明新科技大學　校內專題研究計畫成果報告

一個使用視覺密碼學技術的影像隱藏機制

An Image Hiding Scheme Using Visual Cryptography Technique

計畫類別：☐任務型計畫　☐整合型計畫　■個人計畫

計畫編號：MUST-97-資管-07

執行期間：97 年 01 月 01 日至 97 年 09 月 30 日

計畫主持人：詹森仁

共同主持人：

計畫參與人員：許志偉、陳振利、張淑玲、王婷瑤

處理方式：公開於校網頁

執行單位：資管系

中　華　民　國　九十七　年　九　月　三十　日

摘　要

早期的視覺密碼是一種利用秘密分享機制將機密影像加密成 n 張分享影像，解碼時只要疊合其中 k 張以上的分享影像，就能夠利用人類視覺系統直接解密，無需透過電腦運算；反之，小於 k 張則無法從中獲得任何與機密影像有關的資訊。然而早期的視覺密碼方法有像素擴展與分享影像不具任何意義的缺點。

相關學者提出新的視覺密碼方法，將機密影像利用簡單的數學運算嵌入偽裝影像當中，解密時，透過數學運算就能夠還原機密影像，這是不同於傳統視覺密碼的加密與解密方法，雖然不能直接利用人類視覺系統解密，但是也改善了傳統視覺密碼的像素擴展與分享影像不具任何意義等缺點。

本研究提出一種以秘密分享機制為基礎的灰階影像隱藏技術，其方法是將一張灰階機密影像分成個位數及百位數、十位數二部份，並分別嵌入至 1 張灰階輸入影像與 n-1 張灰階輸入影像當中。透過將機密影像像素值分解，再分別嵌入至灰階輸入影像中的方式，最少只要使用 4 張灰階輸入影像就能夠達到影像隱藏的目的，且所有的分享影像仍然能夠維持不錯的 PSNR 值，並且使攻擊者無法利用肉眼從分享影像中窺視出有關機密影像的任何資訊。解密時，只要取得所有的分享影像，再利用簡單的數學算式，就能夠還原機密影像。

關 鍵 詞：視覺密碼、秘密分享機制、機密影像、分享影像、影像隱藏

Abstract

Original visual cryptography is a secret sharing method that encrypts a secret image into *n* shares, and decrypts the image by overlaying *k* or more shares over each other without any computation. However, by inspecting less than *k* shares, one cannot gain any information on the secret image. The original visual cryptography have two weaknesses which are pixel expansion and noise-like shares.

A lecture review has showed that encrypts a secret image into input images and decrypts the image by applying simple arithmetic operations, which is difference from original visual cryptography. Although, it cannot decrypt by human visual system, it has improved pixel expansion and noise-like shares.

In this study. An image hiding technique based on secret sharing scheme has been proposed. The proposed method divides a gray value of the secret image into two separated parts: unit, hundreds and tens. After the gray value separated, one of the *n* input images was selected for unit encryption and the other input images for hundreds and tens. The experimental result has showed that all shared images similar to the origin input images with high PSNR. The gray value change of the share image if hardly identify by human visual system. Additionally, the decryption of secret image require only simply arithmetic operations to each share.

Keywords : visual cryptography, secret sharing scheme, secret image, share image, image hiding

目錄

表目錄

圖目錄

第一章　緒論

1-1 研究動機

隨著資訊科技與網際網路的發達，數位資訊已充斥在人們日常生活中的各個角落，其中數位影像更是最常在人們生活中出現的數位資訊，加上網路的普及，數位資訊的傳輸已成為電子化社會中生活的一部份。雖然，網路提升了人們生活的便利性，但也讓心懷不軌的人利用網路來犯罪，因此，網路安全、資訊安全與智慧財產權問題已是現代社會的一項重要課題。

影像隱藏（Image hiding）就是將機密影像（Secret image）嵌入到另一張影像中，這張用來嵌入機密影像的影像稱為（Cover image），嵌入後所得到的影像稱為偽裝影像（Stego image）。影像隱藏的目的在於保護數位影像的智慧財產權，避免未經授權的使用者利用其資訊進行犯罪。在這樣的安全需求下，便有學者提出將機密資訊分割成許多等份，再分給不同的參與者保管，只要有"足夠多"的參與者即可以取出原始機密資訊，這便是所謂的「秘密分享」。秘密分享機制[5, 15]是「秘密擁有者」將機密資訊分成多份，再各別分送給不同的參與者，解密時，要在某些參與者共同合作之下，才能夠獲得機密資訊。秘密分享機制擁有門檻（threshold）的概念，當參與者為 n，門檻值為 t，稱為「(t,n) -threshold 秘密分享機制」。

「視覺密碼機制」（Visual Cryptography Scheme）最初是由 Naor 與 Shamir 兩位學者於 1994 年提出[12]，是一種利用人類視覺系統來解密的秘密分享機制，主要應用於黑白影像。視覺密碼機制目前被廣泛的應用於安全實務上，如軍事用途、文件保護機制[6]、金鑰管理、數位浮水印[8]等方面。其運作原理是針對機密影像（Secret image）中所有的像素進行編碼，完成後便會得到藏有機密影像資訊的分享影像（Share images），每張分享影像所呈現出的都是雜亂且沒有規則，所以單靠一張分享影像是無法得到任何與機密影像有關的資訊。解密時，需將經過加密後的分享影像列印在透明投影片上，將全部的投影片疊合後，所產生的疊合影像（Recover image）便能利用人類視覺系統辨識出機密影像中的資訊。視覺密碼機制在解密時不需要大量電腦運算的時間成本，但是，美中不足的地方就是在加密編碼時，在原始機密影像上的每一個像素都會被擴展成 m（$m \geqq 2$）個像素，因此機密分享影像大小將會是原始機密影像的 m 倍，這樣的結果不僅會造成儲存空間的浪費，更會造成疊合影像的扭曲變形，導致解密時不易從疊合影像中辨識出機密影像的資訊。

為了解決上述視覺密碼機制於加密時會造成像素擴展的缺點，Ito 等學者 [15]利用基礎加密矩陣（basis matrices）來對機密影像進行加密編碼，加密後所產生的分享影像不會有像素擴展的問題。但是此方法每次都只針對單一像素加密，如此便很有可能導致疊合影像的辨識效果變差。侯永昌等學者[4]利用多點加密，以 2-out-of-2 視覺式秘密分享機制為例，一次針對連續兩個像素加密，此兩點稱為加密序列。此方法解決了像素擴展的問題，也改進了 Ito 等學者的視覺密碼機制在加

密時可能會破壞影像中黑點分佈的規律性的問題。

大多數的視覺密碼機制研究都著重在黑白影像，僅有少數著重灰階影像與彩色影像。侯永昌[9]利用 CMY 色彩模型與半色調技術，將彩色機密影像分成 C（青）、M（洋紅）、Y（黃）三張影像，再分別利用半色調技術二值化之後，採用黑白視覺密碼機制加密編碼，最後產生二張分享影像 Share-1 與 Share-2，只要疊合 Share-1 與 Share-2 便可從中得到原始機密影像的資訊。這套方法亦能夠使用在灰階機密影像上；美中不足的是有像素擴展的缺點。

上述各種不同的加密機制[7, 9, 10, 14, 15]所產生的分享影像，只有雜點並無包含任何有意義的資訊，雖然達到了影像隱藏的目的；然而，只有雜點的影像反而容易被惡意的攻擊者懷疑影像中是否藏有資訊，在網路上傳輸時，需承擔被竊取及破解分享影像的風險。

多位學者致力於將機密影像隱藏在有意義的影像中[11-13, 16]，其中學者 Kim 與 Choi 於 2005 年提出不同於前述視覺密碼機制的新方法[11, 12]，利用簡單的數學運算來對灰階機密影像進行加密與解密，在沒有遭受任何攻擊的條件下，能夠百分之百還原機密影像。其方法主要是將欲傳輸之機密影像利用簡單的運算式將其像素值分散至 n 張相同大小的灰階輸入影像當中。解密時，只要利用簡單的運算式即可從所有的分享影像中還原出來。但此方法由於要將一張機密影像的像素值分散至 n 張灰階輸入影像，可能會造成分享影像過多的缺點。此外，必須要取得所有的分享影像才能夠還原出機密影像中的資訊，如果沒有取得全部的分享影像，便無法還原出機密影像，將會使該方法的應用受到限制。

1-2 研究目的

本研究的目的是，希望改善視覺密碼機制的像素擴展問題，讓分享影像具有偽裝的資訊，以避免讓攻擊者起疑；同時希望改善 Kim 等學者之視覺密碼機制中分享影像過多，導致儲存空間的浪費以及實用性降低的問題。因此，本研究提出了一項新的技術，將灰階機密影像的像素值區分成百位數、十位數與個位數二部份，再將之分散至 n 張灰階輸入影像當中，產生 n 張分享影像。解密時，只要取得 n 張分享影像經過一些簡單的數學運算後，即可還原出機密影像。

本報告的其餘章節分別是，第二章為文獻探討，介紹視覺密碼機制與 Kim 等學者所提出之視覺密碼機制。第三章為我們所提出的方法。第四章為實驗與討論。第五章為結論。

第二章　　文獻探討

2-1 Naor 與 Shamir 之視覺密碼機制

Shamir[15]於 1979 年提出「秘密分享」的概念，機密資訊經過加密後，產生 *n* 份分享資訊，只要獲得 *k* 份以上（$k \leqq n$）的分享資訊，就能夠還原出機密資訊；若只獲得 *k*-1 份以下的分享資訊，就無法獲得任何與機密資訊有關的線索。之後，於 1994 年 Naor 與 Shamir 將此概念延伸應用至影像上，提出了視覺密碼機制，分享資訊不再是一連串的數值而是影像；解密時，只要將影像印在透明投影片上進行疊合，利用人類視覺系統即可直接進行解密，所以不用耗費大量的時間成本。

我們將以 2-out-of-2 視覺密碼機制來說明。圖 2.1.1 是 2-out-of-2 視覺密碼機制，機密影像上的黑點(白點)會依據圖 2.1.1 中黑點(白點)的加密規則被加密為兩個黑點兩個白點，每條加密規則被選用的機率皆相同。假設要加密的機密影像像素是白點，並隨機選取第一條加密規則，接著在 Share-1 依序填入黑白白黑，Share-2 填入黑白白黑，如此，當 Share-1 與 Share-2 疊合時便會呈現黑白白黑(兩黑兩白)；假設要加密的機密影像像素是黑點，並隨機選取第一條加密規則，接著在 Share-1 依序填入黑白白黑，Share-2 填入白黑黑白，如此，當 Share-1 與 Share-2 疊合時便會呈現全黑(四黑)。解密時，代表機密影像黑點的分享影像的 4 個子像素重疊後，黑點個數只要大於 2，便可利用黑白之間的對比使肉眼能夠辨識出機密影像中的資訊。

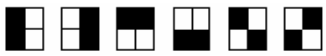
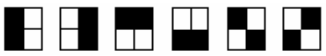
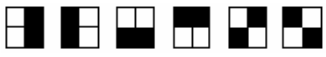
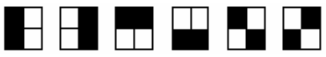
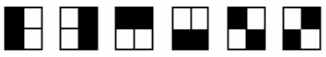
機密影像	機密影像像素（黑）	機密影像像素（白）
Share-1		
Share-2		
疊合影像		

圖 2.1.1 Naor 與 Shamir 所提出之視覺密碼機制

2-2 Kim 與 Choi 等學者之視覺密碼機制

Kim 與 Choi 等學者 [11,12]利用簡單的數學運算來進行加密與解密，解密方式不同於前述利用分享影像疊合的方式解密，而是使用簡單的數學運算來解密，雖然解密的速度較慢，但只需要花費少許的時間就能夠還原出像素不擴展的機密影像。此外，Kim 等學者的方法擁有能夠處理灰階機密影像的優點，將欲傳輸之灰階機密影像（Secret image）利用簡單的運算式將其像素值分散至 *n* 張相同大小的灰階輸入影像（Input image）當中。解密時，要先取得 *n* 張分享影像（Share image），

倘若分享影像都沒有受到損害，只要再利用簡單的運算式即可還原出百分之百的灰階機密影像。此機制的演算法可分為加密與解密兩階段：

加密階段：

$$P(i,j)=\sum_{k=1}^{n} I_k(i,j) \bmod v, \tag{2.2.1}$$

$$\sum_{k=1}^{n}\{I_k(i,j)\pm a(i,j)\}\equiv 0 \bmod v, \tag{2.2.2}$$

$$\sum_{k=1}^{n}\{I_k(i,j)\pm a(i,j)\pm b(i,j)\}\equiv T(i,j) \bmod v, \tag{2.2.3}$$

$$S_k(i,j)=I_k(i,j)\pm a(i,j)\pm b(i,j), \tag{2.2.4}$$

解密階段：

$$T(i,j)=\sum_{k=1}^{n} S_k(i,j) \bmod v, \tag{2.2.5}$$

假使要對機密影像T的像素$T(i,j)$進行加密時，必須先利用公式(2.2.1) 得到$P(i,j)$，$0\le \mathrm{P(i,j)}\le 255$，其中$v$表灰階值（當影像為 8-bit 灰階影像時，$v$ = 256)，再透過公式(2.2.2)將$P(i,j)$平均分散至 n 張輸入影像$I_k(i,j)$中，$1\le k\le n$，使得$P(i,j)$調整為 0，接著再將機密影像$T(i,j)$透過公式(2.2.3)平均分散至公式(2.2.2)的計算結果中，再利用公式(2.2.4)輸出分享影像。其中$a(i,j)$為$P(i,j)$分散至$I_k(i,j)$的數值，$a(i,j)$的總和等於$P(i,j)$；$b(i,j)$是$T(i,j)$分散至$I_k(i,j)$的數值，$b(i,j)$的總和等於$T(i,j)$。

