使用雙偽裝影像之可逆式資訊隱藏改良機制

詹智豪
明新科技大學資訊管理系
研究生
chang5837466@hotmail.com

許俊萍
明新科技大學資訊管理系
助理教授
steenhsu@must.edu.tw

邱川峰
明新科技大學資訊管理系
助理教授
cfchiu@must.edu.tw

詹森仁
明新科技大學資訊管理系
助理教授
srchan@must.edu.tw

陳以裕
明新科技大學資訊管理系
講師
cyy@must.edu.tw

摘要

雙偽裝影像隱藏技術能提高資訊隱藏量、降低影像失真率、無失真還原掩護影像。同時必須兩張偽裝影像都取得才能還原隱密資訊，擁有機密分享的優點；EMD 雙偽裝影像可逆式隱藏技術將掩護影像中每一個像素做±2 之間的修改來藏匿一個五進位位數，具有高資訊隱藏量，約為 1 bpp，其 PSNR 值約為 45 dB。座標關係雙偽裝影像可逆式隱藏技術將掩護影像中每一個像素做±1 之間的修改來藏匿一個四進位位數，具有高的 PSNR 值，約為 52 dB。然而，在嵌入過程中輔助區塊約有 1/2 的機率未嵌入機敏位元，導致資訊隱藏量為 0.75 bpp。因此，本論文將提出雙偽裝影像可逆式資訊隱藏之改良機制，僅對像素值作±1 之間修改，並以能成功還原像素值之五種嵌入組合來藏匿一個五進位位數，有效地提升資訊隱藏量與維持高的影像視覺品質，同時能達到可逆式之特性。實驗結果將證明本論文方法的資訊隱藏量為 1.16 bpp 及 PSNR 值可達 50.35 dB 以上。

關鍵詞：資料隱藏、藏密學、可逆式資訊隱藏、雙偽裝影像。

Abstract

Using two steganographic images, a reversible data hiding technique can enhance embedding capacity, reduce steganographic image distortion and restore the original cover image without any distortion. Moreover, both of the two steganographic images must be obtained simultaneously for extracting the secret information completely. EMD-based reversible data hiding technique using two steganographic images hides a base-5 numeral by modifying each pixel in the cover image at most two. The scheme can provide high embedding capacity, about 1 bpp. But, the PSNR value of a steganographic image is about 45 dB. On the other hand, the coordinate-relationship reversible data hiding technique hides a base-4 numeral by modifying each pixel in the cover image at most one. As the result, the PSNR value of their scheme can reach in a high value about 52 dB; however, the embedding capacity is only about 0.75 bpp because the probability of an auxiliary block cannot be used to embed any secret bits is about 1/2. Therefore, this paper proposes a new reversible data hiding scheme using two steganographic images to hide a base-5 numeral with only modifying each pixel within the range of ±1. Only the five modification combinations which can be used to recover the original pixels successfully are used to embed a base-5 numeral. The proposed scheme can effectively improve embedding capacity; meanwhile, the visual quality can still be kept high, and the characteristic of reversibility can also be achieved. Experimental results show that the proposed scheme can obtain the embedding capacity is about 1.16 bpp and the PSNR value greater than 50.35 dB.

Keywords: Data hiding, steganography, reversible data hiding, dual steganographic images.

1. 前言

隨著網際網路技術的蓬勃發展，運用網路來傳遞訊息與資料已成為現代人彼此通訊的慣用方式之一。然而，在訊息傳遞過程中，容易遭受到攔截、竄改或偽造，使得資料的安全性受到威脅。為了解決機敏資料傳遞的安全議題，密碼學(cryptography)中的加密演算法[6]和資訊隱藏技術(Information Hiding Technique)[1-5,7-9]皆為可行的解決方法。

加密演算法是將機密的影像、文字、聲音等資料透過加密的程序打亂原始的資料來避免外界有心人士的非法擷取，以達保密的目的。然而加密後無意義的密文，卻容易引來非法的有心人士的注意，並可能進一步進行破解、竄改或破壞。

相較於加密演算法著重機敏性資料之隱藏，資訊隱藏技術則著重於通訊之隱藏；藉由將機敏資料隱藏於數位媒介(如影像、聲音、視訊檔等)中，來掩蓋機敏資料通訊的事實。用以作為掩護機敏資料的數位媒介稱之為掩護媒介(Cover Media)，嵌入機敏資料後則產生偽裝媒介(Stego Media)。偽裝媒介應具有不易被發掘的能力，當以灰階影像作為媒介時，偽裝影像的視覺品質十分重要。視覺品質可以用高峰訊號雜訊比(Peak Signal to Noise Ratio, PSNR)來評估，掩護影像與偽裝影像的像素值的差異性越小，PSNR 值越高。除了視覺品質外，資訊隱藏技術亦應考量到其資訊隱藏量的能力。

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)[2,5,7,9]與可逆式資訊隱藏技術(reversible data hiding)[1,3-4,8]，不可逆式資訊隱藏技術指當掩護影像嵌入機敏訊息後，將無法在擷取出機敏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敏訊息後，掩護影像能無失真地被還原。然而可逆式資訊隱藏技術，通常需要紀錄額外資訊以便能無失真地還原掩護影像，造成在資訊隱藏量方面都比不可逆式資訊隱藏技術表現較差。因此，近年來許多學者[1,4]研究如何不需要紀錄額外資訊來提升可逆式資訊隱藏技術的資訊隱藏量。

