可容許金鑰失真之秘密分享技術

莊潤洲
靜宜大學 資訊傳播工程學系
e-mail：lzchung@pu.edu.tw

沈宛瑩
靜宜大學 資訊傳播工程研究所
e-mail：g9773011@pu.edu.tw

摘要

秘密圖像分享方法是將一張秘密圖像透過秘密金鑰加密分享至 *n* 張分享影像中，參與秘密分享的每個人都持有一張分享影像及一組秘密金鑰。在加密系統中，秘密金鑰是系統安全的主要關鍵，當所有授權者將分享影像結合並透過金鑰解密後便可獲得機密影像。傳統的影像秘密分享機制都是應用於無失真金鑰分享，也就是重建後的金鑰不可以和原本金鑰不同。目前並沒有太多討論關於可失真的金鑰分享技術，因此本方法提出一個可失真金鑰之秘密分享機制，利用秘密分享技術及所提出量化技術將機密影像分享至 *n* 張有意義偽裝圖像中。實驗結果顯示，透過我們的方法，不但降低解密的時間，也可獲得良好的回復影像品質。

關鍵詞：秘密分享、金鑰分享、資訊安全

Abstract

Image secret sharing is to share a secret image into *n* shadow image. Each participate owns a part of secret information, but they can not extract the secret data from their own share. The secret image can be recovered only when the number of shadow images is large than the predefine threshold. In traditional secret sharing methods, secret key is the important data, and it cannot be distortion differ from the original key. There are fewer papers discussions about lossy key topic therefore we proposed a lossy key image secret sharing scheme. The proposed scheme has two advantages. First, the secret can be lossy. Second the cover share image is meaningful. From the experimental results, the image quality of the recovery secret image and the embedded image can obtains better image quality.

***Keywords*:** secret sharing, key sharing, data security

1. 前言

秘密分享的動機是源於金鑰安全管理，發展出來的密碼學技術，此方法往往存在於商業或軍事應用中。對於所儲存的秘密、文字或圖像，其安全性是一大問題。秘密分享的技術亦擴展到很多領域與實務系統，如影像、語音…等領域，是理論與實務結合的技術。

但近年來，許多技術的發展都是以增加安全性為主要工作，例如：圖像隱藏、數位浮水印…等。而這些技術皆有一個弱點，即是其均是由單一訊息和載體所構成的機密隱藏機制，一但遭受破壞就會造成秘密訊息的缺失[1]。若要解決這個問題，秘密分享可能會是一種解決的辦法。

在影像秘密分享技術中，大致可分為二大類，如圖 1 所示，分為像素擴展型與像素不擴展型兩大類，接著區分為無意義與有意義的偽裝圖像，底下針對還原後的機密圖像，又分成失真型與非失真型，其原因取決於加密過程的運算，例如：醫療圖像、軍事地圖…等，還原的機密圖像不能有絲毫誤差，則使用非失真型，而一般資訊傳遞或身分驗證…等則可容許還原影像的失真。然而在以往的研究中所提出的方法[2-6]，大多使用像素擴展型，此方式是將機密圖像上的每個像素，擴展成 *n* 倍的子像素，再將擴展後的機密圖像分散至數張偽裝圖像中，所產生的偽裝圖像均為無意義的雜訊圖，且會使得偽裝圖像比原機密圖像大上 *n* 倍，雖可以確保安全性，但也容易遭人懷疑竄改，之後也有許多研究紛紛提出將偽裝圖像改進為有意義偽裝圖像的方法，在安全性上提供了更好的偽裝能力，但擴展之後的圖像仍存在著儲存空間過於浪費的問題。而像素不擴展型[8,9]，不需經過像素擴張，可以減少圖像變形或放大的機會，更可以減少影像儲存的空間，近年來的研究多朝此方向進行。

1979 年，Shamir[2]首先提出一秘密分享概念，此方法稱作(*t*,*n*)-threshold 分享計劃，往後許多相關研究皆是以其為基礎做延伸，1998 年