解密時，只要取得“所有的”分享影像，再利用公式(2.2.5)便能夠還原機密影像，倘若分享影像皆無受損，則能夠百分之百還原出機密影像。透過公式(2.2.3)、(2.2.4)，我們不難發現在嵌入機密影像的過程中，都是利用加法或是減法，這也就表示即使分享影像的品質有輕微的降低，亦能夠利用公式(2.2.5)來進行還原機密影像，但此機密影像的品質不如原始機密影像。圖 2.2.1 為 Kim 等學者之視覺密碼機制示意圖。

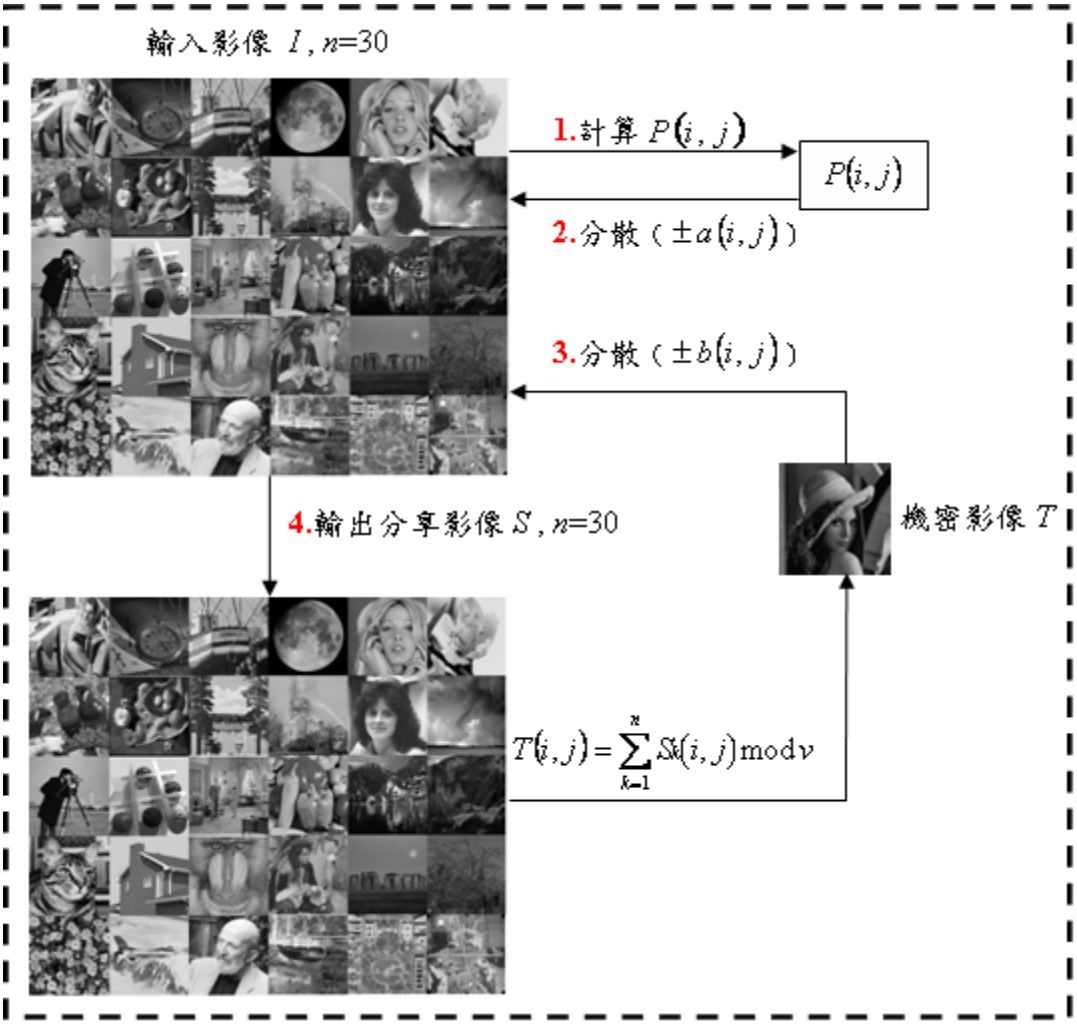


圖 2.2.1 Kim 等學者之視覺密碼機制示意圖

若 $c(i,j)$ 為 $P(i,j)$ 與 $T(i,j)$ 的差值，其計算方式為：（1）首先計算 $c(i,j)=T(i,j)-P(i,j)$；（2）將結果取絕對值 $|c(i,j)|$ 與 128 比較，如果小於 128，則 $c(i,j)=T(i,j)-P(i,j)$；（3）反之，如果大於等於 128，則 $c(i,j)=256-|T(i,j)-P(i,j)|$；透過這樣的方式使 $c(i,j)$ 達到最小，讓分散至 n 張輸入影像的值達到最小，使分享影像與輸入影像之間的像素值相差最小，讓攻擊者較不易察覺分享影像是有嵌入機密資訊的加工品，最重要的是能夠大幅降低輸入影像的數量。

圖 2.2.2 為 Kim 等學者之視覺密碼機制最佳化示意圖，在最佳化的情形下，即使將輸入影像數量減少一半，分享影像的品質仍相當不錯，不易用人眼窺視出影像是人為的加工品，仍然能夠達到影像隱藏的目的。

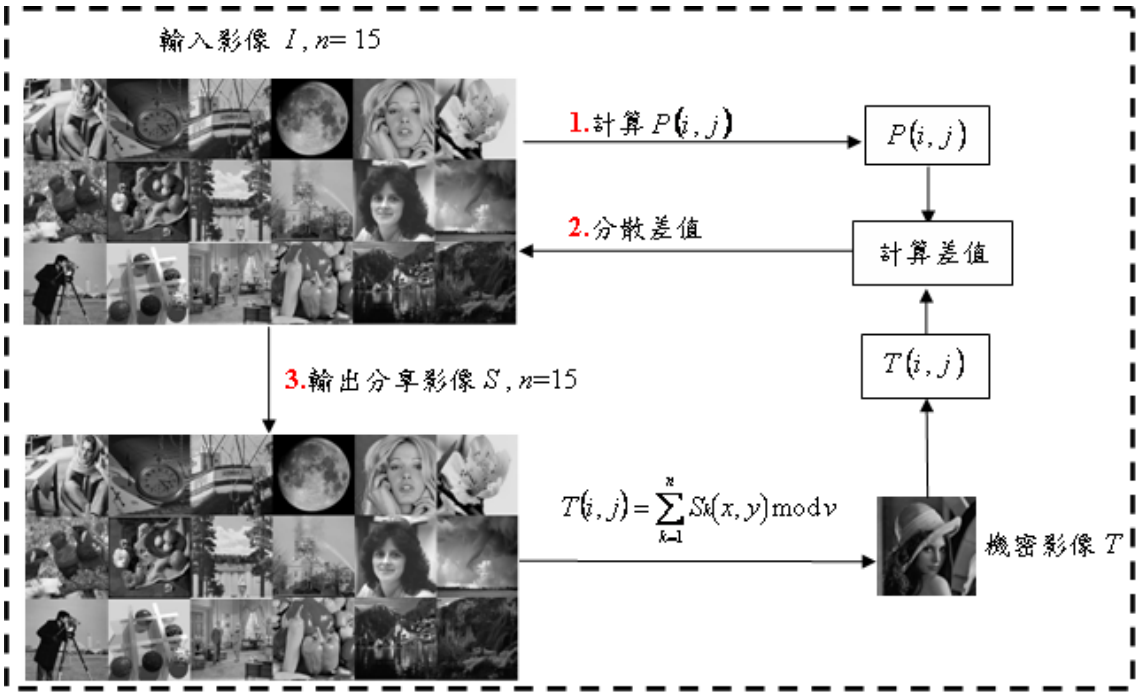


圖 2.2.2 Kim 等學者之視覺密碼機制最佳化示意圖

美中不足的是這套視覺密碼機制還是有些缺點，當要將一張灰階機密影像的像素值分散至 n 張灰階輸入影像時，在最差的情況下，即 $P(i,j)$ 與 $T(i,j)$ 相差 128，此時至少就需要 12~15 張的輸入影像才能夠將差值有效的分散，使攻擊者不易察覺這些影像是加工品。因此會造成分享影像過多，導致不易攜帶及浪費儲存空間的缺點。解密時，必須要取得所有的分享影像才能夠還原出機密影像中的資訊，如果因為網路的不穩造成封包的遺失，使得接收者沒有收到全部的分享影像時，那便無法還原出機密影像，將會使該方法的應用受到限制。若不考慮最佳化，則輸入影像需增加至 30 張才能夠隱藏機密影像的資訊，導致此機制在應用上更為困難。

第三章　秘密分享之影像隱藏方法

Kim 與 Choi 等學者所提出之視覺密碼機制，有分享影像過多，浪費儲存空間及應用性降低的缺點，且解密時，必須要取得所有的分享影像，否則將導致機密影像無法還原。因此，本研究將善用此機制的特性提出一套新的方法，以達到加密後只會產生少許分享影像，以降低儲存空間的浪費，且因為分享影像數量的降低，能夠使得應用性更為提高。

3-1 秘密分享機制於灰階影像隱藏之運作原理

本研究使用空間域影像隱藏的原理，結合秘密分享的概念，將一張灰階機密影像的像素值分成個位數及百位數、十位數二部份，先將個位數嵌入至 1 張輸入影像中，再將百位數與十位數分散嵌入至剩下的 n-1 張灰階輸入影像當中，且每張分享影像中皆隱藏著少許的資訊用來辨識分享影像所隱藏的資訊。透過將機密影像像素值分解，再分別嵌入至輸入影像中的方式，只要使用 4 張輸入影像就能夠達到影像隱藏的目的。解密時，只要取得所有的分享影像，再利用簡單的數學算式，就能夠還原機密影像。

本機制是建構在秘密分享機制的基礎條件上：必須取得所有的分享影像才能夠還原機密影像，只要少任何一張就無法還原出與機密影像有關的資訊。為了能夠更清楚的表達本機制的概念，我們將利用流程圖來說明。

圖 3.1.1 為秘密分享機制之灰階影像隱藏技術第零階加解密流程圖。我們的方法主要可以分成三個階段：影像前置處理、加密處理與解密處理。影像前置處理目的在於將灰階機密影像與輸入影像做分解的動作，使加密的過程更佳順利。加密處理則是利用前置處理產生出的資訊來製造分享影像。解密處理是透過收集所有的分享影像來還原出灰階機密影像；接下來將針對各種處理的細節加以描述。

