

立體魔術方塊在資訊隱藏的應用

冷輝世^{1,2}

¹國立彰化師範大學數學系
lenghs@cc.ncue.edu.tw

曾顯文²

²朝陽科技大學資訊管理系
hwtseng@cyut.edu.tw

摘要

立體魔術方塊是指「將三維空間中立方體的邊長等分割分為相同長度所構成的分割方塊的組合」。我們將灰階影像中相鄰的三像素所構成的三元數對 (x_1, x_2, x_3) 視為立體魔術方塊在三維空間中 X, Y, Z 三個座標軸上的邊，則我們可以模仿 EMD(Exploiting Modification Direction)的概念，定義擷取函數並將每一像素加減 k 的關係與立體魔術方塊所構成的分割方塊做一對應。換句話說，我們可以將一個 $(2k+1)^3$ 進制的機密訊息藏入 (x_1, x_2, x_3) 這個三元數對且其中每一個像素至多加減 k 。

以上機密訊息的藏入過程中，每一像素至多加減 k 的對應關係是唯一的，所以機密訊息的取出可以保證其正確性。而且，此對應關係的存在也代表了機密訊息藏入量與藏入後的影像品質的最佳化。除此之外，我們可以將三元數對擴展至 n 元數對，亦保有以上的好性質。

關鍵詞：立體魔術方塊，EMD。

Abstract

In this study, a magic cube is a 3-dimensional cube, and each side segment into equal length partitions. Suppose (x_1, x_2, x_3) is a triple neighboring pixel group in a grayscale image, and each pixel corresponding to the values of X, Y and Z axis in 3-dimensional space. We define the extraction function as the EMD(Exploiting Modification Direction) method does. Therefore, we can define an extraction function between the values of X, Y and Z of 3-dimensional space of the magic cube and the variations of the pixels in this triple group. In other word, we can embed one n^3 -ary notation secret digit into this triple group, and for each pixel in this triple group the value at most increases or decreases by k .

As we mention above, this mapping relationship of the value at most increases or

decreases by k in the embedding procedure is one-to-one. Therefore, we can extract the secret digits correctly. In addition, this mapping relationship also shows a optimize results for the payload and the quality of stego image. Besides, we can extend triple group to n -tuple group, it also owns this good properties.

Keywords: magic cube, EMD.

1. 前言

由於網際網路的快速發展，大量的資訊在網際網路上流通。近年來，由於對隱私權的重視，如何保護這些資訊不被有心人士所竄改或攔截已成為重要的課題。常見的解決方法有兩種：第一種方式是加密與解密，由傳送方與接收方協定加密與解密的方式，所以即使有心人士攔截亦無法得知資訊的內容。另一種方式稱為資訊隱藏，由於第一種方式可能引起有心人士的懷疑以至於竄改或破壞，所以藉由將欲傳遞的資訊隱藏於常見的一般多媒體媒介中(例如：文字、影像、聲音、視訊等)，避免引起有心人士的注意。由於影像廣泛的被使用於網際網路以及其容量大的特性，使其成為理想的載體，傳送方將資訊以特定方式藏入影像後成為偽裝影像再傳遞給接收方，並以協定的方式擷取其中的內容還原資訊。

資訊隱藏依其特性又分為可逆與不可逆兩種方式。可逆資訊隱藏是指接收方在擷取出資訊後載體可以還原成原始影像，沒有任何改變。不可逆資訊隱藏則是指接收方擷取出資訊後載體無法還原成原始影像，必有部份遭到破壞。由於特定資訊的藏入會造成載體部份內容被破壞，所以要有一定的標準評估。一般常見的評量標準包括藏入量與影像品質兩方面：藏入量愈大愈好，可是相對的造成的影像失真也愈大。單位像素的藏入量一般是以 bpp 為單位。