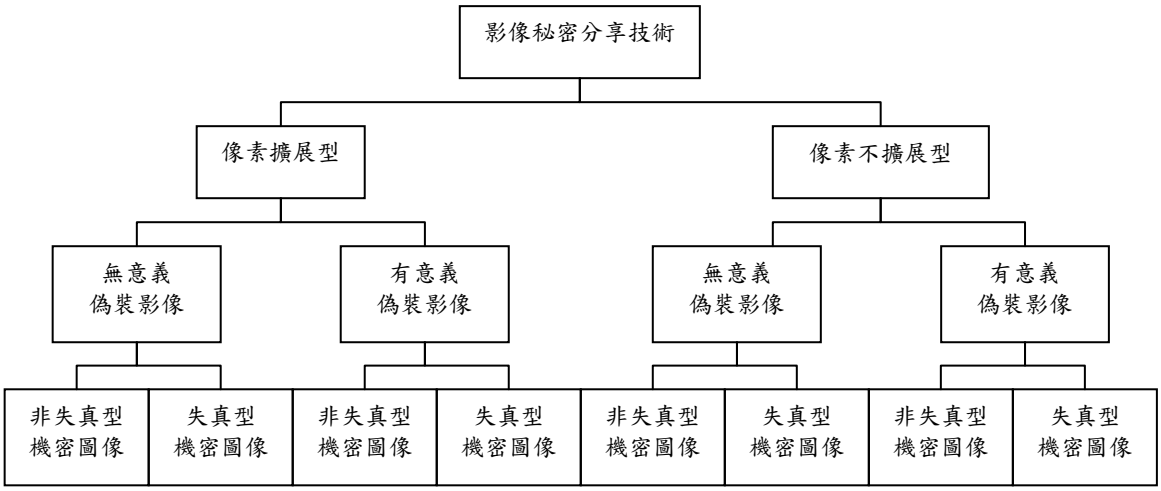


圖 1 影像秘密分享技術區分示意圖

Hwang 和 Chang[5]提出一有意義偽裝影像的分享方法，主要是以像素擴展的方式，將分享影像轉變為一張具有意義而另一張則為無意義偽裝影像，雖改善了無意義影像的缺失，提高其偽裝能力，但仍存在部分無意義偽裝影像，及擴展後儲存空間的問題。

2002 年，Lin 和 Thien [7] 提出一個新的秘密分享機制，此方法克服了(*t*,*n*)-threshold 分享計劃所造成儲存空間浪費的問題。且有效的縮減分享影像儲存的空間，進而加速了資料傳遞的速度，但此方法會造成重建後影像的變形失真，與之前的方法皆有一個弱點，其分享影像皆是由機密影像加密產生無意義的偽裝圖像，雖可以造成難以辨讀的效果，但容易遭受非法攻擊。

2004 年，Wu、Thien 和 Lin [15]再度提出一項新的秘密分享計劃，透過 VSQ 量化的方法，將秘密圖像分享至有意義偽裝圖像當中，偽裝圖像為原圖 1/2，且為有意義之偽裝圖像，其藏入之偽裝圖像品質良好，且傳輸量小，改進了無意義雜訊圖所造成圖像的破壞，但其過程步驟繁複，計算時間量較多，是其缺點。

本研究提出一個可失真金鑰之秘密分享機制，利用 Lagrange 多項式及所提出量化區間將機密影像分享至 *n* 張有意義偽裝圖像中，達到像素不擴展之有意義偽裝圖像的分享，透過簡單的步驟直接對祕密圖像的像素值做編碼加密分享的動作，將機密影像資訊分享至 *n* 張有意義偽裝影像中，大大的降低其遭受攻擊的機會，且可有效降低機密影像還原的失真度。

本研究架構如下，第二章為文獻探討，此部份介紹(*t*,*n*)-threshold 秘密分享技術及影像秘密分享技術，第三章為本研究提出的方法，第四章為實驗結果分析，最後，第五章探討本研究的成果。

2. 文獻探討

2.1 (*t, n*)-threshold 秘密分享技術

Shamir 於 1979 年提出[2]，其概念為一個主要的分派者(dealer)選定一個主金鑰，再將其打散成 *n* 份不的同子金鑰，分派給每一位參與者(participant)都獲得一把子金鑰，因此，(1)當子金鑰數目超過或等於門檻值 *t* 時才可導出主金鑰；(2)當子金鑰小於門檻值 *t* 時，無法取得任何有關主金鑰的訊息。這個方法主要是使用平面上 *t* 點可以決定 *t*-1 次方的多項式，以 *t* 點為門檻值，應用 Lagrange 多項式內插法的技術，回復原多項式。接下來介紹 Lagrange 多項式內插法的原理，如下圖 2 所示，直線中任意兩點以上可以決定一直線，可以由 (x_1, y_1)、(x_2, y_2)、…、(x_n, y_n)中取出兩點以上即可求得直線方程式。

