行政院國家科學委員會專題研究計畫期中報告

影像的快速分享與高容量隱藏、及它門在影像修復的應用(第一年期)

Fast sharing, high-capacity hiding, and their applications in images' recovery

計畫編號：NSC 97-2221-E-009-120-MY3

執行期限：97 年 8 月 1 日～98 年 7 月 31 日

主持人：林志青 交通大學資訊科學系所

計畫參與人員：陳李書滕、林憲正

交通大學資訊工程系所

一、 中文摘要

本計畫為期三年，其目的是提出快速影像分享與高容量資訊隱藏方法，及其在影像修復的應用。本年(第一年)的主題是影像的快速分享，主要是基於上一個國科會的影像分享計畫的基礎，提出影像分享技術的加速版。第一年第一個主題為使用布林(Boolean)運算的快速機密影像分享法。在本主題中，我們希望研究出一個新的機密影像分享法，不但它產生的分存影像(shadow image)所需要的儲存空間很小，而且解碼運算量也會非常低。第一年第二個主題是多項式(t, n)分享方法的快速編碼與解碼。我們觀察到機密分享中的多項式運算存在一些相似的模式，而這些相似的模式顯示著其計算複雜度可以下降。因此我們希望利用這些特性，來設計出一套加速運算的演算法。第一年第三個主題為快速編碼與解碼的動態權重多項式分享方法。在本主題中，我們希望設計一個可以快速的建構出不同權重的機密分存影像方法外，當我們希望改變某些分存影像的權重的時候，亦可快速的對分存影像做更新。

關鍵詞：機密分享；布林運算；分存影像放大率；快速傅立葉轉換；蝴蝶圖；權重。

Abstract

This project is the 1st part of a three-year project. The goal of the three-year project is to provide fast secret image sharing methods, high-capacity hiding schemes, and their applications in images' recovery. The first year is for the fast sharing of an image. There are three topics in the first year. The first topic is the fast secret image sharing based on Exclusive-OR operations, and the goal of it is to design a novel secret image sharing technique which provides very small shadow images and very low decoding complexity. The second topic is the fast sharing approach of the polynomial based (t, n)-threshold secret sharing. We observe that there are some patterns in the polynomial computations of the secret image sharing, and this observation is helpful for reducing the time complexity of the polynomial computations. The third topic is the fast sharing approach with shadow images of dynamic weights. The goal of this topic is to design a fast method for a system with shadow images of dynamic weights. Besides, when the weight of a created shadow image has to be changed, the shadow image can also be updated quickly.

二、 計畫緣由與目的

本年度(第一年)的第一個主題是：使用布林運算的快速機密影像分享法。歷史上最常見的機密影像分享方法是多項式機密分享法(polynomial secret sharing)和視覺編碼法(visual cryptography)兩種。其中多項式機密分享法[1]的優點是分存影像所需要的儲存空間比較小，但是它的解碼運算量相當高；而視覺編碼法[2]的優點反而是它的解碼運算量非常低，但是分存影像所需要的儲存空間卻很大。在這個主題中，我們希望設計出一種使用布林運算內的XOR為基礎的可容錯機密影像分享法，使得產生的分存影像大小可以比原來機密影像還要小，而且在事後的重建過程中只需要數個XOR運算就可以重建機密影像的每一個像素值。另外，此機密影像分享法也擁有(t, n)分享方法的容錯能力，並

且能運用在任何黑白、灰階和彩色影像上。

本年度的第二個主題是：多項式(*t, n*)分享方法的快速編碼與解碼。我們在前國科會計畫的研究之中觀察到，有關多項式(*t, n*)分享方法[3]，其編碼與解碼計算有些許的規律。而這些計算上的規律，往往可以利用於進行編碼與解碼時的加速運算上。在做多項式(*t, n*)分享的時候，主要都是利用矩陣運算的方式來計算解答，但是由於這是多項式的運算，因此其運算矩陣會存在一些規律（即每一列都是以$[1 \ x \ x^2 \ x^3 \ \dots \ x^{t-1}]$的形式顯示），而這些規律顯示其計算複雜度有下降的可能。因此我們想要利用這些觀察到的規律性，來設計出一套加速運算的演算法。此方法可以快速地對分存影像做編碼與解碼的動作。尤其是在高的 *t, n* 時候，甚至可以將編碼時間壓縮至 $\Theta(\log t)$，並在 $\Theta(\log^2 t)$的時間下完成解碼（這會快於多項式(*t, n*)分享方法[3]編碼所需的時 $\Theta(t)$及解碼時間 $\Theta(t)$）。

