國立台東大學教育學系教學科技碩士班

碩士論文

指導教授：鄭承昌　先生

靜態影像資訊隱藏技術
—以自組織映射圖爲基礎

研究生：石琢暐　撰

中　華　民　國　九　十　七　年　六　月

國立台東大學教育學系教學科技碩士班

碩士論文

靜態影像資訊隱藏技術
—以自組織映射圖爲基礎

研　究　生：石琢暐　　撰

指 導 教 授：鄭承昌　先生

中 華 民 國 九 十 七 年 六 月

附件十二

國立台東大學
學位論文考試委員審定書

系所別：

本班 石 琢 暐 君

所提之論文 靜態影像資訊隱藏技術－以自組織映射圖為基礎

業經本委員會通過合於 ■碩士學位論文 □博士學位論文 條件

論文學位考試委員會：

（學位考試委員會主席）

（指導教授）

論文學位考試日期：97 年 5 月 16 日

國立台東大學

附註：1. 一式二份經學位考試委員會簽後，送交系所辦公室及註冊組或進修部存查。

2. 本表為日夜學制通用，請依個人學制分送教務處或進修部辦理。

博碩士論文授權書

本授權書所授權之論文爲本人在 國立台東大學 教育學 系(所)
教學科技碩士 班 96 學年度第 2 學期取得 碩 士學位之論文。
論文名稱：靜態影像資訊隱藏技術—以自組織映射圖爲基礎

本人具有著作財產權之論文全文資料，授予下列單位：

同意	不同意	單　位
■	□	國家圖書館
■	□	本人畢業學校圖書館

得不限地域、時間與次數以微縮、光碟或其他各種數位化方式重製後散布發行或上載網站，藉由網路傳輸，提供讀者基於個人非營利性質之線上檢索、閱覽、下載或列印。

本論文爲本人向經濟部智慧財產局申請專利(未申請者本條款請不予理會)的附件之一，申請文號爲：＿＿＿＿＿＿＿＿，請將全文資料延後半年再公開。

公開時程

立即公開	一年後公開	二年後公開	三年後公開
V			

上述授權內容均無須訂立讓與及授權契約書。依本授權之發行權爲非專屬性發行權利。依本授權所爲之收錄、重製、發行及學術研發利用均爲無償。上述同意與不同意之欄位若未鉤選，本人同意視同授權。

指導教授姓名：鄭彩常　(親筆簽名)

研究生簽名：石琬婷　(親筆正楷)

學　　號：9501007　(務必填寫)

日　　期：中華民國 97 年 6 月 30 日

1.本授權書 (得自 http: //www.lib.nttu.edu.tw/theses/ 下載) 請以黑筆撰寫並影印裝訂於書名頁之次頁。
2.依據 91 學年度第一學期一次教務會議決議:研究生畢業論文「至少需授權學校圖書館數位化，並至遲於三年後上載網路供各界使用及校內瀏覽。」

授權書版本:2005/06/09

博碩士論文電子檔案上網授權書

（提供授權人裝訂於紙本論文書名頁之次頁用）

本授權書所授權之論文為授權人在 國立臺東大學 教育學系(所) _____組 96 學年度第 二 學期取得 碩士 學位之論文。

論文題目： 靜態影像資訊隱藏技術—以自組織映射圖為基礎
指導教授： 鄭承昌

茲同意將授權人擁有著作權之上列論文全文（含摘要），非專屬、無償授權國家圖書館及本人畢業學校圖書館，不限地域、時間與次數，以微縮、光碟或其他各種數位化方式將上列論文重製，並得將數位化之上列論文及論文電子檔以上載網路方式，提供讀者基於個人非營利性質之線上檢索、閱覽、下載或列印。

- 讀者基非營利性質之線上檢索、閱覽、下載或列印上列論文，應依著作權法相關規定辦理。

授權人： 石琢曄
簽　名： 石琢曄　　中華民國 97 年 06 月 28 日

致謝辭

回首碩士班的兩年時光，最要感謝的莫過於　鄭承昌老師的指導與教誨，鄭老師不僅在教育領域上有其專業，並對於計算機領域亦有深入的研究，是故本論文的完成，鄭老師是居功首偉。而其對於做學問的嚴謹態度，更是我輩足以仿效的典範。

當然同時也要感謝　王朱福老師與　謝昆霖老師在論文計劃和口試時點出本研究的問題，由於兩位老師寶貴的建議與意見，使得本論文得以更加的完整與嚴謹。

謝謝在台東大學這幾年的日子裡，電算中心的同仁們對我的包容與關懷。由於我的不成熟，帶給大家不少的困擾。在心情低落時能給予我適時的鼓勵與協助，讓我得已有繼續下去的動力。

最後要感謝的是我的家人和我最愛的女朋友耕儀，沒有他們在背後的默默支持，我也無法順利的完成學業。以本文獻給所有關心、鼓勵我的所有人，沒有大家的協助，不會有今日的我！感謝你們！

琢暐謹誌於

西元二００八年六月二十七日

靜態影像資訊隱藏技術

—以自組織映射圖爲基礎

作者：石琢暐

國立台東大學教育學系教學科技碩士班

摘要

過去研究以密碼學（Cryptography）爲基礎來進行資訊隱藏，導致忽略加密對結果的影響。因此本研究提出一個新的資訊隱藏技術，以自組織映射圖（Self-Organizing Map）爲基礎，輔以最低位元取代法（Least Significant Bit）來嵌入合併資訊。且實驗過程不僅侷限在靜態影像上，還嘗試藏入 WAVE 聲音此種非影像的媒體於掩護影像中。由演算法推導出可藏容量的極限大小略小於原掩護影像，解決過去研究可藏容量太小的問題。從實驗結果來看，本研究的僞裝影像和還原後的機密影像品質較 Linde-Buzo-Gray 演算法好，PSNR值大部份高於 1～4 dB。然還原後的 WAVE 聲音品質兩者則無太大的差異。

關鍵字：資訊隱藏、密碼學、自組織映射圖、最低位元取代法

Information Hiding in Static Image Based on Self-Organizing Map

Cho-wei Shih

Abstract

Originally, for studies in information hiding using vector quantization(VQ) techniques, data or images are encrypted before they are embedded into a cover image. However, using such a scheme is difficult to determine the capacity that a cover image can manage. In this study, an information hiding scheme using Self-Organizing Map and Least Significant Bit techniques is proposed to facilitate hiding unencrypted information in cover images. With the proposed scheme, the information hiding capacity of a cover image is deterministic; a cover image can embed information that its size is slightly less than the size of the cover image. Comparing with Linde-Buzo-Gray(LBG) algorithm applied to traditional VQ, the proposed scheme produces better quality of stego and secret images based on PSNR measurement. There are no significant quality differences between the proposed scheme and VQ, if secret information is in audio format.

keyword: Information hiding, Self-Organizing Map, Least Significant Bit, Linde-Buzo-Gray, Vector Quantization

目錄

表目錄

圖目錄

第壹章　緒論

本章說明本研究的背景動機與目的，以及過去研究的問題。

第壹節　研究背景與動機

隨著網際網路的蓬勃發展，已經由早期單純的分享資訊發展出各式各樣的用途，舉凡人際溝通、交易付款、出版刊物等，網際網路已經不再那樣的單純，儼然已經發展成另一個社會形態了。基於網路的服務愈來愈多元，其中潛在的危機也愈來愈大，駭客（Cracker）非法竊取重要的私人資訊，造成無辜使用者的損失。再者，電子刊物、線上出版品和數位教學媒材等數位媒體的風行，著作權、智慧財產權的保護和宣告相形之下更爲重要。

過去向量量化（Vector Quantization）是以密碼學（Cryptography）爲基礎來進行資訊隱藏。儘管密碼學是保護個人資訊的一項利器，可是隨著電子晶片技術的不斷突破，電腦運算能力的向上提昇，傳統密碼學的優勢或許無法維持。因此，資訊隱藏（Information Hiding）的議題逐漸受到了重視與青睞，和密碼學不同的是，密碼學注重的是將機密資訊以特殊的加密方式轉換成亂碼資料，讓人無法一眼得知原本的機密資訊，而資訊隱藏將資料隱藏在數位媒體中，以達到秘密通訊／隱藏機密訊息的目的。且以密碼學作爲基礎所進行的資訊隱藏，研究結果可能最大的影響因素是在於加密演算法，而非資訊隱藏本身的演算法，此會失去原本使用資訊隱藏技術來嵌入機密訊息的本意。

數位媒體的可塑性相當高，若對數位媒體做些輕微的改變，人眼是較難以發現的因此過去許多論文便是針對數位媒體做資訊隱藏（Petitcolas, Anderson & Kuhn,

1999; Huang, Chu & Huang, 2006; Lin & Delp, 1999; Marvel, Retter & Boncelet, 1998），而且在網路上傳送機密資訊時，將機密資訊嵌入在掩護影像（Cover Image）中後再送出，可更加確保資料的安全性與機密性，較不容易造成其他人的懷疑。然而藉由數位影像來隱藏資訊時，學者也提出必須具備幾個基本條件（李秀月，2003）：隱密性（Imperceptibility）、可藏容量（Capacity）、強韌性（Robustness）、安全性（Security），所以建構一個具上述基本條件的資訊隱藏方法一直是許多研究者努力的目標。因此，研究者在此提出一個以資料壓縮（Data Compression）爲基礎的僞裝法（Steganography），以達到資訊隱藏的目的。

第貳節　研究目的

研究者在此論文提出一個資訊隱藏的僞裝法，是以資料壓縮作爲基礎。在資料壓縮的部分，主要是以類神經網路（Neural Networks）中的自組織映射圖（Self-Organizing Map，以下簡稱 SOM）來實作壓縮，選擇 SOM 的原因是它的演算流程和向量量化（Vector Quantization，以下簡稱 VQ）編碼非常相似。而過去的許多研究，研究者便是使用 VQ 來處理壓縮、浮水印等和資訊隱藏相關的議題（Huang et al., 2006; Mohanty, 1999），且 SOM 在影像壓縮方面，Barbalho 等人（2001）提出分層自組織映射圖（Hierarchical SOM，HSOM），建立樹狀結構，以減少傳統 SOM 搜尋的時間，其結果顯示影像品質較 Linde-Buzo-Gray 演算法優良。Amerijckx 等人（1998）在選擇 SOM 做爲其壓縮的主要方法，就是看中 SOM 其自組織特性，冀望在獲得高壓縮率下不減少影像的品質。嵌入資料（Data Embedding）的方式，則是空間域機制（Spatial Domain

Mechanism）中最典型的代表技術－最低位元取代法（Least Significant Bit，以下簡稱 LSB），利用人眼對於最低位元的變化不易察覺，以達成資料隱藏的目的。

過去和資訊隱藏相關的研究中，有些研究者會選擇其他不同的加密方式（如 Data Encryption Standard）來處理要嵌入的資料，再依此產生的偽裝影像來做實驗（如圖 1），然而此實驗結果便會受到兩個最主要的研究方法之影響：

- 研究者提出的偽裝演算法或流程
- 加密法

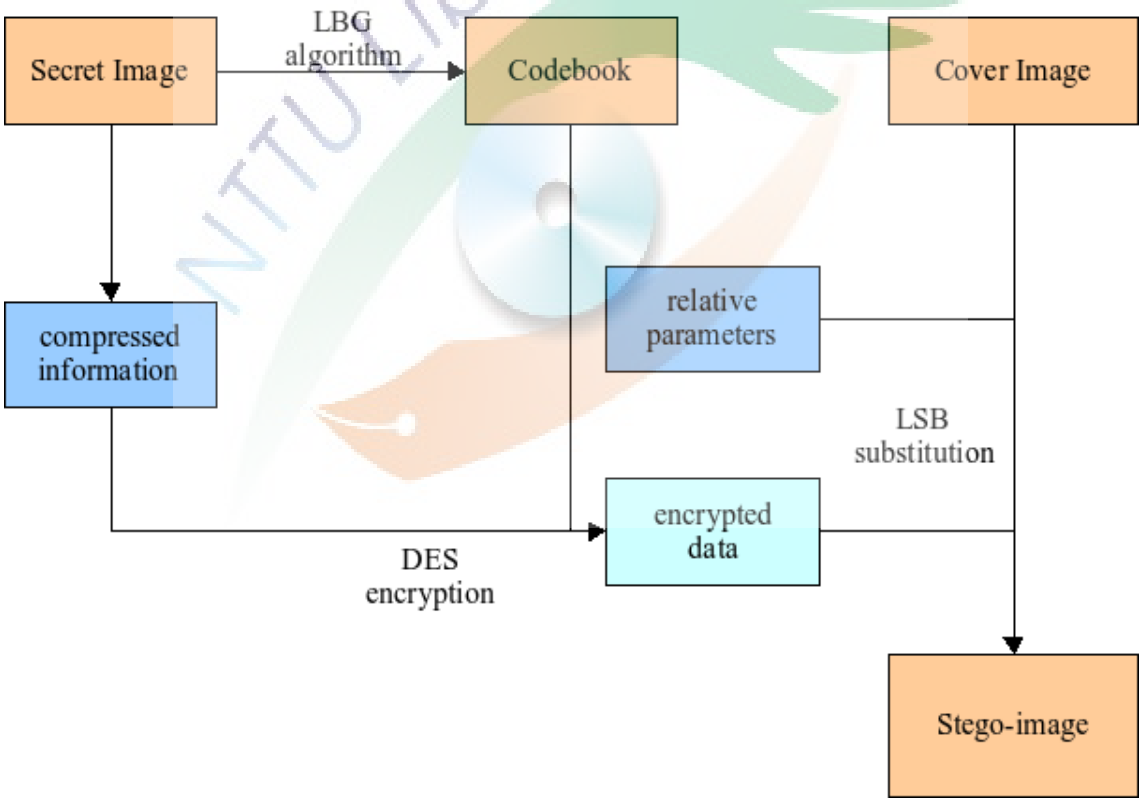


圖 1、一般常見 VQ 的資訊隱藏流程

因此實驗數據的結果可能並非是由研究者提出的偽裝演算法所導致的，有可

能是加密法的關係，甚至兩者合併使用所導致的結果，而這個問題也是過去研究者在其研究中較少提及的部份。所以在本文中，研究者提出的演算流程並不考慮最後加密動作，而是單純地看待整個研究實驗結束後帶給我們的結果。未來研究者可依此做爲基礎，配合已發展穩定的加密法（如 DES）、無失眞壓縮（Lossless Compression）等技術來應用在各方面，以提高安全性或可藏容量（Capacity）。

總結來說，本研究的目的如下：

1. 運用 SOM 與 LSB 這兩個演算法應用在資訊隱藏上；
2. 解構出理論上可藏匿影像的最大極限大小；
3. 解構出理論上可藏匿聲音的最大極限大小；
4. 比較掩護影像和僞裝影像（Stego-image）的品質；
5. 比較原機密影像和擷取出的機密影像的品質；
6. 比較原機密聲音和擷取出的機密聲音的品質。

第參節　論文架構

本文共分爲五章，其中研究者在第參章詳細說明提出的演算流程，且在文中提及如何在掩護影像中嵌入灰階影像和 WAVE 聲音檔，也是本研究最主要的部份各章節簡述如下：

1. 第壹章：說明本研究的背景、動機和研究目的
2. 第貳章：說明資訊隱藏的基礎原理、SOM 和 LSB 法，及過去相關研究
3. 第參章：說明本研究如何結合 SOM 和 LSB 這兩種技術應用在資訊隱藏
4. 第肆章：分別對機密影像和機密 WAVE 聲音做資訊隱藏的實驗結果
5. 第伍章；結論與未來的研究方向