2007 年 Chang 等學者運用模數函式藏匿法(Exploiting Modification Direction, EMD)[9]的概念提出兩張偽裝影像的可逆式隱藏技術[1]，我們稱之為 EMD 雙偽裝影像可逆式隱藏技術。該技術將掩護影像以兩個像素為一區塊來藏匿兩個五進位位數。以區塊的兩像素值作為平面座標上的一個座標點，在通過該點的兩條對角線上找到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。在擷取機敏訊息時，將兩偽裝影像相對應區塊中的像素值作為兩座標點，藉由求得通過此兩個座標點的兩條對角線之交點能順利還原掩護影像，無需記錄額外的資訊。其資訊隱藏量大約為 1 bpp(bit per pixel)與偽裝影像 PSNR 值可達到 45 dB。

2009 年 Lee 等學者也提出一種使用兩張偽裝影像的可逆式隱藏技術[4]，我們稱之為座標關係雙偽裝影像可逆式隱藏技術。該技術將兩偽裝影像以兩個像素為一區塊，並分為主要區塊與輔助區塊來藏匿訊息。主要影像區塊以座標點的上下左右四個相鄰點來嵌入 2 位元值，輔助區塊則依主要區塊藏匿方向與欲藏匿 2 位元值的藏匿方向之空間關係來決定是否藏匿，其主要目的是能夠不需記錄額外的資訊，則達到可逆式資訊隱藏技術。由於僅修改一個像素值且修改值介於±1 之間，可達 52dB 以上的 PSNR 值；然而，在嵌入過程中輔助區塊約有 1/2 的機率未嵌入機敏位元，導致資訊隱藏量約為 0.75 bpp。

為了兼具前述兩種技術的優點，本論文將提出新的隱藏技術，僅對掩護影像中每一個像素僅做±1 之間的修改來藏匿機敏訊息。將掩護影像像素值做(-1, 0, 1)之修改組合方式共有九種，為能藉由兩張偽裝影像像素值之和的平均來還原掩護影像，兩張偽裝影像像素值修改量之和必須介於 0 到 1 之間，其中符合上述條件僅有五種組合，將用於藏匿一個五進位位數，以達到可逆式之特性。同時，為避免單張偽裝影像能獲取片段機敏資訊，機敏訊息將藉由五進位隨機串流來使得真正的嵌入數字具有隨機性。進一步，我們將探討在進位轉換時，位元區塊大小與資訊隱藏量之關聯性，以找出符合程式語言基本資料型態中較高隱藏量之區塊大小。藉由實驗結果驗證本論文所提出方法的資訊隱藏量可達 1.16 bpp 及影像視覺品質為 50.35 dB 以上。

本論文其餘章節架構如下：第 2 節將介紹相關的雙偽裝影像可逆式資訊隱藏技術；本論文所提出的方法將於第 3 節中說明；並於第 4 節針對實驗結果進行分析比較；最後，於第 5 節提出結論。

2. 相關文獻

2.1 Exploiting Modification Direction 藏匿法

Zhang 與 Wang 學者於 2006 年提出 Exploiting Modification Direction(EMD) 藏匿法，將機敏訊息隱藏於灰階影像中[9]。EMD 藏匿法藉由僅修改 n 個像素中一個像素值來藏匿一個(2n+1)進位的數字。首先，將掩護影像以 n 個像素為一區塊進行分割，並將機敏訊息轉成(2n+1)進位。區塊 i 的像素值($p_1, p_2, ..., p_n$)以公式(1)計算出 f 值，

$$f = f(p_1, p_2, \cdots, p_n) = (\sum_{j=1}^{n} j \times p_j) \bmod (2n+1) \quad .(1),$$

並以公式(2)計算欲藏入數字 S_i 與 f 之差值，t。

$$t = (S_i - f) \bmod (2n+1) \quad .....(2).$$

當 $t = 0$ 時，區塊 i 的像素值無需更改。當 $0 < t \le n$ ，則將第 t 個像素的像素值加 1，區塊 i 的像素值修改為 $(p_1, p_2, \cdots, p_t + 1, \cdots, p_n)$ 。當 $t > n$ ，則將第(2n + 1 - t)個像素的像素值減 1，區塊 i 的像素值修改為 $(p_1, p_2, \cdots, p_{2n+1-t} - 1, \cdots, p_n)$ 。

欲擷取機敏訊息時，將偽裝影像以 n 個像素為一區塊進行分割，並依序將每個區塊的像素值代入公式(1)，即可獲得所藏匿的秘密訊息。由於沒有任何有關原始像素之資訊可由偽裝影像中得知，導致無法還原出掩護影像。

2.2 EMD 雙偽裝影像可逆式隱藏技術

2007 年 Chang 學者等人基於 EMD 的概念，提出一個可逆式雙偽裝資訊隱藏技術[1]，將掩護影像以兩個像素為一區塊來藏匿 2 個五進位位數。以區塊的兩像素值作為平面座標上的一個點座標，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代入公式(1)即可擷取出隱藏之機敏訊息；同時，將兩偽裝影像相同區塊中像素值作為兩座標點，只需求得通過此兩個座標點的兩條對角線之交點，即可還原回掩護影像。在下面章節將更詳細地說明整個嵌入及擷取的運作方式。

