Communications of the CCISA
Vol. 22 No. 2 Apr. 2016

多秘密影像分享技術

詹啟祥
亞洲大學行動商務與多媒體應用學系
CSChan@asia.edu.tw

摘要

在本文中，我們介紹兩個「多秘密影像分享技術」。所謂的「多秘密影像分享技術」是將多張秘密影像分享成若干張分享影像，當分享影像結合起來，就可以重建多張的秘密影像。在低計算度的「多秘密影像分享技術」中，有兩種常被提到的技術，分別是「階層式多秘密影像分享技術」以及「環狀式多秘密影像分享技術」。前者所產生的分享影像之重要性並不一樣，也就是握有較重要的分享影像的擁有者，當其拒絕與其他擁有者合作時，會導致大部分的秘密影像無法重建回來。相反的，後者所產生的分享影像，每張分享影像的重要性皆相同，所以任何一張分享影像擁有者拒絕合作，只會導致固定張數的秘密影像無法重建回來。

關鍵詞：布林運算為基礎之影像分享技術、多秘密影像分享技術、秘密影像分享技術

Multi-Secret Images Sharing Schemes

Chi-Shiang Chan
[1]Department of M-Commerce and Multimedia Applications,
Asia University, Taichung, Taiwan.
CSChan@asia.edu.tw

Abstract

In this article, two Multi-Secret Images Sharing Schemes (*MSISS*) are introduced. The meaning of *MSISS* is to share secret images into shadow images. The secret images can be reconstructed when the owners of certain shadow images are cooperated each other. Among all low computation *MSISS*, two schemes are mentioned frequently. The one is "Hierarchy based *MSISS*" and the other is "Cycle based *MSISS*." In "Hierarchy based *MSISS*", not all shadow images are equally important. If the owner with the important shadow image does not want to cooperate with other owners, most secret images cannot be reconstructed. On the other hand, in "Cycle based *MSISS*", all shadow images are equally important. If one owner refuses to cooperate with other owners, only two secret images cannot be reconstructed.

Keywords: Boolean-based VSS, Multi-secret image sharing, Secret image sharing

壹、前言

由於資料的數位化，如何保護秘密資料不被非法擁有者竊取，是現今數位資料安全的一個非常重要議題。為了保護秘密資料的安全以及防止秘密資料的遺失，Shamir 學者提出「(t, n)門檻機制的祕密分享技術」[7]，此技術為第一個提出秘密分享概念的技術。此技術會利用秘密資訊產生 n 個分享資訊(shadow)，當這 n 個分享資訊中的任何 t 個分享資訊合作，便可以將解出秘密資訊。因此，任何少於 t 個的分享資訊之間的合作，並無法解出解密資訊。如此，縱使有一個分享資訊被竊取或遺失，並不會對秘密資料產生危害。而且，一份分享資訊的遺失，也不會導致秘密資料無法解開。值得注意，在(t, n)門檻機制的祕密分享技術中，每個分享資訊的重要性都一樣，也就是縱使有任何擁有者拒絕交出分享資訊，其他分享資訊的擁有者合作，仍然有辦法解出祕密資訊出來。

在「(t, n)門檻機制的祕密分享技術」提出之後，許多延伸應用與技術也隨之發展。其中，在 1995 年，Naor 與 Shamir 學者運用「(t, n)門檻機制的祕密分享技術」的概念到影像中，以發展「可視秘密影像分享技術」(Visual Secret Sharing : VSS)[6]。利用此技術將秘密影像分享到 n 張分享影像(shadow image)後，會產生 n 張雜亂、無任何資訊的分享影像。當這 n 張分享影像中的任何 t 張分享影像進行疊合，在不需要使用任何電腦運算幫助的情況下，利用肉眼就可看到祕密影像。

上述的方法是只能將單張的秘密影像分享到多張分享影像。隨後的研究，將重點擺在「可視多祕密影像分享機制」(Visual Multiple Secret Sharing) [3][8][10][11]。Wu 與 Chen 學者所提的方法中[11]，將兩張秘密影像分享到兩張分享影像，當這兩張分享影像疊合後，會顯示出第一張秘密影像。當其中一張分享影像旋轉 90^o 後進行疊合，會顯示第二張秘密影像。而[3][8][10]學者則是延伸 Wu 與 Chen 學者的技術，以發展「可視多祕密影像分享機制」技術。

然而，無論上述所提的單張或者是多張的秘密影像分享機制，都必須以手動的方式疊合兩張分享影像，以顯示秘密影像。如此導致此類的技術會有先天上的缺點，第一個缺點在於分享影像的對齊問題，也就是兩張分享影像內相對應位置的像素，必須百分之百對齊，才有辦法顯示出祕密影像。一旦有一個像素沒有對齊，整個祕密影像將無法顯示出來。第二個缺點則是會產生分享影像擴張的問題，也就是分享影像的大小會比祕密影像大的多。第三個缺點是有關祕密影像的影像品質問題，由於上述所提影像分享機制是以疊合的方式顯示祕密影像，如此導致祕密影像之黑白對比度必須降低，也就是所顯示的祕密影像，會有較差的影像品質。

