國立勤益科技大學
研發科技與資訊管理研究所

碩士論文

高容量可逆式影像資訊隱藏技術之研究

A Study of High Capacity and Reversible Image Information Hiding Schemes

指 導 教 授 ： 王清德 博士

研 究 生 ： 李林軍

中華民國 一〇一 年 六 月

國立勤益科技大學

研究所碩士班

論文口試委員會審定書

本校 研發科技與資訊管理研究所碩士班 李林軍 君
所提論文 高容量可逆式影像資訊隱藏技術之研究
合於碩士資格水準，業經本委員會評審認可。

論文口試委員會：

召 集 人：詹寶竜

委　　員：王清材

王清德

詹寶竜

指導教授：王清德

所　　長：[illegible]

中　華　民　國　一　〇　一　年　六　月

國 立 勤 益 科 技 大 學

博碩士論文全文上網授權書

（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勤益科技大學研發科技與資訊管理研究所資訊管理組 100 學年度第二學期取得碩士學位之論文。

論文題目：高容量可逆式影像資訊隱藏技術之研究
指導教授：王清德

■ 同意

本人具有著作權之論文全文資料，非專屬、無償授予本人畢業學校圖書館，不限地域、時間與次數，以微縮、光碟或數位化等各種方式重製與利用，提供讀者基於著作權法合理使用範圍內之線上檢索、閱覽、下載及列印。

論文全文上網公開之範圍及時間：

論文全文上網公開之範圍及時間：載路	
校內區域網路	■ 中華民國 102 年 6 月 19 日公開
校外網際網路	■ 中華民國 102 年 6 月 19 日公開

授 權 人：李林軍
簽　　名：李林軍
中　華　民　國 101 年 6 月 19 日

國家圖書館
博碩士論文電子檔案上網授權書

本授權書所授權之論文爲授權人在國立勤益科技大學研發科技與資訊管理研究所 100 學年度第二學期取得碩士學位之論文。

論文題目：高容量可逆式影像資訊隱藏技術之研究
指導教授：王清德

茲同意將授權人擁有著作權之上列論文全文(含摘要)，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，此項授權係非專屬、無償授權國家圖書館及本人畢業學校之圖書館，不限地域、時間與次數，以微縮、光碟或數位化方式將上列論文進行重製，並同意公開傳輸數位檔案。

☐ 立即開放

☐ 上列論文爲授權人向經濟部智慧財產局申請專利之附件或相關文件之一（專利申請案號：　　），請於 2013 年 6 月 19 日 後再將上列論文公開或上載網路。

☑ 因上列論文尚未正式對外發表，請於 2013 年 6 月 19 日 後再將上列論文公開或上載網路。

☐ 其他

授權人：李林軍

親筆簽名及蓋章：李林軍　　**民國**101**年**6**月**
日

E-Mail：kkkkk8310@yahoo.com.tw

高容量可逆式影像資訊隱藏技術之研究

中文摘要

近年來數位影像資料在網路上傳輸日益頻繁，影像資訊安全益顯重要，影像資料隱藏為保護數位多媒體智慧創作權的重要技術，然而，在此類相關研究中，考慮機密資訊安全性固然重要，但如何提升藏密容量又不失去影像品質成為研究重點。空間域資訊隱藏中利用統計直方圖修改技術隱藏機密資訊方法已成趨勢，此類領域常受到直方圖峰點頻率不高的限制，導致可藏空間降低。因此，本研究將提出植基於鄰近像素預測方式產生差值直方圖(Difference Histogram)之可逆性資料隱藏技術。首先，利用二階段鄰近像素與區塊預測技術，盡可能善用影像每一像素產生可藏匿空間，第一階段使用中位數、平均數與鄰近像素計算預測差值，統計成第一差值直方圖，而第二階段則使用反向 S 型預測方式，統計成第二差值直方圖，使用兩個直方圖之二對峰點資訊作為隱藏容量並可調式嵌入容量，將機密浮水印嵌入於影像中。更進一步，欲提升更大隱藏容量，本研究應用區塊眾數預測方法，由於眾數像素在鄰近範圍內具有高度像素相似性，因此將每一區塊眾數當作預測值，之後計算差值並產出差值直方圖，眾數像素預測準確高代表差值集中於零，也就是可藏容量有效提升。此外，本研究也設計新的方法以動態矩陣藏入機密資訊，利用兩個亂數產生動態矩陣，並將影像餘數配合動態矩陣為基礎進行資訊隱藏，藏匿時，四個像素為一組可嵌入兩個九進位浮水印資訊，比傳統 LSB 隱藏技術容量更為提高，在影像承載機密資訊量大幅提升。本研究之資訊隱藏方法每個像素最多僅調整一個單位，在偽裝影像可以達成優良的品質，不僅如此，本論文所設計的方法皆為可逆式資訊隱藏，偽裝影像萃取機密資訊後，無需利用原始影像資訊尚可回朔成最原始影像，經實驗與文獻比較，直方圖修改與動態矩陣資訊隱藏技術，不僅具有高負載容量及高影像品質外，而且具有影像可逆性的特點。

關鍵字：可逆式資料隱藏、直方圖、預測差值、動態矩陣。

高容量可逆式影像資訊隱藏技術之研究

英文摘要

The data communication is becoming more and more rapidly and conveniently due to the information technology and Internet expeditious development. Therefore, the protections of information security and integrity are becoming very important in the network transmission. The data hiding schemes and the embedding security are needed to consider in the image research, but how to enhance embedding capacity without losing image quality is become priority research centers. Spatial domain information hiding using histogram modification techniques to hide secret has become trend, but the lower embedding capacity often subject to the histogram peak point frequency restriction. For this reason, we will propose reversible data hiding techniques based on the neighboring pixels prediction method that using two levels prediction makes the pixels effective exploitation. In the first phase, we use the neighbor pixels, median and mean values to evaluate the prediction difference and compute the difference histogram of the image. The second phase uses an inverse S form to scan image and compute the prediction difference that can generate the second difference histogram. By the use of two histograms, the system generates two pairs of peak point, which can be used to embed the watermark and adjust the hiding capacity. Furthermore, we promote a greater hiding capacity that using pixel frequency of block as prediction data hiding technique. This method explores the frequency of pixels in each block and uses them as the predictive values. Because the neighboring pixels of blocks have the similar characteristics and the differences of prediction pixels are approximately that the hiding capacity can effectively increase. Furthermore, our study will propose the new data hiding technique that design a dynamic matrix to embed secret information. We use two random numbers to generate a dynamic matrix, and the remainder of pixels match with matrix to embed the information. In the hiding process, we use four pixels as one group to embed two of novenary system data, and the capacity is higher than LSB hiding technique. Thus, the proposed data hiding techniques can increase the image carrying data capacity. In this study, each pixel in the image only adjusts one unit, and the stego-image can attain to excellent quality. Moreover, our data hiding techniques are always the reversible data hiding, the stego-image is extracted information without use the original image information, and can still be reversed to the original image. From the experimental results, the histogram modification techniques and the dynamic matrix data hiding schemes not only have high capacity and good PSNR values of image quality, but also have reversible characteristics of data hiding.

Keywords: Reversible data hiding, Histogram, Prediction difference, Dynamic matrix.

致謝

隨著碩士論文口試的結束，代表兩年來的研究所求學生涯即將告一段落，回憶起過去同學在研究室學術上討論及分享生活的點滴彷彿歷歷在目但已不復在。本論文辛苦完成的背後，首先要誠摯地感謝王清德博士擔任我的指導教授，要不是有您的提攜與栽培，學生我也不會取得論文口試資格，甚至不可能取得碩士學位，所有的過程都承蒙老師的鼓勵與賞識，有老師的細心指導，使我在研究能夠得心應手，研究成果能夠更上層樓，求學與問題解決的心態也能成長許多，在此向王老師致上最真誠的謝意。此外，求學的過程中，遇到了許多研發科技與資訊管理所老師們對我的諄諄教誨，感謝老師在課程中思辨與討論的醍醐灌頂，成就了學生更高深的學問邁進。論文口試得以進行順利完成，特別要感謝口試委員詹永寬老師以及王清林老師，因為有你們的寶貴意見，使本論文能夠更加完整且嚴謹。

另外感謝研發科技與資訊管理研究所的同學，感謝小孟、小郭、加樂、士哲、凱崴、建志、智鴻、冠誌、瑞元、文傑、士田與淳葶在課業與生活與到迷惘時，總能為我及時解惑，還有許多未提及的研究室的夥伴們，有你們陪伴的研究生涯中，讓我在論文的寫作不在孤單。再者，感謝助教、技佐與學弟妹們，有你們的鼓勵與協助，讓我的學業有關的事物得以順利進行，謝謝你們點綴的我在研究過程中的絢麗的色彩。

最後，我要感謝最摯愛的雙親支持我念研究所，在我失意時他們給我最最最大的溫暖，有了他們的支持鼓勵與包容讓我順利渡過求學階段，飲水思源溢於言表，謹以此文獻給摯愛的家人。

李林軍 謹致

目錄

圖目錄

表目錄

第一章 緒論

近年來，資料的數位化與網路的普及化，人們利用網際網路分享多媒體資訊變得更為便利與快速，也解除了時間與空間的限制。在傳輸過程中，數位資訊容易被複製與傳播充斥著不安全性，加上隱私權的思維高漲，為了保護智慧財產權(Intellectual Property Rights, IPR)，資訊安全議題逐漸受到重視，因此衍生出資訊多媒體智慧財產權安全問題。目前多媒體保護方式大多利用密碼學(Cryptography)的加密(Encoding)技術[1]與資料隱藏(Data hiding)技術，例如在影像、音樂與影片等多媒體中嵌入版權資訊等[27]，以防止非法人士盜取或竄改影響到原創作者的權益。因此，為維護影像智慧財產權，將版權或機密資訊完整嵌入到原始影像中(Original Image)，不讓有心人士察覺，以保護訊息安全，影像隱藏技術具有其重要性，並有深入研究之必要性。

1.1 研究背景

數位時代的來臨，人們可以經由網路傳遞多媒體資訊，若要傳送重要的機密文件或避免訊息外洩，其資訊安全為重要的考量，過去資訊傳輸常使用加密技術如 RSA 與 DES 技術[4]來確保資訊的安全，此技術是將重要的祕密訊息利用加密產生密文，而密文為雜亂無章看起來無意義的亂碼，除了擁有秘密金鑰的人解的開，其餘人士無法解讀該機密訊息，但加密技術並無遮蔽媒體保護，因此易被察覺文件內容有異常，攻擊者會試圖阻擋並且破解及破壞密文，導致接收方無法得到完整正確的訊息，因此，網路安全與資訊安全領域的專家學者提出資訊隱藏技術，資訊隱藏概念就是在公開的場合下不易被第三方發現傳送資料中含有重要的訊息，為保護傳遞訊息安全與隱密性，將機密資訊隱藏於數位媒體而不被偵測出的藝術[29]。數位影像資訊隱藏技術方面著重於將機密資訊或浮水印藏匿於負載影

像(Cover image)中，使得影像在網路傳遞時，人類視覺無法察覺影像中帶有秘密訊息的存在避免有心人士破壞的機會，這也使重要資訊可以安全的傳送達成密密通訊的目的。隱藏資訊最簡單的方式就是最低位元取代法 LSB(Least-significant bit) [20][26]，影像之像素用二進制 8 bits 表示，將機密資訊藏入像素於較後面不重要的位元，而像素變化性不大，當機密資訊藏入後產生的偽裝影像(Stego-image)不易被察覺有隱藏資訊，最低位元嵌入技術為簡易實作的資訊隱藏技術。目前，大多數的影像隱藏技術會稍微改變原始影像像素，導致偽裝圖像與原始影像有稍許不同，若影像還有其他用途所在，隱藏方式可以設計成嵌入與擷取演算法相融方式，換句話說，當機密資訊取出後，仍可恢復至原始狀態影像，即為無失真(Lossless)或可逆式資訊隱藏技術(Reversible data hiding techniques)[19][24][34]。反之，有些多媒體在網路傳輸時考慮速度問題而利用壓縮方式解決，一旦影像藉由壓縮所還原後的影像都會產生失真的情況，如 JPEG 就為影像失真壓縮格式[18]，顧名思義，若影像壓縮後的擷取演算法沒有能力恢復回失真的像素，即是失真性(Lossy) [31]隱藏演算法。

可逆式影像隱藏技術為兼顧資訊隱藏與原始影像保存目的之研究，隱藏技術將機密資訊藏入至原始影像中，藏入後的偽裝影像讓人類視覺觀看不出有任何變化，達成不可察覺的特性，當機密資訊取出後又可將偽裝影像恢復成原始影像，這類研究不希望因藏入機密資訊導致影像的破壞，在需高精確度、無容許誤差性、避免專業誤判等領域中具有應用價值，如醫學領域中，病人私密資訊嵌入影像以保護病患隱私，取出資料後此影像還可做醫療診斷；在軍事領域中，可將機密訊息放在影像中傳遞當作軍事通信橋梁，取出機密後影像有更進一步的戰略用途等。目前，可逆式影像隱藏技術在處理上一般可分為空間域、頻率域與壓縮域三種方式[2]。空間域的隱藏技術為將原始像素直接進行寫入動作，像素不需經由任何的轉換流程，常見的有差值擴張(Difference Expansion, DE)[6][16][21][32]利用相

鄰像素之間進行差值的擴張，然後將機密資訊藏匿於擴張後差值之最後一位元，另外，直方圖修改技術[17][27][36][38][42]為影像之像素統計產生的直方圖，對直方圖中的像素值做修改，達到隱藏效果，這兩類都屬於空間域隱藏技術。頻率域的嵌入技術係利用離散餘弦轉換(Discrete Cosine Transformation, DCT)[5][8][41]或離散小波轉換(Discrete Wavelet Transformation, DWT)[13][14]，將機密資訊藏入於轉換之後的頻率係數中。在壓縮域的嵌入技術以向量量化(Vector Quantization, VQ)[7][9][25][35]透過壓縮編碼，將產出的編碼簿進行分群並隱藏機密資訊。

