一個可多次使用且具安全性及有效率之一般多重機密影像分享機制

A Multi-Use Secure and Efficient Multi-Secret Images Sharing Scheme for General Access Structure

林鈺庭
國立暨南國際大學資訊工程學系
s95321015@ncnu.edu.tw

阮夙姿*
國立暨南國際大學資訊工程學系
jsjuan@ncnu.edu.tw

摘要—多重機密影像分享機制是處理多張機密影像。如何同時分配給一群參與者一些分享影像或秘密片段，並且藉由合法的參與者所持有的分享影像或秘密片段，即可還原合法的原始的機密影像;而非合法之任何部分參與者子集合，皆無法還原任何影像。很多相關研究皆探討機密影像分享技術，然而其研究大部分皆只適用於特殊的授權者集合或者只能分享單張灰階機密影像。在 2008 年，Shyu 和 Chen 提出針對一般授權者集合所設計的多重機密影像分享機制，但是其機制上存在一個缺失，集合一群不合法的參與者子集合，將可能解出其它合法的參與者集合的機密影像。因此，在 2009 年 Lee 和 Juan 改善了 Shyu 和 Chen 機制的不安全，也降低時間複雜度以及公佈的公開影像大小。然而，在 Shyu 和 Chen 以及 Lee 和 Juan 所提出的方法中，其演算法依舊含有較高的計算量，而且無法達到多次使用的目的。因此，本文利用兩變數的單向雜湊函數，設計出針對任意一般授權者集合，可使用於灰階或彩色圖像的多重機密影像分享機制，使得計算量以及功能性上皆明顯優於先前的研究。另外，本文也針對簡和陳於 2006 年提出之機制提出改善，使得其公佈的公開影像可減少一張，降低公佈成本的花費。

關鍵詞—多重機密影像分享機制、秘密片段、授權者集合、多次使用、兩變數的單向雜湊函數。

***Abstract*—Multiple secret images sharing scheme deals with the problem that how to secretly distribute several secret images among a group of participants at the same time, and reconstruct these secret images by collecting the shared images or the shares held in qualified subsets. Many studies explore the technique about the secret image sharing, but most of them only can be applied in special access structure or distributed single gray-level image. Shyu and Chen proposed multiple secret images sharing scheme for general access structure in 2008, but there may exists an unqualified subset which can reconstruct the secret images that should not be reconstructed by them in their scheme. Hence, Lee and Juan solved this insecure situation. In the mean time, they also reduced the time complexity, and the sizes of the public image are smaller than those for Shyu and Chen's scheme. However, the computation of Shyu and Chen's scheme and Lee and Juan's scheme still can be reduced, and they both do not achieve the property of multi-use. Therefore, this paper uses two-variables one-way hash function to design a multiple secret images sharing scheme for general access structure, and makes the cost of computation and capability are better than the previous results. Besides, this paper also improve Jian and Chen's**

* Corresponding author. Tel.: +886-49-2910960 ext.4875.

scheme held in 2006 that makes the number of the public images less than that of Jian and Chen's scheme, so the cost can be decreased.

Keywords—multi-secret images sharing scheme, share, access structure, multi-use, two-variable one-way hash function.

一、簡介

隨著網路的蓬勃發展，人們愈來愈依賴網路來傳播資訊，但在傳遞機密資料的過程中，機密資料若被惡意的攻擊者所擷取，則會導致企業嚴重的損失或是國家安全遭受威脅。因此，資料傳輸的安全性也愈來愈受重視。為了保護機密資料洩漏的問題，機密資料的擁有者常事先將資料進行加密，再傳送之。之後，即使傳送中的資料被竊取，仍無法得知機密資料的任何相關資訊。在 1979 年， Blakley [2] 和 Shamir [7] 兩學者分別以不同的方法提出秘密分享機制 (*Secret sharing scheme*)，使得機密資料能分散地保管。其主要的想法是將一機密透過分配演算法，產生 n 個秘密片段(*Share*)並分配給 n 位參與者 (*Participant*)，使得每位參與者皆可得到有關於此機密的部分秘密片段。當合法的參與者交出各自的秘密片段，即可經計算還原機密。

Shamir 所設計的 (t, n)-門檻值秘密分享機制((t, n)-*threshold secret sharing scheme*)，其中 $t \le n$，是以 Lagrange 多項式插入法為基礎。此機制可將一機密分配給 n 位參與者，使得集合任意 t 位或 t 位以上的參與者，即可還原此機密; 反之，小於 t 位的參與者將無法得知此機密的任何資訊。其中可還原機密的參與者集合稱之為合法子集合 (*Qualified subset*)。1992 年，Noar 與 Shamir [6]利用人類視覺敏銳度的弱點，提出視覺密碼 (*Visual cryptography*)。其機制於還原時只需重疊足夠的分享影像，即可還原機密影像，然而還原的機密影像會產生失真以及影像擴大的問題。因此，在 2002 年 Thien 和 Lin [9] 兩學者將 Shamir 的秘密分享技術運用於影像分享上，其機制可解決還原影像所產生的失真與擴大之問題，但是其機制無法同時分享多張機密影像。

