使用雙偽裝影像之可逆式資訊隱藏與機密分享技術
A Novel Reversible Data Hiding and Secret Sharing Scheme Using Two Steganographic Images

許俊萍* 邱川峰 詹森仁 陳以裕 劉正意
明新科技大學資訊管理系
*steenhsu @must.edu.tw

摘要

本論文將提出一個同時具有可逆式資訊隱藏與機密分享功能的雙偽裝可逆式資訊隱藏技術，讓使用者可以依照所要藏匿的資料量來決定使用的像素值修改量組合，以最適切的資料可藏量與最小的影像失真量來藏匿資料。由於雙偽裝可逆式資訊隱藏技術的可藏量可在藏匿資料前計算得知，我們將可先決定嵌入時所需使用的組合個數(也就是使用的進位數值)，x。為了能達到可逆式資料隱藏的目的，兩偽裝影像的像素值修改量之和必須介於 0 到 1 之間，我們將以變化量最少的前 x 種組合來藏匿一個 x 進位位數。藉由所推導出的公式計算出嵌入 x 進位位數時像素值的修改量，進而產生兩張偽裝影像。在擷取訊息與還原掩護影像時，必須同時取得兩張偽裝影像來達到機密分享的功能。掩護影像的還原可藉由計算兩張偽裝影像相對應像素之和的平均來還原，並藉由將兩偽裝影像與掩護影像之像素差值代入所推導出的公式中來計算出所藏匿的機密位數。進一步，我們對所提出的方法進行效能分析，計算在不同進位值時的資訊隱藏量與影像視覺品質。在使用 2 進位時，資訊隱藏量為每個掩護影像像素可用來藏匿 1 個位元(1 bbp)，同時其視覺品質的期望值可達 54.151dB。當使用 16 進位時，資訊隱藏量則可達 4 bpp，且仍能維持 40.727 dB 的高視覺品質。同時，也將與先前文獻中的雙偽裝影像可逆式隱藏技術進行分析比較，來驗證本論文所提出的方法能有較佳的效能表現。

關鍵詞：藏密學、機密分享、可逆式資料隱藏、雙偽裝影像。

1. 前言

近年來網際網路的興起，網路成為人們傳遞訊息的工具之一。然而，在訊息傳遞的過程中，容易遭受到有心人士的攔截、竄改、偽造等，使得資料的安全性受到威脅。為了提高機密資料傳遞時的安全性，可運用資訊隱藏技術[1]-[10]來保護機密資料。資訊隱藏技術依可否還原掩護影像，分為不可逆式資訊隱藏技術(non-reversible data hiding) [1]-[4]與可逆式資訊隱藏技術(reversible data hiding) [5]-[9]，不可逆式資訊隱藏技術指當掩護影像嵌入機密訊息後，將無法在擷取出機密訊息後被無失真地還原。而可逆式資訊隱藏技術就是擷取出機密訊息後，掩護影像能無失真地被還原。

Ni 學者等人於 2006 年提出基於直方圖之可逆式資訊隱藏技術[5]，主要概念是統計掩護影像像素值的出現次數，藉由將峰點(peak point)與零點(zero point)之間的像素值位移一個位置，並利用修改峰點像素值來藏匿一個機密位元，還原時只要收到峰點與零點像素值，即可提取機密訊息與還原掩護影像。由於僅對掩護影像中峰點與零點像素值之間的像素進行位移一個位置的修改，能得到高視覺品質的偽裝影像。然而由於掩護影像中峰點像素值的像素量通常約僅佔 10% ~ 20%，導致所得到的資訊隱藏量只能達到約 0.1~0.2bpp (bit per pixel)。Tian 學者於 2003 年提出基於差異擴張可逆式資訊隱藏技術[6]，主要作法是將掩護影像以兩個像素為一區塊，藉以將區塊中兩像素值之間的差值擴張為兩倍來藏匿一個機密位元。提取機密訊息時，只需利用 LSB 替代法[1]提取偽裝影像區塊中兩像素值之間的差值之最不重要位元，即能提取出機密位元；同時將偽裝影像區塊中兩像素值之間的差值減半即能將掩護影像還原。由於差值擴張將使得偽裝影像的視覺品質較差，而且資訊隱藏量也只有 0.5 bpp。

