修正式通式化高容量 EMD 資料隱藏技術

郭文中[1]、王軍証[2]
國立雲林科技大學 [1]資訊工程系、[2]工程科技研究所
[1]simonkuo@yuntech.edu.tw, [2]D10110015@yuntech.edu.tw

摘要

如何能安全有效的傳遞訊息向來就是人們所考慮的一大問題，而其中資料隱藏技術就是一項安全有效的訊息傳遞技術。一般資料隱藏技術就是在不引起他人懷疑的前提下，盡可能地將秘密訊息隱藏於載體之中。而通式化高容量 EMD 資料隱藏技術就是一種強而有力的方法，其擁有良好的偽裝影像品質且能維持 1bpp 以上的高容量。但是在載體本身受限制的同時，就只能被迫放棄部分限制區域，使得此方法仍有改進之處。因此我們提出了修正式通式化高容量 EMD 資料隱藏技術，能夠透過一個簡單的修正步驟，解決部分像素位置無法修改的困擾，讓 EMD 資料隱藏相關技術能夠更有彈性的使用，不受載體本身的限制。

關鍵詞：EMD、資料隱藏、載體影像

壹、前言

自有文字以來，人們傳遞訊息就不再限於面對面的溝通或他人傳話。傳遞訊息可透過文字記載於載體(如書信)上，傳送給接收訊息之人。然而許多訊息並不希望被第三者得知訊息內容，如軍事機密、公文傳遞、商業機密等等。根據使用者的需求而產生了許多的保護措施，如在信封外面加上封條確認沒有被第三者偷看或竄改；將文字訊息轉變為其他人無法解讀的圖形或亂碼；或是將真正欲傳遞的訊息記載於其他看似無關的載體上。

隨著網路通訊技術發展快速進步，人們傳遞訊息的方式也逐漸地改變。使用網際網路傳送資訊漸漸取代了傳統的書信傳遞，已成為現代人傳遞訊息的主流方式。透過網路傳遞訊息雖然方便快速，但也面臨同樣的安全問題。尤其網際網路為公開環境，在傳送資料的過程中是具有高度危險性的。為了保護訊息能安全傳遞，同樣的措施也逐漸轉型運用在網路通訊技術上。最為普遍運用的技術可分為兩大類，一是將訊息內容轉為其他人無法解讀的密碼傳遞給接收者，再由接收者將其解密為原來的訊息，也就是密碼學相關技術；另一類則是將訊息藏匿於其他正常載體(如文字、聲音和影像等)之中，在不引起他人懷疑的情況下安全傳遞至接收者手中，也就是資料隱藏相關技術。

資料隱藏技術為了達到資訊安全的目的，必須具備一些基本準則以避免各式各樣的風險。於此我們歸納出以下幾個主要的條件：

1. 安全性(Security)：安全性是第一必須具備的特性，少了安全性可言的資料隱藏技術再怎麼隱藏也都是枉然。一般安全性雖是以強韌性以及不可察覺性兩項需求為基礎，最終的目還是為了使資料隱藏技術達到安全。在傳輸過程中必須不會引起有心人士察覺；並且防止遭到攔截後被竊取出其中的秘密訊息。
2. 容量(Capacity)：如何維持一定的偽裝影像品質損失下又能夠藏入大量的秘密訊息，是資料隱藏領域裡重要的目標。能藏匿的秘密訊息大小是足以判定該資料隱藏技術優劣的關鍵之一。照理來說，藏匿的秘密訊息愈多犧牲的偽裝影像品質也愈大；不可察覺性同時也愈差。藏匿的秘密訊息少時，雖可降低偽裝影像的品質損失，但載體影像能藏匿的資訊量太少時，在藏匿大量秘密訊息時便需多張的影像。因此兩者間該如何取得最佳的平衡點，藏匿之演算法和欲藏匿之秘密訊息資料量將是非常重要的考量。
3. 強韌性(Robustness)：強韌性代表的就是資料隱藏內可以容忍的破壞程度。高強韌性的偽裝影像在經過有心人士懷疑並攻擊的情況下，仍能夠取出原先所藏匿的訊息。
4. 不可察覺性(Imperceptibility)：該項條件可說是資料隱藏技術中最基本的要求，同時也是最為關鍵的要素。其要求為藏入秘密訊息後，偽裝影像之變化必須是無法從肉眼所輕易觀察出來的。一個不可察覺性高的資料隱藏技術，不易引起有心人士的懷疑而攻擊，當然也提升了偽裝影像之安全性。
5. 明確性(Unambiguousness)：當接收方收到偽裝影像後，所取出的秘密訊息，必須跟發送方所藏匿的秘密訊息相符合。
6. 不可移除性(Nonremovable)：在傳送過程中即使遭受到一些非法攻擊或竄改，尚能保證藏匿在偽裝影像內的秘密訊息不會因此而輕易移除或改變，以確保所藏匿秘密訊息的完整性。