2006 年，簡和陳 [1] 兩學者提出多重灰階機密影像分享機制，其機制運用 Thien 和 Lin [9]的概念，進一步推演出可同時分享多張機密影像，而且不會使參與者所持有的分享影像份數增加。然而其機制所分享的多張機密影像須一致，且還原的影像具有失真的問題。此外，[9] 和 [1] 所提出的機制皆只能分享灰階影像，而且也無法適用於任意一般的授權者集合。所謂授權者集合 (*Access structure*) Γ 為所有合法子集合的集合。假設一個合法子集合 $A \in \Gamma$，則 A 的超集合 (*Superset*) 也會是一個合法子集合。換句話說，授權者集合應滿足單調遞增之特性 (*Monotone increasing property*): 若 $A \in \Gamma$ 且 $A \subseteq B \subseteq P$，則 $B \in \Gamma$。最小授權者集合(*Minimal access structure*) $\Gamma' \subseteq \Gamma$ 定義為 $\Gamma' = \{A \in \Gamma: A' \not\subset A \ \forall \ A' \in \Gamma - \{A\}\}$。

由於前人所提出的影像分享機制皆只適用於特殊授權集合而且並無實作出彩色影像，因此 Shyu 和 Chen [8] 在 2008 年提出針對一般授權者集合所設計的多重機密影像分享機制。其機制可分享多張彩色機密影像之外，也適用於一般授權者集合。然而卻潛藏著不安全的情況，以及其公開影像之大小可能較原始機密影像大。因此，在 2009 年，Lee 和 Juan [5] 改進 Shyu 和 Chen 機制中的不安全部分，同時也提昇了演算法的效率。另外，其機制的公開影像之大小與每張機密影像之大小相同。然而 Lee 和 Juan 機制中的所有運算是建立於 GF(p^m) 上，其中 p 為夠大的質數，m 為正整數。因此其演算法的計算量較高。此外，[8] 與 [5] 中每位參與者所持有的秘密片段皆為一對數值(大小為 O(p^2))。基於上述問題，本文首先改進 [1]，降低其公佈資訊量;接著提出一個簡易、安全且可多次使用之機

制，以針對任意一般授權者集合，分配多張彩色或灰階機密影像，使得每位參與者只需要持有一個數值(大小為 $O(p)$)作為秘密片段，並且降低了演算法之計算量。

本文接下來三章節安排如下:首先於第二章說明兩變數的單向雜湊函數之特性。其次，於第三章的相關研究中略述簡和陳 [1] 的多重機密影像分享機制以及 Lee 和 Juan [5] 的多重機密影像分享機制。主要成果列於第四章，分別提出一個改進 [1] 的機制，以及針對一般授權者集合所設計的可多次使用之多重機密影像分享機制。定義針對所提出的機制實作進行測試，並將實驗結果於第五章陳述。第六章為分析前人所提出的機制與我們的機制，以作優劣比較。最後於第七章，描述本文結論與未來研究方向。

二、預備知識

由於本文針對一般授權者所設計的多重機密影像分享機制的主要想法是利用兩變數的單向雜湊函數之特性為核心，因此以下先介紹此其雜湊函數的特性。假設 $h(e, v)$ 為兩變數的單向雜湊函數，特性如下，可參考文獻 [3] 中之詳細證明特性。

(1) $h(e, v)$ 會產生固定長度的位元串。
(2) 已知 e 與 v，可以很輕易的計算出 $h(e, v)$。
(3) 已知 v 與 $h(e, v)$，不容易計算出 e。
(4) 已知 e 與 $h(e, v)$，不容易計算出 v。
(5) 在不知 v 的情況下，對於任意的 e，不容易計算出 $h(e, v)$。
(6) 已知 v，但不容易找出兩個不同值 e_1 與 e_2 使得 $h(e_1, v) = h(e_2, v)$。
(7) 已知多組 e_i 與 $h(e_i, v)$，在 $e_0 \neq e_i$ 時不容易計算出 $h(e_0, v)$。

三、相關研究

在本章中，首先回顧簡和陳 [1] 兩學者所提出的 (t, n)-門檻值之多重灰階機密影像分享機制，於本文中簡稱為 JC 機制。其次，回顧 Lee 和 Juan [5] 提出的一般授權者集合之多重機密影像分享機制，於本文中簡稱為 LJ-G。假設 $P = \{P_i \mid 1 \le i \le n\}$ 為 n 位參與者的集合，$Q = \{I_j \mid 1 \le j \le s\}$ 為 s 張機密影像的集合，其中機密影像 I_j 之大小為 $w_j \times h_j$。注意，每張機密影像的大小可以是不同的。

(一) JC 機制

JC 機制 的運算皆於 GF(251)中，且每張機密影像之大小皆相等。此機制分為機密影像之張數小於門檻值以及機密影像之張數大於或等於門檻值兩個部分。於此節僅略述機密影像之張數大於或等於門檻值之情況，簡稱為 JC ($s \ge t$)機制。

