行政院國家科學委員會補助專題研究計畫　成果報告

影像的快速分享與高容量隱藏、及它們在影像修復的應用

Fast sharing, high-capacity hiding, and their applications in images' recovery

計畫類別：個別型計畫
計畫編號：NSC 97-2221-E-009-120-MY3
執行期間：97 年 8 月 1 日至 100 年 7 月 31 日

執行機構及系所：交通大學資訊工程系所

計畫主持人：林志青
共同主持人：無
計畫參與人員：陳李書滕、林憲正、李相賢

成果報告類型(依經費核定清單規定繳交)：完整報告

本計畫除繳交成果報告外，另須繳交以下出國心得報告：
□赴國外出差或研習心得報告
□赴大陸地區出差或研習心得報告
□出席國際學術會議心得報告
□國際合作研究計畫國外研究報告

處理方式： 涉及專利或其他智慧財產權，二年後可公開查詢

中　華　民　國　100　年　10　月 25　日

目錄

圖目錄

表目錄

中英文摘要及關鍵字

這是一個三年期計畫。第一年主題是快速影像分享;第二年主題是高容量資訊隱藏方法之設計與資訊隱藏量上限之探討;第三年主題是快速影像分享法與高容量資訊隱藏法在影像驗證與修復之應用。

第一年計畫(快速影像分享)的第一個子題是使用布林(Boolean)運算的快速機密影像分享法。在這個子題中，我們研究出一個新的機密影像分享法，不但分存影像所需要的儲存空間很小，而且解碼運算量也會非常少。該年第二個子題是多項式(t, n)分享方法的快速編碼與解碼。多項式機密分享法的優點是分存影像所需要的儲存空間比較小，但是 n 大時，它的編碼與解碼運算量相當大。我們利用運算的規律性來設計出一套演算法，以加速運算。該年第三個子題是快速編碼與解碼的動態權重分享方法。在公司的各種不同的應用環境中，常會希望每個分存的持有者權重會不相同；而且會希望依公司的發展，可以動態地調整其分存的權重大小。本子題設計出一套可以這樣快速編碼與解碼的動態權重的分享方法。

第二年計畫(高容量資訊隱藏方法之設計與資訊隱藏量上限之探討)的第一個子題是以機密影像之漢明長度(Hamming norm)為基礎的“無失真”資訊隱藏方法。相較於其它常見的無失真資訊隱藏法，我們所提方法可以藏入較高的資訊量，而仍然保有好的偽裝影像品質。該年第二個子題是基於機密影像中相鄰像素間相似性而得的高容量隱藏方法。人類的視覺系統相對於電腦的數位化數據而言是較為遲鈍的，我們利用此一現象設計出一個高容量隱藏方法，讓機密影像可以容忍有一點失真，但藏入的機密影像可以不必比掩護影像小。第三個子題是資訊隱藏量上限之探討，以量度每張掩護影像的隱藏容量上限。我們要求這個上限的計算簡單，而不是利用大量的模擬來估計出解答。該年第四個主題是基於多維像素空間而得的影像隱藏方法。我們將目前的影像隱藏方法以高維度像素空間的角度觀察，並分析出如何提高隱藏率，從而設計出高隱藏率的影像隱藏演算法。

第三年計畫(快速影像分享法與高容量資訊隱藏法在影像驗證與修復之應用)的第一個子題是區塊式的影像驗證與自我還原系統。我們利用第二年針對資訊隱藏的研究成果，搭配第一年多項式機密分享法的加速，發展出一個系統，能有效地偵測出受保護影像被惡意竄改的區域，並對這些遭竄改的區域進行修復。該年第二個子題為使用分享法做影像快速修復。在這子題中，我們將 XOR 型的分享法用在影像修復技術上。我們將影像分解成數個分存後，隱藏這些分存時，仍要求處理後的影像畫質依然保持某個水準以上。且影像對遭竄改的區域進行修復時，影像修復的速度非常快。

關鍵詞:機密分享；布林運算；分存影像放大率；快速傅立葉轉換；權重;資訊隱藏；隱藏容量；多維球體空間;影像驗證;影像自我還原;漸進式影像還原。

Abstract.

This was a 3-year project. Year 1 was for the fast sharing of an image. Year 2 was for the design of high-capacity hiding methods, including the study of the upper bound of each cover image's hiding capacity. Year 3 was for images' authentication and recovery, by applying the fast sharing methods and high-capacity hiding methods designed in Years 1 and 2.

Year 1 was for fast sharing of an image, and there were three subtopics 1a−1c, as introduced below. 1a): the design of a fast sharing method based on Boolean operations. The storage space was small, and the decoding time was very short. 1b): to accelerate the polynomial-based (t, n) threshold sharing method of an image. In general, polynomial-based image-sharing method was good in getting small-size shares; however, it was not fast if n was large. Therefore, we analyzed the repeated patterns appearing in the coding/decoding, and thus designed a new algorithm to accelerate the processing speed. 1c): fast sharing for a system with shares of dynamic weights. In many companies, people of different importance levels might have different weights when they vote for the disclosure of a shared secret image. The weights might also be dynamic to match the company's dynamic developing. We designed a fast coding/decoding method for such sharing system.

Year 2 was for the design of high-capacity hiding methods, and the study of the upper bound of each cover image's hiding capacity. There were four subtopics 2a−2d, as introduced below. 2a): a lossless high-capacity image-hiding method based on the Hamming norm of the secret image. 2b): a high-capacity image hiding method based on the similarity between neighboring pixels of the secret image. The secret image was not necessarily smaller than the cover image. The distortion of the recovered secret image was small. 2c): an upper bound of a cover image's hiding capacity. It was a natural barrier for all hiding methods. We required this upper bound be as low as possible. The bound could be evaluated without using too many operations. 2d): a high-capacity image hiding method based on a high-dimensional space for pixels. We designed a new method whose hiding-rate was very high.

Year 3 was for images' authentication and recovery, which was an application of the sharing methods and hiding methods designed in Years 1 and 2. The subtopics were 3a): a block-based image authentication method with self-recovery of tampering. The method utilized the accelerated-polynomial-based sharing of Year 1 and a hiding method of Year 2. The method detected which parts of the image were tampered, and then did automatic repairing. 3b): using fast sharing in image's fast-repairing. The given image was shared by a module-based sharing method so that each share was small and easy to be hidden. After our processing, image still looked natural. Later, if being tampered, the image could still be recovered fast.

Keywords: Secret sharing；Boolean operations；I/O ratio；Fast Fourier Transform; weighted sharing; data hiding；image authentication; image recovery; progressive recovery; module-based sharing。

報告內容

一、前言與研究目的

第一年的第一個主題是：使用布林運算的快速機密影像分享法。最常見的機密影像分享方法是多項式機密分享法(polynomial secret sharing)和視覺編碼法(visual cryptography)兩種。其中多項式機密分享法[1]的優點是分存影像所需要的儲存空間比較小，但是它的解碼運算量相當高；而視覺編碼法[2]的優點反而是它的解碼運算量非常低，但是分存影像所需要的儲存空間卻很大。在這個主題中，我們希望設計出一種使用布林運算內的 XOR 為基礎的可容錯機密影像分享法，使得產生的分存影像大小可以比原來機密影像還要小，而且在事後的重建過程中只需要數個 XOR 運算就可以重建機密影像的每一個像素值。另外，此機密影像分享法也擁有(t, n)分享方法的容錯能力，並且能運用在任何黑白、灰階和彩色影像上。

第一年的第二個主題是：多項式(t, n)分享方法的快速編碼與解碼。多項式分享法[1]的運算量相當高; 但我們在前國科會計畫的研究之中觀察到，有關多項式(t, n)分享方法[3]，其編碼與解碼計算有些許的規律。而這些計算上的規律，往往可以利用於進行編碼與解碼時的加速運算。在做多項式(t, n)分享的時候，主要都是利用矩陣運算的方式來計算解答，但是由於這是多項式的運算，因此其運算矩陣會存在一些規律(即每一列都是以$[1\ x\ x^2\ x^3\ \ldots\ x^{t-1}]$的形式顯示)。我們想要利用這些規律性，來設計一套加速運算的演算法。此方法可以快速地對分存影像做編碼與解碼的動作，尤其是在 t, n 高的時候。

第一年的第三個主題是：快速編碼與解碼的動態權重多項式分享方法。在各種不同的應用環境之中，我們或許會希望每個分存影像的權重會不相同。例如當資料在網路間流動的時候，路由器可依據每條路徑的頻寬而將資料用不同權重的分存影像傳輸出去，這樣只要接收端收到一定量的分存影像之後，便可以重建出原本的資料，由於我們強調演算法比須是快速的，所以各路徑亦會各自加速。因此，在這個主題中，我們希望在一個分存影像有不同權重的情況下，設計出一套快速編碼與解碼的資訊分享方法。此方法除了可以快速的建構出不同權重的分存影像外，當我們希望改變某些分存影像權重的時候，亦可快速的對分存影像做更新。

第二年的第一個主題是：以邊緣吻合向量量化為基礎的資訊隱藏方法。在資訊隱藏法中，藏入資訊量的多寡與偽裝影像的品質的好壞往往是一個取捨問題，也就是若藏入較高資訊量，則其偽裝影像的品質會較差;若藏入較低的資訊量，則其偽裝影像的品質會較佳。因此我們希望設計出一個以邊緣吻合向量量化為基礎的資訊隱藏方法，相較於其它的以邊緣吻合向量量化為基礎的資訊隱藏法，我