2.2.1 機敏訊息之嵌入

首先，將機敏訊息 S 轉成 5 進位數字(S_0, S_1, …)，每次以兩個位數(S_{2i}, S_{2i+1})為單位，依序進行嵌入。同時，掩護影像也以 2 個像素為一個區塊進行分割，C_i 用以代表掩護影像的區塊 i。將區塊 i 的像素值(p_{2i+1}, p_{2i})代入公式(1)計算出 f 值，並以公式(2)計算欲藏入之 S_{2i} 與 S_{2i+1} 和 f 之差值，以 t_0 與 t_1 表示。t_0 與 t_1 將用於決定兩張偽裝影像的區塊 i 的像素值。當 t_0= 0 時，則第一張偽裝影像區塊 i 的像素為(p_{2i+1}, p_{2i})；當 $1 \le t_0 \le 2$，像素為 $(p_{2i+1} + t_0,\ \ p_{2i} - t_0)$ ；當 $t_0 > 2$，像素為 $(p_{2i+1} - 5 + t_0,\ \ p_{2i} + 5 - t_0)$ 。當 $t_1 = 0$ 時，則第二張偽裝影像區塊 i 的像素為(p_{2i+1}, p_{2i})；當 t_1 = 1 或 3 時，像素為 $(p_{2i+1} + (2 * t_1) \bmod 5, p_{2i} + (2 * t_1) \bmod 5)$ 。當 t_1 = 2 或 4 時，則像素為 $(p_{2i+1} - 5 + (2 * t_1) \bmod 5,\ p_{2i} - 5 + (2 * t_1) \bmod 5)$ 。

以利用掩護影像區塊 i 來藏匿機敏訊息(1, 3)為例作說明，掩護影像的像素值為(8, 7)，以公式(1)計算出 f 等於 2，並以公式(2)計算出 t_0 = 4, t_1 = 1。因 $4 > 2$，則將區塊 i 的像素值修改為 $(7 - 1, 8 + 1) = (6, 9)$，作為第一張偽裝影像區塊 i 的兩個像素值。因 t_1 = 1，則將區塊 C_1 的像素值修改成 $(7 + (2*1) \bmod 5, 8 + (2*1) \bmod 5) = (9, 10)$ ，作為第二張偽裝影像區塊 i 的兩個像素值。

2.2.2 邊界溢出問題

由於在嵌入過程時，將像素值的修改介於-2 到+2 之間，為了避免溢位的產生，區塊中任一個像素值均需大於等於 2 且小於等於 223。若不符上述條件時，則該區塊將不用於藏匿機敏訊息，兩偽裝影像所對應的區塊像素值與原掩護影像區塊之像素值維持相同。

2.2.3 機敏訊息之擷取

當接收到兩張偽裝影像，首先以兩個像素為單位進行區塊切割。從區塊 0 開始，逐一提取出兩偽裝影像的區塊 i 之像素值，分別以 (p^1_{2i+1}, p^1_{2i}) 與 (p^2_{2i+1}, p^2_{2i}) 表示，來進行機敏訊息的擷取。

當 $p^1_{2i+1} = p^2_{2i+1}$， $p^1_{2i} = p^2_{2i}$ 且 p^1_{2i+1} 或 p^1_{2i} 不在 2 到 253 之範圍內，則此兩區塊都沒有藏匿機敏訊息；否則，將 (p^1_{2i+1}, p^1_{2i}) 代入公式(1)計算

所得之 f 值即為 S_{2i}；將 (p^2_{2i+1}, p^2_{2i}) 代入公式(1)計算所得之 f 值即為 S_{2i+1}。

2.2.4 掩護影像之還原

找出與第一張偽裝影像的區塊 i 之像素 (p^1_{2i+1}, p^1_{2i}) 在左斜對角線上最鄰近五個點的集合，亦即為 $\{(p^1_{2i+1}+2, p^1_{2i}-2)$, $(p^1_{2i+1}+1, p^1_{2i}-1)$, (p^1_{2i+1}, p^1_{2i}), $(p^1_{2i+1}-1, p^1_{2i}+1)$, $(p^1_{2i+1}-2,\ p^1_{2i}+2)\}$；與第二張偽裝影像的區塊 i 之像素 (p^2_{2i+1}, p^2_{2i}) 在右斜對角線上最鄰近的五個點的集合，亦即為 $\{(p^2_{2i+1}+2, p^2_{2i}+2)$, $(p^2_{2i+1}+1, p^2_{2i}+1)$, (p^2_{2i+1}, p^2_{2i}), $(p^2_{2i+1}-1, p^2_{2i}-1)$, $(p^2_{2i+1}-2,\ p^2_{2i}-2)\}$，在兩集合中找出相同的座標點，即為原始掩護影像區塊 i 之像素值。

下面以收到兩個偽裝影像的區塊 i 之像素值(9, 10)與(6, 9)來說明如何擷取機敏訊息與還原原始掩護影像之過程。首先分別將區塊 i 之像素值(9, 10)與(6, 9)代入公式(1)計算所得之(1, 3)即為機敏訊息之(S_{2i}, S_{2i+1})。接著找出第一張偽裝影像的區塊 i 之像素(9, 10)在左斜對角線上最鄰近五個點的集合，亦即為{ (8, 7), (7, 8), (6, 9), (5, 10), (4, 11)}，與第二張偽裝影像的區塊 i 之像素(6, 9)在右斜對角線上最鄰近的五個點的集合，亦即為{(11, 12) ,(10, 11) ,(9, 10) ,(8, 9) , (7, 8)} ；然後於兩集合中找出相同的座標點為(7, 8)，即為原始掩護影像區塊 i 之像素值(8, 7)。