在分配階段，分配者首先對所有 $1 \le j \le s$，將機密影像 I_j 中，大於 250 的像素值皆設定成 250，形成截斷影像 I_j'。其次，建構 s 次多項式 $f_j^m(x) = a_{s_m} x^s + \ldots + a_{1_m} x + a_{0_m}$ ，其中 a_{j_m} 為截斷影像 I_j' 的第 m 個像素值，而 a_{0_m} 為隨機亂數，$1 \le j \le s$，$1 \le m \le N$，其中，$N = w_j \times h_j$ 為截斷影像 I_j' 之大小。之後，分配者任選相異 x_i 值，$1 \le i \le n + s - t + 1$，其中 $x_1, x_2, \ldots, x_n$ 分別為參與者 $P_1, P_2, \ldots, P_n$ 之識別碼，並且將 x_i 代入多項式 $f_j^m(x)$。最後，分配者將 $y_{i_m} = f_j^m(x_i)$ 合併成分享影像 $Y_1, Y_2, \ldots, Y_n, Y_{n+1}, \ldots, Y_{n+s-t+1}$，其中 $Y_1, Y_2, \ldots, Y_n$ 分別分配給參與者 $P_1, P_2, \ldots, P_n$，而剩餘的 $Y_{n+1}, \ldots, Y_{n+s-t+1}$ 為公開影像。若要還原截斷影像 I_j'，則需取回公開的分享影像 $Y_{n+1}, \ldots, Y_{n+s-t+1}$ 以及從參與者 $P_1, P_2, \ldots, P_n$ 持有的 $Y_1, Y_2, \ldots, Y_n$ 任意收集 t 張分享影像，即可還原截斷影像 I_j'。

(二) LJ-G

LJ-G 的運算皆於 GF(2^8)中。令 $\Gamma_j' = \{A_{j,u} \mid 1 \le u \le |\Gamma_j'|\}$ 為機密影像 I_j 所對應的最小授權者集合，$1 \le j \le s$ 。其中，合法子集合 $A_{j,u} = \{P_{j,u,1}, P_{j,u,2}, \ldots, P_{j,u,|A_{j,u}|}\}$，$1 \le j \le s$，$1 \le u \le |\Gamma_j'|$。

在分配階段，首先分配者會隨機亂數選取 (x_i, y_i) 並分配給參與者 P_i，$1 \le i \le n$。其次，分配者集合參與者 $P_{j,u,k} \in A_{j,u}$ 的 ($x_{j,u,k}$, $y_{j,u,k}$) 利

用 Lagrange 多項式插入法公式還原$|A_{j,u}|-1$次多項式$f_{j,u}(x)=a_{|A_{j,u}|-1}x^{|A_{j,u}|-1}+...+a_1x+a_0$，並選擇 s 個合適的片段大小 d_j，用其切割所對應的機密影像 I_j 以造出 α_j 個 (d_j − 1) 次多項式 $g_j^{\alpha}(x)=\sum_{\beta=1}^{d_j}z_j^{\alpha,\beta}x^{d_j-\beta}$，其中 $z_j^{\alpha,\beta}$ 為機密影像 I_j 的第 α 片段之第 β 個像素值，$1\le\alpha\le l_j=w_j\times h_j/d_j$。之後，分配者使用多項式 $f_{j,u}(x)$ 進而建構 (d_j − 1) 次多項式 $f'_{j,u}(x)=b_{d_j-1}x^{d_j-1}+...+b_1x+b_0$，其中 $b_c=a_{(c \bmod |A_{j,u}|)}$，$0\le c<d_j-1$ 且 $b_{d_j-1}=a_{|A_{j,u}|-1}$。接下來分配者再計算 $h_{j,u}^{\alpha}(x)=A\times(B+g_j^{\alpha}(x))$，其中，若 $\alpha=1$ 時，則 $A=b_{d_j-1}$，$B=f'_{j,u}(x)$；反之，$B=f'_{j,u}(x)+h_{j,u}^{\alpha-1}(x)$。而且當 $z_j^{\alpha-1,\omega}+b_{d_j-1-\omega}=0$ 時，$A=z_j^{\alpha-1,\omega}$；當 $z_j^{\alpha-1,\omega}+b_{d_j-1-\omega}\neq 0$ 時，$A=z_j^{\alpha-1,\omega}+b_{d_j-1-\omega}$，其中 $\omega=(\alpha-1)\bmod d_j$，$1\le j\le s$，$1\le u\le|\Gamma'_j|$，$1\le\alpha\le l_j$。最後，分配者會合併所有多項式 $h_{j,u}^{\alpha}(x)$ 的所有係數，進而形成公開影像 $H_{j,u}$，$1\le j\le s$，$1\le u\le|\Gamma'_j|$，$1\le\alpha\le l_j$。

若要還原機密影像 I_j 則可利用公佈欄的公開資訊並且集合參與者 $P_{j,u,k}\in A_{j,u}$ 的 ($x_{j,u,k}$, $y_{j,u,k}$)，即可還原多項式 $f_{j,u}(x)$ 與 $f'_{j,u}(x)$。其次，使用片段大小 d_j 切割所對應的公開影像 $H_{j,u}$ 形成數個多項式 $h_{j,u}^{\alpha}(x)$，用其反推出數個多項式 $g_j^{\alpha}(x)$，$1\le j\le s$，$1\le u\le|\Gamma'_j|$，$1\le\alpha\le l_j$。最後，將所有多項式 $g_j^{\alpha}(x)$ 的係數合併，即可還原機密影像 I_j。