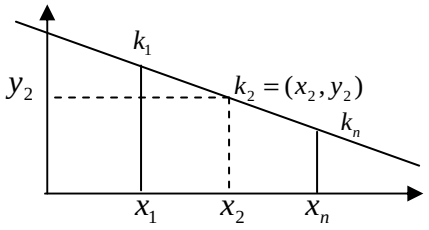


圖 2 Lagrange 多項式方法原理

以下為此秘密分享步驟：

[分享步驟]

1. 分派者選定一主金鑰 k 及一個質數 p，且滿足 $p \geq k$。
2. 任意選定一個 n-1 次方的多項式 $f(x)$，如公式(1)，其中參數 $a_{n-1}, a_{n-2}, ..., a_1$ 是任意整數，分佈在區間[1, p]中。

$$f(x_i) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} ... + a_1x_1 + a_0 (\text{mod } p) \quad \textbf{(1)}$$

3. 分派者任選 n 個不為 0 的相異值 $x_1, x_2, ..., x_n$，代入公式(1)求得 $y_1, y_2, ..., y_n$，且每一個 $y_i = f(x_i)$。
4. 分派者將計算過後產生的 n 把次金鑰 (x_i, y_i)，分派給每位秘密分享的參與者 x_i，x_i 為次金鑰之識別碼，y_i 為次金鑰值。

以下舉例說明：

分派者令(t,n)=(3,5)-threshold，分享主金鑰為 5 個次金鑰，任意三個次金鑰可以回復主金鑰。首先選定主金鑰 $k = 7$ 及一個質數 $p = 17$，且滿足 $p \geq k$，任意選定二次多項式 $f(x) = 4x^2 + 8x + 17$，及五組不為 0 的整數值，分別為 1、2、3、4、5，計算多項式在曲線上的點 $y_i = f(x_i)$，算式如下。

$$y_1 = f(1) = 4 \times 1^2 + 8 \times 1 + 17 (\text{mod} 17) = 2$$
$$y_2 = f(2) = 4 \times 2^2 + 8 \times 2 + 17 (\text{mod} 17) = 5$$
$$y_3 = f(3) = 4 \times 3^2 + 8 \times 3 + 17 (\text{mod} 17) = 16$$
$$y_4 = f(4) = 4 \times 4^2 + 8 \times 4 + 17 (\text{mod} 17) = 1$$
$$y_5 = f(5) = 4 \times 5^2 + 8 \times 5 + 17 (\text{mod} 17) = 11$$
$$\Rightarrow (1,2); (2,5); (3;16); (4,1); (5,11)$$

[重建步驟]

1. 選取 t 組以上不一樣的次金鑰之識別碼與次金鑰值。
2. 將(x_i, y_i)代入 Lagrange 多項式內插法(如公式 2)中，即可重建出原多項式 $f(x)$ 原始秘密金鑰 k。

$$f(x) = \sum_{b=1}^{t} y_{ib} \prod_{j=1, j \neq b}^{t} \frac{x - x_{ij}}{x_{ib} - x_{ij}} (\text{mod } p) \quad \textbf{(2)}$$

3. 令 x=0，置入重建的多項式 $f(x)$ 中(公式 2)，即可求得原始秘密金鑰 k。

以下舉例說明：

延續上一個例子，選取三組不一樣的金鑰值(1,2)、(2,5)、(4,1)三點當做輸入的次金鑰，代入公式(2)，計算得原多項式：

$$f(x) = 2(\frac{x-2}{1-2} \times \frac{x-4}{1-4}) + 5(\frac{x-1}{2-1} \times \frac{x-4}{2-4}) + 1(\frac{x-1}{4-1} \times \frac{x-2}{4-2})$$
$$= 2(-x^2 + 6x - 8) + 5(x^2 - 5x + 4) + (\frac{1}{3}x^2 + x + \frac{2}{3})$$
$$= 4x^2 + 8x + 17$$

令 $x = 0$，代入 $4x^2 + 8x + 17$ 求得秘密金鑰 $k = 17$。

2.2 Lin 和 Thien 秘密分享計劃

Lin 及 Thien 於 2002 年提出一祕密分享技術，此技術是基於 Shamir 提出的(t, n)-threshold 分享技術所完成的灰階秘密分享[2]。此方法主要特色是使用一金鑰重新排列灰階值，並使用 Shamir 秘密分享方法應用於機密影像中，更使秘密分享影像的大小為原機密影像大小 1/t，在傳統秘密分享方法中[3,9,12,14]，如需以半色調處理及還原機密影像，必會造成影像間尺寸擴散的問題，此方法解決了傳統秘密分享方法在灰階影像分享的限制。

接下來介紹他們的秘密分享流程：(如圖 3)

[分享步驟]