為了解決這些的缺點，一些改進方法被提出[2][4][5][9]。其中一個即是「布林運算為基礎之秘密影像分享技術」(Boolean-based VSS) 。更精確的來說，傳統「可視秘密影像分享技術」可以視為兩張分享影像的像素進行 AND 運算，也就是在疊合的過程中，只要有一個像素是黑色，則最後疊出來的像素也會是黑色。而「布林運算為基礎之秘密影

像分享技術」則是以 XOR 運算來取代 AND 運算，來達到祕密影像的分享的目的。

第一個「布林運算為基礎之秘密影像分享技術」是由 Wang 等學者[9]所提，他們利用此方法將一張祕密影像分享到 *n* 張分享影像上。在 Wang 等學者的方法中，會先產生 *n*-1 個亂數矩陣，而後 *n* 張分享影像會依序產生，產生方式是利用 XOR 運算執行於亂數矩陣與祕密影像。

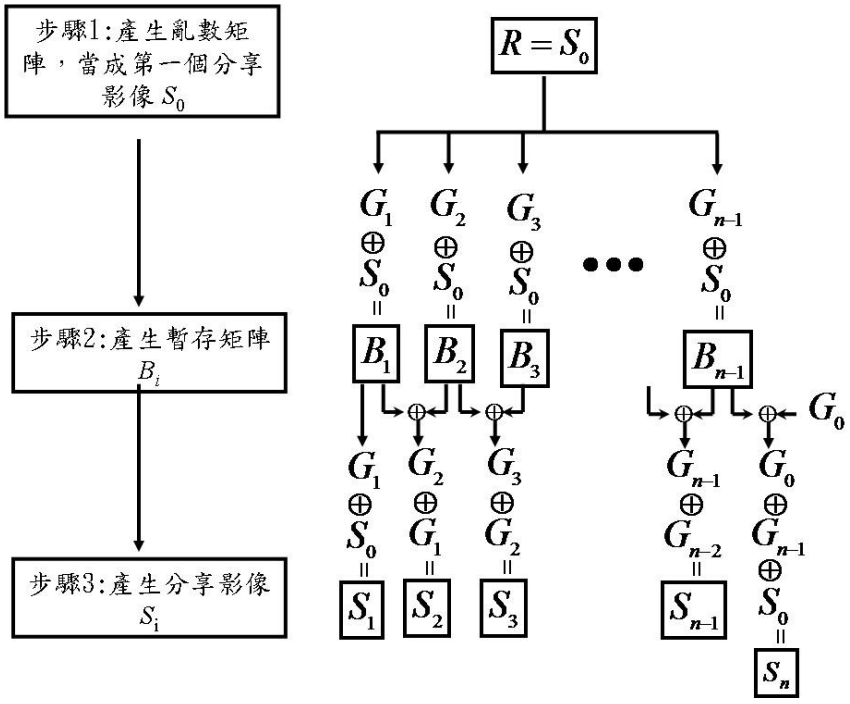
為了要分享更多的祕密影像，Chen 與 Wu [4]學者修改 Wang 等學者的方法，只產生一個亂數矩陣當作是第零號分享影像，接著第 *i* 號祕密影像依序與前一號分享影像進行 XOR 運算，而得到第 *i* 號分享影像，最後便會產生共 *n*+1 張分享影像。此方法所產生的分享影像之重要性皆不一樣，也就是握有較重要的分享影像的擁有用者，當其拒絕與其他擁有者合作時，會導致大部分的秘密影像無法重建回來。此即本文所言「階層式多秘密影像分享技術」。

為了發展具相同重要性的分享影像，Chan 等學者[1]提出「環狀式多秘密影像分享技術」，此技術所產生的每張分享影像的重要性皆相同，所以任何一張分享影像的擁有者拒絕合作，只會導致固定張數的秘密影像無法重建回來。雖然 Guo 等學者[5]所提的方法，也可以達到每個分享影像同等重要的目的，但是 Guo 等學者所提的方法，必須要使用複雜的電腦運算，來產生分享影像，而分享影像的疊合亦需要複雜的電腦運算。此外，Guo 等學者的方法所產生的分享影像，其的影像大小會比祕密影像的影像大小大很多。基於上述原因，我們在本文中介紹 Chan 等學者[1]所提出的「環狀式多秘密影像分享技術」。

我們接著會在下面的文章中介紹「布林運算為基礎之多秘密影像分享技術」。首先，我們會在第二節介紹「階層式多秘密影像分享技術」。而後，我們會在第三節介紹 Chan 等學者所提「環狀式多秘密影像分享技術」。接著，第四節會比較兩者之間的差異。最後，我們會在第五節，對針對這些方法做結論。

貳、階層式多秘密影像分享技術

在此節中，我們介紹 Chen 與 Wu 學者的「階層式多秘密影像分享技術」[4]。值得注意的是，Chen 與 Wu 學者的方法首先假設所有的祕密影像都是複雜的影像，在此情況下，可以利用 Chen 與 Wu 學者所提的方法進行多秘密影像分享，其分享與秘密重建的步驟，會在第一小節中敘述。然而，當秘密影像有任何一張不是複雜影像時，會導致有些分享影像上會顯示部分秘密資料的情況，為了解決這個問題，Chen 與 Wu 學者在論文[4]提供其修正方案，此部分會在第二小節中敘述。