四、主要成果

在本章中，我們將提出二個多重機密影像分享機制，其一為改進簡與陳 [1] 之 JC 機制，簡稱為 IJC 機制，使其所公佈的公開影像與 JC 機制在 $s\ge t$ 的情況下相比會減少一張公開影像；其二為針對一般授權者集合所設計的多重機密影像分享機制，簡稱為 GMSISS。其中 GMSISS 主要的想法是利用兩變數的單向雜湊函數的特性所設計，使其達到可多次使用的目的。而且 GMSISS 可避免在 Shyu 和 Chen 機制 [8] 中，不合法的子集合可解出不應解出的機密影像之問題，且運算量之每個參與者持有之秘密片段的大小皆優於 [5] 之 LJ-G 機制。假設 $P=\{P_i\mid 1\le i\le n\}$ 為 n 位參與者的集合，$Q=\{I_j\mid 1\le j\le s\}$ 為 s 張機密影像的集合。

(一) IJC 機制

本節機制針對相關研究 JC ($s\ge t$)機制提出改善，其改進之處為將原先的 s 次多項式 $f_j^m(x)=a_{s_m}x^s+...+a_{1_m}x+a_{0_m}$ 改成 $s-1$ 次多項式 $f'^m_j(x)=a_{s-1_m}x^{s-1}+...+a_{1_m}x+a_{0_m}$，其中多項式 $f'^m_j(x)$ 的各係數分別為截斷影像 I'_j 的第 m 個像素值，使得改進後的 IJC 機制所需公佈的公開影像會比 JC ($s\ge t$)機制減少一張。計算量也將因此稍降，而其安全性將不變。

(二) GMSISS

設每張機密影像 I_j 會分享於對應的授權者集合 $\Gamma_j=\{A\subseteq P\mid B\subseteq A\ \exists\ B\in\Gamma'_j\}$，其中 $\Gamma'_j=\{A_{j,u}\mid 1\le j\le s, 1\le u\le|\Gamma'_j|\}$ 為機密影像 I_j 所對應的最小授權者集合，$1\le j\le s$。其中合法子集合 $A_{j,u}=\{P_{j,u,1}, P_{j,u,2}, \ldots, P_{j,u,|A_{j,u}|}\}$，$1\le j\le s$，$1\le u\le|\Gamma'_j|$，將能夠還原機密影像 I_j。本機制可分為初始化、分配演算法與還原演算法三部份，分別描述如下:

初始化：

可信賴的分配者會將每張機密影像 I_j 給予編號 j，$1\le j\le s$;並於 GF(p) 中，隨機亂數選取 n 個公開、不重覆且非零的亂數作為參與者 P_i 唯一識別碼 ID_i 以及 n 個不公開的秘密片段 y_i，其中 $1\le i\le n$，而 p 是一個夠大的質數。本方法之計算皆於 GF(p)中。

分配演算法：

可信賴的分配者會依據每一個合法子集合 $A_{j,u}\in\Gamma'_j$ 處理所對應的機密影像 I_j 進而產生 $A_{j,u}$ 的公開影像 $H_{j,u}$。

1. 分配者亂數公佈一個隨機亂數 r 於公佈欄。
2. 分配者計算每一個合法子集合 $A_{j,u}=\{P_{j,u,k}\mid 1$

$\le j \le s$，$1 \le u \le |\Gamma'_j|$，$1 \le k \le |A_{j,u}|\} \in \Gamma'_j$ 的 $\text{seed}_{j,u}$ 如下:

$$\text{seed}_{j,u} = \bigoplus_{P_{j,u,k} \in A_{j,u}} h(\sum_{P_{j,u,k} \in A_{j,u}} \text{ID}_{j,u,k} + r + j, y_{j,u,k}) \quad (1)$$

其中，$h(,)$為兩變數的單向雜湊函數，r 為公佈的隨機亂數值，j 為欲還原的機密影像之編號。

3. 分配者將 $\text{seed}_{j,u}$ 作為亂數種子，使其產生置換序列，用此序列作為置換依據，進而置換機密影像 I_j 的像素，$1 \le j \le s$，$1 \le u \le |\Gamma'_j|$。

<u>還原演算法：</u>

根據公佈欄上的隨機亂數 r 使得機密影像 I_j 可由任一個合法子集合 $A_{j,u} \in \Gamma'_j$ 來還原，$1 \le j \le s$，$1 \le u \le |\Gamma'_j|$。方法如下:

1. 每一個參與者 $P_{j,u,k} \in A_{j,u}$ 計算 $h_{j,u,k} = h(\sum_{P_{j,u,k} \in A_{j,u}} \text{ID}_{j,u,k} + r + j, y_{j,u,k})$。
2. 任一個參與者 $P_{j,u,k} \in A_{j,u}$ 接收全部 $P_{j,u,k} \in A_{j,u}$ 所算出之 $h_{j,u,k}$ 值，計算合法子集合 $A_{j,u}$ 的 $\text{seed}_{j,u} = \bigoplus_{P_{j,u,k} \in A_{j,u}} h_{j,u,k}$。
3. 任一個參與者 $P_{j,u,k} \in A_{j,u}$ 可從公佈欄上取得合法子集合 $A_{j,u}$ 的公開影像 $H_{j,u}$。
4. 任一個參與者 $P_{j,u,k} \in A_{j,u}$ 可使用 $\text{seed}_{j,u}$ 進行反置換公開影像 $H_{j,u}$ 進而求得機密影像 I_j。

五、實驗結果

本文的實驗環境於 Windows XP 作業系統，使用 Visual Studio 2005 for C# 程式開發環境實作本文所提出的方法。由於第四章之第一小節的改進，很顯然可以減少公佈一張公開影像; 因此，於本章中，只針對第四章之第二小節所提出的方法進行實驗測試來驗證所提出的方法之可行性與正確性。本實驗所測試的每一張機密影像其寬度與高度是可以不一致的。