1.2 研究動機

現今，可逆式資訊隱藏在影像處理已經成為研究重點，在流程設計上較不可逆資訊隱藏演算法繁複，如直方圖隱藏技術中的還原資訊峰值需經由計算且要紀錄，由於影像還原後還可做為特定領域之用途，應用上也較有彈性，因此本研究將針對影像可逆式資訊藏匿作深入探討，並設計與改進影像可逆式資訊隱藏技術。一般而言，可逆式影像隱藏技術在頻率域與壓縮域需要進行轉換流程，該流程需要大量計算，然而資訊嵌入實作就略顯繁複，且頻率域藏匿資訊在低頻會嚴重破壞影像，高頻又容易被攻擊，中頻為最佳藏匿點，單憑中頻當作藏匿點，影像負載量自然會低，而在空間域利用差值擴張法隱藏，影像像素要進行差值擴張，擴張後的像素與原始影像像素差異性大，影像品質也會較差。因此本研究將探討以直方圖修改的資訊隱藏技術，使用空間域技術在資訊隱藏運算複雜度上會較頻率域與壓縮域低，因為只修改原始像素且不需轉換流程，在藏入機密資訊容量方面會較頻率域大，藏入時只修改像素正負一個單位即可藏入資訊，影像品質也較差值擴張提升，因此本研究將以直方圖修改可逆式隱藏技術作為設計重點。然而另一運用修改方向 EMD (Exploiting Modification Direction, EMD)[3]資訊隱藏技術，雖然藏入量高且影像品質也不錯，但此種技術也有其缺陷，當取出機密資訊

後，偽裝影像不可還原至原始影像，造成之後影像的可利用性降低。另外，EMD 產出的矩陣表非常大，通常大小為 256×256 矩陣，運算複雜度較高，因此本研究將自行設計動態矩陣影像可逆式技術，此動態矩陣可縮小魔術矩陣尺寸與降低藏入的運算複雜度，藉而改善 EMD 隱藏技術不足的部分。

1.3 研究目的

本論文將探討直方圖修改及動態矩陣可逆式資訊隱藏技術，基於機密資訊安全為首要基礎，本研究將設計能嵌入大量秘密訊息於負載媒體，且偽裝影像傳遞於公開場合不被人類視覺所發現有異狀，也就是存在良好的影像品質的資訊隱藏方法。除此之外，偽裝影像最終能還原至初始影像，達成機密資訊與原始資訊共存為目的之研究。本研究先設計直方圖位移高容量技術，利用原始影像鄰近區塊相似的特性，產生較準確的預測像素，計算其二階段區塊預測差值，分別利用區塊內差值與區塊間差值，經由統計產生二個直方圖之後藏匿資訊，主要預測技術能產出較大量的隱藏空間。更進一步，為了增加更大負載影像容量，則使用區塊眾數當成預測值，區塊眾數具有區塊像素的相似性，因此預測後的計算出較細微的差值，其趨近於零的差值頻率增加，使差值直方圖的峰點能夠明顯增加，即可產生更多的隱藏容量。除此之外，本研究設計動態矩陣高容量資訊隱藏，除了設計縮減的動態矩陣並在運算矩陣有著簡單實作的特性，容量方面比 LSB 技術改善並藏匿更多的二進位資訊，大幅增進資訊隱藏的容量。

為了保有機密資訊的安全性，本方法利用隨機亂數打亂欲藏匿機密資訊或浮水印，使其嵌入的資訊轉換成雜亂無章的資訊，即便讓有心人士取出機密資訊後，也無法得知機密的真實內容，使資訊隱藏存在安全性。在影像品質的設計，本文提出以空間域為基礎的隱藏方式，機密資訊的寫入都以像素值進行修改，為了不讓影像像素變動甚多，嵌入時只調整像素加一、減一或不改變像素為原則，因此

影像品質可以維持到一定水準，不讓人類視覺系統觀察到差異，達成不可察覺特性並擁有良好的影像品質。直方圖資訊隱藏可逆性的設計已成基本要件，但利用動態矩陣隱藏方式，本方法改善先前學者在資訊隱藏不可逆方式，提出一種嵌入與寫入相對應性的演算法，記錄少數的還原資訊，讓取出機密資訊後的影像回復至原貌，使原始資訊不流失，在特殊專業領可以增加其貢獻。

1.4 論文架構

本文內容分為七章，第一章介紹本研究的背景、動機與目的，並概述本研究的架構，第二章介紹相關資訊隱藏文獻，包含資訊隱藏技術分類、可逆式直方圖修改技術與利用魔術矩陣技術隱藏資訊等相關文獻，第三章提出二階段直方圖位移之高容量可逆性影像隱藏技術，第四章為應用影像區塊眾數之高容量可回復式隱藏技術，第五章提出動態矩陣機密資訊隱藏技術，其中第三、四與五章包含機密資訊藏匿、擷取機密資訊設計及還原演算法，第六章實驗結果分析與討論，第七章為本研究的結論。

第二章 文獻探討

本章將介紹資訊隱藏技術的分類架構以及隱藏的特性，藉此有助於對資訊隱藏實作有更明確的認知，不僅如此，本章也將介紹空間域可逆資訊隱藏方法，包含兩項技術，分別為直方圖預測差值[17][27][42]與魔術矩陣資訊隱藏[11]之相關文獻，首先為基於直方圖位移嵌入之預測技術，此技術可達成擴充影像隱藏資訊容量，內容包含直方圖位移的設計方法與流程、利用差異性的預測方式產生預測差值直方圖之嵌入設計等方法。再者，將介紹利用修改方向(Exploiting Modification Direction, EMD)產出魔術矩陣方法，並利用矩陣當成資訊隱藏的對照方式，主要包括保護機密資訊安全性的濕紙編碼法(Wet Paper Coding, WPC)與利用修改方向產出矩陣的製作方式，並敘述如何利用兩者做為資訊隱藏的方法。

2.1 資訊隱藏技術

資料隱藏技術最早是在 1984 年由密碼學大師 Simmons[30]提出，在一場密碼會議中他提出「監獄中分隔兩地的囚犯如何計畫逃獄」，囚犯平常可以透過書信傳遞訊息，但需由典獄長嚴格檢查書信，在逃獄計畫中該如何利用最不起眼的書信內容使得典獄長不被發現囚犯傳送訊息內容有問題，這就是所謂的資訊隱藏技術。數位化的時代來臨，網路傳輸文件之資訊安全更顯重要，資訊領域的學者紛紛投入資訊隱藏的研究及發展，資訊隱藏相關技術提出後，Petitcolas 等學者[28]在 1999 年在資訊隱藏領域做出整體架構明確的分類，如圖 2-1，目前在資訊隱藏技術學者們都以偽裝學(Steganography)和浮水印(Watermarking)兩大方向做為研究，雖然兩項技術都屬於影像資訊隱藏，但應用的目的卻完全不同，偽裝學是將負載媒體藏匿秘密資訊，即將有意義的訊息資訊隱藏至數位媒體中，在公開環境下，傳遞數位媒體過程中不被有心人士察覺而提出攻擊，達成偽裝影像的隱密性

與不可察覺性。浮水印技術則是將智慧財產商標嵌入至數位媒體中，當數位媒體被侵權或盜用時，可以取出嵌入於影像的商標資訊，即使嵌入的負載媒體遭受各種訊號處理的攻擊，還是可以取出完整可辨識的浮水印，達成影像的強韌性(Robustness)，因此，浮水印技術可解決數位媒體智慧財產權歸屬的問題。

影像資訊隱藏實作時，必須考量影像或機密資訊在隱藏階段存在的特性，清楚了解特性後，藉由資訊隱藏演算法改善並解決這些問題，資訊隱藏技術的提出才有其貢獻。由於整張影像的像素個素有限，影像像素負載量(Capacity)為資訊隱藏首要注意的問題。機密資訊或浮水印嵌入影像後，產生的偽裝影像是否能夠欺瞞第三方，達成不可察覺的特性(Imperceptibility)。影像傳輸過程中可能會讓非法人士進行竄改破壞，在影像接收訊息後，是否可以取出完整機密訊息，達成影像的強韌性(Robustness)。最後，影像取出機密資訊後，偽裝影像能否還原至原始影像之可逆性(Reversibility)，這些都為資訊隱藏必須考量的主要特性：

- 負載量(Capacity)：資訊隱藏的目標就是偽裝影像維持一定的影像品質下，又可藏入大量的資訊，但所謂魚與熊掌不可兼得，也就是要藏匿大量資訊至影像中，必然會破壞影像的品質，藏入少量資訊，雖然可以減少影像品質的損失，資訊含量少資訊隱藏顯而無益於機密資訊傳遞，因此該找到兩者兼顧的平衡點，資訊安全藏匿演算法就彰顯其重要性。
- 不可察覺性(Imperceptibility)：資訊隱藏技術中最關鍵的特性，嵌入資料後的偽裝影像要從人類視覺達到不被察覺影像有被更動，達成此特性的優良資訊隱藏技術，可為偽裝影像在傳輸過程提升及其安全性，而此特性通常利用 PSNR 值當作評估指標，當 PSNR 值越高，影像不易被察覺有異，反之，影像品質差且容易被人類視覺發現有藏匿資料。
- 強韌性(Robustness)：為影像傳輸過程中可以容忍的破壞程度，機密資訊藏匿於影像後，有心人士透過數位訊號處理，如切割、旋轉與雜訊攻擊情況下，

若要取出完整的機密資訊並能夠保證資訊不易被移除或改變，資訊隱藏技術之強韌性已形成關鍵。

■可逆性(Reversibility)：資訊隱藏除了可以夾帶機密資訊外，尚可以保留原始資訊，換句話說，不僅要讓接收方取出機密資訊後，偽裝影像還可以利用還原資訊回復至原始影像，此特性可為特殊用途之資訊隱藏帶來判斷及使用的貢獻。

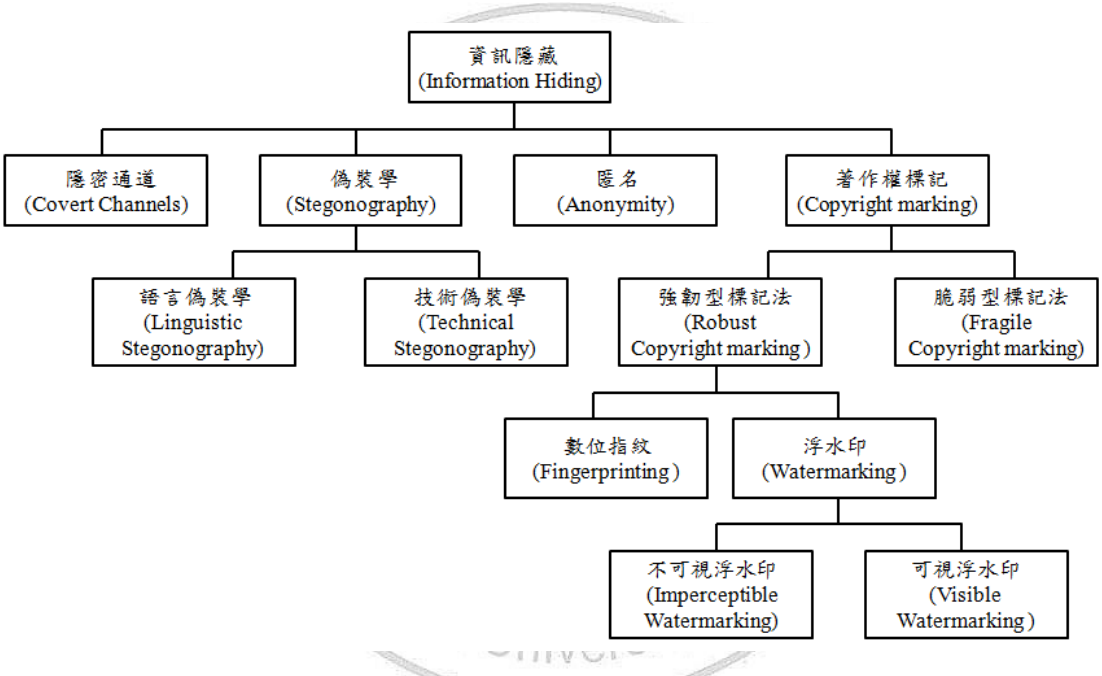


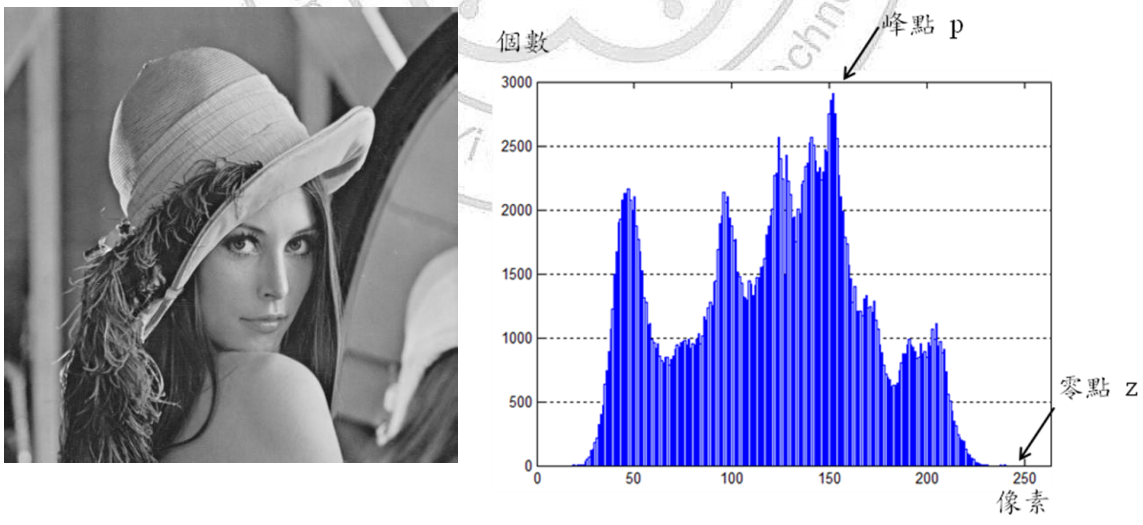
圖 2-1　資訊隱藏技術分類圖

2.2 Ni 等學者所提之方法

2006 年，Ni 等學者 [27] 提出一以修改直方圖為基礎的可逆資料嵌入技術，此技術將機密資訊嵌入於影像中，接收者從偽裝影像取出機密資訊後，可回復成原始影像，又可稱為無失真資訊隱藏技術，此方法簡單又具其效率，亦可維持良好影像品質。在 Ni 等學者提出的可逆資料隱藏演算法中，統計整張原始影像的像素值產生直方圖。直方圖中出現次數最多的像素值稱之為峰點(Peak Point)，而峰

