影像秘密分享方法之偵測與鑑別

孫光耀
玄奘大學資訊科學研究所
inventor@ms40.url.com.tw

陳建彰
玄奘大學資訊科學研究所
cchen34@hcu.edu.tw

摘要

欺騙偵測與鑑別在影像秘密分享中是一個重要的議題。在系統重建時，若參與者不誠實地拿出其次金鑰，則可能只有欺騙者才能解出主金鑰，造成系統不公平之現象。有鑑於此，本文提出一種具備欺騙偵測與鑑別影像秘密分享之方法，此方法包含影像秘密分享與偵測鑑別兩部分，第一部份為無失真影像秘密分享方法，利用 Shamir 所提出的作法，讓還原的機密影像無失真。第二部份透過影像秘密分享的偵測與鑑別方法，在影像秘密分享重建階段，能夠有效的偵測及鑑別出偽裝者。實驗結果顯示，本文方法除可還原失真之單張機密影像外，在還原多張機密分享影像下，亦可偵測及鑑別偽裝者，讓還原的影像為不失真且真實的機密影像。

關鍵字：欺騙偵測、欺騙者鑑別、門檻值、影像秘密分享

Abstract

Cheating detection and cheater identification are important issues in the secret sharing scheme. These two abilities mainly detect attackers who utilize fake shared images. In this paper, we propose an image authentication approach with the abilities of cheating detection and cheater identification. The proposed approach contains two main parts. One is the Shamir-based lossless secret image sharing approach. The other detects cheating and identifies cheaters in the recovering procedure. Experimental results show that the proposed approach can losslessly share an image secretly and identify cheaters in recovering procedure.

Keywords: cheating detection, cheater identification, threshold, secret image sharing

1. 前言

秘密分享起源於金鑰安全管理方法上所發展出來的一種密碼技術。在加密系統中，對於主金鑰的管理是系統安全中最重要的一個問題，如果系統的主金鑰交由系統管理員保管或存放於某一處，會產生一些風險，例如主金鑰遺失或管理者將主金鑰出售，可能會使得整個系統資料被竊取進而危害整個系統安全。為解決這個問題，我們可以將打造多份的主金鑰，交由不同的管理者進行保管，如此將可以降低管理員遺失主金鑰的風險。然而，這個方法卻將面臨眾多管理者之間的忠誠問題，其中只要有一個管理員將主金鑰洩漏或轉賣，系統的安全性就沒有保障。為解決以上問題所發展出來的秘密分享技術，其基本概念為：將機密分割成多個等份，其中“ 擁有足夠多”之部份即可回復原始機密。

Blakley (1979)及 Shamir (1979) 兩位學者分別發表了(t, n)門檻式密碼系統的概念。其中 n 代表莊家（dealer）負責將主金鑰分成 n 個次金鑰，交由 n 個參與者分別保管，而 t 代表至少要有 t 個參與者相互合作才可以導出主金鑰，少於 t 個參與者是無法得到任何秘密資訊的，兩人提出不同的方法皆能達到秘密分享的目的。其後 Noar 及 Shamir (1994)[1]利用人類視覺敏銳度的弱點，提出視覺性影像秘密分享技術，不僅輕易達成保護機密影像之目的，並且不需任何補助設備及複雜運算下即可還原機密影像，是一個觀念簡單且機密性完善的方法，唯一缺點便是會使得原有機密性影像在還原之後產生失真及擴大的效果。Thien 及 Lin (2002)[3]以 Shamir 秘密分享方法為基礎架構，成功延伸應用於影像秘密分享中，改善 Noar 及 Shamir 視覺性影像秘密分享中分享影像及還原影像擴張問題，也大幅降低影像失真議題。

上述 Thien 及 Lin (2002)[3]方法中，質數 P 是取 251，在灰階影像上的像素值是介於 0 到 255 之間，因此會失去 251 到 255 這五個灰階

像素值，在 Thien 及 Lin (2002)[3]方法中，做法是將灰階像素值大於 250 以上的以 250 取代，因此當還原機密影像時，會造成影像的失真情形。為了解決此問題我們提出一種新方法，就是保留影像中像素值 251 到 255 的做法，讓機密影像在還原之後無失真情形。