我們假設四位參與者 $P = \{P_1, P_2, P_3, P_4\}$ 分享兩張機密影像 $Q = \{I_1, I_2\}$，其分別是編號 $j = 1$ 之 512×512 "*Baboon*" 與編號 $j = 2$ 之 192×321 "*Ncnu*"，如圖 1 的 (a) 與 (b) 所示。依據機密影像給定其最小授權者集合分別為 $\Gamma'_1 = \{A_{1,1}, A_{1,2}\}$ 與 $\Gamma'_2 = \{A_{2,1}\}$，其中 $A_{1,1} = \{P_1, P_2, P_3\}$ 與 $A_{1,2} = \{P_1, P_4\}$ 為可還原機密影像 I_1 的合法子集合，而 $A_{2,1} = \{P_1, P_4\}$ 為可還原機密影像 I_2 的合法子集合。本實驗所公佈的大質數為 $p = 1999$ 以及隨機亂數為 $r = 45$。而且，分配者會分配給每位參與者一識別碼 ID 與秘密片段 y 分別如表 1 所示。

表 1: 四位參與者之識別碼與秘密片段

	P_1	P_2	P_3	P_4
識別碼 ID	1	2	3	4
秘密片段 y	652	392	48	613

表 2 為分配者利用所公佈的隨機亂數 45 去分別計算在 $A_{1,1}$，$A_{1,2}$ 與 $A_{2,1}$ 這三組合法子集合中的各個參與者之雜湊值 $h(\sum_{P_{j,u,k} \in A_{j,u}} \text{ID}_{j,u,k} + r + j, y_{j,u,k})$，其中雜湊值是利用 MD5 雜湊演算法 (此 MD5 雜湊演算法會輸出一個訊息摘要，其組成為 16 個區塊，每一區塊有 8 個位元) 所計算而來，並且對此計算結果取模 1999。

表 2: $A_{1,1}$，$A_{1,2}$ 與 $A_{2,1}$ 中各個參與者的雜湊值

	$A_{1,1}$			$A_{1,2}$		$A_{2,1}$	
參與者組合	P_1	P_2	P_3	P_1	P_4	P_1	P_4
雜湊值	1716	735	1520	869	1200	1716	515

分配者會利用各別合法子集合中所有參與者的雜湊值轉成二進位後執行互斥或 (exclusive-or) 運算，進而求得每個合法子集合的亂數種子如下：

$A_{1,1}$ 的亂數種子: $1716 \oplus 735 \oplus 1520 = 411$。

$A_{1,2}$ 的亂數種子: $869 \oplus 1200 = 6$。

$A_{2,1}$ 的亂數種子: $1716 \oplus 515 = 1207$。

之後，分配者會利用每一個合法子集合的亂數種子將其所對應的機密影像執行置換機密影像的像素，進而產生每一個合法子集合的公開影像，如圖 1 的 (c)，(d)，(e) 分別為 $A_{1,1}$，$A_{1,2}$，$A_{2,1}$ 的公開影像 $H_{1,1}$，$H_{1,2}$，$H_{2,1}$。

在還原時，可分別由 $A_{1,1}$，$A_{1,2}$，$A_{2,1}$ 使用

其還原的亂數種子執行反置換圖 1 的 (c)，(d)，(e) 的像素值，即可使 $A_{1,1}$，$A_{1,2}$，$A_{2,1}$ 分別求得圖 1 的 (f)，(g)，(h)。

六、效能分析與比較

在本章中，我們會從安全性、效率性以及功能性，這三方面來分析 GMSISS 的效能，首先在本章的第一小節，我們會試圖說明 GMSISS 的安全性。其次，我們將 Shyu 和 Chen [8] 與 Lee 和 Juan [5] 分別設計的一般授權者集合之多重機密影像分享機制，簡稱為 SC-G 與 LJ-G，並且與我們提出的 GMSISS 做效率比較。最後，根據前人所提出的機制與我們的機制列出功能性比較。

(一)安全性

欲還原合法子集合 $A_{j,u}$ 的亂數種子 $\text{seed}_{j,u}$，則合成者必須對每位參與者 $P_{j,u,k} \in A_{j,u}$ 收集其 $h(\sum_{P_{j,u,k} \in A_{j,u}} \text{ID}_{j,u,k} + r + j, y_{j,u,k})$，其中 $y_{j,u,k}$ 為參與者 $P_{j,u,k}$ 之秘密片段。攻擊者在不知道參與者 $P_{j,u,k}$ 的秘密片段 $y_{j,u,k}$ 時是無法獲得任一合法子集合 $A_{j,u}$ 的亂數種子 $\text{seed}_{j,u}$。這是根據兩變數有單向雜湊函數的特性(5)可知的。