點的右側找出沒有出現次數的像素值則稱為零點(Zero Point)，若找不到該像素值，則尋找峰值右側出現最少次數的像素值，將此像素值視為零點。例如一張 512×512 的 Lena 影像如圖 2-2(a)，將此影像像素統計產生直方圖，其中 p 點為峰點、z 點為與零點如圖 2-2(b)。

為隱藏機密資訊，需將直方圖位移(Histogram Shifting)，亦即將峰點與零點之間的像素分別向右位移一個像素值，由左而右從上至下掃瞄影像像素值 x，若 $x \in [p+1, z-1]$，則像素值要加一，位移一個單位，位移後的像素值，即 $x \in [p+2, z]$ 的範圍中，因此最高峰右邊的位元，即 p+1 處之像素位置就會空出來，此即為嵌入機密資訊的使用位置。隱藏資訊時，循序掃瞄整張影像像素值，若像素值等於峰點值，且欲嵌入的機密資訊位元為$(0)_2$，該像素維持不變；若嵌入的機密資訊位元為$(1)_2$時，則將像素值加一，嵌入後的像素值為 p+1。執行整張影像產生嵌入機密資訊的偽裝影像，並記錄峰點與零點作為檔頭資訊，峰點與零點之額外資訊(Side information)可作為金鑰，以便日後擷取機密資訊及還原影像使用。



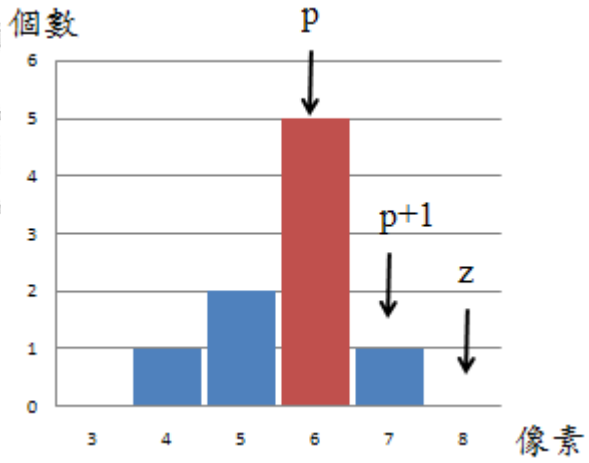
(a)　　(b)

圖 2-2　Lena 影像與直方圖

在取出機密資訊程序時，以相同順序將掃描偽裝影像，比對影像像素值 x' 與峰點資訊 p，若 $x'=p$，代表該像素嵌入的資訊為 $(0)_2$，還原時該像素不做改變；若該影像像素 $x'=p+1$，則代表該像素嵌入訊息為 $(1)_2$，即可取出此資訊 $(1)_2$，並回復位移還原成原始影像像素值 p。當機密訊完全取出後，偽裝影像像素值 $x'\in[p+2,z]$，在此範圍的像素值須減一，回復為原始影像像素值 $x'\in[p+1,z-1]$。

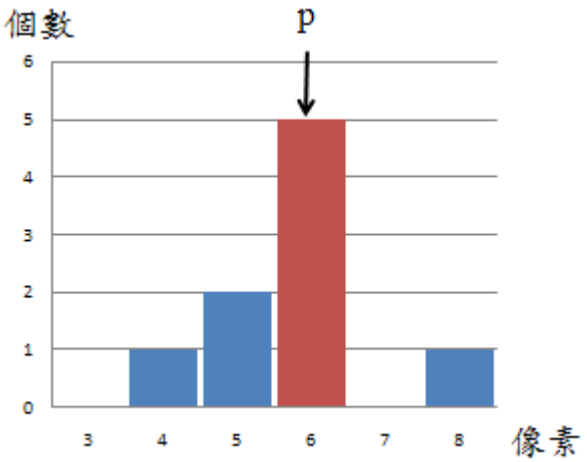
例如一張大小為 3×3 之原始影像如圖 2-3(a)，經由統計產生直方圖如圖 2-3(b)，由直方圖可知峰點之像素值 $p=6$ 與零點像素值 $z=8$，找出峰點與零點後，由左至右從上而下掃描整張影像，找出峰點右邊的像素值為 7，將其值加 1，即可得到位移的像素值如圖 2-4(a)，而統計後之位移直方圖如圖 2-4(b)。假設欲隱藏的機密資訊為 $(11010)_2$，掃描位移影像，當 $p=6$ 且欲嵌入機密資訊為 $(1)_2$，則該像素值加 1，即 $p=7$。而當 $p=6$ 且欲嵌入機密資訊為 $(0)_2$ 則像素不做改變，即 $p=6$。最後得到嵌入機密資訊的偽裝影像像素值如圖 2-5(a)，其直方圖的結果呈現於圖 2.5(b)。

6	5	5
6	6	4
6	7	6



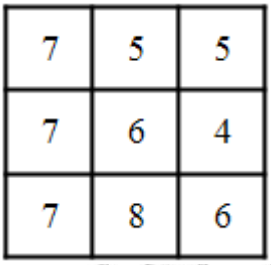
(a)原始像素值　　(b)原始直方圖

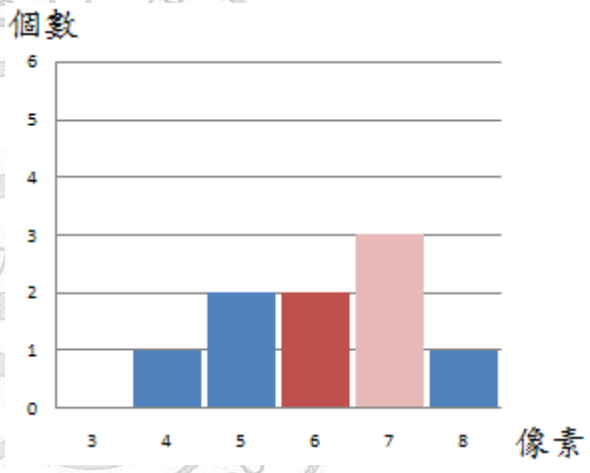
圖 2-3　影像像素統計直方圖



(a)位移後像素值　　(b)位移後直方圖

圖 2-4　影像像素值位移





(a)偽裝影像　　(b)嵌入機密資訊直方圖

圖 2-5　嵌入機密訊息之偽裝影像

在 2006 年 Ni 等人提出以直方圖為基礎的資料嵌入技術，許多學者發現統計的直方圖，其峰點像素出現的次數有限即不足以藏匿大量資訊問題，因此，近年學者們也紛紛提出增加峰值出現次數的研究，如改善單峰利用雙峰進行機密資訊隱藏，或者是利用預測差值的方式讓峰點可以增加出現頻率，以便嵌入容量提升，在 2.3 與 2.4 小節的文獻探討中將會介紹預測差值可增加隱藏容量的特色。本研究將嘗試利用雙峰作二階段嵌入方式並使用預測差值產生二個直方圖，以增加藏秘容量，不僅如此，本研究又提出應用眾數預測之資訊隱藏技術，區塊眾數可精準

預測區塊像素的相似性，預測差值可以趨近於零，實驗結果顯示本文利用預測差值嵌入的機密資訊確實可增加大量的隱藏容量。

2.3 Hong 等學者所提之方法

2010 年，Hong 等學者提出了以可控制區塊變異的可逆資料嵌入方法[17]，與 Ni 等學者不同的是，Hong 利用了預測差值(Prediction error)產生直方圖來藏匿機密資訊，利用鄰近的像素計算差值後，產出與本身像素更近似的值，像素差值與本身像素值相減後為預測差值，其目的就是讓預測差值近似於 0，使預測差值統計後的直方圖可產生更高的峰點，亦即可增加嵌入的機密資訊容量。更進一步利用區塊的變異控制嵌入，利用 Hong 定義的門檻，找出低變異與高變異的區塊，而低變異的區塊可以加入嵌入流程，以改善嵌入後的影像品質。

此方法每個區塊利用五個基礎像素、提供八個非基礎像素的預測方式如圖 2-6，使用一個基礎像素 b_i 與四個衛星基礎像素 b_i^L 、b_i^R 、b_i^U 與 b_i^D ，經由加權式計算後，非基礎像素較靠近基礎像素的權重較大，較遠者權重較小，這樣可以使預測差值更加精確，其中八個非基礎像素分別為 $nb_{i,1}$、$nb_{i,2}$、$nb_{i,3}$、$nb_{i,4}$、$nb_{i,5}$、$nb_{i,6}$、$nb_{i,7}$ 與 $nb_{i,8}$ ，而八個非基礎像素的預測值計 $p_{i,1}$ 、$p_{i,2}$ 、$p_{i,3}$ 、$p_{i,4}$ 、$p_{i,5}$ 、$p_{i,6}$ 、$p_{i,7}$ 與 $p_{i,8}$ 算如公式(2.1)-(2.8)：

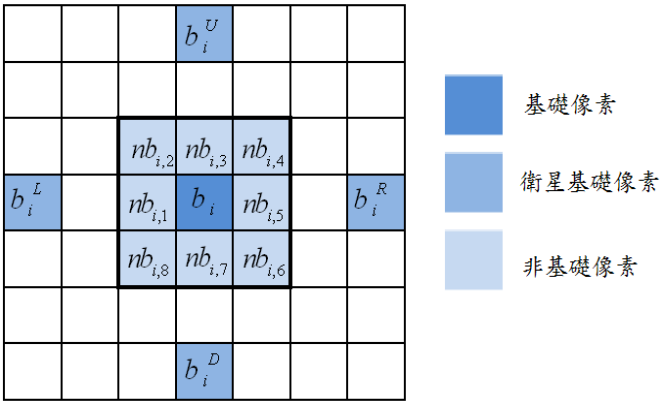


圖 2-6　預測像素位置圖

$$p_{i,1} = round(\frac{1}{3}(2b_i + b_i^L))\ ，\tag{2.1}$$

$$p_{i,2} = round(\frac{1}{3}(b_i + b_i^L + b_i^U))\ ，\tag{2.2}$$

$$p_{i,3} = round(\frac{1}{3}(2b_i + b_i^U))\ ，\tag{2.3}$$

$$p_{i,4} = round(\frac{1}{3}(b_i + b_i^U + b_i^R))\ ，\tag{2.4}$$

$$p_{i,5} = round(\frac{1}{3}(2b_i + b_i^R))\ ，\tag{2.5}$$

$$p_{i,6} = round(\frac{1}{3}(b_i + b_i^R + b_i^D))\ ，\tag{2.6}$$

$$p_{i,7} = round(\frac{1}{3}(2b_i + b_i^D))\ ，\tag{2.7}$$

$$p_{i,8} = round(\frac{1}{3}(b_i + b_i^D + b_i^L))\ ，\tag{2.8}$$

其中 $round(x)$ 為四捨五入函數。

在基礎像素中，像素差異大的區塊可能會導致非基礎像素的預測直不準確，產生預測差值分散的狀況，因此計算基礎像素的變異以預測此區塊是處於平滑的區塊或者複雜區塊，計算預測區塊變異方式如公式(2.9)。

$$\text{var}(b_i) = \frac{1}{5}((b_i - b_m)^2 + (b_i^L - b_m)^2 + (b_i^R - b_m)^2 + (b_i^U - b_m)^2 + (b_i^D - b_m)^2)\ ，\tag{2.9}$$

其中 b_m 為 b_i 、 b_i^L 、 b_i^R 、 b_i^U 與 b_i^D 的平均值。

在嵌入機密資訊時，將判斷該區塊的變異 $\text{var}(b_i)$ 是否大於門檻值 TH ，TH 為方法定義之門檻值，若 $\text{var}(b_i) > TH$ ，則此區塊屬於變異大的複雜區塊，不進行嵌入機密資訊。若 $\text{var}(b_i) < TH$ ，則此區塊屬於變異數小的平滑區塊，即可進行嵌入機密資訊。嵌入與取出機密資訊的方式與 Ni 等學者提出的直方圖嵌入步驟相為類似，但在此方法的嵌入步驟中，利用出現預測差值次數最多 Phd 與出現次多的 Pld 當作雙峰，預測差值峰值的左右差值經由位移後，差值 $Phd+1$ 與 $Pld-1$ 可作嵌入

機密資訊$(1)_2$空間，因此可增加嵌入資訊容量。

在此方法中，隨然較 Ni 學者提出直接統計直方圖隱藏方式增加藏秘容量，但仍會受限於複雜區塊與基礎像素值不能提供預測差值計算的限制，造成像素使用率降低且嵌入量會減少，原因出自於計算區塊變異時複雜區塊時，有幾個預測值可能與非基礎像素的值相等，此情況少了嵌入機密資訊的容量；在基礎像素方面，該像素不可藏匿資訊，此像素需當成還原的資訊，然而像素使用率也降低，以大小 512×512 的影像為例，會失去$\frac{512\times512}{3\times3}$的嵌入資訊容量。基於擴增隱藏資訊容量，本研究將提出二階段預測差值嵌入機密資訊方法，充分利用預測差值，儘量可以達成每一預測差值都可以嵌入機密資訊，亦增加資訊隱藏容量。

2.4 Zhao 等學者所提之方法

2011 年，Zhao 等人提出了可回復資料隱藏技術[42]，此技術利用鄰近像素相似的特性當作預測值，像素值與預測值的差值稱為鄰近像素差異，其預測規則是使用反向 S 型掃描影像如圖 2-7，例如一張 3×3 大小的影像當作掃描預測值，其掃描的路徑，依反向 S 型順序找出預測值 p_1、p_2、…、p_9。預測差值計算方式為上一個像素值減去本身像素值，如公式(2.10)，算出預測差值後可以統計成值方圖進行機密資訊隱藏流程。

