植基於通式化之高容量 EMD 資料隱藏技術

郭紹宏
南台科技大學資訊工程研究所
m95g0230@webmail.stut.edu

席家年
南台科技大學資訊工程系
shyi@mail.stut.edu.tw

郭文中
虎尾科技大學資訊工程系
simonkuo@nfu.edu.tw

摘要

最近，Chang 等人提出高容量 EMD 資料隱藏技術來改善 Zhang 等人所提的利用方向修改特性的 EMD 資料隱藏技術。但 Chang 等人所提之隱藏技術權重值設定與 EMD 技術所採用的方式皆為固定形式。因此只要公開其藏匿技術將會使得機密資料被洩露出去。在本篇論文中，我們設計出一個權重值變化特性的通式化之高容量 EMD 且為可公開的資料隱藏技術；來改進此安全性方面的問題，也就是說，就算公開本文所提之藏匿技術，機密資料被洩露的可能性也降至很低。

關鍵詞：資料隱藏、安全性、通式化。

Abstract

Recently, Chang *et al.* proposed a high capacity technique of data hiding scheme in order to improve the capacity of EMD proposed by Zhang *et al.*. However, this new technology is using fixed equation to calculate and to store data just as EMD dose; as a result, once the encoding formula is published, the data hiding will no longer be safe. Therefore, a generally equation of high embedding capacity by exploiting modification direction was designed to use different weighting-evaluations instead of fixed weighting-calculation in this paper. Also, even if the encoding technology is public, the chance of leaking personal information is rare; it decreases the chance of exposing secret codes that is hidden behind cover image, and publishing the encryption technique will not be a threat anymore.

Keywords: Data-Hiding, Security, Generally

1. 前言

隨著網路的普及，數位化的 e 世代隨之降臨。因此許多的訊息傳遞只需要透過網際網路即可輕鬆完成。不過，便利的網際網路卻暗藏著許多的危險性，像是許多私密的資料在網路上傳遞的過程中；隨時隨地都有可能被非法人士攔截、竄改、冒用等等的不法問題發生。有鑑於此，我們更需要做好防範資料外洩的各種可能性。其中最廣為人知的方法就是利用資料隱藏的技術，也就是將秘密訊息透過運算式藏匿於載體影像(Cover image)中形成所謂的偽裝影像(Stego image)，並且在不被第三者察覺之情況下，將偽裝影像安全地傳遞至接收者手上。利用這樣的資料隱藏技術早在二千多年前的古希臘時代就有案例可循。再把時間拉回 2006 年，當時的熱門電影達文西密碼中也有許多利用資料隱藏的技術。再舉個簡單例子來說，例如 2007 年播映的炙手可熱影集越獄風雲（Prison Break），劇中人物將整個監獄結構圖與逃亡計畫採用刺青的方式刺在身上，乍看之下只是個稀鬆平常的天使與惡魔刺青，但卻隱藏著許多秘密資訊。這就是一個普遍常用的資料隱藏方式；也算一種具備較佳高安全性的資料隱藏方法。

然而一個完善的資料隱藏技術不單方面只考慮到安全性或者藏入容量如此而已。而是必須包含以下條件：安全性（Security）、不可察覺性（Imperceptibility）、強韌性（Robustness）及容量（Capacity）；本研究針對的方向就是藏匿資料的安全性和能夠藏入的訊息容量。尤其安全性的部分更是著重的焦點。Cayer 等人就曾經提出一個浮水印安全性的理論與實踐[1]，將其論點套用於資料隱藏來看也是相當重要的，畢竟公開的技術上要有相當的安全性；以避免第三者輕易的破解取得秘密資訊。

現階段的資料隱藏研究中大多著墨於灰階影像圖的藏匿。在灰階圖中每一像素值的範圍在 0 至 255 間；故能用 8 位元的二進制來表示。現今常用的資料隱藏技術有許多都是利用 LSB（Least Significant Bits）位置來隱藏秘密資訊，也就是說先將秘密訊息轉換成位元串列（Bit Stream）後，再將它藏入於載體影像的最後一個位元中[3, 7, 8]。儘管 LSBs 法將秘密訊息藏入像素的方法雖然可以降低藏匿後偽裝影像的失真，不過其造成的失真度仍然可以輕易的被肉眼或是程式察覺。