在一個(t, n)門檻方法裡，那些分享的秘密被保護著，未經授權的參與者，無法回復原始機密秘密，只有經過授權的參與者才有能力透過提供他們的次金鑰恢復秘密。一個秘密分享方法的基本假定之一是所有參與者必須提供個人真實分享的次秘鑰，不過此假定可能是不實用的。Tompa 及 Woll (1988)[4]提出 Shamir 的方法無法抵抗欺騙問題的發生，假設有一個經過授權的參與者想要欺騙其它參與者，在秘密重建時期，將本身錯誤的次金鑰提供給其它誠實的參與者，以這樣的方法，欺騙其它的參與者，使本身有機會得到正確真實的秘密，而其它參與者獲得錯誤的秘密，因此，如何鑑別參與者提出一個錯誤的次金鑰，在秘密分享方法的應用過程中是個重要的課題。為了解決欺騙問題， Tompa 及 Woll (1988)[4]修改了 Shamir 無法抵抗欺騙問題的方法，並且成功降低可能發生欺騙的機率。上述所提到 Shamir 的方法無法抵抗欺騙問題的發生，因此本文提出一種解決的方法，利用 T.C.Wu 及 T.S.Wu (1995)[5]所提出欺騙偵測及欺騙者鑑別方法，架構在解決影像秘密分享中參與者的欺騙偵測與欺騙者鑑別技術，讓參與者的分享影像在還原後成為真實的機密影像。

本文在第 2 章文獻探討略述前人所提秘密分享策略及應用於數位影像上之方法。第 3 章描述本文所提出之無失真性影像秘密分享方法與影像秘密分享欺騙參與者的偵測及鑑別方法。第 4 章陳述本文所提方法之實驗結果，第 5 章為結論。

2. 文獻探討

本章探討前人門檻值(t, n)之影像秘密分享，t 為回復人數，n 為影像秘密分享人數，若回復人數為 *t-1* 或更少人時，則無法得知機密影像資訊。

Shamir (1979)[2]在(t, n)門檻值中，建構一 *t-1* 次方多項式，公式(1)如下：

$$q(x_i)=a_{t-1}x_i^{t-1}+\cdots+a_1x_i+a_0 \pmod P \qquad (1)$$

將主金鑰 K（主秘密訊息）經過莊家(dealer)加密運算後，得到 n 個次金鑰(次秘密訊息)，將 n 個次金鑰分派於秘密分享參與者(participant)，只要收集 t 個次金鑰，代入 Lagrange 多項式插入法，公式(2)如下，主金鑰資訊便能回復。

$$q(x)=\sum_{b=1}^{t} y_{i_b} \prod_{j=1, j\neq b}^{t} \frac{x-ID_{i_j}}{ID_{i_b}-ID_{i_j}} \pmod P \qquad (2)$$

Shamir 的方法無法防備參與者欺騙問題的發生，因此如果有一個想要欺騙他人的參與者存在，在秘密重建時期，將本身錯誤的次金鑰提供給其它誠實的參與者，以這樣的方法，只有欺騙者本身有機會得到正確真實的秘密，而其它參與者獲得錯誤的秘密。

Thien 及 Lin (2002)[3]提出使用 Shamir 秘密分享技術完成影像之秘密分享。他們提出之步驟如下所述，欲秘密分享影像中每一像素之像素值設定小於 P 值，若像素值 $\geq P$ ，令此像素值為 *P-1*。使用一金鑰將機密影像重新排列，排列後影像呈現隨機影像，無法由重新排列之影像觀察出原機密影像資訊。選定(t, n)門檻值，將影像中像素每 t 個像素視為一區塊，分別依序置入像素值，求得產生之相對對應值，代入新分享影像中像素值內，莊家將新產生的分享影像分配予每位參與者。還原時，任意取回至少 t 張不同之分享影像，參與者公開自己的 ID 號碼。將分享影像中每一像素值依序置入，代入 Lagrange 多項式插入法中，取出 $a_0, a_1, ..., a_{t-1}$ 為像素值，依序置入新影像區塊中。重覆直至分享影像每一像素都完成運算，將回復新影像再使用一金鑰重新排列，即得回原始機密影像。Thien 及 Lin 使用$(3,5)$門檻值實驗結果不難發現不僅確實能達到秘密分享，且分享影像為原始影像尺寸 $1/t$ ，具有壓縮效果，是一個做法簡單又能達到資訊保護的方式。Thien 及 Lin 的方法無法防止參與者欺騙的問題發生。假如有一個參與者想要欺騙時，在影像秘密分享重建時期，將本身錯誤的分享影像提供給其它誠實的參與者，以這樣的方法，只有欺騙者本身有能力得到正確真實的機密影像，而其它參與者獲得錯誤的機密影像。

Tompa 及 Woll (1988)[4]利用 Shamir 秘密分享技術定義出欺騙者與如何欺騙。提出之步驟如下所述，s 代表主金鑰秘密(secret)，將主金鑰分成 n 個次金鑰，發給 n 個參與者