第貳章　文獻探討

此章節說明資訊隱藏的基礎原理與相關議題的比較，以及 SOM 和 LSB 演算法，與過去資訊隱藏的相關研究。

第壹節　資訊隱藏（Information Hiding）

資訊隱藏的領域其實相當的廣泛，而資訊隱藏技術之分類如圖 2 所示（Mohanty, 1999），其中偽裝法（Steganography）是研究者比較關心的部分，所以在此討論的重點會放在偽裝法和其他相關議題的比較上。

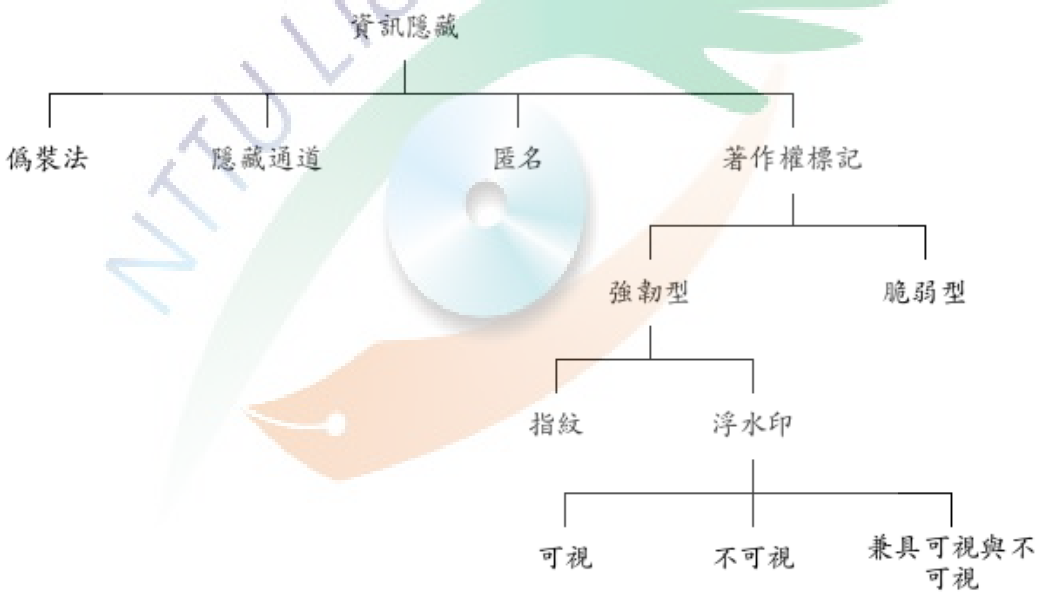


圖 2、資訊隱藏技術（引自 Marvel et al., 1998）

以數位影像來說，偽裝法是在數位影像中隱藏機密訊息，來藉此達到秘密通訊的一種研究，典型的偽裝法編碼過程如圖 3 所示（Lin & Delp, 1999）：掩護影像（Cover Image）和機密訊息（Message）經由偽裝函數（f）產生偽裝影像（Stego-image），其中的金鑰（Stego-key）是可以忽略的，通常在嵌入過程中

會利用此金鑰做加密過程以提高安全性。和密碼學（Cryptography）不同，編碼過程（圖 4）通常將明文（Plain Text）經過編碼函數（E）以產生密文（Cipher Text），再將密文透過解碼函數（D）還原成原本的密文，其中有幾個值得注意的地方（Lin & Delp）：

1. 密碼學編碼過後是亂碼，偽裝法則是一張有嵌入機密訊息的偽裝影像；
2. 密碼學著重還原後的明文，偽裝法則重視可藏容量（Capacity）及隱密性（Imperceptibility）；
3. 和密碼學相比，偽裝法較不需要秘密通訊。

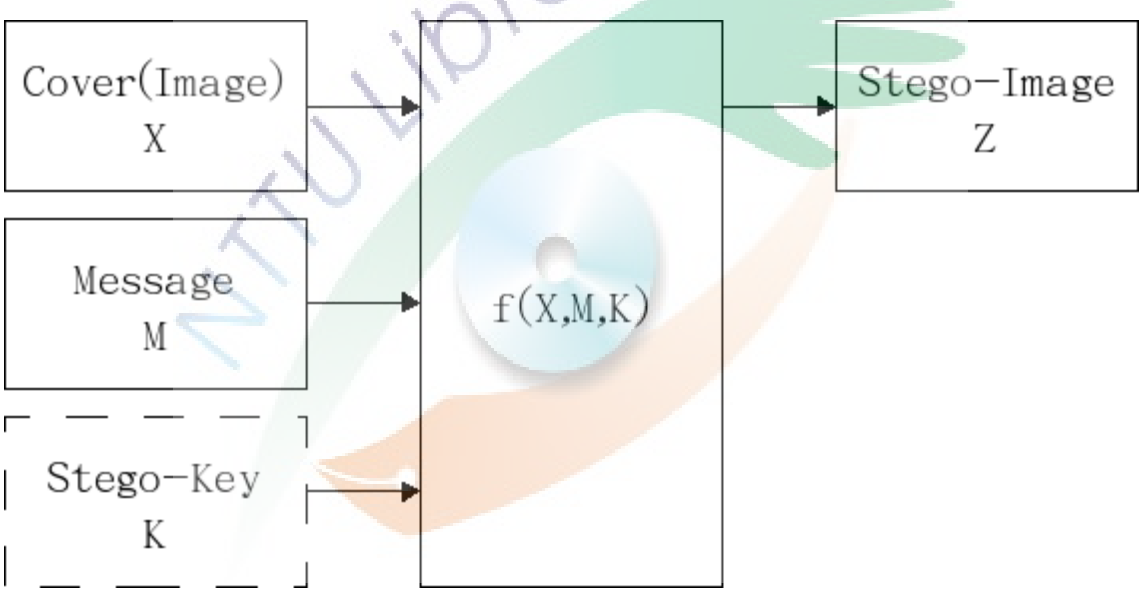


圖 3、典型偽裝法加密過程（引自 Lin & Delp, 1999）

儘管偽裝法和數位浮水印（Digital Watermarking）同屬資訊隱藏的一環，兩者也有相異之處，強韌性（Robustness）是浮水印所關心的重點，且浮水印可能會包含一些資訊，譬如：著作權、版權、追蹤（Tracking）、原作者等等，而且浮水印還可以是可視（Visible）或不可視（Invisible），甚至兩者都有，而偽裝法要藏入的機密訊息可能和掩護影像一點關係也沒有且通常是不可視的

（Mohanty, 1999）。

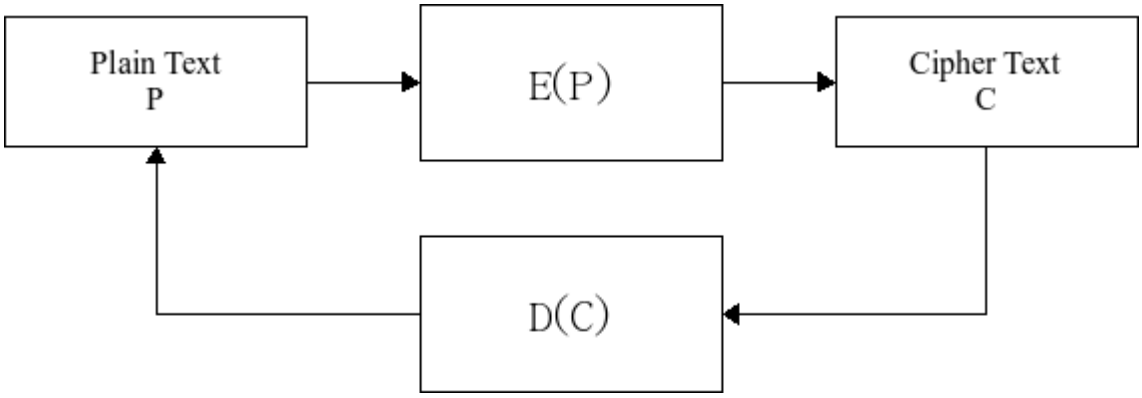


圖 4、密碼學加密、解密過程

第貳節　向量量化（Vector Quantization）與Linde-Buzo-Gray演算法

一般資料壓縮最常見的方法是透過向量量化（Vector Quantization，以下簡稱 VQ）來實做，且 VQ 的應用範圍相當的廣泛，包括語音、音訊、心電圖和影像等等，其應用在影像壓縮上的演算程序如下（王和發，2004）：

1. 將影像切割成大小相等的小區塊；
2. 從區塊中訓練出編碼簿（Codebook），包含多個編碼字（Codeword），且對應至一個索引值（Index）；
3. 對每一個區塊，到編碼簿中搜尋最相似的編碼字，並以其索引值取代小區塊；
4. 解碼時，利用索引值找出對應的編碼字，以此來代表原小區塊即可。

很顯然的，解碼的部分相當的方便，僅僅是作一個查表的動作而已，編碼簿的訓練是一個問題，因爲編碼簿會直接影響解壓縮後影像的品質優劣，而如何快速搜尋最接近的編碼字也是許多研究者感興趣的題目之一（戴顯權，2002）。其

中最常被使用來訓練編碼簿的就是 Linde-Buzo-Gray（LBG）演算法。

LBG 演算法藉由選擇一個失眞估算函數 d 及設定一個失眞改善臨界值 ε，經過重覆訓練的方式來獲得編碼簿。每次的訓練皆尋找與訓練向量最接近的編碼字，再計算全部訓練向量對編碼簿的平均失眞值 D。如果此次與前一次平均失眞值的差異小於臨界值 ε，則停止訓練，此即最後所得的編碼簿。否則計算每一編碼字內訓練向量的中心，並取代原編碼字，再重複整個訓練過程。整個 LBG 演算法流程如下（Gersho & Gray, 1992）：

1. 設定起始編碼簿 $C_t=\{y_i, i=1...N\}$，N為編碼簿大小，t 為第幾次的訓練，失眞估算函數 d，失眞改善臨界值 ε
2. 尋找與訓練向量最接近的編碼字

$$R_i=\{x: d(x, y_i)<d(x, y_j), \forall i\neq j\} \quad \text{.....(1)}$$

x：訓練向量

y_i：編碼字

$d(x, y_i)$：訓練向量 x 和 編碼字 y_i 的距離

R_i：將訓練向量x 歸類到此分類

3. 兩個平均失眞值的差異小於臨界值 ε，停止訓練

$$IF \quad \frac{D_{t-1}-D_t}{D_{t-1}}\leq \varepsilon \quad THEN \quad stop. \quad \text{.....(2)}$$

t：第幾次

D_t：第 t 次的平均失眞值

D_{t-1}：前一次（$t-1$）平均失眞值

4. 將每一個編碼字內訓練向量的中心取代原編碼字

$$C_t=\{cent(R_i), i=1...N\} \ , \ t=t+1, \ GOTO(2) \quad \text{.....(3)}$$

C_t：編碼簿

$cent(R_i)$：取 R_i 內訓練向量的中心

t：第幾次

N：編碼簿大小

第參節　自組織映射圖（Self-Organizing Map）

基於生物神經組織，相似功能群聚現象的特性，Kohonen（1984）提出自組織映射圖（Self-Organizing Map，SOM），經由競爭式學習的訓練，將高維度的輸入向量對應到低維度空間中，整個訓練完成後，其輸出向量用以表現原輸入向量，且產生的輸出向量有彼此群聚的現象。

過去研究者選擇 SOM 做影像壓縮，一部分的因素是它已經成功地應用在各種領域上，且它除了向量量化的特性之外，SOM 其拓撲保留（Topology-Preserving）的特性也被使用在影像的漸進傳輸（Progressive Transmission）上（Riskin, Atlas & Lay, 1991）。自組織（Self-Organizing）也是一個相當重要的因素，利用其『物以類聚』的特性應用在影像壓縮上，可以將影像切割後的區塊分類、聚類成較少的代表向量，藉此達成影像壓縮的目的。而 Amerijckx 等人選擇 SOM 的理由也是因爲這個特性可獲得高壓縮率而不減少影像品質（Amerijjckx et al., 1998）。研究者利用其低維度空間來表現高維度輸入向量的特性，推廣至資訊隱藏上，不僅希望得到較大的可藏容量，且能夠兼顧其影像及聲音品質。

SOM 整個演算法分爲兩個過程：學習過程和回想過程，分述其步驟如下（Kohonen, 1984）：

- 學習過程

1. 初始化：隨機化加權值矩陣 W，神經元個數爲 M；

2．尋找優勝單元：即每輸入一筆訓練向量（X），計算與每一輸出單元最近的距離，此距離最短的輸出單元即爲優勝單元（Winner, W'），而距離的測量是以歐幾里得距離（Euclidean distance, $d(\cdot,\cdot)$）爲衡量的標準（式4）；

$$d(X,W')=min(d(X,W_j)),1\leqslant j\leqslant M \quad \text{.....(4)}$$

X：訓練向量

W'：優勝單元

W_j：加權值矩陣 W 的元素

3．更新加權值矩陣：找出優勝單元後，便是對加權值矩陣做更新，會受到學習速率（η）和鄰近係數（γ）的影響（式5）；

$$W=W+\eta\cdot(X-W)\cdot\gamma \quad \text{.....(5)}$$

$$\gamma=\exp\left(\frac{-d(W',W)}{R}\right) \quad \text{.....(6)}$$

η：學習速率

γ：鄰近係數

R：鄰近半徑

4．重覆步驟2、3，直到收斂或一定數目的學習循環。

- 回想過程

1．初始化：讀入加權值矩陣 W；

2．尋找優勝單元：輸入一個輸入向量 X 後，同學習過程，計算歐氏距離最小者，則此優勝單元即爲輸出層輸出向量。

第肆節　最低位元取代法（Least Significant Bit）

將機密訊息嵌入至影像的方法可以歸納爲三種：最低位元法（Least Significant Bit）、轉換技術（Transform Techniques）和知覺遮罩（Perceptual Masking）（Lin & Delp, 1999）。許多早期的研究藉由修改 LSB 平面（LSB plane）來達到資訊隱藏的目的，最主要的原因是因爲它相當的簡單，

其實 LSB 的原理相當的容易理解，且低位元代表著低亮度或低彩度，因此對人眼來說，修改影像的 LSB 平面是非常的不容易來察覺。

以一張灰階影像爲例，每一像素皆以 8 個位元來表示，若像素值爲 181，二進位表示爲 10110101_2，其中將最後一個位元 1 修改爲 0，亦即 10110100_2，此時兩者的差距僅爲 1 而已。如果以一張圖來示範的話，將其所有像素的最後一個位元修改爲 0（如圖 5），以人眼幾乎是無法觀察出其中的差異。

圖 5、(a)原圖，(b)將原圖中每一像素值最後依位元修改爲 0 後

因此將機密訊息依某種特定順序嵌入在 LSB 平面，藉此瞞過人眼以達到資訊隱藏的目的。然而，LSB 法對於變形、旋轉、裁切等幾何變形，或是再透過失眞壓縮後的影像，都很容易破壞原來所嵌入的機密訊息，顯然的，LSB 法的強韌性（Robustness）是不夠的，儘管如此，還是有許多研究使用 LSB 做爲嵌入資料的方法（林信鋒，2005）。王旭正等人（2007）將機密文字資料編碼後透過文字秘密分享機制產生的子訊息，藏在掩護影像第七層位元平面中，而二維座標位置經視覺安全技術處理產生的 Shares，取代第八層位元平面。Wang 等人（引自

詹啓詳，2005）提出一對一取代表（One-to-one Substitution Table）技術，將秘密資料轉換成另一秘密資料以求更加接近原影像中的不重要位置的值。本研究中，將單純地使用 LSB 的技術來藏入合併資訊及相關資料。