們可以藏入較高的資訊量，而仍然保有較佳的偽裝影像品質。

第二年的第二個主題是：基於機密影像中相鄰像素間相似性的高容量資訊隱藏方法。一般來說，影像的資訊量都很大，因此若要將超越掩護影像大小之機密影像藏入於該掩護影像，是有難度的。但由於人類的視覺系統相對於電腦的量化數據而言較為遲鈍，亦即人眼是無法分辨影像本身的細微變化。因此我們利用此一現象配合影像鄰近周圍的像素具有極高的相似性，讓藏入至掩護影像的機密影像可以容忍有一點失真，但藏入的機密影像的大小可以不必比掩護影像小。

第二年計畫的第三個主題是資訊隱藏量之上限研究。在許多的應用上，如何去評估一張影像的資訊隱藏量是重要的課題。因為我們可以在做隱藏之前便可以大略評估一下到底機密資訊是否可以隱藏進去，這樣便可避免因機密資訊的大小太大而無法隱藏進偽裝影像裡面，進而省去許多無謂的時間。一般而言，一個好的影像隱藏方法可以在差不多的影像品質之下，達到較高的資訊隱藏量；但是，我們知道不管是如何優秀的資訊隱藏法，總會有一個理論上的極限(例如，一張 256×256 大小的 8 位元灰階影像不能放進 512×512 Byte 大小且不壓縮的機密資訊)。有些人可能在評估一張偽裝影像的隱藏容量大小時，指定一個特定的影像隱藏方法(例如，指定 LSB 隱藏法)，但是這種資訊隱藏量的評估方法會受到所使用的影像隱藏方法影響，所估計出來的數字並無法代表該影像真正的資訊隱藏量的極限。而本題目便是希望可以研究出一套測量的方法以量度每張影像的容量上限。這個上限值所表示的是一個天然障礙。我們也希望這個計算方法可以簡單的計算出來（而不是利用大量的模擬來估計出解答）。

第二年計畫的第四個主題是基於多維像素空間而得的影像隱藏方法。過去的研究觀察到，當我們想要做影像隱藏時，向量空間的效果總是會比純量空間的效果好上一些。因此本題目主要便是將目前的影像隱藏方法以高維度像素空間的角度觀察，並分析設計出更高隱藏率的影像隱藏演算法。

第三年的第一個主題是區塊式的影像驗證與自我還原系統。我們藉由前兩年研究成果，預計發展出一個能有效地偵測出受保護影像被惡意竄改的區域，並對這些遭竄改的區域進行修復以還原原始影像的視覺含意。

第三年的另一個主題是使用分享法做影像快速修復。在這子題中，我們將 XOR型的分享法用在影像修復技術上。我們將影像分解成數個分存後，隱藏這些分存時，仍要求處理後的影像畫質依然保持某個水準以上。且影像對遭竄改的區域進行修復時，影像修復的速度非常快。

二、文獻探討

在第一年中，我們研究的是機密是分享(sharing)。Shamir[4]和 Blakley[5]在 1979 年各提出一套機密分享的方法。Shamir 提出利用多項式運算的方法，而 Blakley 提出利用空間平面交錯的方式來達成機密分享。關於機密分享與影像處理的相關發展，C.C. Chang 在 1998 年提出混合向量編碼(Vector Quantization)和機密分享技術的機密影像分享方法[6]。2002 年，本實驗室[7]將 Shamir 的方法做了一些改變，並套用至影像之中，使得在(t, n)機密分享之下，每份機密分存的

大小降至只有原始機密影像的 1/t。視覺密碼學(Visual Cryptography)亦是機密分享領域的一個分支。Naor 與 Shamir[8]在 1994 年提出一套利用人眼解碼的機密分享技術。此技術可以利用投影片疊合的方式來達成解密效果，但是如果將疊合的投影片分開來，卻只能看到一片沒意義的雜點。由於一般的投影片分存的大小會遠遠超過原始的機密影像，因此，C.N. Yang 在[9]利用機率的方式將每張投影片分存縮小到和一般的機密影像大小相同。關於使用布林運算的快速機密影像分享法方面，[10]是典型的例子，他們應用 XOR 運算讓(n, n)-threshold 無失真機密影像分享法的分存影像不需要很大的儲存空間，而且解碼運算量也相對減少非常多。[11]則主要利用 bit-level 的機密分享來達成加解密的效果。

在第二年中，我們研究的是資訊隱藏方法。資訊隱藏主要可分為無失真與有失真兩大類。無失真資訊隱藏法，主要是強調機密影像可以完全無失真藏入，且偽裝影像的品質不能太差。這方面的期刊論文不少，例如[12]的S.J.Wang 藉由 modulus function 來將機密影像藏入。而[13]的C.C. Chang et al.利用run-length 概念，將二進位影像或一般影像藏入掩護影像中。而在有失真資訊隱藏法，機密影像可以容忍有一點失真，但人類的視覺系統確是無法分辨此細微變化，在這方面的期刊論文，例如[14]的Y.C. Hu利用VQ的特性，將機密影像先做壓縮，再將VQ indices 藏入掩護影像，以藏入較高容量，而[15]的R.Z. Wang and Y.D. Tsai 亦利用VQ與k-means 概念，來達到影像隱藏技術。因此相關方面的研究非常熱門。

在第三年中，我們研究的是影像修復，Fridrich等人在[16]提出利用DCT 轉換抽出重要資訊，並將重要資訊隱藏至空間域的方式，來達到影像可以自我修復的功能。P.L. Lin等人在[17]提出利用階層式的偵測架構來偵測影像被破壞的區域並還原。其他相關研究還有Wu等人的[18]; Li等人的[19]; Wan等人的[20]。關於使用快速分享法的影像修復技術方面，Chung等人在[21]提出一個使用餘數法而達到高容量的影像隱藏技術，而Hu等人在[22]是使用多項式影像分享法去達到將機密影像隱藏進非機密影像內的重要技術。若能整合這些技術便能達到使用快速分享法的影像修復技術。

三、研究方法

第一年的第一主題：我們使用布林運算產生快速的機密影像分享法，首先使用基本的(2, 2)-threshold 的 XOR 機密影像分享法[10]產生兩張亂碼圖，再將這兩張亂碼圖進行分割，切成所需要的大小與數量。然後，將以上切割好的亂碼圖小碎塊使用 XOR 運算重新組合成 n 張一樣大小的亂碼圖。最後，這 n 張亂碼圖立即成為擁有多項式(t, n)分享方法的容錯能力的分存影像。如圖一，本實驗所設定的門檻值是(t=4, n=4)，(a)為本實驗用的 768×512 彩色機密影像，(b)-(e)為產生的四張分存影像，每張分存影像大小為 768×256，(f)為利用前面產生的所有四張分存影像所還原的無失真機密影像。從實驗結果可看出，本布林運算法所產生的分存影像有可能以比原來機密影像還要小。我們亦做了其他實驗，結果顯示我們的

方法亦具有 (t, n)分享的容錯能力。另外，表一比較本方法和[2, 3]重建機密影像中的一個像素值所需的時間複雜度，採用本方法重建一個機密像素值只需要花費三個 XOR 運算，因此 比[2, 3]快。

第一年的第二主題『多項式(*t, n*)分享方法的快速編碼與解碼』: 我們使用在 GF(2^{k+1})上的快速傅立葉轉換(FFT)來達成加速的目的，以下將分成編碼和解碼來分開討論。

(*t, n*)分享編碼:

我們使用快速傅立葉轉換的蝴蝶圖來加速運算。圖二顯示一個大小為 8 的蝴蝶圖，其中 d_i 是輸入值，而 $F(w_j)$是輸出值。首先，從機密影像拿出 *t* 個未處理的像素，然後將這 *t* 個像素當成蝴蝶圖的 d_i 輸入值。經過 $\Theta(t\log^2 t)$的蝴蝶圖運算後，便可以取出 *t* 個分存影像數值$\{F(w_8^i) \mid i = 0,1,...,t-1\}$。如果分存影像不夠的話，則可以利用如下的運算(先令 j=1):

$$\left\{d_0 w_N^{0\times j}, d_1 w_N^{1\times j}, ..., d_{t-1} w_N^{(t-1)\times j}\right\}$$

以獲得新的 d_i, 然後將這些新數值重新輸入蝴蝶圖中獲得新的 *t* 個分存影像數值:

$$\left\{F(w_N^{0+j}), F(w_N^{N/t+j}), ..., F(w_N^{N/t(t-1)+j})\right\}$$

如果分存影像還不夠，則令 j=j+1 然後回到前面的步驟以繼續產生運算新的分存影像。依照以上的步驟，我們可以在 $\Theta(n\log t)$時間內獲得 *n* 個分存影像數值。依照如上的步驟，直到機密影像的像素全部處理完畢，然後 *n* 張分存影像便可以產生出來。

(*t, n*)分享解碼:

[23]介紹了一種 $\Theta(t\log^2 t)$複雜度的快速計算的 Lagrange polynomial 方法。我們將這個方法運用在 GF(2^{k+1})上，然後利用它來做分享解碼。最後獲得了可以在 $\Theta(t\log^2 t)$時間內解碼的快速演算法。表二顯示利用本方法對於 512×512 Lena 的機密影像的分享所需編碼時間;表三顯示利用一般多項式計算對於該 512×512 機密影像的分享所需編碼時間。比較表二，我們發現當 t 越大，我們所提出的快速(*t, n*)分享運算編碼的減少時間越明顯。表三比較本方法和傳統方法(反矩陣)對於該 512×512 的機密影像的分享所需解碼時間，從觀察中可知，當 *t* 越大時，採用本方法運算解碼所減少的時間也越明顯。

第一年的第三主題『快速編碼與解碼的動態權重多項式分享方法』: 首先將 512×512 Lena 機密影像(圖三(a))做加密，然後將得到的加密影像(圖三(b))利用我們所提出的動態權重(t=256, n=7)多項式分享方法，依權重 160; 64; 24; 8; 134; 12; 3 分別產生 n=7 個分存影像，結果分別如圖三(c-i)所示。之後，若收集到的分存影像其總權重超過 t=256 時，便可無失真還原回 512×512 機密影像 Lena。圖三(j)為利用四個分存影像(圖三(c-f)，因為 160+ 64+ 24+ 8=256≥*t*)所還原的無失真機密影像。表四比較我們的快速動態權重多項式分享方法與直接合併傳統多項式分享

方法[7]的 w_1 張分存以產生 1 個權重為 w_1 的加權分存影像所需之時間。對於 512×512 Lena 機密影像分享運算的編碼時間，從表四可知，當權重 w_1 大於 1 時，採用本方法所需的編碼時間皆優於直接使用傳統多項式(t, n)分享方法[3]所需的編碼時間。

第二年的第一主題『邊緣吻合向量量化為基礎的資訊隱藏方法』:首先將一張掩護影像切割成多個不重疊的 4×4=16 像素的區塊。該張掩護影像的第一列或第一行的區塊不用來藏任何機密資訊，故這些區塊經由向量量化壓縮後再即刻解壓縮，而這些解壓縮的區塊資訊便成為偽裝影像相對位置的區塊內容。剩下的每個區塊 (即不是掩護影像的第一列或第一行的區塊)，則利用其相鄰區塊的解碼資訊來產生一本子編碼簿，再從此編碼簿找出一個離此區塊距離最近的 16 維碼向量 X，與離 X 最近的 16 維碼向量 Y，然後根據 X 與 Y，定義一個以 X 為球心，半徑為 $\lceil \|X-Y\|/2 \rceil - 1$ 的球體。為了可以將資料藏到 16 維碼向量 X 的每一個分量中，必需算出每一個分量的隱藏量。一般來說，若要將 v $(1 \le v \le 4)$ 個位元的機密資訊，利用 v-LSB 替換法藏入到 16 維碼向量 $X = (x_0, x_1, \ldots, x_{15})$，得到偽裝碼向量 $Z = (z_0, z_1, \ldots, z_{15})$，則 z_i 與 x_i $(0 \le i \le 15)$ 的差值最多為 $2^v - 1$，因此 $\sum_{i=0}^{15}(z_i - x_i)^2 \le 16(2^v-1)^2$。另一方面，我們要求 X 與 Z 的距離不能超過球體半徑，因此 $\sum_{i=0}^{15}(z_i - x_i)^2 \le (\lceil \|X-Y\|/2 \rceil - 1)^2$。只要 v 滿足 $16(2^v-1)^2 \le (\lceil \|X-Y\|/2 \rceil - 1)^2$ 就可。因此，$v = \lfloor \log_2[(\lceil \|X-Y\|/2 \rceil - 1)/4 + 1] \rfloor$。在算出 v 值之後，16 維碼向量 X 的某幾個(假設有 w 個)分量有可能可以再多藏一個位元的機密資訊。此時，為了仍然可以滿足 X 與 Z 的距離不能超過球體的半徑的條件，則

$$w[(2^{v+1}-1)^2 - (2^v-1)^2] \le (\lceil \|X-Y\|/2 \rceil - 1)^2 - 16(2^v-1)^2 \text{。}$$

因此，$w = \left\lfloor \dfrac{t^2 - 16(2^v-1)^2}{(2^{v+1}-1)^2 - (2^v-1)^2} \right\rfloor$。故 16 維碼向量 X 的每一個分量的隱藏量為

$C(x_0) = C(x_1) = \ldots = C(x_{w-1}) = v+1$; $C(x_w) = C(x_{w+1}) = \ldots = C(x_{16}) = v$;最後，分別取出機密資訊的 x_i 位元，再利用 x_i 位元 LSB 替換法，將 x_i 位元藏入到分量 x_i，便會得到偽裝碼向量 Z。如圖四，(a)為 512×512 的邊緣吻合向量量化影像(未藏入任何資訊)，(b)為利用本主題方法所產生的 512×512 偽裝影像，(c)為將圖(a)的鼻子與嘴巴放大的影像， (d)為將圖(b)的鼻子與嘴巴放大的影像。因此，本方法與邊緣吻合向量量化影像比較，具有較佳的影像品質。另外，表五比較本方法與隱藏法[24]之隱藏量與偽裝影像品質(方法[24] 亦使用邊緣吻合向量量化)。由表五得知，本方法的隱藏量與偽裝影像品質皆優於[24]。

第二年的第二主題『基於機密影像中區塊間相似性的高容量資訊隱藏方法』:首先將機密影像利用向量量化技術壓縮，再利用 Thien and Lin's 的方法[26]，將壓縮檔藏入到掩護影像的像素值。機密影像的大小可以不必比掩護影像小。表六比較本向量量化隱藏法與其它用向量量化的隱藏法[21]、[25]的影像品質。由表六得知，採用本方法所得的偽裝影像品質優於[21]、[25]，而且，經由偽裝影像擷取之機密影像的品質與[21]、[25]的差距不大。

第二年的第三主題『資訊隱藏量之上限研究』:我們利用多維球體的公式來計算出 PSNR 上限值。首先，對於一張 $w\times h$ 的影像 H，其 PSNR 公式為 $PSNR=10\log\frac{255^2}{MSE}$，其中 $MSE=\frac{1}{wh}\sum_{i=0}^{w-1}\sum_{j=0}^{h-1}(H(i,j)-H'(i,j))^2$。由公式可知，PSNR 最大化即是 MSE 最小化，而 MSE 代表的是多維空間下的歐氏距離。假設

1. 掩護影像 H 是均勻分布。
2. 機密資料是均勻分布。
3. 掩護影像與機密資料是互相獨立。

由以上三個假設，我們可以畫出如圖六的模型。其中圓心代表在多維空間中一個表示影像 H 的點，而 x 點代表影像 H 藏入一種機密資料後可能的位置(即為偽裝影像)。因為一個 x 點代表一種機密資料，所以 x 點的數量代表隱藏量，x 點越多，代表隱藏量越大。假設我們要隱藏 s 位元至影像 H 之中，則 x 點的個數為 2^s。另一方面，為了最小化 MSE，這些 x 點將會以影像 H 為圓心分布在一個半徑為 R 的多維球體內，而球體積可計算出。代入多維球體的公式後，我們可計算出 $R=\left[\frac{(wh/2)!2^s}{\pi^{wh/2}}\right]^{1/wh}$。將 R 代回 MSE 公式後，可得 $MSE_{worst}=(\frac{wh}{2\pi})^{-0.5}\left[(wh/2)!2^s\right]^{1/wh}$。

此為 MSE 最佳解的下界。另一方面，我們可以用積分法求 MSE 的期望值為 $MSE_{avg}=((wh+2)\pi)^{-0.5}\left[(wh/2)!2^s\right]^{1/wh}$。此代表 MSE 最佳解的期望值。

第二年的第四主題『基於多維像素空間而得的影像隱藏方法』:我們先將掩護影像 H 切成每個大小為 n 像素($p_0, p_1, \ldots, p_{n-1}$)的區塊，且每個區塊藏入一 m 位元的機密資料 B_m。我們使用的公式為

$$f(p'_0, p'_1, \ldots, p'_{n-1})$$
$$=1p'_0+c_1p'_1+\ldots+c_{n-1}p'_{n-1}=B_m \pmod{2^m}$$

其中$(1, 2, \ldots, c_{n-1})$是 n 個給予的正整數，$p'_i=p_i+\Delta p_i$ 代表隱藏資料後獲得的掩護像素，而 Δp_i 代表其差值。將上式轉換後，我們可以獲得以下結果

$$1\Delta p_0+c_1\Delta p_1+\ldots+c_{n-1}\Delta p_{n-1}$$
$$=B_m-(1p_0+c_1p_1+\ldots+c_{n-1}p_{n-1})\pmod{2^m}$$

其中公式的右半邊是可以計算出來的，令其結果等於 R_m，而公式的左半邊是必

須解決的問題。對於不同的 R_m 值，我們可以利用動態規劃演算法去求解 $(\Delta p_0, \Delta p_1, ..., \Delta p_{n-1})$，並將其記錄於表格中以利隱藏時的速度。當資料全部隱藏完後，解碼端只需要計算 $f(p'_0, p'_1, ..., p'_{n-1})$ 便可解出機密資料 B_m。然而，如何獲得好的$(1, 2, \ldots, c_{n-1})$是另一個問題，我們提供了表七，使用者可以依照不同的隱藏率選擇不同的$(1, 2, \ldots, c_{n-1})$。表七亦提供預測的 PSNR，也就是說，使用者可以在不進行隱藏過程之前便可以預知做完後大致上的 PSNR 數值。表八則列出本方法與其他隱藏方法[26]的偽裝影像品質比較。由表八可看出，在不同的隱藏率下，本方法都可獲得較其他隱藏方法[26]為佳的 PSNR 值。