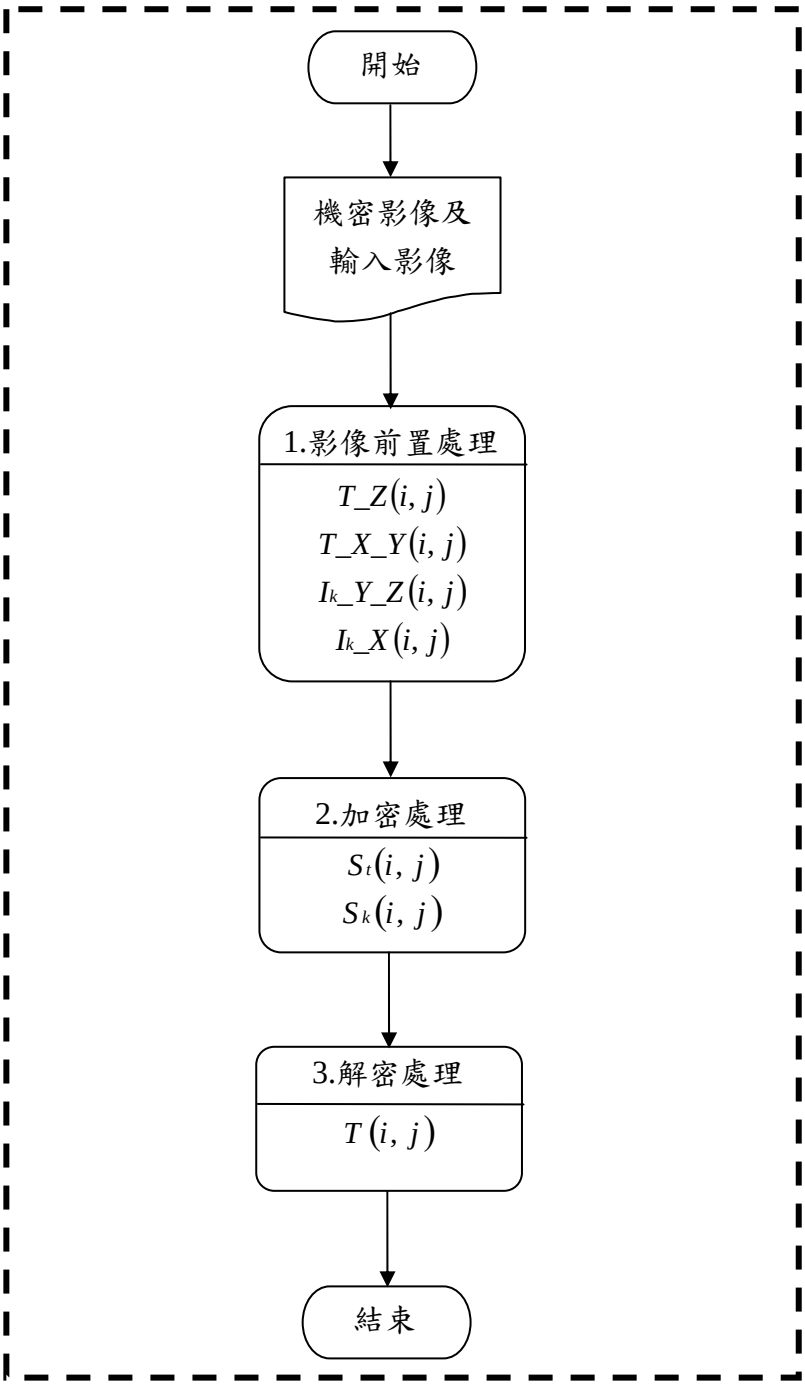


圖 3.1.1 秘密分享機制之灰階影像隱藏技術第零階加解密流程圖

1. 影像前置處理：

秘密分享機制之灰階影像隱藏技術影像前置處理分成兩個部份：灰階機密影像T及輸入影像I_k的像素值分解，如圖 3.1.2 所示。

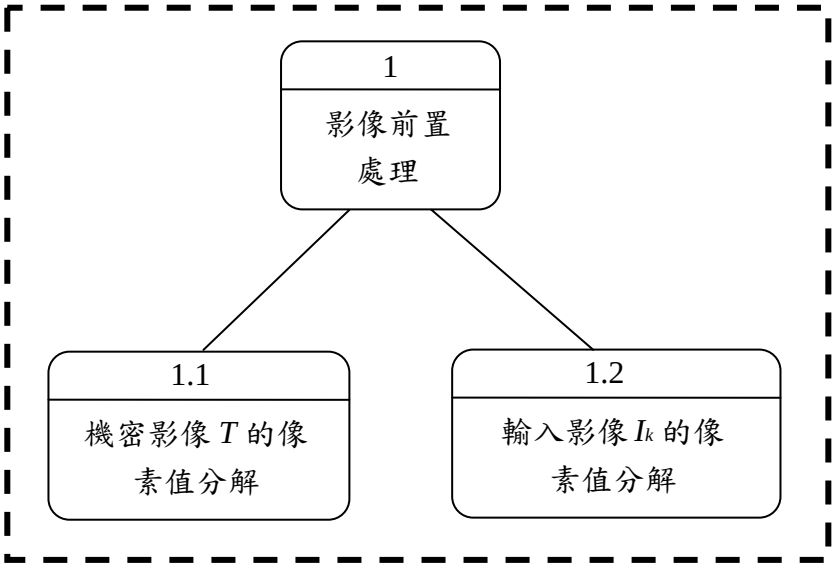


圖 3.1.2 秘密分享機制之灰階影像隱藏技術影像前置處理架構圖

1.1 灰階機密影像T的像素值分解：

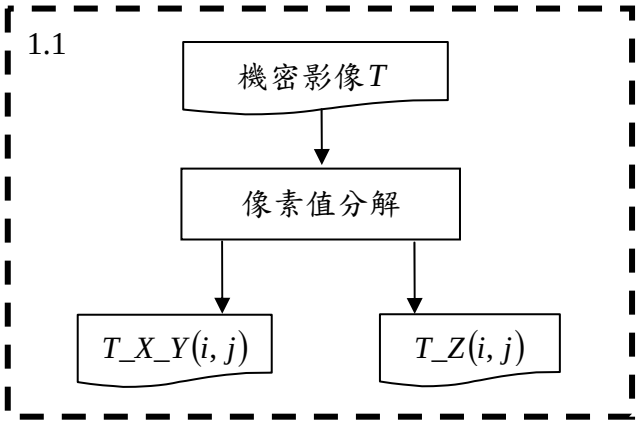


圖 3.1.3 灰階機密影像之像素值分解流程圖

圖 3.1.3 顯示將灰階機密影像$T(i,j)$的像素值分解成百、十位數($T\_X\_Y(i,j)$)及個位數($T\_Z(i,j)$)兩部份，例如：157 經過分解後，可得 15 及 7。

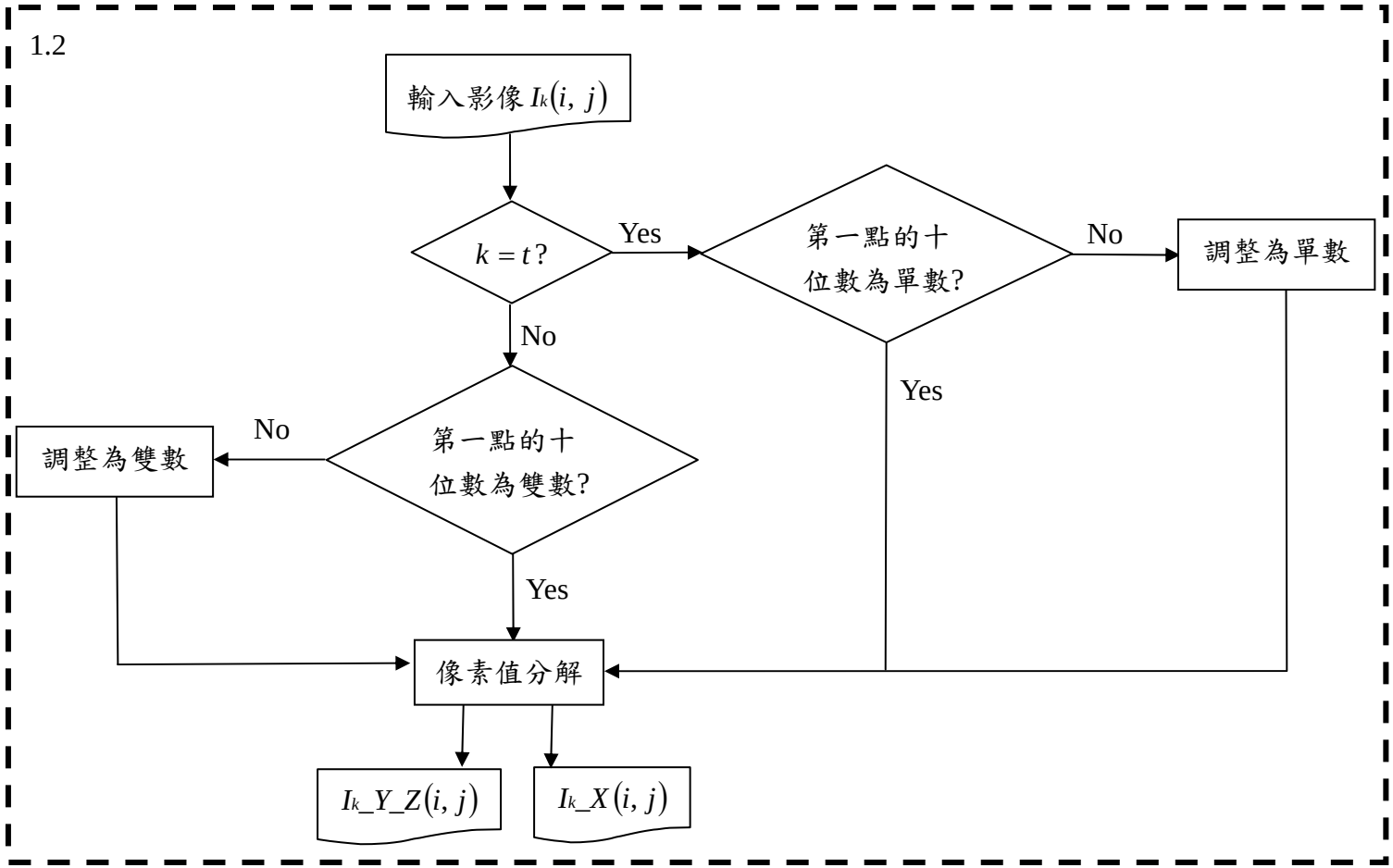


圖 3.1.4 輸入影像之像素值分解流程圖

1.2 輸入影像 I_k 的像素值分解：

如圖 3.1.4 所示，從 n 張輸入影像 $I_k(i,j)$，$k=1,\ldots,n$，先挑選一張輸入影像 $I_t(i,j)$ 來藏 $T\_Z(i,j)$，t 為 1 到 n 之間的一個整數，並使其第一個像素點(0,0)的十位數 mod 2 等於 1。再使 $n-1$ 張藏 $T\_X\_Y(i,j)$ 的輸入影像其第一個像素點(0,0)的十位數 mod 2 等於 0。再將 n 張輸入影像的像素值分解成百位數($I_k\_X(i,j)$)及十、個位數($I_k\_Y\_Z(i,j)$)。這麼做的原因是由於本機制對 $T\_Z(i,j)$ 與 $T\_X\_Y(i,j)$ 的加密方式不同，因此，解密時，必須要能夠區別出哪一張是藏 $T\_Z(i,j)$ 的分享影像，哪些是藏 $T\_X\_Y(i,j)$ 的分享影像才能夠進行解密。接著我們舉個例子說明輸入影像像素值分解的流程。假設藏 $T\_Z(i,j)$ 的輸入影像 I_2，$I_2(0,0)$ 為 221，將其十位數調整為單數，可以得到 211，經分解後可得 $I_2\_X(0,0)$ 為 2 及 $I_2\_Y\_Z(0,0)$ 為 11；假設輸入影像 I_3 是藏 $T\_X\_Y(i,j)$ 的輸入影像之一，$I_3(0,0)$ 為 155，將其十位數調整為雙數，可以得到 145，經分解後可得 $I_3\_X(0,0)$ 為 1 及 $I_3\_Y\_Z(0,0)$ 為 45。

2. 加密處理：

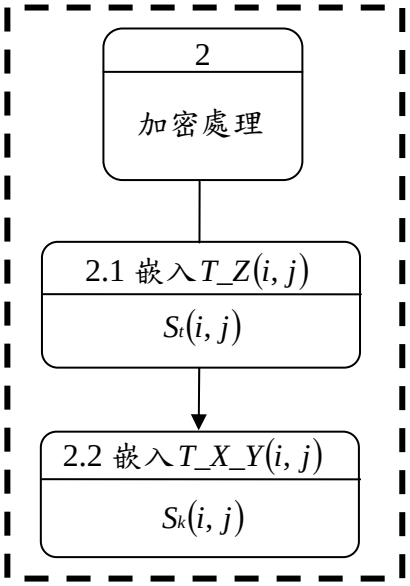


圖 3.1.5 秘密分享機制之灰階影像隱藏技術加密處理架構圖

秘密分享機制之灰階影像隱藏技術加密處理可以分成兩個部份：首先，先嵌入機密影像的 $T\_Z(i,j)$，緊接著再嵌入 $T\_X\_Y(i,j)$，如圖 3.1.5 所示。

2.1 嵌入機密影像$T_Z(i,j)$：

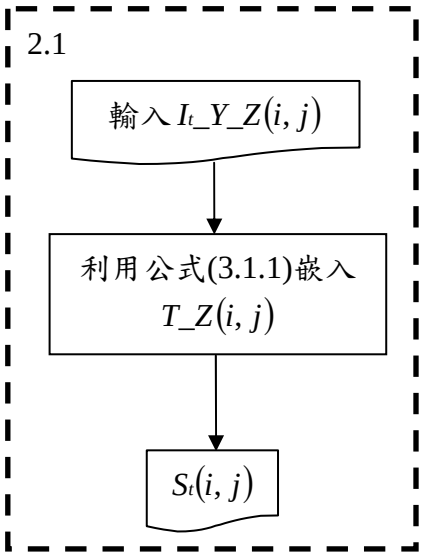


圖 3.1.6 嵌入機密影像 $T_Z(i,j)$之流程圖

由於$T_Z(i,j)$的重要性在影像中並不高，因此為了節省加密的時間，嵌入$T_Z(i,j)$的方式，見圖 3.1.6，就是將$T_Z(i,j)$直接取代要藏$T_Z(i,j)$的輸入影像其像素值的個位數。如公式(3.1.1)，t 代表藏$T_Z(i,j)$的輸入影像，$I_t_Z(i,j)$為第 t 張輸入影像座標(i,j)的個位數，加密完成後，便能夠獲得第 t 張分享影像$S_t(i,j)$。

$$S_t(i,j)=I_t\_X(i,j)\times 100+I_t\_Y\_Z(i,j)-I_t\_Z(i,j)+T\_Z(i,j), \qquad (3.1.1)$$

2.2 嵌入機密影像$T_X_Y(i,j)$：

由於本機制在解密時，必須利用分享影像上的第一個像素點的十位數來判斷該影像中隱藏的資訊為何，因此，$T_X_Y(0,0)$與其他點使用不同的嵌入方式，見圖 3.1.7。第一個像素點的加密方式：首先，將 n-1 張要藏$T_X_Y(i,j)$的輸入影像其第一個像素點的個位數調整為 0，再將$T_X_Y(0,0)$以“平均法”分散至 n-1 張輸入影像的個位數中。