EMD(Exploiting Modification Direction)[6] 是著名的不可逆資訊隱藏方法。它將載體分割成每 n 個像素為一組，並定義擷取函數 f ，使

這其中的每一個像素唯一對應於 n 進制的每一個數字。由於對每一組 n 個像素只改變其中一個像素值加減 1，所以偽裝影像與做為載體的原始影像差異性非常小，故有良好的 PSNR 值。可是 EMD 也有缺點，其藏入量可預估為 $(\log_2(2n+1))/n$ bpp，而且隨著 n 值的變大，其單位像素藏入量卻會顯著的減少，當 $n=2$ 時約為 1.1610 bpp，當 $n=3$ 時則為 0.9358 bpp，當 $n=4$ 時則為 0.7925 bpp，當 $n=5$ 時約為 0.6919bpp。依此類推，隨著 n 值的變大，其單位像素藏入量卻會顯著的減少。

如何改善這個缺點，有許多相關的研究。以下我們將著重在其改進的方式以及單位像素藏入量的提昇。

2. 文獻探討

首先，我們介紹 EMD 的嵌入與取出程序。

將載體影像分割成每 n 個像素為一組，並定義擷取函數 f ：

$$f(x_1, x_2, \dots, x_n) = \left(\sum_{i=1}^n (x_i \cdot i) \right) \bmod (2n+1)$$

其嵌入方式如下：假設 $(2n+1)$ 進制的機密訊息為 d ，若 $d=f$ ，則所有像素值不須改變，否則令 $s=(d-f) \bmod (2n+1)$ ，若 $s \leq n$ 則 $x'_s \leftarrow x_s + 1$ ，若 $s > n$ ，則 $x'_{2n+1-s} \leftarrow x_{2n+1-s} - 1$ 。機密訊息的取出只須將偽裝影像的像素組 $(x'_1, x'_2, \dots, x'_n)$ 代入擷取函數，得到的值即為機密訊息。

由於 EMD 在 $n=2$ 時有最大的單位像素藏入量，所以部份學者針對 EMD 做改進時都是以兩個像素為基礎，針對擷取函數的定義做修改以增加其單位像素藏入量。

例如，學者 Lee C.F、Wang Y.R.和 Chang C.C.[5]提出

$$f(x_1, x_2) = (x_1 \times 1 + x_2 \times 3) \bmod 8$$

提昇其單位像素載入量約 1.5 倍。

Chen K.N、Chang C.C.和 Lin H.C.[2]提出

$$f(x_1, x_2) = (x_1 \times n^0 + x_2 \times n^1) \bmod n^2$$

雖然對單位像素載入量沒有明顯的改變但提出解決一般常忽略的溢位問題的方法。

Chao R.M、Wu H.C、Lee C.C.和 Chu Y.P.[1]提出

$$f(x_1, x_2) = (x_1 \times 1 + x_2 \times 2) \bmod 5$$

利用菱形編碼區塊中找出最適合藏入的像素以減少失真並提昇其單位像素載入量至 $\log_2(2k^2 + 2k + 1)$ 。

Kieu T.D.和 Chang C.C.[4]提出

$$f(x_1, x_2) = ((s-1) \times x_1 + s \times x_2) \bmod s^2$$

利用矩形區塊擴大進位制的基底提昇提昇其單位像素載入量並找出最適合藏入的像素。

Hong W.和 Chen T.S.[3]提出

$$f(x_1, x_2) = (x_1 + C_B \times x_2) \bmod B$$

此法提供比菱形區塊更緊密的鄰近像素區塊，所造成的失真更小，同時可使用於任意進位制系統。

與以上各位學者不同的是，本研究引入奇數階魔術方塊(Odd-Sided Magic Cube)的概念，以三個像素為一組，將 EMD 的概念立體化，並將三元數對擴展至 n 元數對，解決隨著 n 值的變大，其單位像素藏入量減少的問題。