2007 年 Chang 等學者[7]提出基於 EMD 之雙偽裝影像可逆式隱藏技術，將掩護影像中以兩個像素為一區塊進行分割，並對每一個像素做±2 之間的修改來藏匿一個五進位位數。將區塊中的兩個像素值作為平面上的一個點座標，並藉由 EMD (Exploiting Modification Direction) [4]方法來計算點座標的 f 值；在通過該點的兩條對角線上找到 f 值與欲藏匿的位數數字相同之最鄰近兩點分別作為兩偽裝影像所對應區塊之像素值。在擷取機密訊息時，將兩偽裝影像相對應區塊中的像素值作為兩個點的座標，並分別計算其 f 值即可提取出機密訊息；進一步藉由求得通過此兩點的兩條對角線之交點即可還原掩護影像。此方法具有高隱藏量約為 $\log_2 5$ bpp (每個掩護影像像素的藏匿量)，而其 PSNR (Peak Signal to Noise Ratio)值約為 45 dB。

2009 年 Lee 等學者[8]提出座標關係雙偽裝影像可逆式隱藏技術，以兩個像素為一區塊進行分割，並將每個區塊複製成兩個偽裝區塊，分別為主要區塊與輔助區塊。藏匿機密位元時，先以主要區塊做為座標平面上的一個點座標，利用該座標之上下左右相鄰的 4 個點來藏匿一個 2 位元值。為了可以還原掩護影像的像素值，輔助區塊依主要區塊藏

匿 2 位元值後的座標位置與接續兩個機密位元值之空間關係來決定是否用於藏匿。提取機密位元與還原掩護影像時，可藉由計算主要區塊與輔助區塊之差值即可推導出機密位元與原始掩護影像。由於每個區塊只修改一個像素且修改量為+1 或-1，因此具有高的 PSNR 值，約為 52 dB；然而輔助區塊約有 1/2 的機率未嵌入機密位元，導致平均每個掩護影像像素的資訊隱藏量僅達 1.5 bpp。

另一方面，於 1979 年學者 Blakley 和 Shamir 提出了機密分享機制的概念[10][11]，稱之(***t***, ***n***)-threshold scheme，將一機密資料切割成 ***n*** 份的分享資料，由 ***n*** 個合法擁有者分開保管。當要重組機密資料時，只需收集其中任 ***t*** 份分享資料，即可重組出原始機密資料；換言之少於或等於 ***n-t*** 份分享資料遭受破壞或遺失，並不會影響到原始機密資料的重組。因此，機密分享機制能避免因單一密文遭到破壞或遺失而無法還原的問題。同時，也藉由將一份機密資料分割成多份分享資料分散保管，也分散密文被破壞竊取的風險，藉以強化機密資料的安全性與隱密性。然而所產生的分享影像是一張看似雜訊(Noisy-like)的影像，在安全性上較容易吸引攻擊者注意力，且造成分享影像管理上的不便。因此，學者們[12][13]進一步結合資料隱藏技術來保護經由機密分享機制所產生的分享影像。

我們在先前文獻中提出了失真限制雙偽裝可逆式資訊隱藏技術[9]，將掩護影像中每一個像素做±1之間的修改來產生兩張偽裝影像之相對應像素。為了達到可逆之特性，限制修改量之和必需為 0 或 1，符合上述條件僅有五種修改組合，將用於藏匿一個五進位位數。因此，掩護影像可以藉由計算兩張偽裝影像相對應像素之和的平均來還原；進一步，利用兩張偽裝影像與掩護影像相對應像素的差值，即可提取出機密訊息。每個掩護影像像素的資訊隱藏量可達到$\log_2 5$ bpp，PSNR 值也有 50.35 dB 以上，同時也能具有(**2**, **2**)-threshold 機密分享的功能。

然而，實際要隱藏的資訊量可能大於或小於掩護影像所能提供的隱藏量，而且使用者對於偽裝影像的影像品質要求或許也可以放寬些。因此，本論文將延伸我們先前的作法，提出一個新的雙偽裝可逆式資訊隱藏技術，讓使用者可以依照所要藏匿的資料量來決定像素值修改量的組合數，以最適切的資料隱藏量與最小的影像失真量來藏匿資料，同時達到可逆式資訊隱藏與機密分享的功能。由於雙偽裝可逆式資訊隱藏技術的可藏量可在藏匿資料前計算得知，所以，我們將可先決定嵌入時所需使用的組合個數(也就是使用的進位數值)，x。為了能達到可逆式資料隱藏的目的，兩偽裝影像的像素值修改量之和必須介於 0 到 1 之間，同時以變化量最少的前 x 種組合來藏匿一個 x 進位位數，來獲得最小的影像失真。進一步，藉由所推導出的公式計算出嵌入 x 進位位數時像素值的修改量，來產生兩張偽裝影像。在擷取訊息與還原掩護影像時，必須同時取得兩張偽裝影像來達到機密分享的功能。掩護影像的還原可藉由計算兩張偽裝影像相對應像素之和的平均來還原，並藉由將兩偽裝影像與掩護影像之像素差值代入所推導出的公式中來計算出藏匿的機密位數。