其餘像素點的加密方式：首先，將已嵌入$T_Z(i,j)$的分享影像$S_t(i,j)$其十、個位數($S_t\_Y\_Z(i,j)$)，與其餘 n-1 張輸入影像的十、個位數($I_k\_Y\_Z(i,j)$)利用公式(3.1.2)計算$P_Y_Z(i,j)$，這個數值的目的是要用於計算與$T_X_Y(i,j)$之間的差值$a(i,j)$，$a(i,j)$的計算方式為：利用$T_X_Y(i,j)$減去$P_Y_Z(i,j)$，將結果取絕對值與 13 比較，如果小於等於 13，則 $a(i,j)=T\_X\_Y(i,j)-P\_Y\_Z(i,j)$；反之，如果大於 13，則 $a(i,j)=26-\left|T\_X\_Y(i,j)-P\_Y\_Z(i,j)\right|$，透過這樣的方式使$a(i,j)$達到最小，讓分散至 n-1 張輸入影像$I_k_Y_Z(i,j)$的$b(i,j)$最小，以達到最佳的嵌

入效果。

$$P\_Y\_Z(i,j)=\left\{\sum_{k=1}^{n-1} I_k\_Y\_Z(i,j)\right\}+S_t\_Y\_Z(i,j) \bmod 26, \tag{3.1.2}$$

公式(3.1.3)是將$T_X_Y(i,j)$嵌入至 $n-1$ 張輸入影像中的重要步驟。

$$\sum_{k=1}^{n-1}\{I_k\_Y\_Z(i,j)\pm b(i,j)\}\equiv T\_X\_Y(i,j) \bmod 26, \tag{3.1.3}$$

$b(i,j)$的選擇要非常小心，不能被攻擊者一眼就發現分享影像是人為加工品。當完成加密後，便能利用公式(3.1.4)取得第 k 張的分享影像。當整張機密影像的$T_X_Y(i,j)$嵌入完成後，可得 $n-1$ 張藏$T_X_Y(i,j)$的分享影像。

$$S_k(i,j)=I_k\_X(i,j)\times 100+I_k\_Y\_Z(i,j)\pm b(i,j), \tag{3.1.4}$$

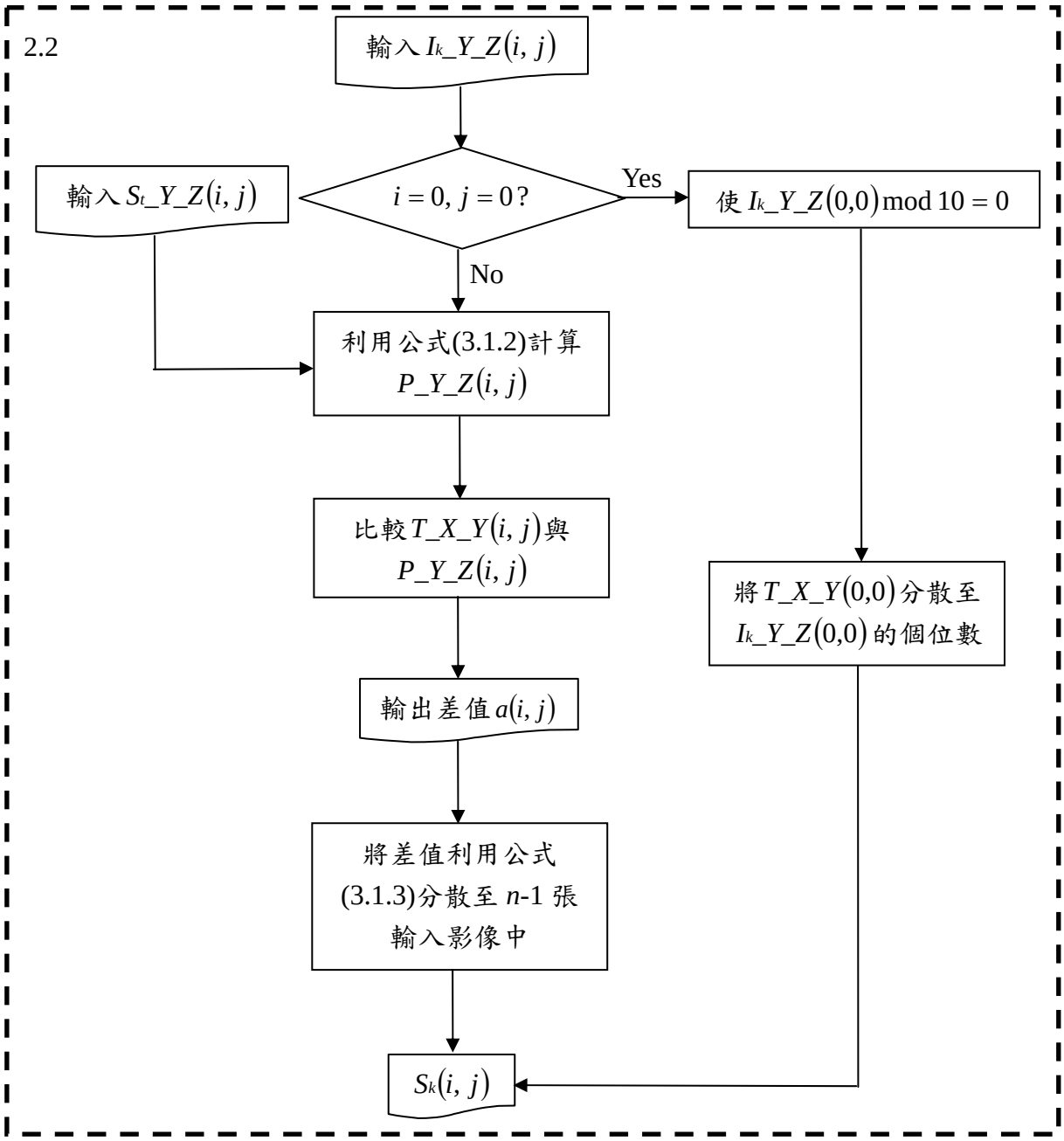


圖 3.1.7 嵌入機密影像 $T\_X\_Y(i,j)$ 之流程圖

為了更清晰地說明我們所提出的加密流程，我們將利用以下這個簡單的範例說明本機制的加密流程。

範例 1 假設 $I_k(1,1)$，$k=1,\ldots,5$，像素值分別為 25、50、86、170 及 221。$T(1,1)$ 的像素值為 50。

1. 假設選取第三張影像來藏 $T\_Z(1,1)$。經過影像前置處理後可得機密影像的 $T\_X\_Y(1,1)$ 為 5 及 $T\_Z(1,1)$ 為 0；5 張輸入影像的 $I_k\_X(1,1)$ 分別為 0、0、0、1 及 2，$I_k\_Y\_Z(1,1)$ 分別為 25、50、86、70 及 21。

2. 經過公式(3.1.1)後，$S_3(1,1)$為 80。
3. $P\_Y\_Z(1,1)=$ (25+50+70+21)+80 mod 26 = 12。
4. 比較$P_Y_Z(1,1)$與$T_X_Y(1,1)$，計算兩者之間的差值，可得-7。
5. 使用“平均法”將-7 分散至$I_k_Y_Z(1,1)$中，$k=1$、2、4、5，完成後，像素值分別為 23、48、68 及 20。輸出$S_k(1,1)$的像素值分別為 23、48、168 及 220。
6. 輸出$S_k(1,1)$，$k=1,\ldots,5$。

根據上述簡單地說明本機制的加密流程後，接著將說明本機制解密流程。

3. 解密階段：

如圖 3.1.8 秘密分享機制之灰階影像隱藏技術解密處理流程圖所示，解密處理亦可分成三個步驟：判斷哪張分享影像是藏$T_Z(i,j)$及哪些分享影像是藏$T_X_Y(i,j)$、取出機密影像的$T_Z(i,j)$及$T_X_Y(i,j)$，以及還原影像。

1.1 當取得 n 張分享影像時，首先要將分享影像第一個像素點(0,0)的十位數 mod 2，若結果為 1，即表示該分享影像是藏$T_Z(i,j)$，剩下的 $n-1$ 張分享影像則是藏$T_X_Y(i,j)$。

1.2 將藏$T_Z(i,j)$的分享影像利用公式(3.1.5)取出$T_Z(i,j)$。

$$T\_Z(i,j)=S_i(i,j)\bmod 10, \tag{3.1.5}$$

接著利用公式(3.1.6)與公式(3.1.7)從 n 張分享影像中取出$T_X_Y(i,j)$。由於第一個像素點(0,0)嵌入$T_X_Y(0,0)$的方式不同，所以取出時是利用公式(3.1.6)。其餘的像素點則使用公式(3.1.7)取出$T_X_Y(i,j)$。

$$T\_X\_Y(0,0)=\sum_{k=1}^{n-1}S_k(0,0)\bmod 10, \tag{3.1.6}$$

$$T\_X\_Y(i,j)=\sum_{k=1}^{n}S_k\_Y\_Z \bmod 26, \tag{3.1.7}$$

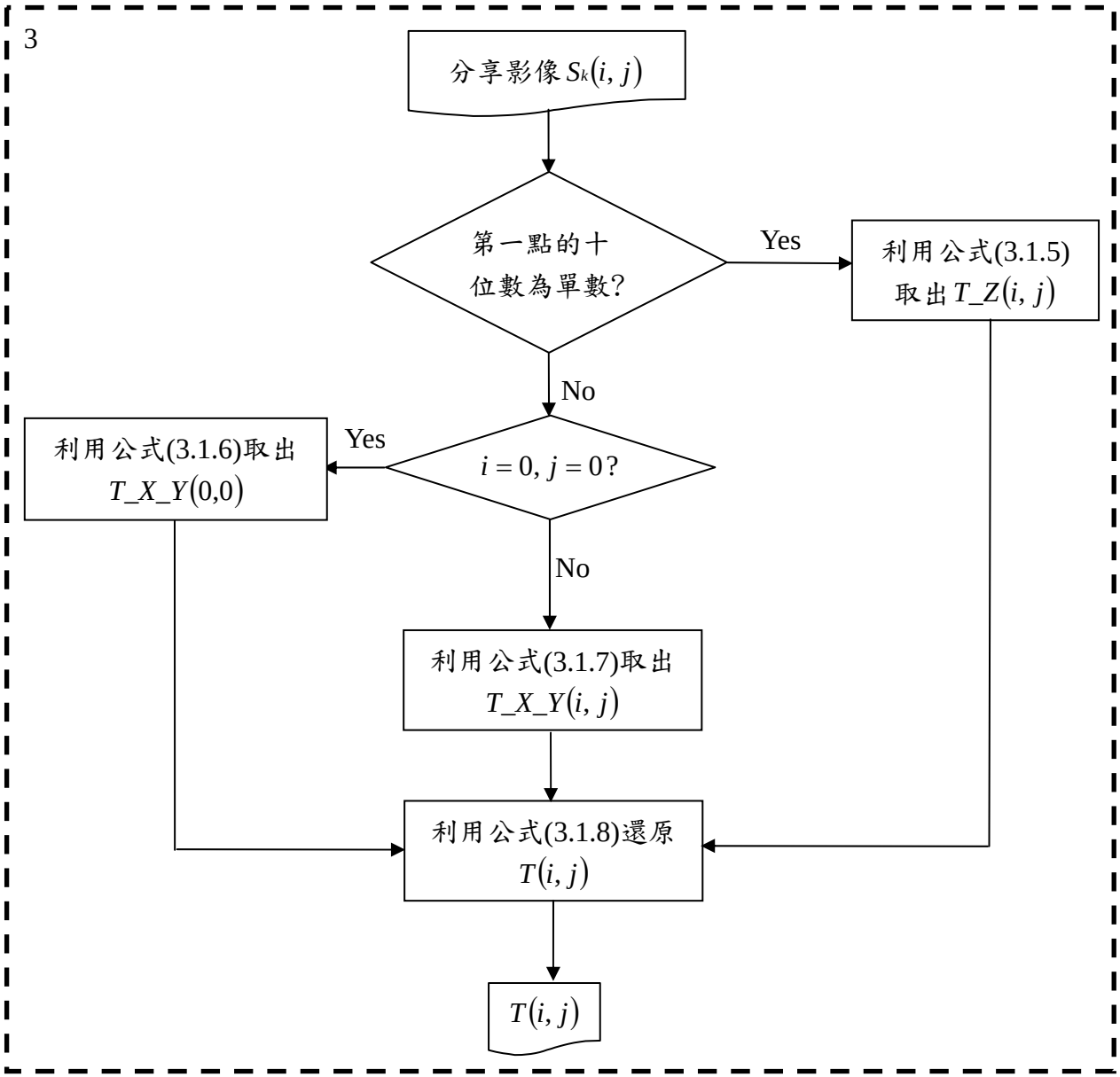


圖 3.1.8 秘密分享機制之灰階影像隱藏技術解密處理流程圖

1.3 當取得$T_X_Y(i,j)$與$T_Z(i,j)$後，經過公式(3.1.8)重組後即可還原機密影像$T(i,j)$。

$$T(i,j)=T\_X\_Y(i,j)\times 10+T\_Z(i,j), \tag{3.1.8}$$

在簡單地說明本機制的解密流程後，接下來我們要再利用先前的範例來說明，使大家能夠對解密流程更加清楚明白。

範例 2 假設我們取得$S_k(1,1)$，$k=1,\ldots,5$，像素值分別為 23、48、80、168 及 220。假設在第一個像素點(0,0)已經判斷出藏$T_Z(i,j)$為第三張分享影像。

1. 運用公式(3.1.5)可以從$S_3(1,1)$中取出$T_Z(1,1)$，80 mod 10 = 0。接著運用公式(3.1.7)從$S_k(1,1)$中，$k=1,\ldots,5$，取出$T_X_Y(1,1)$，(23+48+80+68+20) mod 26 = 5。