圖一：產生分享影像步驟之流程圖[1]

2.1 Chen 與 Wu 學者的方法

Chen 與 Wu 學者的方法在分享階段，總共有三個主要步驟，流程圖顯示於圖一中。第一個步驟會產生一個與祕密影像相同大小的亂數矩陣，當成第一個分享影像 S_0。亂數矩陣內的每個元素都是介於 0 到 255 之間的整數。第二個步驟則是依據公式(1)，產生第 i 個暫存矩陣 B_i，而 i 值介於 1 到 n-1 之間的整數。公式(1)如下所示：

$$B_i = G_i \oplus S_0, \tag{1}$$

其中⊕表示 XOR 運算。

在第三步驟中，利用公式(2)產生分享影像 S_1~ S_n。

$$S_i = \begin{cases} B_i & \text{假如 } i = 1, \\ B_i \oplus B_{i-1} & \text{假如 } i = 2 \text{到} n\text{-}1, \\ G_0 \oplus B_{i-1} & \text{假如 } i = n. \end{cases} \tag{2}$$

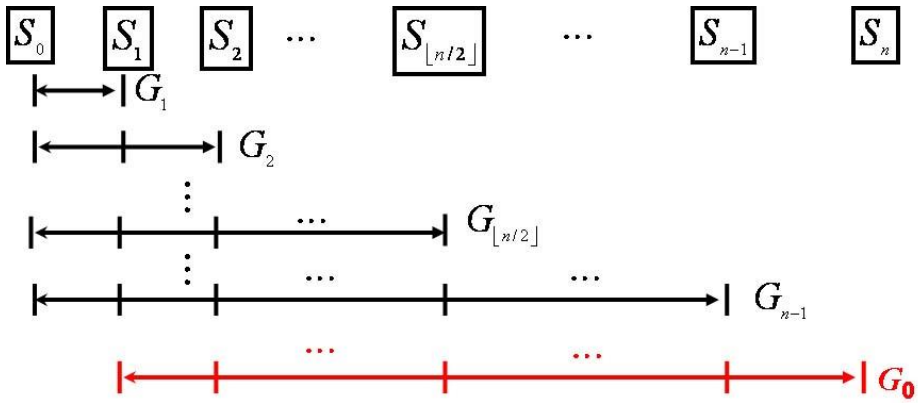
經過三個步驟以後，便可以產生所有的分享影像 S_0~ S_n。

在秘密影像重建階段，第 i 個祕密影像 G_i 的重建方式，如公式(3)所示：

$$G_i = \begin{cases} \Psi_{k=1}^{n} S_k & \text{假如} i = 0, \\ \Psi_{k=0}^{i} S_k & \text{其他情況} \end{cases} \tag{3}$$

其中 $\Psi_{k=1}^{i} S_k$ 代表 $S_1 \oplus S_2 \oplus \ldots \oplus S_i$。

此方法中秘密影像與分享影像之間的關係，如圖二所示。



圖二：Chen 與 Wu 學者方法所產生分享影像與秘密影像的關係圖[1]

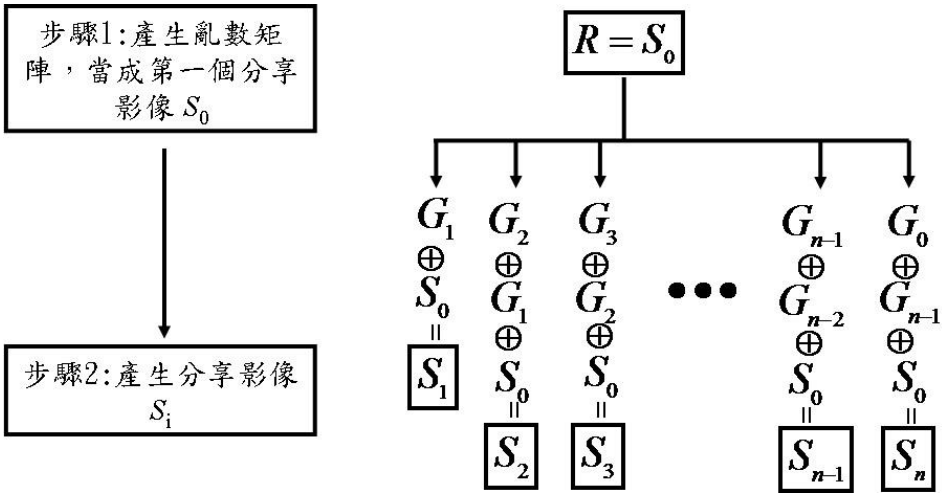
在圖二中，秘密影像 G_1 必須利用分享影像 S_0 與 S_1 來重建。秘密影像 G_2 必須利用分享影像 S_0~S_2 來重建，以此類推。根據圖二可以發現，當分享影像的編號值越小，其重要性也越重要。也就是當分享影像 S_i 的擁有者拒絕與其他擁有者合作時，則秘密影像 G_j ($j \geq i$)都會無法重建。此即本文所言「階層式多秘密影像分享技術」。在此機制中，掌握重要分享影像的人，擁有較重大的權力，可以決定是否讓大部分的秘密影像重建回來。而掌握不重要影像的人，最多只能影響一張秘密影像的重建與否。