本年度的第三個主題是：快速編碼與解碼的動態權重多項式分享方法。在各種不同的應用環境之中，我們或許會希望每個分存影像的權重會不相同。例如當資料在網路間流動的時候，路由器可依據每條路徑的頻寬而將資料用不同權重的分存影像傳輸出去，這樣只要接收端收到一定量的分存影像之後，便可以重建出原本的資料，由於我們強調演算法比須是快速的，所以各路徑亦會各自加速。因此，在這個主題中，我們希望在一個分存影像有不同權重的情況下，設計出一套快速編碼與解碼的資訊分享方法。此方法除了可以快速的建構出不同權重的分存影像外，當我們希望改變某些分存影像權重的時候，亦可快速的對分存影像做更新。

三、 結果與討論

在第一主題：使用布林運算的快速機密影像分享法，首先使用基礎的(2, 2)-threshold 的 XOR 機密影像分享法[4]產生兩張亂碼圖，再將這兩張亂碼圖進行分割，切成所需要的大小與數量。然後，將以上切割好的亂碼圖小碎塊使用 XOR 運算重新組合成 *n* 張一樣大小的亂碼圖。最後，這 *n* 張亂碼圖立即成為擁有多項式(*t, n*)分享方法

的容錯能力的分存影像。如圖例一，本實驗所設定的門檻值是(t=4, n=4)，(a)為本實驗用的 768×512 彩色機密影像，(b)-(e)為產生的四張分存影像，每張分存影像大小為 768×256，(f)為利用前面產生的所有四張分存影像所還原的無失真機密影像。從實驗結果可看出，本方法具有多項式(t, n)分享方法的容錯能力，而且所產生的分存影像可以比原來機密影像還要小。另外，表一比較本方法和[3]重建機密影像中的一個像素值所需的時間複雜度，採用本方法重建機密影像中的一個像素值只需要花費三個 XOR 運算，因此優於[3]。

在第二個主題：多項式(t, n)分享方法的快速編碼與解碼，我們使用在 GF(2^{k+1})上的快速傅立葉轉換(FFT)來達成加速的目的，以下將分成編碼和解碼來分開討論。

(t, n)分享編碼： 我們使用快速傅立葉轉換的蝴蝶圖來加速運算。圖例二顯示一個大小為 8 的蝴蝶圖，其中 d_i 是輸入值，而 $F(w_j)$是輸出值。首先，從機密影像拿出 t 個未處理的像素，然後將這 t 個像素當成蝴蝶圖的 d_i 輸入值。經過 $\Theta(t\log^2 t)$的蝴蝶圖運算後，便可以取出 t 個分存影像數值 $\{F(w_8^i) \mid i = 0,1,...,t-1\}$。如果分存影像不夠的話，則可以利用如下的運算(先令 j=1)：

$$\left\{d_0 w_N^{0\times j}, d_1 w_N^{1\times j}, ..., d_{t-1} w_N^{(t-1)\times j}\right\}$$

以獲得新的 d_i, 然後將這些新數值重新輸入蝴蝶圖中獲得新的 t 個分存影像數值:

$$\left\{F(w_N^{0+j}), F(w_N^{N/t+j}), ..., F(w_N^{N/t(t-1)+j})\right\}$$

如果分存影像還不夠，則令 j=j+1 然後回到前面的步驟以繼續產生運算新的分存影像。依照以上的步驟，我們可以在 $\Theta(n\log t)$時間內獲得 n 個分存影像數值。依照如上的步驟，直到機密影像的像素全部處理完畢，然後 n 張分存影像便可以產生出來。

(t, n)分享解碼： [5]介紹了一種 $\Theta(t\log^2 t)$ 複雜度的快速計算的 Lagrange polynomial 方法。我們將這個方法運用在 GF(2^{k+1})上，然後利用它來做分享解碼。最後獲得了可以在 $\Theta(t\log^2 t)$時間內解碼的快速演算法。表二顯示利用本方法對於 512×512 Lena 的機密影像的分享所需編碼時間；表三顯示利用一

般多項式計算對於該 512×512 機密影像的分享所需編碼時間。比較表二，我們發現當 t 越大，我們所提出的快速 (t, n) 分享運算編碼的減少時間越明顯。表三比較本方法和傳統方法(反矩陣)對於該 512×512 的機密影像的分享所需解碼時間，從觀察中可知，當 t 越大時，採用本方法運算解碼所減少的時間也越明顯。