最近，Zhang 等人提出了 EMD（Exploiting

Modification Direction)[9]方法來提升隱藏秘密資訊的容量以及藏匿後偽裝影像具有相當高的 PSNR 值。事實上，EMD 法中只能將兩像素值中的其中一個像素作加減一或是不改變共三種變化。若以空間的角度來看，即是兩像素只能作上下左右的移動或是不動等五種變化情況。緊接著，Chang 等人[4]就針對此缺失加以改進；並且提出了一次抓取兩個像素分別給予固定的權重值的方法。此方式能對空間做出更多位置改變，能達到以像素點為中心的八個方向作變化；其中一種變化重複，故比起 Zhang 等人的方法多出 3 種方向。因此 Chang 等人能夠將藏匿的秘密資訊容量提升約略 1.5 倍。可是 Chang 與 Zhang 等人的方法都採用固定的權重值形式，所以他們所提出的隱藏技術一旦被公開出來就會輕易的遭到破解；也因此有了安全性方面改進的考量出現。在本論文中就針對此缺點設計了一個多變化權重值特性的通式化之方程式，共有八種不同配對的權重值。再加上隨機種子（Seed）配對選擇方式，就算公開本文所提的藏匿技術的情形，也會使得機密資料被洩露的可能性降至很低。

本文的架構如下。第二章節首先將 Zhang 等人與 Chang 等人的技術作詳細的介紹，第三章節介紹本研究所提出的方法，包括改進部分以及藏匿時的詳細過程，第四章節則是本文的實驗結果並與 Chang 等人的作比較。最後本文的結論則是在第五章節呈現。

2. EMD隱藏技術起源與演進

本章節主軸是放在Zhang等人[9]最先提出的 EMD 資料隱藏法以及 Chang 等人[4]所提出的高容量 EMD 資料隱藏法之介紹。

2.1 EMD 隱藏法

EMD 法最早是由 Zhang 等人[9]於 2006 年所提出。這是利用修改方向的新穎資料藏匿技術。依據 EMD 設定的藏匿法，是將一個二元的位元串列秘密訊息藏入 n 個像素為一組的載體像素群的(2n+1)-ary 系統中。EMD 藏匿過程中；首先將所有載體影像之像素值表示成 $g_1, g_2, \ldots g_n$ 的形式，而 n 就是像素群中的像素個數。在執行藏匿動作前要先將像素值轉換成(2n+1)-ary 型態，例如:一組原先為(1111 1011 1001 0111)$_2$ 的二元序列轉換成(30 21 14 12)$_5$ 5-ary 形態。再針對上述轉換形式與所有像素群定義了一個提取函數 f 如下：

$$f(g_1, g_2, \cdots g_n) = \left[\sum_{i=1}^{n}(g_i \cdot i)\right] \bmod(2n+1) \quad (1)$$

其中 g_i 為像素值，n 為像素個數。

但是 EMD 藏匿法存在著；只有於 5-ary（$2n+1, n=2$）情況下才達到最佳的隱藏位元率的缺點。當 n 遞增時，也就是越多像素分成一組時，其隱藏位元率將會逐次遞減。例如：當 n = 2 時，為兩個像素裡其中一個像素加減一或者兩個像素都不變動；然而在 n 值增加的狀況下能夠藏入的訊息自然減少，以至於隱藏位元率下降。不過 PSNR 值方面，其高於 50 dB 的 PSNR 值以及隱藏的高容量還是有著顯著貢獻。

在 EMD 隱藏資料法中也特別針對了在 n = 2 時 5-ary 的情況而製訂出一張 2D 的 Hyper-cubes 表，如下圖 1.所示。由圖 1.中我們可以更明確的了解到 EMD 提取函數的物理意義，即是在每一個 0 至 4 值的上下左右四個方向，均可找到與之相異的 4 個值。舉例來說，以（g_1, g_2）=（2, 4）而藏匿值為 3 來說，(2, 4）的位置是 0；透過圖 1.可在其周遭找到下方位置（2, 3）處為 3 來滿足要藏匿的值 3。此時，則將原先的（g_1, g_2）=（2, 4）改變成（g'_1, g'_2）=（2, 3），即可達到藏匿的動作。