為了瞭解所提出方法的效能，我們進一步計算出在不同進位值時的資訊隱藏量與影像視覺品質期望值。由分析結果可知：在使用 2 進位時，資訊隱藏量可達每個掩護影像像素可藏匿 1 個位元(1 bbp)，同時其視覺品質的期望值可達 54.151dB。當使用 16 進位時，資訊隱藏量則可達 4 bpp，且仍能維持 40.727 dB 的高視覺品質。我們亦將與先前三種雙偽裝影像可逆式隱藏技術進行效能上的比較，來驗證本論文所提出的方法因能依照所要藏匿的資料量來決定使用的像素值修改量組合，以最適切的資料可藏量與最小的影像失真量來藏匿資料，在偽裝影像的影像品質期望值上能優於其它方法；且當隱藏量較大而其它方法不夠空間來藏匿時，本論文所提出的方法仍能以不錯的視覺品質方式來藏匿機密資訊。

本論文其餘章節架構如下：第 2 節將針對雙偽裝影像可逆式資訊隱藏技術相關文獻進行探討；本論文所提出的方法將於第 3 節中說明；並於第 4 節針對所提出的方法進行效能分析；最後，第 5 節為本論文的結論。

2. 文獻探討

2.1 基於 EMD 之雙偽裝影像可逆式隱藏技術

2007 年 Chang 學者等人基於 EMD 藏匿法的概念，提出一個可逆式雙偽裝資訊隱藏技術，我們稱為基於 EMD 之雙偽裝影像可逆式隱藏技術。首先將像素值 0 到 255 作為一個平面上的 X 軸和 Y 軸的可能值，進一步以區塊中的兩個像素作為平面上的一個座標(x,y)，並以公式(1)計算其 f 值。

$$f = (x + 2y) mod\ 5 \quad \text{.....(1).}$$

掩護影像以兩個像素為一區塊進行分割，並以區塊中的像素作為一個點座標，同時將機密訊息轉成五進位位數，在通過該點的左斜(右斜)對角線上找到 f 值與欲藏匿的第一位數(第二位數)相同且距離該點之最鄰近點作為第一張(第二張)偽裝影像所對應區塊之像素值。

在擷取時，依序將偽裝影像的區塊像素值作為平面上的一個點座標並代入公式(1)即可擷取出隱藏之機密訊息；同時，將兩偽裝影像相對應區塊中像素值作為兩點座標，只需求得通過此兩個點座標的兩條對角線之交點，即可還原回掩護影像。

基於 EMD 之雙偽裝影像可逆式隱藏技術以兩張偽裝影像來藏匿機密訊息，必須同時收到兩張偽裝影像方能完全擷取出機密訊息，以提升在傳遞過程的安全性，其資訊隱藏量可達為$\log_2 5$ bpp (約

2.32 bpp)；然而，由於像素修改值介於-2 與+2 之間，使得 PSNR 值大約為 45 dB。

2.2 座標關係雙偽裝影像可逆式隱藏技術

Lee 等學者在 2009 年提出基於座標概念之可逆式雙偽裝影像資訊隱藏技術，我們稱為座標關係雙偽裝影像可逆式隱藏技術。首先將掩護影像以兩個像素為一區塊進行分割，掩護影像中每個區塊(p_{2i}, p_{2i+1})將產生兩個偽裝影像區塊分別為主要區塊(p_{2i}^1, p_{2i+1}^1)與輔助區塊(p_{2i}^2, p_{2i+1}^2)。為了可以還原掩護影像的像素值，輔助區塊依主要區塊藏匿 2 位元值後的位置與接續兩個機密位元值之空間關係來決定是否藏匿。將掩護影像的 2 個像素值當作平面的點座標，並將該點上下左右相鄰的 4 個點用以藏匿一個 2 位元值(10, 01, 11, 00)，輔助區塊則以四個點之間的順時鐘旋轉 90 度或 180 度之關係來決定是否藏匿機密位元。為了提升藏匿機密位元之不確定性，Lee 學者以私密金鑰來產生一位元串流，用以決定主要區塊與輔助區塊之所在。

機密訊息擷取時，必須使用私密金鑰作為亂數產生器的種子產生串流以區分哪一個偽裝影像區塊為主要區塊，接著分別計算主要區塊與輔助區塊的第一個像素及第二個像素的差值，分別以d_1和d_2表示，經由查詢表 1 即可將機密位元還原。