2. 取得$T_X_Y(1,1)$與$T_Z(1,1)$後，運用公式(3.1.8)重建機密影像$T(1,1)$，$5\times10+0=50$。

3-2 秘密分享機制之灰階影像隱藏技術安全性分析

此章節將探討上一節所提出之方法，遭受到攻擊者竊取部份分享影像時，攻擊者是否能夠從少數的分享影像破解出灰階機密影像。我們以 3.1 節範例 2 的分享影像來進行模擬。針對攻擊者取得的分享影像中所隱藏的資訊，與取得分享影像的數量，使用不同的範例來證明本機制的安全性。

模擬情境一：假設攻擊者少取得一張藏$T_X_Y(i,j)$的分享影像。

範例 3 假設攻擊者偷到$S_k(1,1)$，$k=1,\ldots,4$，像素值分別為 23、48、80 及 168，假使攻擊者已經破解了藏在$S_3(1,1)$中的$T_Z(1,1)$，得知$T_Z(1,1)$為 0，接下來想要從這 4 張分享影像中破解出$T_X_Y(1,1)$，將$S_1_Y_Z(1,1)$、$S_2\_Y\_Z(1,1)$、$S_3_Y_Z(1,1)$及$S_4_Y_Z(1,1)$利用公式(3.1.7)計算後，所取出的值為 11，因此重建出的像素值為 110，與機密影像$T(1,1)$的 50 相差甚遠。

模擬情境二：假設攻擊者僅取得一張藏$T_X_Y(i,j)$的分享影像。

範例 4 假設攻擊者偷到$S_1(1,1)$，像素值為 23，欲從這張分享影像中破解出$T_X_Y(1,1)$，因此將$S_1_Y_Z(1,1)$利用公式(3.1.7)計算後，所取出的值為 23，因此重建出的像素值為 230，與機密影像$T(1,1)$的 50 相差甚遠。

模擬情境三：假設攻擊者少取得藏$T_Z(i,j)$的分享影像。

範例 5 假設攻擊者取得所有藏$T_X_Y(1,1)$的分享影像$S_k(1,1)$，$k=1$、2、4、5，像素值分別為 23、48、168 及 220，欲從這 4 張分享影像中破解出$T_X_Y(1,1)$，將$S_1_Y_Z(1,1)$、$S_2\_Y\_Z(1,1)$、$S_4_Y_Z(1,1)$及$S_5_Y_Z(1,1)$利用公式(3.1.7)計算後，所取出的值為 3，因此重建出的像素值為 30，與機密影像$T(1,1)$的 50 仍有些差距。

模擬情境四：假設攻擊者僅取得藏$T_Z(i,j)$的分享影像。

範例 7 假設攻擊者僅取得藏$T(1,1)$的分享影像$S_3(1,1)$，像素值為 80，因此只能夠從此分享影像利用公式(3.1.5)取出$T(1,1)$，其值為 0，因此重建出的像素值為 0，與機密影像$T(1,1)$的 50 相差甚遠。

透過以上四個模擬情境與四個對應的範例，我們可以了解，無論攻擊者取得藏$T_X_Y(i,j)$或是藏$T_Z(i,j)$的分享影像，只要少竊取到任何一張分享影像，就無法輕易的破解出機密影像的資訊，即使攻擊者採取「暴力破解法」來進行破解，在攻擊者不知道機密影像資訊的情況下，亦無法還原機密影像$T(i,j)$。因此，本機制的安全性是足夠的。

第四章　實驗結果與討論

4-1 秘密分享機制之灰階影像隱藏技術實作

為了驗證第三章所提出之方法，我們使用 DEV C++語言將所提出之方法實作出來。我們所使用的灰階機密影像為圖 4.1.1 的“Lena”（128×128 pixels）。為了增加實驗結果的可信度，我們嘗試以各種不同的灰階輸入影像來進行實驗；同時，我們也依照灰階輸入影像的對比將輸入影像分成三類作測試：一般對比、低對比以及高對比灰階輸入影像，以探討不同對比的灰階輸入影像是否會對本機制的分享影像品質造成影響。

圖 4.1.1 灰階機密影像“Lena”

由於，透過本機制加密處理後的分享影像皆無法以人眼辨識其與原圖的差異，因此，我們使用影像信號雜訊比（Peak Signal to Noise Ratios, PSNR）作為分享影像品質的評估工具。PSNR 值的定義如公式(4.1.1)所示。

$$PSNR = 10 \times \log\left(\frac{255^2}{MSE}\right), \tag{4.1.1}$$

MSE（Mean Square Error）是均方差，MSE 值的計算方式如公式(4.1.2)：

$$MSE = \frac{\sum_{n=1}^{FrameSize} (I_n - P_n)^2}{FrameSize}, \tag{4.1.2}$$

I_n 是指原始影像第 n 個像素值，P_n 是指經處理後第 n 個的像素值。PSNR 的單位為 dB。一般而言，當經過處理的影像 PSNR 值大於 30 dB 時，人眼就不易發現該影像與原影像的差異性。

- 一般對比之灰階輸入影像：

  在實驗一中，我們將把圖 4.1.1 的“Lena”嵌入至圖 4.1.2 的 15 張灰階輸入影像（128×128 pixels）。緊接著在實驗二中，將只使用 4 張灰階輸入影像來嵌入機密影像的資訊，以驗證本機制可以有效的降低分享影像的數量，且能夠達到資訊隱藏的目的。

圖 4.1.2 實驗一之 15 張灰階輸入影像

實驗一 將圖 4.1.1 “Lena” 的 $T\_X\_Y(i,j)$ 嵌入至圖 4.1.2 的 14 張灰階輸入影像（128×128 pixels），$T\_Z(i,j)$ 藏於圖 4.1.2 的 “mandrill” 中。

圖 4.1.3 實驗一之 15 張分享影像

經加密處理後，輸出 15 張分享影像（128×128 pixels），如圖 4.1.3 所示。

(a)輸入影像 1 “Barbara”

(b)輸入影像 2 “Bird”

(c)輸入影像 3 “Woman_darkhair”

(d)輸入影像 4 “Cat”

圖 4.1.4 實驗二之灰階輸入影像

實驗二 圖 4.1.4(a)、(b)、(c)藏“Lena”的$T_X_Y(i,j)$，圖 4.1.4(d)藏“Lena”的$T_Z(i,j)$。

(a)分享影像 1

(b)分享影像 2

(c)分享影像 3

(d)分享影像 4

圖 4.1.5 實驗二之分享影像

經加密處理後，可以得到 4 張分享影像（128×128 pixels），如圖 4.1.5 所示。

表 4.1.1 為當輸入影像為一般對比灰階影像時，透過本機制加密後所輸出的分享影像其 PSNR 值。

表 4.1.1 一般對比灰階輸入影像實驗結果之 PSNR 值

實驗序號	灰階輸入影像	灰階機密影像	PSNR [dB]	平均 PSNR [dB]
實驗一	Barbara	Lena	51.47 dB	50.39 dB
	Woman_darkhair		51.46 dB	
	Bird		51.35 dB	
	Cat		51.50 dB	
	Cameraman		51.30 dB	
	Clock		51.50 dB	
	Flower		51.35 dB	
	Fruit		51.53 dB	
	Hacker		51.47 dB	
	House		51.54 dB	
	F-16		51.51 dB	
	Boat		51.36 dB	
	Lake		51.27 dB	
	Livingroom		51.33 dB	
	Mandrill		35.88 dB	
實驗二	Barbara	Lena	40.03 dB	38.94 dB
	Bird		39.96 dB	
	Woman_darkhair		39.93 dB	
	Cat		35.85 dB	

如表 4.1.1 所示，透過本機制所輸出的分享影像，藏$T_X_Y(i,j)$的分享影像其平均 PSNR 值皆可高達 39 dB 以上，甚至當使用 15 張灰階輸入影像時，其平均 PSNR 值更可高達 50.64 dB，這也就表示，我們所提出的機制當輸入影像愈多時，分享影像的品質愈接近原始輸入影像的品質，因此更能夠有效地欺瞞攻擊者，達到資訊隱藏的目的。在二個實驗中，都有一張分享影像與其餘分享影像的 PSNR 值有一些落差，是因為這張是藏$T_Z(i,j)$的分享影像，由於我們在嵌入$T_Z(i,j)$的方式，是直接取代藏$T_Z(i,j)$那張輸入影像的個位數，因此，其像素值的變動量大約是$\pm 4 \sim \pm 5$左右，導致此分享影像的 PSNR 值大約在 35.8 dB 左右。

- 低對比之灰階輸入影像：

  在此類的實作測試中，我們仍舊使用圖 4.1.1 的“Lena”作為灰階輸入影

像。我們使用 Adobe Photoshop CS v8.0 的軟體降低本研究所使用的測試影像對比，以作為此實作測試之低對比灰階輸入影像。同樣地，我們使用影像信號雜訊比（Peak Signal to Noise Ratios, PSNR）作為分享影像品質的評估工具。

在實驗一中，我們將把圖 4.1.1 的“Lena”嵌入至圖 4.1.6 的 15 張低對比灰階輸入影像（128×128 pixels）。在實驗二中，將只使用 4 張低對比灰階輸入影像來嵌入機密影像的資訊，以驗證當輸入影像為低對比灰階影像時，本機制仍可以有效地降低分享影像的數量，並維持分享影像的品質，達到資訊隱藏的目的。

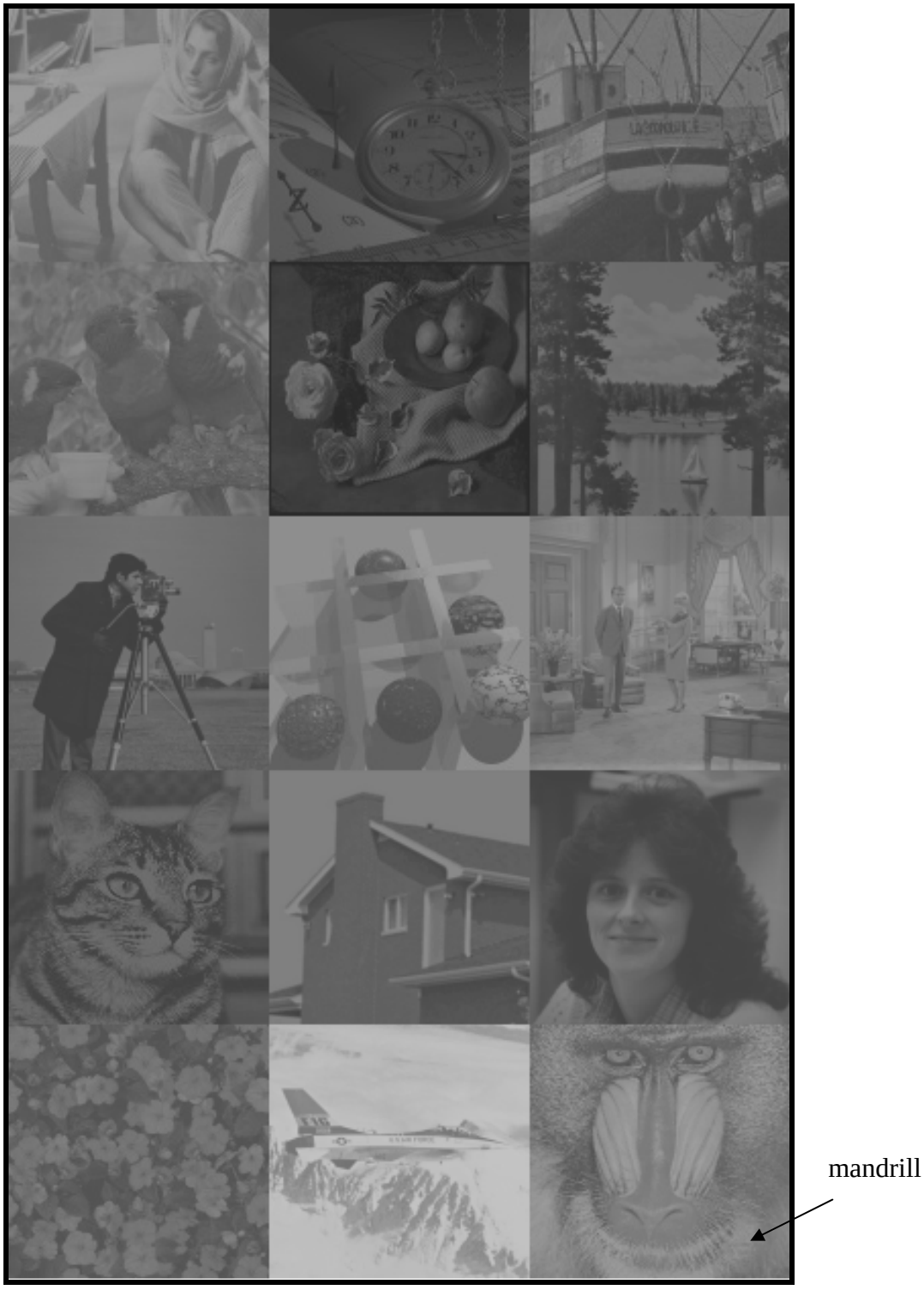


圖 4.1.6 實驗一之 15 張低對比灰階輸入影像

實驗一 將圖 4.1.1 “Lena” 的 $T\_X\_Y(i,j)$ 嵌入至圖 4.1.6 的 14 張低對比灰階輸入影像（128×128 pixels），$T\_Z(i,j)$ 藏於圖 4.1.6 的 “mandrill” 中。

圖 4.1.7 實驗一之 15 張分享影像

經加密處理後，輸出 15 張分享影像（128×128 pixels），如圖 4.1.7 所示。

(a)輸入影像 1 “Barbara”