第三年的第一主題:『區塊式的影像驗證與自我還原系統』。我們將 DCT 資訊藉由分享機制嵌入原始宿主影像，產生一個具備影像驗證與修復的架構。方法拆成兩個主要部份。1).產生一組浮水印：藉由將數個分存$\{E_i\}$產生出一個可供還原的浮水印，並將$\{E_i\}$藏在 DCT 區塊裡。2).偵測與修復：一旦查覺到區塊遭受竄改，藉由兩階層的分享解碼[35]，用嵌入的浮水印來修復竄改後的影像。在不失一般性之下，假設我們所用的影像大小為 512×512 影像，並將影像拆成 4096 個 8×8 不重疊區塊。在產生浮水印階段，我們依序做下面四個步驟:

1. 產生區塊資料集合$\{P_i | i = 1,2,...,4096\}$。
2. 區塊集合利用多項式分享法(Galois fields)[3]產生 4096 個分存$\{E_i | i = 1,2,...,4096\}$。
3. 為了增加安全性，對於每個區塊 i，產生一組 12-bits 的雜湊編碼；對於每個 E_i，和對應的 12-bits 做 Exclusive-OR 運算，並得到加密後的密文。
4. 將(加密後的) E_i 嵌入，且將 DCT 係數轉回空間域取得浮水印。

在偵測與修復階段，主要技術是使用兩階層的分享解碼[35]，先取出影像中各區塊的 E'_i，將這些解碼過後的分存 E'_i 產生雜湊碼，做 12-位元的 Exclusive-OR 運算。除此之外，我們使用(t, n)分享公式

$$(t, n) = (4096(2\alpha - 1), 4096)$$

來判斷整體區塊是否有受到竄改。當竄改區塊的比率高於 $1-\alpha$，我們即認定此影像受到竄改。其中α值經過我們推導，適合的區間為$1 > \alpha \geq 6/(c+12)$，其中 c 是 P_i 的大小。在安全性方面，我們做了三種攻擊測試，分別為複製-貼上攻擊[36]，拼貼(collage)攻擊[37]和向量量化(VQ)攻擊[38]，這三種攻擊測試結果分別列在圖七至圖九。實驗結果證明我們的方法能有效偵查上述三種攻擊，並具備一定程度的影像還原能力。圖十(e)-(f)畫出復原後的比較: 我們復原後的 31.89 dB 影像不會有怪東西在雪地出現, 別人復原後的 29.3 dB 影像卻會有怪東西在雪地出現(其浮水印影像的 dB 也比我們的 32.29 dB 稍差)。

在這子題中，我們將 XOR 型的分享法用在影像修復技術上(圖十一、圖十二)。我們將影像分解成數個分存後，隱藏這些分存時，仍要求處理後的影像畫質依然保持某個水準以上。且影像對遭竄改的區域進行修復時，影像修復的速度非常快。

第三年的另一主題『使用快速分享法的影像修復技術。為了達到此目標，我們不用上述所使用的 Galois fields 多項式分享法，而改用第一年的研究成果:XOR 型的快速分享法。圖十一畫出影像編碼過程與影像修復解碼過程。利用某些相關於影像區塊的性質產生驗證資料，並嵌入影像區塊中，它能用來檢測影像的完整性。同時，為了使影像本身除了能偵測是否遭到惡意的竄改之外，還具有修復被破壞區域的能力。我們產生關於影像的修復資料(index file)，並搭配(*t, n*)門檻 XOR 型分享方法平均分散地藏於影像本身中，使其具備容錯的特質來達成修復的能力。圖十二的(1a)-(1d)是四張經過影像驗證處理後的加工影像，其影像品質令人滿意；(2a)-(2d)是對圖進行惡意的竄改；(3a)-(3d)是進行修復的結果，可以看出使用快速分享法的影像修復後，修復的影像畫質仍舊良好。

四、結果與討論

四-1. 在第一年計畫(快速影像分享)的第一個子題，我們使用 Boolean 運算研究出一個新的機密影像分享法，不但分存影像所需要的儲存空間很小(如圖一)，而且解碼運算量也非常少(如表一之比較)，重建一個像素值只需要花費三個 XOR 運算，因此比[2, 3] 快。我們也使用 Mod 運算設計出一套漸進式演算法，而另得到一套新的漸進式影像分享法，發表在 2009 JEI, Vol. 18(3)。我們該年第二個子題是多項式(t, n)分享方法的快速編碼與解碼。多項式機密分享法的優點是分存影像所需要的儲存空間比較小，但是 n 大時，它的編碼與解碼運算量相當大。我們利用運算的規律性來設計出一套加速運算的演算法。表二顯示:當 t 越大，我們所提出的快速(t, n)分享編碼的加速越明顯。表三顯示解碼時間。多項式機密分享法[3]中使用反矩陣和矩陣乘法來解碼，複雜度為Θ(t)，我們提出的快速解碼方法的複雜度則為Θ(log2t)。在該年第三個子題，我們設計出一套快速編碼的動態權重分享方法(圖三與表四)。從表四可知，當權重 w1 大於 1 時，採用本方法所需的編碼時間，皆優於直接合併傳統多項式分享方法[3]的 w1 張分存以產生一個權重為 w1 的分存影像所需之時間。在一般公司的各種不同的應用環境中，每個員工持有的分存的權重，可以依員工的地位不同而不相同；而且依公司的發展，公司常會希望動態地調整其員工分存的權重大小。我們設計出的快速編碼的動態權重分享法，可以應用到這樣的公司環境，也可以應用到存有機密影像(例如藍圖)又常要打開影像以供開會討論的公司。

在第一年計畫(快速影像分享)，我們已發表 3 篇 journal papers:

1. K.Y. Chao and J.C. Lin. “Secret Image Sharing: a Boolean-operations based Approach Combining Benefits of Polynomial-based and Fast Approaches,” International Journal of Pattern Recognition and Artificial Intelligence Vol. 23, No. 2, 2009, pp. 263-285

2. S. J. Lin, L.S.T. Chen, and J.C. Lin. “Fast weighted secret image sharing," Optical Engineering, Vol. 48, No. 7, 2009, 077008.

3. K.Y. Chao and J.C. Lin. "User-friendly sharing of images: a progressive approach based on modulus operations" Journal of Electronic Imaging, Vol. 18, No.3, 2009, 033008.

四-2. 第二年計畫(高容量資訊隱藏方法之設計與資訊隱藏量上限之探討)的第一個子題是『以機密影像之漢明長度(Hamming norm)為基礎的“無失真”資訊隱藏方法』。相較於其它的無失真資訊隱藏法，我們所提方法可以藏入較高的資訊量，而仍然保有好的偽裝影像品質。如圖四，(a)為邊緣吻合向量量化影像(未藏入任何資訊)，(b)為利用本主題方法所產生的偽裝影像，(c)(d)分別為圖(a)(b)的放大。(c)(d)顯示本方法與邊緣吻合向量量化影像比較，具有較佳的影像品質。另外，表五比較本方法與隱藏法[24]之隱藏量與偽裝影像品質(方法[24] 亦使用邊緣吻合向量量化)。由表五得知，本方法的隱藏量與偽裝影像品質皆優於[24]。該年第二個子題是『基於機密影像中區塊間相似性的高容量資訊隱藏方法』。人類的視覺系統相對於電腦的數位化數據而言是較為遲鈍的，我們利用此一現象，設計出一個高容量隱藏方法，讓機密影像可以容忍有一點失真，但藏入的機密影像不必比掩護影像小。我們將機密影像利用向量量化技術壓縮，再利用方法[26]，將壓縮檔藏入到掩護影像的像素值。表六比較本向量量化隱藏法與其它用向量量化的隱藏法[21]、[25]的影像品質。由表六得知，採用本方法所得的偽裝影像品質優於[21]、[25]，而且，經由偽裝影像擷取之機密影像的品質與[21]、[25]的差不多。該年第三個子題是『資訊隱藏量上限之探討』，以量度每張掩護影像的隱藏容量上限。這個上限值表示一個天然障礙，亦即不存在可以突破此上限的資訊隱藏法。我們要求這個上限的計算簡單，而不是利用大量的模擬來估計出解答。針對此，我們推理出 MSE 最小解的下界(因為 PSNR 最大化即是 MSE 最小化)。另一方面，我們也用積分法求 MSE 的期望值，此代表最佳隱藏的 MSE 期望值。該年第四個主題是『基於多維像素空間而得的影像隱藏方法』。我們將目前的影像隱藏方法以高維度像素空間的角度觀察，並分析出如何提高隱藏率，從而設計出高隱藏率的影像隱藏演算法。我們提供了表七，使用者可以依照不同的隱藏率選擇不同的係數使用者可以依照不同的隱藏率選擇不同的係數($c_1, c_2, \ldots, c_{n-1}$)。表七亦提供預測的 PSNR，也就是說，使用者可以在不進行隱藏過程之前便可以預知做完後大致上的 PSNR 數值。表八則列出本方法與其他隱藏方法[26]的偽裝影像品質比較。由表八可看出，在不同的隱藏率下，本方法都可獲得較其他隱藏方法[26]為佳的 PSNR 值。

在第二年計畫(高容量資訊隱藏)，我們發表 3 篇 journal papers:

4. L.S.T. Chen, S. J. Lin and J.C. Lin. "Reversible JPEG-based hiding method with high hiding-ratio", International Journal of Pattern Recognition and Artificial Intelligence, Vol. 24, No. 3, 2010, pp. 433-456.