在第三個主題：快速編碼與解碼的動態權重多項式分享方法，首先將 512×512 Lena 機密影像(圖例三(a))做加密，然後將得到的加密影像(圖例三(b))利用我們所提出的動態權重(t=256, n=7)多項式分享方法，依權重 160; 64; 24; 8; 134; 12; 3 分別產生 7 個分存影像，結果分別如圖例三(c-i)所示。之後，若搜集到的分存影像其總權重超過 t=256 時，便可無失真還原回 512×512 機密影像 Lena，圖例三(j)為利用四個分存影像(圖例三(c-f))所還原的無失真機密影像。表四比較我們的快速動態權重多項式分享方法與直接合併傳統多項式分享方法[3]的 w_1 張分存以產生 1 個權重為的 w_1 加權分存影像所需之時間。對於 512×512 Lena 機密影像分享運算的編碼時間，從表五可知，當權重 w_1 大於 1 時，採用本方法所需的編碼時間皆優於直接使用傳統多項式(t, n)分享方法[3]所需的編碼時間。

四、 計畫成果與自評

第一年的第一、二、三主題，我們均成功的達成預期目標與成果。而第一主題已投稿至 IJPRAI 期刊且被接受；第二主題已投稿至 IEEE 會議且被接受；第三主題已經投稿至國際期刊。本計劃第一年之申請經費為 325,450 元(核定為 440,000 元，因加列主持人費用)。大概會發表 2 至 3 篇國際期刊論文。以這樣的成果應該還算可以。

五、 參考文獻

[1] R. Z. Wang and C. H. Su, Secret image sharing with smaller shadow images, *Pattern Recognition Letters*, Vol. 27, pp. 551-555. 2006.

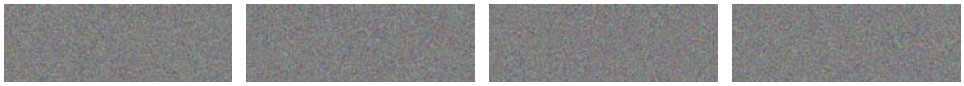
[2] R. Lukac and K. N. Plataniotis, Bit-level based secret sharing for image encryption, *Pattern Recognition*, Vol. 38, pp. 767-772, 2005.

[3] C. C. Thien and J. C. Lin, Secret image sharing, *Computer and Graphic*, Vol. 26, pp. 765-770. 2002.

[4] D. Wang, L. Zhang, N. Ma, X. Li, Two secret sharing schemes based on Boolean operations, *Pattern Recognition*, Vol. 40, pp. 2776-2785, 2007.

[5] D. Bini and V.Y. Pan, *Polynomial and Matrix Computations*, *Volumn 1:Fundamental Algorithms*, Birkhauser, Boston, 1994.

(a)



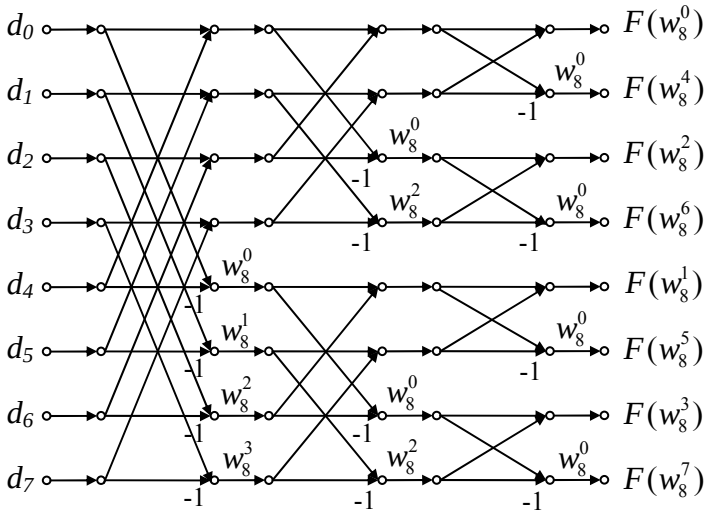
(b) (c) (d) (e)

(f)

圖例一 第一主題－使用布林運算的快速機密影像分享法的實驗結果。在這個實驗中，使用的門檻值(threshold)為(t=4, n=4)。(a)為輸入的 768×512 機密影像，(b-e)為產生的 n=4 張分存影像，每張大小為 768×256，(f)為使用全部四張分存影像所重建的無失真機密影像。

表一 重建機密影像中一個像素值所需的解碼運算複雜度比較。

	(t, n) threshold	t=n 時
[2]的 OR 運算解碼方法	$O(t \times per)$ OR 運算	$O(n \times per)$ OR 運算
[3]的多項式方法解碼方法	$\Theta(t)$四則運算	$O(\log^2 n)$四則運算
我們的布林運算快速解碼方法	3 XOR 運算	3 XOR 運算