2.3 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[4]，將掩護影像複製成兩張相同的掩護影像，並以兩個像素為一區塊進行分割，掩護影像中每個區塊將產生的兩個偽裝影像區塊(主要區塊與輔助區塊)。為了可以還原掩護影像的像素值，輔助區塊則依主要區塊所藏匿的兩位元值與接續兩個機敏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)，以四個點之間的逆時鐘旋轉 90 度或 180 度之關係來藏匿機敏位元。為了提升藏匿機密位元之不確定性，避免單一偽裝影像能擷取部份機敏訊息，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。詳細的運作方式將於下面章節中說明。

2.3.1 隨機位元串流

傳送端與接受端共有一把私密金鑰，用以當作亂數產生器的種子(Seed)來產生一個二進位位元串流$(K = k_0k_1k_2...)$，並以 k_i 位元來決定兩張偽裝影像的區塊 i，哪一個為主要區塊，哪一個為輔助區塊。

將掩護影像 C 複製成兩張相同的掩護影像 C_1 與 C_2，並以兩個像素為一區塊進行分割。B_i^j 用以代表掩護影像 C_j 的區塊 i。當 $k_i = 0$ 時，$B_i^1 = (p^1_{2i}, p^1_{2i+1})$ 作為主要區塊，$B_i^2 = (p^2_{2i}, p^2_{2i+1})$ 作為輔助區塊；否則，B_i^2 為主要區塊，B_i^1 為輔助區塊。以下將以 k_i=0，來說明嵌入的規則。

2.3.2 機敏訊息之嵌入

首先，機敏訊息$(S = s_0s_1s_2...)$以兩位元(s_j, s_{j+1})為單位，依序提取進行嵌入。以 (p^1_{2i}, p^1_{2i+1}) 座標點之{右 $(p^1_{2i}+1, p^1_{2i+1})$ 、下 $(p^1_{2i}, p^1_{2i+1}-1)$ 、上 $(p^1_{2i}, p^1_{2i+1}+1)$ 、左 $(p^1_{2i}-1, p^1_{2i+1})$ }四個像素值修改方向分別用以藏匿(s_j, s_{j+1})四種可能的值{00、 01、10、 11}，如圖 1 所示。修改後的像素值則作為第一張偽裝影像 I_1 區塊 i 的像素值。然後，依下兩個機敏位元(s_{j+2}, s_{j+3})與(s_j, s_{j+1})在藏匿時像素值修改方向的關係來決定第二張偽裝影像 I_2 的區塊 i 是否用以藏匿機敏位元。若(s_{j+2}, s_{j+3})在方向上為(s_j, s_{j+1})逆時鐘旋轉 90 度或 180 度，則提取出(s_{j+2}, s_{j+3})並依表 1 所示藏入 I_2 的區塊 i 中；否則 I_2 的區塊 i 之像素值不變。

表 1 為機敏訊息嵌入規則

Case	$S_j\ S_{j+1}$	$S_{j+2}\ S_{j+3}$	stego image (p^2_{2i}, p^2_{2i+1})
1	00	11	$(p_{2i}\text{-}1, p_{2i+1})$
2		01	$(p_{2i}, p_{2i+1}\text{-}1)$
3		00 或 10	(p_{2i}, p_{2i+1})
4	10	01	$(p_{2i}, p_{2i+1}\text{-}1)$
5		00	$(p_{2i}+1, p_{2i+1})$
6		10 或 11	(p_{2i}, p_{2i+1})
7	11	00	$(p_{2i}+1, p_{2i+1})$
8		10	$(p_{2i}, p_{2i+1}+1)$
9		01 或 11	(p_{2i}, p_{2i+1})
10	01	10	$(p_{2i}, p_{2i+1}+1)$
11		11	$(p_{2i}\text{-}1, p_{2i+1})$
12		00 或 01	(p_{2i}, p_{2i+1})

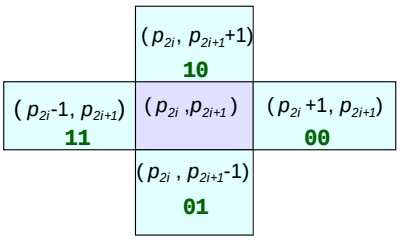

圖 1 機敏位元藏匿值與像素值修改方向之關聯

2.3.3 邊界溢出問題

由於嵌入機敏訊息時，只對像素值作-1 到+1 之間的變動；為避免產生溢位，區塊中任一個像素值等於 0 或 255 時，主要區塊和輔助區塊都將不藏匿機敏訊息，兩偽裝影像所對應的區塊像素值與原始掩護影像區塊之像素值維持相同。

2.3.4 機敏訊息之擷取

當接收端收到兩張偽裝影像 I_1 與 I_2 時，首先以使用私密金鑰作為亂數產生器的種子來產生位元串流($K = k_0k_1k_2\ldots$)，並將 I_1 與 I_2 以兩個像素為單位進行區塊切割。從區塊 0 開始，逐一取出兩區塊之像素值 (p^1_{2i}, p^1_{2i+1}) 與 (p^2_{2i}, p^2_{2i+1})。若 $k_i = 0$ 時，則偽裝影像 I_1 之區塊 i 為主要區塊。當 $(p^1_{2i}, p^1_{2i+1}) = (p^2_{2i}, p^2_{2i+1})$，則該區塊並未藏匿任何機敏訊息;否則，計算 p^1_{2i} 與 p^2_{2i} (p^1_{2i+1} 與 p^2_{2i})之差值 $d_0(d_1)$；以 $d_0(d_1)$之值來決定 $S_j\,S_{j+1}$ 與 $S_{j+2}\,S_{j+3}$ 的值，如表 2 所示。