2.2 高容量 EMD 隱藏法

最近，Chang 等人提出的高容量資料隱藏法[4]主要是改善 Zhang 等人[9]的 EMD 隱藏容量。也就是說，Chang 等人針對原 EMD 方法的缺點，提出了 8-ary 的資料隱藏方法。根據此法一次可藏入 3 位元資訊（$000_2 \sim 111_2$）比起原 EMD 一次可藏 2 或 3（$00_2 \sim 100_2$）位元，相對能提升隱藏的資料量。

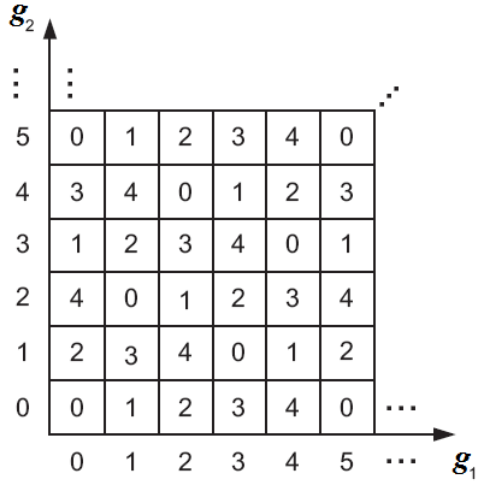

圖 1. 5-ary 之 2D Hyper-cubes 表

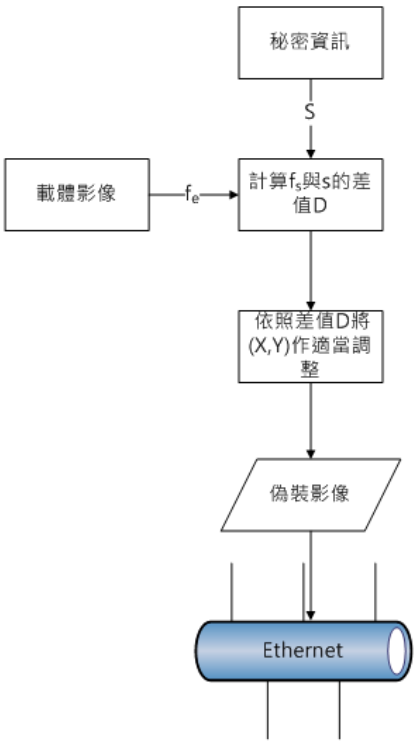

圖 2. Chang 等人之藏匿過程流程圖

Chang 等人藏匿時也是先將秘密訊息轉換為二位元形式後再將二元序列轉換成 8-ary；即原先一般資料隱藏技術一次藏匿 1 位元資料變成為一次藏匿 3 位元。載體影像部分皆為灰階圖（grayscale），像素值分群方面也是一次擷取兩個相鄰像素值；定義為 X 與 Y 來做為分群依據。提取函數 f_e 部分，其權重值定義為第一個像素值乘上 1 及第二個像素值乘上 3；最後的加總值再模 8 取其餘數。當作要隱藏秘密資料的參考標點。這與原先的 EMD 提取函數並不相同。Chang 等人所提出的提取函數 f_e 與藏匿流程如圖 2.所示：

$$f_e(X,Y)=(X\times 1+Y\times 3)\bmod 8 \qquad (2)$$

2.2.1 藏匿秘密資訊流程

步驟 1：將所有像素作成對分配。
步驟 2：將每對（X, Y）均帶入提取函數 f_e。
步驟 3：依照所有的秘密資訊作以下調整，
（3-1）當 $s=f_e(X,Y)$，則 $X=X, Y=Y$。
（3-2）當 $s=f_e(X+1,Y)$，則 $X=X+1$。
（3-3）當 $s=f_e(X-1,Y)$，則 $X=X-1$。
（3-4）當 $s=f_e(X,Y+1)$，則 $Y=Y+1$。
（3-5）當 $s=f_e(X,Y-1)$，則 $Y=Y-1$。
（3-6）當 $s=f_e(X+1,Y+1)$，則 $X=X+1, Y=Y+1$。
（3-7）當 $s=f_e(X+1,Y-1)$，則 $X=X+1, Y=Y-1$。