Zhao 等人所提方法[42]與文獻[17][36][38]提出以直方圖嵌入機密資訊技術，主要差異在於提高機密資訊隱藏容量，利用多層式直方圖差異計算以為嵌入資訊，其中嵌入層級定義為$EL\,(EL\geq0)$，$EL=0$為單一峰點嵌入，即是 Ni 等學者所提出的嵌入流程；$EL=1$為峰點之左右各一個像素當作嵌入容量，當$EL=1$做為嵌入時，有三個峰值可以當作嵌入容量；$EL=2$為峰點之左右各兩個像素當作嵌入容量，當$EL=2$時，總共有五個峰當作嵌入容量，各層級可以此類推。嵌入流程

是由大的層級 EL 先執行，以遞減方式嵌入至 $EL=0$。

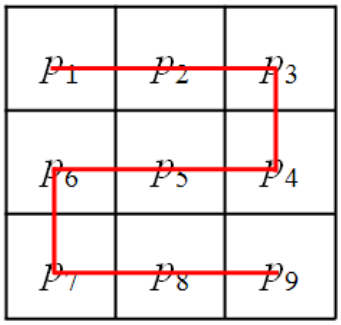


圖 2-7　反向 S 型掃描影像

$$d_i=\begin{cases}p_1, i=1\\ p_{i-1}-p_i, 2\le i\le M\times N\end{cases}, \tag{2.10}$$

例如以 $EL=1$ 時，預測差值之直方圖統計如圖 2-8(a)。$EL=1$ 為峰點左邊與右邊的像素，在峰點像素之左邊所有像素需要位移一個單位，此像素右邊所有像素要位移兩個單位，差值位移後直方圖如圖 2-8(b)。機密資訊嵌入，首先嵌入 $EL=1$，當機密資訊$(0)_2$ 且掃描至差值為-1 時，差值不做改變；當機密資訊$(1)_2$ 且掃描至差值為-1 時，差值減一；當機密資訊$(0)_2$ 且掃描至差值為 1 時，差值加一；當機密資訊$(1)_2$ 且掃描至差值為 1 時，差值加二，如圖 2-8(c) ，紅色箭頭為嵌入機密資訊$(0)_2$，藍色箭頭為嵌入機密資訊$(1)_2$。圖 2-8(d)為 $EL=1$ 嵌入資訊於差值完成後的統計直方圖。隨後 EL 遞減至零，當機密資訊要嵌入峰點時，若機密資訊為$(0)_2$ 且掃描至差值為 0 時，差值不做改變；若機密資訊為$(1)_2$ 且掃描至差值為 0 時，差值加一，如圖 2-8(e)，紅色箭頭為嵌入機密資訊$(0)_2$，藍色箭頭為嵌入機密資訊$(1)_2$，如圖 2-8(f)為 $EL=0$ 嵌入資訊於差值完成後的統計直方圖，再將嵌入後的預測差值還原成原始像素即可得到偽裝影像。

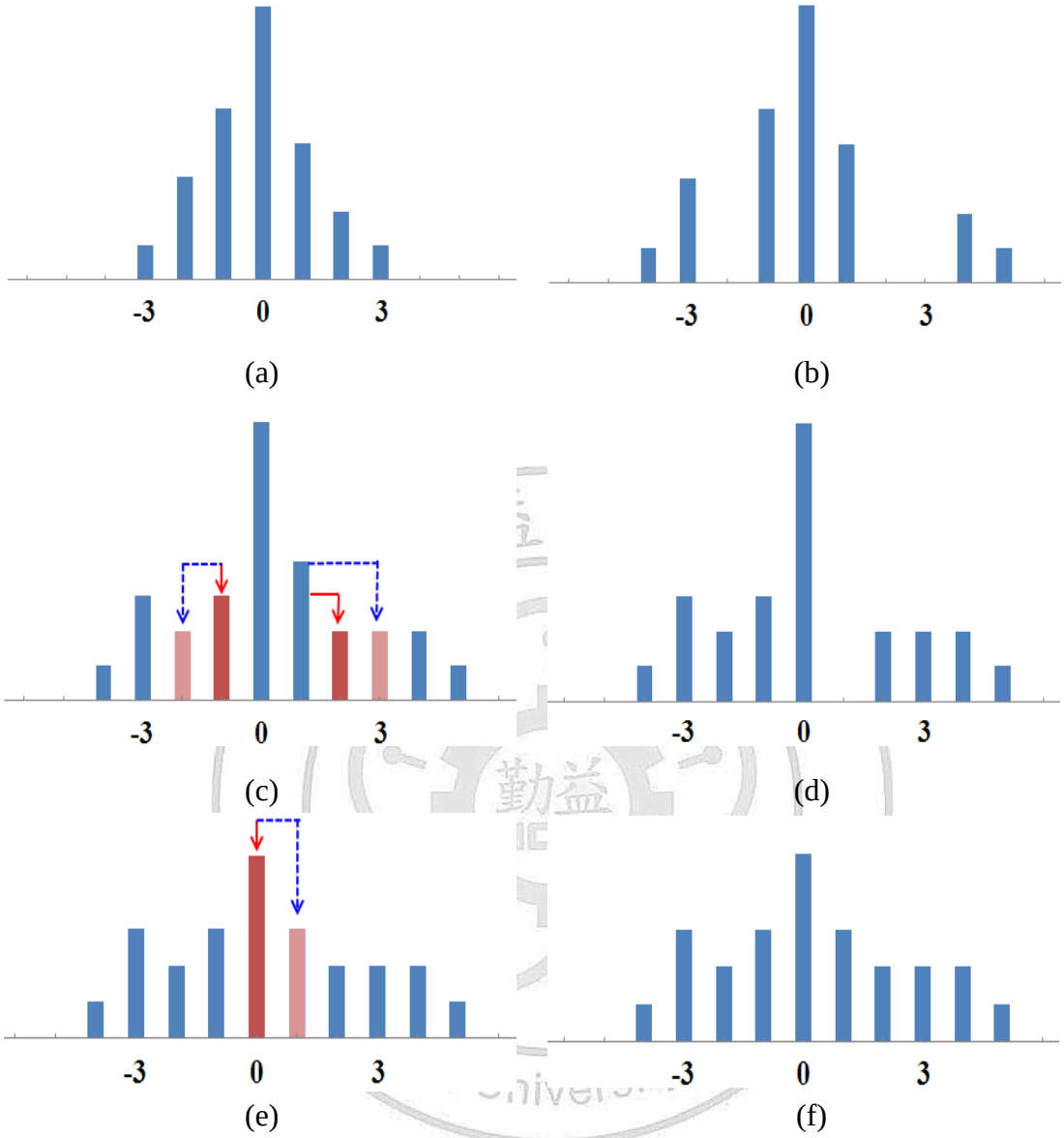


圖 2-8　*EL* = 1 嵌入示意圖

在此方法中，利用鄰近像素作為預測差值可以產生較高的峰點，但是單純以反向 S 型的預測效果在嵌入容量方面，無法顯示其效果會較好，因此 Zhao 等人提出了以嵌入層級 *EL* 進行調整的嵌入容量方式，當 *EL* 越大時其容量相對增加，但是當 *EL* 越大的時候，預測差值改變就越大，嵌入機密資訊預測差值製做成偽裝影像後品質也會變差。因此，此方法雖然提出了高容量隱藏，卻也犧牲了影像品質。本研究將提出二階段直方圖預測差值與應用區塊眾數作為嵌入機密資訊預測差值

方式，使隱藏容量可以提升，同時也維持一定的影像品質。

2.5 Chang 等學者所提之方法

2009 年，Chang 等學者[11]提出魔術矩陣與濕紙編碼法之資料隱藏技術，此方法結合兩種技術當作資訊隱藏重點，其中濕紙編碼法(Wet Paper Coding, WPC) [10][15][39]概念即是紙張遇水淋濕的情況下，紙張會有淋濕與未淋濕的兩個部分，淋濕位置不能寫下訊息，未淋濕位置將可寫下訊息，這個概念也被應用在影像處理中，將影像利用虛擬隨機亂數(Pseudo-random)挑選乾與濕的像素，乾像素可以被寫入資訊，濕像素則不能，挑選完畢後即可將機密資訊藏匿於乾的像素值中，當影像傳送到接受方時，由於接收方無法得知乾與濕像素值，因此傳送與接收雙方需要共享金鑰，即隨機挑選影像乾與濕像素之亂數種子，若接收方取得金鑰，則可取出藏匿的機密訊息，WPC 的優點為攻擊者無法得知影像藏匿訊息位置，增強機密資訊之安全性，此篇技術先利用 WPC 處理欲藏入資料的像素，增加隱藏的安全性。

其次，使用魔術矩陣 (Magic Matrix)隱藏技術[12]，又稱利用修改方向(Exploiting Modification Direction, EMD)資訊隱藏技術 [23][37][40]，概念為將機密資訊切割並分組轉換表示為$(2n+1)$-ary(進制)的數值，每一組機密資訊值即可藏入 n 個負載影像像素中，利用 EMD 公式計算出魔術矩陣，如公式 2.11，魔術矩陣特色在於$(2n+1)$的範圍內，不會出現相同的數值，且矩陣各個行、列與對角線相加之和都相等的性質，對於藏匿機密資訊，有最適合的隱藏對照方式。

$$f(g_1, g_2, ..., g_n) = \left(\sum_{i=1}^{n} (g_i \cdot i) \right) \bmod (2n+1) \tag{2.11}$$

其中 n 代表向量的維度，g_n 代表 n 維度空間各座標軸之對應值，通常取 n＝2，在 2 維的平面空間中，如圖 2-9，換句話說，藏入時抓取兩個像素 g_1 與 g_2 為一組，

兩個像素分別對應魔術矩陣的 X 與 Y 軸，可得對應於矩陣內部之值，將此值為中心點，尋找中心點附近欲藏入的機密資訊值，再將機密資訊值對應回 X 與 Y 軸，g_1 與 g_2 原始像素將被修改成機密資訊對應回的 X 與 Y 軸，依序執行此步驟，將可完成機密資訊藏入，並得到偽裝影像。EMD 與 LSB 都屬於空間域資訊隱藏，相較於 LSB 將機密資訊嵌入於最不重要位元，EMD 利用矩陣對照像素進行嵌入機密資訊，可藏入容量較大，且都屬於改變像素加一、減一或不更動像素，藏匿後的影像不易被肉眼察覺有變動，使得偽裝影像影像品質相當高。

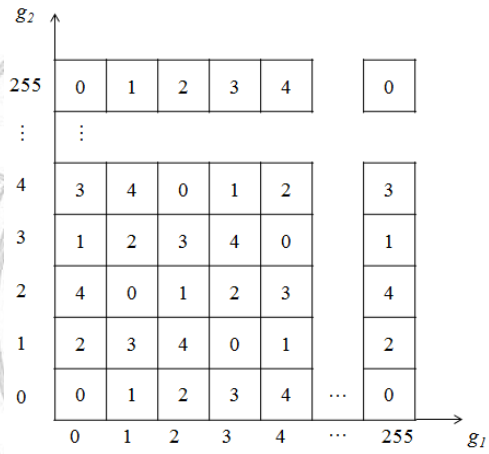


圖 2-9　5-ary 之魔術矩陣範例

Chang 等學者在此篇研究中，利用了兩個隱藏技術，WPC 可以增加資訊藏入的安全性，而魔術矩陣藏入方式則可以增加隱藏容量，且藏入時影像像素變動不大，因此偽裝影像達到不錯的品質，不過利用 WPC 隨機亂數挑選藏入的位置，雖然可增加機密資訊的安全性，但在挑選像素過程中，濕的像素不可藏入資料，可能會造成影像的負載容量縮小。再者，利用魔術矩陣當作藏入的方法，雖相較 LSB 藏入技術可提升負載影像容量增大，但此技術需要經由計算魔術矩陣的公式，且矩陣的大小可能太大，矩陣部分的值可能沒用到，增加記憶體負擔，因此，本研究欲改進 Chang 等學者提出魔術矩陣與濕紙編碼法之資料隱藏技術，提升負載影像的嵌入容量，縮減魔術矩陣大小並提出影像可還原的技術。

第三章 二階段直方圖位移之高容量可逆性影像隱藏技術

本章將提出一種以預測差值與直方圖修改為基礎的機密資訊隱藏技術，將改善 Hong 等人[17]與 Zhao 等人[42]所提出的資訊隱藏技術，本方法將預測區塊縮小提升預測能力，使預測差值趨近於零並可增加隱藏容量，並善用影像像素使差值出現次數提高。本方法將一張大小 M × N 之原始影像切割至大小 2x2 且互不重疊的區塊，利用數學運算產生預測差值，再經由統計運算產生預測差值之直方圖。為了增加嵌入與可調整的影像隱藏容量，盡可能善加利用每一像素，因此區塊間未被使用的像素再次進行預測差值的計算，可得另一預測差值直方圖。直方圖出現最多與次多預測差值次數，即為本方法設計之嵌入隱藏容量，利用兩對峰值，隱藏容量也可隨之動態調整。在 3.1 節為資訊隱藏演算法，3.2 為取出機密資訊與還原影像演算法，3.3 節為本方法的範例實做，詳細嵌入與取出還原影像與實作如以下小節所述。

3.1 二階段直方圖位移之資訊隱藏

本方法將利用鄰近像素與鄰近區塊的特性，進行二階段運算預測差值提升影像負載與可調式容量方法。假設以 Lena 原始影像為例，將大小為 M × N 的原始影像切割成 2x2 且互不重疊的區塊，以四宮格為基礎循序搜尋影像區塊，計算每一區塊影像之中位數、平均數，利用其差值產生預測差值，並將轉換成預測差值區塊。其次利用反向 S 型搜尋像素值，每個像素相減後方可取得預測差值。浮水印藉由亂數排列並轉換為二進制機密資訊，利用 LSB 法藏匿於預測差值影像中，最後再以預測差值影像轉換成偽裝影像。嵌入演算步驟如下：

【二階段直方圖位移之資訊隱藏演算法】

輸入：原始影像，浮水印

輸出：偽裝影像，二對峰點資訊

【Step 1】影像切割

將一張大小為 M × N 之灰階原始影像 I 切割成大小為 2×2 且互不重疊的區塊 B_k，其中 $\{B_k \mid k=1,2,...,T\}$，$T = \frac{M \times N}{2 \times 2}$。每一區塊均有四個像素值，總共的切割出 T 個區塊數量，如圖 3-1 所示。