表 1 機密位元擷取之規則

Case	(d_1, d_2)	s_j s_{j+1}	s_{j+2} s_{j+3}
1	(2, 0)	00	11
2	(-2, 0)	11	00
3	(0, 2)	10	01
4	(0, -2)	01	10
5	(1, 1)	00	01
6	(1, -1)	01	11
7	(-1, -1)	11	10
8	(-1, 1)	10	00
9	(1, 0)	00	
10	(-1, 0)	11	
11	(0, 1)	10	
12	(0, -1)	01	

還原掩護影像時，則根據d_1與d_2之絕對差值來決定如何還原掩護影像相對應區塊之像素：若絕對差值為+2 或-2 時，則將主要區塊與輔助區塊的像素值代入公式(2)，來還原掩護影像該區塊之像素，(p_{2i}, p_{2i+1})；

$$(p_{2i}, p_{2i+1}) = \left(\frac{p_{2i}^1 + p_{2i}^2}{2}, \frac{p_{2i+1}^1 + p_{2i+1}^2}{2}\right) \quad \text{.....(2),}$$

若絕對差值為+1 或-1 時，則$(p_{2i}, p_{2i+1}) = (p_{2i}^2, p_{2i+1}^2)$；若絕對差值為 0 時，則$(p_{2i}, p_{2i+1}) = (p_{2i}^2, p_{2i+1}^1)$。

由於每個區塊只修改一個像素且修改量為+1 或-1；因此，可獲得 52.3 dB 左右的高視覺品質。然而在嵌入過程中約有 1/2 的機率輔助區塊未嵌入機密位元，導致平均資訊隱藏量約為 1.5 bpp。

2.3 失真限制雙偽裝影像可逆式隱藏技術

為了提升雙偽裝影像可逆式隱藏技術的資訊隱藏量且兼顧偽裝影像視覺品質，我們於先前文獻中提出失真限制雙偽裝可逆式資訊隱藏技術，將掩護影像中每一個像素僅做±1之間的修改來產生兩張偽裝影像之相對應像素。為了藉由兩張偽裝影像像素值之和的平均來還原掩護影像，我們限制修改量之和必須為 0 或 1，符合上述條件僅有五種修改組合，將用於藏匿一個五進位位數。進一步為了提高安全性，我們使用私密金鑰作為亂數產生器的種子(seed)來產生隨機五進位位數串流，再將欲藏匿的五進位機密訊息與隨機五進位位數串流利用公式(3)可得到一個S_j'，

$$S_j' = (S_j + k_j) \bmod 5 \quad \text{.....(3),}$$

在此S_j為五進位機密位數，k_j 為隨機五進位位數。然後以S_j'作為表 2 的索引值即可找到相對應的修改量Δ_i^1和Δ_i^2，並對掩護影像像素值p_i進行修改來分別產生兩張偽裝影像相對應位置之像素p_i^1和p_i^2。

在擷取機密訊息時，先藉由兩張偽裝影像像素值之和的平均來還原掩護影像，並計算出兩張偽裝影像與掩護影像相對應位置的像素差值，由表 2 找出相對應之S_i'，接著利用私密金鑰所產生的五進位位數串流$K(k_0 k_1 k_2 \ldots)_5$與S_i'代入公式(4)，即可擷取出機密訊息。

$$S_i = (S_i' - k_i) \bmod 5 \quad \text{.....(4).}$$

表 2 機密數字嵌入之規則組合

S_i'	Δ_i^1	Δ_i^2
0	−1	+1
1	0	0
2	0	+1
3	+1	0
4	+1	−1

失真限制雙偽裝可逆式資訊隱藏技術僅對掩護影像的像素值做±1 之間的修改來藏匿一個五進位位數，PSNR 值可達 50.35 dB 以上，資訊隱藏量約為 2.32 bpp。同時，也具備有(**2**,**2**)-threshold 機密分享的功能，必需兩張偽裝影像都取得才能擷取出機密訊息。

3. 本論文所提出的方法

然而，實際要隱藏的資訊量可能大於或小於掩護影像所能提供的隱藏量，而且使用者對於偽裝影像的影像品質要求或許也可以放寬些。因此，本論文將延伸我們先前的作法，提出一個新的雙偽裝可逆式資訊隱藏技術，讓使用者可以依照所要藏匿的

資料量來決定像素值修改量的組合，以最適切的資料隱藏量與最小的影像失真量來藏匿資料，同時完成可逆式資訊隱藏與機密分享的功能。

3.1 修改量組合的選擇與計算

為了能還原掩護影像，修改量Δ^1和Δ^2必須滿足$0 \le (\Delta^1 + \Delta^2) \le 1$的條件。為了讓偽裝影像能有最佳的影像品質，在挑選所要使用的組合時，必須考量其失真量的大小。表 3 以前 16 種最小失真量的組合為例，依其失真量的大小排列出修改量Δ^1和Δ^2的組合。