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 3.Chang 等人藏匿修改法

（3-8）當 $s=f_e(X-1,Y+1)$，則 $X=X-1, Y=Y+1$。

2.2.2 取出秘密資訊值 s 時：

步驟 1：將所有偽裝過的像素值作成對分配。
步驟 2：將每對偽裝過的像素（X', Y'）帶入提取函數 f_e，可得到 F'函數：

$$F'=f_e(X',Y')=(X'\times 1+Y'\times 3)\bmod 8 \qquad (3)$$

步驟 3：再將所有的 F’值轉換為原來 2 位元的秘密訊息。

3.通式化高容量EMD隱藏技術

於第二章節的詳細介紹中，都能了解到無論是最原始 EMD[9]法或者是高容量 EMD 法[4]，在作法上都是運用權重值的變化並配合模數運算；來滿足任意一個點皆能在其周圍找到所適當的位置。此二法的藏匿容量上都有顯著的貢獻。但是，卻也因為這樣的方法皆存在著其隱藏方式固定且其模式不能公開等兩個安全上的問題，接下來在本章節中也將針對這兩項安全性的問題提出探討與改進方式。

3.1 Chang 等人與 Zhang 等人方法的缺點

Zhang 等人[9]提出有別於以往的 EMD 資料隱藏方法，此法能藏匿的秘密訊息比一般 LSB[3, 7, 8]能藏入的容量還多。之後，Chang 等人更能再進一步從 EMD 中再找出更高容量的資料隱藏法[4]，但是其提取函數之權重值與 Zhang 所提出的 EMD 模式類似，皆為固定或有規則的形式。因此我們認為這樣的既定形式非常容易遭到有心人士破解並且無法公開其藏匿的提取函數。畢竟公開方法的同時，安全的大門也隨之敞開，如此一來即使藏匿的資訊再龐大再多麼的不易查覺也是有安全性方面的隱憂存在。故本文將針對其權重值模式固定的部分加以改善，並且有效的提升安全性。

3.2 通式化之高容量 EMD 隱藏技術

縱觀 Zhang 等人[9]或是 Chang 等人[4]所提出的 EMD 或是高容量 EMD 法，於提取函數之權重值的設定都是影響整個隱藏技術的關鍵所在。在 Zhang 等人 EMD 方法中，以取兩個像素值之權重值 1 及 2 為例。其主要目的可於圖 1.中清楚了解到。即要達到任意一個點都能夠在其上下左右位置處找到對應於藏匿值的位置。而 Chang 等人的方式則是更制式化的固定權重與特定模數來達到更多藏匿方向。雖然此二者的藏匿方法均能夠大幅提升藏匿資料容量。不過，卻都忽略了安全性方面的問題，畢竟這樣固定形式之權重值提取函數都是無法公開的。

因此本研究將提出一個針對安全性方面來改善的通式化之高容量 EMD 隱藏技術。提取函數方面大致上是與 Chang 等人所提出的高容量隱藏技術雷同。藏匿方式是將每對（X,Y）代入所定義的提取函數 f_s。提取函數 f_s 與藏匿流程圖如下式所示：

$$f_s(X,Y)=(X\times a+Y\times b)\bmod 8 \qquad (4)$$

其中係數 a 與 b 的關係為 $a,b\in\{1,3,5,7\}$。當 a 與 b 在選擇時尚需滿足 $a\neq b$ 且 $(a+b)\bmod 8\neq 0$ 的條件。如此，即可找出有八種不同權重值的配對組合滿足上述條件，分別是：(1, 3)、(1, 5)、(7, 3)、(7, 5)、(3, 1)、(5, 1)、(3, 7)、(5, 7)。之後再配合利用亂數產生器所隨機產生出的種子（Seed）。每一個不同的 Seed（0~7 共 8 個）傳送前會與所有的權重值依序作出對應並且和接受端協調好。例如：0 對應（1, 3），1 對應（1, 5）等等…以此類推。所以在藏匿時即可隨機的配合種子變化挑選出不同權重值。