第伍節　影像資訊隱藏

較早的研究中，學者直接將未壓縮過的原始影像（Raw Image）藏入掩護影像之中。可以想見的，這種方式會出現兩個問題：沒有效率、需要較高的可藏容量。有鑑於此，Chen 等人（1998）提出以向量量化（VQ）的方式對機密影像做壓縮，並針對相關的重要資訊做加密的動作，以提高其安全性，此方法稱之爲虛擬影像加密法（Virtual Image Cryptosystem）。

Hu（2003）提出一個改良過的虛擬影像加密法，目的在減少訓練時的計算成本並提高可藏容量。首先，將掩護影像的每一個像素分成兩個部份，高位元的部份用來訓練 VQ 的編碼簿，低位元部份則當作資料取代的地方。這個方法不僅達到了上述兩個目的，且僞裝影像的品質也較 Chen 等人的結果爲佳，不過，還原後機密影像的品質則較差。

Jo 和 Kim（2002）提出以 VQ 作爲基礎，將機密資料藏在壓縮過的編碼中。首先由影像訓練出一編碼簿 C，並分割成三個子編碼簿（Subcodebook），分別是 C_{-1}、C_0、C_1，滿足 $C=C_{-1}\cup C_0\cup C_1$ ，亦即編碼簿 C 中每一個編碼字會被歸類到子編碼簿其中之一。分類規則是兩個編碼字如果非常相似（藉由計算歐式距離且小於臨界值），會成對地分類到 C_1、C_0，如果超過一個臨界值，則歸類到 C_{-1}。嵌入資料的階段中，將每一區塊依序找出最接近的編碼字 w_i，如果 w_i 屬於

C_{-1}，依原來的索引值來代表原區塊，表示沒有藏入任何資料。如果 w_i 屬於 C_1，且目前要嵌入的資料（長度爲 1 bit）爲 1_2，則以此索引值代表原區塊，表示這裡藏入了 1_2；反之，嵌入的資料是 0_2，則以 C_0 所相對應的索引值來代表原索引值，表示這裡藏入了 0_2。也就是說，依序找出索引值屬於在那一個子編碼簿內，即可知道原嵌入的完整資料（bit stream）。不過此方法可能會有一個問題，即是當子編碼簿 C_{-1} 內編碼字非常多時，其可藏容量則會迅速減少。

Chang 和 Wu（2005）延伸了 Jo 和 Kim（2002）所提出的概念，利用邊緣吻合向量量化（Side Match Vector Quantization, SMVQ）和 VQ 來藏入機密資料。首先將影像切割成不重複的區塊，採用 VQ 來壓縮種子區塊（seed blocks），且種子區塊並不藏入任何機密資料，機密資料是藏在剩餘區塊（residual blocks）之中。接著，每個剩餘區塊是藉由 SMVQ 巧妙地初使化。依據機密資料，從狀態區塊（state blocks）挑選適當的編碼字，如果找不到的話，採用 VQ 從原編碼簿尋找適當的編碼字。如果此編碼字會產生明顯的失眞，則不藏入任何機密資料在這個區塊中。最後，不只得到壓縮過的掩護影像，而且可以從壓縮過的編碼字得知隱藏的機密資料。然而，此研究需要額外的資訊來識別區塊是使用 VQ 或是 SMVQ 來編碼，且額外的指標同時也降低了壓縮率（compression rate）。

因爲上述 Chang 和 Wu（2005）的缺點，且該研究屬於失眞壓縮，Chang 等人（2006）提出另一個新的無失眞資訊隱藏方法，同樣也是基於 SMVQ 壓縮，其優點是不需要額外的指標。將機密資料表示爲 $B=(b_0, b_1, \cdots, b_r), b_i=\{0,1\}$。對於每一個剩餘區塊（resideual block），利用上方和左方區塊來產生編碼簿

$K=(k_{0,}k_{1,}\cdots,k_{N-1})$ ，k_a 表示從編碼簿 K 中找出最接近的編碼字。如果 b_i 等於 0，用編碼字 k_a 來取代原區塊；如果 b_i 等於 1，找最接近 k_a 的編碼字 k_b，並用 $(2k_a+k_b)/3$ 來取代原區塊。在還原／萃取階段中，只要計算 k_a 和目前區塊 X_i 的歐氏距離 $ED(X_i,k_a)$ ，如果歐氏距離爲 0，即代表此機密資料位元爲 0，反之則是 1。由於需要重新找出最接近的編碼字 k_a，因此還原階段會花費太多時間，且一個區塊僅藏入 1 位元的資料，可藏容量明顯不夠。

第陸節　音訊資訊隱藏

過去針對音訊資訊隱藏的研究中，最主要是以保護智慧財產權的數位浮水印爲主，其中最常見的方式就是最低位元取代法（LSB）。因爲其簡單、運算快速的特性，更可應用在即時通訊的領域上，相對於原音訊來說，則會產生失眞的現象。

Gruh1 和 Lu（1996）提出利用迴音（Echo）的特性來藏入機密訊息，稱爲迴音隱藏（Echo Hiding）。依據人耳有時間上的遮蔽效應，加上因爲時間延遲造成後面輸出的音訊被前面音訊遮蔽的迴音現象，因此將較小的機密訊息加在較強的音訊之後，只要時間處理掌握得宜，在此遮蔽時間內人耳便聽不到這些訊息此方法的優點是強韌性較佳，然而其可藏容量略顯太低（Huang & Yeo, 2002; Oh et a1, 2001）。

因爲人耳對於相位（phase）的變化較不敏感，Tilki 和 Beex（1997）兩位學者提出相位編碼（Phase Coding）的觀念。首先將原始音訊分成許多區段，再利用離散傅利葉轉換（Discrete Fourier Transform），將每個區段的訊號轉換

成相位和量值，計算每個區段相位間的差異。在維持區段相位差異不變之下，將機密訊息嵌入初始音訊區段的相位中，再調整其他音訊區段相位。最後依此新相位還原成音訊，便可達到資訊隱藏的目的。然而此方法在其解碼過程中略顯複雜且還原之前，必須知道音訊區段的長度、傅利葉轉換長度等訊息（施奕安，2006）。

Zhou 等人（2006）提出以漢明碼（Hamming Code）的編碼冗餘（encoding redundancy）來做音訊資訊隱藏。因爲漢明碼的特徵（syndrome）s 和 Error Map（e）有著一對一的對應關係，因此可建一個 mapping encoding 使其也滿足一對一對應關係（如圖 6）。

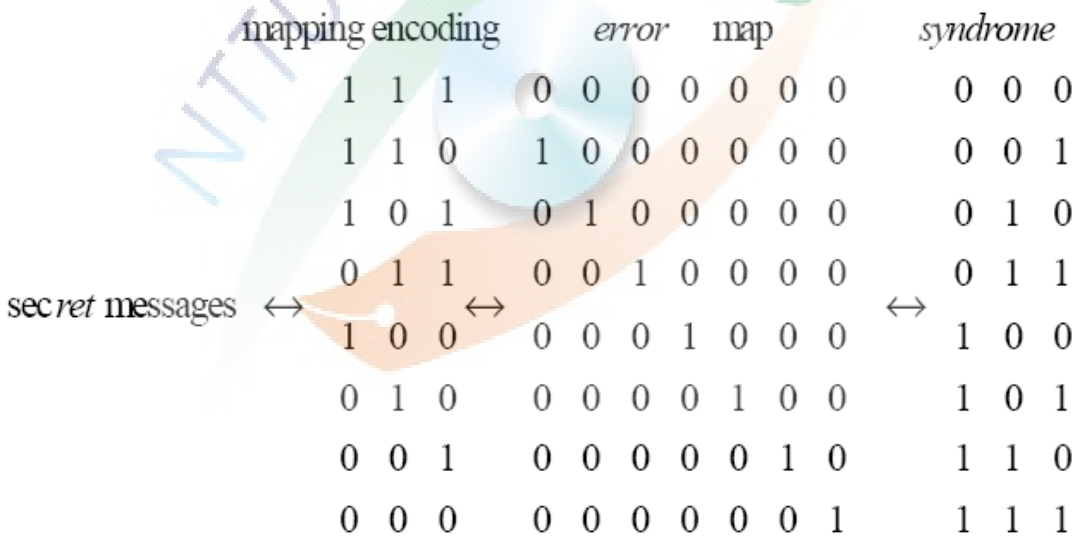


圖 6、Mapping encoding（引自 Zhou et. al., 2006）

舉例來說，一個機密訊息 110 和編碼字 V=[1011010]，將 V 修改成 r=[0011010]，亦即故意修改成有錯誤發生，來表示有機密訊息被嵌入。解碼時，計算 r 的特徵 s 得 001，即可知道原藏入的機密訊息爲 110。相反的，如果

s=[000] 即代表這裡沒有藏入機密訊息。其缺點是必須將 error map 也藏入掩護音訊中，造成其可藏容量的降低，不過其最大優點是此方法不僅可應用在聲音亦可應用在不同的數位媒體上，如靜態影像、動態影像等。

第參章　研究方法

過去有學者使用掩護影像（Chen et a1., 1998）或機密影像（李秀月，2003）來訓練編碼簿，不過可能會影響機密影像或掩護影像的品質，因此研究者在此使用機密訊息和掩護影像一起訓練編碼簿，藉此兼顧嵌入機密訊息後的僞裝影像及還原後機密訊息的品質。研究者在此提出以 SOM 資料壓縮爲基礎的資訊隱藏方法，分別對灰階機密影像和 WAVE 聲音檔做研究，以解決過去研究可藏容量太小與使用密碼學加密對實驗的影響。

第壹節　灰階機密影像

研究者在這裡所使用的影像，皆是使用灰階影像，檔案格式是未經任何處理過的像素資料，因此影像不會帶有任何的表頭，以方便研究者在處理影像時可以單純化，而僅專注於演算流程上。

一、　編碼簿的訓練及僞裝影像的初始化

將機密影像和掩護影像切割成小區塊，然後將這些小區塊當作訓練向量，例如：機密影像大小爲　256×256　，掩護影像大小爲　512×512　，切割成　4×4　的小區塊，則可以得到　4096＋16384＝20480　個長度爲　4×4＝16　的訓練向量。將訓練向量透過 SOM 來訓練一編碼簿，此編碼簿和一般向量量化所訓練的編碼簿有所差異，因爲 SOM 的輸出向量是一個二維平面，所以訓練出來的編碼簿是一個二維平面的編碼簿。訓練完編碼簿之後，依序將原始掩護影像的小區塊搜尋編碼簿中最相似的編碼字，並以此編碼字取代原來的掩護影像來初使化一僞裝影像，此時同時紀錄編碼字對應原始掩護影像小區塊的索引值（索引表

一），將原始機密影像的小區塊搜尋編碼簿中最相似的編碼字，僅紀錄對應編碼字的索引值（索引表二）。偽裝影像初使化的流程如圖 7，步驟如下：

1. 掩護影像（C_{img}）和機密影像（S_{img}）切割成小區塊，形成訓練範例（Ts）；
2. 將訓練範例透過 SOM 訓練出一編碼簿（Cb）；
3. 透過 SOM 回想過程，將原始掩護影像小區塊取代成一偽裝影像（St_{img}），並紀錄編碼字對應原始小區塊的索引值（ $Index_{Cb \to C_{img}}$ ）；
4. 透過 SOM 回想過程，紀錄原始機密影像小區塊對應編碼字的索引值形成一索引表（ $Index_{S_{img} \to Cb}$ ）。

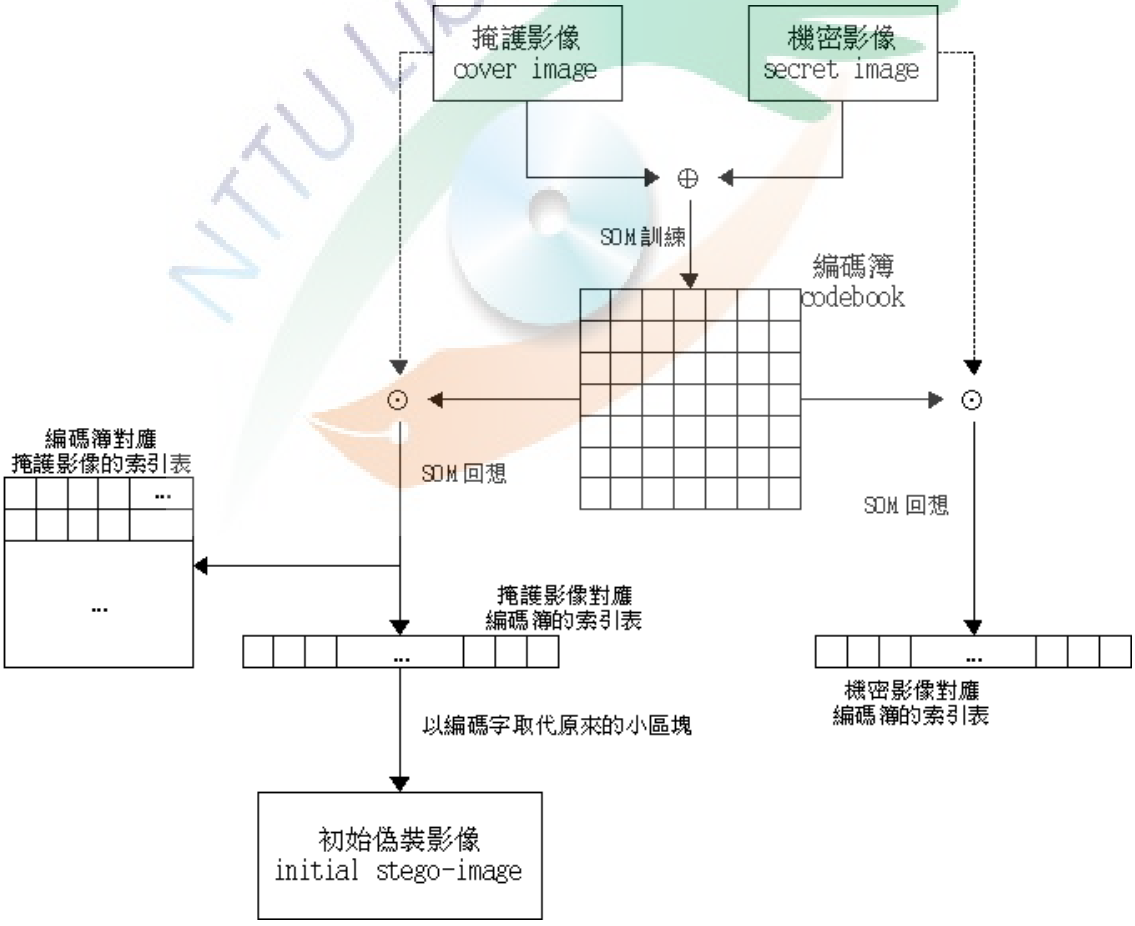


圖 7、偽裝影像的初始化

經過 SOM 的處理之後，會得到一初始僞裝影像(Initial Stego-image)、機密影像對應編碼簿的索引表，和編碼簿對應掩護影像的索引表。初使僞裝影像的建立，僅是對掩護影像經過 SOM 訓練及回想過程所得到，還會有一張索引表，紀錄著編碼簿對應掩護影像的索引表（如圖 8），因爲機密影像必須要能透過編碼簿來還原，也因此編碼簿也需要嵌入 到僞裝影像中。而紀錄編碼簿的方式是透過已經還原完成的掩護影像，未對應到掩護影像的編碼字，則是在編碼簿中尋找最相似的編碼字來取代原編碼字。