一般而言，資料隱藏技術最重要的就是不可察覺性與容量，在不引起有心人士懷疑的前提下盡可能提高容量[1]，而 EMD 資料隱藏技術[8]就是兩者兼具的方法。EMD 資料隱藏技術經過眾多學者的研究與改良，由 Kuo 等人[5]於 2013 年提出通式化高容量 EMD 資料隱藏技術，維持高容量與良好影像品質。但在很多情況下資料隱藏技術可能會因為載體本身的限制而造成無法藏匿的情況，此時必須額外記錄這些無法藏匿的部分，造成使用者的負擔。例如載體為灰階影像時，像素值範圍為 0~255，當像素修改超過這個範圍，偽裝影像無法正確顯示；或是在某些較特殊的像素位置，像素調整後易引起懷疑，此時就必須將這些超出範圍的像素記錄下來，再利用其他方式重覆藏匿於載體影像中或額外傳遞給接收者。無論是何種方法對於使用者都是一種負擔。因此本論文針對此種情況，提出了修正式通式化高容量 EMD 資料隱藏技術，此方法可以保留某些位置的像素不被修改而無須記錄的資料隱藏技術，在使用上極其便利，有效增加通式化 EMD 資料隱藏技術的彈性。

本論文的架構如下：第貳章探討相關的 EMD 資料隱藏技術；第參章介紹本論文所提出的方法；第肆章為實驗結果與分析；最後第伍章為結論。

貳、文獻探討

資料隱藏技術最基本的安全要求就是偽裝載體要能夠不引起他人懷疑；於此前提下又要能盡可能藏匿大量的秘密訊息。但一般而言，此兩項特性可謂魚與熊掌不可兼得，因為在增加秘密訊息藏量的情況下，通常也不可避免地大幅改變了偽裝載體。

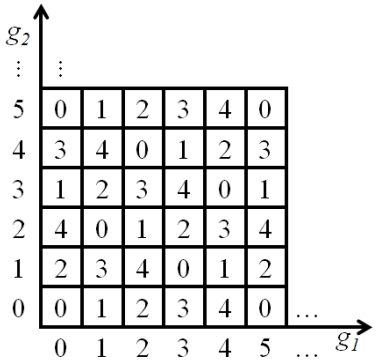
在 2006 年 Zhang 等人[8]就提出了利用模數來修改方向特性的 EMD(Exploiting Modification Direction)資料隱藏技術就成功的達到兩者兼具的目標，引起眾多學者專家的研究，許多相關的 EMD 資料隱藏技術[2][3][4][5][6][7]陸續被提出，針對不同的需求而做了許多改進。接下來我們針對 EMD 相關資料隱藏技術做一個簡單的介紹。

一、EMD 資料隱藏技術[8]

EMD 資料隱藏技術是由 Zhang 等人[8]於 2006 年所提出。Zhang 等人[8]以數位影像為載體，將載體影像進行分割，取 n 個像素為一個群組，代入提取函數式(1)計算提取函數值，藉由提取函數值與秘密訊息的差值對群組像素值進行最小差異的調整。調整後的群組像素值變化極小，因此藏匿後的偽裝影像與原始影像極為相近，滿足其不可察覺性，能有效保證秘密訊息的安全性；此技術同時提供了 1 bpp 以上的藏量(在 n=2 的情況下)。

$$f(g_1, g_2, \cdots, g_n) = \sum_{i=1}^{n} g_i \times i \bmod (2n+1) \qquad (1)$$