2.3.5 掩護影像之還原

機敏訊息擷取時，若該主要區塊未藏匿機敏位元時，則還原原始掩護影像區塊 i 的像素值 (p_{2i}, p_{2i+1}) 為 (p^1_{2i}, p^1_{2i+1})；否則，可依 d_0 與 d_1 的絕對值來決定如何還原：當 d_0 與 d_1 的絕對值之差為±2 時，則將 (p^1_{2i}, p^1_{2i+1}) 與 (p^2_{2i}, p^2_{2i+1}) 代入公式(3)，來還原 (p_{2i}, p_{2i+1});

$$P(p_{2i}, p_{2i+1}) = \left(\frac{p^1_{2i} + p^2_{2i}}{2}, \frac{p^1_{2i+1} + p^2_{2i+1}}{2} \right) \quad \text{.....(3).}$$

當 d_0 與 d_1 的絕對值之差為$|d_0|-|d_1| = \pm 1$ 時，則 $(p_{2i}, p_{2i+1}) = (p^2_{2i}, p^2_{2i+1})$；當 d_0 與 d_1 的絕對值之差為 0 時，則 $(p_{2i}, p_{2i+1}) = (p^2_{2i}, p^1_{2i+1})$。

表 2 d_0, d_1 值與機敏位元擷取之規則

Case	(d_0, d_1)	$s_j\ s_{j+1}$	$s_{j+2}\ s_{j+3}$
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	

2.4 討論

EMD 雙偽裝影像可逆式隱藏技術改善了 EMD 方法不能還原掩護影像的問題，且以兩張偽裝影像來藏匿機敏訊息，利用區塊的兩像素值作為平面座標上的一個座標點，在通過該點的兩條對角線上找到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用以嵌入兩個五進位位數，使得資訊隱藏量可達 1 bpp；然而，像素修改值介於-2 與+2 之間，因此影像品質(PSNR 值)大約為 45 dB。

座標關係雙偽裝影像可逆式隱藏技術以主要區塊與輔助區塊來藏匿訊息。主要影像區塊以座標點的上下左右四個相鄰點來嵌入 2 位元值，輔助區塊則依主要區塊藏匿方向與欲藏匿 2 位元值的藏匿方向之空間關係來決定是否藏匿，在嵌入機敏訊息時對掩護影像的像素值之修改僅介於±1 之間，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敏位元，導致資訊隱藏量約為 0.75 bpp。

3. 本論文所提出的方法

本論文提出一個新穎的隱藏技術，將掩護影像中每一個像素僅做±1 之間的修改來藏匿一個五進位位數，並產生兩張偽裝影像。掩護影像像素值做(-1, 0, 1)之修改組合方式共有九種，為能藉由兩張偽裝影像像素值之和的平均來還原掩護影像，兩張偽裝影像像素值修改量之和必須介於 0 到 1 之間，如表 3 所示，其中僅有五種組合符合上述條件，將用於藏匿一個五進位位數，以達成可逆式資訊隱藏技術，同

時提升資訊隱藏量與影像視覺品質。詳細的運作方式將於下面章節中說明。

表 3 九種修改組合

掩護影像與偽裝影像 1 的差值，Δ_i^1	掩護影像與偽裝影像 2 的差值，Δ_i^2	是否符合條件(Y/N)
0	0	Y
0	+1	Y
0	-1	N
+1	0	Y
+1	+1	N
+1	-1	Y
-1	0	N
-1	+1	Y
-1	-1	N

3.1 機敏訊息之嵌入

首先，私密金鑰作為亂數產生器的種子(seed)來產生五進位位數串流 $K(k_0k_1k_2\cdots)_5$，同時機敏訊息以 n 個位元為一組轉換成$\lceil n\log_5 2\rceil$個五進位位數。在此將轉換後的五進位機敏訊息以$(S_0S_1S_2\cdots)_5$表示。運用公式(4)與串流 k 來對機敏訊息進行處理，而得 $S'=(S_0'S_1'S_2'\cdots)_5$。每次提取一個位數$S_j'$，依序嵌入掩護影像的像素$p_i$中來獲得兩張偽裝影像對應位置的像素值 p_i^1 與 p_i^2 。如表 4 所示，找出相對應的機敏數值 S_j' 可獲得 p_i^1 (p_i^2)與 P_i 之間的差值 $\Delta_i^1(\Delta_i^2)$。將 P_i 加上 $\Delta_i^1(\Delta_i^2)$，來產生第一張偽裝影像 I_1 第 i 個像素值 p_i^1 與第二張偽裝影像 I_2 第 i 個像素值 p_i^2 。

$$S_j' = (S_j + k_j) \bmod 5 \quad \text{.....(4).}$$

表 4 機敏數字嵌入之規則組合

S_j'	Δ_i^1	Δ_i^2	P_i^1	P_i^2
0	-1	1	P_i^1-1	P_i^2+1
1	0	0	P_i^1	P_i^2
2	0	1	P_i^1	P_i^2+1
3	1	0	P_i^1+1	P_i^2
4	1	-1	P_i^1+1	P_i^2-1