2.2 Chen 與 Wu 學者的修正版的「多祕密影像分享機制」

依據前一小節所述，第 i 個分享影像 S_i($2 \leqq i \leqq n$-1) 是利用公式(2) ，執行 XOR 運算於 B_i 與 B_{i-1} 而得到，而 B_i 與 B_{i-1} 分別來自於公式(1)中 $G_i \oplus S_0$ 與 $G_{i-1} \oplus S_0$，所以經由運算可以知道第 i 個分享影像 S_i 等於 $B_i \oplus B_{i-1} = (G_i \oplus S_0) \oplus (G_{i-1} \oplus S_0) = G_i \oplus G_{i-1}$，即第 i 個分享影像 S_i($2 \leqq i \leqq n$-1)等於 $G_i \oplus G_{i-1}$。此即代表亂數矩陣 S_0 在產生第 i 個分享影像 S_i 的過程中，已經被移除。假若兩個祕密影像 G_i 與 G_{i-1} 不是複雜的影像，則祕密影像的部分區域，在執行 XOR 運算後仍然會顯示在分享影像上。

為了克服此問題，Chen 與 Wu 學者提出修正版的方法，將第一小節產生的第 i 個分享影像 S_i 與亂數矩陣 S_0 執行 XOR 運算，以產生修改過後的分享影像。由於 S_0 是亂數矩陣，任何與其執行 XOR 運算的影像，皆會變成凌亂的影像。產生分享影像 S_i 的方式如下所示：

$$S_i' = \begin{cases} G_i \oplus S_0 & \text{假如 } i = 1, \\ G_i \oplus G_{i-1} \oplus S_0 & \text{假如 } i = 2 \text{ 到 } n\text{-}1, \\ G_0 \oplus G_{i-1} \oplus S_0 & \text{假如 } i = n. \end{cases} \quad (4)$$

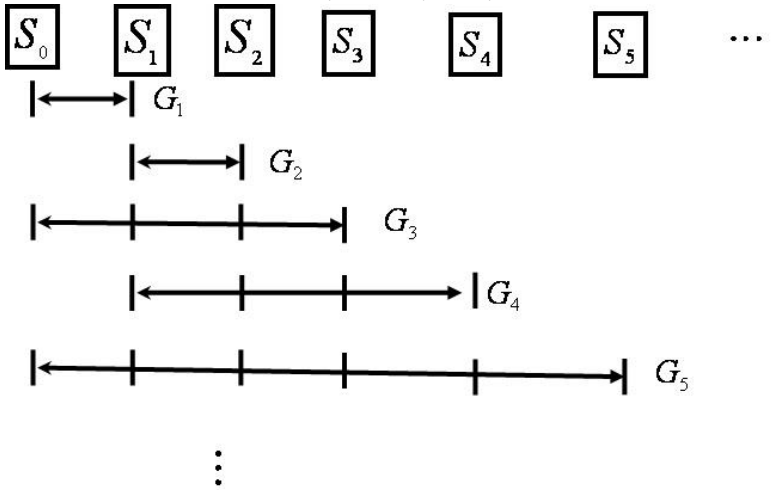


圖三：修正版方法中產生分享影像步驟之流程圖[1]

在秘密影像重建階段，要先判斷要重建的秘密影像的奇偶數，假若是要重建的秘密影像 S_i 的 i 值為奇數，則秘密影像的產生方式為 $S_0 \oplus S_1 \oplus \ldots \oplus S_i$。假若是要重建的重建的秘密影像 S_i 的 i 值為偶數，則秘密影像的產生方式為 $S_1 \oplus S_2 \oplus \ldots \oplus S_i$。秘密影像的重建方式如下面的公式所示：

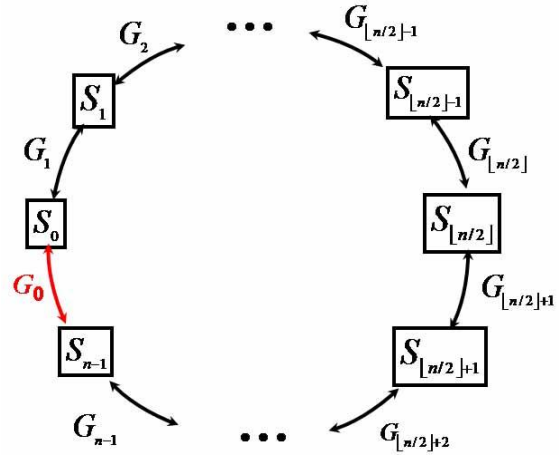
$$G_i = \begin{cases} \Psi_{k=(n+1) \bmod 2}^{n} S_k & \text{假如} i = 0, \\ \Psi_{k=(i+1) \bmod 2}^{i} S_k & \text{其他情況} \end{cases} \tag{5}$$