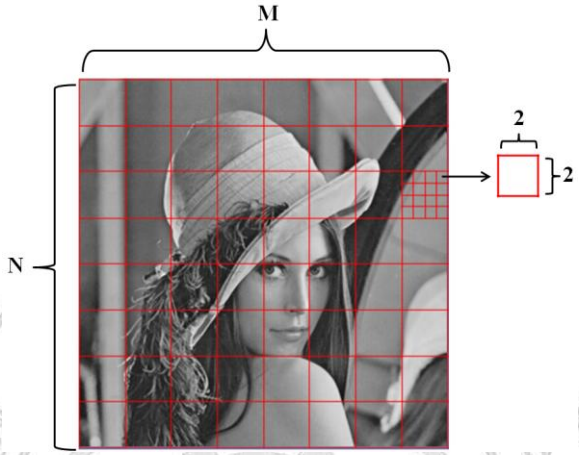


圖 3-1　影像切割

【Step 2】轉換影像區塊為預測差值影像

對於每一區塊 B_k，$\{B_k \mid k=1,2,...,T\}$ 均含有四個像素，$\{b_{i,j} \mid i,j \in 1,2\}$，亦即每一區塊像素值為 $b_{1,1}$、$b_{1,2}$、$b_{2,1}$ 與 $b_{2,2}$ 如圖 3-2(a)所示，在設計方法上，將每一區塊 B_k 轉換成預測差值區塊 D_k，$\{D_k \mid k=1,2,...,T\}$，其中預測差值區塊 D_k 含有四個像素 $\{d_i \mid i \in 1,2,3,4\}$，影像區塊轉成預測差值區塊如圖 3-2(b)所示。本方法以鄰近像素值為基礎之預測方式，每個區塊分二個階段計算出預測差值區塊，第一階段運算出三個預測差值，第二階段利用影像區塊未利用的第四個像素作為計算第四個預測差值，形成一個完整的預測差值區塊。

每一區塊 B_k，$\{B_k \mid k=1,2,...,T\}$ 要取得預測值，首先計算 $b_{1,2}$、$b_{2,1}$ 與 $b_{2,2}$ 之中位數 Mb，即 $Mb = median\{b_{1,2}, b_{2,1}, b_{2,2}\}$，其中 $median$ 表示為中位數計算函數，函數計算為先排序 $b_{1,2}$、$b_{2,1}$ 與 $b_{2,2}$ 數值大小，之後再取中間值的運算。再者，計算 $b_{1,2}$ 與

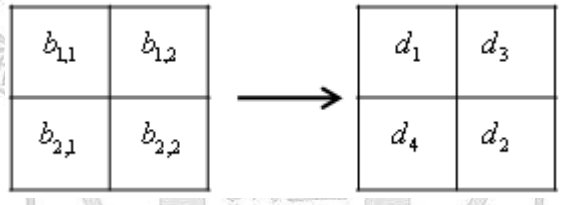
$b_{2,1}$ 平均之上限整數 Cb ，即 $Cb=\left\lceil \frac{b_{1,2}+b_{2,1}}{2} \right\rceil$ ，其中⌈ ⌉表取上限整數函數。第一階段預測差值區塊 D_k ，$\{D_k | k=1,2,...,T\}$ ，其四個像素值 $d_i, i=1,2,3,4$ 之預測差值計算如公式如下：

第一個預測差值： $d_1=b_{1,1}-Mb=b_{1,1}-median\{b_{1,2},b_{2,1},b_{2,2}\}$ (3.1)

第二個預測差值： $d_2=b_{2,2}-Cb=b_{2,2}-\left\lceil \frac{b_{1,2}+b_{2,1}}{2} \right\rceil$ ， (3.2)

第三個預測差值： $d_3=b_{1,2}-b_{2,1}$ ， (3.3)

第四個預測差值： $d_4=b_{2,1}$ ， (3.4)



(a) (b)

圖 3-2 影像區塊轉換成預測差值區塊示意圖

每一個影像區塊轉換成預測差值區塊，第一階段可得三個預測差值分別為 d_1 、d_2 、d_3 ，而第四個預測差值 $d_4=b_{2,1}$ 尚為原始區塊像素值，將於第二階段進行預測的運算，預測差值 $d_i, i=1,2,3,4$ 將之存成區塊陣列如圖 3-2(b)，所有的差值區塊形成一 M × N 之預測差值影像 $I1D$ 。

【Step 3】計算預測差值影像 *I1D* 之第一階段直方圖 *H1D*

計算預測差值影像 $I1D$ 之第一階段直方圖 $H1D$ ，假設預測差值像素 $I1d_i$ ，$I1d_i \in I1D$ ，其中 $I1d_i \in [-255,255]$ ，在預測差值影像中，計算所有區塊之 d_1 、d_2 、d_3 出現之次數統計製作直方圖，產生第一個直方圖 $H1D$ 。

【Step 4】找出第一直方圖之兩對峰點與零點

從 $H1D$ 直方圖中尋找預測差值像素出現最多與次多的數值，稱之為最高峰點 PH_1 與次高峰點 PL_1，其中 $PH_1 > PL_1$，假設峰點 PH_1 於右側、次高峰點 PL_1 於左側，其對應之零點 ZH_1 與 ZL_1，其中零點表此像素皆未出現於預測差值影像 $I1D$ 中；峰點紀錄二個資訊，一為該像素值出現次數，即 PH_1 與 PL_1，其對應之差值像素值為 Pd_1 與 Ld_1，即 $Pd_1 > Ld_1$；並找出 PH_1 右側對應的零點 ZH_1，PL_1 左側對應的零點 ZL_1，亦即從 $H1D$ 找出出現零次的點 ZH_1，其中 ZH_1 之差值像素值 $Pzd_1 \in [Pd_1 + 1, 255]$，從 $H1D$ 找出出現零次的點 ZL_1，其中 ZL_1 之差值像素值 $Lzd_1 \in [-255, Ld_1 - 1]$。

【Step 5】計算第二階段預測差值並求得縮減影像 $I2D$

由於計算第一階段區塊差值時，尚有一個預測差值像素 $d_4 = b_{2,1}$ 未被使用，為了增加嵌入空間的使用，本方法將善用每一區塊之 $b_{2,1}$ 以增加嵌入容量。首先，利用預測差值影像 $I1D$ 中，每一差值區塊之未被改變像素 $b_{2,1}$，依序儲存於陣列中，如圖 3-3，形成一縮減影像 $I2D$，在 $I2D$ 中，總共有 $\frac{M \times N}{2 \times 2}$ 個像素值。

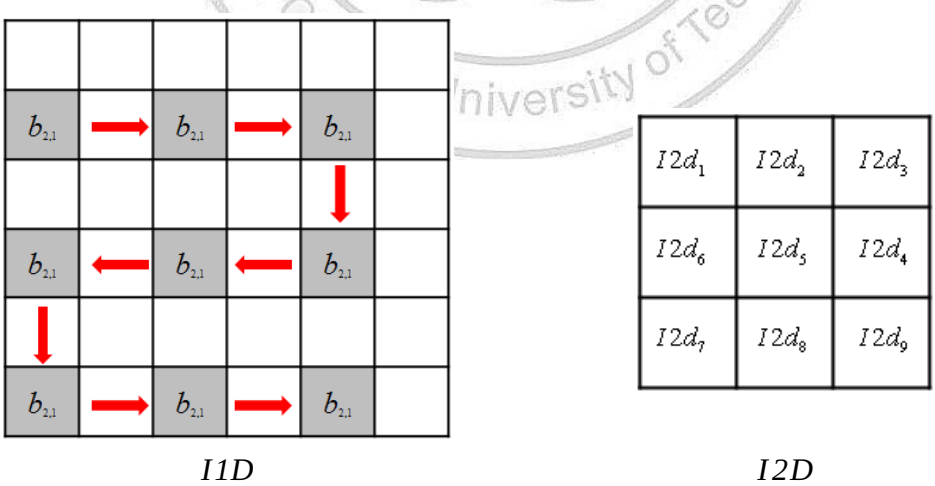


圖 3-3　縮減影像示意圖

【Step 6】轉換縮減影像 $I2D$ 為預測差值陣列 $I3D$

取得縮減影像 $I2D$ 後，假設 $I2D$ 之像素值為 $I2d_i$ ，$i \in \{1,2,...,T\}$ 其中 $T = \frac{M \times N}{2 \times 2}$，將縮減影像 $I2D$ 依反 S 方向順序排列，儲存於縮減影像之預測差值陣列 $I3D$ 如圖 3-4， 預測差值計算方式為前一個像素值減後一個像素值，依序執行，縮減影像之預測差值 Id_i ，計算公式如下：

$$I3d_i = \begin{cases} I2d_i, i = 1 \\ I2d_{i-1} - I2d_i, 2 \le i \le T \end{cases}, \tag{3.5}$$

因此總共得到 $\frac{M \times N}{2 \times 2} - 1$ 個預測差值，計算預測差值後，依序儲存於縮減影像之預測差值陣列 $I3D$，即預測差值像素值 $I3d_i, i = 1,2,...,T$ 。

圖 3-4　預測差值陣列 $I3D$

【Step 7】計算預測差值影像 $I3D$ 產生第二直方圖 $H2D$

假設預測差值像素 $I3d_i$，$I3d_i \in I3D$，其中 $I3d_i \in [-255, 255]$ ，在預測差值陣列中，計算所有差值之出現之次數，統計製作其直方圖，產生第二個直方圖 $H2D$。

【Step 8】找出第二直方圖 $H2D$ 之兩對峰點與零點

從 $H2D$ 直方圖中尋找預測差值像素出現最多與次多的數值，即為最高峰點 PH_2 與次高峰點 PL_2，其中 $PH_2 > PL_2$，其對應之差值像素值為 Pd_2 與 Ld_2。假設峰點 PH_2 於右側、次峰點 PL_2 於左側，即 $Pd_2 > Ld_2$，並分別找出 PH_2 與 PL_2 對應的零點 ZH_2 與 ZL_2，其中 ZH_2 之差值像素值為 $Pzd_2 \in [Pd_2 + 1, 255]$， ZL_2 之差值像素值 $Lzd_2 \in [-255, Ld_2 - 1]$ 。

【Step 9】計算可藏入機密資訊容量

本方法可計算藏入機密資訊容量之最大值，藏入資訊容量即為二個直方圖之雙峰次數總和，設可藏入容量為*Total*，計算如下：

$$Total = PH_1 + PL_1 + PH_2 + PL_2 \text{，} \tag{3.6}$$

在隱藏資訊時，將機密資訊拆開分為兩個部分，分別嵌入於第一與第二直方圖之雙峰點，假設欲藏入第一直方圖之機密資訊為*Secret*1，其資訊量為NS_1，即$NS_1 = PH_1 + PL_1$；藏入第二直方圖之機密資訊為*Secret*2，其資訊量為NS_2，即$NS_2 = PH_2 + PL_2$。假設嵌入之機密資訊為浮水印資訊，需要*Total*開平方根並取整數，此整數為藏匿的浮水印影像的長與寬之值，藏入後有剩下的空間再利用零補足可藏匿空間。

【Step 10】修改預測差值產生第一位移直方圖*H1D'*

為隱藏機密資訊於預測差值影像*I1D*中，假設差值影像*I1D*所對應之直方圖*H1D*，欲藏匿資訊於直方圖之雙峰點位置，需將峰值右側至零點間的像素值分別向右位移一個位元，而將次高峰值左側至零點間的像素值分別向左位移一個位元，空出來的位置可作為藏匿資訊使用，此步驟稱為位移直方圖。在預測差值影像*I1D*中，若預測差值$I1d_i$介於此區間$[Pd_1+1, Pzd_1-1]$，則預測差值加一；若預測差值$I1d_i$介於此區間$[Lzd_1+1, Ld_1-1]$，則預測差值減一，修改預測差值，計算公式如下：

$$I1d_i^{'} = \begin{cases} I1d_i, if\ I1d_i = Pd_1 \mid I1d_i = Ld_1 \\ I1d_i + 1, if\ Pd_1 + 1 \le I1d_i \le Pzd_1 - 1 \\ I1d_i - 1, if\ Lzd_1 + 1 \le I1d_i \le Ld_1 - 1 \end{cases} \text{，} \tag{3.7}$$

經位移後產生之第一位移直方圖即為$H1D^{'}$。

【Step 11】嵌入機密資訊*Secret*1

欲將機密資訊*Secret*1嵌入預測差值影像*I1D*時，掃瞄預測差值影像，若預測

差值等於最高峰值Pd_1，且*Secret* 1值為 0 時，則預測差值不做改變；若預測差值等於最高峰值Pd_1，且*Secret* 1值為 1，則預測差值加一。若預測差值等於次高峰值Ld_1且*Secret*1值為 0 時，則預測差值不做改變；若預測差值等於次高峰值Ld_1且*Secret*1值為 1，則預測差值減一。設預測差值影像$I1D$之像素值為$I1d_i$，藏入後之預測差值$I1d_i^{'}$計算如下：

$$I1d_i^{'}=\begin{cases} I1d_i, if\ Secret1=0\ \&\ (I1d_i=Pd_1 \mid I1d_i=Ld_1) \\ I1d_i+1, if\ Secret1=1\ \&\ I1d_i=Pd_1 \\ I1d_i-1, if\ Secret1=1\ \&\ I1d_i=Ld_1 \end{cases}, \tag{3.8}$$

重複此步驟直到整張預測差值影像執行完畢為止。

【Step 12】製作第一階段偽裝影像*CI*

將預測差值影像製作成藏匿機密資訊的偽裝影像CI，利用預測差值$I1d_i^{'}$與相對應的原始像素b_i計算，假設偽裝影像像素值Cb_i，若預測差值$I1d_i^{'}$為雙峰值，則原始影像素值不變；若預測差值$I1d_i^{'}$介於區間$[Pd_1+1, Pzd_1-1]$之間，則原始影像像素值b_i加一，若預測差值$I1d_i^{'}$介於區間$[Lzd_1+1, Ld_1-1]$，則該原始像素值b_i減一，偽裝影像像素計算如公式如下：

$$Cb_i=\begin{cases} b_i, if\ (I1d_i^{'}=Pd_1 \mid I1d_i^{'}=Ld_1) \\ b_i+1, if\ Pd_1+1\le I1d_i^{'}\le Pzd_1-1 \\ b_i-1, if\ Lzd_1+1\le I1d_i^{'}\le Ld_1-1 \end{cases}, \tag{3.9}$$