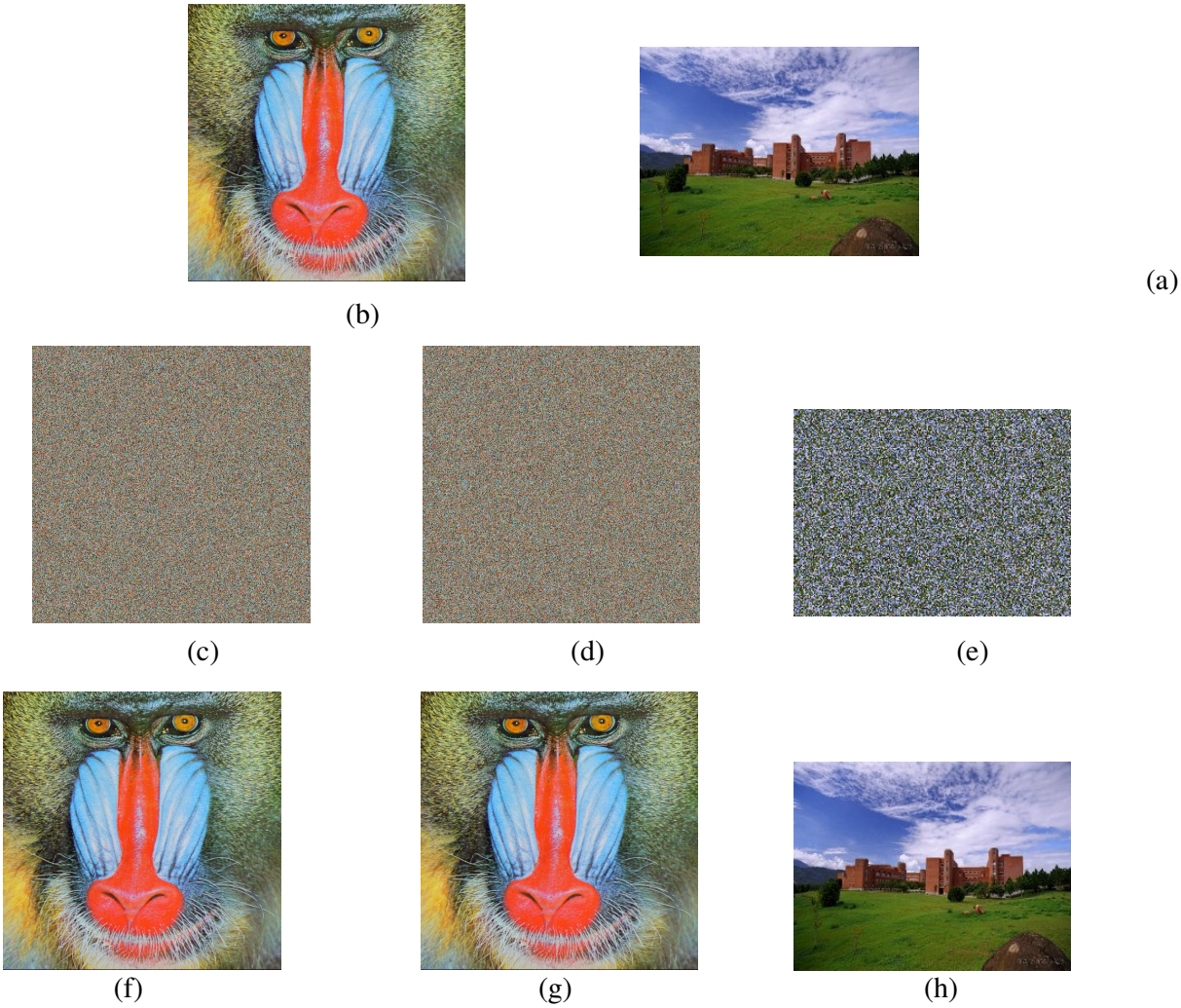

Figure 1. (a) I_1: *Baboon*; (b) I_2: *Ncnu*; (c) $H_{1,1}$: 為 $A_{1,1}$ 的公開影像; (d) $H_{1,2}$: 為 $A_{1,2}$ 的公開影像; (e) $H_{2,1}$: 為 $A_{2,1}$ 的公開影像; (f)-(h) $A_{1,1}, A_{1,2}, A_{2,1}$ 還原後的機密影像。

表 3: SC-G、LJ-G 與 GMSISS 分享多張機密影像的計算量比較表

	SC-G		LJ-G		GMSISS	
	DC	RC	DC	RC	DC	RC
+	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert}(l_j v_{j,u} + l_j d_j - l_j)$	0	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert}(2l_j d_j + l_j - d_j - 1)$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert}(l_j d_j + l_j - d_j - 1)$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert}(v_{j,u}+1)$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert}(v_{j,u}+1)$
−	0	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} l_j v_{j,u} d_j$	0	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} l_j d_j$	0	0
⊕	0	0	0	0	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert}(v_{j,u}-1)$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert}(v_{j,u}-1)$
×	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} l_j v_{j,u} d_j$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} l_j v_{j,u} d_j$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} l_j d_j$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} l_j d_j$	0	0
h	0	0	0	0	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} v_{j,u}$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} v_{j,u}$
mi	0	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} l_j$	0	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} l_j$	0	0

表 4: 表 3 之簡化表

	SC-G		LJ-G		GMSISS	
	DC	RC	DC	RC	DC	RC
+−⊕	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert}(l_j v_{j,u} + l_j d_j - l_j)$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} l_j v_{j,u} d_j$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert}(2l_j d_j + l_j - d_j - 1)$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert}(2l_j d_j + l_j - d_j - 1)$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} 2v_{j,u}$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} 2(v_{j,u}-1)$
×h	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} l_j v_{j,u} d_j$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} l_j v_{j,u} d_j$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} l_j d_j$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} l_j d_j$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} 1.2 v_{j,u}$	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} v_{j,u}$
mi	0	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} l_j$	0	$\sum_{j=1}^{s}\sum_{u=1}^{\lvert\Gamma'_j\rvert} l_j$	0	0