1. **機密像素值調整：**將欲分享的秘密影像像素值設定小於 p 值(p =251)，若像素值≥ p，則令此像素值為 $p-1$。
2. **機密影像像素排列打亂：**使用一金鑰將秘密圖像重新排列，所產生的影像為隨機影像，且此影像無法藉由重新排列觀察到原來的機密影像。
3. **選定回復門檻值：**將隨機影像中每個像素值 t 設為一個區塊，分別依序帶入公式(1)，$a_1, a_2, ..., a_n (p = 251)$。
4. **分享圖像生成：**分派者任選 n 個相異值 $x_1, x_2, ..., x_n$ 代入算式(3)，可求得 $f(x_i)$。

$$f(x) = ax + b (\text{mod } 251) \quad \textbf{(3)}$$

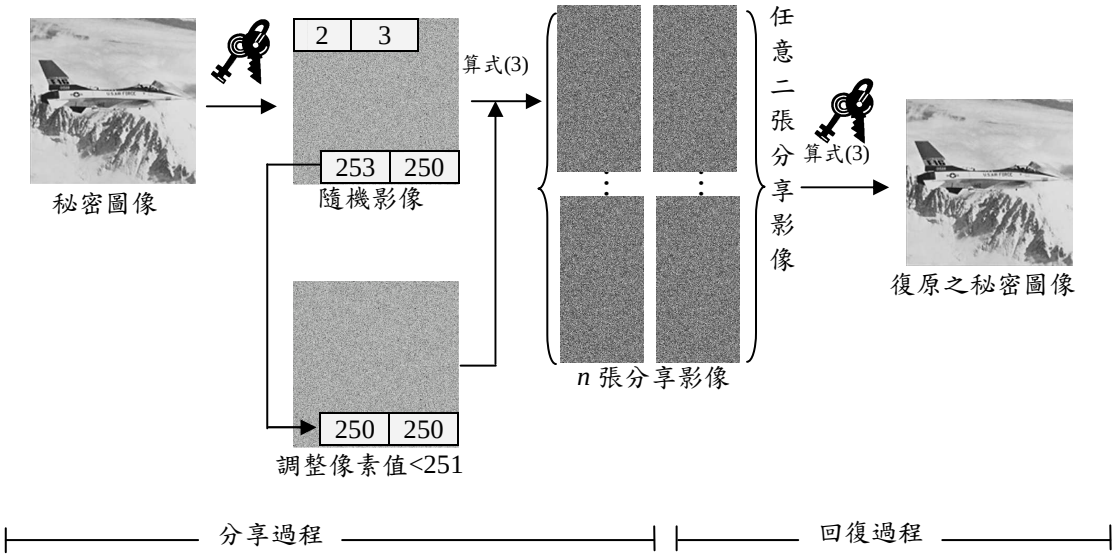


圖 3 Lin 和 Thine 秘密分享計劃流程圖

5. 分派者再將得到的分享影像分給每一位參與者(participant)。

[重建步驟]

1. 聚集 t 位參與者，每位參與者公開其識別值 x_i，並交出所持有的分享影像。
2. 將分享影像的每一像素值帶入算式(3)，可求出 $a_0 + a_1 x + ... + a_{t-1} x^{t-1}$，最後取出 $a_1, a_2, ..., a_{t-1}$ 的像素值，再依序置入新的影像區塊中。
3. 重複步驟 2，直到分享影像的每一像素都運算完成。
4. 將回覆影像使用金鑰再重新排列一次，即求回原始機密影像。

此方法確實成功的使分享影像為原始機密影像的 1/t，且具有壓縮的效果，是一個既簡單又可達到秘密分享效果的方法。然而，此方法雖然可以簡單又輕易的達到秘密分享的效果，但卻隱含著一些缺點：

- 還原影像失真：因質數的關係，當原始影像像素值大於250時，皆必需重新設定像素值為250。
- 原始機密影像加密分享前，必需經過一金鑰重新排列影像：在後續許多學者提出相關機密影像分享之研究及方法中[4,6,7,9,13,15]，確實達到影像分享之目的，美中不足的是所產生的影像皆為雜訊圖，且仍有存在解密影像失真度過高或無法達成(2,4)-threshold的問題。

2.3 Wu、Thien 和 Lin 的秘密分享計畫

Wu、Thien 和 Lin 於 2004 年提出一秘密分享技術[15]，改善了先前 Thien 及 Lin 所提出的方法，其主要特色是將秘密圖像透過 VSQ(Variable-Size-Quantization) 量化步驟及 S_E Table 的處理，將量化過後的機密訊息使用 (t, n)-threshold 分享至 n 張有意義的圖像當中，其分享影像的效果良好。