$(U_1,U_2,\cdots U_n)$，在一般情況下，假如U_2是參與的欺騙者，那他就可以取得其它參與者的次金鑰，執行建構一個多項式$\Delta(x)$，次方至多為$t-1$次，得到結果依序為$\Delta(0)=-1$，$\Delta(2)=\Delta(3)=\cdots\Delta(t)=0$。將$s_2+\Delta(0)$代替原本的$s_2$，如果其它的參與者提交正確的次金鑰$s_i(i=1,2,3,\cdots,t)$，當重建$(t-1)$次方多項式，則多項式的結果為$f(x)+\Delta(x)$，所有誠實的參與者都得到一個錯誤的主金鑰$f(0)+\Delta(0)=f(0)-1$，最後只有欺騙的參與者，經過加 1 的計算，得到一個真實的主金鑰。

T.C.Wu 及 T.S.Wu (1995)[5]秘密分享方法之偵測與鑑別是利用算數編碼以及單向雜湊函數，提出的方法適用於任何門檻值秘密分享之欺騙偵測與欺騙者的鑑別。首先介紹雜湊函數的特性，雜湊函數是一個依據輸入的任意位元組(或位元)字串，產生固定結果的函數。雜湊函數的大小通常是 128 到 512 位元。雜湊函數必須是一個單向(one-way)的函數：假設設定訊息m，必須容易算出$h(m)=x$。換句話說，單向函數是一個可以計算，卻不能逆向求得的函數。「防止碰撞 (collision resistance)」，碰撞指的是兩個不同的輸入m_1與m_2，其$h(m_1)=h(m_2)$，當然每一個雜湊函數都會有無限多個碰撞可能，因此雜湊函數絕對不是無碰撞的，防止碰撞只是定義上的聲明，雖然碰撞一定會存在，但必須讓人難以發現。透過以上特性與 Shamir 方法做結合，初始過程，產生次金鑰以及一些參數的設定，使用 Shamir (*t, n*) 門檻方法，將主金鑰分成n個次金鑰$s_1,s_2,\cdots s_n$。選擇單向雜湊函數$h(x)$與一個質數p，$h(x)<p$，接著計算算數編碼值，其中$1\le c<p$，公佈T值與p值。在欺騙偵測與欺騙者鑑別時，假設在n個參與者之中，有t個參與者想要利用個別的次金鑰重建秘密時，必須透過每位參與者與他們的次金鑰，才能重建分享的秘密，利用所提方法容易偵測與鑑別出在參與者之中的欺騙者。如果計算出的結果為 0 時，則此參與者U_j是誠實的，否則U_j是個欺騙者。T.C.Wu 及 T.S.Wu(1995)[5]提出秘密分享方法之偵測與鑑別方法是使用算數編碼以及單向雜湊函數的方式，他們提出的方法適用於任何門檻值秘密分享的欺騙偵測與欺騙者鑑別，上述方法的確能夠達到秘密分享欺騙偵測與欺騙者鑑定，這是一個做法簡單又能達到資訊防護的效果。

3. 影像秘密分享之欺騙偵測與欺騙者鑑別方法

本章介紹本文所提出之步驟及實驗方法，最後介紹所提影像秘密分享方法之架構圖。參考前人的方法，以實現影像秘密分享及欺騙偵測與欺騙者鑑定技術，方法如下：

(*t, n*)門檻值，*I*：機密影像(主金鑰)，*t*：還原解密人數，*n*：參與者人數，T_k：*n*個參與者的分享影像中，計算個別雜湊像素值$h(y_{(i,k)})$與P值做相乘，將n個參與者所得到的值做加總，此為加總後的結果，$T_{(j,k)}$：*t*個參與者的分享影像，將自己雜湊像素值$h(y_{(j,k)})$與P值做相乘後的結果，k：分享影像像素點個數。

影像分享欺騙偵測與欺騙者鑑定之步驟：

1．將欲機密分享影像 *I* 中每一像素I_W進行下列處理：

1.1 若像素值小於 *P-1* 值，則

$$a_0=I_W, \tag{3}$$

a_1為介於 0 到*P-1* 間之隨機數

1.2 若像素值大於或等於 *P-1* 值，則代入公式

$$a_0=P-1,$$
$$a_1=(I_w-250)+\left\lfloor\frac{240\times rand}{10}\right\rfloor\times 10 \tag{4}$$

其中，*rand* 為介於 0 到 1 間之隨機數。

2．莊家選定(*t, n*)門檻值，莊家建構一 *t-1* 次方多項式公式(1)，將機密分享影像 *I* 中每一機密像素值$I_W=a_0$置於多項式中，$a_1,a_2,...,a_{t-1}\in Z$且隨意分佈於[*0, P*)，*P* 值設為 251。