3. 研究方法

以奇數階魔術方塊 $3 \times 3 \times 3$ 和 $5 \times 5 \times 5$ 為例(如圖 1)。

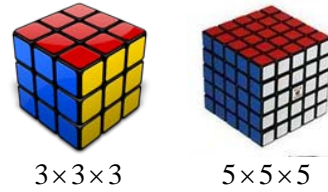


圖 1 奇數階魔術方塊

當 $k=1$ 時 $2k+1=3$ ，在 $3 \times 3 \times 3$ 的魔術方塊中，假設我們將灰階影像中相鄰的三像素所構成的三元數對 (x_1, x_2, x_3) 視為且每個邊只有 $-1, 0, 1$ 三個值，則我們模仿 EMD (Exploiting Modification Direction) 的概念，定義擷取函數 f 如下：

$$f(x_1, x_2, x_3) = \left(\sum_{i=0}^2 (x_i \cdot 3^i) \right) \bmod 3^3$$

$$s = (d-f) \bmod 33$$

由於 (x_1, x_2, x_3) 中每一個像素 x_1, x_2, x_3 都有三種可能 $-1, 0, 1$ ，所以我們可以得到以下唯一的對應關係(表 1)。

表 1 $3 \times 3 \times 3$ 魔術方塊中 (x_1, x_2, x_3) 與機密訊息 d 與 s 的對應關係

x_1	x_2	x_3	s	x_1	x_2	x_3	s	x_1	x_2	x_3	s
0	0	0	0	0	0	1	9	0	0	-1	18
1	0	0	1	1	0	1	10	1	0	-1	19
-1	1	0	2	-1	1	1	11	-1	1	-1	20
0	1	0	3	0	1	1	12	0	1	-1	21
-1	-1	1	5	1	1	1	13	-1	-1	0	23

1	1	0	4	-1	-1	-1	14	1	1	-1	22
0	-1	1	6	0	-1	-1	15	0	-1	0	24
1	-1	1	7	1	-1	-1	16	1	-1	0	25
-1	0	1	8	-1	0	-1	17	-1	0	0	26

其嵌入方式如下： $(3^3=27)$ 若 27 進制的機密訊息 $d=f$ ，則所有像素值不須改變，否則令 $s=(d-f) \bmod 27$ ，依照表 1 的對應方式修改 (x_1, x_2, x_3) 的值做改變。機密訊息的取出只須將偽裝影像的像素組 (x'_1, x'_2, x'_3) 代入擷取函數，得到的值即為機密訊息。

範例：像素組(10,10,10)，欲嵌入的機密訊息 $d=(26)_{27}$ 。

$$\begin{aligned} f(10,10,10) &= (10 \times 1 + 10 \times 3 + 10 \times 3^2) \bmod 3^3 \\ &= 131 \bmod 27 = 23 \end{aligned}$$

因為 $d \neq f$ ，令 $s=(26-23) \bmod 27=3$ ，由表一可知 $x'_2 \leftarrow x_2 + 1$ ，所以藏入機密訊息後的像素組 $(x'_1, x'_2, x'_3) = (10, 11, 10)$ 。欲取出機密訊息則將(10,11,10)代入擷取函數，即可取得機密訊息為 $(26)_{27}$ 。

$$\begin{aligned} f(10,11,10) &= (10 \times 1 + 11 \times 3 + 10 \times 3^2) \bmod 3^3 \\ &= 134 \bmod 27 = 26 \end{aligned}$$

當 $k=2$ 時 $2k+1=5$ ，在 $5 \times 5 \times 5$ 的魔術方塊中，假設我們將灰階影像中相鄰的三像素所構成的三元數對 (x_1, x_2, x_3) 視為且每個邊只有 -2, -1, 0, 1, 2 五個值，則我們模仿 EMD (Exploiting Modification Direction) 的概念，定義擷取函數 f 如下：

$$\begin{aligned} f(x_1, x_2, x_3) &= \left(\sum_{i=0}^2 (x_i \cdot 5^i) \right) \bmod 5^3 \\ s &= (d-f) \bmod 5^3 \end{aligned}$$