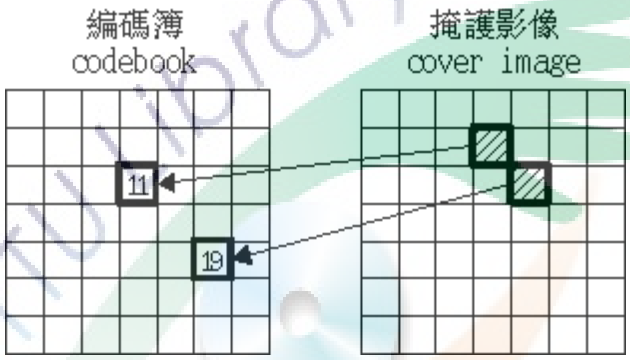


圖 8、編碼簿對應掩護影像的索引表

二、 嵌入機密資訊

本研究中，研究者選擇使用 LSB 來作爲嵌入資料的方式。有一些必要的資訊需先嵌入到僞裝影像中，包含區塊大小、二維編碼簿大小和機密影像大小，而這些合併資訊依序嵌入在僞裝影像的像素中，且定義區塊大小最大爲 8+8=16 個位元，二維編碼簿大小最大爲 8+8=16 個位元，機密影像大小最大爲 16+16=32 個位元，故合併資訊總共佔 64 個位元。經過 SOM 的訓練回想過程後，將上述 64 個位元的合併資訊藏入初始僞裝影像，以及編碼簿對應掩護影像的索引表、機密影像對應編碼簿的索引表，然而藏入這兩張索引表的方式和藏入合併資訊有

所不同。假設我們將一張灰階影像，藏在一個位元組的最後兩個位元，且小區塊的大小爲 4×4 ，則共需 64/2/4 = 8 個小區塊，則索引表第一個索引值將藏在第九個小區塊，且此時可發現索引值必須小於 $2^{4\times4}=2^{16}$ ，餘類推。因此，嵌入機密資訊的步驟大致分爲三步（如圖 9）：

1. 長度爲 64 位元的合併資訊（Ndata），依照像素順序來嵌入（圖 10）；
2. 依照區塊的順序藏入「編碼簿對應掩護影像的索引表」（圖 11）；
3. 依照區塊的順序藏入「機密影像對應編碼簿的索引表」（圖 11）。

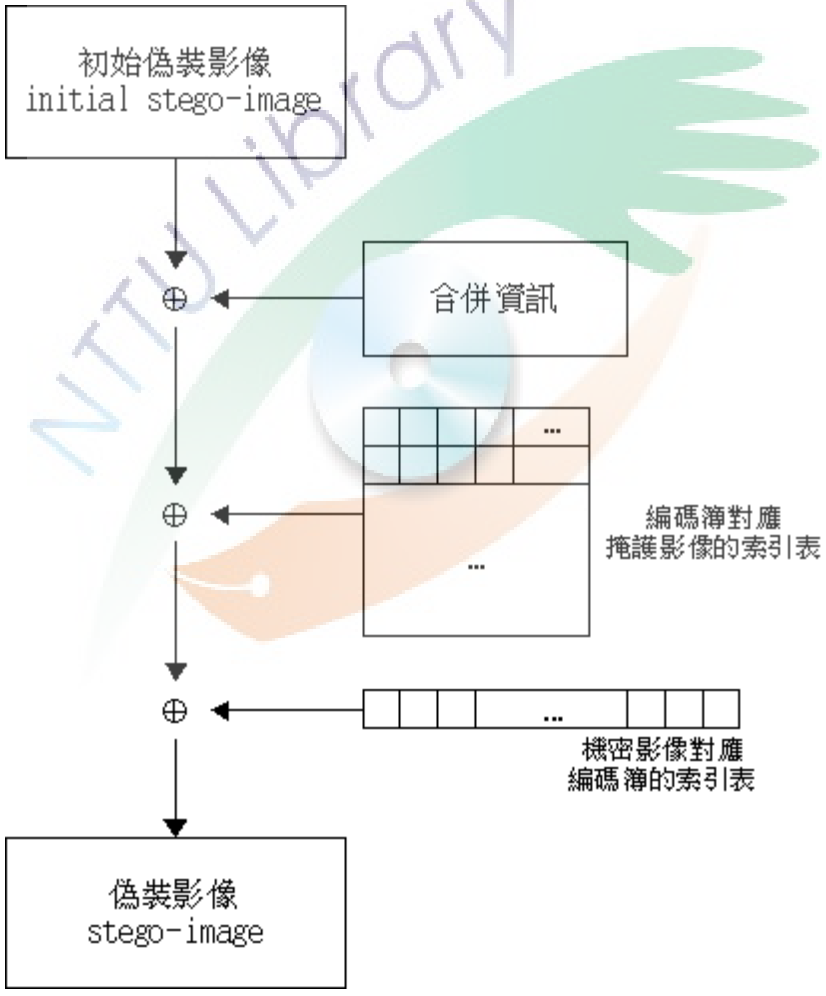


圖 9、嵌入機密資料流程

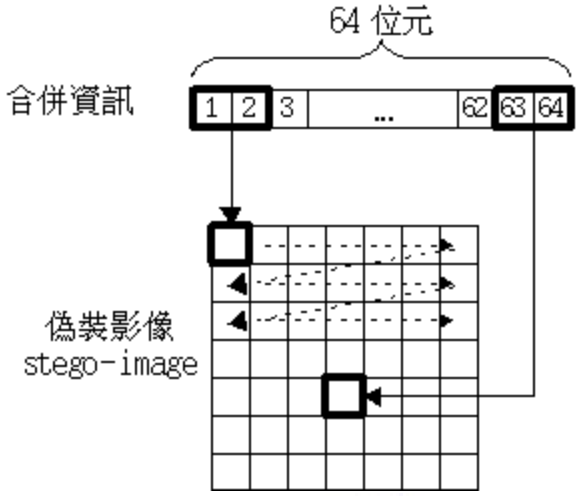


圖 10、嵌入合併資訊至偽裝影像（以藏２個位元爲例）

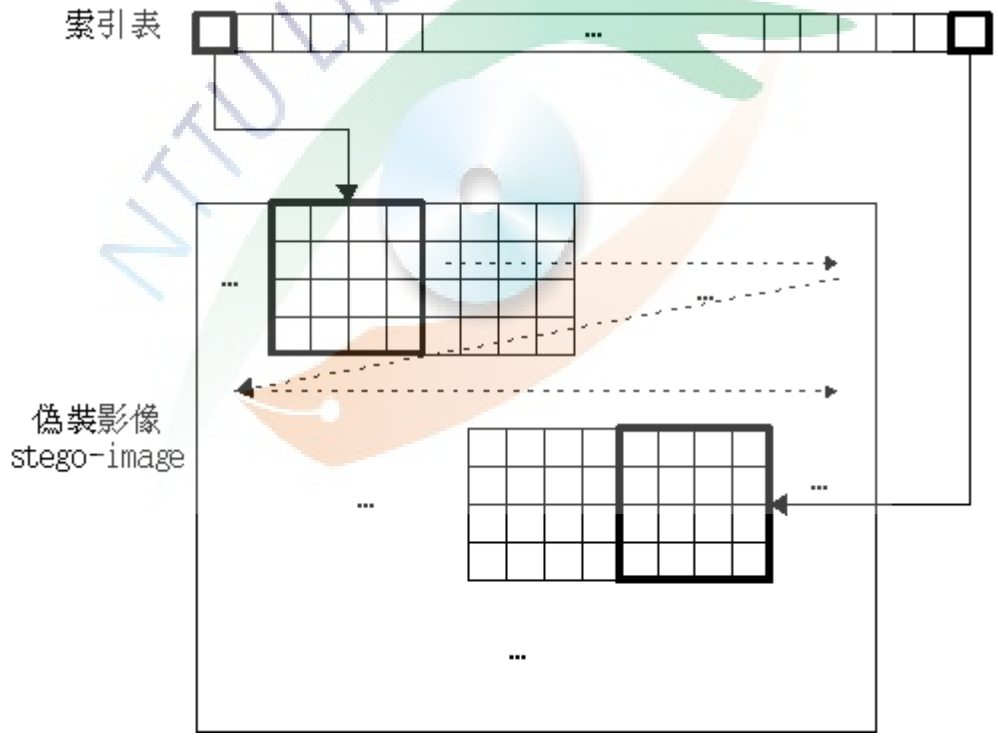


圖 11、嵌入索引表至偽裝影像（以小區塊大小 4x4 爲例）

三、 解密：還原機密影像

解密的過程是依照嵌入資料的順序，依序地將資訊取出。首先取出長度爲

64 位元的合併資訊，包含區塊大小、二維編碼簿大小和機密影像大小，接下來從下一個小區塊依序取出便可得編碼簿對應掩護影像的索引表、機密影像對應編碼簿的索引表。最後的解密，僅是透過兩次的對應：機密影像對應編碼簿、編碼簿對應掩護影像，而僞裝影像本來就是從掩護影像訓練後回想、對應所產生。也就是說，編碼簿對應掩護影像即是對應僞裝影像。透過兩次的對應之後，以對應僞裝影像後的小區塊對應原機密影像區塊即可，便可還原出機密影像，而此動作也僅僅是一個查表的動作而已。

還原機密影像的步驟如下（圖 12）：

1. 取出長度爲 64 位元的合併資訊，包含區塊大小、二維編碼簿大小和機密影像大小；
2. 切割僞裝影像成小區塊，形成一索引表；
3. 從小區塊依序取出「編碼簿對應掩護影像的索引表」；
4. 從小區塊依序取出「機密影像對應編碼簿的索引表」；
5. 產生機密影像，透過「機密影像對應編碼簿、編碼簿對應掩護影像」。

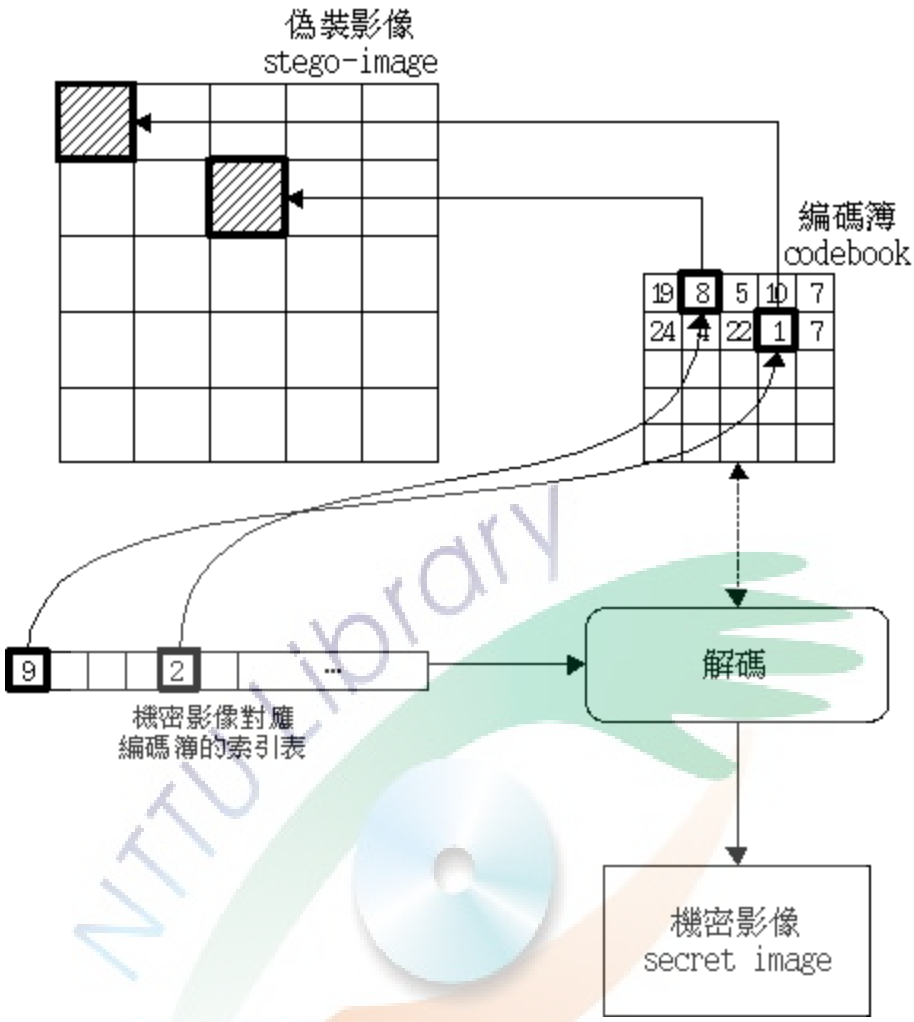


圖 12、還原機密影像

第貳節　WAVE 聲音檔

在處理 WAVE 聲音檔時和處理灰階機密影像是很相似的，比較不同的是 WAVE 聲音檔屬於有既有格式的一種檔案，在檔案前面有表頭、剩下的便是眞正聲音的資料，所以研究者在處理 WAVE 聲音檔時會有一些和灰階機密影像不同的地方，也就是長度爲 44 Bytes 表頭。

一、 編碼簿的訓練及僞裝影像的初始化

一開始的處理便是要將 WAVE 聲音檔的表頭和資料分開來，且表頭包含的資訊是不容許有絲毫的失眞，也因此表頭的部份會單純的透過 LSB 法來嵌入，剩下的資料部份便以處理機密影像的方式做處理。處理步驟如下：

1. 將機密 WAVE 聲音檔（W）分開出 WAVE 檔表頭（W_{header}）、WAVE 聲音資料（S_{wave}）；
2. 掩護影像（C_{img}）和 WAVE 聲音資料切割成小區塊，形成訓練範例（Ts）；
3. 將訓練範例透過 SOM 訓練出一編碼簿（Cb）；
4. 透過 SOM 回想過程，將原始掩護影像小區塊取代成一僞裝影像（St_{img}），並紀錄編碼字對應原始小區塊的索引值（ $Index_{Cb \to C_{img}}$ ）；
5. 透過 SOM 回想過程，紀錄原始 WAVE 聲音資料小區塊對應編碼字的索引值（ $Index_{S_{wave} \to Cb}$ ）。

二、 嵌入機密資訊

一些必要的資訊必須先嵌入僞裝影像之中，其中包含區塊大小、編碼簿大小、WAVE 聲音檔大小和 WAVE 聲音檔的表頭，且將這些資訊依序嵌入，定義的大小如上節所數，另定義 WAVE 聲音檔大小爲 32 位元（等同於機密影像大小）。而 WAVE 聲音檔表頭是固定的，大小爲 44bytes，亦即 352 位元，故這些合併資訊總共佔了 416 位元。而嵌入機密資訊的步驟則和上節所述相同，僅僅是合併資訊的大小有所調整。

三、 解密：還原機密 WAVE 聲音檔

解密的步驟也和上節所述差不多，其還原的步驟如下（表 5）：

1. 取出長度爲 416 位元的合併資訊（Ndata），包含區塊大小、編碼簿大小、WAVE 聲音檔大小和 WAVE 聲音檔的表頭；
2. 切割僞裝影像成小區塊，形成一索引表；
3. 從小區塊依序取出「編碼簿對應掩護影像的索引表」；
4. 從小區塊依序取出「機密 WAVE 聲音資料對應編碼簿的索引表」；
5. 產生機密 WAVE 聲音資料檔，透過「機密 WAVE 聲音資料對應編碼簿、編碼簿對應掩護影像」；
6. 合併 WAVE 聲音檔表頭和 WAVE 聲音資料檔成一完整的 WAVE 聲音檔。

第參節　機密資訊品質評鑑標準

爲了衡量兩張影像的品質，研究者採用的方式是計算 PSNR 值（Peak Signal-to Noise Ratio），其值越大越好，代表兩者間的差異較小，相對於人眼來說，是一個較爲客觀的參考值。

假設兩張灰階影像分別爲 $I(i,j)$ 和 $K(i,j)$，其影像大小皆爲 $m\times n$，且最大灰階值爲 255，則：

$$MSE=\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}|I(i,j)-K(i,j)|^2 \quad \text{.....(7)}$$

$$PSNR = 10\times\log\frac{255^2}{MSE} = 20\times\log\frac{255}{\sqrt{MSE}} \quad \text{.....(8)}$$

