, London, Artech House, 2000.