我們將此修改方法中，秘密影像與分享影像之間的關係，顯示於圖四。



圖四：修正方法中分享影像與秘密影像的關係圖

根據圖四可以發現，與第一小節方法一樣，當分享影像編號的號碼值越小，其重要性也越高，此趨勢與第一小節方法相同。只不過在修正的方法中，每兩個分享影像的重要性會一樣。更精確的說明，我們將每兩個分享影像分成一群，也就是分享影像 S_0 與 S_1 屬於第一群，分享影像 S_2 與 S_3 屬於第二群，依此類推。第一群內的分享影像 S_0 與 S_1 其重要性是一樣重要的。但是群與群之間的重要性，則是前面群的分享影像會比後面群的分享影像來的重要，也就是第一群的分享影像會比第二群的分享影像還要重要。

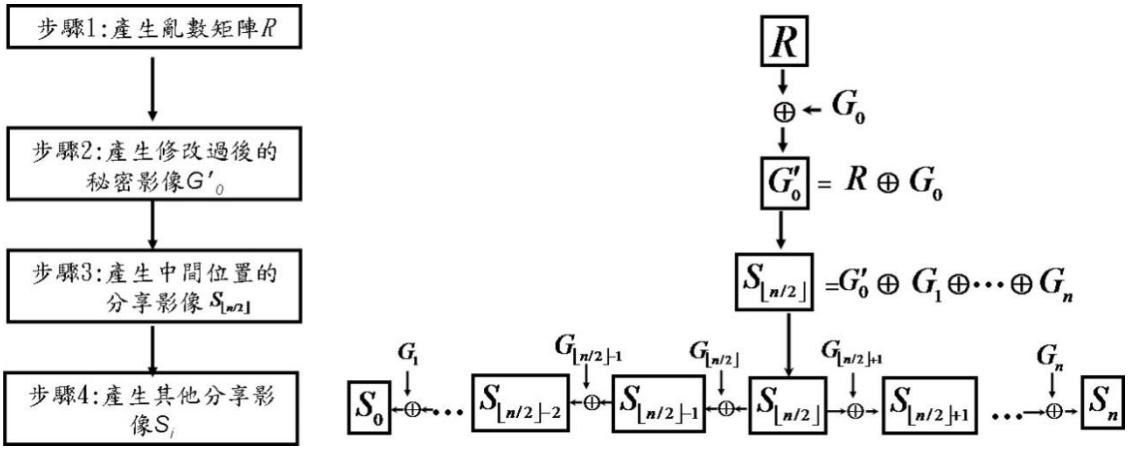


圖五：分享影像與秘密影像的環狀關係[1]

參、環狀式多秘密影像分享技術

為了發展具相同重要性的分享影像，Chan 等學者[1]提出「環狀式多秘密影像分享技術」，其目標是要將分享影像與秘密影像的關係，設計成如圖五的環狀關係。在圖五中，任何秘密影像 G_i 是利用兩張分享影像 S_{i-1} 與 S_i 執行 XOR 運算而得。所以，每一張分享影像只會跟兩張秘密影像有關係。在此模型底下，假如某一分享影像擁有者拒絕與其他擁有者合作，只會導致兩張秘密影像無法重建。

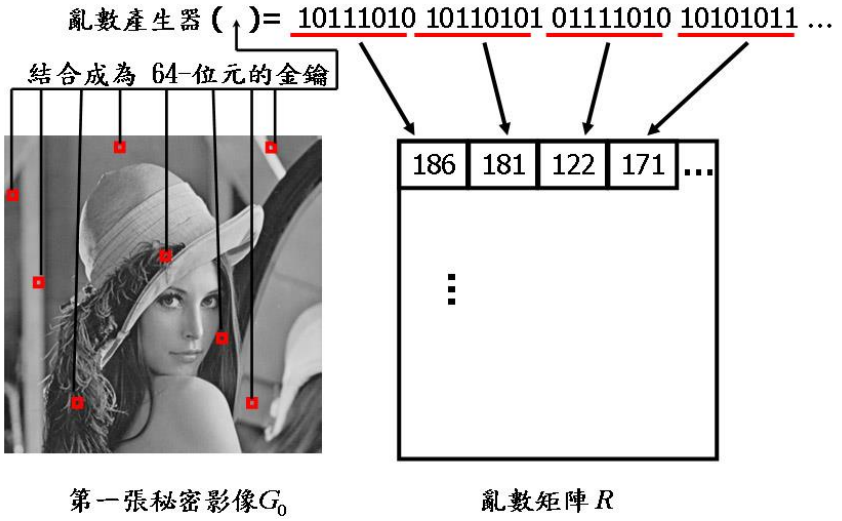
我們接著介紹 Chan 等學者的方法。在 Chan 等學者的方法包含四個步驟，如圖六所示：



圖六：Chan 等學者方法的流程圖[1]

第一個步驟是產生亂數矩陣 R，如圖七所示。首先第一張秘密影像的中心位置的像素被拿出來當作是亂數的種子，來產生八個亂數以決定八個位置，而後這八個位置的像

素被組合起來當作亂數的種子，來產生一連串與秘密影像一樣大小的的亂數，經由這些亂數，便可以組成第一步驟所要的亂數矩陣 R。



圖七：亂數矩陣 R 的產生方式[1]