(b)輸入影像 2 “Bird”

(c)輸入影像 3 “Woman_darkhair”

(d)輸入影像 4 “Cat”

圖 4.1.8 實驗二之低對比灰階輸入影像

實驗二 圖 4.1.8(a)、(b)、(c)藏“Lena”的百、十位數（$T\_X\_Y(i,j)$），圖 4.1.8(d)藏“Lena”的個位數（$T\_Z(i,j)$）。

(a)分享影像 1

(b)分享影像 2

(c)分享影像 3

(d)分享影像 4

圖 4.1.9 實驗二之分享影像

經加密處理後，可以得到 4 張分享影像（128×128 pixels），如圖 4.1.9 所示。

表 4.1.2 低對比灰階輸入影像實驗結果之 PSNR 值

實驗序號	低對比灰階輸入影像	灰階機密影像	PSNR [dB]	平均 PSNR [dB]
實驗一	Barbara	Lena	51.45 dB	50.35 dB
	Woman_darkhair		51.45 dB	
	Bird		51.28 dB	
	Cat		51.39 dB	
	Cameraman		51.42 dB	
	Clock		51.26 dB	
	Flower		51.36 dB	
	Fruit		51.36 dB	
	Hacker		51.41 dB	
	House		51.62 dB	
	F-16		51.36 dB	
	Boat		51.34 dB	
	Lake		51.36 dB	
	Livingroom		51.23 dB	
	Mandrill		35.93 dB	
實驗二	Barbara	Lena	39.79 dB	38.80 dB
	Bird		39.61 dB	
	Woman_darkhair		39.90 dB	
	Cat		35.90 dB	

採用低對比灰階輸入影像做為測試影像，是為了測試當所有輸入影像中的某些像素點利用 $\sum_{k=1}^{n-1} I_k\_Y\_Z(i,j)$ 的結果小於 $|a(i,j)|$。假使 $a(i,j)$ 為負數，將導致公式(3.1.3)不可以使用 $-b(i,j)$，因為不夠減，所以必須使用 $+b(i,j)$，因此，要分散到 $I_k\_Y\_Z(i,j)$ 的 $b(i,j)$ 就會增加，導致沒辦法將 $a(i,j)$ 以最佳化的形態進行分散。接下來我們來看當使用的輸入影像為低對比灰階影像時，分享影像的平均 PSNR 值，如表 4.1.2 所示。可以發現表 4.1.2 與表 4.1.1 所顯示的 PSNR 值沒有太大的差異，這也就表示，本機制不會因為輸入影像為低對比灰階輸入影像，而造成藏 $T\_X\_Y(i,j)$ 與藏 $T\_Z(i,j)$ 分享影像的品質大幅降低，導致攻擊者察覺到分享影像是人為的加工品。

- 高對比之灰階輸入影像：

在看過低對比灰階輸入影像的實驗結果後，接著，我們將使用高對比灰階輸入影像進行實驗，此實驗中仍使用圖 4.1.1 的“Lena”作為灰階輸入影

像。我們使用 Adobe Photoshop CS v8.0 的軟體增加本研究所使用的測試影像對比，以作為此實作測試之高對比灰階輸入影像。同樣地，我們使用影像信號雜訊比（Peak Signal to Noise Ratios, PSNR）作為分享影像品質的評估工具。

在實驗一中，我們將把圖 4.1.1 的“Lena”嵌入至圖 4.1.10 的 15 張高對比灰階輸入影像（128×128 pixels）。在實驗二中，將只使用 4 張高對比灰階輸入影像來嵌入機密影像的資訊，以驗證當輸入影像為高對比灰階影像時，本機制仍可以有效地降低分享影像的數量，並維持分享影像的品質，達到資訊隱藏的目的。

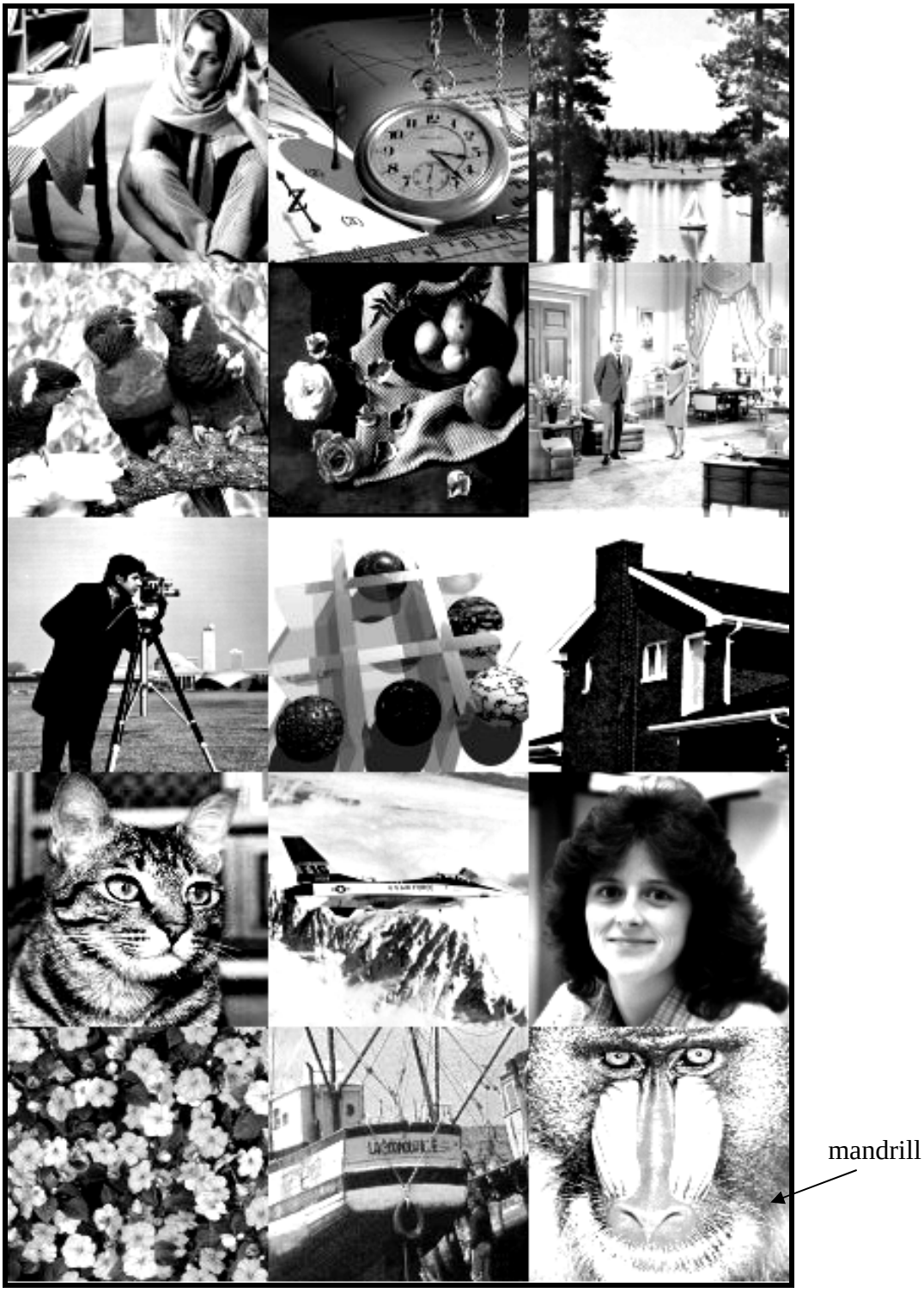


圖 4.1.10 實驗一之 15 張高對比灰階輸入影像

實驗一 將圖 4.1.1 “Lena” 的 $T\_X\_Y(i,j)$ 嵌入至圖 4.1.10 的 14 張高對比灰階輸入影像（128×128 pixels），$T\_Z(i,j)$ 藏於圖 4.1.10 的 “mandrill” 中。

圖 4.1.11 實驗一之 15 張分享影像

經加密處理後，輸出 15 張分享影像（128×128 pixels），如圖 4.1.11 所示。

(a)輸入影像 1 “Barbara”

(b)輸入影像 2 “Bird”

(c)輸入影像 3 “Woman_darkhair”

(d)輸入影像 4 “Cat”

圖 4.1.12 實驗二之高對比灰階輸入影像

實驗二 圖 4.1.12(a)、(b)、(c)藏“Lena”的百、十位數（$T\_X\_Y(i,j)$），圖 4.1.12(d)藏“Lena”的個位數（$T\_Z(i,j)$）。

(a)分享影像 1

(b)分享影像 2

(c)分享影像 3

(d)分享影像 4

圖 4.1.13 實驗二之分享影像

經加密處理後，可以得到 4 張分享影像（128×128 pixels），如圖 4.1.13 所示。

表 4.1.3 高對比灰階輸入影像實驗結果之 PSNR 值

實驗序號	高對比灰階輸入影像	灰階機密影像	PSNR [dB]	平均 PSNR [dB]
實驗一	Barbara	Lena	51.23 dB	50.06 dB
	Woman_darkhair		51.32 dB	
	Bird		51.15 dB	
	Cat		50.99 dB	
	Cameraman		51.34 dB	
	Clock		50.89 dB	
	Flower		50.94 dB	
	Fruit		51.75 dB	
	Hacker		51.49 dB	
	House		52.46 dB	
	F-16		51.37 dB	
	Boat		50.58 dB	
	Lake		51.19 dB	
	Livingroom		51.01 dB	
	Mandrill		33.20 dB	
實驗二	Barbara	Lena	38.62 dB	37.42 dB
	Bird		39.09 dB	
	Woman_darkhair		38.72 dB	
	Cat		33.26 dB	

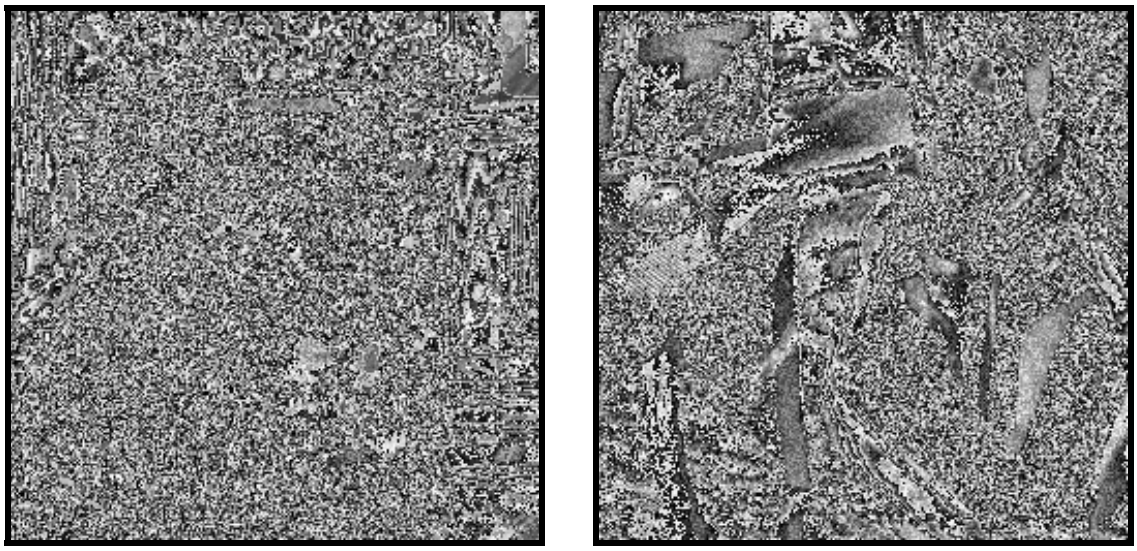
採用高對比灰階輸入影像做為測試影像，是為了測試當所有輸入影像中的某些像素點利用 $99-I_k\_Y\_Z(i,j)$ 與 $55-I_k\_Y\_Z(i,j)$ 計算每張輸入影像該點可分散多少 $b(i,j)$。因為在本機制中 $I_k\_Y\_Z(i,j)$ 的值介於 0~99 之間，我們不希望 0 減 1 後變 99，或是 99+1 後變成 0，所以只要該點像素值小於 200，便利用前者的方式計算，會使用 55 即代表該點的像素值大於等於 200，於是使用後者的方式計算，再將計算後的值加總起來，如果其結果小於 $|a(i,j)|$，假使 $a(i,j)$ 為正數，將導致公式(3.1.3)不可以使用 $+b(i,j)$，因為不夠加，所以必須使用 $-b(i,j)$，因此，要分散到 $I_k\_Y\_Z(i,j)$ 的 $b(i,j)$ 就會增加，導致沒辦法將 $a(i,j)$ 以最佳化的形態進行分散。接下來我們來看當使用的輸入影像為高對比灰階影像時，分享影像的平均 PSNR 值，如表 4.1.3 所示。可以發現表 4.1.3 的 PSNR 值比表 4.1.1 所顯示的 PSNR 值有稍稍降低的現象，但是其降低的幅度並不大。這也就表示，本機制不會因為輸入影像為高對比灰階輸入影像，

而造成藏$T_X_Y(i,j)$分享影像的品質大幅降低，導致攻擊者察覺到分享影像是人為的加工品。但是，卻會影響藏$T_Z(i,j)$分享影像的品質，主要是因為當輸入影像的對比與亮度拉大時，影像中會有許多像素點的像素值大於 250，在這樣的情形下，假使$T_Z(i,j)$的值大於 5，便無法順利取代輸入影像的個位數，因此，本機制對於當某一個像素點無法嵌入$T_Z(i,j)$的時候，我們會將其十位數減 10 後，再進行嵌入，因此，分享影像與輸入影像間像素值的差異可能高達 5~6，所以會導致藏$T_Z(i,j)$分享影像的 PSNR 值只有 33~34 dB。