3．莊家任選 *n* 個相異值$x_{(1,k)},x_{(2,k)},...,x_{(n,k)}$代入公式(1)求得$y_{(1,k)},y_{(2,k)},...,y_{(n,k)}$，每一$y_{(i,k)}=q(x_{(i,k)})$，每一$x_i$值為參與者識別代號($i=1,2,...,n$)。

4．產生 $y_{(i,k)}$ 值分別置入相對應的新分享影像中。

5．選擇單向雜湊函數 h 及一個質數 p, 令 $h<p$ 。

6．n 個參與者的分享影像中，計算個別雜湊像素值 $h(y_{(i,k)})$ 與 P 值做相乘，將 n 個參與者所得到的值做加總，此為加總後的結果，公式(5)如下：

$$T_k \text{ 值：} T_k=\sum_{i=1}^{n} h(y_{(i,k)})p^{i-1} \qquad (5)$$

7．公佈 T 值與 p 值。

8．莊家計算產生 n 張分享影像 $(x_{(i,k)},y_{(i,k)})$ ，分配予每個參與者。

分享影像回復、欺騙偵測與欺騙者鑑定步驟：

1．任意取回至少 t 張分享影像。

2．參與者公開自己的 ID 號碼 $x_{(i,j)}, i=1,2,...,n, j=1,2,...,t$ 。

3．取回公佈 T 值與 P 值。

4．參與者計算自己的 $T_{(j,k)}$ 值，參與者各別的像素值經過雜湊計算，公式(6)如下：

$$T_{(j,k)}=\sum_{U_j\in s} h(y_{(j,k)})^{j-1} \qquad (6)$$

5．每一個參與者拿自己的 $T_{(j,k)}$ 值，與公開的 T_k 值作計算，鑑定參與者是否為誠實者，鑑定公式(7)如下，如果計算結果為 0 時，U_j 為誠實者，則往第 6 步驟進行重建原架構多項式，如果計算結果不為 0 時，則 U_j 為欺騙者，中止重建原架構多項式的動作，並說明 U_j 為欺騙者。

$$\left\lfloor \frac{T_k-T_{(j,k)}}{p^{2(j-1)}} \right\rfloor (\text{mod } P)=0 \qquad (7)$$

6．當上式成立時，表示 $h(y_{(i,k)})=h(y_{(j,k)})$ 。

7．重建原架構多項式，將分享影像中每一像素值依序置入公式(2)，求得多項式 $a_0+a_1x+...+a_{t-1}x^{t-1}$ ，取出 $a_0,a_1,...,a_{t-1}$ 為像素值，依序置入新影像區塊中。

8．若影像中之像素值小於 *P-1* 值，則使用上述公式(3)，a_0 代入原來機密像素值 I_W ，則使用下列公式(8)，令此 a_0 為 250，

$$a'=a_1 \bmod 10 \qquad (8)$$

最後兩數值 a_0 與 a' 相加，再回存到像素值 I_W 中。

9．重複步驟 7 與步驟 8，直至分享影像每一像素都完成運算，即可回復原始機密影像 I。

以下為範例說明所提出之方法的執行步驟及結果。

範例：設機密影像第一個像素值 I_W 為 252，建構一 (3, 5) 門檻值。

分享步驟：

．設 P=251，並檢查每個像素值是否大於 *p-1*，若像素值大於 *p-1* 則該像素值 $I_W=a_0$ 重新給定為 250，

$a_1=(I_w-250)+\left\lfloor \frac{240\times rand}{10} \right\rfloor \times 10$ ，如公式(4)所示。

．莊家選定(*t*,*n*)門檻值，建構一 *t-1* 次方多項式，設 $I_w=252$ ，設定 a_0 =250，*rand* =0. 85

$$a_1=(I_w-250)+\left\lfloor \frac{240\times rand}{10} \right\rfloor \times 10$$
$$=2+\left\lfloor \frac{240\times rand}{10} \right\rfloor \times 10=202$$

．令 $a_2\le p-1$ 的一個隨機亂數，假設為 4，代入公式(1)，求得

$$x_{(1,1)}=1, q(x_{(1,1)})=4x_{1,1}^2+202x_{1,1}+250 (\text{mod } 251)=205$$
$$x_{(2,1)}=2, q(x_{(2,1)})=4x_{2,1}^2+202x_{2,1}+250 (\text{mod } 251)=168$$
$$x_{(3,1)}=3, q(x_{(3,1)})=4x_{3,1}^2+202x_{3,1}+250 (\text{mod } 251)=139$$
$$x_{(4,1)}=4, q(x_{(4,1)})=4x_{4,1}^2+202x_{4,1}+250 (\text{mod } 251)=118$$
$$x_{(5,1)}=5, q(x_{(5,1)})=4x_{5,1}^2+202x_{5,1}+250 (\text{mod } 251)=105$$