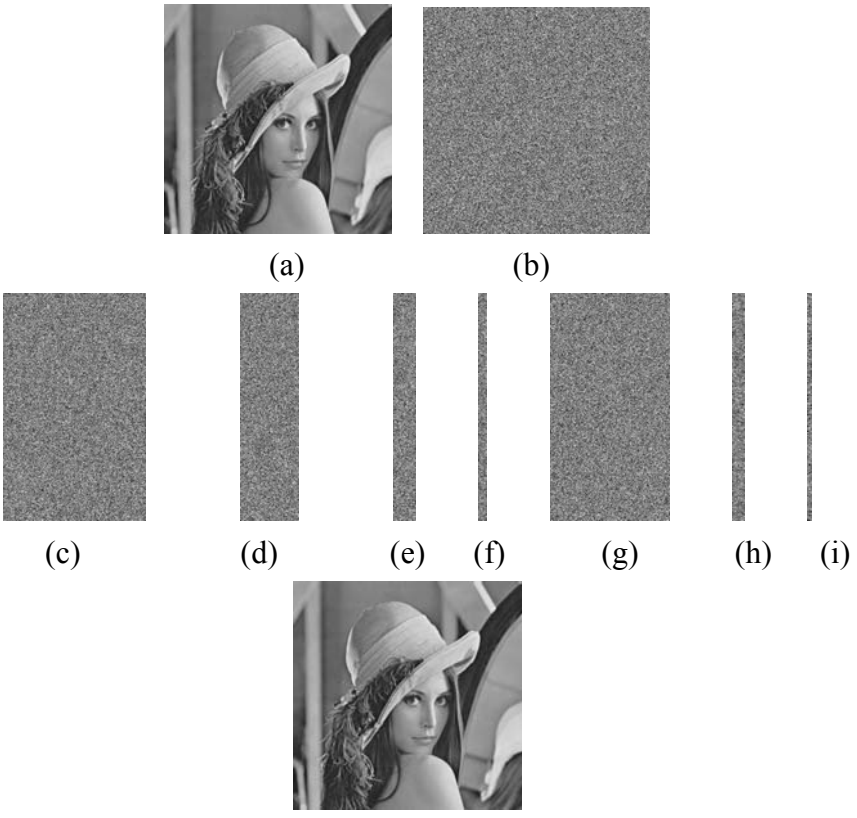
圖例二 具有 8 個輸入的 FFT 蝴蝶圖。其中 d_i 是輸入值，而 $F(w_j)$是輸出值。

表二 512×512 Lena 機密影像的(t, n)分享編碼時間(時間單位:千分之一秒)。

方法 \ n		4	16	64	256	1024	4096
T & L [3]	t=4	31	141	250	1937		
Ours		78	140	281	1829		
T & L [3]	t=16		93	406	2594	6907	
Ours			94	203	718	2750	
T & L [3]	t=64			391	1500	6297	25953
Ours				93	265	953	4594
T & L [3]	t=256				1484	5906	23953
Ours					110	328	1375
T & L [3]	t=1024					6000	23922
Ours						141	438
T & L [3]	t=4096						24047
Ours							172

表三 512×512 Lena 機密影像的傳統(t, n=t)分享解碼時間(時間單位:千分之一秒)。一為在[3]中使用反矩陣和矩陣乘法運算的解碼方法(複雜度為 $\Theta(t)$),另一為我們提出的快速解碼方法(複雜度為 $\Theta(\log^2 t)$)。

方法 \ t	2	4	8	16	32	64	128	256	512	1024	2048
T & L [3]	31	62	125	234	437	875	1766	3531	7094	14297	28922
Ours	62	109	172	234	313	375	484	593	703	859	1015



圖例三 第三主題－快速編碼與解碼的動態權重多項式分享方法的實驗結果。在這個實驗中,使用的權重總合的門檻值為 t=256。(a)為輸入的 512×512 機密影像,(b)為(a)加密後的結果,(c-i)為分別依權重 160; 64; 24; 8; 134; 12; 3,產生 n=7 張分存影像,(j)為利用四張分存影像(c-f)所重建的無失真機密影像。

表四 512×512 Lena 機密影像的動態權重多項式分享運算編碼時間(時間單位:千分之一秒)。一為[3]的動態權重編碼多項式 $t=w_1$ 分享方法，另一為我們提出的快速動態權重編碼多項式 $t=w_1$ 分享方法。

權重 w_1 / 方法	1	2	4	8	16	32	64	128
T & L [3]	7	15	31	62	110	203	406	813
Ours	7	7	7	6	6	6	6	5