透過這三類的實作測試後，我們發現灰階輸入影像的對比度較不易影響本機制所產生的分享影像品質，反倒是，灰階輸入影像的數量是影響分享影像品質的直接因素，話雖如此，即使只有少數的灰階輸入影像，本機制的分享影像品質無論是在視覺效果或是 PSNR 值中都有不錯的表現。

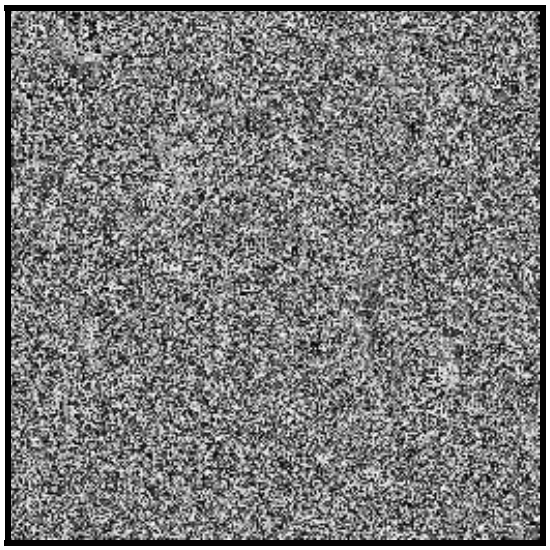
4-2 秘密分享機制之灰階影像隱藏技術安全性實作

為了驗證 3.2 節所探討的秘密分享機制之灰階影像隱藏技術遭受到攻擊者竊取到部份分享影像時，攻擊者是否能夠從少數的分享影像破解出灰階機密影像。我們利用圖 4.1.5 的分享影像來驗證本機制擁有相當高的安全性。

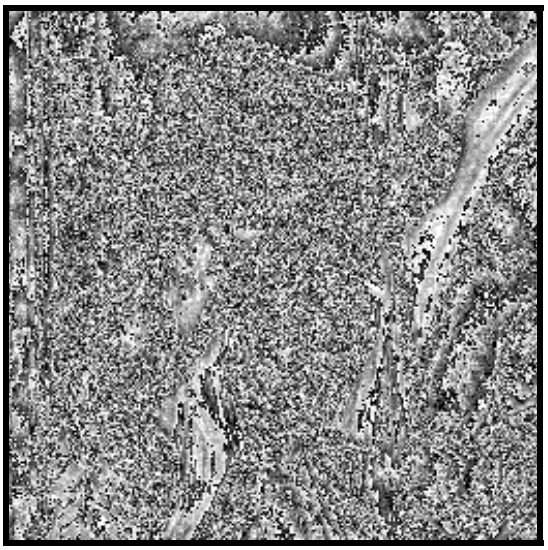


(a)少圖 4.1.5 藏$T_Z(i,j)$的分享影像 4　　(b)少圖 4.1.5 的分享影像 1

圖 4.2.1 秘密分享機制之灰階影像隱藏技術之安全性實作(cont.)



(c)少圖 4.1.5 分享影像 1 及分享影像 2



(d)僅有圖 4.1.5 藏$T_Z(i,j)$的分享影像 4

圖 4.2.1 秘密分享機制之灰階影像隱藏技術之安全性實作

當攻擊者沒有取得藏$T_Z(i,j)$的分享影像(少圖 4.1.5(d))時，其還原影像如圖 4.2.1(a)所示。僅取得兩張藏$T_X_Y(i,j)$與一張藏$T_Z(i,j)$共三張分享影像(少圖 4.1.5(a))，其還原影像結果如圖 4.2.1(b)所示。僅取得一張藏$T_X_Y(i,j)$與一張藏$T_Z(i,j)$共兩張分享影像(少圖 4.1.5(a)、圖 4.1.5(b))時，還原影像結果如圖 4.2.1(c)所示。由於僅取得藏$T_Z(i,j)$之分享影像(圖 4.1.5(d))，其還原影像中的只有$T_Z(i,j)$的資訊，換言之，在還原影像中每個像素點的像素值介於 0 至 9 之間，其視覺效果看起來有如一張全黑的影像，為了顯示出看似全黑的還原影像中有何資訊，因此，我們使用 PhotoImpact-10 對此影像進行等化處理，其結果如圖 4.1.5(d)所示。

從圖 4.2.1 與上段的描述可以發現，當攻擊者只要少取得任何一張分享影像時，便無法輕易還原出百分之百的灰階機密影像。因此，本機制能夠有效的防止攻擊者利用少數分享影像破解出灰階機密影像，亦表示本機制的安全性是足夠的。

接下來我們將測試本機制可以承受 JPEG 品質壓縮的程度，測試方式為從 JPEG 品質壓縮後的分享影像取出還原影像之 PSNR 值。本研究使用 PhotoImpact 10 對分享影像進行 JPEG 品質壓縮。本實驗所採用之分享影像為圖 4.1.5 之 4 張分享影像。表 4.2.1 為分享影像經 JPEG 品質壓縮後之 Average PSNR 值。表 4.2.2 為從經過 JPEG 品質壓縮後分享影像所取得的機密影像之 Average PSNR 值。

表 4.2.1 經 JPEG 品質壓縮後分享影像之 Average PSNR 值

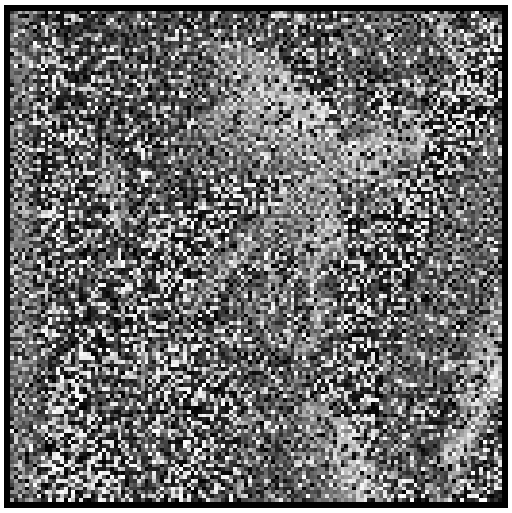
JPEG Compression Quality Factor [%]	Average PSNR [dB]
100	38.89 dB
95	38.25 dB
90	37.71 dB

表 4.2.2 自 JPEG 品質壓縮後分享影像取得的機密影像之 Average PSNR 值

JPEG Compression Quality Factor [%]	Average PSNR [dB]
100	22.44 dB
95	9.77 dB
90	8.54 dB

(a) 100% Quality Factor (b) 95% Quality Factor

圖 4.2.2 自 JPEG 品質壓縮後的分享影像所取得的機密影像(cont.)



(c) 90% Quality Factor

圖 4.2.2 自 JPEG 品質壓縮後的分享影像所取得的機密影像

本機制所產生之分享影像可以承受些微的 JPEG 品質壓縮，當分享影像經過 95%的 JPEG 品質壓縮後，從中所取出的還原影像還能夠分辨出一些機密影像輪廓資訊，如圖 4.2.2 (b)；但是，當分享影像經過 90%的 JPEG 品質壓縮後，則只能看到雜點以及些許與機密影像有關的資訊，如圖 4.2.2 (c)。這是因為本機制在加密時，是將機密影像的像素值較重要的百位數以及十位數藏於輸入影像的十位數及個位數中，當經過 JPEG 品質壓縮之後，分享影像的十位數與個位數資訊遭到破壞，因而導致還原影像嚴重失真。

4-3 Kim 等學者之視覺密碼機制實作

為了與 Kim 等學者之視覺密碼機制相比較，於是我們使用 DEV C++語言將 Kim 等學者的機制實作出來。為了與他們在同等的條件下相比較，因此在此章節我們同樣使用圖 4.1.1“Lena”（128×128 pixels）作為灰階機密影像為。同樣地，我們也會使用一般對比、低對比及高對比灰階輸入影像作為測試影像。以探討不同對比的灰階輸入影像是否會對 Kim 等學者機制的分享影像品質造成影響。

- 一般對比之灰階輸入影像：

  實驗一至實驗二所使用的灰階輸入影像分別為圖 4.1.2 與圖 4.1.4。其實驗結果分別如圖 4.3.1 及圖 4.3.2 所示。

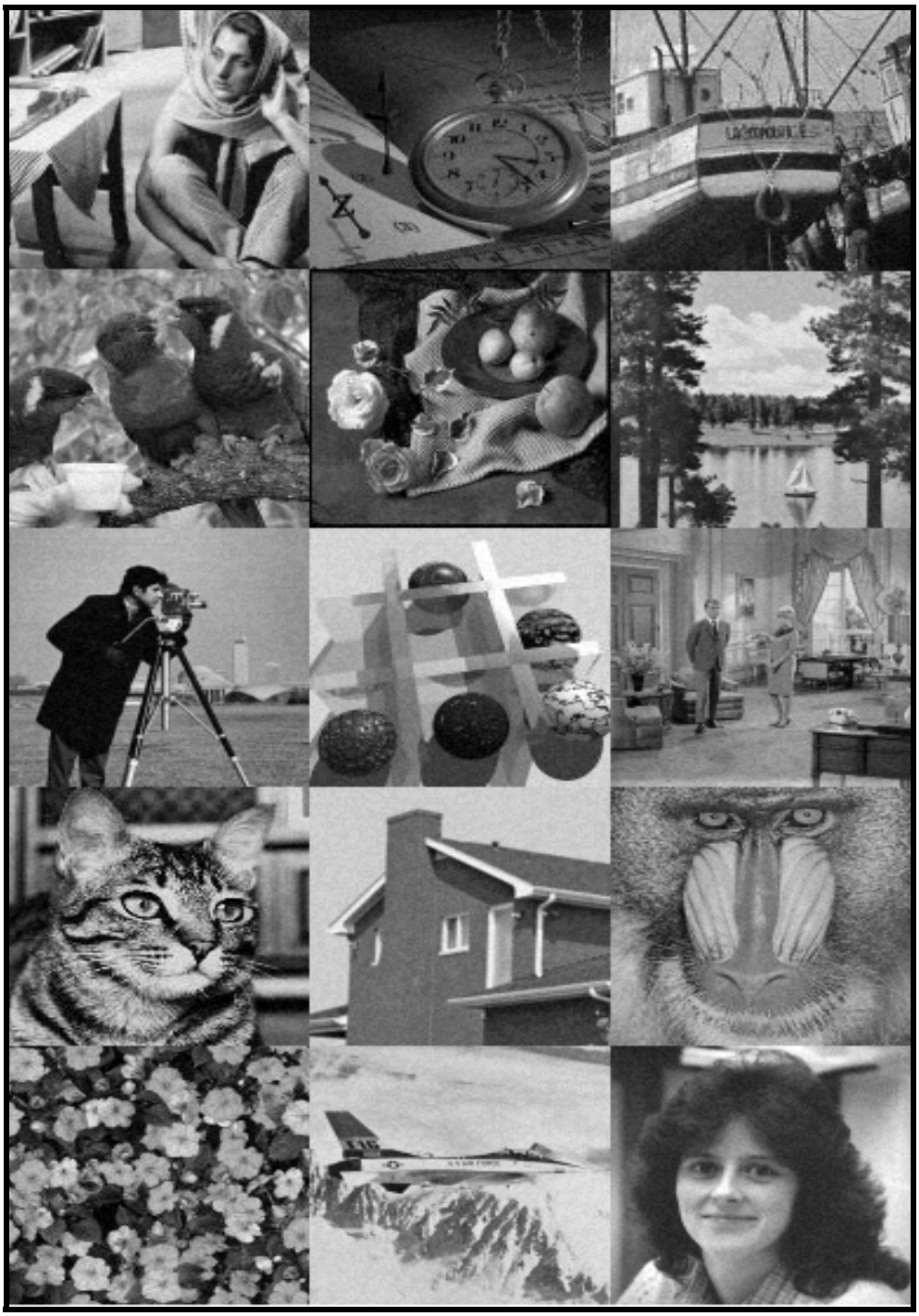


圖 4.3.1 實驗一之 15 張分享影像

(a)分享影像 1

(b)分享影像 2

(c)分享影像 3

(d)分享影像 4

圖 4.3.2 實驗二之分享影像

從實驗結果以及表 4.3.1 中，除實驗一的 15 張分享影像看起來還算可以接受外，實驗二的結果都是一眼就看出是加工品，無法達到欺瞞攻擊者的目的，非常不理想。透過以上這些實驗結果我們不難發現，Kim 等學者的機制必須要用龐大的輸入影像才可以隱藏灰階機密影像的資訊，加上此機制解密時，需要所有的分享影像才能夠還原出灰階機密影像，因此造成了此機制的實用性降低。

表 4.3.1 一般對比灰階輸入影像實驗結果之 PSNR 值

實驗序號	灰階輸入影像	灰階機密影像	PSNR [dB]	平均 PSNR [dB]
實驗一	Barbara	Lena	34.26 dB	34.28 dB
	Woman_darkhair		34.26 dB	
	Bird		34.26 dB	
	Cat		34.30 dB	
	Cameraman		34.26 dB	
	Clock		34.27 dB	
	Flower		34.30 dB	
	Fruit		34.37 dB	
	Hacker		34.30 dB	
	House		34.25 dB	
	F-16		34.26 dB	
	Boat		34.26 dB	
	Lake		34.27 dB	
	Livingroom		34.26 dB	
	Mandrill		34.26 dB	
實驗二	Barbara	Lena	22.81 dB	22.80 dB
	Bird		22.71 dB	
	Woman_darkhair		22.76 dB	
	Cat		22.93 dB	