其中 MSE 指的是 Mean Square Error，其意義是兩者的距離差異，故值要越小越好，值越小則 PSNR 越大，影像品質越好。

而衡量聲音的品質亦是採用 PSNR 值，惟 MSE 的計算方式稍有不同。假設以音效格式爲 8000Hz、8Bit，亦即「一秒鐘取樣 8000 次，每次取樣以 8 個

bit 來儲存」，其聲音取樣最大值爲255，此時 MSE 爲：

$$MSE=\frac{1}{m}\sum_{i=0}^{m-1}|I(i)-K(i)|^2 \quad \text{.....(9)}$$

I 和 K 指的是兩段取樣數爲 m 的聲音。

第肆節　可藏容量大小

掩護影像的大小是固定的，自然而然可以想見可以容量會有一定的上限。假設掩護影像大小爲 $C_x \times C_y$ ，切割成 $m \times n$ 大小，編碼簿大小爲W，合併資訊長度爲H_0位元，WAVE 聲音表頭長度爲H_w位元，藏在最後的bitsize位元，機密資料長度爲S，而將掩護影像大小切割後的區塊數是上限，大於等於表頭長度所需的區塊數 + 編碼簿所需的區塊數 + 機密資料所需區塊數（式10），則機密資料的長度受限在式11：

$$\frac{C_x \times C_y}{m \times n} \geq \frac{H_0}{n \times bitsize} + W + \frac{S}{m \times n} \quad \text{.....(10)}$$

$$S \leq C_x \times C_y - \frac{H_0 \times m}{bitsize} - m \times n \times W \quad \text{.....(11)}$$

$C_x \times C_y$：掩護影像大小（高×寬），單位：像素

$m \times n$：切割後的小區塊大小（高×寬），單位：像素

H_0：合併資訊長度，單位：位元

$bitsize$：要藏入的位元長度，單位：位元

W：編碼簿大小

S：機密影像大小

如果是藏入 WAVE 聲音還需加上其表頭長度所需的區塊數（式 12），則機密資料的長度受限在式 13：

$$\frac{C_x \times C_y}{m \times n} \geq \frac{H_0}{n \times bitsize} + W + \frac{S}{m \times n} + \frac{H_w}{n \times bitsize} \quad \text{.....(12)}$$

$$S \leq C_x \times C_y - \frac{(H_0 + H_w) \times m}{bitsize} - m \times n \times W \quad \text{.....(13)}$$

$C_x \times C_y$：掩護影像大小（高×寬），單位：像素

$m \times n$：切割後的小區塊大小（高×寬），單位：像素

H_0：合併資訊長度，單位：位元

$bitsize$：要藏入的位元長度，單位：位元

W：編碼簿大小

S：機密聲音大小

H_w：WAVE 聲音表頭長度，單位：位元

假設掩護影像大小爲 $512 \times 512 (C_x \times C_y)$，切割成 $4 \times 4 (m \times n)$ 的大小，編碼簿大小爲 $256 (W)$，藏在最後的 $2 (bitsize)$ 個位元，則機密影像的大小上限是 $512 \times 512 - \frac{64 \times 4}{2} - 4 \times 4 \times 256 = 257920$，亦即可藏入大小爲 507×507 的灰階影像。

假設掩護影像大小爲 $512 \times 512 (C_x \times C_y)$，切割成 $4 \times 4 (m \times n)$ 的大小，編碼簿大小爲 $256 (W)$，藏在最後的 $2 (bitsize)$ 個位元，而 WAVE 聲音格式爲「取樣頻率 8000HZ、取樣樣本大小 1 Byte、單音」，機密 WAVE 聲音的長度

上限是 $512\times512-\frac{(64+352)\times4}{2}-4\times4\times256=257216$ ，亦即在設定條件的機密 WAVE 聲音下，可以藏入 32 秒左右的聲音。

第肆章　實驗結果與討論

實驗結果將與 LBG 演算法來做比較，分別對影像和聲音做討論。

第壹節　實驗用影像與聲音

實驗用影像使用過去學者使用的灰階影像進行實驗，每張掩護影像（圖 13）大小爲 512×512 像素，每張機密影像（圖 14）大小爲 256×256 像素，機密 WAVE 聲音（圖 15）爲「取樣頻率 8000HZ、取樣樣本大小 1 Byte、單音、長度爲 9 秒」，聲音來源則是研究者本身講話錄製下來的聲音。

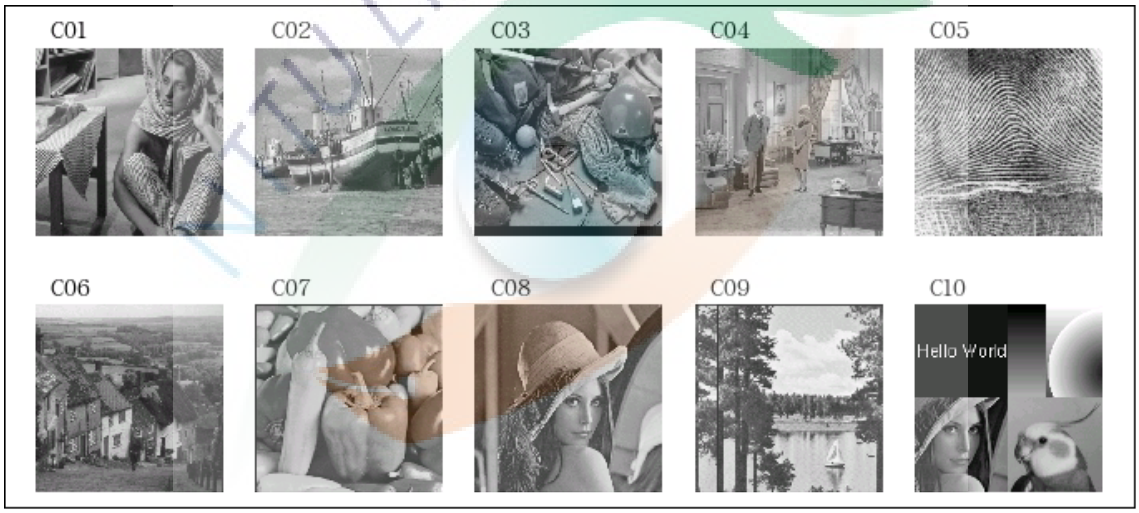


圖 13、實驗用掩護影像

圖 14、實驗用機密影像

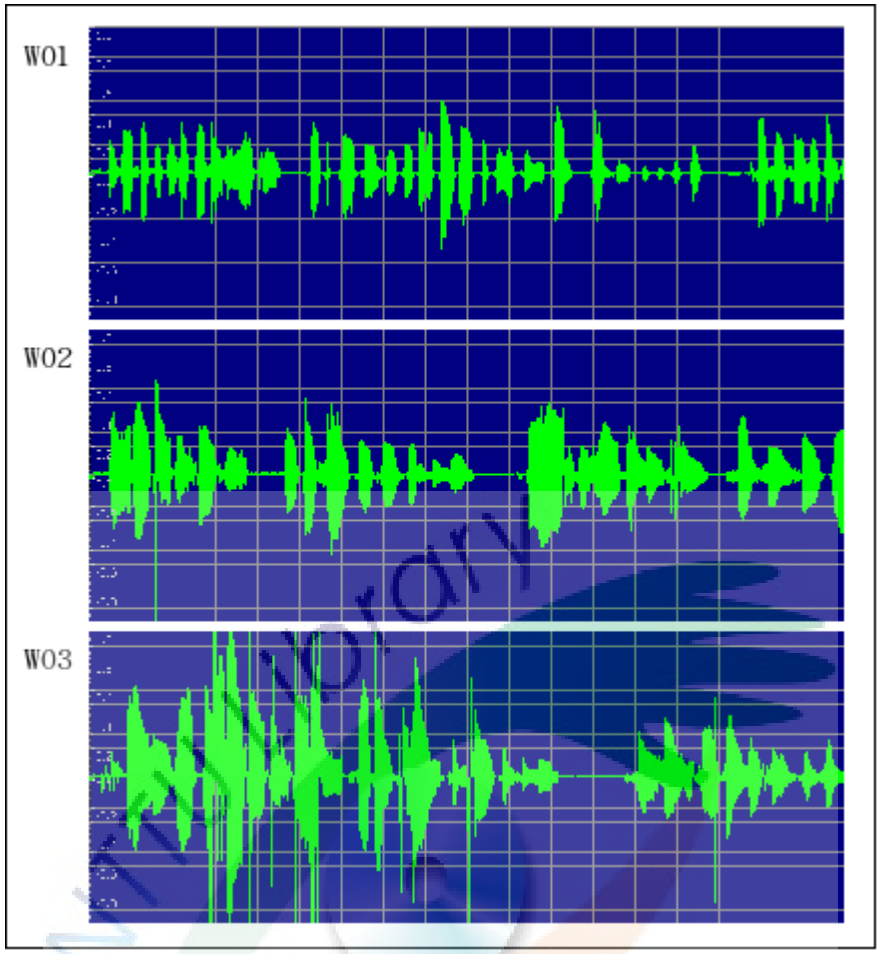


圖 15、實驗用機密 WAVE 聲音

第貳節　實驗結果－靜態灰階影像

實驗的設定條件如下：

1. 以圖 13 作爲掩護影像，大小皆爲 $512\times512(C_x\times C_y)$ 像素；
2. 以圖 14 作爲機密影像，大小皆爲 $256\times256(S)$ 像素；
3. 切割成 $4\times4(m\times n)$ 像素的小區塊；
4. 編碼簿大小 W 爲 256 ；
5. 藏在最後 $2(bitsize)$ 個位元。

依據上述的設定條件將每個機密影像分別藏入掩護影像中，得到偽裝影像如圖 16、17（其餘見附錄 A），由肉眼觀察偽裝影像顯示此方法能有效的隱藏機密資訊。再利用還原機密影像的演算法取出偽裝影像中的機密影像，萃取出來後的機密影像如圖 16、17 所示（其餘見附錄 B），整個實驗的花費時間、掩護影像與偽裝影像的 PSNR 值與原機密影像和還原後機密影像的 PSNR 值整理後如表 1。

圖 16、實驗結果（C01：掩護影像，St01：偽裝影像，S01：機密影像，R01：還原後機密影像）

圖 17、實驗結果（C02：掩護影像，St02：偽裝影像，S02：機密影像，R02：還原後機密影像）

在設定相同的條件之下，以 Linde-Buzo-Gray（LBG）演算法進行模擬實驗，整個實驗結果如表 2。

和本研究提出的演算法的比較結果如圖 18～20，從花費時間（圖 18）來看，本研究提出演算法所花費的時間不一定比 LBG 演算法較短，LBG 演算法所花費

的時間相當的穩定，皆在 50 秒上下，然而本研究的演算法則振幅差異相當大，並不是相當的穩定。從偽裝影像的品質（圖 19）上來看，本研究提出的演算法優於 LBG 演算法，且從圖上發現，不管藏入的機密影像爲何，同一掩護影像訓練出的偽裝影像 PSNR 值沒有明顯的差異。從還原後機密影像的品質（圖 20）來看，大致上可以說本研究演算法較好，僅有兩個結果（圖 20－S03 的 C07、C10）較 LBG 演算法差。

表 1、實驗結果－靜態灰階影像（SOM，藏在最後 2 個位元）

	S01			S02			S03			S04		
	Sec	Stego PSNR	Secret PSNR	Sec	Stego PSNR	Secret PSNR	Sec	Stego PSNR	Secret PSNR	Sec	Stego PSNR	Secret PSNR
C01	47	27.41	26.99	58	27.48	28.59	52	27.52	31.06	68	27.48	27.56
C02	46	29.04	27.52	43	29.10	28.89	59	29.15	31.80	81	29.15	27.92
C03	32	26.57	27.87	41	26.67	28.44	68	26.76	31.41	68	26.73	27.63
C04	45	28.63	27.87	44	28.63	28.94	73	28.68	31.80	61	28.68	27.87
C05	52	26.45	27.09	36	26.48	28.31	39	26.54	31.41	59	26.51	27.37
C06	34	30.14	26.45	36	30.27	29.38	47	30.27	30.42	43	30.20	27.96
C07	74	33.66	27.87	71	33.66	28.79	138	33.82	29.68	59	33.51	27.37
C08	86	30.42	28.79	46	30.27	29.04	80	30.27	30.35	70	30.27	27.60
C09	39	26.51	27.75	34	26.48	28.39	38	26.57	31.50	36	26.51	27.44
C10	60	35.83	28.04	56	35.58	28.59	56	35.83	25.60	39	35.58	27.52

Sec：花費時間(單位：秒)

Stego PSNR：偽裝影像的 PSNR 值(單位：dB)

Secret PSNR：還原後機密影像的 PSNR 值(單位：dB)

表 2、實驗結果－靜態灰階影像（LBG，藏在最後 2 個位元）

	S01			S02			S03			S04		
	Sec	Stego PSNR	Secret PSNR	Sec	Stego PSNR	Secret PSNR	Sec	Stego PSNR	Secret PSNR	Sec	Stego PSNR	Secret PSNR
C01	50	25.72	25.95	49	25.74	27.41	50	25.65	29.21	50	25.77	26.33
C02	50	27.67	26.17	49	27.63	27.56	49	27.60	29.68	50	27.63	26.64
C03	49	25.34	26.39	52	25.25	27.37	50	25.25	30.07	49	25.31	26.57
C04	49	27.23	26.00	50	27.16	27.44	50	27.16	29.87	51	27.19	26.54
C05	52	24.98	25.84	50	25.01	27.30	50	25.01	30.00	50	24.98	26.33
C06	50	28.84	26.09	50	28.84	27.83	50	28.79	29.87	50	28.84	26.48
C07	49	31.23	26.39	50	31.06	27.67	50	31.06	30.00	51	31.14	26.60
C08	50	28.59	26.79	50	28.44	27.60	50	28.39	29.87	50	28.39	26.60
C09	51	25.20	26.42	50	25.13	27.63	50	25.09	30.20	51	25.16	26.64
C10	49	31.69	26.64	49	30.88	27.56	50	31.06	29.68	50	31.14	26.51

Sec：花費時間(單位：秒)

Stego PSNR：偽裝影像的 PSNR 值(單位：dB)

Secret PSNR：還原後機密影像的 PSNR 值(單位：dB)