[嵌入演算法]

輸入：機敏訊息、掩護影像、秘密金鑰、位元區塊大小(n)

輸出：偽裝影像 1、偽裝影像 2

步驟 1: 利用秘密金鑰作為亂數產生器的種子(seed)來產生五進位位數串流 $K(k_0k_1k_2\cdots)_5$。

步驟 2: 將機敏訊息$(b_0b_1b_2\cdots)_2$以 n 個位元為一區塊轉換成$\lceil n\log_5 2\rceil$個五進位位數。並以$(S_0S_1S_2\cdots)_5$代表所有區塊轉換後的五進位數。

步驟 3: 令 $i=0$；$j=0$。

步驟 4: 當掩護影像的像素值 p_i 等於 0 或 255 時，跳到步驟 8，則 $(p_i^1, p_i^2)=(p_i, p_i)$。

步驟 5:將 S_j 代入公式(4)求得 S_j'。

步驟 6:當 $S_j'=0$ 時，$(p_i^1, p_i^2)=(p_i-1, p_i+1)$；

當 $S_j'=1$ 時，$(p_i^1, p_i^2)=(p_i, p_i)$；

當 $S_j'=2$ 時，$(p_i^1, p_i^2)=(p_i, p_i+1)$；

當 $S_j'=3$ 時，$(p_i^1, p_i^2)=(p_i+1, p_i)$；

當 $S_j'=4$ 時，$(p_i^1, p_i^2)=(p_i+1, p_i-1)$。

步驟 7: $j=j+1$。

步驟 8:$i=i+1$，重複步驟4～7，直到機敏位元全部嵌入。

以二進位的機敏訊息$(101000110\ldots)_2$與掩護影像像素值(151, 189, 200, 212, …)為例來說明機敏訊息之隱藏過程；同時假設位元區塊大小為9。首先將機敏訊息以9個位元為一區塊進行區塊切割，並將每個區塊轉成4個五進位位數，因此機敏訊息$(101000110\ldots)_2$將轉換成(2, 3, 0, 1, …)$_5$。使用私密金鑰作為亂數產生器的種子來產生五進位位數串流K = (3, 1, 2, 4, …)$_5$；然後將S_0=2與k_0 = 3代入公式(4)可獲得 S_0' = 0。由表4得到Δ_0^1 = -1和 Δ_0^2 = +1，因此求得 p_0^1 = 150， p_0^2 = 152。接著依序前述方式來藏匿S_1 ,S_2 ,…，則可獲得第一張偽裝影像I_1 = (150, 190, 200, 211, …)與偽裝影像I_2=(152, 188, 201, 213, …)。

3.2 機敏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五進位位數串流(K = $k_0k_1k_2\ldots)_5$。接著，從 I_1與 I_2中每次各提取出一個像素， p_i^1 與 p_i^2 。若 $p_i^1=p_i^2$ 且等於 0 或 255，則沒有藏匿任何機敏數字，否則代入公式(5)中來還原原始掩護影像像素值 p_i 。

$$p_i = \left\lfloor \frac{p_i^1 + p_i^2}{2} \right\rfloor \quad \text{.....(5),}$$

然後，計算 $\hat{\Delta}_i^1 = p_i^1 - p_i$ 與 $\hat{\Delta}_i^2 = p_i^2 - p_i$ 之差值。依表 5 所示，利用 $\hat{\Delta}_i^1$ 及 $\hat{\Delta}_i^2$ 找出相對應的 $\hat{S}_j$，並與 k_j 代入公式(6)，即可擷取出五進位位數 S_j。

$$S_j = (\hat{S}_j - k_j) \bmod 5 \quad \text{.....(6).}$$

表 5 機敏數字擷取

$\hat{\Delta}_i^1$	$\hat{\Delta}_i^2$	$\hat{S}_j$
-1	1	0
0	0	1
0	1	2
1	0	3
1	-1	4

[機敏訊息的擷取與掩護影像的還原之演算法]

輸入：偽裝影像 1、偽裝影像 2、秘密金鑰、位元區塊大小(n)

輸出：機敏訊息、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五進位位數串流($K = k_0k_1k_2\ldots)_5$。

步驟 2:令 $i = 0$；$j = 0$。

步驟 3:從 I_1 與 I_2 中每次各提取出一個像素，p_i^1 與 p_i^2 代入公式(5)中還原原始掩護影像像素值 p_i 。

步驟 4:若 $p_i^1 = p_i^2$ 且等於 0 或 255，則跳到步驟 8，否則計算 $\hat{\Delta}_i^1 = p_i^1 - p_i$ 與 $\hat{\Delta}_i^2 = p_i^2 - p_i$ 。

步驟 5:若 $\hat{\Delta}_i^1 = -1$ 且 $\hat{\Delta}_i^2 = 1$，則 $\hat{S}_j = 0$；

若 $\hat{\Delta}_i^1 = 0$ 且 $\hat{\Delta}_i^2 = 0$，則 $\hat{S}_j = 1$；

若 $\hat{\Delta}_i^1 = 0$ 且 $\hat{\Delta}_i^2 = 1$，則 $\hat{S}_j = 2$；

若 $\hat{\Delta}_i^1 = 1$ 且 $\hat{\Delta}_i^2 = 0$，則 $\hat{S}_j = 3$；

若 $\hat{\Delta}_i^1 = 1$ 且 $\hat{\Delta}_i^2 = -1$，則 $\hat{S}_j = 4$。

步驟 6:將 $\hat{S}_j$ 與 k_j 代入公式(6)，即可獲得機數字 S_j。

步驟 7: $j = j + 1$。

步驟 8: $i = i + 1$，重複步驟 3 ~ 7，直到所有機敏數字全部提取。

步驟 9:將機敏訊息$(S_0S_1S_2\cdots)_5$ 以$\lceil n\log_5 2 \rceil$個五進位位數為一組轉換成 n 個二進位位數，將可還原機敏訊息位元$(b_0b_1b_2\cdots)_2$。