接著第二步驟產生第一張修改過的秘密影像 G'_0。其產生方式，是將第一張秘密影像與第一階段所產生的亂數矩陣，執行 XOR 運算。值得注意的事，是第一階段用來當種子來產生亂數的這些像素，並不參與 XOR 運算，如此可以保證亂數矩陣 R 可以由修改過的秘密影像 G'_0 產生。亂數矩陣可以由秘密影像 G'_0 來產生的目的，是為了要讓秘密影像重建程序，有能力將修改過的秘密影像 G'_0，轉換回秘密影像 G_0。產生第一張修改過的秘密影像 G'_0 之程序，公式(6)所示：

$$G'_0 = R \oplus G_0 \tag{6}$$

第三步驟則是產生中間的分享影像 $S_{\lfloor n/2 \rfloor}$，其產生方式是依照公式(7)所示：

$$S_{\lfloor n/2 \rfloor} = G'_0 \oplus \Psi_{k=1}^{n-1} G_k \tag{7}$$

其中 n 代表的是所有秘密影像的個數。

第四步驟則是產生其他的分享影像。分享影像依據中間的分享影像 $S_{\lfloor n/2 \rfloor}$，切割成前半部分享影像(編號小於 $\lfloor n/2 \rfloor$)與後半部分享影像(編號大於 $\lfloor n/2 \rfloor$)。前半部與後半部的產生並不一樣，其產生方式如公式(8)所示：

$$S_i = \begin{cases} G_{i+1} \oplus S_{i+1} & \text{假如 } 0 \le i < \lfloor n/2 \rfloor, \\ G_i \oplus S_{i-1} & \text{假如} \lfloor n/2 \rfloor < i \le n-1. \end{cases} \tag{8}$$

最後，n 個分享影像皆可以得到。由公式(6)-(8)可以知道，每一個分享影像都包含修改過的秘密影像 G'_0， 所以每一個分享影像也是雜亂的影像，並不會有任何的秘密影像的資訊被洩漏在分享影像上。

在秘密影像的重建階段，除了修改過的秘密影像 G'_0 較特別外，其他的秘密影像皆

是利用相同的方式重建。我們將重建 G'_0 以及其他的秘密影像的方式，列於公式(9)與公式(10)。

$$G_i = S_{i-1} \oplus S_i. \quad (\text{假如 } 0<i\leqq n\text{-}1) \tag{9}$$

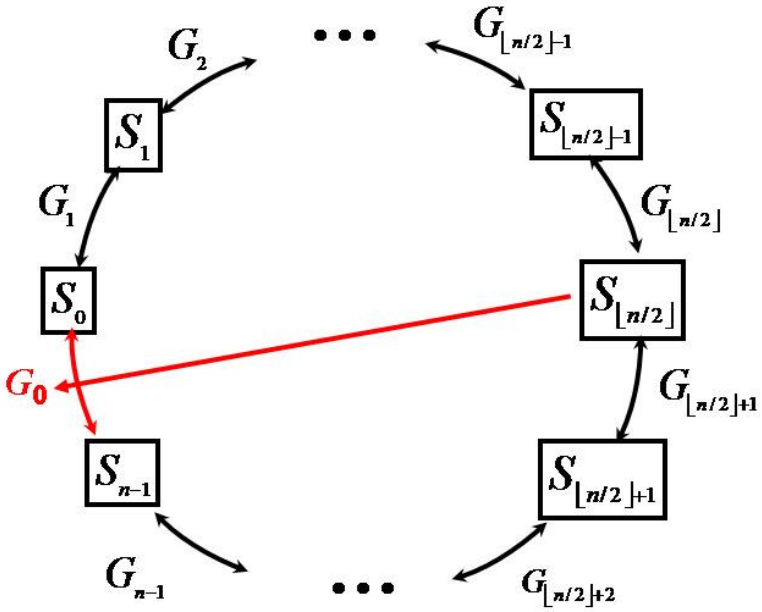
$$G'_0 = S_0 \oplus S_{n-1} \oplus S_{\lfloor n/2 \rfloor}. \tag{10}$$

當修改過的秘密影像 G'_0 從公式(10)中還原後，將修改過的秘密影像 G'_0 中心位置的像素拿出來當作是亂數的種子，以產生八個亂數以決定八個位置，而後這八個位置的像素被組合起來當作亂數的種子，來產生一連串與秘密影像一樣大小的的亂數，經由這些亂數，便可以組成第一步驟所要的亂數矩陣 R。接著對秘密影像 G'_0 與亂數矩陣 R 執行 XOR 運算，便可以重建回第一張秘密影像 G_0。其公式如下所示：

$$G_0 = G'_0 \oplus R. \tag{11}$$

如此，所有的秘密影像皆可以順利重建。

我們將 Chan 等學者的方法所產生的分享影像與秘密影像之間的關係，顯示於圖八中。根據圖八可以發現，除了分享影像 $S_{\lfloor n/2 \rfloor}$ 會與 3 張秘密影像有關以外，其他的分享影像只會與 2 張秘密影像有關，所以此方法所產生的的分享影像，幾乎已經具有相同的重要性。