由於 (x_1, x_2, x_3) 每一個像素都有五種可能 $(-2, -1, 0, 1, 2)$ ，所以我們可以得到以下唯一的對應關係(表 2)。

表 2 $5 \times 5 \times 5$ 魔術方塊中 (x_1, x_2, x_3) 與 s 的對應關係

x_1	x_2	x_3	s	x_1	x_2	x_3	s	x_1	x_2	x_3	s
0	0	0	0	2	-2	2	42	-1	2	-2	84
1	0	0	1	-2	-1	2	43	0	2	-2	85
2	0	0	2	-1	-1	2	44	1	2	-2	86
-2	1	0	3	0	-1	2	45	2	2	-2	87
-1	1	0	4	1	-1	2	46	-2	-2	-1	88
0	1	0	5	2	-1	2	47	-1	-2	-1	89
1	1	0	6	-2	0	2	48	0	-2	-1	90
2	1	0	7	-1	0	2	49	1	-2	-1	91

-2	2	0	8	0	0	2	50	2	-2	-1	92
-1	2	0	9	1	0	2	51	-2	-1	-1	93
0	2	0	10	2	0	2	52	-1	-1	-1	94
1	2	0	11	-2	1	2	53	0	-1	-1	95
2	2	0	12	-1	1	2	54	1	-1	-1	96
-2	-2	1	13	0	1	2	55	2	-1	-1	97
-1	-2	1	14	1	1	2	56	-2	0	-1	98
0	-2	1	15	2	1	2	57	-1	0	-1	99
1	-2	1	16	-2	2	2	58	0	0	-1	100
2	-2	1	17	-1	2	2	59	1	0	-1	101
-2	-1	1	18	0	2	2	60	2	0	-1	102
-1	-1	1	19	1	2	2	61	-2	1	-1	103
0	-1	1	20	2	2	2	62	-1	1	-1	104
1	-1	1	21	-2	-2	-2	63	0	1	-1	105
2	-1	1	22	-1	-2	-2	64	1	1	-1	106
-2	0	1	23	0	-2	-2	65	2	1	-1	107
-1	0	1	24	1	-2	-2	66	-2	2	-1	108
0	0	1	25	2	-2	-2	67	-1	2	-1	109
1	0	1	26	-2	-1	-2	68	0	2	-1	110
2	0	1	27	-1	-1	-2	69	1	2	-1	111
-2	1	1	28	0	-1	-2	70	2	2	-1	112
-1	1	1	29	1	-1	-2	71	-2	-2	0	113
0	1	1	30	2	-1	-2	72	-1	-2	0	114
1	1	1	31	-2	0	-2	73	0	-2	0	115
2	1	1	32	-1	0	-2	74	1	-2	0	116
-2	2	1	33	0	0	-2	75	2	-2	0	117
-1	2	1	34	1	0	-2	76	-2	-1	0	118
0	2	1	35	2	0	-2	77	-1	-1	0	119
1	2	1	36	-2	1	-2	78	0	-1	0	120
2	2	1	37	-1	1	-2	79	1	-1	0	121
-2	-2	2	38	0	1	-2	80	2	-1	0	122
-1	-2	2	39	1	1	-2	81	-2	0	0	123
0	-2	2	40	2	1	-2	82	-1	0	0	124
1	-2	2	41	-2	2	-2	83				

其嵌入方式如下： $(5^3=125)$ 若 125 進制的機密訊息 $d=f$ ，則所有像素值不須改變，否則令 $s=(d-f) \bmod 125$ ，依照表 1 的對應方式修改 (x_1, x_2, x_3) 的值做改變。機密訊息的取出只須將偽裝影像的像素組 (x'_1, x'_2, x'_3) 代入擷取函數，得到的值即為機密訊息。