5. L. S. T. Chen and J. C Lin. "Steganography scheme based on side match vector quantization" Optical Engineering Vol. 49, No.3, 2010, 037008.

6. L.S.T. Chen, W.K Su, and J.C. Lin. “Secret Image Sharing based on Vector Quantization”, International Journal of Circuits, Systems and Signal Processing, Vol. 3, No. 3, 2009, pp 137-144.

四-3. 第三年計畫(分享法與高容量資訊隱藏法在影像驗證與修復之應用)的第一個子題是『區塊式的影像驗證與自我還原系統』。我們利用第一年多項式機密分享法的加速，搭配 Lattice Embedding 進行資訊隱藏，發展出一個系統，能有效地偵測出受保護影像被惡意竄改的區域,並對這些遭竄改的區域進行修復(圖七、圖八、圖九、圖十)。由圖十(e-f)亦可看出我們復原後的品質比別人復原後的好。此系統可以應用到網頁維護。該年第二個子題為『使用快速分享法做影像快速修復』。在這子題中，我們將 XOR 型的分享法用在影像修復技術上(圖十一、圖十二)。我們將影像分解成數個分存後，隱藏這些分存時，處理後的影像畫質依然保持某個水準以上。且影像對遭竄改的區域進行修復時，影像的修復速度快。

在第三年計畫(分享法與高容量資訊隱藏法在影像驗證與修復之應用)，我們已發表 3 篇 journal papers (另外的在投稿或 revise 中):

7. S. J. Lin and J. C. Lin. "Authentication and Recovery of an Image by sharing and lattice-embedding", Journal of Electronic Imaging, Vol. 19, No. 4, 2010.

8. L.S.T. Chen and J.C. Lin. “Multi-threshold progressive image sharing with compact shadows.” Journal of Electronic Imaging, Vol. 19, No. 1, 2010, 013003.

9. L.S.T. Chen, W.K Su, and J.C. Lin. “Secret Image Recovery based on Search Order Coding”, International Journal of Computers, Vol. 3, No. 3, 2010, pp. 321-328.

五、成果發表

在本三年計畫，我們已發表9篇國際期刊論文，即上面列出的9篇。本計劃每年之申請經費約為33萬(核定為45萬，因加列主持人費用)。每年之成果發表3篇國際期刊論文。這樣的經費成果比，應該還算可以。

參考文獻

[1]. R. Z. Wang and C. H. Su, “Secret image sharing with smaller shadow images,” *Pattern Recognition Letters*, Vol. 27, pp. 551-555, 2006.

[2]. R. Lukac and K. N. Plataniotis, “Bit-level based secret sharing for image encryption”, *Pattern Recognition*, Vol. 38, pp. 767-772, 2005.

[3]. C. C. Thien and J. C. Lin, “Secret image sharing,” *Computer and Graphic*, Vol. 26, pp. 765-770, 2002.

[4]. Shamir, “How to share a secret,” Communications of the ACM, Vol. 22 (4), pp.612−613, 1979.

[5]. G.R. Blakey, “Safeguarding cryptography keys,” *Proceedings of AFIPS National Computing Conference*, pp. 313-317, 1979.

[6]. C.C. Chang and R.J. Huang, “Sharing secret images using shadow codebooks,” *Information Sciences*, Vol. 111, pp. 335−345, 1998.

[7]. R.Z. Wang, C.F. Lin and J.C. Lin. “Image hiding by optimal LSB substitution and genetic algorithm,” Pattern Recognition, Vol. 34, No. 3, pp.671-683. 2001.

[8]. Moni Naor and Adi Shamir, “Visual Cryptography,” *EUROCRYPT*, pp.1–12, 1994.

[9]. C.N. Yang, “New visual secret sharing schemes using probabilistic method,” *Pattern Recognition Letters*, Vol. 25, pp.481-494, 2004.

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

[11]. R. Lukac, K.N. Plataniotis, “Bit-level based secret sharing for image encryption,” *Pattern Recognition*, Vol. 38, pp.767-772, 2005.

[12]. S.J. Wang, “Steganography of capacity required using modulo operator for embedding secret image,” *Applied Mathematics and Computation*, Vol. 164, pp.99-116, 2005.

[13]. C.C. Chang, C.Y. Lin and Y.Z. Wang, “New image steganographic methods using,” *Information Sciences*, Vol. 176, pp.3393-3408, 2006.

[14]. Y.C. Hu, “High-capacity image hiding scheme based on vector quantization,”

Pattern Recognition, Vol. 39(9), pp.1715-1724, 2006.

[15]. R.Z. Wang and Y.D. Tsai, "An image-hiding method with high hiding capacity based on best-block matching and k-means clustering," *Pattern Recognition*, Vol. 40(2), pp.398-409, 2007.

[16]. Fridrich, J. and Goljan, M, "Images with Self-Correcting Capabilities," *ICIP'99*, Kobe, Japan, pp.25-28, 1999.

[17]. P.L. Lin, C.K. Hsieh, and P.W. Huang, "Hierarchical Digital Watermarking Method for Image Tamper Detection and Recovery," *Pattern Recognition*, Vol. 38(12), pp.2519-2529, 2005.

[18]. H.C. Wu and C.C. Chang, "Detection and Restoration of Tampered JPEG Compressed Images," *Journal of Systems and Software*, Vol. 64, pp.151-161, 2002.

[19]. K.F. Li, T.S. Chen, and S.C. Wu, "Image Tamper Detection and Recovery System based on Discrete Wavelet Transformation," Conf. on Communications, Computers and Signal processing, Vol. 1, pp.26-28, 2001.

[20]. J. Wan and L. Ji, "A Region and Data Hiding Based Error Concealment Scheme for Images," *IEEE Transactions on Consumer Electronics*, Vol. 47, No. 2, 2001.

[21]. K.L. Chung, C.H. Shen, and L.C. Chang, "A novel SVD- and VQ-based image hiding scheme," *Pattern Recognition Letters*, Vol.22, pp.1051-1058, 2001.

[22]. Y.C. Hu and M.H. Lin, "Secure image hiding scheme based upon vector quantization", *International Journal of Pattern Recognition and Artificial Intelligence*, Vol.18(6), pp.1111-1130, 2004.

[23]. D. Bini and V.Y. Pan, "Polynomial and Matrix Computations," *Fundamental Algorithms*, Vol.1, Birkhauser, Boston, 1994.

[24]. C. C. Chang, W. L. Tai, and C. C. Lin, "A reversible data hiding scheme based on side match vector quantization," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 16, No. 10, pp.1301-1308, 2006.

[25]. Y. C. Hu and M. H. Lin, "Secure image hiding scheme based upon vector quantization," *International Journal of Pattern Recognition and Artificial Intelligence*, Vol. 18, No. 6, pp.1111-1130, 2004.

[26].C. C. Thien and J. C. Lin, “A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function,” *Pattern Recognition*, Vol. 36, No. 12, pp.2875-2881, 2003.

[27].I. C. Lin, Y. B. Lin, C. M. Wang, Hiding data in spatial domain images with distortion tolerance, *Computer Standards & Interfaces*, Vol. 31, No. 2, pp.458-64, 2009.

[28].J. Mielikainen, “LSB Matching Revisited,” *IEEE Signal Processing Letters*, Vol. 13, No. 5, pp.285-287, 2006.

[29].X. Li, B. Yang, D. Cheng, T. Zeng, “A generalization of LSB matching,” *IEEE Signal Processing Letters*, Vol. 16, No. 2, pp.69-72, 2009.

[30].X. Zhang, S. Wang, “Efficient Steganographic Embedding by Exploiting Modification Direction,” *IEEE Communications Letters*, Vol. 10, No. 11, pp.781-783, 2006.

[31].D. C. Wu and W. H. Tsai, “A steganographic method for images by pixel-value differencing,” *Pattern Recognition Letter*, Vol. 24, No. 9-10, pp.1613-1626, 2003.

[32].C. M. Wang, N. I. Wu, C. S. Tsai, M.S. Hwang, “A high quality steganographic method with pixel-value differencing and modulus function,” *Journal of Systems and Software*, Vol. 81 No. 1, pp.150-158, 2008.

[33].C. H. Yang, C.Y . Weng, S. J. Wang, H. M. Sun, “Adaptive data hiding in edge areas of images with spatial LSB domain systems,” *IEEE Transactions on Information Forensics and Security*, Vol. 3, No. 3, pp.488-497, 2008.

[34].H. Yang, X. Sun, G. Sun, “High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution,” *Radio-engineering*, Vol. 18, No. 4, pp.509-516, 2009.

[35].Y. J. Chang, S. J. Lin, and J. C. Lin, “Authentication and cross-recovery for multiple images,” *Journal of Electronic Imaging*, Vol. 17(4), 2008.