分享影像 1 的第一個像素值為 205，分享影像 2 的第一個像素值為 168，…，分享影像 5 的第一個像素值為 105

・選擇單向雜湊函數 h 及一個質數 p, 令 $h < p$

・n 個參與者的分享影像中，計算個別雜湊像素值 $h(y_{(i,k)})$ 與 P 值做相乘，將 n 個參與者所得到的值做加總，此為加總後的結果，代入公式(5)，求得 T 值：

$$T = \sum_{i=1}^{n} h(x_{(i,k)})\, p^{i-1}$$
$$= h(y_{1,1}) \times p^0 + h(y_{2,1}) \times p^1 + h(y_{3,1}) \times p^2 + h(y_{4,1}) \times p^3 + h(y_{5,1}) \times p^4$$
$$= 102 \times 251^0 + 84 \times 251^1 + 69 \times 251^2 + 59 \times 251^3 + 52 \times 251^4$$
$$= 207331902116$$

・公佈 T 值與 P 值。

・莊家計算產生 5 張分享影像，分配予 5 個參與者。

回復步驟：

・任意取回三張分享影像，假設分別為第一張、第二張及第四張。

・參與者公開自己的 ID 號碼 $x_{(i,j)}, i = 1,2,...,n,\ j = 1,2,...,t$

・取出分享影像第一個像素值，$(1,205),(2,168),(4,118)$，代入 $h(y_{(j,k)})$

・取回公佈 T 值與 P 值。

・計算參與者自己的 T_j 值，代入公式(6)，得到 $h(y_{(1,1)}) = 102$ 、$h(y_{(2,1)}) = 84$ 及 $h(y_{(4,1)}) = 59$

$$T_{(j,k)} = \sum_{U_j \in s} h(y_{(j,k)})\, p^{j-1} \qquad T_{(j,k)} = \sum_{U_j \in s} h(y_{(j,k)})\, p^{j-1}$$
$$= \sum_{U_1 \in s} h(y_{(1,1)})\, p^{1-1} \qquad = \sum_{U_2 \in s} h(y_{(2,1)})\, p^{2-1}$$
$$= 102 \times 251^0 = 102 \qquad = 84 \times 251^1 = 21084$$

$$T_{(j,k)} = \sum_{U_j \in s} h(y_{(j,k)})\, p^{j-1}$$
$$= \sum_{U_4 \in s} h(y_{(4,1)})\, p^{4-1}$$
$$= 59 \times 251^3 = 932981809$$

・每一個參與者拿自己的 $T_{(j,k)}$ 值，與公開的 T 值作計算，鑑定參與者是否為誠實者，代入公式(7)得到，如果計算結果為 0 時，U_j 為誠實者，則往下進行重建原架構多項式，如果計算結果不為 0 時，則 U_j 為欺騙者，中止重建原架構多項式的動作，說明 U_j 為欺騙者。

$T_{(1,1)} = 102$, $T_{(2,1)} = 21084$, $T_{(4,1)} = 932981809$,

$$\left\lfloor \frac{T_k - T_{(j,k)}}{p^{j-1}} \right\rfloor (\text{mod } P) = 0$$

$$U_1 : \left\lfloor \frac{T_1 - T_{(1,1)}}{p^{j-1}} \right\rfloor (\text{mod } P) = \left\lfloor \frac{2073319021\,16 - 102}{251^{1-1}} \right\rfloor (\text{mod } 251)$$
$$= 0, U_1 \textit{ is a honest}$$

$$U_2 : \left\lfloor \frac{T_1 - T_{(2,1)}}{p^{j-1}} \right\rfloor (\text{mod } P) = \left\lfloor \frac{2073319021\,16 - 21084}{251^{2-1}} \right\rfloor (\text{mod } 251)$$
$$= 0, U_2 \textit{ is a honest}$$