範例：像素組(10,10,10)，欲嵌入的機密訊息 $d=(100)_{125}$ 。

$$\begin{aligned} f(10,10,10) &= (10 \times 1 + 10 \times 5 + 10 \times 5^2) \bmod 5^3 \\ &= 310 \bmod 125 = 60 \end{aligned}$$

因為 $d \neq f$ ，令 $s=(100-60) \bmod 127=40$ ，由表 2 可知 $x'_2 \leftarrow x_2 - 2$ ， $x'_3 \leftarrow x_3 + 2$ ，所以藏入機密訊息後的像素組 $(x'_1, x'_2, x'_3) = (10, 8, 12)$ 。欲取出機密訊息則將(10,8,12)代入擷取函數，即可取得機密訊息為 $(100)_{125}$ 。

$$\begin{aligned} f(10,8,12) &= (10 \times 1 + 8 \times 5 + 12 \times 5^2) \bmod 5^3 \\ &= 350 \bmod 125 = 100 \end{aligned}$$

以上機密訊息的藏入過程中，每一像素至多加減 k 的對應關係是唯一的，所以機密訊息的取出可以保證其正確性。

4. 實驗結果

影像品質的評估則是希望偽裝影像與做為載體的原始影像的差異性愈小愈好，一般是由 MSE (Mean Square Error) 計算 PSNR (Peak-Signal-Noise Ratio)，其中 PSNR 以 dB 為單位，其值愈大表示偽裝影像愈接近原始影像。


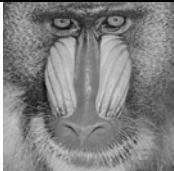





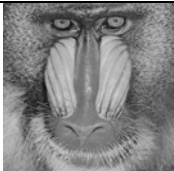

$$MSE = \frac{1}{w \times h} \sum_{i=1}^w \sum_{j=1}^h (P'(i, j) - P(i, j))^2$$




$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \text{ (dB)}$$

其中 $P'(i, j), P(i, j)$ 分別表示偽裝影像與原始影像中相對位置為 i, j 的像素值， w, h 分別表示原始影像的寬度與高度。

我們選用 SIPI 影像資料庫中的六張標準測試影像 (Tiffany、Baboon、Lena、Jet、Scene 和 Peppers) 做實驗。實驗結果如表 3：

表 3 實驗結果 ($k=1, 2$)

$k=1$		
		
PSNR=52.45dB Payload=1.58bpp	PSNR=52.43dB Payload=1.58bpp	PSNR=52.43dB Payload=1.58bpp
		
PSNR=52.43dB Payload=1.58bpp	PSNR=52.43dB Payload=1.58bpp	PSNR=52.45dB Payload=1.58bpp
$k=2$		
		
PSNR=45.20dB Payload=2.32bpp	PSNR=45.19dB Payload=2.32bpp	PSNR=45.18dB Payload=2.32bpp

		
PSNR=45.18dB Payload=2.32bpp	PSNR=45.19dB Payload=2.32bpp	PSNR=45.20dB Payload=2.32bpp

所以，當 $k=1$ 時 $(2k+1)^3=27$ ，表示每一像素至多加減 1，我們可以將一個 27 進制的機密訊息藏入，其平均負載量為 $(\log_2 27)/3=1.5850$ bpp。當 $k=2$ 時 $(2k+1)^3=125$ ，表示每一像素至多加減 2，我們可以將一個 125 進制的機密訊息藏入，其平均負載量為約為 $(\log_2 125)/3=2.3219$ bpp。由此可知，本研究的設計並沒有 EMD 隨著 n 值的變大，其單位像素藏入量減少的問題。

我們將 EMD ($n=2, 3, 4, 5$) 與本研究 ($k=1, 2$) 之比較整理如表 4。表 4 中的 PSNR 數據為使用相同的六張標準測試圖形實驗的平均值。