表 3 最小影像失真量的前 16 種組合

Δ^1	Δ^2	位數值	Δ^1	Δ^2	位數值
0	0	0	-2	2	8
0	1	1	-2	3	9
1	0	2	3	-2	10
1	-1	3	3	-3	11
-1	1	4	-3	3	12
-1	2	5	-3	4	13
2	-1	6	4	-3	14
2	-2	7	4	-4	15

我們選擇使用前 x 種組合來藏匿資料時，每一個掩護影像的像素將用來藏匿一個 x 進位位數。公式(5)和公式(6)可用來有效地計算出兩張偽裝影像與掩護影像相對應像素之修改量，Δ^1與Δ^2。將掩護影像像素值p_i依照Δ^1與Δ^2來修改分別產生兩張偽裝影像相對應位置之像素p_i^1和p_i^2。

$$\Delta^1 = -1^{\left\lfloor \frac{S}{2} \right\rfloor + 1} \cdot \left\lfloor \frac{s}{4} + \frac{1}{2} \right\rfloor \quad \text{.....(5),}$$

$$\Delta^2 = -1^{\left\lfloor \frac{S}{2} \right\rfloor} \cdot (s \bmod 2) + \left\lfloor \frac{s \bmod 4}{2} \right\rfloor - \Delta^1 \quad \text{.....(6).}$$

在此 S 為要藏匿的位數值，$\lfloor m \rfloor$為取不大於 m 的最大整數，$a \bmod b$ 是求 a 除以 b 的餘數值。

3.2 進位數的決定

若使用 x 進位時，為避免藏匿時產生溢位的問題，對於可能產生溢位的像素值將不會用來藏匿資料，可由公式(7)與公式(8)分別計算出其下限(L_x)與上限值(U_x)；當像素值小於L_x或大於U_x時，將不用於藏匿機密訊息。

$$L_x = \left\lfloor \frac{x}{4} \right\rfloor \quad \text{.....(7),}$$

$$U_x = 255 - \left\lfloor \frac{x+2}{4} \right\rfloor \quad \text{.....(8),}$$

在此 x 為所要使用的進位數。

當使用者選擇所要使用的掩護影像後，可依公式(9)計算出使用 x 進位時該掩護影像的資訊可藏量。

$$\boldsymbol{C} = (H \cdot W - \mathrm{N}H) \cdot \log_2 \mathrm{x} \quad \text{.....(9),}$$

在此，$\boldsymbol{C}$ 為資訊可藏量，單位為位元數，$\boldsymbol{H}$ 與 $\boldsymbol{W}$ 分別為掩護影像的長與寬，$\boldsymbol{NH}$ 為不可用於藏匿的像素數，x 代表嵌入時所使用的進位數。

然後，依據所要隱藏的資料量來決定最適切的進位值，x；也就找到最小的 x 值使得該掩護影像的資訊可藏量大於或等於要藏匿的資料量。

3.3 機密訊息之嵌入

為加強機密資訊之安全性，我們將藉由 x 進位隨機串流對機密位數進行前處理，讓嵌入數字具有隨機的特性。首先使用私密金鑰作為亂數產生器的種子(seed)來產生 x 進位位數串流$K(k_0 k_1 k_2 \ldots)_{\mathrm{x}}$，並將機密資訊轉換成 x 進位。在此將轉換後的 x 進位機密訊息以$(S_0 S_1 S_2 \ldots)_x$表示。運用公式(10)與串流 K 對機密訊息進行處理，

$$S_i' = (S_i + k_i) \bmod \mathrm{x} \quad \text{.....(10),}$$

將會得到$S' = (S_0' S_1' S_2' \ldots)_x$。每次提取一個位數$S_i'$，接著將$S_i'$代入公式(5)和公式(6)便可獲得$\Delta_i^1$與$\Delta_i^2$。進一步將$\mathrm{p_i}$加上$\Delta_{\mathrm{i}}^{\mathrm{j}}$，將可得到偽裝影像 Ij 的相對應之像素值p_i^j，$1 \le j \le 2$。

為避免產生溢位，掩護影像中任一個像素值不在可隱藏的範圍內，也就是像素值小於L_x或大於U_x時，將不用於藏匿機密訊息，兩偽裝影像所對應的像素值與原始掩護影像區塊之像素值維持相同。詳細的嵌入演算法如下所示。

[嵌入演算法]