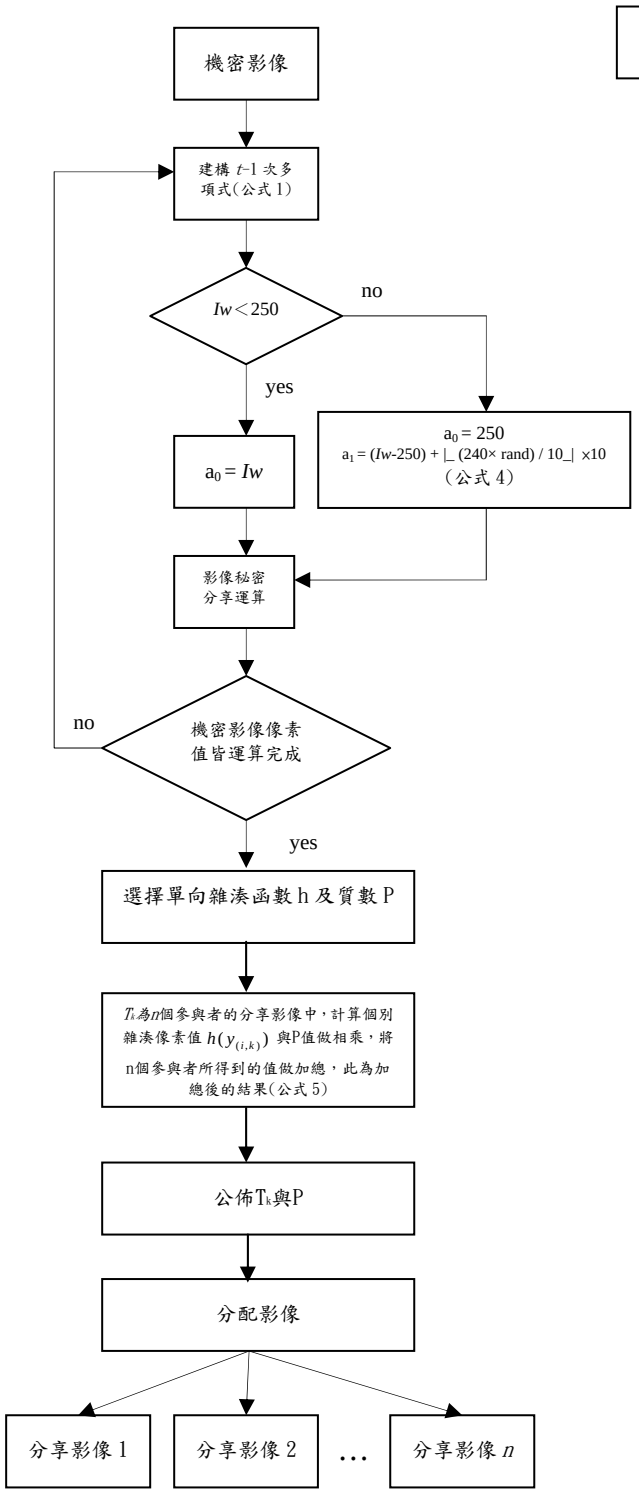
$$U_4 : \left\lfloor \frac{T_1 - T_{(4,1)}}{p^{j-1}} \right\rfloor (\text{mod } P) = \left\lfloor \frac{2073319021\,16 - 932981809}{251^{4-1}} \right\rfloor (\text{mod } 251)$$
$$= 0, U_4 \textit{ is a honest}$$

U_1, U_2, U_4 三個參與者為誠實者，進行重建原架構多項式。

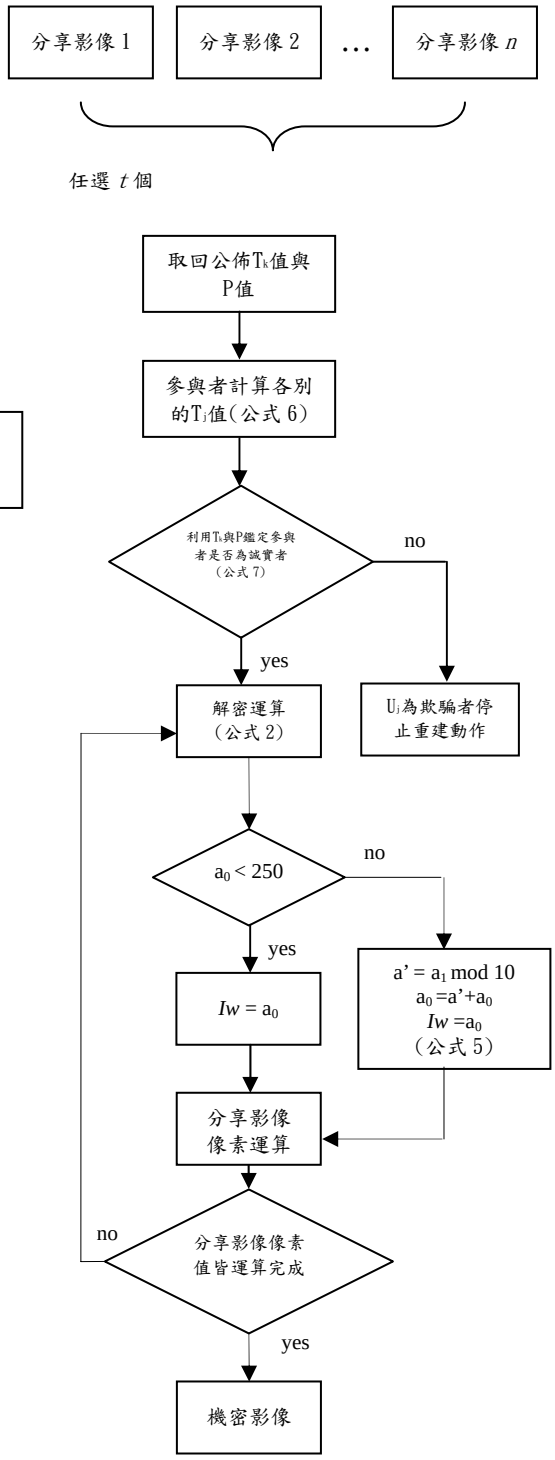
・接著取出分享影像第一個像素值，$(1,205),(2,168),(4,118)$ 代入公式(2)。