[VSQ 量化步驟]

1. **機密影像分割:** 將機密圖像分割成許多不重疊的區塊，每一個區塊大小為 1×2。
2. **平滑區塊及邊緣區塊判定:** 比對目前區塊和先前區塊像素值差異值，如果大於定義的門檻值則判定為邊緣區塊反之為平滑區塊。當前後彼此區塊皆為平穩區塊則將其合併成一個區塊。
3. **機密數值量化:** 根據區塊特性採用不同量化係數對機密像素值進行量化。
4. 重覆步驟 2 至 3，直到所有區塊皆運算完畢，再將其依序置於相對應的位置區塊，即

可得到量化過後的秘密圖像，最後將平滑區塊填入”0”，邊緣區塊填入”1”，即可得一 S_E Table。

圖 4 為此方法的秘密分享流程，此方法的重點即是透過 **VSQ** 量化，將像素值控制在一定的範圍內，經過量化過後的分享影像，再使用秘密分享技術進行分享。此方法 PSNR 值皆介於 37.66-41.64dB，圖像分享的品質良好，唯一美中不足是其量化過程繁複，增加不少運算處理的時間。

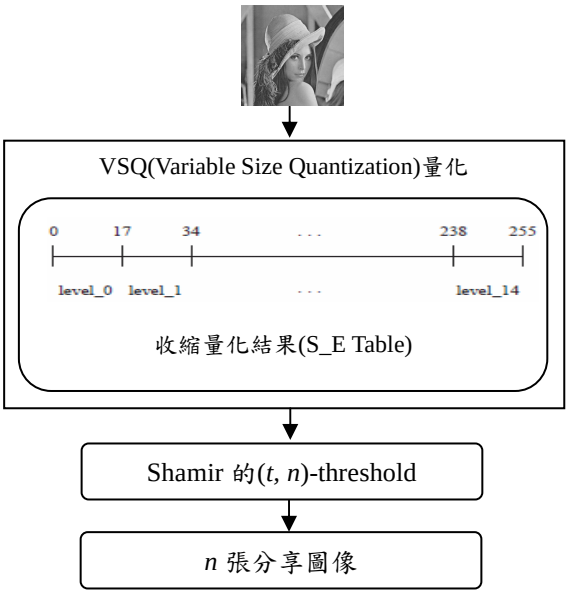


圖 4　Wu、Thien 和 Lin 的秘密分享計畫流程

3. 提出方法

傳統圖像秘密分享技術，偽裝影像皆為雜訊圖，除了不夠美觀之外亦容易遭受有心人士的攻擊竄改，本研究希望使偽裝影像皆為有意義的偽裝圖像，且不影響資料保護的效果。本方法利用 Thien 和 Lin 的量化區間概念，對機密圖像藏入 n 張有意義的偽裝圖像的最不重要位元中，而不被輕易的察覺。在重建秘密圖像程序，透過 Lagrange 公式便可重建原始機密訊息，圖 5 為本方法藏入流程圖。

接下來介紹本方法的秘密分享步驟：

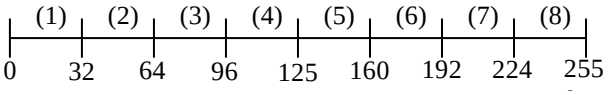
[分享步驟]

1. 分派者選定一張機密圖像與 n 張有意義的偽裝圖像，。
2. **機密像素重排：**將機密圖像重新排列，所產生的影像為隨機影像。
3. **秘密分享：**將隨機影像像素代入公式(1)，其中參數 $a_{n-1}, a_{n-2}, ..., a_1$ 為固定整數值。

$$f(x_i) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} ... + a_1x_1 + a_0 (\mathrm{mod}\, p) \quad \textbf{(1)}$$

4. **區間量化**：將排列過後的 $f(x_i)$，對照表 1 的向量區間編碼表，將編碼值與分享影像之 LSBs 做替換。
5. 替換過 LSBs 的像素值，再將其依序置於相對應的位置區塊，即可得到量化過後的分享圖像。

表 1 向量區間編碼表



編號	編碼值	像素區間	還原像素值
(1)	111	0~32	16
(2)	001	33~64	48
(3)	010	65~96	80
(4)	011	97~128	112
(5)	100	129~160	144
(6)	101	161~192	176
(7)	110	193~224	208
(8)	111	225~255	240