此步驟計算完成後，得第一階段的偽裝影像CI。

【Step 13】修改預測差值產生第二位移直方圖*H2D'*

為隱藏機密資訊於預測差值影像$I3D$中，本步驟作法如 Step10，預測差值影像$I3D$所對應的直方圖$H2D$，須將預測差值直方圖最高峰點之右側與次高峰點之左側的像素分別位移一個單位，因此空下來的像素可以藏匿機密資訊。假設預測差值$I3d$介於區間$[Pd_2+1, Pzd_2-1]$，則預測差值加一；若預測差值$I3d$介於區間

$[Lzd_2+1, Ld_2-1]$，則預測差值減一，預測差值位移計算公式如下：

$$I3d_i^{'}=\begin{cases} I3d_i, if\ I3d=Pd_2 \mid I3d_i=Ld_2 \\ I3d_i+1, if\ Pd_2+1\le I3d_i\le Pzd_2-1 \\ I3d_i-1, if\ Lzd_2+1\le I3d_i\le Ld_2-1 \end{cases}, \tag{3.10}$$

經位移後產生之第二位移直方圖即為$H2D^{'}$。

【Step 14】嵌入機密資訊*Secret*2

將機密資訊*Secret*2嵌入預測差值陣列$I3D$時，作法如 Step11，掃瞄預測差值陣列$I3D$，若預測差值等於最高峰值Pd_2，且*Secret*2值為 0 時，則預測差值不做改變；若預測差值等於最高峰值Pd_2，且*Secret*2值為 1，則預測差值加一。若預測差值等於次高峰值Ld_2且*Secret*2值為 0 時，則預測差值不做改變；若預測差值等於次高峰值Ld_2且*Secret*2值為 1，則預測差值減一。設預測差值影像$I3D$之像素值為$I3d_i$，藏入後的預測差值$I3d_i^{'}$計算如公式 3.11。

$$I3d_i^{'}=\begin{cases} I3d_i, if\ Secret2=0\ \&\ (I3d_i=Pd_2 \mid I3d_i=Ld_2) \\ I3d_i+1, if\ Secret2=1\ \&\ I3d_i=Pd_2 \\ I3d_i-1, if\ Secret2=1\ \&\ I3d_i=Ld_2 \end{cases}, \tag{3.11}$$

重複此步驟直到整張預測差值陣列掃瞄完畢為止。

【Step 15】製作第二階段偽裝影像 *CI'*

假設偽裝影像CI'之像素值b'_i， 利用前一個原始像素b_i與本身預測差值$I3d_i^{'}$相減後可得偽裝像素值b'_i，將偽裝像素值依反向 S 型填補於偽裝影像CI'之區塊$b_{2,1}$位置，可得第二階段偽裝影像CI'如公式 3.12。

$$b_i^{'}=\begin{cases} b_1, i=1 \\ b_{i-1}-I3d_i^{'}, 2\le i\le T \end{cases}, \tag{3.12}$$

【Step 16】輸出檔頭資訊與偽裝影像

輸出檔頭資訊二對峰點資訊$(PH_1, Pd_1, PL_1, Ld_1, PH_2, Pd_2, PL_2, Ld_2)$與藏入浮水

印之偽裝影像CI'，檔頭資訊需利用索引表記錄傳送至接收方，此資訊可以為解開機密資訊的金鑰。

由於隱藏演算法之設計以影像區塊 2x2 大小當作預測，預測時會發生原始影像長寬大小不為二的倍數時，造成些微剩餘的像素不知如何進行預測以及藏匿動作，本方法考量剩餘之像素可用效率不大，因此若有此情形發生，剩下的像素不進行資訊隱藏運算，如此一來，除了可以解決此情況發生，保留原始像素又可維持良好的影像品質。

3.2 二階段直方圖位移之資料取出與還原

在浮水印之機密資訊取出與影像還原流程如同資料結構的後進先出方式，首要步驟是先將第二個預測差值直方圖的機密資訊取出並作影像部分還原，後來再擷取出第一個預測差值直方圖的機密資訊並作完整還原影像。機密資訊取出與影像還原流程如下:

【二階段直方圖位移之資訊取出與還原演算法】

輸入：偽裝影像，二對峰點資訊

輸出：原始影像，浮水印

【Step 1】偽裝影像切割

將一張大小為 M × N 偽裝影像 CI 切割成 $\{B_k \mid k = 1, 2, ..., T\}$ 個互不重疊且大小為 2x2 的區塊，每一區塊均有四個像素值，其中 $T = \frac{M \times N}{2 \times 2}$ 為總共的區塊數量。

【Step 2】反向 S 型搜尋區塊

本步驟為取出嵌入於第二個預測差值直方圖的機密資訊，針對影像區塊，以

反向 S 順序依序搜尋影像每一區塊中的$b_{2,1}$像素值，並將所有的$b_{2,1}$儲存於偽裝像素陣列CD，像素值為bc_i，$i=1,2,...,T$。

【Step 3】取機密資訊*Secret*2

利用峰值資訊，取出機密資訊以作為還原影像像素。為方便還原影像計算，設置三個緩衝陣列(Buffer array) *B1, B2* 與 *RC*，其中 *B1* 表偽裝預測差值陣列，*B2* 表還原預測差值陣列，*RC* 表還原影像陣列。*B1* 陣列儲存計算過程之原直方圖所隱藏資訊及像素位移資訊，*B2* 陣列儲存還原之實際差值，*RC* 陣列儲存還原影像之像素值。假設 $b1_i, b2_i$ 與 br_i 分別表示陣列 *B1*，*B2* 與 *RC* 之像素值，其中 $i=1, 2...,$，首先將偽裝像素值陣列 *CD* 中第一個像素為 bc_1 複製至陣列 *B1*，*B2* 與 *RC* 的第一個位置，如公式 3.13 所示。

$$b1_1 = b2_1 = br_1 = bc_1 \text{，} \tag{3.13}$$

在取出機密資訊過程中，利用 *RC* 陣列之前一像素值減去偽裝像素陣列 *CD* 之後一像素值，產生偽裝預測差值儲存於陣列 *B1* 中，計算如以下所示：

$$b1_i = br_{i-1} - bc_i \text{，} i=2,3,...,T \text{，} \tag{3.14}$$

利用偽裝預測差值判斷以取出機密資訊，若偽裝預測差值 $b1_i$ 為 Pd_2 或 Ld_2，表預測差值位於雙峰值處，即可取出機密資訊為$(0)_2$，並將偽裝預測差值 $b1_i$ 填入還原預測差值陣列，此時之還原預測差值等於偽裝預測差值，即 $b2_i = b1_i$。若偽裝預測差值 $b1_i$ 為 Pd_2+1 或 Ld_2-1，即表預測差值位於最高峰值加一或次峰值減一處，則可取出機密資訊$(1)_2$，並需將位移還原，即若偽裝預測差值 $b1_i$ 為 Pd_2+1，則還原預測差值 $b2_i = b1_i - 1$；若偽裝預測差值 $b1_i$ 為 Ld_2-1，則還原預測差值 $b2_i = b1_i + 1$。若偽裝預測差值 $b1_i =$ “$b1_i > Pd_2+1$”或“$b1_i < Ld_2-1$”，即表偽裝預測差值未嵌入機密資訊，但須位移予以還原，即若 $b1_i > Pd_2 + 1$，則 $b2_i = b1_i - 1$，若 $b1_i < Ld_2-1$，則 $b2_i = b1_i + 1$。機密資訊取出計算如下：

$$Secret2=\begin{cases}0, if\ b1_i = Pd_2 \mid b1_i = Ld_2\\ 1, if\ b1_i = Pd_2+1 \mid b1_i = Ld_2-1\end{cases}, \tag{3.15}$$

還原預測差值計算如下：

$$b2_i=\begin{cases}b1_i, if\ b1_i = Pd_2 \mid b1_i = Ld_2\\ b1_i-1, if\ b1_i \geq Pd_2+1\\ b1_i+1, if\ b1_i \leq Ld_2-1\end{cases}, \tag{3.16}$$

【Step 4】計算還原原始像素值

將還原影像陣列 RC 之前一個像素 br_{i-1} 減去還原預測差值 $b2_i$，即可求還原影像素值 br_i，如公式 3.17。

$$br_i = br_{i-1} - b2_i,\ i=2,3,...,T, \tag{3.17}$$

【Step 5】取機密資訊 *Secret*1 與區塊還原運算

在取出機密資訊 *Secret*1 時，針對每一偽裝影像區塊 $\{B_k \mid k=1,2,...,T\}$ 可還原出三個預測差值之機密資訊，此步驟與嵌入演算法的步驟 2 類似，然在計算順序是相反的。首先針對每一影像區塊之還原影像像素 br_i，$i=1,2,3,...,T$，作為各影像之 2×2 區塊 B_k 中 $b_{2,1}$ 像素值，即 $b_{2,1}=br$。假設偽裝影像之 2×2 區塊，其另三個像素值分別為 $b'_{1,1}$、$b'_{1,2}$ 與 $b'_{2,2}$，像素值 $b'_{1,2}$ 直接減去 $b_{2,1}$ 可求得預測差值 d'_3 如下：

$$d'_3 = b'_{1,2} - b_{2,1}, \tag{3.18}$$

利用預測差值運算即可取出機密資料 *Secret*1，計算如下：

$$Secret1=\begin{cases}0, if\ d'_i = Pd_1 \mid d'_i = Ld_1\\ 1, if\ d'_i = Pd_1+1 \mid d'_i = Ld_1-1\end{cases}, \tag{3.19}$$

還原成原始區塊像素 $b_{i,j}$ 之公式如下：

$$b_{i,j}=\begin{cases} b'_{i,j}, if\ d'_i = Pd_1 \mid d'_i = Ld_1 \\ b'_{i,j}-1, if\ d'_i \geq Pd_1+1 \\ b'_{i,j}+1, if\ d'_i \leq Ld_1-1 \end{cases}, \tag{3.20}$$

計算出$b_{1,2}$後，利用$b_{1,2}$與$b_{2,1}$求出預測差值d'_2，其中d'_2計算如下：

$$d'_2 = b'_{2,2} - \left\lceil \frac{b_{1,2}+b_{2,1}}{2} \right\rceil, \tag{3.21}$$

利用預測差值d'_2及公式 3.19 與 3.20 即可取出機密資料*Secret*1及計算原始區塊像素$b_{2,2}$。相同的，計算出$b_{1,2}$、$b_{2,1}$與$b_{2,2}$，即可求出預測差值d'_1，d'_1計算如下：

$$d'_1 = b'_{1,1} - median\{b_{1,2}, b_{2,1}, b_{2,2}\}, \tag{3.22}$$

利用預測差值d'_1及公式 3.19 與 3.20 即可取出機密資料*Secret*1及原始區塊像素$b_{1,1}$。將像素值$b_{1,1}, b_{1,2}, b_{2,1}$與$b_{2,2}$ 填回原始區塊即可還原完整區塊。

【Step 6】浮水印之機密資訊及原始影像還原計算

*Secret*1與*Secret*2取出之後，代表整個機密資訊已完全取出，將機密資訊重組，利用PH_1、PL_1、PH_2與PH_2之值加總即為浮水印大小，重新排列成原始浮水印機密資訊，即可輸出機密資訊與原始影像。

將還原資訊輸入至擷取與還原演算法即可萃取出機密資訊，取出機密的偽裝影像也可回復至原始影像。換句話說，接收方收到此機密影像與峰值資訊可進行機密資訊取出，首先取出第二個預測差值之直方圖機密資訊，再取出第一個預測差值直方圖機密資訊，組合兩個機密資訊即便完成取出動作。此外，利用峰點資訊將位移的像素進行還原，原始影像即可獲得，因此本法為可逆式影像資訊隱藏技術。

3.3 範例說明

為便於闡述說明，假設一張大小為 6×6 的原始灰階影像如圖 3-5，在嵌入過程需統計出兩個直方圖，第一個預測直方圖以區塊計算作為說明，因計算過程相同，以第一個區塊 K=1 當為計算範例，第二個預測直方圖以每個像素逐一做出說明。資料嵌入與取出說明如下所示：

3.3.1 資訊隱藏流程

為製作第一預測差值直方圖 $H1D$，以影像第一個區塊 K=1 當作範例說明，先計算區塊四個預測差值影像 $d_1 = b_{1,1} - median\{b_{1,2}, b_{2,1}, b_{2,2}\} = 4 - median\{5,3,4\} = 4-4 = 0$、 $d_2 = b_{2,2} - \lceil (b_{1,2}+b_{2,1})/2 \rceil = 4 - \lceil (5+3)/2 \rceil = 0$、$d_3 = b_{1,2} - b_{2,1} = 5-3 = 2$ 與 $d_4 = b_{2,1} = 3$，後續之區塊依序執行相同步驟，當所有區塊執行完畢可產出預測差值影像 $I1D$ 如圖 3-6(a)，並統計第一階段預測差值直方圖 $H1D$ 如圖 3-6(b)，依據直方圖，可得兩對峰點與零點，其峰點值與像素值分別為 $PH_1 = 13$、$Pd_1 = 0$、$ZH_1 = 0$、$Pzd_1 = 3$、 $PL_1 = 6$、 $Ld_1 = -1$、 $ZL_1 = 0$ 與 $Lzd_1 = -4$。

$b_{1,1}$	$b_{1,2}$	$b_{1,1}$	$b_{1,2}$	$b_{1,1}$	$b_{1,2}$
$b_{2,1}$	$b_{2,2}$	$b_{2,1}$	$b_{2,2}$	$b_{2,1}$	$b_{2,2}$
$b_{1,1}$	$b_{1,2}$	$b_{1,1}$	$b_{1,2}$	$b_{1,1}$	$b_{1,2}$
$b_{2,1}$	$b_{2,2}$	$b_{2,1}$	$b_{2,2}$	$b_{2,1}$	$b_{2,2}$
$b_{1,1}$	$b_{1,2}$	$b_{1,1}$	$b_{1,2}$	$b_{1,1}$	$b_{1,2}$
$b_{2,1}$	$b_{2,2}$	$b_{2,1}$	$b_{2,2}$	$b_{2,1}$	$b_{2,2}$