- 低對比之灰階輸入影像：

我們將圖 4.1.1 的“Lena”嵌入至圖 4.1.6 的 15 張低對比灰階輸入影像（128×128 pixels）。觀察當輸入影像為低對比灰階影像時，Kim 等學者的機制是否仍可以維持分享影像的品質，達到資訊隱藏的目的。其結果之分享影像為圖 4.3.3。

圖 4.3.3 低對比灰階輸入影像之實驗結果

從圖 4.3.3 中，能夠清楚的發現分享影像當中隱隱約約洩露出機密影像的

輪廓，亦表示當輸入影像為 15 張低對比灰階影像時，Kim 等學者的機制無法有效地隱藏機密影像的資訊。接下來我們將測試以高對比灰階影像來當作輸入影像。

- 高對比之灰階輸入影像：

  我們將圖 4.1.1 的“Lena”嵌入至圖 4.1.10 的 15 張高對比灰階輸入影像（128×128 pixels），其結果之分享影像為圖 4.3.4。

圖 4.3.4 高對比灰階輸入影像之實驗結果

表 4.3.2 高對比灰階輸入影像實驗結果之 PSNR 值

實驗序號	高對比灰階輸入影像	灰階機密影像	PSNR [dB]	平均 PSNR [dB]
實驗一	Barbara	Lena	33.47 dB	33.51 dB
	Woman_darkhair		33.66 dB	
	Bird		33.50 dB	
	Cat		33.21 dB	
	Cameraman		33.50 dB	
	Clock		33.10 dB	
	Flower		33.11 dB	
	Fruit		33.69 dB	
	Hacker		33.88 dB	
	House		35.06 dB	
	F-16		33.92 dB	
	Boat		32.89 dB	
	Lake		33.50 dB	
	Livingroom		33.32 dB	
	Mandrill		32.92 dB	

由於從圖 4.3.4 分享影像的亮度與對比較高，因此我們的肉眼不易辨識出分享影像與輸入影像中的差異，因此我們利用 PSNR 值來觀察每張分享影像的品質，其結果能夠發現高對比的輸入影像，會導致 Kim 等學者視覺密碼機制的分享影像品質較差，其 PSNR 值最差是 32.89 dB。

從 Kim 等學者之視覺密碼機制的實作測試結果中可以發現，除了輸入影像的數量會影像該機制分享影像的品質外，輸入影像的對比度亦會影響分享影像的品質。Kim 等學者的機制受到許多限制，倘若選擇的輸入影像數量或是對比度不恰當，將會使其分享影像的品質大幅降低，導致攻擊者察覺到分享影像是人為的加工品。反倒是本報告所提出機制雖然在使用高對比灰階輸入影像時，分享影像的 PSNR 值在本報告所提出機制的表現是最差的，藏 $T_Z(i,j)$的分享影像品質只有 33~34 dB，但仍舊不易被攻擊者發現該分享影像是人為的加工品。這也就表示本報告所提出機制優於 Kim 等學者的視覺密碼機制。

4-4 本報告提出之機制與 Kim 等學者之視覺密碼機制之比較分析

在看過我們所提出的機制與 Kim 等學者的機制兩種資訊隱藏技術的實驗結果

後，我們將探討輸入影像的數量對兩機制的影響程度。其結果如圖 4.4.1 所示。

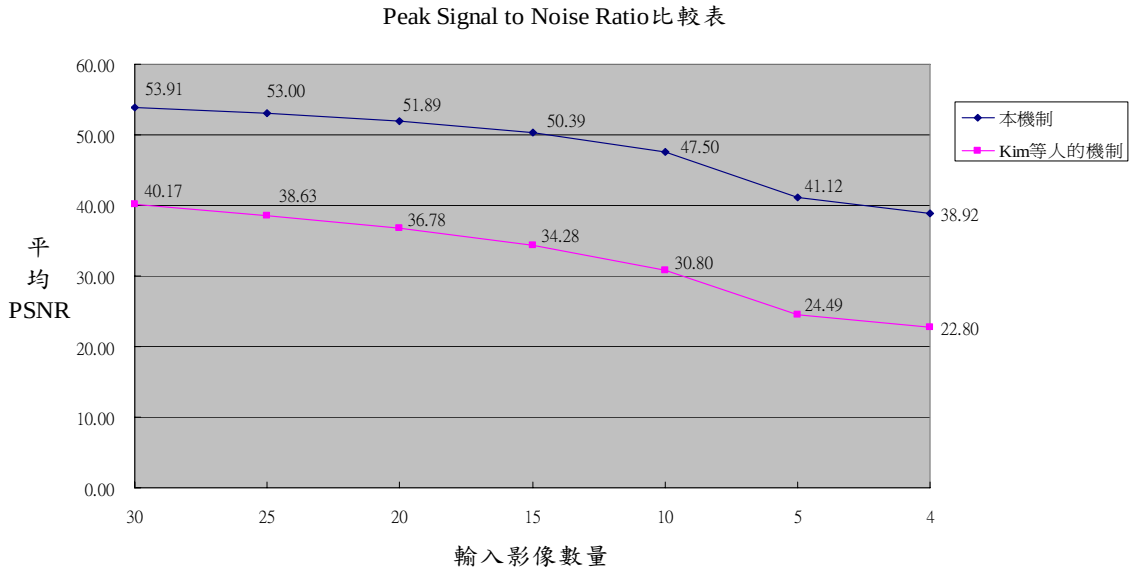


圖 4.4.1 輸入影像數量對兩機制之影響圖表

當輸入影像為 30 張時，我們的 Average PSNR 值高達 55.26 dB，Kim 等學者的機制其 Average PSNR 值為 40.17 dB。當輸入影像減少到只有 4 張時，我們的 Average PSNR 值為 38.92 dB，Kim 等學者之視覺密碼機制其 Average PSNR 值為 22.8 dB；這也就表示輸入影像數量與兩機制分享影像的品質成正比，當輸入影像數量愈多時，分享影像的品質愈接近原始輸入影像的品質。從圖 4.3.1 可以發現，輸入影像數量的增減，對 Kim 等學者的機制影響較大，尤其是當輸入影像減少至 10 張以下時，其分享影像的 PSNR 值已經在容許範圍 30 dB 上下，使得有些分享影像可能會洩露出一些機密影像的相關資訊；反觀，本研究所提出的「秘密分享機制之灰階影像隱藏技術」即使輸入影像只有 4 張，亦能將 Average PSNR 值維持在 38.92 dB，避免分享影像一眼就被攻擊者看穿是加工品。

第五章　結論與未來研究方向

為了改善 Kim 等學者之視覺密碼機制的缺點：分享影像過多，導致不易攜帶及浪費儲存空間。因此本研究提出秘密分享機制之灰階影像隱藏技術，將一張灰階機密影像分成百、十位數及個位數二部份，將個位數嵌入至一張輸入影像中，再將百、十位數分散嵌入至剩下的 n-1 張灰階輸入影像當中，且每張分享影像中皆隱藏著少許的資訊用來辨識分享影像所隱藏的資訊。透過將機密影像像素值分解，再分別嵌入至輸入影像中的方式，只要使用 4 張輸入影像就能夠達到影像隱藏的目的，且所有的分享影像仍然能夠維持不錯的 PSNR 值，並且使攻擊者無法利用肉眼從分享影像中窺視出有關機密影像的任何資訊。

此項技術不僅改善了 Kim 等學者的缺點，且當灰階輸入影像減少至 4 張時，仍可以維持相當不錯的 PSNR 值，無論是在客觀的評比，或是直接利用人眼去觀察分享影像，亦無法輕易的窺視出有關機密影像的資訊，因此更大大地提升了此技術的實用性與安全性。

大部份秘密分享技術只應用於黑白影像或灰階影像上，只有少許的學者將其應用於彩色影像上。一般而言，若直接將應用於灰階影像的秘密分享技術套用至 24-bit 全彩影像時，將彩色影像分成 RGB 三張灰階影像再分別進行秘密分享技術，此時，由於同時改變 RGB 三個顏色，如此，將可能會發生跨色階的問題，導致分享影像與原始機密影像的顏色有明顯落差，使得攻擊者一眼就看出分享影像是人為的加工品。因此，本研究未來的方向將探討如何將此機制套用於彩色影像上，相信更有助於秘密分享機制之灰階影像隱藏技術的應用。

參考文獻

1. 陳同孝，張真誠，黃國峰，*數位影像處理技術*，松崗電腦圖書資料股份有限公司，民 89 年。
2. 張真誠，陳同孝，黃國峰，*電子影像技術*，松崗電腦圖書資料股份有限公司，民 92 年
3. 繆紹綱譯，*數位影像處理*，普林斯頓國際有限公司，民 92 年。
4. 侯永昌，杜淑芬，許慶昇，“像素不擴展的視覺式秘密分享方法”，第十四屆全國資訊安全會議論文集，2004.06，第 508 - 515 頁。
5. Blakley, B., “Safeguarding Cryptographic Keys”, In Proceedings of the National Computer Conference, Vol. 48, 1979, pp. 313-317.
6. Chang, C. C., and Chuang, J. C., “An image intellectual property protection scheme for gray-level images using visual secret sharing strategy”, Pattern Recognition Letters, 23, 2002, pp. 931-941.
7. Lin, C. C., and Tsai, W. H., “Visual cryptography for gray-level images by dithering techniques”, Pattern Recognition Letters, 24, 2003, pp. 349-358.
8. Lou, D. C., Tso, H. K., and Liu, J. L., “A copyright protection for digital images using Visual Cryptography technique”, Computer Standards & Interfaces, 29, 2007, pp. 125-131.
9. Hou, Y. C., “Visual Cryptography for Color Images”, Pattern Recognition, 36, 2003, pp. 1619-1629.
10. Hou, Y. C., and Tu, S. F., “A Visual Cryptographic Technique for Chromatic Images Using Multi-pixel Encoding Method”, Journal of Research and Practice in Information Technology, Vol. 37, 2005, pp. 179-191.
11. Kim, H. J., and Choi, Y., “A New Visual Cryptography Using Natural Images”, IEEE International Symposium on Circuits and System, Vol. 6, 2005, pp. 5537-5540.
12. Kim, H. J., and Choi, Y., “Visual Secret Sharing Over Natural Images”, The 6th International Workshop on Image Analysis for Multimedia Interactive Services, WIAMIS 2005.
13. Nakajima, M., and Yamaguchi, Y., “Extended Visual Cryptography for Natural Images”, Proceedings of the 10th International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision, University of West Bohemia, Czech Republic, Vol. 1.2, 2002, pp. 303-310.
14. Naor, M., and Shamir, A., “Visual Cryptography”, in Advances in Cryptology-EUROCRYPT ’94, LNCS 950, 1995, pp. 1-12.
15. Ito, R., Kuwakado, H., and Tanaka, H., “Image Size Invariant Visual Cryptography”,

IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, Vol. E82-A:10, 1999, pp. 2172-2177.

16. Hwang, R. J., and Chang, C. C., “Hiding a picture in two pictures”, Optical Engineering. Vol. 40, 2001, pp. 342-351.
17. Shamir A., “How to Share a Secret”, Communication of the ACM, Vol. 22, 1979, pp. 612-613.

明新科技大學九十七年度校內專題研究計畫執行成果自評表

計 畫 類 別 ： □任務導向計畫 □整合型計畫 ■個人計畫
所 屬 院 (部) ： □工學院 ■管理學院 □服務學院 □通識教育部
執 行 系 別 ： 資管系(中心)
計 畫 主 持 人 ： 詹森仁 職 稱：助理教授
計 畫 名 稱 ： 一個使用視覺密碼學技術的影像隱藏機制
計 畫 編 號 ： MUST-97-資管-07
計畫執行時間： 97 年 1 月 1 日 至 97 年 9 月 30 日

計畫執行成效

教學方面

1. 對於改進教學成果方面之具體成效：

更了解資訊隱藏的演算法，及各演算法的優缺點，及目前的應用方向。

2. 對於提昇學生論文/專題研究能力之具體成效：

同學於實作過程中更加熟悉影像資訊的隱藏方法，研究結果已於國內研討會發表。

3. 其他方面之具體成效： 參與計畫之同學，熟悉研究過程中所探討之影像隱藏演算法與程式實作。

學術研究方面

1. 該計畫是否有衍生出其他計畫案 □是 ■否

計畫名稱：

2. 該計畫是否有產生論文並發表 ■已發表 □預定投稿/審查中 □否

發表期刊(研討會)名稱： 2008 現代管理與創新學術研討會

發表期刊(研討會)日期： 97 年 4 月 18 日

3. 該計畫是否有要衍生產學合作案、專利、技術移轉 □是 ■否

請說明衍生項目：

成果自評

計畫預期目標：研究、了解現有之影像隱藏方法、以期改進現有方法之缺點或提出新的解決方法，並探討可能支應用方向。

計畫執行結果：探究不同的影像隱藏方法，並了解各種方法之優缺點，提出以秘密方享機制為基礎之影像隱藏技術，並經由實作實驗證明，所提出之方法具有良好的效果。

預期目標達成率：98 %

其它具體成效：

於實作過程中，所寫作、測試完成之影像隱藏演算法程式，可供後續研究、比較之用途，亦可作為教學之範例。

(請下載使用達最大列印效率)