以下舉例說明：

取得一張秘密圖素 $a_0 = 170$ 及三張分享圖素，取得每一個點的分享金鑰，$x_1 = 52$、$x_2 = 76$、$x_3 = 66$，秘密金鑰 k 值為 1000，代入公式(1)。

$$f(x_i) = 1000x + 170$$

$$\Rightarrow (1,1170) = 1000 \times 1 + 170 (\mathrm{mod}\, 256) = 146$$

$$\Rightarrow (2,2170) = 1000 \times 2 + 170 (\mathrm{mod}\, 256) = 122$$

$$\Rightarrow (3,3170) = 1000 \times 3 + 170 (\mathrm{mod} 256) = 98$$

得到 146、122、98 三個區間值，對照表 1，其編碼值為 100 與 011，做 LSBs 替換，得到的像素值如下。

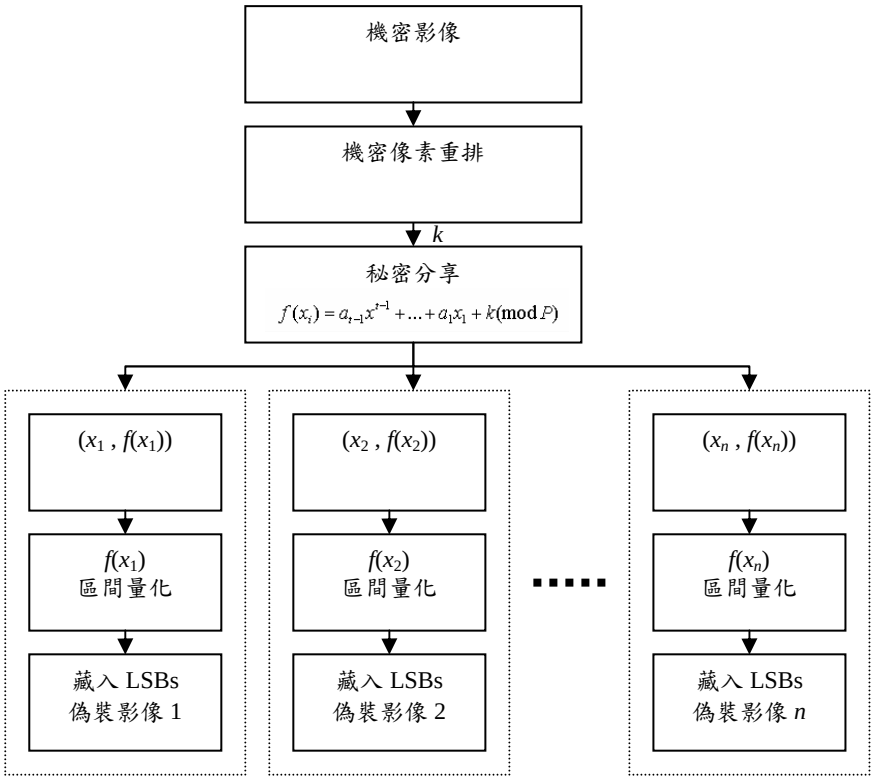


圖 5 本方法藏入流程圖

52=00110100→00110100=52；

76=01001100→01001100=76；

66=01000010→01000011=67

⇒(1,52)；(2,76)；(3,67)

可得到三張分享影像的像素值分別為 52、76、67。

[重建步驟]

1. **取得編碼值：**只需由任意二張有意義偽裝圖像中取得像素值 x_1 及 x_2（如圖 6），取得其 LSBs 的編碼值，對照表 1，取得還原之區間數值。
2. **Lagrange 解密運算：**將步驟 2 取得之還原像素值代入 Lagrange 公式，即可求得還原後機密影像的像素值，再依序置入新的影像區塊中。
3. 將計算過後的像素值依序置入新的影像區塊中，即得到原機密影像。

以下舉例說明：

延續上一個例子，必須先取得二張偽裝圖像像素值，對照表 1，取得還原像素值，再將其值代入 Lagrange 公式，即可求得還原機密影像像素值。

(1,52)= 00110100→LSBs=100→144

(3,67)= 01000011→LSBs=011→112

代入 Lagrange 公式：

$$l_0 = x - x_1 / x_0 - x_1 = (2 - x)$$

$$l_0 = x - x_1 / x_0 - x_1 = (2 - x)$$

$$\Rightarrow f(x) = 144 \times (2 - x) + 112 \times (x - 1)$$
$$= 288 - 144x + 112x - 112$$
$$= -32x + 176$$