當收到兩張偽裝影像 I_1 = (150, 190, 200, 211, …) 與 I_2 = (152, 188, 201, 213, …)，依序提取偽裝影像來進行機敏訊息的擷取與掩護影像的還原。先使用私密金鑰作為亂數產生器的種子來產生五進位位數串流 K = (3, 1, 2, 4, …)。提取 p_0^1 與 p_0^2 代入公式(5)來還原掩護影像像素值 p_0 = 151。由於 p_0^1 =150 與 p_0^2 =152 不相等，則計算 p_0^1 和 p_0^2 與 p_0 之差值 $\hat{\Delta}_0^1$ = -1 和 $\hat{\Delta}_0^2$ = +1，在表 5 中找出相對應的 $\hat{S}_0$ = 0，並與 k_0 = 3 代入公式(6)，即擷取出機敏訊息 S_0= 2；接著提取 p_1^1 = 190 與 p_1^2 = 188，代入公式(5)，還原掩護影像像素值 p_1 = 189；計算 p_1^1 和 p_1^2 與 p_1 之差值 $\hat{\Delta}_1^1$ = +1 和 $\hat{\Delta}_1^2$ = -1，在表 5 中找出相對應的 $\hat{S}_1$ = 4，並與 k_1 = 1 代入公式(6)，即擷取機敏訊息 S_1= 3，依上述相同步驟提取兩張偽裝影像 I_1 與 I_2 其餘的像素以進行機敏訊息的擷取與掩護影像的還原，即可得到五進位位數(2, 3, 0, 1, …)$_5$，接著將以 4 個為一組轉成 9 個位元，即可獲得機敏訊息 (101000110…)$_2$ 與還原掩護影像像素值為(151, 189, 200, 212, …)。

3.3 位元區塊大小之探討

若直接考慮 2 個像素值來藏匿一個五進位位數，理論上可達 $\frac{\lceil \log_2 5 \rceil}{2}$ =1.1609 bpp 的資訊隱藏量；然而在實作上，為了考量進制轉換的執行效率，由於現有程式語言(如 C++、 Java 等)其基本資料型態(Primitive Data Types)中長整數(Long)長度為 64 位元。因此，我們將評估 2 到 64 位元之間的位元區塊大小與資訊隱藏量之關係。

當位元區塊為 n 時將轉換成$\lceil n\log_5 2 \rceil$個五進位位數，因此，其資訊隱藏量(C)為

$$C = \frac{n}{2 \times x} \quad \text{.....(7).}$$

圖 2 為 2 到 64 位元之間的位元區塊大小與資訊隱藏量之關係。由圖可知，當 n = 58 時，其資訊隱藏量最高，約為 1.16 bpp，且非常接近理論值的資訊隱藏量(1.1609 bpp)。因此，我們認為 n = 58 為較適當的區塊位元大小。

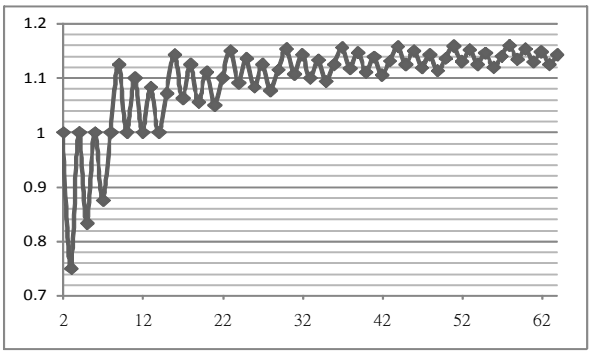

圖 2 資訊隱藏量與區塊位元之關係

4. 實驗結果

為驗證本論文提出方法的效能，我們將以偽裝影像的視覺品質與資訊隱藏量作為評估之基準。視覺品質可以用高峰訊號雜訊比(Peak Signal to Noise Ratio, PSNR)來測量，如公式(8)所示，PSNR 值越大，影像視覺品質相對越好。

$$PSNR = 10 \times \log_{10}\left(\frac{255^2}{MSE}\right) \quad \text{.....(8),}$$

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。

資訊隱藏量可藉由每個像素藏匿的位元數來測量(bit per pixel, bpp)，可由公式(9)來計算。

$$C = \frac{|S|}{(2 \times H \times W)} \quad \text{.....(9).}$$

在此，C 代表每個像素藏匿的位元數，$|S|$代表偽裝影像上嵌入的機敏訊息位元總數。

本實驗環境是在 Microsoft® Windows Server2003 R2 作業系統下，使用 VB.net 程式語言開發環境來實作本論文所提的方法、EMD 雙偽裝影像可逆式隱藏技術以及座標關係雙偽裝影像可逆式隱藏技術，硬體設備為 CoreDuo-2.13 CPU，3GB RAM 的桌上型電腦。在實驗中，機敏訊息是以亂數產生，並使用 Babala、Baboon、Cartoon、Couple、Gold Hill、House、F-14、Lena、Pepper、Toy 等 10 張 256*256 的灰階影像作為掩護影像，如圖 3 所示，來進行效能評估與比較。