另外，攻擊者欲從已知的 $h(\sum_{P_{j,u,k}\in A_{j,u}} \mathrm{ID}_{j,u,k} + r + j, y_{j,u,k})$ 去嘗試求出參與者 $P_{j,u,k}$ 的秘密片段 $y_{j,u,k}$ 則是不可行的，其原因在於兩變數的單向雜湊函數存在不可逆的特性(特性(4))。另外，在 GMSISS 中利用兩變數的單向雜湊函數之特性 (7) 可避免某一參與者透過參與者彼此之間的關係進而解出其他合法子集合的機密影像。

(二) 效率性

在本節中，我們各別統計 SC-G，LJ-G 與所提出的 GMSISS 中之機密影像分配和重建演算法的計算量。表 3 為 SC-G、LJ-G 與 GMSISS 分享多張機密影像的效率比較。在表 3 中，DC 代表分配演算法的計算量、RC 代表還原演算法的計算量、+ 代表加法的計算量、− 代表減法的計算量、⊕ 代表互斥或的計算量、× 代表乘法的計算量、h 代表兩變數的單向雜湊函數的計算量、m_i 代表乘法反元素的計算量，並且假設 $v_{j,u}$ 表示為合法子集合 $A_{j,u}$ 中參與者的人數，$1 \le j \le s, 1 \le u \le \Gamma'_j$、$d_j$ 表示為將機密影像 I_j 以每 d_j 個像素為一區段、l_j 表示為機密影像 I_j 有 $l_j\,(=w_j \times h_j / d_j)$ 個區段，其中 w_j 為機密影像 l_j 之寬度，h_j 為機密影像之高度。

為了清楚地比較，我們將加法、減法與互斥或的運算合併成一個運算，因此將此三個計算量加總起來。由於一個單向雜湊函數運算時間，約為 1.2 個乘法的計算時間 [4]，故也將乘法與兩變數的單向雜湊函數的計算量加總成一個計算量如表 4 所示。

根據表 4，我們可以很容易地發現當 $l_j d_j > 2v_{j,u}$ 時，則 GMSISS 的分配演算法的計算量皆比 LJ-G 的分配與還原演算法的計算量少。一般而言，機密影像 I_j 的大小 $(=l_j d_j)$ 一定會大於合法子集合 $A_{j,u}$ 中參與者人數的兩倍。因此 GMSISS 的效率上會比 LJ-G 的效率來得好。由

表中可看出之效率比 SC-G 的效率來得好。故我們所提出的 GMSISS 也會比 SC-G 的效率來得好。

(三) 功能性

本文簡稱 Thien 和 Lin 機制為 TL 機制，並且於本節針對我們的 GMSISS 與前人的 TL、JC ($s \geq t$)、SC-G、LJ-G 列出多項特性，進而比較各機制之優缺點，以便提供使用者選擇出一個最適合的影像分享機制。如何選擇一個最適合的影像分享機制？通常使用者會以低成本高性能作為衡量的標準。因此，首先我們會評估各機制中會有多少資訊及影像需要傳輸及公佈，這些將會延伸成所需花費的成本。表 5 為各機密影像分享機制中所需分配的分享影像以及須公佈的公開影像。

表 5: 機密影像分享機制中分享影像與公開影像之比較(分享 s 張影像時)

機制	TL	JC ($s \geq t$)	SC-G	LJ-G	GMSISS
分享片段資訊	-	-	2	2	1
分享影像張數	sn	n	-	-	-
分享影像大小	$\geq \frac{w_j h_j}{t}$	$w_j h_j$	-	-	-
公開影像張數	-	$s-t+1$	$\sum_{j=1}^{s} \lvert\Gamma_j'\rvert$	$\sum_{j=1}^{s} \lvert\Gamma_j'\rvert$	$\sum_{j=1}^{s} \lvert\Gamma_j'\rvert$
公開影像大小	-	$w_j h_j$	$l_j(v_{j,u}+d_j+1) > w_j h_j$	$w_j h_j$	$w_j h_j$

在表 5 中，TL 機制 與 JC ($s \geq t$) 機制皆適用於 (t, n)-門檻值的授權者集合。其中 TL 機制未提供公佈欄，所以每位參與者會分配到一張分享影像，其大小至少為 $w_j h_j / t$，然而其餘的機制皆提供公佈欄的設計，使得 SC-G 機制、LJ-G 機制與 GMSISS 無須讓每位參與者持有分享影像，而是將相關的影像公佈在公佈欄上。只有在 JC ($s \geq t$) 機制中，不但讓每位參與者持有一張分享影像，其大小為 $w_j h_j$，而且也將額外的影像公佈在公佈欄上，其公開影像大小為 $w_j h_j$。從另一方面來說，不管是讓參與者持有分享影像或是公佈在公佈欄上的公開影像，皆是在分配階段產生而在還原階段會使用到的影像。因此，我們以分享 s 張機密影像來作比較，比較 SC-G、LJ-G 與 GMSISS 這些機制中可能會公佈多少張公開影像以及分配多少張分享影像，其比較的單位為像素。根據表 5，我們發現當 $s > 1$，$n > t > 1$，$s \geq t$ 時，$\sum_{j=1}^{s} \lvert\Gamma_j'\rvert (l_j v_{j,u} + l_j d_j + l_j) > \sum_{j=1}^{s} \lvert\Gamma_j'\rvert w_j h_j$。所以 LJ-G 與 GMSISS 所公佈的公開影像與分配的分享影像會比其餘的機制少。因此 GMSISS 與 LJ-G 相同，皆可降低傳輸成本及公佈成本。另外，我們所提出的 GMSISS 中，每位參與者所持有的分享片段資訊是 LJ-G 的 1 / 2，因此傳輸成本上的花費又會比 LJ-G 機制少。