其中g_i為第i個群組像素值，n為群組像素數量。由於影像的灰階值是整數值，因此所有像素值可表示為一個在n-維度空間中的向量$[g_1, g_2, \cdots, g_n]$。例如n=2時，向量$[g_1, g_2]$會形成像圖一的Hyper-Cube。在此Hyper-Cube中可以發現，任兩個像素值的提取函數值與其周圍的值皆不相同，這表示當秘密訊息與提取函數值不同時，可在群組函數值的上下左右一格範圍內找到符合秘密訊息的函數值，也就是只需要針對某一個像素值+1或-1即可使得提取函數值滿足秘密訊息。



圖一：n=2 的 Hyper-Cube

EMD 資料隱藏技術雖然滿足了基本需求，但仍有不足之處。其藏量唯有在 n=2 的情況下才有 1 bpp 以上的藏量，隨著 n 值增大，藏量則迅速下降。

二、高容量 EMD 資料隱藏技術[7]

為了改良 EMD 資料隱藏技術，Lee 等人[7]於 2007 年提出了高容量 EMD 資料隱藏技術。Lee 等人[7]修改了提取函數為式(2)，在一像素對中可藏匿 3 位元(模數為 8)的秘密訊息。

$$f_e(g_1, g_2) = \sum_{i=1}^{n}(g_1 \times 1 + g_2 \times 3) \bmod 8 \qquad (2)$$

此方法藉由修改提取函數權重值與增加群組像素變化範圍，讓整體像素藏量一口氣提升至 1.5bpp。其主要概念就是以提取函數值為基準點，將 EMD[7]的 5 種移動方式調整成在該提取函數值周圍相鄰的八格範圍內都能找到滿足不同提取函數值的修改結果。其修改示意圖如圖二所示，可在九宮格範圍內找出 8 種不同的提取函數值，由於右上角與左下角的函數值是相同的，所以只保留右上角的修改方式。可以看出其調整方法由上下左右四個方向擴張至包含斜角的八個方向，其群組像素的調整方式也改變為單一像素最多+1 或-1，雖然像素修改量略高於 EMD 資料隱藏法，但影像品質仍然非常良好。

X-1, Y+1	X, Y+1	X+1, Y+1
X-1, Y	X, Y	X+1, Y
	X, Y-1	X+1, Y-1

圖二：高容量 EMD 的像素修改方式

三、通式化高容量 EMD 資料隱藏技術[5]

Lee 等人[7]的方法雖然提升了藏量，卻限制了像素群組大小，使用上缺乏彈性與安全性，易受有心人士所定像素群組範圍。因此 Kuo 等人[5]於 2013 年提出了通式化高容量 EMD 資料隱藏技術，將高容量 EMD 的像素群組大小再次擴充為可任意選擇的 n 值，兼具前面兩種方法特性。Kuo 等人[5]修改提取函數如式(3)，且提供簡單的藏匿與取出訊息步驟。

$$f_b(g_1, g_2, \cdots, g_n) = \sum_{i=1}^{n} g_i \times (2^i - 1) \bmod 2^{n+1} \qquad (3)$$

其中g_i為第 i 個群組像素值，n 為群組像素數量。由公式(三)可看出藉由修改權重值

與模數，n 個像素可藏匿 n+1 個位元，藏量可維持 1bpp 以上，且不受 n 值改變而藏量大幅下降。其藏匿步驟如下所示：

藏匿步驟：

步驟一: 依序提取n個像素$(g_1, g_2, \cdots, g_n)$代入提取函數f_b計算。

步驟二: 依序提取$n+1$位元秘密訊息並將其轉制為十進制資料s。

步驟三: 計算其差值$d = (s - f_b) \bmod 2^{n+1}$。

步驟四: 若$d = 0$，不作任何調整。

若$d = 2^n$，像素$g_n + 1$且$g_1 + 1$。

若$d < 2^n$，將d轉為二進制$(b_n, b_{n-1}, \cdots, b_0)_2$，並依序搜尋，若$b_i = 0$且$b_{i-1} = 1$，則$g_i + 1$；若$b_i = 1$且$b_{i-1} = 0$，則$g_i - 1$。