即可得到還原後原始機密圖像像素值 176，取得失真金鑰值=−32 。

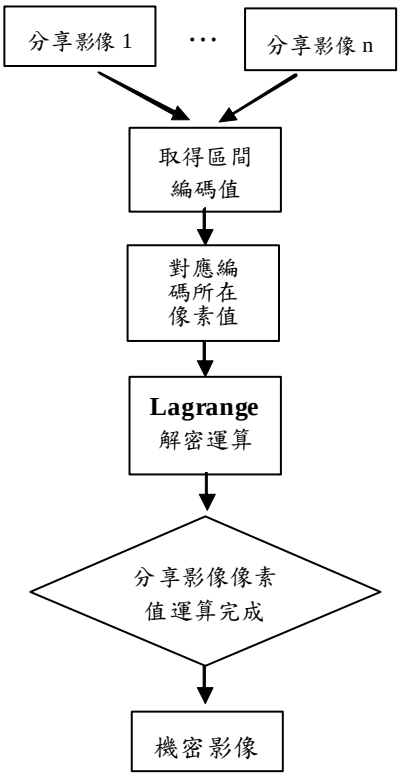
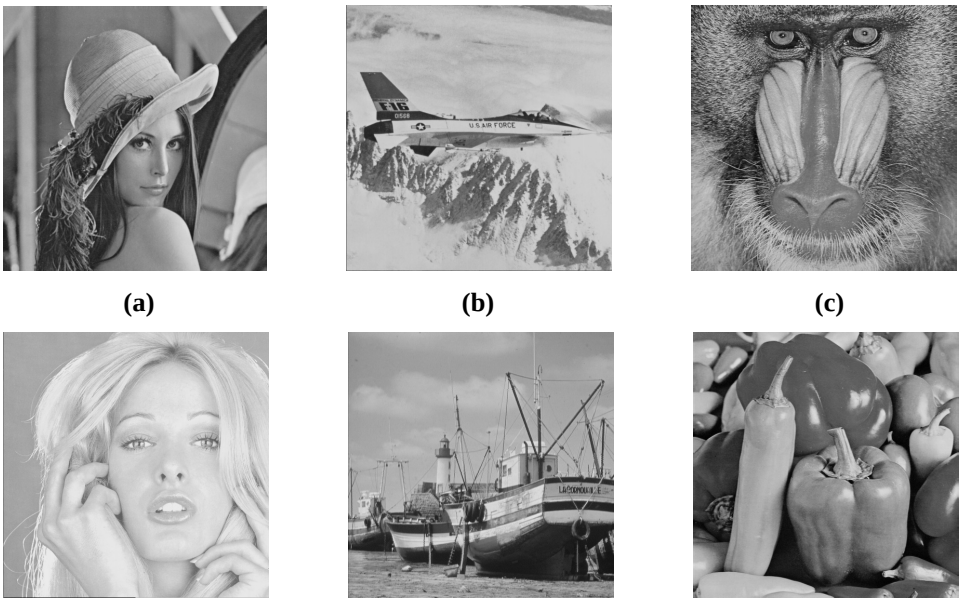


圖 6 機密圖像重建架構圖

4.實驗結果及比較



(a) **(b)** **(c)**

(d) **(e)** **(f)**

圖 7 (a)原始機密圖像 Lana (512×512)；(b)(c)(d)(e)(f)原始分享影像(512×512)

(a) **(b)** **(c)**

(d) **(e)** **(f)**

圖 8 (a)還原之機密圖像(PSNR：41.4db)；
(b)(c)(d)(e)(f)藏入後偽裝圖像(PSNR：40.4db~42.1db)

表 2 藏入後偽裝圖像 PSNR 值

分享影像	Airplane	Baboon	Tiffany	Boat	Peppers
PSNR(db)	41.3	40.4	41.9	42.1	41.5

表 3 機密影像總合比較表

比較項目	機密影像分享 (Thien 及 Lin)	機密影像分享 (Wu、Thien和Lin)	機密影像分享 (本研究方法)
解密影像失真度(PSNR)	34 db	37.9db	41.4db
加密影像不需金鑰重新排列	×	∨	∨
分享影像為有意義圖像	×	∨	∨
單張分享影像尺寸	m/t	$m/2$	m
解密執行時間	1.38(s)	2.45(s)	1.26(s)

我們提出分享多張具有意義偽裝圖像的技術，使用像素不擴展的方式，可避免還原影像資訊的破壞，如變形，放大、模糊...等，且使用區間量化的方法，將機密影像資訊隱藏入 *n* 張分享影像的 LSBs 中，減少對分享影像的影響程度，且儲存的資訊量少，相對的資料傳送的時間上較為快速，亦不會成儲空間的浪費，而每一位參與者，皆無法由自身得到的單張分享影像中取回原始機密圖像，擁有良好的安全性，又每一張分享影像皆為有意義影像所以也提高了更好的偽裝能力，取回機密影像時，只需要 2 張以上的分享影像，透過 Lagrange 內插法公式，我們可以簡單又快速的獲得良好的還原影像品質。