圖八：Chan 等學者的方法中分享影像與秘密影像的關係圖

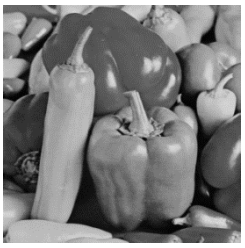
肆、秘密影像分享技術之比較

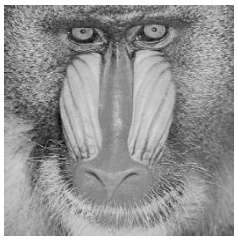
我們在此節描述種分享技術之比較。首先在實驗結果方面，兩種方法皆是利用四張實驗圖 Lena、Pane、Pepper 與 Baboon 來進行實驗，這四張圖分別用來當作秘密影像，

如圖九所示。每張圖的大小為 512×512 個像素，分別用 G_0、G_1、G_2 與 G_3 來表示。


(a) Lena
(秘密影像 G_0)

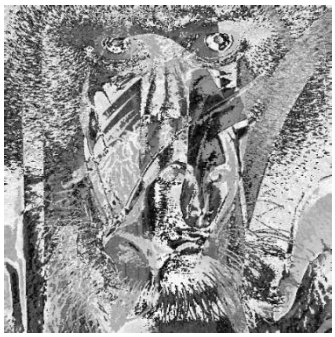

(b) Plane
(秘密影像 G_1)

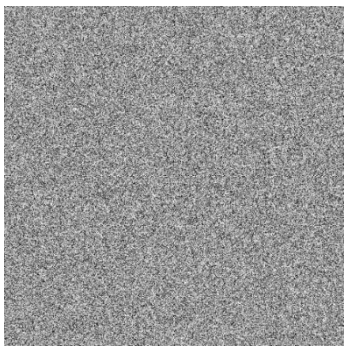

(c) Pepper
(秘密影像 G_2)

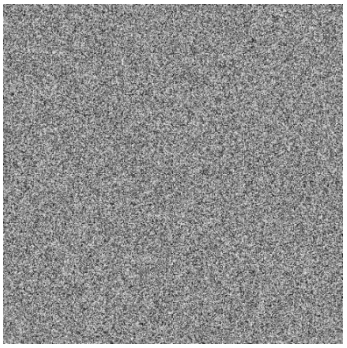

(d) Baboon
(秘密影像 G_3)

圖九：實驗影像

利用「階層式多秘密影像分享技術」與「環狀式多秘密影像分享技術」所得到的分享影像如圖十所示。由圖十(a)可以發現，Chen 與 Wu 學者的「階層式多秘密影像分享技術」所產生的分享影像，對於不夠複雜的秘密影像，會導致分享影像洩漏秘密影像的部份資料。而 Chen 與 Wu 學者的修正版的方法，會使得分享影像變成凌亂的分享影像，如圖十(b)所示。然而，所付出的代價即是必須在重建秘密影像時，要知道秘密影像的編號是奇數還是偶數，依據不同的情況，會有不同的重建方式。而 Chan 等學者的「環狀式多秘密影像分享技術」，其所產生的分享影像，皆為凌亂的分享影像，圖十(c)所示。


(a) Chen 與 Wu 學者的方法產生之分享影像


(b) Chen 與 Wu 學者的修正版方法產生之分享影像


(c) Chan 等學者的方法產生之分享影像

圖十：分享影像

接著，我們比較不同方法間的差異，並將其差異列於表一中。表一中的「是否像素擴張」特性，代表利用相對應的方法產生的分享影像，其像素是否有擴張。若像素有擴張，代表分享影像的大小，將會大於秘密影像的影像大小。所以一般狀況下，沒有擴張的方法優於有擴張的方法。此外，另外一個特性「資訊分享量」(*sharing capacity*)，代表平均一張相同大小的分享影像可以承載多少比例的秘密資料，所以此值越大，代表可以承載更多的秘密影像，也代表該技術較好。「資訊分享量」的公式如下所示：

$$\text{資訊分享量}=\frac{\text{秘密影像張數}}{\text{分享影像張數}\times\text{像素擴張倍率}}. \tag{12}$$

表一：不同方法特性的比較[1]

方法 / 特性	Wang 等學者的方法[9]	Chen 與 Wu 學者的方法[4]	Chen 學者的方法[2]	Guo 等學者的方法[5]	Chan 等學者的方法[1]
是否像素擴張	否	否	否	是	否
重建使用運算	布林運算	布林運算	加法、乘法	加法、乘法	布林運算
資訊分享量	$\frac{1}{n\times 1}$	$\frac{n}{(n+1)\times 1}$	$\frac{1}{(n)\times(1/n)}=1$	$\frac{n}{(n)\times(15/8)}=\frac{8}{15}$	$\frac{n}{(n)\times 1}=1$

因為 Chen 與 Wu 學者的方法[4]，會由 n 張秘密影像產生 n+1 張分享影像，所以其「資訊分享量」的值為 $n/(n+1)$。Guo 等學者的方法[5]中，秘密影像的每個像素值，在產生分享影像後，會變成 15 個位元，因此“像素擴張”為 15/8。Chen 學者的方法[2]所產生的分享影像之大小，與分享影像的個數有關，假如分享影像的個數為 n，則分享影像之大小為秘密影像大小的 1/n。而 Chan 等學者的方法[1]，會由 n 張秘密影像產生 n 張分享影像，所以其「資訊分享量」的值為 n/n，等於 1。