若$d > 2^n$，$d = 2^{n+1} - d$，將d轉為二進制$(b_n, b_{n-1}, \cdots, b_0)_2$，並依序搜尋，若$b_i = 0$且$b_{i-1} = 1$，則$g_i - 1$；若$b_i = 1$且$b_{i-1} = 0$，則$g_i + 1$。

取出步驟：

步驟一: 依序提取n個像素$(g_1, g_2, \cdots, g_n)$代入提取函數f_b計算。

步驟二: 將求得的提取函數值轉為二進制即為秘密訊息。

參、修正式通式化高容量 EMD 資料隱藏技術

通式化高容量 EMD 資料隱藏技術兼具高容量與良好的影像品質，適用於一般資料隱藏。但是當載體影像的某些像素位置不適合被修改的時候，就必須找尋其他相同函數值的像素群組。EMD 相關的資料隱藏技術若要維持此種方式就必須不斷嘗試其他可能的像素群組直至找到同樣的函數值為止，過程極為花費時間。

為此我們提出修正式通式化高容量 EMD 資料隱藏技術，針對在像素群組中若有被限制不能修改的像素在藏匿步驟中遭到修改時，會再對像素群組進行修正。其詳細步驟如下所示：

藏匿步驟：

步驟一: 依序提取n個像素$(g_1, g_2, \cdots, g_n)$代入提取函數f_b計算。

步驟二: 依序提取$n+1$位元秘密訊息並將其轉制為十進制資料s。

步驟三: 計算其差值$d = (s - f_b) \bmod 2^{n+1}$。

步驟四: 若$d = 0$，不作任何調整。

若$d = 2^n$，像素$g_n + 1$且$g_1 + 1$。

若$d < 2^n$，將d轉為二進制$(b_n, b_{n-1}, \cdots, b_0)_2$，並依序搜尋，若$b_i = 0$且$b_{i-1} = 1$，則$g_i + 1$；若$b_i = 1$且$b_{i-1} = 0$，則$g_i - 1$。

若$d > 2^n$，$d = 2^{n+1} - d$，將d轉為二進制$(b_n, b_{n-1}, \cdots, b_0)_2$，並依序搜尋，若$b_i = 0$且$b_{i-1} = 1$，則$g_i - 1$；若$b_i = 1$且$b_{i-1} = 0$，則$g_i + 1$。

完成藏匿步驟後，若群組像素中有限制像素且被修改時，則保留限制像素的原始像

素值並依據下列步驟進行修正：

修正步驟：

步驟一: 若限制像素為g_1且藏匿步驟修改g_1+1，則再將像素g_i+1，$g_{i-1}-2$；若限制像素為g_1且藏匿步驟修改g_1-1，則再將像素g_i-1，$g_{i-1}+2$，其中$1<i\leqq n$。

步驟二: 若限制像素為g_2且藏匿步驟修改g_2+1，則再將像素g_1+1，g_n-2；若限制像素為g_2且藏匿步驟修改g_2+1，則再將像素g_1+1，g_n-2。

步驟三: 若限制像素為g_i，且藏匿步驟修改g_i+1，則再將像素g_1+1，$g_{i-1}+2$；若限制像素為g_i，且藏匿步驟修改g_i-1，則再將像素g_1-1，$g_{i-1}-2$；其中$i>2$。

取出步驟：

步驟一: 依序提取n個像素$(g_1, g_2, \cdots, g_n)$代入提取函數f_b計算。

步驟二: 將求得的提取函數值轉為二進制即為秘密訊息。

在這裡我們舉個例子依據上述的步驟來說明，若n=4，載體像素群組為(g_1, g_2, g_3, g_4)=(10, 20, 30, 40)，秘密訊息s=11000_2。假設g_3為不可修改的像素，則其藏匿過程為：