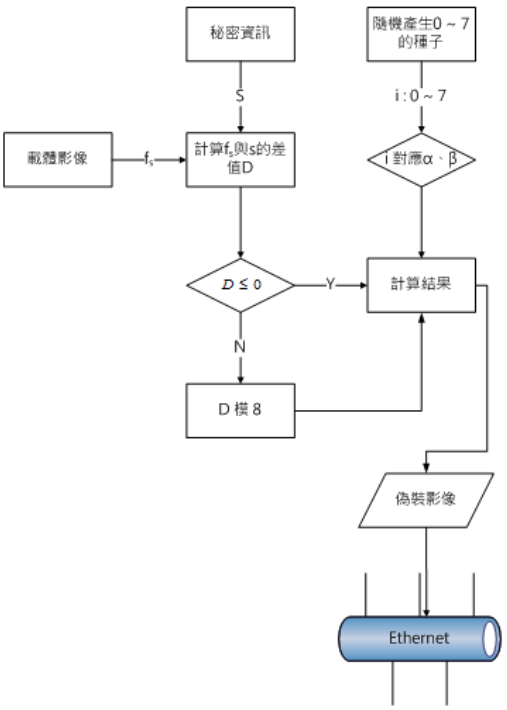

圖 4. 藏匿流程圖

接下來將定義整個通式化之 EMD 資料隱藏技術的核心部分，也就是藏匿時像素值；該如何作出對應調整來達到藏匿效果。原先 Chang 等人高容量 EMD 藏匿時的修改方法如圖 3.所示。而本研究將其固定的形式改變成對應我們所提出通式化之 EMD 資料隱藏技術，改變後的藏匿修改方式如圖 5.所示。其中的 α 與 β 關係如表 1.所示。

X-α, Y+β	X, Y+β	X+α, Y+β
X-α, Y	X, Y	X+α, Y
	X, Y-β	X+α, Y-β

圖 5. 通式化 EMD 藏匿修改法

表 1. α、β 關係表

Seed	0	1	2	3
(a,b)	(1,3)	(1,5)	(7,3)	(7,5)
α	1	1	-1	-1
β	1	-1	1	-1
Seed	4	5	6	7
(a,b)	(3,1)	(5,1)	(3,7)	(5,7)
α	1	-1	1	-1
β	1	1	-1	-1

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 6. α = -1、β = 1 時 *X*, *Y* 之變化

舉例來說：首先我們取得一對像素值(*X,Y*) =（190,143），Seed = 2；對應的權重值為（7,3）而 α 與 β 分別為-1、1，秘密資訊為 s = 6。接著將（190,143）代入提取函數 f_s 後可得 f_s = 7。而藏匿秘密資訊 s 與 f_s 差值為 D = 6 – 7 = -1 ，D 為負值故模 8 後等於 7。此時再將 α、β 代入圖 5.的通式中可得圖 6.的結果，緊接著再透過圖 6.中的各個修改過的 *X*、*Y* 值帶入提取函數 f_s 即可得到當（*X+1,Y*）時 f_s = s = 6。表示最後的結果是將（190,143）改變成（191,143）。