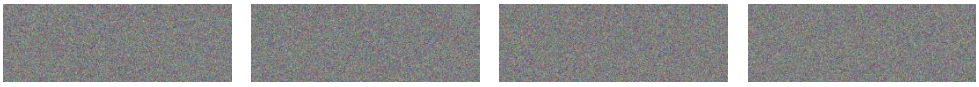
[36].P. S. L. M. Barreto, H. Y. Kim, and V. Rijmen, " Toward secure public-key blockwise fragile authentication watermarking," *IEE Proc. Vision, Image and Signal Processing*, Vol.149(2), pp.57-62, 2002.

[37].J. Fridrich, M. Goljan, and N. Memon, "Further attacks on Yeung-Mintzer fragile watermarking scheme," *Proc. SPIE conference on Security and Watermarking of Multimedia Contents II*, 3971, pp.428-437, 2000.

[38]. M. Holliman, and N. Memon, “Counterfeiting attacks on oblivious block-wise independent invisible watemarkhg schemes,” *IEEE Trans. on Image Proc*., Vol. 9(3), pp.432-441, 2000.

圖表

(a)



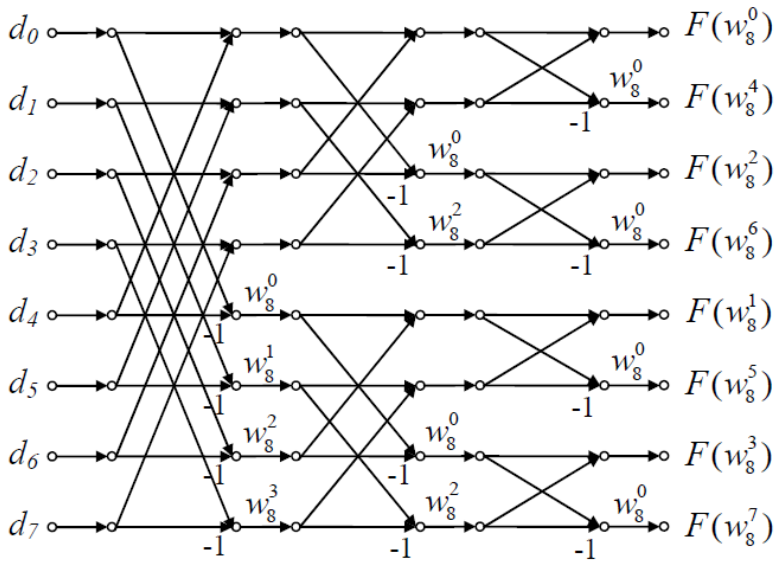
(b) (c) (d) (e)

(f)

圖一、第一年第一主題(使用布林運算的快速機密影像分享法)的實驗結果。在這個實驗中，使用的門檻值(threshold)為(t=4, n=4)。(a)為輸入的 768×512 機密影像，(b-e)為產生的 n=4 張分存影像，每張大小為 768×256，(f)為使用全部四張分存影像所重建的無失真機密影像。

表 1、第一年第一主題:重建機密影像中一個像素值所需的解碼運算複雜度比較。

	(t, n) threshold	t=n 時
[2]的 OR 運算解碼方法	$\Theta(t)$個 OR 運算	$\Theta(n)$個 OR 運算
[3]的多項式方法解碼方法	$\Theta(t)$個四則運算	$\Theta(\log^2 n)$個四則運算
我們的布林運算快速解碼方法	3 個 XOR 運算	3 個 XOR 運算



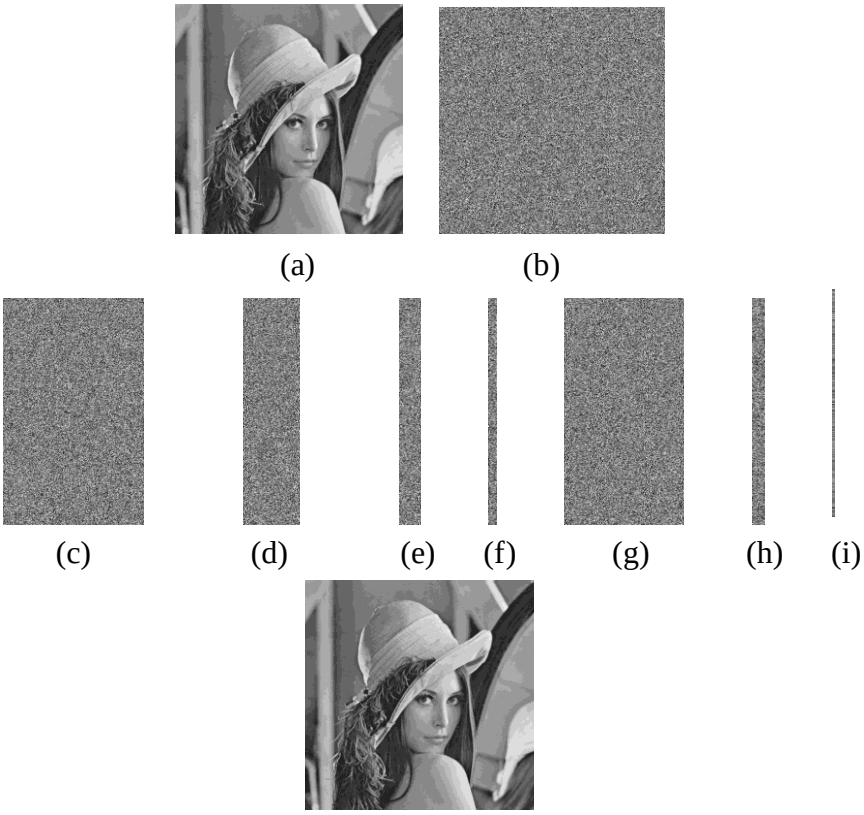
圖二、第一年第二主題:具有 8 個輸入的 FFT 蝴蝶圖。其中 d_i 是輸入值，而 $F(w_j)$ 是輸出值。

表 2、第一年第二主題:512×512 Lena 機密影像的(t, n)分享編碼時間(時間單位:千分之一秒)。

方法 \ n		n=16	n=64	n=256	n=1024	n=4096
T & L [3]	t=16	93	406	2594	6907	
Ours		94	203	718	2750	
T & L [3]	t=64		391	1500	6297	25953
Ours			93	265	953	4594
T & L [3]	t=256			1484	5906	23953
Ours				110	328	1375
T & L [3]	t=1024				6000	23922
Ours					141	438
T & L [3]	t=4096					24047
Ours						172

表 3、第一年第二主題:512×512 Lena 機密影像的傳統(t, $n=t$)分享解碼時間(時間單位:千分之一秒)。一為在[3]中使用反矩陣和矩陣乘法運算的解碼方法(複雜度為 $\Theta(t)$)，另一為我們提出的快速解碼方法(複雜度為 $\Theta(\log^2 t)$)。

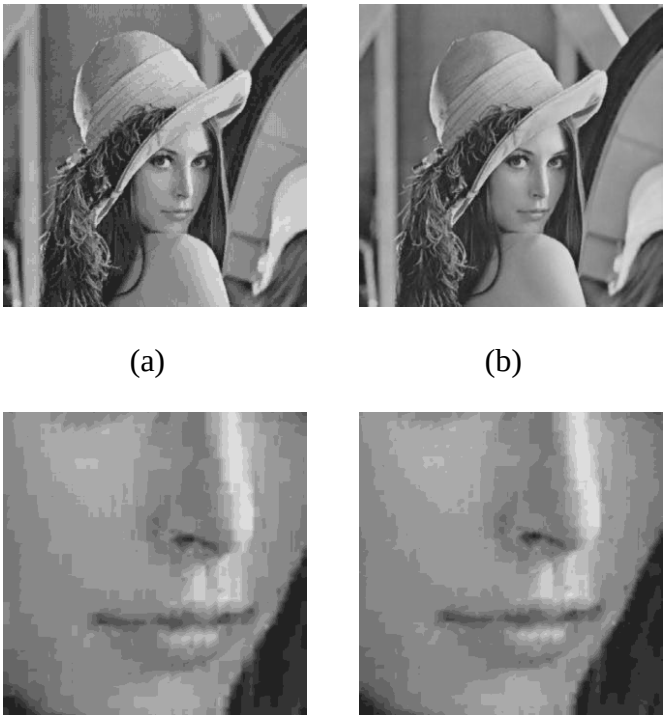
方法 \ t	16	32	64	128	256	512	1024	2048
T & L [3]	234	437	875	1766	3531	7094	14297	28922
Ours	234	313	375	484	593	703	859	1015



圖三、第一年第三主題(快速編碼與解碼的動態權重多項式分享方法)的實驗結果。在這個實驗中，使用的權重總合的門檻值為 t=256。(a)為輸入的 512×512 機密影像，(b)為(a)加密後的結果，(c-i)為分別依權重 160; 64; 24; 8; 134; 12; 3，產生 n=7 張分存影像，(j)為利用四張分存影像(c-f)所重建的無失真機密影像 (160+ 64+ 24+ 8=256≥t)。

表 4、第一年第三主題:512×512 Lena 機密影像的動態權重多項式分享運算編碼時間(時間單位:千分之一秒)。一為[3]的動態權重編碼多項式 $t=w_1$ 分享方法，另一為我們提出的快速動態權重編碼多項式 $t=w_1$ 分享方法。

權重 w_1 / 方法	1	2	4	8	16	32	64	128
T & L [3]	7	15	31	62	110	203	406	813
Ours	7	7	7	6	6	6	6	5



(a) (b)