輸入：機密訊息、掩護影像、秘密金鑰

輸出：偽裝影像 1、偽裝影像 2

步驟 1：根據機密訊息的位元數與掩護影像來決定最小的進位數，x。

步驟 2：利用秘密金鑰作為亂數產生器的種子(seed)來產生 x 進位位數串流$K(k_0 k_1 k_2 \ldots)_{\mathrm{x}}$。

步驟 3：將機密訊息$(b_0 b_1 b_2 \ldots)_2$的二進位機密訊息轉換成 x 進位位數並以$(S_0 S_1 S_2 \ldots)_x$代表。

步驟 4：計算使用 x 進位進行資料隱藏時像素值的上下限，L_x和U_x。

步驟 5：令 $i = 0$；$j = 0$。

步驟 6：當掩護影像的像素值p_i小於L_x或大於U_x時，則$(p_i^1, p_i^2) = (p_i, p_i)$，跳到步驟 10。

步驟 7：將S_j代入公式(10)求得S_j'。

步驟 8：將S_j'代入公式(5)和(6)來計算Δ_i^1與Δ_i^2後，即可得$(p_i^1, p_i^2) = (p_i + \Delta_i^1, p_i + \Delta_i^2)$。

步驟 9：$j = j + 1$。

步驟 10：$i = i + 1$，重複步驟 5 ~ 10，直到機密位元全部嵌入。

3.4 機密訊息的擷取與掩護影像的還原

當接收端收到兩張偽裝影像 I_1 與 I_2 後，首先使用雙方共同擁有的私密金鑰作為亂數產生器的種子來產生 x 進位位數串流$K(k_0k_1k_2\ldots)_x$。接著，分別從 I_1 與 I_2 中各提取出一個像素，p_i^1與p_i^2，代入公式(11)中來還原原始掩護影像像素值p_i。

$$p_i=\left\lfloor\frac{p_i^1+p_i^2}{2}\right\rfloor \quad\ldots\ldots(11),$$

然後計算$\Delta_i^1=p_i^1-p_i$與$\Delta_i^2=p_i^2-p_i$。將Δ_i^1及Δ_i^2代入公式(12)即可獲得$\hat{S}_i$，

$$\hat{S}_i=\begin{cases}4\Delta_i^1+(\Delta_i^1+\Delta_i^2+1)mod\,2-2, & if\ \Delta_i^1>0\\ -3\Delta_i^1+\Delta_i^2, & otherwise\end{cases}\quad(12),$$

最後再利用獲得的$\hat{S}_i$與k_i代入公式(13)即可擷取出 x 進位位數S_i。

$$S_i=(\hat{S}_i-k_i)\bmod x \quad\ldots\ldots(13),$$

詳細的機密訊息的擷取與掩護影像的還原演算法如下所示。

[機密訊息的擷取與掩護影像的還原之演算法]

輸入： 偽裝影像 1(I_1)、偽裝影像 2(I_2)、進位數(x)、秘密金鑰

輸出： 機密訊息、掩護影像

步驟 1： 使用私密金鑰作為亂數產生器的種子來產生 x 進位位數串流$K(k_0k_1k_2\ldots)_x$。

步驟 2：計算使用 x 進位進行資料隱藏時像素值的上下限，L_x和U_x。

步驟 3： 令 $i=0$；$j=0$。

步驟 4： 分別從 I_1 與 I_2 中提取出像素p_i^1與p_i^2，若p_i^1=p_i^2且小於L_x或大於U_x時，則$p_i=p_i^1$且跳到步驟 8。

步驟 5：將p_i^1與p_i^2代入公式(11)來還原原始掩護影像像素值p_i

步驟 6： 計算$\Delta_i^1=p_i^1-p_i$與$\Delta_i^2=p_i^2-p_i$。並代入公式(12)可得到$\hat{S}_i$。

步驟 7：將$\hat{S}_i$與k_j代入公式(13)，即可得機密數字S_j。

步驟 8： j ＝ j ＋1。

步驟 9： $i=i+1$，重複步驟 4 ~ 9，直到所有機密數字全部提取。

步驟 10：將機密訊息$(S_0,S_1,S_2,\ldots)_x$轉換成二進位位數，即可還原機密訊息位元$(b_0,b_1,b_2,\ldots)_2$。

4. 效能分析

我們以偽裝影像的視覺品質與資訊隱藏量為基準，來分析本論文提出方法的效能。視覺品質之測量可以利用高峰訊號雜訊比(PSNR)，如公式(14)所示。PSNR 值越大，影像視覺品質相對越好。