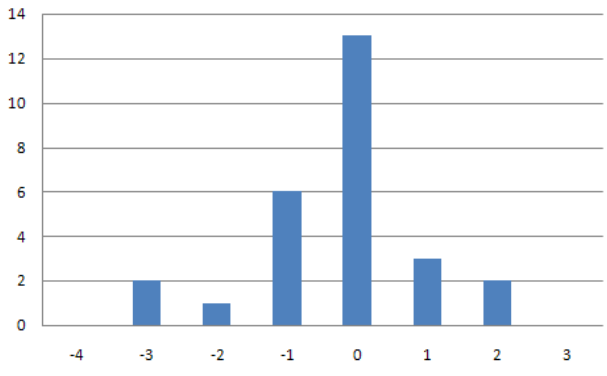
=

4	5	3	2	3	3
3	4	3	3	3	2
6	5	4	4	3	4
4	4	3	3	4	4
5	4	3	6	6	6
6	5	6	3	6	5

圖 3-5　原始影像位置對應

0	2	0	-1	0	0
3	0	3	0	3	-1
2	1	1	1	-1	0
4	-1	3	-1	4	0
0	-2	-3	0	0	0
6	0	6	-3	6	-1

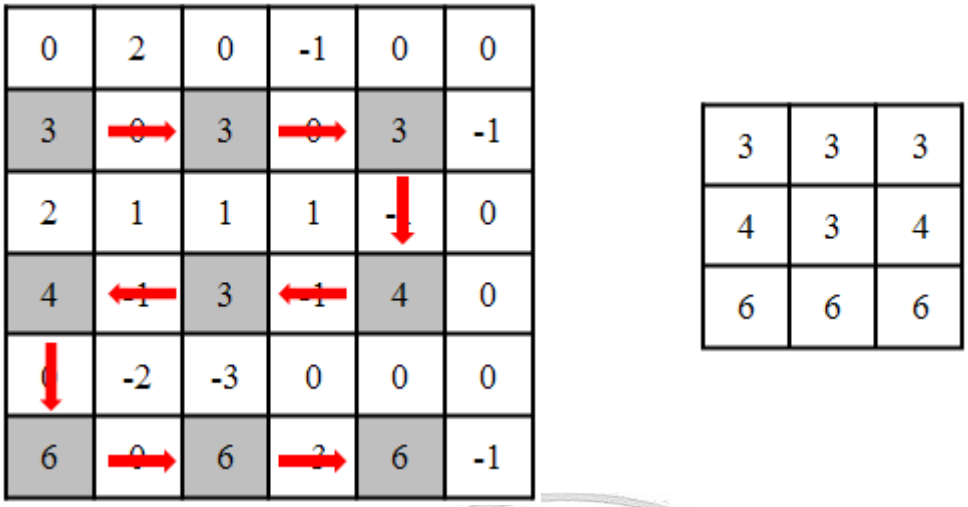
(a) *I1D*



(b) *H1D*

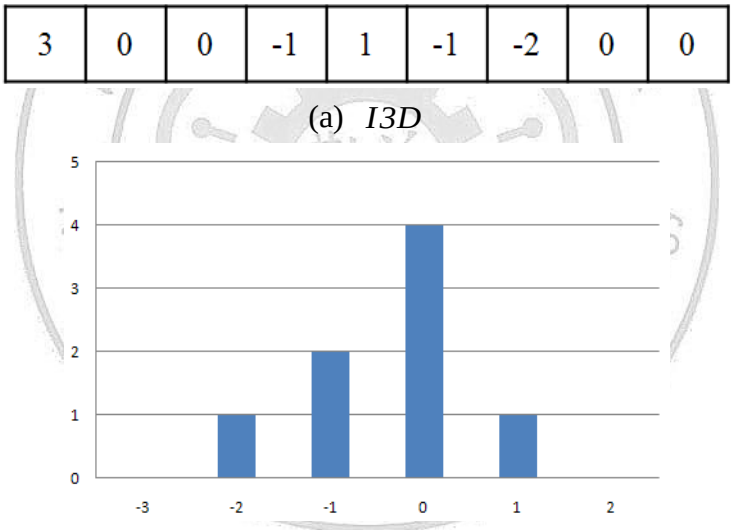
圖 3-6　第一階段預測差值直方圖

取得第一預測差值直方圖 *H1D* 後，計算第二預測差值直方圖 *H2D*，利用反向 S 型取出預測差值影像 *I1D* 每一區塊的 $b_{2,1}$ 像素如圖 3-7(a)，並放入縮減影像 *I2D* 中如圖 3-7(b)，並將 *I2D* 像素利用反向 S 型方式排列，計算成預測差值陣列 *I3D*，預測差值計算方式為 $I3d_1 = I2d_1 = 3$、$I3d_2 = I2d_1 - I2d_2$ =3 − 3=0、$I3d_3 = I2d_2 - I2d_3$ =3 − 3=0、…、$I3d_8 = I2d_7 - I2d_8$ =6 − 6=0、$I3d_9 = I2d_8 - I2d_9$=6−6=0，預測差值計算出後如圖 3-8(a)，並統計成第二預測差值直方圖 *H2D* 如圖 3-8(b)，根據直方圖，可得兩對峰點與零點，其峰點值與像素值分別為 $PH_2 = 4$、$Pd_2 = 0$、ZH_2 =0、Pzd_2=2、$PL_2 = 2$、$Ld_2 = -1$、ZL_2 =0 與 $Lzd_2 = -3$。



(a) *I1D* (b) *I2D*

圖 3-7 縮減影像



(a) *I3D*

(b) *H2D*

圖 3-8 第二階段預測差值直方圖

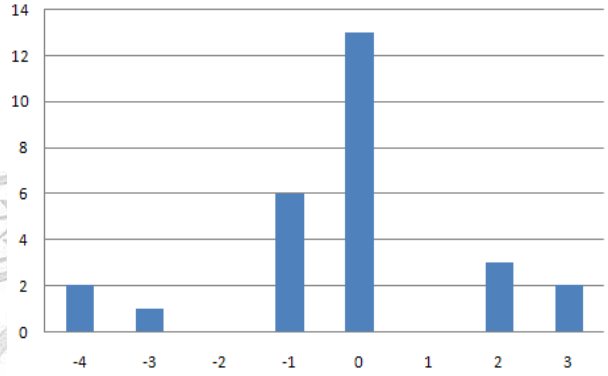
產生出兩個預測差值直方圖 *H1D* 與 *H2D* 後，計算藏入機密資訊的容量，$Total = PH_1 + PL_1 + PH_2 + PL_2 = 13 + 6 + 4 + 2 = 25$，*Secret*1 的嵌入量為 $NS_1 = PH_1 + PL_1 = 13+6 = 19$，*Secret*2 的嵌入量為 $NS_2 = PH_2 + PL_2 = 4+2 = 6$，假設浮水印機密資訊設為 $Secr = (10100011000111011000010101)_2$，*Secret*1 = $(10100011000111011000)_2$ 與 *Secret*2 =$(010101)_2$。

預測差值影像 *I1D* 經位移後產生位移差值影像 *I1D*' 如圖 3-9(a)，並統計成位

移直方圖 $H1D'$ 如圖 3-9(b)，假設欲嵌入機密資訊 $Secret1$，以第一個區塊 K=1 為例，因 $Secret1=1$ 且 $I1d_1=Pd_1$ 故 $Id1'_1=I1d_1+1=0+1=1$；因 $Secret1=0$ 且 $I1d_2=Pd_1$ 故 $I1d'_2=I1d_2=0$；因 $I1d'_3$ 不等於峰點，不嵌入資料，故 $I1d'_3=I1d_3$。後續的區塊依序執行相同步驟，直到所有區塊執行完畢可產出修改預測差值影像 $I1D'$ 如圖 3-10，其中灰色底表示有嵌入機密資訊。

0	3	0	-1	0	0
3	0	0	0	0	-1
3	2	2	2	-1	0
-1	-1	1	-1	-1	0
0	-3	-4	0	0	0
-2	0	0	-4	0	-1

(a) $I1D'$



(b) $H1D'$

圖 3-9　第一階段位移直方圖

1	3	1	-1	0	1
3	0	0	0	0	-2
3	2	2	2	-1	1
-1	-1	1	-1	-1	1
1	-3	-4	1	1	0
-2	0	0	-4	0	-1

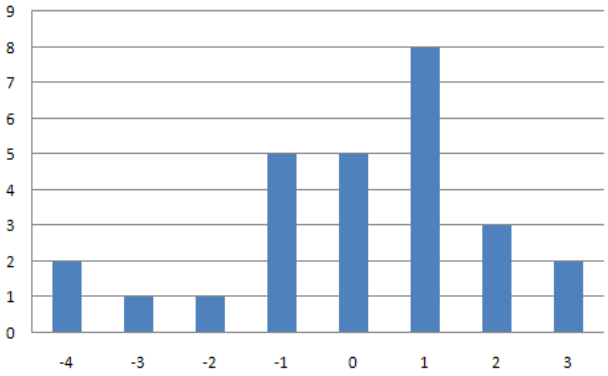


圖 3-10 嵌入機密資訊之差值影像 $I1D'$

在產生第一階段偽裝影像 CI 時，以第一區塊三個像素為例，因 $Pd_1+1\le Id1'_1\le Pzd_1-1$ 故 $Cb_1=b_1+1=4+1=5$；因 $Pd_1=Id1'_2$ 故 $Cb_2=b_2=4$；因 $Pd_1+1\le Id1'_3\le Pzd_1-1$ 故 $Cb_3=b_3+1=5+1=6$，後續區塊依序執行相同步驟，直

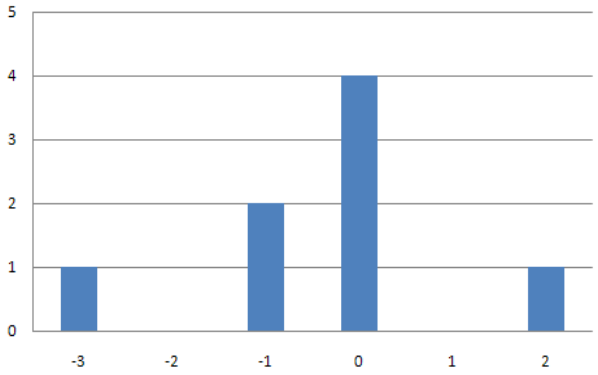
到所有區塊執行完畢可產出第一階段偽裝影像CI如圖 3-11。再者，欲產生第二階段偽裝影像時，將預測差值陣列$I3D$轉換產生位移差值$I3D'$如圖 3-12(a)，並統計成位移直方圖$H2D'$如圖 3-12(b)，計算位移與嵌入機密資訊$Secret2$時，其計算方式與第一階段預測差值計算相同，統計後的直方圖如圖 3-13，其中灰色預測差值像素表示嵌入機密資訊，製作出第二階段偽裝影像CI'如圖 3-14，其中$b_1'=3$，$b_2'=3-0=3$，$b_3'=3-1=2$，…，$b_8'=6-0=6$，$b_9'=6-1=5$，第二階段偽裝影像CI'如圖 3-14。

5	6	4	2	3	4
3	4	0	3	0	1
7	6	5	5	3	5
-1	4	1	3	-1	5
6	3	2	7	7	6
-2	5	0	2	0	5

圖 3-11 第一階段偽裝影像CI

3	0	0	-1	2	-1	-3	0	0

(a) $I3D'$



(b) $H2D'$

圖 3-12 第二階段位移直方圖

3	0	1	-1	2	-2	-3	0	1

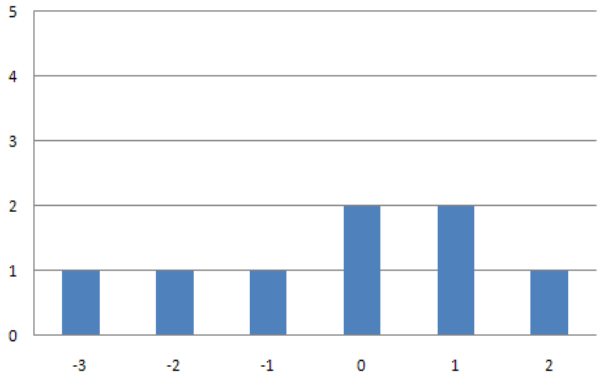


圖 3-13 嵌入機密資訊之差值影像 *I3D'* 與直方圖

5	6	4	2	3	4
3	4	3	3	2	1
7	6	5	5	3	5
5	4	2	3	4	5
6	3	2	7	7	6
7	5	6	2	5	5

圖 3-14 第二階段偽裝影像 *CI'*

3.3.2 機密資訊擷取與影像還原流程

在取出 *Secret*2 的運算程序時，先以反向 S 型順序依序搜尋影像每一區塊中的 $b_{2,1}$ 像素值，將所有區塊的 $b_{2,1}$ 儲存於偽裝像素陣列 *CD* 中，其像素值表示為 bc_i，並設置三個緩衝陣列(Buffer array) *B1, B2* 與 *RC*，分別表示偽裝預測差值陣列、還原預測差值陣列及原始像素陣列，其像素值分別表示為 $b1_i$、$b2_i$ 與 br_i，將偽裝像素值陣列 *CD* 中第一個像素為 bc_1 複製至陣列 *B1*, *B2* 與 *RC* 的第一個位置，即 $b1_1 = b2_1 = br_1 = bc_1 = 3$；計算偽裝預測差值儲存於陣列 *B1* 中，$b1_2 = br_1 - bc_2 = 3-3 = 0$，利用偽裝預測差值判斷 $b1_2 = Pd_2 = 0$，故取出機密資訊 $(0)_2$，儲存至還原預測差值陣列 *B2* 中，$b1_2 = Pd_2 = 0$，則 $b2_2 = b1_2 = 0$，再還原回