(c) (d)

圖四、第二年第一主題(以邊緣吻合向量量化為基礎的資訊隱藏方法)的實驗結果。(a)為 512×512 的邊緣吻合向量量化影像 (未藏入任何資訊); (b)為利用本主題方法產生的 512×512 偽裝影像; (c)為將圖(a)的鼻子與嘴巴放大的影像; (d)為將圖(b)的鼻子與嘴巴放大的影像。

表 5、第二年第一主題與隱藏法[24]之隱藏量與偽裝影像品質比較。(方法[24] 亦使用邊緣吻合向量量化)。

掩護影像	Chang et al. [24]		Ours	
	隱藏量 (bits)	偽裝影像品質 (dB)	隱藏量 (bits)	偽裝影像品質 (dB)
Lena	16,129	32.45	413,667	33.86
Jet	16,129	31.09	433,881	32.53
Boat	16,129	29.93	467,367	31.39
Peppers	16,129	29.19	413,322	33.94
Baboon	16,129	23.66	675,226	26.52

(a)

(b)

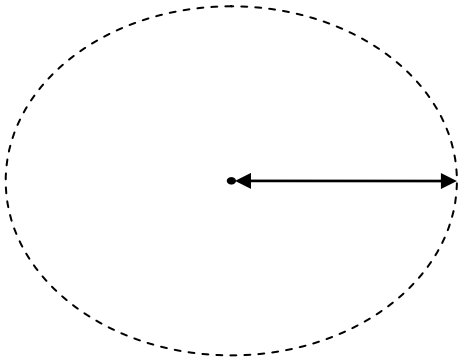
(c)

(d)

圖五、第二年第二主題(基於機密影像中相鄰像素間相似性的高容量資訊隱藏方法)的實驗結果。(a)為輸入的 512×512 機密影像，(b)為輸入的 512×512 掩護影像，(c)為將(a)藏入(b)所得的 512×512 偽裝影像，(d)為從(c)擷取出的 512×512 機密影像。

表 6、第二年第二主題與其它隱藏方法[21][25]的擷取機密影像與偽裝影像品質之比較。

掩護影像	方法	機密影像	偽裝影像品質 (dB)	由偽裝影像擷取之機密影像的品質 (dB)
512×512 Lena	Chung et al. [21]	512×512 Jet	32.50	30.01
	Hu and Lin [25]	512×512 Tiffany	44.42	32.02
	Ours	512×512 Tiffany	51.68	32.02
		512×512 Jet	51.69	31.43



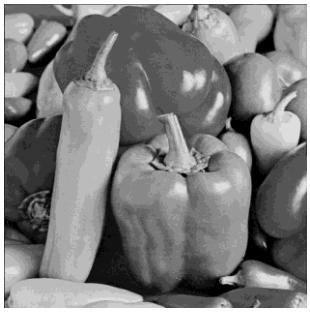
圖六、第二年第三主題(資訊隱藏量之上限研究)的概念圖。其中圓心代表影像 H，x 代表 H 隱藏資料後可能的位置，而這些位置 x 距離 H 不會超過 R。

表 7、第二年第四主題:對於不同的隱藏率所建議的$(1, c_1,..., c_{n-1})$。

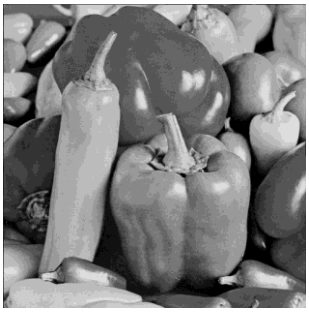
隱藏率(bpp)	m, n	PSNR 預測值(dB)	$1, c_1,..., c_{n-1}$
0.500	4, 8	57.44	1, 2, 3, 4, 5, 6, 7, 8
0.571	4, 7	56.58	1, 2, 3, 4, 5, 6, 7
0.667	4, 6	55.40	1, 2, 3, 4, 5, 6
0.750	6, 8	54.81	1, 2, 3, 4, 5, 6, 13, 26
0.875	7, 8	54.25	1, 2, 8, 12, 24, 29, 47, 62
1.000	6, 6	53.33	1, 2, 5, 12, 20, 28
1.167	7, 6	52.26	1, 3, 8, 18, 42, 54
1.200	6, 5	52.04	1, 6, 10, 18, 31
1.250	5, 4	51.64	1, 2, 6, 11
1.333	8, 6	51.40	1, 3, 9, 27, 50, 93
1.400	7, 5	50.97	1, 3, 9, 28, 52
1.500	6, 4	50.34	1, 3, 8, 22
1.600	8, 5	49.75	1, 3, 58, 87, 124
1.667	5, 3	49.09	1, 4, 10
1.750	7, 4	48.65	1, 4, 40, 58
1.800	9, 5	48.46	1, 36, 86, 146, 215
2.000	10, 5	47.31	1, 9, 23, 243, 324
2.250	9, 4	45.73	1, 13, 149, 232
2.500	10, 4	44.23	1, 26, 33, 221
2.750	11, 4	42.72	1, 364, 559, 986
3.000	12, 4	41.22	1, 9, 350, 491
3.333	10, 3	39.10	1, 20, 195
3.500	7, 2	38.00	1, 12
3.667	11, 3	37.10	1, 61, 597
4.000	12, 3	35.10	1, 1210, 2026

表 8、第二年第四主題:比較第四主題與其它隱藏方法[26]的偽裝影像品質。其中掩護影像是 Lena，且隱藏資料是亂數資料。

隱藏率(bpp)	方法	PSNR (dB)
0.50	[26][27]	54.14
0.50	ours	57.44
0.75	[26][27]	52.38
0.75	ours	54.82
1.00	[21]	51.14
1.00	[26][27]	51.14
1.00	[28] $_{(n=2)}$	52.39
1.00	[29] $_{(n=6)}$	53.33
1.00	ours$_{(m=n=6)}$	53.33
1.16	[30]	52.11
1.17	ours	52.26
1.50	[27]	48.12
1.50	[26]$_{(\text{mod } 3)}$	49.89
1.50	ours	50.34
1.56	[31]	41.79
1.56	[32]	44.10
1.99	[34]	45.14
2.00	[26][27]	46.37
2.00	ours	47.30
2.19	[33]	43.95
2.25	ours	45.73
2.39	[33]	36.96
2.50	[27]	42.69
2.50	[26] $_{(\text{mod } 6)}$	43.12
2.50	ours	44.23
2.89	[34]	39.31
3.00	[26][27]	40.73
3.00	ours	41.22
3.19	[33]	36.28
3.33	ours	39.11
3.50	[27]	36.82
3.50	[26] $_{(\text{mod } 12)}$	37.29
3.50	ours	38.00
3.53	[34]	34.54
3.67	ours	37.10
4.00	[26][27]	34.80
4.00	ours	35.10

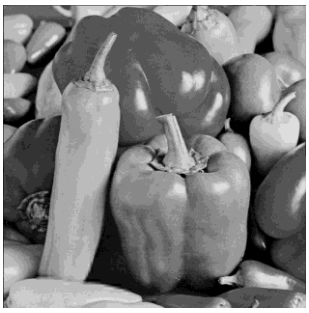


(a)



(b)

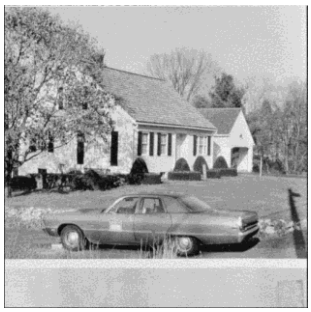
(c)



(d)

圖七、第三年(影像的驗證與修復): 遭受複製再貼上([36])的攻擊。 (a).我們嵌入浮水印後的影像。(b). 浮水印影像遭受複製再貼上的攻擊。(c). 我們驗證的結果。(d). 我們復原後的影像。

(a)



(b)

(c)

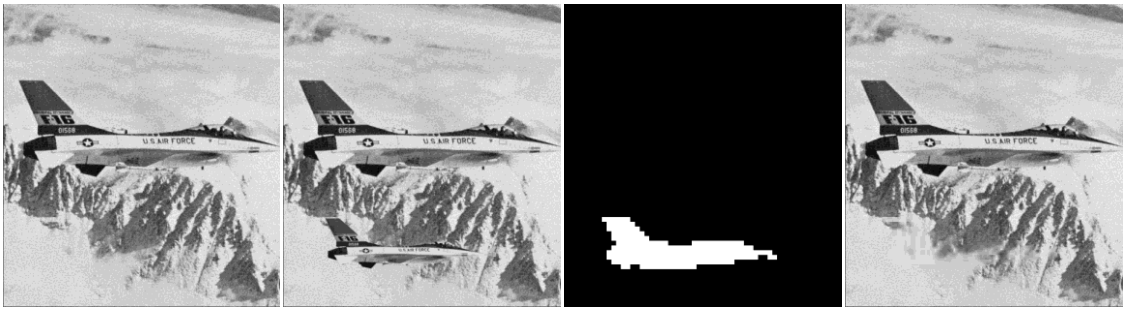
(d)

(e)

圖八、第三年(影像的驗證與修復):遭受拼貼攻擊(collage attack [37])的復原。(a). 嵌入浮水印後的影像—船。(b).嵌入浮水印後的影像—車子和房子。(c).在(b)中的車子被移花接木放到(a)裡。(d). 我們驗證的結果。(e). 我們復原後的影像。