藏匿步驟：

步驟一: 將載體像素群組帶入提取函數f_b計算，得到$f_b(10, 20, 30, 40)=16$。

步驟二: 將秘密訊息轉為s十進制，s=11000_2=20。

步驟三: 計算其差值$d=(20-16)\text{mod}32$=4。

步驟四: $d=4<2^4$，將d轉為二進制$(00100)_2$，並依序搜尋，其中$b_3=0$且$b_2=1$，所以$g_3+1=31$；$b_2=1$且$b_1=0$，則$g_2-1=19$。

當完成藏匿過程後，偽裝像素群組為(10, 19, 31, 40)，我們發現不可修改的像素g_3被修改為31，因此我們保留$g_3=30$並對偽裝像素群組再進行修正，其修正過程如下：

修正步驟：因為不可修改像素為g_3，則採取步驟三進行修正。

步驟三: 因為藏匿步驟修改g_3+1，因此修正方式為$g_1+1=11$，$g_2+2=21$。

最後得到的偽裝像素群組為(11, 21, 30, 40)，並將其傳送給接收者，當接收者收到此偽裝像素群組時，可依照取出步驟得到偽裝像素，其取出過程如下：

取出步驟：

步驟一: 將偽裝像素帶入提取函數f_b計算，得到$f_b(11, 21, 30, 40)=20$。

步驟二: 將提取函數f_b轉為二進制，f_b=20=11000_2即為秘密訊息。

當群組像素內中有某個位置的像素禁止被修改或是修改後會造成溢位時，可透過簡單的修正步驟進行調整，無需棄用此群組或額外記錄像素差異資訊。對使用者而言只需依據上述步驟完成藏匿或取出，無額外記錄資訊需傳送，更可保證其安全性與使用彈性。

肆、實驗結果與分析

我們選擇了八張資料隱藏技術常使用的測試影像作為載體影像，如圖三分別為 Airplane、Baboon、Boat、Elaine、Gold Hill、Lena、Pepper 以及 Tiffany。影像皆為 512×512 的 8 位元灰階影像。

圖三：載體影像

在實驗過程中我們在每一分割的像素群組中隨機選擇一個位置作為禁止修改像素，並與通式化高容量 EMD 資料隱藏技術做比較。圖四為通式化高容量 EMD 資料隱藏技術的偽裝影像，圖五為修正式通式化高容量 EMD 資料隱藏技術的偽裝影像。

51.00dB　50.99dB　51.00dB　51.01dB

50.98dB　50.99dB　51.00dB　51.00dB

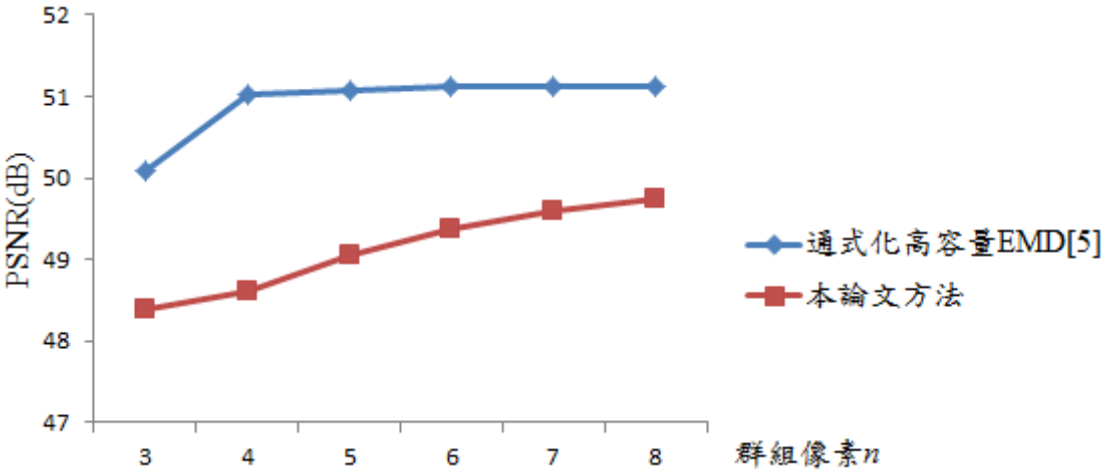
圖四：通式化高容量 EMD 資料隱藏偽裝影像與 PSNR 值(n=4)