表 6：機密影像分享機制之功能比較表

機制	TL	JC ($s \geq t$)	SC-G	LJ-G	GMSISS
還原影像不失真	是	否	是	是	是
影像大小不受限	是	否	是	是	是
分享多張影像	否	是	是	是	是
分享彩色影像	否	否	是	是	是
一般性	否	否	是	是	是
安全性	是	是	否	是	是
多次使用	否	否	否	否	是

其次，我們檢視各機制提供哪些功能。根據表 6，我們可以很清楚地看出僅有 JC 機制 所還原的影像會失真，其原因在於大於 250 的像素值皆被視為 250。且在分享時，JC 機制中每張影像的大小必須一致。在表 6 中，除了 TL 機制無法同時分享多張機密影像之外，其它機制皆可同時分享多張機密影像。同時，在機制 SC-G、LJ-G 與 GMSISS 機制中不僅可分享灰階或彩色影像，而且可適用於一般授權者集合; 但 TL 機制 與 JC 機制 只能適用於 (t, n)-門

檻值授權者的集合，而且也未實作出可分享彩色影像。另外，我們發現只有 SC-G 機制存在不合法子集合可解出其它合法子集合的機密影像，導致其系統的不安全;而其餘的機制中，不會有相同的情況。更重要的是我們所提出的 GMSISS 利用兩變數的單向雜湊函數達到多次使用的目的，如此在不同的分享階段時，分配者不必重新選擇每位參與者的秘密片段，只須在分享前重新公佈新的亂數 r 值於公佈欄上，進而降低傳輸成本，達到可多次使用的目的。

根據表 5 與表 6，我們可以知道我們所提出的 GMSISS 不僅可以降成本之外，還可以達成表 6 所列的所有功能。

七、結論

本文改進簡和陳 [1] 兩學者所提出的多重影像秘密分享機制，使得在 $s \geq t$ 的情況下，所公佈的公開影像的張數與他們的機制相比會減少一張，如此可減少成本的浪費。

此外，本文針對一般授權者集合設計出多重機密影像分享機制 GMSISS，使得影像分享機制不再限制於特殊的授權者集合上，並且能夠達到多次使用的目的。我們所提出的 GMSISS 與 LJ-G 一樣可以避免在 SC-G 中可能存在一群不合法的子集合可能會解出其它合法子集合的機密影像，而且 GMSISS 所公佈的公開影像的大小與原始的機密影像的大小一樣大，相較於 SC-G 機制所公佈的公開影像的大小會比原始的機密影像的大小來得大，GMSISS 是較好的。另外，GMSISS 在效率上與每一個參與者所持有的秘密片段皆勝於 LJ-G。因此我們可設 GMSISS 是目前所知最佳可多次使用、且具安全性之有效率的一般多重機密影像分享機制。

致謝

本研究感謝行政院國家科學委員會（NSC 98-2221-E-260-013-）的補助。

八、參考文獻

[1] 簡祐緯、陳建彰，“多重影像之秘密分享方法”，TBI 2006 台灣商管與資訊研討會，台北大學，台北，台灣，2006 年 11 月 1 日。

[2] George Robert Blakley, “Safeguarding cryptographic keys”, Proceedings of the National Computer Conference, Vol. 48, pp. 313-317, Arlington, Virginia, June, 1979.

[3] Lein Harn, “Efficient sharing (broadcasting) of multiple secrets”, IEEE Proceedings Computers and Digital Techniques, Vol. 142, No. 3, pp. 237-240, 1995.

[4] Neal Koblitz, Alfred Menezes and Scott Vanstone, “The state of elliptic curve Cryptography”, Designs, Codes and Cryptography, Vol. 19, No. 2-3, 2000, pp 173-193.

[5] Ching-Fan Lee and Justie Su-Tzu Juan, “Multi-secret images sharing scheme with general access structure”, Proceedings of the 19th Cryptology Information Security Conference, National Taiwan University of Science and Technology, Taipei, Taiwan, June 3-5, 2009, A201.

[6] Moni Noar and Adi Shamir, “Visual Cryptography”, Advances in Cryptology: Eurpocrypt’94, Springer-Verlag, Berlin, pp. 1-12, May, 1995

[7] Adi Shamir, “How to share a secret”, Communications of the ACM, Vol. 22, No. 11, pp. 612-613, 1979.

[8] Shyong-Jian Shyu and Ying-Ru Chen, “On secret multiple image sharing”, Proceeding of the 25th Workshop on Combinatorial Mathematics and Computation Theory, Chung-Hwa University, Hsinchu, Taiwan, April 24-25, 2008.

[9] Chih-Ching Thien and Ja-Chen Lin, “Secret image sharing”, Computers and Graphics, Vol. 26, No. 5, pp. 765-770, 2002.