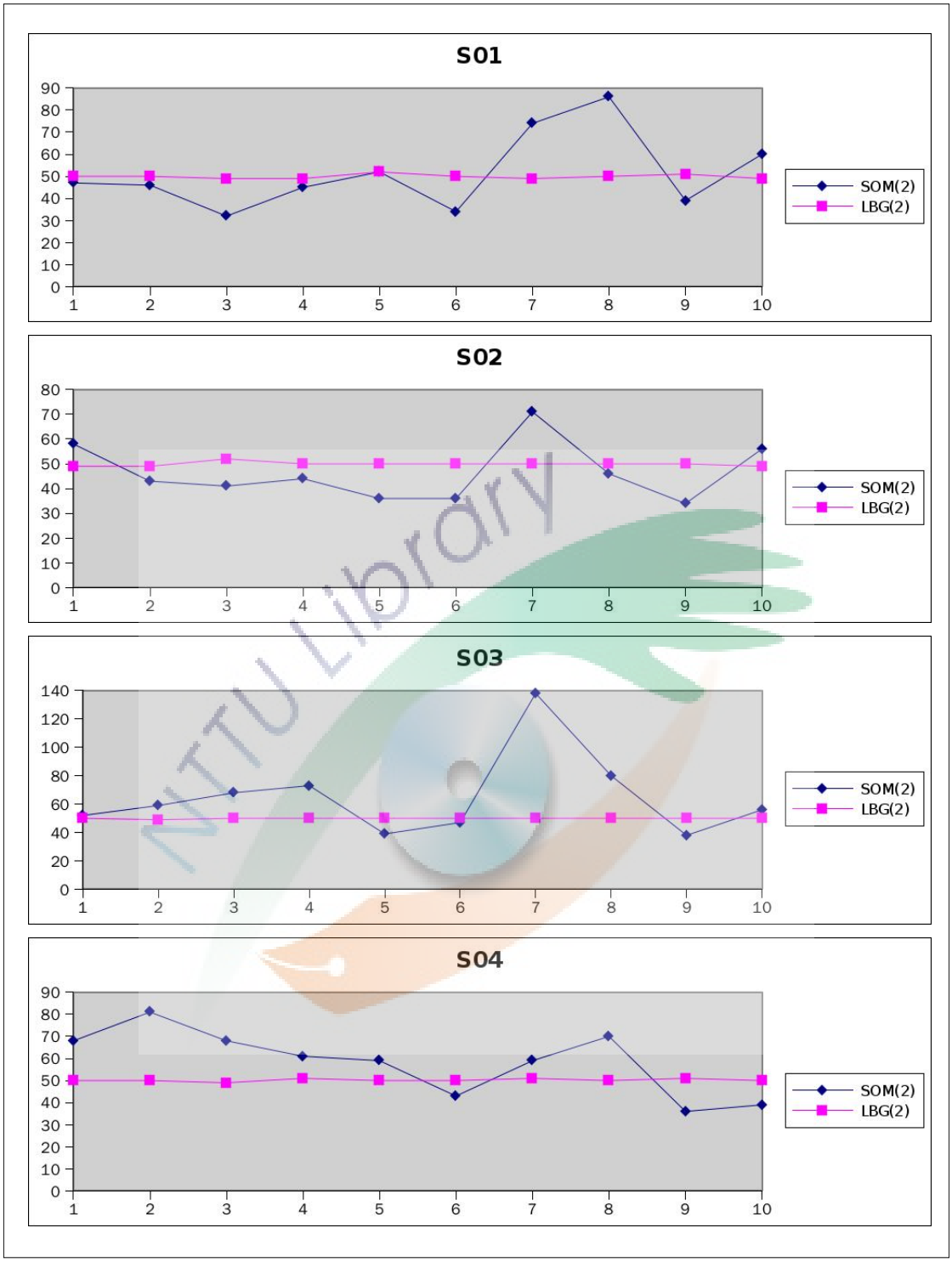


圖 18、花費時間的比較（機密影像）

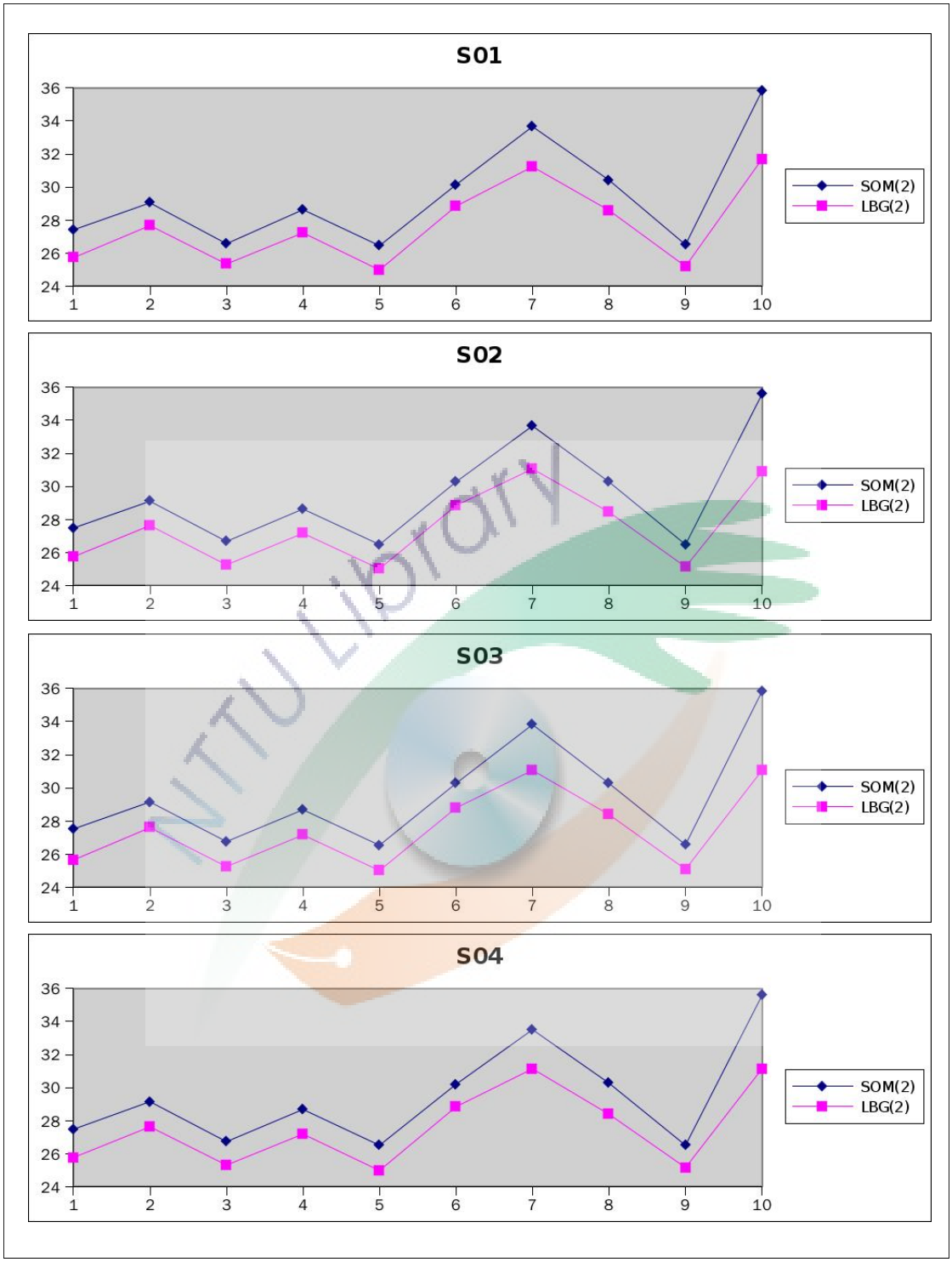


圖 19、偽裝影像的 PSNR 值比較

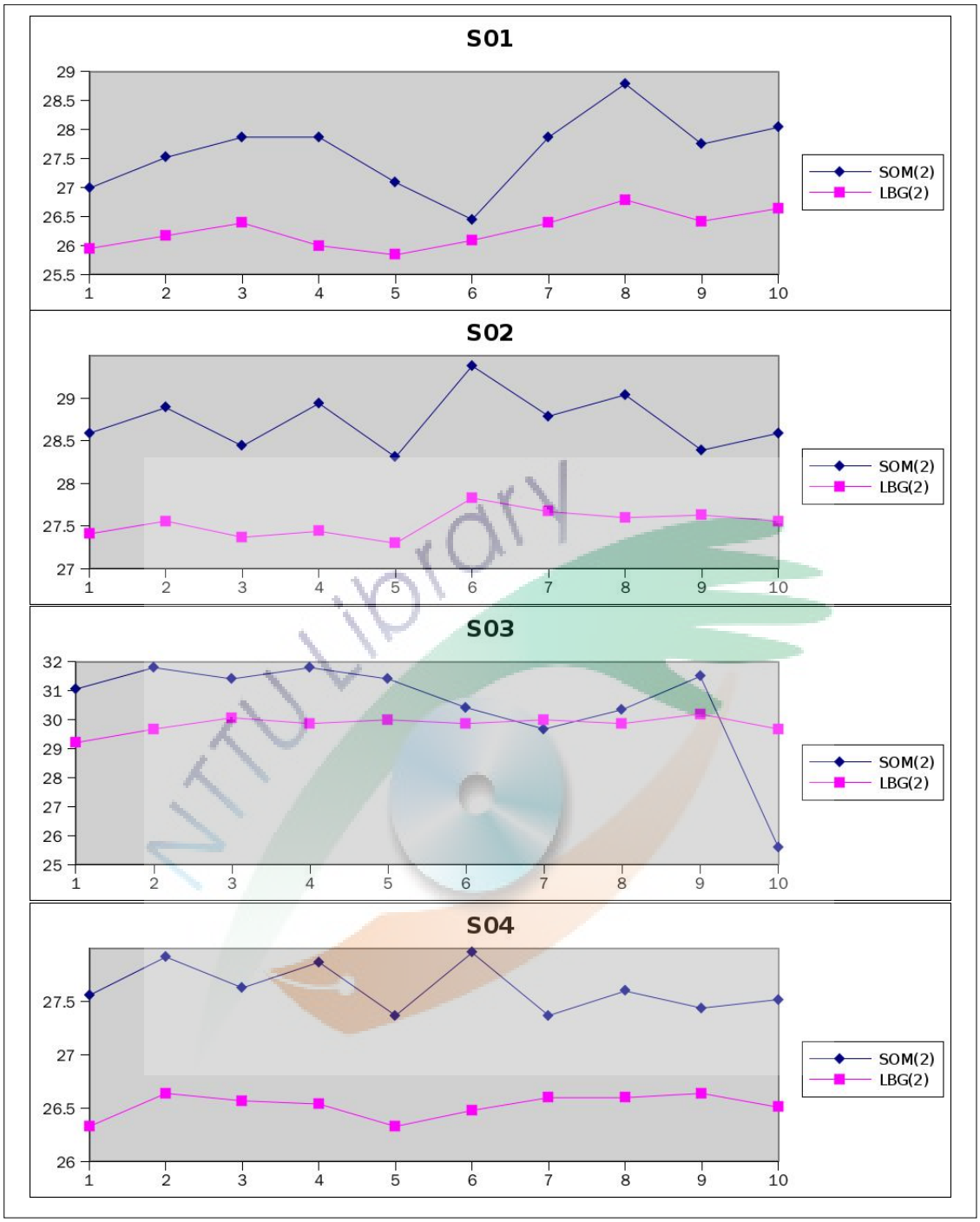


圖 20、還原後機密影像的 PSNR 值比較

第參節　實驗結果－機密 WAVE 聲音

實驗的設定條件如下：

1. 以圖 13 作爲掩護影像，大小皆爲 $512\times512(C_x\times C_y)$ 像素；
2. 以圖 15 作爲機密 WAVE 聲音，取樣頻率 8000HZ、取樣樣本大小 1 Byte、單音、長度爲 9 秒；
3. 切割成 $4\times4(m\times n)$ 像素的小區塊。；
4. 編碼簿大小 W 爲 256；
5. 藏在最後 $2(bitsize)$ 個位元。

依據上述的設定條件，整個實驗後的結果整理如表 3，LBG 演算法的結果整理如表 4。在花費時間（圖 21）上，大致上來說，LBG 演算法花費時間比本研究的演算法短，且 LBG 演算法的花費時間相當穩定。從僞裝影像品質（圖 22）來看，本研究提出的演算法則較 LBG 演算法好，然而還原後的 WAVE 聲音品質（圖 23），兩者則沒有較顯著的優劣之分，單純來看 C07、C08 和 C10 這三個掩護影像，本研究提出的演算法的還原機密 WAVE 聲音品質明顯較 LBG 演算法差。

表 3、實驗二結果－WAVE 聲音檔（SOM，藏在最後 2 個位元）

	W01			W02			W03		
	Sec	Stego PSNR	Secret PSNR	Sec	Stego PSNR	Secret PSNR	Sec	Stego PSNR	Secret PSNR
C01	42	27.44	35.58	76	27.44	33.22	45	27.33	23.38
C02	108	29.21	36.09	39	28.99	33.82	56	29.04	30.73
C03	93	26.76	35.12	50	26.64	33.36	44	26.64	30.81
C04	56	28.63	36.67	62	28.59	34.33	64	28.59	30.42
C05	67	26.54	34.91	189	26.54	32.45	60	26.48	29.80
C06	79	30.27	36.37	44	30.20	34.33	58	30.20	25.67

表 3（續）

C07	53	33.51	29.38	37	33.36	23.24	46	33.36	22.58
C08	54	30.20	36.37	57	30.14	26.14	88	30.20	21.99
C09	126	26.64	34.91	81	26.57	33.22	63	26.54	30.97
C10	79	35.58	25.90	67	35.58	21.49	49	35.34	24.68

Sec：花費時間(單位：秒)

Stego PSNR：偽裝影像的 PSNR 值(單位：dB)

Secret PSNR：還原後機密影像的 PSNR 值(單位：dB)

表 4、實驗二結果－WAVE 聲音檔（LBG，藏在最後 2 個位元）

	W01			W02			W03		
	Sec	Stego PSNR	Secret PSNR	Sec	Stego PSNR	Secret PSNR	Sec	Stego PSNR	Secret PSNR
C01	51	25.50	35.12	53	25.45	32.57	55	25.37	29.15
C02	51	27.44	35.58	51	27.37	33.08	54	27.37	28.84
C03	52	25.12	35.12	52	25.12	32.69	52	25.01	29.74
C04	51	26.99	35.58	51	26.92	33.08	54	26.99	29.74
C05	51	24.89	34.51	53	24.81	32.22	54	24.84	28.99
C06	51	28.63	36.09	52	28.63	33.36	55	28.59	29.87
C07	52	30.65	35.58	51	30.57	30.42	54	30.65	27.72
C08	51	28.22	35.83	52	28.13	31.80	54	28.13	28.84
C09	52	25.01	32.81	52	24.93	32.94	54	24.93	29.74
C10	52	30.50	33.98	56	30.27	29.56	54	30.57	27.44

Sec：花費時間(單位：秒)

Stego PSNR：偽裝影像的 PSNR 值(單位：dB)

Secret PSNR：還原後機密影像的 PSNR 值(單位：dB)