圖 3 掩護影像機密影像

4.1 效能評估

表 6 為 EMD 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以及本論文的方法在資訊隱藏量上的比較。由表中可知，我們的方法之資訊隱藏量約為 1.16 bpp 優於其他兩種方法。然而，由於當掩護影像像素中有極端值時，將無法到達最佳資訊隱藏量，如 Cartoon 與 F-14。表 7 探討各張掩護影像在不同方法中極端值像素數的比較。由於我們的方法與座標關係雙偽裝影像可逆式隱藏技術皆僅做±1 之間的修改來藏匿機敏訊息，所以極端值總數是一致的，如表 7 所示皆為相同。然而，EMD 雙偽裝影像可逆式隱藏技術做±2 之間的修改，導致其極端值總數較多。

表 6 資訊隱藏量之比較

方法 / 掩護影像	EMD 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	本論文提出方法
	資訊隱藏量(bpp)	資訊隱藏量(bpp)	資訊隱藏量(bpp)
Babala	0.99	0.75	1.160
Baboon	1	0.75	1.160
Cartoon	0.93	0.67	1.108
Couple	0.99	0.75	1.160
Gold Hill	1	0.75	1.160
House	1	0.75	1.160
F-14	0.99	0.74	1.158
Lena	1	0.75	1.160
Pepper	0.99	0.75	1.160
Toy	1	0.75	1.160
平均	**0.989**	**0.741**	**1.1546**

表 7 溢位像素數之比較

方法 / 掩護影像	EMD 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	本論文提出方法
	極端值像素總數	極端值像素總數	極端值像素總數
Babala	1	0	0
Baboon	0	0	0
Cartoon	4321	4321	4321
Couple	46	0	0
Gold Hill	0	0	0
House	0	0	0
F-14	224	70	70
Lena	0	0	0
Pepper	5	0	0
Toy	0	0	0
平均	**459.7**	**439.1**	**439.1**

由表 8 中可知，本論文提出的方法的平均 PSNR 值約為 50.39 dB，優於 EMD 雙偽裝影像可逆式隱藏技術，但略差於座標關係雙偽裝影像可逆式隱藏技術的 52.45 dB。

表 8 視覺品質(PSNR 值)之比較

掩護影像	EMD 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		本論文提出方法	
	偽裝影像 1	偽裝影像 2	偽裝影像 1	偽裝影像 2	偽裝影像 1	偽裝影像 2
Babala	45.017	45.103	52.410	52.402	50.358	50.359
Baboon	45.118	45.096	52.363	52.403	50.358	50.359
Cartoon	45.914	45.867	52.822	52.809	50.653	50.656
Couple	45.118	45.136	52.403	52.408	50.358	50.359
Gold Hill	45.100	45.111	52.400	52.408	50.358	50.359
House	45.108	45.093	52.408	52.407	50.358	50.359
F-14	45.146	45.127	52.432	52.417	50.363	50.364
Lena	45.130	45.103	52.399	52.408	50.358	50.359
Pepper	45.067	45.156	52.438	52.408	50.358	50.359
Toy	45.163	45.093	52.390	52.508	50.358	50.359
平均	**45.1881**	**45.1885**	**52.4465**	**52.4578**	**50.388**	**50.3892**
總平均	**45.1883**		**52.45215**		**50.3886**	

5. 結論

本論文提出新的雙偽裝影像可逆式隱藏技術，藉由僅對像素值作±1 修改中能成功還原掩護影像像素的五種組合來嵌入一個五進位位數，能有效增加資訊隱藏量與維持高的視覺品質。同時，使用了五進位隨機數字串流對機敏訊息做隨機化處理，避免有心人能由單張偽裝影像中獲取任何有關機敏資訊之有用訊息。經由位元區塊大小與資訊隱藏量之關係分析結果得知當位元區塊大小為 58 時，可直接使用基本資料型態來進行進位轉換，且能得到最接近的理論值之資訊隱藏量。實驗結果證明本論文所提出隱藏技術的資訊隱藏量可達 1.160 bpp 且 PSNR 值能達 50.35 dB。

參考文獻

[1] Chang, C. C., Kieu, The. Duc., Chou, Yung. Chen., "Reversible Data Hiding Scheme Using Two Steganographic Images," ***Proceedings of TENCON 2007***, pp. 1-4, October 2007.

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

[3] Kalker, T. and Willems, F.M.J., "Capacity Bounds and Constructions for Reversible Data-Hiding," ***Proceedings of 14th International Conference on Digital Signal Processing***, Vol. 1, pp. 71-76, 2002.

[4] Lee, C. F., Wang, Kuo. Hui., Chang, Chin.Chen. and Huang, Yu. Lin., "A Reversible Data Hiding Scheme Based on Dual Steganographic Images," ***Proceedings of the Third International Conference on Ubiquitous Information***, pp. 228-237, February 2009.

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

[6] Stallings, W., "Cryptography and Network Security," ***third edition***, Prentice Hall, 2003.

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

[8] Zhicheng, Ni., Shi, Y.Q., Ansari, N., Su, Wei.,"Reversible data hiding," ***International Symposium on Circuits and Systems***, Vol. 2, Issue 25-28, pp. II-912 - II-915, 2003.

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