$$q(x) = 205 \times \frac{(x-2)\times(x-4)}{(1-2)\times(1-4)} + 168 \times \frac{(x-1)\times(x-4)}{(2-1)\times(2-4)}$$
$$+ 118 \times \frac{(x-1)\times(x-2)}{(4-1)\times(4-2)} (\text{mod } 251)$$
$$= 205 \times 3^{-1} \times (x-2)\times(x-4) + 168 \times (-2)^{-1} \times (x-1)\times(x-4)$$
$$+ 118 \times 6^{-1} \times (x-1)\times(x-2) (\text{mod } 251)$$
$$= 4x^2 + 202x + 250 (\text{mod } 251)$$

・依序將個別係數值置放於新影像中，如果 $a_0 = 250$ 時，把 a_1 的數值 mod 10，得公式(8) $a' = 202 \bmod 10 = 2$，再將 a_0 的值與 a' 的值做相加，回存到 a_0，這裡將 250 + 2 = 252 的值回存 a_0，所以 a_0 =252，最後將 a_0 存放到機密影像的第一個像素值位置上，使得 $I_w = 252$。



(a)分享步驟架構圖



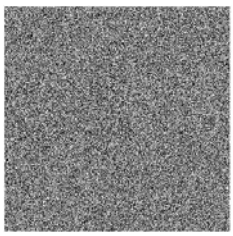
(b)回復步驟架構圖

圖 1、影像秘密分享之欺騙偵測與欺騙者鑑定方法架構圖

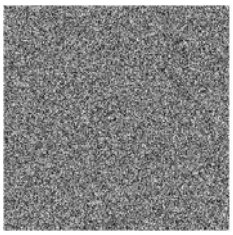
4. 實驗結果及比較

本章呈現第三章方法實驗結果，圖 2 為本文實驗方法(3,5)門檻值之結果，並將此與前人方法比較差異。

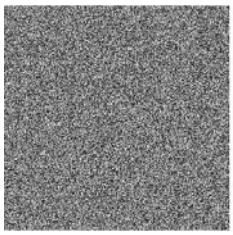
(a)機密影像



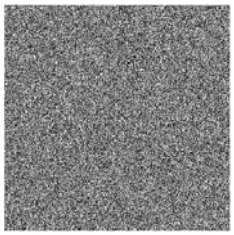
(b)分享影像 1



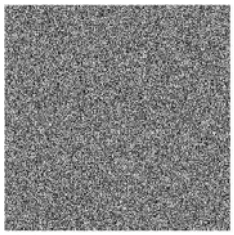
(c)分享影像 2



(d)分享影像 3



(e)分享影像 4



(f)分享影像 5

(g)還原影像

圖 2.(3,5)門檻值實作及結果

第一部分影像秘密分享方法，圖 2 為(3,5)門檻值使用本文方法實作及結果。原始機密影像為(a)，分享影像為(b)、(c)、(d)、(e)、(f)，還原影像為(g)。由此實驗結果可以看出，在我們所提出的方法中，原始機密影像加密分享後，只需要任選分享影像其中三張，即可解密還原不失真機密影像。相較於前人 Thien 及 Lin 的方法，影像像素值的取捨必須小於 P，本方法不受限於 P 值，對於影像中像素點介於 251~255 值，能夠加以利用，讓還原的影像不會產生失真問題。