表 4 EMD ($n=2, 3, 4, 5$) 與本研究 ($k=1, 2$) 之比較

	EMD			
	$n=2$	$n=3$	$n=4$	$n=5$
PSNR (dB)	52.58	53.79	54.79	55.46
Payload (bpp)	1.1610	0.9358	0.7925	0.6919
本研究				
	$k=1$	$k=2$		
PSNR (dB)	52.44	45.19		
Payload (bpp)	1.5850	2.3219		

本研究中每一像素至多加減 k 的對應關係也代表了機密訊息藏入量與藏入後的影像品質的最佳化。除此之外，我們可以將三元數對擴展至 n 元數對，亦保有以上的良好性質。亦即

$$f(x_1, x_2, x_3, \dots, x_n) = \left(\sum_{i=0}^{n-1} (x_i \cdot 3^i) \right) \text{ mod } 3^n$$

$$f(x_1, x_2, x_3, \dots, x_n) = \left(\sum_{i=0}^{n-1} (x_i \cdot 5^i) \right) \text{ mod } 5^n$$

更進一步推導至

$$f(x_1, x_2, x_3, \dots, x_n) = \left(\sum_{i=0}^{n-1} (x_i \cdot (2k+1)^i) \right) \text{ mod } (2k+1)^n$$

pp. 497-500, Nov. 2007,
doi:10.1109/IIH-MSP.2007.62.

5. 結論

本研究將灰階影像中相鄰的三像素所構成的三元數對 (x_1, x_2, x_3) 視為立體魔術方塊在三維空間中 X,Y,Z 三個座標軸上的邊，利用 EMD(Exploiting Modification Direction) 的概念，定義擷取函數並將每一像素加減 k 的關係與立體魔術方塊所構成的分割方塊做一對應。將 $(2k+1)^3$ 進制的機密訊息藏入 (x_1, x_2, x_3) 這個三元數對中且其中每一個像素至多加減 k 。

由實驗結果證明了此法改進了 EMD 隨著 n 值的變大，其單位像素藏入量減少的問題。在機密訊息的藏入過程中，每一像素至多加減 k 的對應關係是唯一的，所以機密訊息的取出可以保證其正確性。與 EMD 相關的研究比較（兩個像素為一組），本研究代表了三個像素為一組的機密訊息藏入量與藏入後的影像品質的最佳化。更進一步的，本研究可將此性質擴展至 n 元數對，亦保有以上的良好性質。

參考文獻

- [1]Chao, R.M., Wu, H.C., Lee, C.C. and Chu, Y.P., “A novel image data hiding scheme with diamond encoding”, *EURASIP Journal on Information Security*, vol. 2009, Article ID 658047, 9 pages, doi:10.1155/2009/658047.
- [2]Chen, K.N., Chang, C.C. and Lin, H.C., “A Large Payload EMD Embedding Scheme with High Stego-image Quality”, *International Conference on Computational Aspects of Social Networks*, pp.126-130, Sep. 2010, doi:10.1109/CASoN.2010.35.
- [3]Hong, W. and Chen, T.S., “A Novel Data Embedding Method Using Adaptive Pixel Pair Matching”, *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 176-184, Feb. 2012.
- [4]Kieu, T.D. and Chang, C.C., “A steganographic scheme by fully exploiting modification directions”, *Expert systems with Applications*, vol. 38, pp. 11648-10657, Aug. 2011, doi:10.1016/j.eswa.2011.02.122.
- [5]Lee, C.F., Wang, Y.R. and Chang, C.C., “A steganographic method with high embedding capacity by improving exploiting modification direction”, *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*,

- [6]Zhang, X.P. and Wang, S.Z., “Efficient steganographic embedding by exploiting modification direction”, *IEEE Commun. Lett.*, vol. 10(11), pp. 781-783, doi:10.1109/LCOMM.2006.060863.