48.62dB 48.63dB 48.62dB 48.61dB

48.62dB 48.62dB 48.63dB 48.61dB

圖五：本論文方法的偽裝影像與 PSNR 值(n=4)

圖六為在不同群組大小(n=3~8)的情況下的偽裝影像品質，可以看出本論文方法 PSNR 值雖然會略微低一些，但仍可維持在 48dB 以上，偽裝影像仍有良好的不可察覺性。



圖六：不同 n 值的 PSNR 比較

本論文所提出的方法藏量皆與通式化高容量 EMD 資料隱藏技術相同，而在載體影像有所限制之時(如可能造成溢位或容易引起引起懷疑的像素位置)，仍能透過簡單的修正步驟進行藏匿，在使用上極為方便有效，使得 EMD 資料隱藏的相關技術能夠更加有彈性。

伍、結論

大部分的資料隱藏相關技術雖然都能滿足其基本特性，通式化高容量 EMD 資料隱藏技術更是兼具容量與不可察覺性地優秀資料隱藏技術，但這類型的方法往往忽略某些特殊情況，使得真正使用上受到限制，無法完全通用。因此本論文提出修正式通式化高容量 EMD 資料隱藏技術，當載體影像某些像素位置受限制時，只需要透過簡單的步驟將偽裝影像進行修正即可，不需耗費時間盲目計算另一個相同函數值的像素群組或是捨棄不用。從實驗結果可以發現，其偽裝影像品質仍極為良好(PSNR＞48dB 以上)。我們提出的方法能讓 EMD 相關的資料隱藏技術在使用上更加有彈性，即使因為載體本身的限制仍能有效利用。

誌謝:感謝科技部計畫編號 MOST 103-2221-E-224-046 經費補助。

參考文獻

[1] A.A. Abdulla, S.A. Jassimand and H. Sellahewa, "Efficient high-capacity steganography technique," Proc. SPIE8755, *Mobile Multimedia/Image Processing, Security, and Applications* 2013.

[2] W.C. Kuo, H.C. Hou and C.T. Chuang, "Data hiding scheme based on binary coefficient EMD," *NCS2013*, 2013.

[3] W.C. Kuo, J.C. Cheng and C.C. Wang, "Data hiding method with high embedding capacity character," *The 22 IPPR Conference on Computer Vision, Graphics, and Image Processing*, Poster Session D1-7, Aug. 2009.

[4] W.C. Kuo, J.C. Cheng and C.C. Wang, "More efficient steganoraphic embedding and capacity-improvement by generalized exploiting modification direction method," *Fourth International Conference on Innovative Computing, Information and Control*, PID966507, Dec. 2009.

[5] W.C. Kuo and C.C. Wang, "Data hiding based on generalised exploiting modification direction method," *Imaging Science Journal*, Vol.61, No.6, pp.484-490, 2013.

[6] W.C. Kuo, L.C. Wuu, C.N. Shyi and S.H. Kuo, "A data hiding scheme with high embedding capacity based on general improving exploiting modification direction method," *The Ninth International Conference on Hybrid Intelligent Systems (HIS2009)*, pp.69-73, Aug. 2009.

[7] F.Lee, Y.R. Wang andC.C. Chang, "Asteganographicmethod with high embedding capacity by improving exploiting modification direction,"*Proceedings of the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP07)*, 26-28 Nov.2007, pp.497-500, 2007.

[8] X. Zhang and S. Wang,"Efficient steganographic embedding by exploiting modification direction," *IEEE Communications Letters*, Vol.10, No.11, pp.1-3, 2006.