4. 實驗結果

實驗結果方面，共挑選了影像處理常用的四張圖來測試本論文所提出的方法，如圖 7.所示分別為 Lena、Pepper、Baboon、Boat，而藏匿後的偽裝影像結果如圖 8.所示。圖片的規格方面，均採用 *512x512* 的 8 位元灰階影像為基準。經過模擬實驗證實了我們說提出的方法確實能夠提高安全性，並且無需像先前所提出的查詢法額外儲存許多表格[6]。最重要的是，還保持了 Chang 等人的高容量特性。同時我們也做了 PSNR 值的分析比較，我們的 PSNR 值與 Chang 等人的 PSNR 值相似，如表 2.所示。這也同時證明了本研究的實驗結果是正確且維持高容量特性的隱藏方法。在安全性的方面，也因為每一張影像在藏匿的過程中；提取函數至多變換了 131,072（*512x512*÷2）次權重值，故相對的提高了安全性。也因為這樣多變化的權重值特性，使得 PSNR 值的部分甚至有時會有提升的情況。因為，當藏匿值 s 與提取函數計算出的 f_s 吻合度越高時自然改變的像素值越少。故此有助於提升 PSNR 值。這也是本研究除了提高安全性外的另一項重要貢獻。

5. 結論

本研究成功的實現一個安全性高與藏匿容量高的通式化之 EMD 資料隱藏技術。並且擺脫之前所提出的改良式 EMD 資料隱藏技術[6]尚需儲存大量表格的缺失。並且在經過實驗證明下，所提出的隨機產生種子再搭配不同權重值配對；能夠有效的提高提取函數之安全性。並且維持了；所有 PSNR 值均達到 50dB 以上的優點，甚至時有 PSNR 值略高於 Chang 等人方法的情況發生；而這就是隨機配對的效果。當不同權重值所得到的 f_s 與藏匿資訊相同的次數越高自然 PSNR 值也越高。但也因為隨機選取的關係整體上的 PSNR 值會有略低的狀況發生。不過整體上來說，本研究還是一個集安全性高及高藏匿容量於一身的資料隱藏技術。

6. 誌謝

本研究承蒙國科會計畫補助，編號(NSC 97-2221-E-150-038)。

表 7. 本研究方法與 Chang 之 PSNR 值比較

PSNR（dB）	Lena	Pepper	Baboon	Boat
本方法	50.174	50.163	50.180	50.172
Chang[3]	50.173	50.168	50.180	50.176

圖 8. 載體影像

圖 9. 偽裝影像

參考文獻

[1] F. Cayre, C. Fontaine, T. Furon, ”Watermarking Security: Theory and Practice,” IEEE Trans. on Signal Processing Vol.53, No.10, pp.3976- 3987, Oct. 2005.

[2] C. C. Chang and W. C. Wu, “A Novel Data Hiding Scheme for Keeping High Stego-Image Quality,” Proceedings of the 12th International Conference on MultiMedia Modelling, Bijing, China, January 2006, pp. 225-232.

[3] A. Ker, “Steganalysis of LSB Matching in Grayscale Images,” IEEE Signal Processing Letters, vol. 12, no. 6, June 2005, pp.441-444.

[4] C. F. Lee, Y. R. Wang, and C. C. Chang, “A Steganographic Method with High Embedding Capacity by Improving Exploiting Modification Direction,” IIHMSP 2007. Third International Conference on Volume 1, Issue, 26-28 Nov. 2007 Page(s):497 – 500.

[5] J. Mielikainen, “LSB Matching Revisited, ” IEEE Signal Processing Letters, vol. 13 no. 5, May 2006, pp. 285-287.

[6] C. N. Shyi, S. H. Kuo, W. C. Kuo “Data Hiding Method Based on High Embedding Capacity by Improving Exploiting Modification Direction, ” 2008 Conference on Global Logistic Management and Industry Practice Research. 25, December 2008, pp. 455-462.

[7] R. Z. Wang, C. F. Lin, and J. C. Lin, “Image Hiding by Optimal LSB Substitution and Genetic Algorithm, ”Pattern Recognition, vol. 34, no. 3, 2001, pp. 671-683.

[8] H. C. Wu, N. I. Wu, C. S. Tsai, and M.S. Hwang, “Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods, ”IEE Proceedings-Vision, Image and Signal Processing, vol.152, no. 5, October 2005, pp.611-615.

[9] X. Zhang and S. Wang, “Efficient Steganographic Embedding by Exploiting Modification Direction,” IEEE Communications Letters, vol. 10, no. 11, November 2006, pp. 1-3.