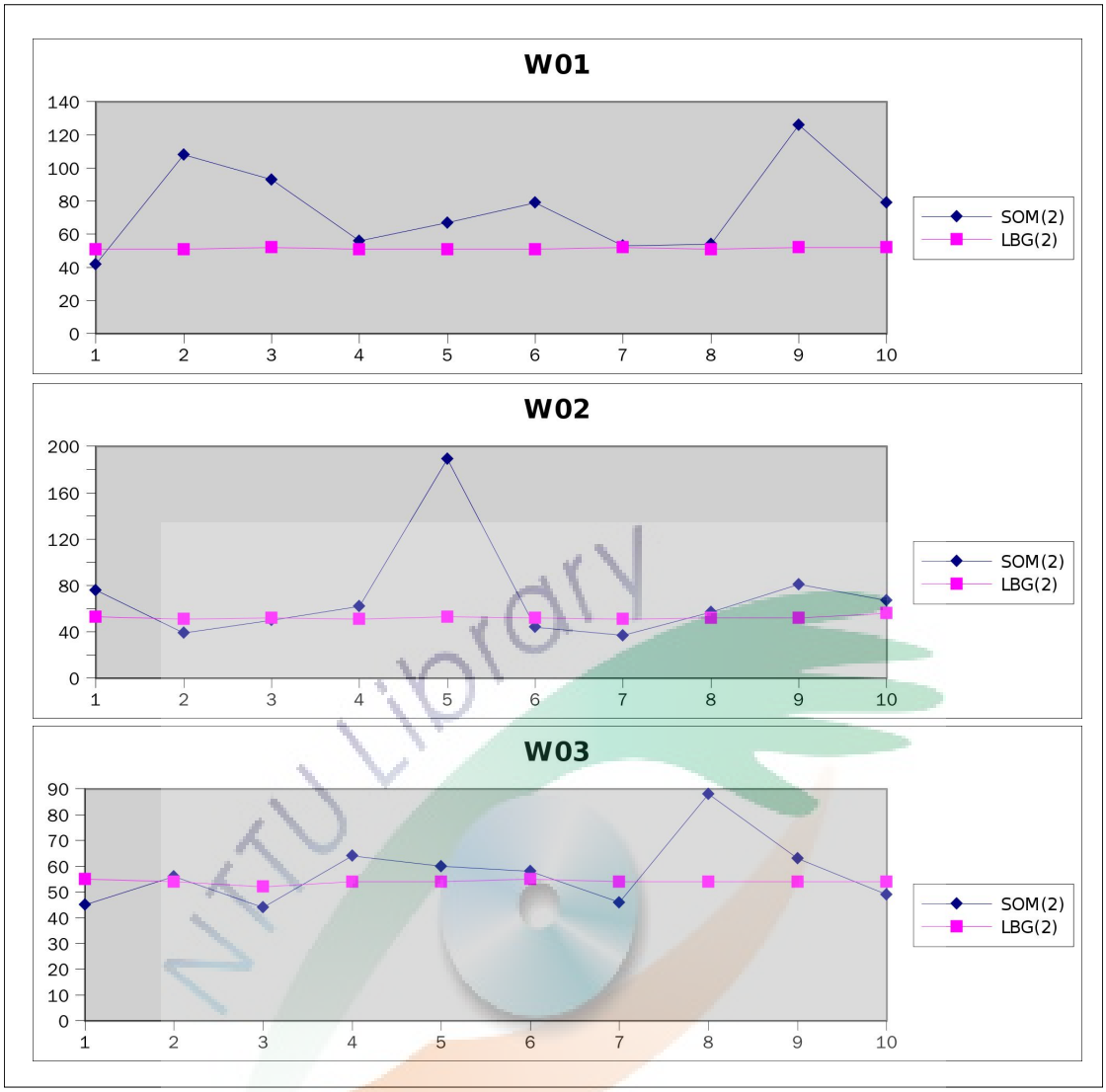


圖 21、花費時間的比較（機密 WAVE 聲音）

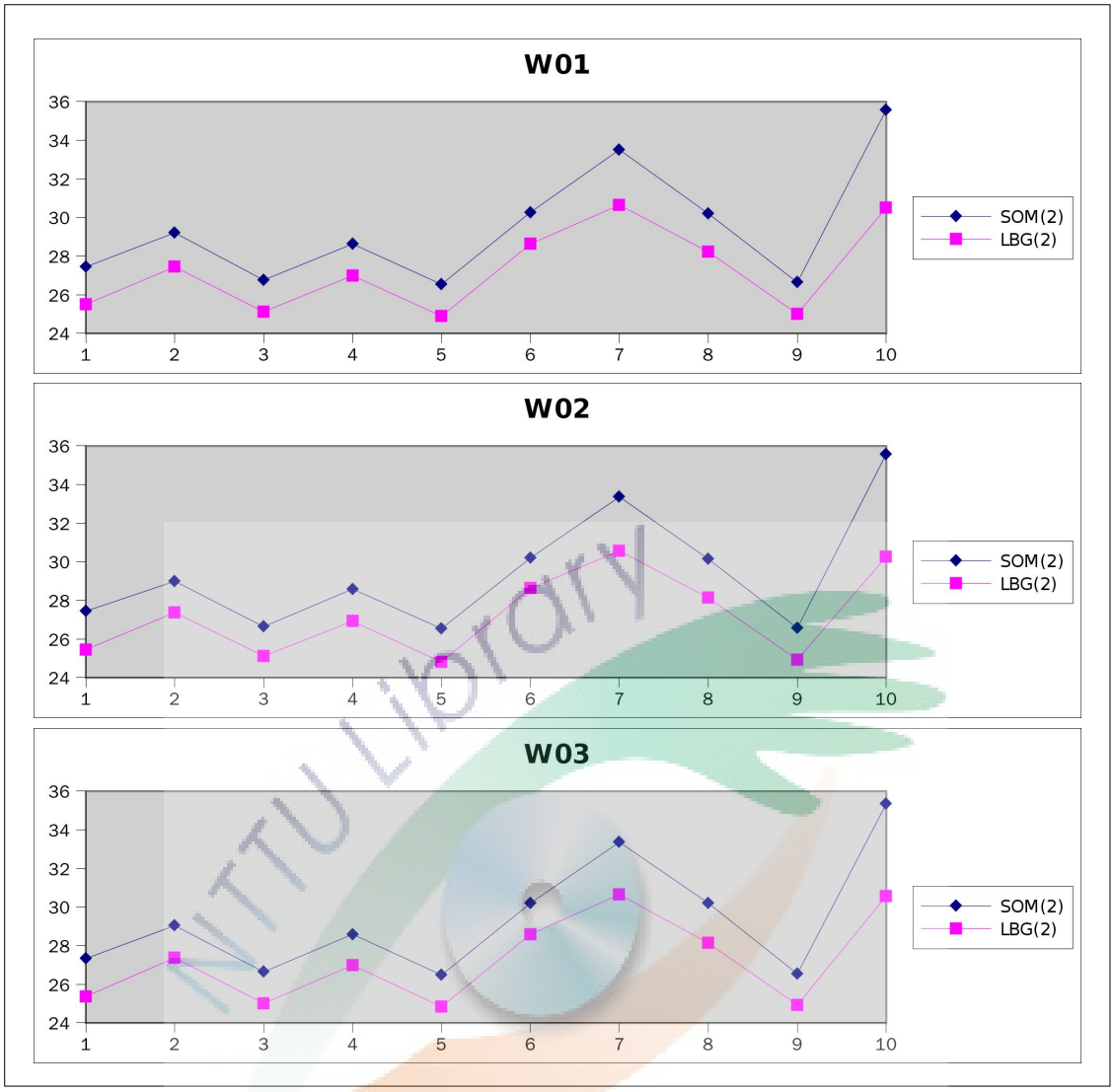


圖 22、偽裝影像 PSNR 值的比較

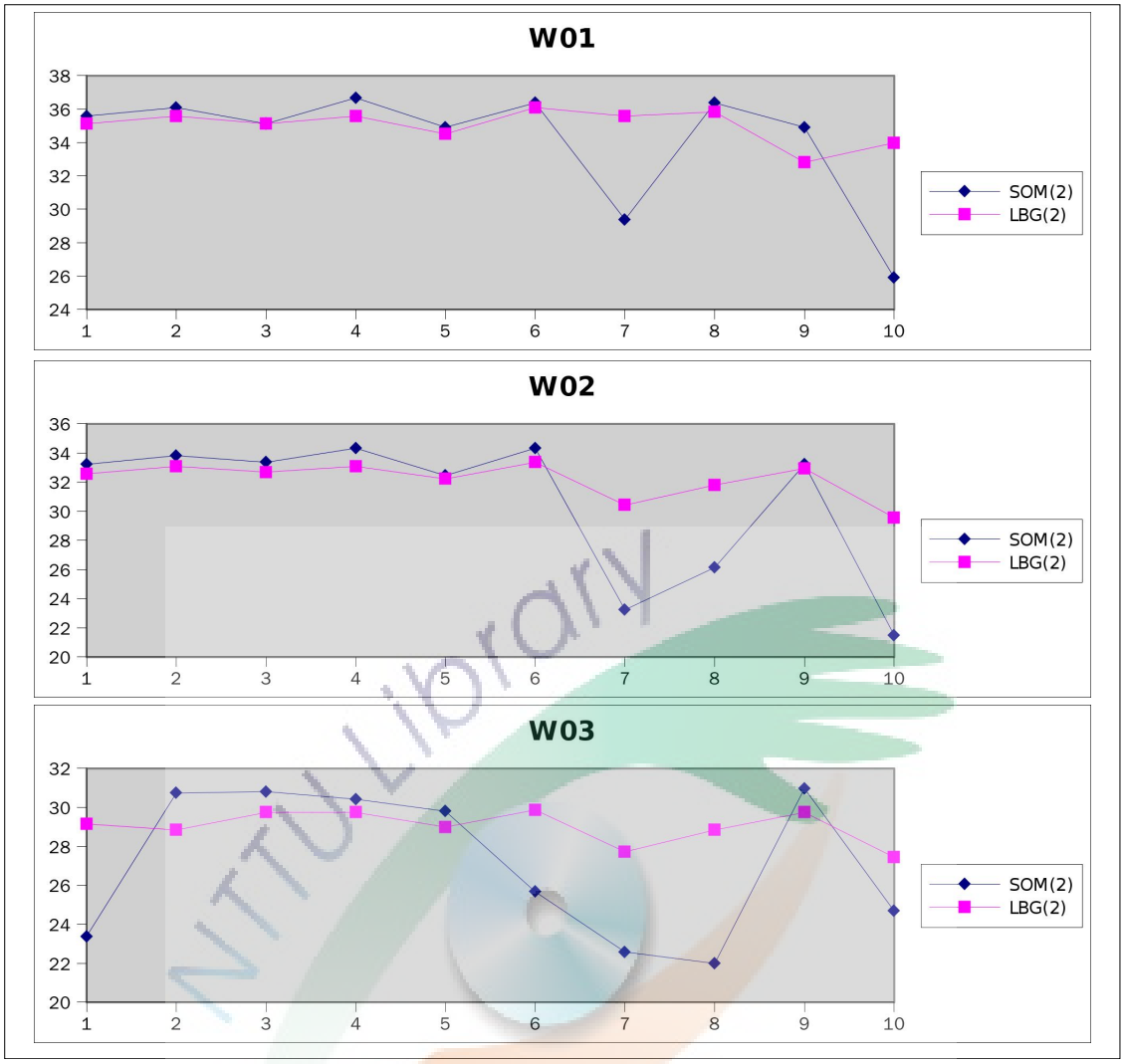


圖 23、還原後 WAVE 聲音 PSNR 值的比較

第肆節　結果討論

總體來看，不管本研究的演算法或是 LBG 演算法無法看出誰花費的時間較短、快速，不過 LBG 演算法的花費時間較穩定，不管是藏入機密影像或是機密 WAVE 聲音檔。從兩者的演算法本質來看，SOM 演算法的預測誤差會逐步回饋至演算法中，而 LBG 演算法是批次更新，應該是造成 LBG 演算法時間較短且較穩定的主因。再從偽裝影像的品質來看，本研究演算法則較 LBG 演算法好，值得注意

的是，不同的機密影像和機密 WAVE 聲音其僞裝影像的品質一致性相當高，可能是因爲掩護影像的大小比機密影像、機密 WAVE 聲音大的多，所以其訓練產生的僞裝影像品質較相似。最後從還原後機密影像品質來看，確實本研究的演算法較 LBG 演算法較好，而另一方面，在機密 WAVE 聲音的品質，無法直接斷言兩個演算法何者較好。

第伍章　結論與未來研究方向

本節將對整個結果做完整結論，並說明未來研究的可行方向。

第壹節　結論

本研究提出以 SOM 資料壓縮作爲基礎，分別以靜態影像與靜態影像、靜態影像與 WAVE 聲音檔作爲編碼簿的訓練向量，藉此顧及僞裝影像與還原後機密影像、聲音的品質，最後將編碼簿索引表、機密影像／聲音索引表與相關資訊透過 LSB 演算法藏入僞裝影像，使得接收者不需要原圖即可完整的萃取出機密影像、聲音，完整地達到資訊隱藏的目的。

本研究同時也在研究方法之後，說明了理論上可藏容量的極限大小，推導出可藏容量幾乎是接近掩護影像的大小，且從實驗結果來看，掩護影像和僞裝影像的品質也相當的好，而這點可有效降低人眼對僞裝影像的懷疑進而嘗試去解密的動機。還原後機密影像的品質整體來看都有不錯的表現，然而還原後 WAVE 聲音的品質有部份卻顯得不太理想。

從資訊隱藏的四個條件來看待整個結果，本研究的優點有：

1. 隱密性高，有效的降低對掩護影像的品質破壞，避免人眼直接觀察出有異而產生懷疑。
2. 可藏容量高，掩護影像可藏入的容量接近掩護影像大小。

而本研究的缺點如下：

1. 強韌性低，由於整個嵌入的過程是以 LSB 取代來實現，受到破壞易造成還原後品質不佳甚至無法還原。

2. 安全性低，不像過去學者使用私鑰來對藏入的資訊作加密，故造成安全性較弱。

未來可針對強韌性與安全性這兩方面做改善，可藉由 DES 加密來提高安全性。以其他嵌入方法來取代或改良 LSB 法，藉此提高其強韌性，例如不單純使用空間域的嵌入方式，可將影像像素值轉換成頻率域或其他轉換域的係數，再將訊息嵌入在係數中。

總結來看，本研究的高可藏容量解決了過去研究可藏容量不足的問題，有效提高了可藏機密訊息長度。且對於過去研究先以密碼學加密後再嵌入到掩護影像中，本研究則是專注在整個嵌入的過程，解決過去研究者忽略密碼學對本身演算法的影響，直接看待整個研究成果，且其結果從影像品質上也較過去使用向量量化的方法佳。

第貳節　未來研究方向

本研究提出的方法無可避免地會產生區塊效應（Blocking Effect），在未來研究中，可針對還原後的機密影像做其他過濾的處理動作，而此部份在本研究便沒有再更進一步的討論。

目前本研究僅針對灰階影像作實驗，對於彩色靜態影像亦可依此方法作基礎，用來藏匿機密訊息，相信會提高其可藏容量，以藏入更多的機密資料。而且本研究屬於失眞型資訊隱藏，未來亦可以此作爲無失眞資訊隱藏的雛型。

本研究是以掩護影像來藏入靜態影像與 WAVE 聲音檔，未來不僅可以嘗試藏入另一種數位媒體－動態影像（Video），更可推展至以聲音或是動態影像做爲掩護的媒體，分別藏入三種不同的數位媒體，擴展不同媒體間資訊隱藏的可行性。

參考文獻

Amerijckx, C., Velerysen, M., Thissen, P. & Legat, J.D.(1998). Image Compression by Self-Organized Kohonen Map. *IEEE Transactions on Neural Networks, 9*(3), 503-507.

Barbalho, J.M., Duarte, A., Neto, D., Costa, J.A.F., Netto, M.L.A(2001). Hierarchical SOM applied to image compression. *Proceedings of International Joint Conference on Neural Networks, 1*, 442-447.

Chang, C.C. & Wu, W.C.(2005). A steganographic method for hiding secret data using side match vector quantization. *IEICE - Transactions on Information and Systems, E88-D*(9), 2159-2167.

Chang, C.C., Tai, W.L. & Lin, C.C.(2006). A Reversible Data Hiding Scheme Based on Side Match Vector Quantization. *IEEE Transactions on Circuits and Systems for Video Technology, 16*(10), 1301-1308.

Chen, T. S., Chang, C. C. & Hwang, M. S.(1998). A virtual image cryptosystem based upon vector quantization. *IEEE Transactions on Image Processing, 7*(10), 1485-1488.

Gersho A. & Gray R.M.(1991). *Vector Quantization and Signal Compression.* Boston, MA, USA: Kluwer.

Gruhl, D., Lu, A. Lu & Bender, A.(1996). *Echo Hiding.* In Proceedings of Information Hiding Workshop, University of Cambridge.

Hu, Y. C.(2003). Grey-level image hiding scheme based on vector quantization. *IEE Electronics Letters, 39*(2), 202-203.

Huang, H.C., Chu, S.C. & Huang, Y.H.(2006). VQ-Based Watermarking Techniques. *Journal of Computers, 17*(2), 37-50.

Huang, D.Y. & Yeo, T.Y.(2002). *Robust and Inaudible Multi-echo Audio Watermarking.* Paper presented at Proceedings of the Third IEEE Pacific Rim Conference on Multimedia: Advances in Multimedia information Processing, London, UK.