(a) (b) (c)

圖九、第三年(影像的驗證與修復):遭受向量量化攻擊([38])。(a). 浮水印影像。(b).VQ 攻擊後，所得到的(a)結果。(c).我們驗證的結果發現在(b)中整張影像均是造假。又，因為整張影像均是造假，沒有未破壞區域，所以不能復原。

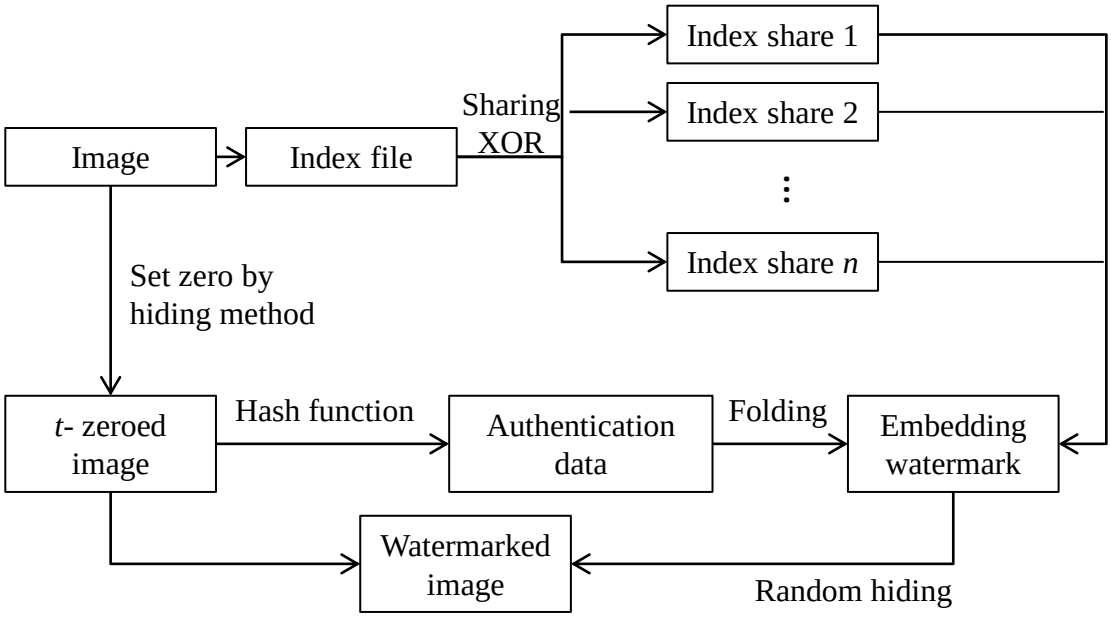


(a) (b) (c) (d)

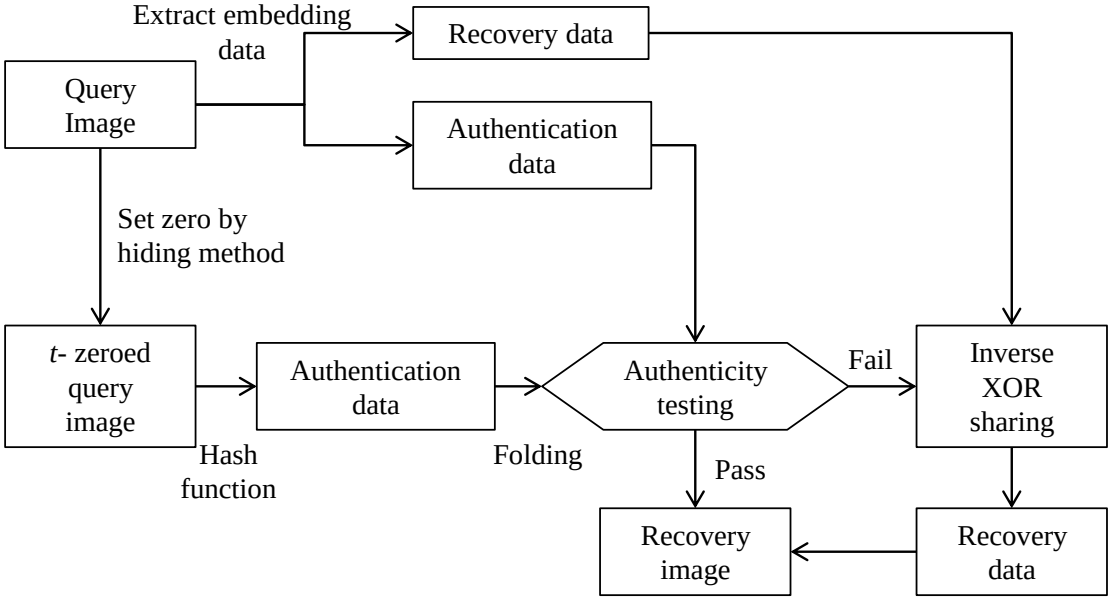
(e)

(f)

圖十、第三年(影像的驗證與修復): 復原後的比較。 (a). 我們的 32.29 dB 浮水印影像. (b). 浮水印影像遭受複製再貼上的攻擊. (c).我們驗證的結果。(d). 我們復原後的 31.89 dB 影像 (e)細節: 我們復原後的 31.89 dB 影像不會有怪東西在雪地出現, (f)細節: 2008 Optical Engineering, Vol. 47 的別人復原後的 29.3dB 影像卻會有怪東西在雪地出現 (其浮水印影像 dB 也比我們的 32.29 dB 稍差)。

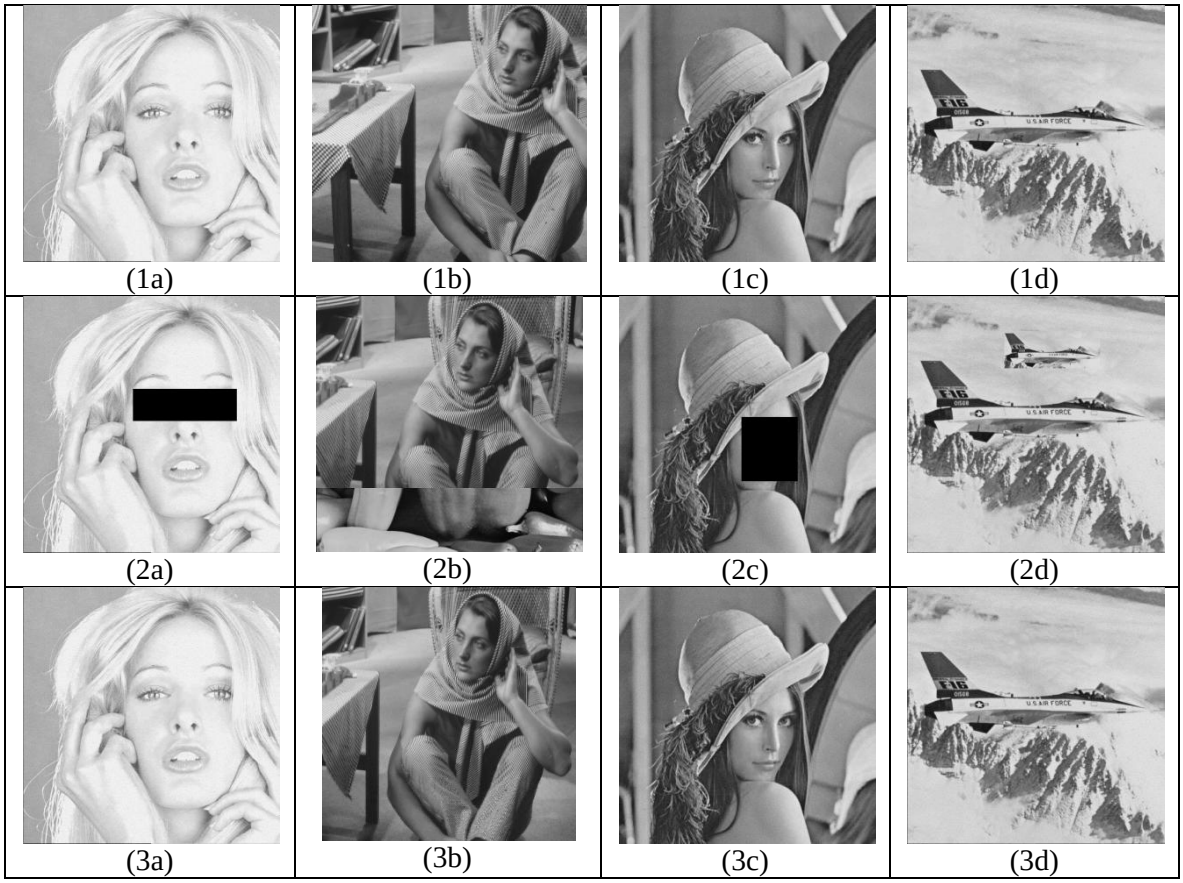


(a)



(b)

圖十一、第三年的使用 XOR 型快速分享法的自我修復法:流程圖。(a).編碼(watermarking)程序。(b).解碼(verification-and-recovery)程序。



圖十二、第三年的使用 XOR 型分享法的自我修復法:結果。(1a-1d).四張具有修復功能的圖片(watermarked image)。(2a-2d).四張圖片分別遭受竄改。(3a-3d).藉由修復(2a-2d)而得到的還原。