表二：分享影像的重要性[1]

	S_0	S_1	S_2	…	$S_{\lfloor n/2\rfloor-1}$	$S_{\lfloor n/2\rfloor}$	$S_{\lfloor n/2\rfloor+1}$	…	S_{n-1}	S_n
Wang 等學者的方法 [9]	1^*	1^*	1^*	…	1^*	1^*	1^*	…	1^*	X
Chen 與 Wu 學者的方法[4]	n-1	n	n-1	…	$\lfloor n/2\rfloor-2$	$\lfloor n/2\rfloor-1$	$\lfloor n/2\rfloor$	…	2	1
Chen 學者的方法[2]	1^*	1^*	1^*	…	1^*	1^*	1^*	…	1^*	X
Guo 等學者的方法 [5]	2	2	2	…	2	2	2	…	2	X
Chan 等學者的方法[1]	2	2	2	…	2	3	2	…	2	X

接著，我們比較不同方法間，分享影像的重要性，列於表二中。在表二中的數字，代表該張分享影像的擁有者拒絕與其他人合作，會有多少張秘密影像無法重建。在這些方法中，只有 Chen 與 Wu 學者的方法[4]會產生 n+1 張分享影像，所以在表二中只有

Chen 與 Wu 學者的方法之分享影像 S_n 有值，其他方法皆無。另外 Chen 學者的方法[2]與 Wang 等學者的方法[9]是由單一張秘密影像分享而產生多張分享影像，所以每一張分享影像皆跟此秘密影像有關連，是故在表二中這兩個方法的數值皆為 1，並且以「*」來表示此為單張秘密影像。

伍、結論

在本文中，我們介紹「多秘密影像分享技術」。在所有的「多秘密影像分享技術」中，我們挑選了兩個低運算量的技術來介紹。這兩個技術，依據其不同的目的，發展「階層式多秘密影像分享技術」與「環狀式多秘密影像分享技術」。「階層式多秘密影像分享技術」所產生的分享影像，有不同的重要性，此技術適用於要產生不同重要性給不同階級的人。握有較重要的分享影像的擁有者，當其拒絕與其他擁有者合作時，會導致大部分的秘密影像無法重建回來。而「環狀式多秘密影像分享技術」所產生的分享影像，具有相同的重要性，此技術適用於要產生相同重要性給相同階級的人。所以任何一張分享影像擁有者拒絕合作，只會導致固定張數的秘密影像無法重建回來。根據秘密影像分享技術之比較，可以知道這兩種方法是所有比較的方法中，具有低運算量優點的技術，且可以達到分享影像的重要性需求(即分享影像不同重要性或相同重要性)的多秘密影像分享技術。

參考文獻

[1] C. C. Chan, Y. C. Chou, Y. H. Chen, and Y. Y. Tsai " Role-Balance Based Multi-Secret Images Sharing using Boolean Operations," *KSII Transactions on Internet and Information Systems*, vol. 8, no. 5, pp. 1785-1800, 2014.

[2] W. K. Chen, "Image Sharing Method for Gray-level Images," *Journal of Systems and Software*, vol. 86, no. 2, pp. 581-585, 2013.

[3] J. Chen, Y. S. Chen, H. C. Hsu, and H. W. Chen, "New Visual Cryptography System Based on Circular Shadow Image and Fixed Angle Segmentation," *Journal of Electronic Imaging*, vol. 14, no. 3, pp. 0330181 - 033018-5, 2005.

[4] T. H. Chen and C. S. Wu, "Efficient Multi-secret Image Sharing based on Boolean Operations," *Signal Processing*, vol. 91, pp. 90-97, 2011.

[5] C. Guo, C. C. Chang, N. Ma, and C. Qin, "A Multi-threshold Secret Image Sharing Scheme Based on MSP," *Pattern Recognition Letters*, vol. 33, pp. 1594-1600, 2012.

[6] M. Naor and A. Shamir, "Visual Cryptography," *Lecture Notes in Computer Science*, vol. 950, pp. 1-12, 1994.

[7] A. Shamir, "How to Share a Secret," *Communication of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[8] S. J. Shyu, S. Y. Huang, Y. K. Lee, and R. Z. Wang, "Sharing Multiple Secrets in Visual Cryptography," *Pattern Recognition*, vol. 40, no. 12, pp. 3633-3651, 2007.

[9] D. Wang, L. Zhang N. Ma, and X. Li, "Two Secret Sharing Schemes Based on Boolean Operations," *Pattern Recognition*, vol. 40, no. 10, pp. 2776-2785, 2007.

[10] H. C. Wu and C. C. Chang, "Sharing Visual Multi-secrets using Circle Shares," *Computer Standards & Interfaces*, vol. 134, no. 28, pp. 123-135, 2005.

[11] C. C. Wu and L. H. Chen, "A Study on Visual Cryptography," Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, 1998.