圖 7 為本秘密分享方法之實驗圖像，實驗機密影像 Lenna 及 5 張偽裝影像皆為 512×512 的灰階圖像。圖 8 為實驗過後的偽裝圖像及還原之機密影像。表 2，為藏入後偽裝圖像之 PSNR 值，其值介於 40.4(db)~42.1(db)之間，且平均為 41.44(db)，表 3，為本實驗結果與 Wu、Thien 和 Lin 的方法做一比較。

本章上述方法及舉例中完成機密影像的分享，其最大特色為：

- 偽裝影像與機密影像大小相同，且為有意義之偽裝圖像。
- 無須經過複雜運算，透過簡單的編碼即可做分享與還原的動作。
- 運算快速，還原品質良好。

5. 結論

本研究提出一個可失真金鑰之秘密分享機制，利用秘密分享技術及量化技術將機密影像分享至 *n* 張有意義偽裝圖像中，不需經過像素擴展且偽裝影像都是有意義，降低其遭受非法攻擊的機會。當要解回機密影像時，亦只需要透過 Lagrange 計算即可輕易又快速的解出機密影像，無論在運算速度、儲存空間或影像品質皆達到了良好的標準。

參考文獻

[1] 潘正祥、張真誠、林詠章，***挑戰影像處理: 數位浮水印技術***，台北，麥格羅希爾，民國 96 年。

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

[3] Bakley GR. “Safeguarding cryptographic keys. ”, ***Proceedings AFIPS 1979 National Computer Conference,*** vol. 48, New York, USA, 4–7 June 1979. p. 313–7.

[4] Lin-Chen Chang, Ren-Junn Hwang, “Sharing Secret Images Using Shadow Codebooks”, ***Information Sciences – Applications : An International Journal***, Vol. 111, pp. 335-345, 1998.

[5] C. Chang, and R. J. Hwang, “A Simple Picture Hiding Scheme,” ***Computer processing of Oriental Languages***, Vol. 12, No. 2, 1998, pp.237-247.

[6] Chang-Chou Lin, Wen-Hsiang Tsai, “Secret Image Sharing with Steganography and Authentication”, ***The Journal of Systems and Software***, Vol: 73, Issue: 3, Nov.-Dec., pp.405-414, 2004.

[7] Chih-Ching Thien, Ja-Chen Lin, “Secret image sharing”, ***Computers & Graphics***, Vol. 26, pp.765-770, 2002.

[8] C. N. Yang “New Secret sharing Schemes Using Probabilistic Method,” ***Pattern Recognition Letters***, Vol.25, Issue 4, 2004, pp.481-494.

[9] D. Wang, L. Zhang, N. Ma, X. Li, “Two secret sharing schemes based on Boolean operations,” ***Pattern Recognition***, Vol. 40, Issue 10, 2007, pp.2776-2785.

[10] G.R. Blakley, “Safeguarding cryptographic keys”, ***Proceedings AFIPS National Computer Conference***, Vol. 48, pp. 313-317, 1979.

[11] Gonzalo Álvarez Marañón, Luis Hernández Encinas, Ángel Martín del Rey, “A New Secret Sharing Scheme for Images Based on Additive 2-Dimensional Cellular Automata”, ***pringer-Verlag Berlin Heidelberg***, Vol. 3522, pp.411-418, 200543

[12] Karnin, E. Greene, J. Hellman, “On Secret Sharing Systems”, ***IEEE Transactions on nformation Theory***, Vol. 29, PP. 35-41, 1983

[13] M. Noar, A. Shamir, “Visual Cryptogrphy”, ***Advances in Cryptology : Eurpocrypt’94, pringer-Verlag, Berlin***, pp. 1-12, 1995.

[14] Wang Mingsheng, Wang Guilin, Feng Dengguo, “A Secret Sharing Scheme Based On Linear Transformation”, ***Institute of Software, Chinese Academy of Science (ISCAS)***, pp. 134-139, 2001

[15] Yu-Shan Wu, Chih-Ching Thien, Ja-Chen Lin, “Sharing and Hiding Secret Images with Size Constraint”, ***The Journal of the Pattern Recognition Society***, Vol. 37, pp.1377-1385 , 2004.