$$PSNR=10\times\log_{10}\left(\frac{255^2}{MSE}\right)\quad\ldots\ldots(14),$$

在此$MSE=\frac{1}{H\times W}\sum_{i=0}^{H\times W}(\overline{p}_i-p_i)^2$，$H$ 與 W 分別代表掩護影像的長與寬，$\overline{p}_i$代表偽裝影像像素 i 的像素值，p_i代表掩護影像像素 i 的像素值。資料隱藏量則使用平均每個偽裝影像像素可嵌入的位元數來評量，如公式(15)。

$$資料隱藏量=\frac{(H\cdot W-NH)\cdot log_2 x}{H\cdot W}\quad\ldots\ldots(15),$$

在此，H 與 W 分別為掩護影像的長與寬，NH 為不可用於藏匿的像素數，x 代表嵌入時所使用的進位數。

4.1 分析的結果

由於嵌入前我們利用了 x 進位隨機串流對機密位數進行前處理，讓嵌入數字具有隨機的特性。因此嵌入時每種組合使用的機率相同，所以我們可以容易地計算出再使用不同進位時，兩張偽裝影像的 MSE 與 PSNR 值，如表 4 所示。

表 4 兩張偽裝影像影像品質的期望值

進位數	MSE_1	$PSNR_1$	**MSE_2**	$PSNR_2$
2	0	∞	0.5	51.141
3	0.3333	52.902	0.3333	52.902
4	0.5	51.141	0.5	51.141
5	0.6	50.349	0.6	50.349
6	0.6667	49.892	1.1667	47.461
7	1.1429	47.551	1.1429	47.551
8	1.5	46.370	1.5	46.370
9	1.7778	45.632	1.7778	45.632
10	2	45.120	2.5	44.151
11	2.6364	43.921	2.6364	43.921
12	3.1667	43.125	3.1667	43.125
13	3.6154	42.549	3.6154	42.549
14	4	42.110	4.5	41.599
15	4.8	41.318	4.8	41.318
16	5.5	40.727	5.5	40.727

由表 4 可知在大多數的情況下，兩張偽裝影像的影像品質期望值為相同，但在進位 2、進位 6、進位 10 與進位 14 等情況，第二張偽裝影像的影像品質比第一張偽裝影像差了一點，這是由於表 3 的排列順序所導致。為使兩張影像品質能有一致的期望值，我們可以進一步使用私密金鑰來產生一個隨機位元串流作為修改量的選擇依據。當位元值為 0 時，第一張偽裝影像與掩護影像的差值為公式(5)所計算的結果，第二張偽裝影像與掩護影像的差值為公式(6)所計算得到的結果；當位元值為 1 時，則第一張偽裝影像與掩護影像的差值則使用公式(6)所計算出的值，第二張偽裝影像則使用公式(5)所計算得到出的值作為變化量。由於位元串流具有隨機性，兩張偽裝影像選擇公式(5)或公式(6)作為變化量計算之機率相同，因此，兩張影像品質期望值會相同。

表 5 列出在隨機選取公式的情況下，偽裝影像的影像品質期望值。同時，表 5 也列出了在假設沒有像素發生溢位的情況下(也就是 NH=0)，掩護影像的資料隱藏量。由表 5 可知，在使用 2 進位的方式來藏匿資料，資訊隱藏量為 1bpp，視覺品質可達 54.151dB，在使用 16 進位時，資訊隱藏量可達 4 bpp，且仍能維持 40.727 dB 的高視覺品質。

表 5 影像品質與隱藏量的期望值

進位數	MSE	PSNR	**資料隱藏量 (bits/pixel)**
2	0.25	54.151	1
3	0.3333	52.902	1.585
4	0.5	51.141	2
5	0.6	50.349	2.322
6	0.9167	48.509	2.585
7	1.1429	47.551	2.807
8	1.5	46.370	3
9	1.7778	45.632	3.170
10	2.25	44.609	3.322
11	2.6364	43.921	3.459
12	3.1667	43.125	3.585
13	3.6154	42.549	3.700
14	4.25	41.847	3.807
15	4.8	41.318	3.907
16	5.5	40.727	4

進一步我們分析本論文所提出的方法與先前三種雙偽裝影像可逆式隱藏技術(基於 EMD 之雙偽裝影像可逆式隱藏技術、座標關係雙偽裝影像可逆式隱藏技術和失真限制雙偽裝影像可逆式隱藏技術)在藏匿幾種大小不同的位元數量後，偽裝影像的影像品質期望值之比較。以一張 256 × 256 的灰階影像作為掩護影像為例，表 6 列出偽裝影像的影像品質期望值之比較。由表 6 可知，本論文所提出的方法在影像品質期望值能優於其它方法，且當隱藏量為 180000 時，其它方法已不夠空間來藏匿，本論文所提出的方法仍能藏匿且維持 47.634 dB 的高視覺品質。