Jo, M. & Kim, H.D.(2002). A digital image watermarking scheme based on vector quantization. *IEICE Transactions on Information and System, E85-D*(6), 1054—1056.

Kohonen, T.(2001). *Self-Organizing Maps.* (3rd ed.). New York: Springer-Verlag.

Lin, E.T. & Delp, E.J.(1999). A review of data hiding in digital images. *Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference, PICS'99,* 274-278.

Marvel, L.M., Retter, C.T. & Boncelet, C.G., Jr.(1998). *Hiding information in images.* Paper presented at Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference, Chicago, IL, USA.

Oh, H.O., Seok, J.W., Hong, J.W. & Youn, D.H.(2001). New Echo Embedding Technique for Robust and Imperceptible Audio Watermarking. *Proceedings of the International Conference on Acoustic, Speech and Signal Processing,* 3, 1341-1344.

Petitcolas, F., Anderson, R., Kuhn, M.(1999). Information hiding-a survey. *Proceedings of the IEEE, 87*(7), 1062-1078.

Riskin, E.A., Atlas, L.E. & Lay, S.R.(1991). *Ordered neural maps and their applications to data compression.* Paper presented at

Proceedings of the 1991 IEEE Workshop, Princeton, NJ, USA.

Mohanty, S.P.(1999), *Digital Watermarking : A Tutorial Review*. http://www.csee.usf.edu/~smohanty/research/Reports/WMSurvey1999Mohanty.pdf

Tilki, J. F. and A. A. Beex(1997, April). *Encoding a Hidden Auxiliary Channel onto a Digital Audio Signal Using Psychoacoustic Masking.* Proceedings of the IEEE South East Conference, Blacksburg, Virginia.

Zhou, L.N.,, Liu, C.Q., Ping, X.J., Zhang, T. & Wang, Y.H.(2006). *Information Hiding Method in Digital Audio Signal Based on Perfect Codes.* Paper presented at Intelligent Information Hiding and Multimedia Signal Processing, Pasadena, CA, USA.

王和發（2004）。**精鍊VQ灰階影像壓縮法與低失眞彩色影像壓縮法**。朝陽科技大學資訊管理系碩士班碩士論文，未出版，台中。

王旭正、陳宏和、林庭宇（2007）。**網路傳輸之視覺僞裝機制研究**。台灣大學：TANET2007 臺灣網際網路研討會。

李秀月（2002）。**影像壓縮技術爲基礎之資訊隱藏研究**。屏東科技大學資訊管理系碩士論文，未出版，屏東。

林信鋒（2005）。**影像資訊隱藏技術之研究**。國立東華大學資訊工程學系博士論文，未出版，花蓮。

施奕安（2006）。**以線性區塊編碼提高音訊浮水印之強健性**。國立中央大學電機工程研究所碩士論文，未出版，桃園。

詹啓祥（2005）。**影像僞裝術與數位浮水印之研究**。國立中正大學資訊工程所博士論文，未出版，嘉義。

戴顯權（2002）。**資料壓縮**（2版）。高雄：紳藍。

附錄一

- C01：掩護影像
- S01～S04：機密影像
- St01-S01：偽裝影像，C01 嵌入 S01
- St01-S02：偽裝影像，C01 嵌入 S02
- St01-S03：偽裝影像，C01 嵌入 S03
- St01-S04：偽裝影像，C01 嵌入 S04

C01

St01-S01

St01-S02

St01-S03

St01-04

- C02：掩護影像
- S01～S04：機密影像
- St02-S01：偽裝影像，C02 嵌入 S01
- St02-S02：偽裝影像，C02 嵌入 S02
- St02-S03：偽裝影像，C02 嵌入 S03
- St02-S04：偽裝影像，C02 嵌入 S04

C02

St02-S01

St02-S02

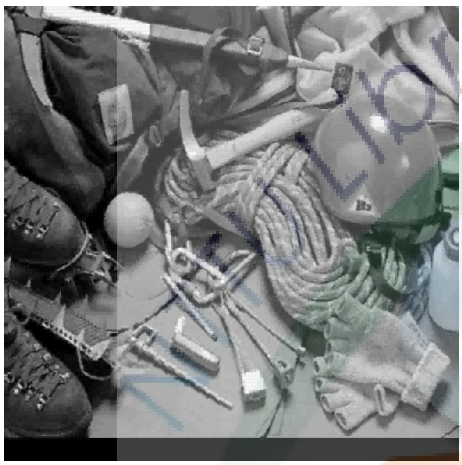
St02-S03

St03-S04

- C03：掩護影像
- S01～S04：機密影像
- St03-S01：偽裝影像，C03 嵌入 S01
- St03-S02：偽裝影像，C03 嵌入 S02
- St03-S03：偽裝影像，C03 嵌入 S03
- St03-S04：偽裝影像，C03 嵌入 S04

C03

St03-S01



St03-S02

St03-S03

St03-S04

- C04：掩護影像
- S01～S04：機密影像
- St04-S01：偽裝影像，C04 嵌入 S01
- St04-S02：偽裝影像，C04 嵌入 S02
- St04-S03：偽裝影像，C04 嵌入 S03
- St04-S04：偽裝影像，C04 嵌入 S04

C04

St04-S01

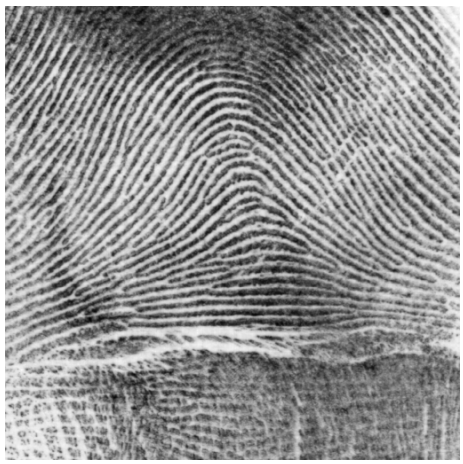
St04-S02

St04-S03

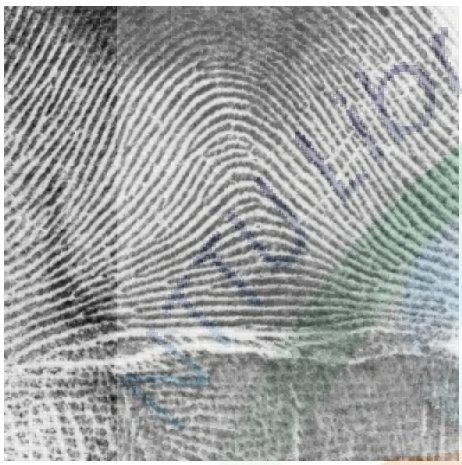
St04-S04

- C05：掩護影像
- S01～S04：機密影像
- St05-S01：偽裝影像，C05 嵌入 S01
- St05-S02：偽裝影像，C05 嵌入 S02
- St05-S03：偽裝影像，C05 嵌入 S03
- St05-S04：偽裝影像，C05 嵌入 S04

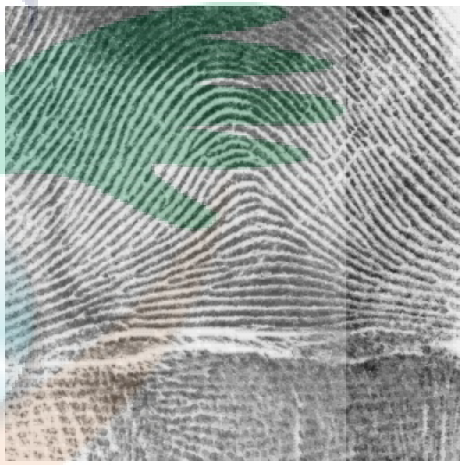
C05



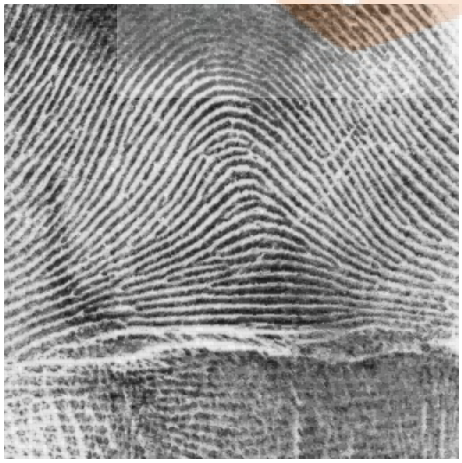
St05-S01



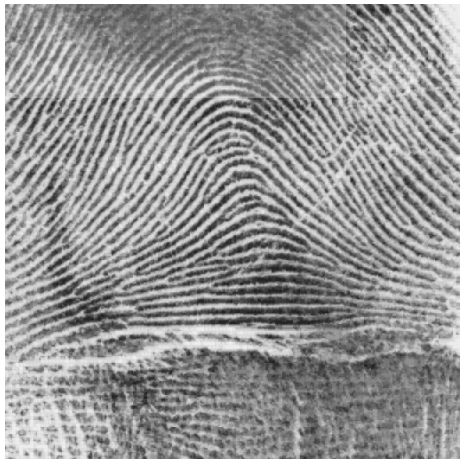
St05-S02



St05-S03



St05-S04



- C06：掩護影像
- S01～S04：機密影像
- St06-S01：偽裝影像，C06 嵌入 S01
- St06-S02：偽裝影像，C06 嵌入 S02
- St06-S03：偽裝影像，C06 嵌入 S03
- St06-S04：偽裝影像，C06 嵌入 S04

C06

St06-S01

St06-S02

St06-S03

St06-S04

- C07：掩護影像
- S01～S04：機密影像
- St07-S01：偽裝影像，C07 嵌入 S01
- St07-S02：偽裝影像，C07 嵌入 S02
- St07-S03：偽裝影像，C07 嵌入 S03
- St07-S04：偽裝影像，C07 嵌入 S04

C07

St07-S01

St07-S02

St07-S03

St07-S04

- C08：掩護影像
- S01～S04：機密影像
- St08-S01：偽裝影像，C08 嵌入 S01
- St08-S02：偽裝影像，C08 嵌入 S02
- St08-S03：偽裝影像，C08 嵌入 S03
- St08-S04：偽裝影像，C08 嵌入 S04

C08

St08-S01

St08-S02

St08-S03

St08-S04

- C09：掩護影像
- S01～S04：機密影像
- St09-S01：偽裝影像，C09 嵌入 S01
- St09-S02：偽裝影像，C09 嵌入 S02
- St09-S03：偽裝影像，C09 嵌入 S03
- St09-S04：偽裝影像，C09 嵌入 S04

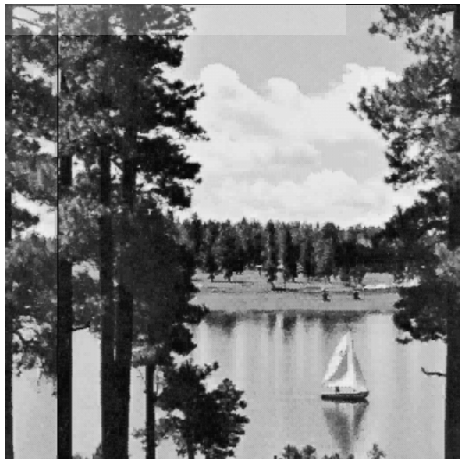
C09

St09-S01

St09-S02

St09-S03

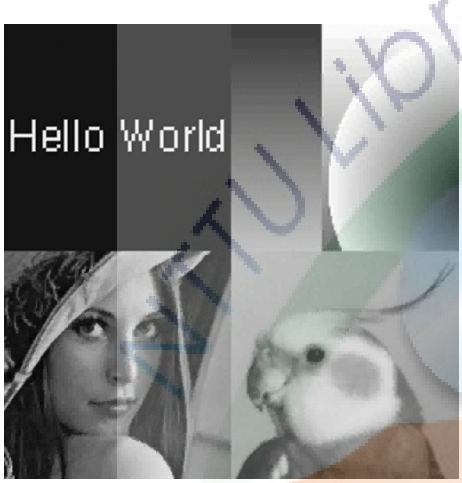
St09-S04



- C10：掩護影像
- S01～S04：機密影像
- St10-S01：偽裝影像，C10 嵌入 S01
- St10-S02：偽裝影像，C10 嵌入 S02
- St10-S03：偽裝影像，C10 嵌入 S03
- St10-S04：偽裝影像，C10 嵌入 S04

C10

St10-S01



St10-S02

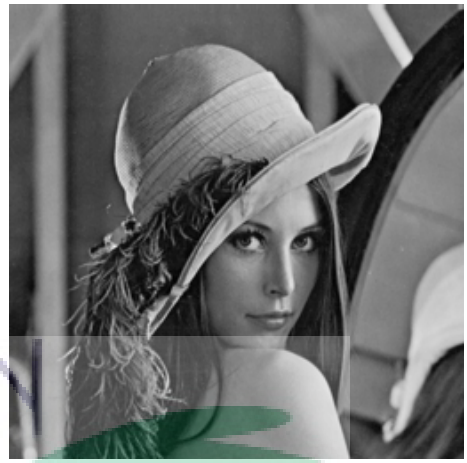
St10-S03

St10-S04

附錄二

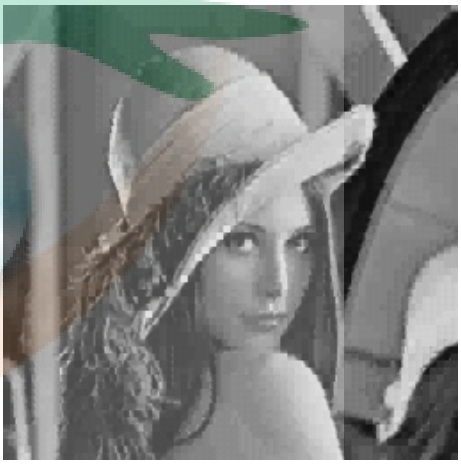
- S01：機密影像
- St01~St10：偽裝影像
- R01-St01：從 St01 還原出 S01
- R01-St02：從 St02 還原出 S01
- 其餘類推

S01



R01-St01

R01-St02



R01-St03

R01-St04

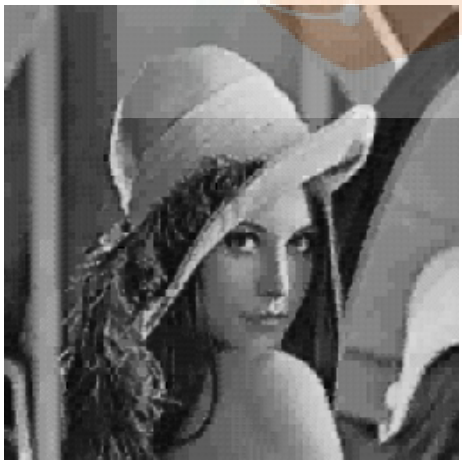
R01-St05

R01-St06

R01-St07

R01-St08

R01-St09



R01-St10

- S02：機密影像
- St01~St10：偽裝影像
- R02-St01：從 St01 還原出 S02
- R02-St02：從 St02 還原出 S02
- 其餘類推

S02

R02-St01

R02-St02

R02-St03

R02-St04

R02-St05

R02-St06

R02-St07

R02-St08

R02-St09

R02-St10

- S03：機密影像
- St01~St10：偽裝影像
- R03-St01：從 St01 還原出 S03
- R03-St02：從 St02 還原出 S03
- 其餘類推

S03

R03-St01

R03-St02

R03-St03

R03-St04

R03-St05

R03-St06

R03-St07

R03-St08

R03-St09

R03-St10

- S04：機密影像
- St01~St10：偽裝影像
- R04-St01：從 St01 還原出 S04
- R04-St02：從 St02 還原出 S04
- 其餘類推

S04

R04-St01

R04-St02

R04-St03

R04-St04

R04-St05

R04-St06

R04-St07

R04-St08

R04-St09

R04-St10