第二部分影像秘密分享欺騙偵測及鑑別方法，原始機密影像加密分享後，利用算數編碼與單向雜湊函數，經過計算後產生一個公佈的 T_k 值，準備做分享參與者鑑定使用，只需要任選分享影像其中三張，計算個別參與者的 $T_{(j.k)}$ 值，最後做鑑定，如果參與者為誠實者，即可還原回原機密影像。

表 1：機密影像比較表

比較項目	機密影像分享(Thien 及 Lin)	無失真性機密影像之分享
解密影像無失真	×	∨
加密影像不需金鑰重新排列	×	∨
單張分享影像尺寸	$\frac{M}{t}$	M
安全性	$(\frac{1}{251})^{M/t}$ ※1	$(\frac{1}{251})^{M}$

「∨」表示符合「比較項目」敘述。

「×」表示不符合「比較項目」敘述。

t 為本文實驗之圖形，M：分享影像單張影像像素量，單位時間：秒。Thien 及 Lin 實驗影像為圖 1 影像，無失真性機密影像之分享實驗影像一般型為圖 3 影像。

※1：數據由 Thien 及 Lin (2003)之 Secret Image Sharing 一文提出。

由表 1 得知，本文提出的方法在安全性方面，每張分享影像的每一個機密影像分享像素值分佈範圍為[0, 251)，共有 251 一種可能，而第一個像素值與第二個像素值因為建構於 Shamir分享式子中，其a_0係數為原始影像像素值，a_1為一隨機亂數，故即使原始機密影像第一個像素與第二個像素為同一像素值，分享之後其分享影像兩像素值仍為不同數值，第一像素值猜中機率為 $\frac{1}{251}$，第二像素值猜中機率為 $\frac{1}{251}$，兩者皆屬獨立性機率，故猜中每張分享影像像素值機率為 $(\frac{1}{251})^M$（M：分享影像單張影像像素量）。安全性比機密影像分享提升不少，使得機密影像保護更加安全。

本文影像秘密分享方法與前述所提 Thien 及 Lin 影像秘密分享，相同架構於 Shamir 秘密分享方法之下，並加以應用完整還原多項式

特性，讓每位參與者持有一份分享影像，即有能力還原原本機密影像。在影像秘密分享方法之中，欺騙偵測與欺騙者的鑑別架構於 T.C.Wu 及 T.S.Wu 所提出的秘密分享方法之欺騙偵測與鑑別下，此方法適用於任何門檻值秘密分享的欺騙偵測與欺騙者鑑別，如果鑑定為真，參與者為誠實者，則還原回原機密影像。

5. 結論

本文提出之無失真影像秘密分享及欺騙偵測與欺騙者的鑑別，架構於 Shamir 秘密分享方法之下，每位分享者需持有一份分享影像，原始機密影像分享後，利用本方法所提出之方式，經過計算後產生公佈資訊值與一個質數，準備作為分享參與者鑑別之用，在影像回復時，任選分享影像其中三張，個別計算三個參與者的個別資訊值，最後進行鑑別，如果三個參與者都為誠實者，即可還原回原機密影像，如果三個參與者中有其中一人不誠實，則無法還原原機密影像。本方法同於 Shamir 秘密分享方法，所以分享影像大小與機密影像相同。在取得任何 t 張分享影像時，即可還原原機密影像，還原的機密影像不失真。結合以上兩部分，既可以達到還原影像不失真，又可偵測及鑑別分享影像中參與者的欺騙，在影像秘密分享中是個完善並且有效的方法。

本文提出影像秘密分享欺騙偵測與欺騙者的鑑別，利用公佈資訊值與一個質數，作為分享參與者鑑別之用，因為是不同分享影像同一位置像素點作鑑別，因此當公佈資訊值做加總時會產生一個很大的數值，這個數值隨著分享影像多寡而增減，在未來將朝向縮小公佈資訊為目標前進。

參考文獻

[1]. Naor, M. and Shamir, A. (1995), “Visual Cryptography”, ***Advances in Cryptology: Eurpocrypt’94***, May, Springer-Verlag, Berlin, pp. 1-12

[2]. Shamir, A. (1979), “How to Share a Secret”, ***Communication of the ACM***, November, Vol. 22, pp. 612-613

[3]. Thien, C.C., Lin, J.C. (2002), “Secret image sharing”, ***Computers & Graphics***, Vol. 26, pp.765-770

[4]. Tompa, M. and Woll, H. (1988), “How to secret with cheaters”, ***J. Crytol.***, 1988,1, (2), pp. 133-138

[5]. Wu, T.C. and Wu , T.S. (1995), “Cheating detection and cheater identification in secret sharing schemes”, ***IEE Process-Computer Digit. Tech.***, Vol. 142, No. 5, September 1995