表 4 偽裝影像影像品質期望值之比較

藏匿位元數	基於 EMD	座標關係	失真限制	本論文方法
30000	52.169	57.545	57.397	57.545
60000	49.159	54.535	54.387	54.535
90000	47.398	52.774	52.626	53.529
120000	46.148	不夠藏	51.377	51.524
150000	45.179	不夠藏	50.408	50.408
180000	不夠藏	不夠藏	不夠藏	47.634

5. 結論

本論文提出一個新的雙偽裝可逆式資訊隱藏技術，讓使用者可以依照所要藏匿的資料量來決定像素值修改量的組合，以最適切的資料隱藏量與最小的影像失真量來藏匿資料。由於修改量Δ^1 和 Δ^2 必須滿足 $0 \le (\Delta^1 + \Delta^2) \le 1$ 的條件，掩護影像的像素值能輕易地由兩張偽裝影像的像素值平均來還原，同時我們推導出公式讓嵌入時能很容易地計算出修改量Δ^1 和Δ^2 以及可用來嵌入資料的像素值之上下限，L_x和U_x。在擷取時也能經由公式輕鬆地計算出嵌入的機密位數。同時，必需兩張偽裝影像都取得才能擷取出機密訊息，因此也具備有(**2**,**2**)-threshold 機密分享的功能。經由效能分析，所提出的方法在使用 2 進位來藏匿資料時，資訊隱藏量為 1bpp，視覺品質可達 54.151dB，在使用 16 進位時，資訊隱藏量可達 4 bpp，且仍能維持 40.727 dB 的高視覺品質。在與先前三種雙偽裝影像可逆式隱藏技術進行分析比較，本論文所提出的方法確實能以最適切的資料隱藏量與最小的影像失真量來來藏匿資料，同時完成可逆式資訊隱藏與機密分享的功能。

參考文獻

[1] C. K. Chan and L. Cheng, "Hiding Data in Images by Simple LSB Substitution," Pattern Recognition, Vol. 37, Issue 3, pp. 469-474, March 2004.

[2] J. Mielikainen, "LSB matching revisited," IEEE Signal Processing Letters, Vol. 13, Issue 5, pp. 285-287, April 2006.

[3] R. Z. Wang, C. F. Lin, and J. C. Lin, "Image Hiding by Optimal LSB Substitution and Genetic Algorithm," Pattern Recognition, Vol. 34, Issue 3, pp. 671-683, March 2001.

[4] X. Zhang and S. Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction," IEEE Communications Letters, Vol. 10, Issue 11, pp. 781-783, November 2006.

[5] Ni. Zhicheng, Y. Q. Shi, N. Ansari, and Wei Su, "Reversible data hiding," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 16, Issue 3, pp. 354-362, March 2006.

[6] J. Tian, "Reversible Data Embedding Using a Difference Expansion," IEEE Transactions on Circuits and Systems for Video Technology, Vol 13, Issue 5, pp. 890-896, August 2003.

[7] C. C. Chang, K. T. Duc, and Y. C. Chou, "Reversible Data Hiding Scheme Using Two Steganographic Images," Proceedings of TENCON 2007, pp. 1-4, October 2007.

[8] C. F. Lee, K. H. Wang, C. C. Chang, and Y. L. Huang, "A Reversible Data Hiding Scheme Based on Dual Steganographic Images," Proceedings of the Third International Conference on Ubiquitous Information, pp. 228-237, February 2009.

[9] 詹智豪、許俊萍、邱川峰、詹森仁、陳以裕, "雙偽裝影像之可逆式資訊隱藏," 論文集光碟 of AIT 2011 資訊科技國際研討會, 朝陽大學, April, 2011.

[10] G. R. Blakley, “Safeguarding cryptographic keys,” Prceedings of the AFIPS National Computer Conference, pp. 313-317, June 1979.

[11] A. Shamir, “How to share a secret,” Communications of the ACM, Vol. 22, Issue 11, pp. 612-613, Nov. 1979.

[12] Y. S. Wu, C. C. Thien and J. C. Lin, “Sharing and hiding secret images with size constraint,” Pattern Recognition, Vol. 37, pp. 1377-1385, July 2004.

[13] C. C. Thien and J. C. Lin, “An image-sharing method with user-friendly shadow images,” IEEE Transactions on Circuits and systems for Video Technology, Vol. 13, No. 12, pp. 1161-1169, Dec. 2003.