原始像素值為 RC，$br_2 = br_1 - b2_2 = 3-0=3$，後續的像素還原作法相同，重複執行所有像素，取出 $Secret2=(010101)_2$，還原原始像素陣列如圖 3-15。

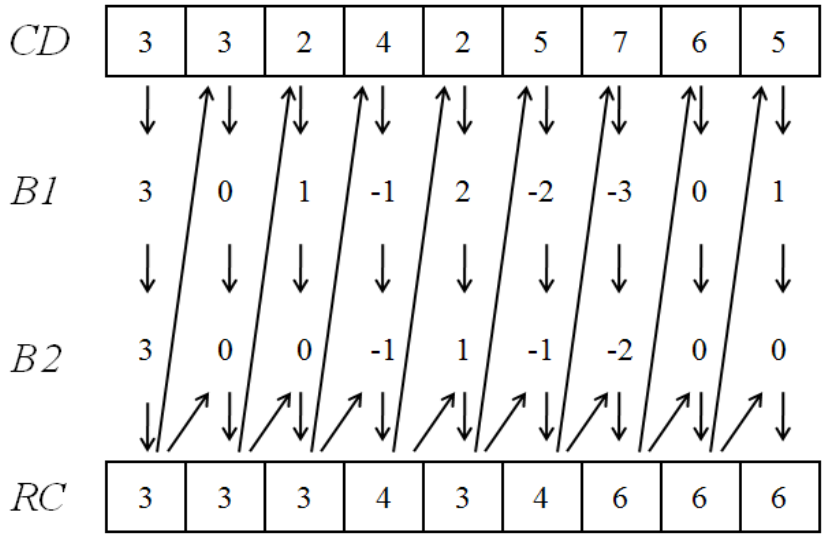


圖 3-15 第二階段還原示意圖

在取出 $Secret1$之計算程序時，偽裝影像之預測差值為 $d_3^{'} = b_{1,2}^{'} - b_{2,1} = 6-3=3$，公式 3.19 未成立，不需擷取資訊，故直接還原像素，利用公式 3.20 $d_3^{'} \geq Pd_1 + 1$，故 $b_{1,2} = b_{1,2}^{'} - 1 = 6-1 = 5$；偽裝影像之預測差值為 $d_2^{'} = b_{2,2}^{'} - \lceil (b_{1,2} + b_{2,1})/2 \rceil = 4 - \lceil (5+3)/2 \rceil = 0$，因 $d_2^{'} = Pd_1$，可取出機密資訊$(0)_2$，故還原影像像素 $b_{2,2} = b_{2,2}^{'} = 4$；偽裝影像之預測差值為 $d_1^{'} = b_{1,1}^{'} - median\{b_{1,2}, b_{2,1}, b_{2,2}\} = 5 - median\{5,3,4\} = 1$，$d_1^{'} = Pd_1 + 1 = 1$，可取出機密資訊$(0)_2$，因 $d_1^{'} \geq Pd_1 + 1$，故還原像素 $b_{1,} = b_{1,}^{'} - 1 = 5-1=4$。重複進行此計算，直到所有的區塊還原完成，可取出 $Secret1=(1010001100011101100)_2$，將兩機密資訊 $Secret1$ 與 $Secret2$ 組合，即 $Sec = Secret1 + Secret2$，形成一個浮水印機密資訊並還原成原始影像如圖 3-5。

藉由範例大小 6×6 的原始影像說明，以 2×2 大小切割成九個區塊，第一階段預測及差值直方圖統計以第一個區塊進行解說，第二階段則利用九個未被使用像素做出預測及直方圖運算，機密資訊為隨機產生的二進位資訊，直方圖經由位移

及嵌入資訊後，即可獲得偽裝影像。機密資訊擷取與還原時，首先設置三個陣列，擷取第二直方圖之機密資訊並可還原部分原始像素值，再者擷取與還原區塊內的三個像素，最後可得機密資訊與原始影像，這個簡單範例可以完整說明二階段直方圖位移之高容量可逆影像隱藏實作過程，也充分說明了本方法有效使用像素進行藏匿，嵌入時的像素變動性不大，達成容量與品質兼具的資訊隱藏法。

第四章 應用影像區塊眾數之高容量可逆式隱藏技術

本文將提出另一無失真資訊隱藏方法並以直方圖位移為基礎，由於第三章資訊隱藏技術容量稍嫌不足，因此本方法又提出不僅有效提高嵌入容量外，影像品質亦可維持一定水準的資訊隱藏技術，最主要的是利用索引表當作金鑰可增加其安全性。因此，本方法設計影像區塊眾數當成預測值，使直方圖預測差值之峰點值更為提高，嵌入容量也因此增加。在 4.1 節為區塊眾數之機密資訊隱藏演算法，設計原則為高隱藏資訊容量的情況下，亦能使偽裝影像維持良好品質。機密資訊擷取與還原影像演算法於 4.2 節提出，其目的為完整擷取藏匿於影像之機密資訊，亦可將偽裝影像還原回復至原始影像，且達到影像無失真的效果。4.3 節為本方法的範例實做，詳細隱藏、擷取與還原影像與實作如以下小節所述。

4.1 應用影像區塊眾數資訊隱藏技術

本方法再次利用影像鄰近像素具有相似性之特性，設計出一可回復式資訊隱藏技術，假設一張大小為 $M \times N$ 之影像 I，將影像 I 切割成不重疊之 3×3 區塊，以區塊當作一個運算單元，找出每一區塊出現最多次數之像素值，即為此區塊之眾數，利用眾數作為此一區塊預測值，區塊內每一像素值與預測值作相減運算，產生預測差值，紀錄區塊預測值於索引表中，為還原資訊使用。影像區塊由左至右、由上至下運算完成後，可得到預測差值影像 I'，統計預測差值影像之像素值可產生差值影像直方圖，找出直方圖之最高及次高峰點與其相對應之零點計有兩組，進行直方圖位移動作，並騰出空間來藏匿機密資訊。隱藏後再進行預測差值的轉換，也就是再以預測值對該區塊內像素做相減運算，產生偽裝影像，嵌入演算步驟如下：

【應用影像區塊眾數資訊隱藏演算法】

輸入：原始影像，浮水印

輸出：偽裝影像、峰點值、零點值、眾數索引表

【Step1】影像輸入與分割

輸入一灰階影像I，大小為M × N，將之切割為大小為 3×3 且互不重疊的區塊B_k，$\{B_k | k=1,2,...,T\}$，其中$T=\frac{M\times N}{3\times 3}$，即總共分割成 T 個區塊，如圖 4-1。

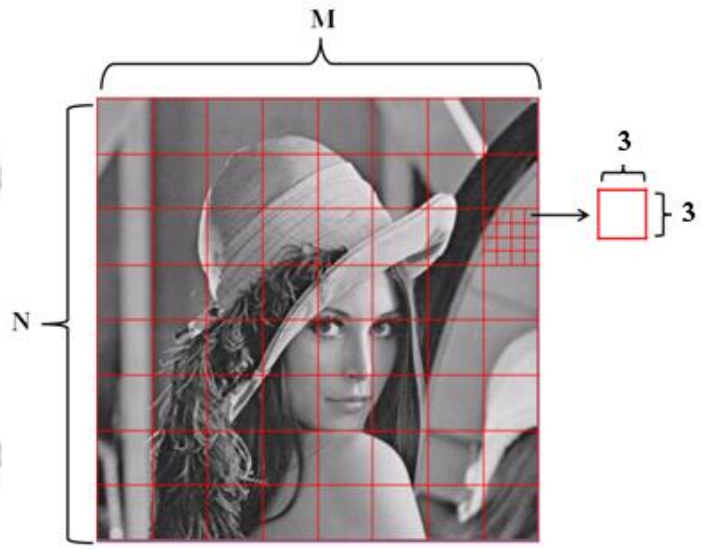


圖 4-1　影像切割

【Step2】計算區塊眾數並記錄

針對每個區塊B_k的九個像素值b_i，$\{b_i | i\in 1,2,...,9\}$，如圖 4-2 所示。將區塊B_k之像素值b_i統計計算，找尋$b_1,b_2,...,b_9$出現次數最多的像素值，即為區塊之眾數，設$mode$表示計算區塊之眾數函數，m_k表區塊眾數，計算如下式：

$$m_k=mode\ \{b_1,b_2,b_3,b_4,b_5,b_6,b_7,b_8,b_9\}\ ,\qquad (4.1)$$

將所有區塊眾數$\{m_k | k=1,2,...,T\}$，$T=\frac{M\times N}{3\times 3}$，依序儲存並製作成一索引表$MT$，此索引表可用來當作隱藏時的預測值，且在還原時當作取出機密的金鑰使用。

b_1	b_2	b_3
b_4	b_5	b_6
b_7	b_8	b_9

圖 4-2　區塊像素值

【Step3】計算預測差值影像

對每個區塊B_k，$k=1,2,...,T$，取出其區塊預測值，即為眾數m_k，計算區塊眾數與各個像素值之差值，產生預測差值，設區塊B_k之預測差值d_i，$i=1,2,...,9$，其中d_i值滿足$-255 \le d_i \le 255$，預測差值計算如公式(4-2)。

$$d_i = m_k - b_i, \quad i=1,2,...,9, \tag{4.2}$$

計算完成每個區塊之預測差值並儲存成一大小為$M \times N$之陣列D，即產生預測差值影像D。

【Step4】統計預測差值影像之直方圖

計算預測差值影像D之預測差值d_i出現的次數，統計並繪製成預測差值直方圖HD。

【Step5】直方圖之峰點與零點取出並記錄

尋找預測差值影像直方圖HD之兩對峰點與零點，從直方圖中找出預測差值之正數群組（$0 \le d_i \le 255$）與負數群組（$-255 \le d_i \le -1$）中各一對峰點與零點，其中直方圖中的峰點是指預測差值出現最多次數的像素值；零點則代表第一個預測差值出現次數為零的像素值。直方圖峰點說明如圖 4-3，直方圖HD之正數群組中峰點的像素值PH=0，出現次數為 12，零點像素值為PZ=3，出現次數為 0；負數群組的峰點為NH=-1，出現次數為 8，零點為NZ=-4，出現次數為 0。取出PH、PZ、NH、NZ後，要將此資訊記錄下來，以作為擷取機密資訊時使用。

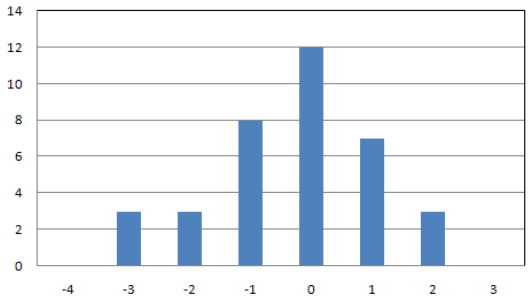


圖 4-3　預測差值之直方圖 HD

【Step6】計算位移影像及直方圖位移

為了要藏入機密資訊於兩對峰點中，須要將峰點與零點之間的預測差值分別往左與右各位移一位元，即預測差值像素值 d_i 介於區間 $[PH+1, PZ-1]$，則預測差值加一，即 $d_i = d_i + 1$；另一方面，若預測差值 d_i 介於此區間 $[NZ+1, NH-1]$，則預測差值減一，即 $d_i = d_i - 1$。經由位移後，空出的兩個位置 $PH+1$ 與 $NH-1$，將可作為藏入機密資訊使用。預測差值像素值計算公式(4.3)。

$$d_i' = \begin{cases} d_i, if\ d_i = PH \mid d_i = NH \\ d_i + 1, if\ PH + 1 \le d_i \le PZ - 1 \\ d_i - 1, if\ NZ + 1 \le d_i \le NH - 1 \end{cases}, \quad (4.3)$$

位移直方圖說明如圖 4-4，預測差值像素值 d_i 在區間[1,2]中，預測差值加一，$d_i = d_i + 1$，即右移一個單位；預測差值 d_i 在區間[-3,-2]中，預測差值減一，$d_i = d_i - 1$，即左移一個單位，即可得預測差值的位移影像 D'，及其位移直方圖 HD'。

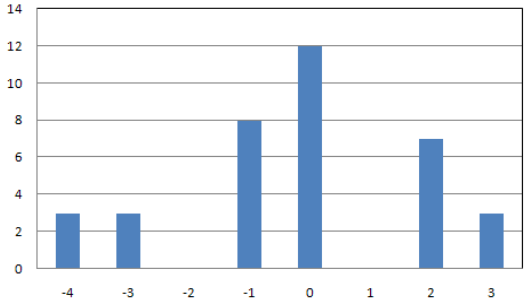


圖 4-4　預測差值之位移直方圖 HD'

【Step7】隱藏機密資訊

設一機密資訊 *Secret* 表示為二進位資訊，欲將 *Secret* 藏入位移差值影像 D' 中，首先要掃描整個位移差值影像，若其像素值 d_i' 等於正數峰點值 PH 或負數峰點值 NH ，且藏入機密資訊值為$(0)_2$，則像素值不變；如果要藏入機密資訊為$(1)_2$ 時，則正數峰點值加一，即 $d_i' = d_i' + 1$，負數峰點值減一，即 $d_i' = d_i' - 1$，藏入資訊後的像素值 d_i'' 計算如公式(4.4)。

$$d_i'' = \begin{cases} d_i', if\ Secret = 0 \,\&\, (d_i' = PH \mid d_i' = NH) \\ d_i' + 1, if\ Secret = 1 \,\&\, d_i' = PH \\ d_i' - 1, if\ Secret = 1 \,\&\, d_i' = NH \end{cases}, \tag{4.4}$$

重複此步驟直到機密資訊完全藏入為止，完成隱藏機密資訊後的嵌入影像 D''。

【Step8】製作偽裝影像

依據藏入機密資訊影像 D'' 製作成偽裝影像 I'，此步驟將影像 D'' 切割成大小為 3×3 且不重疊的區塊，讀取索引表 MT 找尋區塊 B_k 所對應的預測值 m_k ，並以此眾數 m_k 減去區塊內各個像素值 d_i'' ，計算如公式(4.5)。

$$b_i' = m_k - d_i'' , \tag{4.5}$$

重複此步驟將所有的位移差值製作成偽裝影像之像素值，即可得到藏有機密資訊的偽裝影像 I'。

【Step 9】輸出檔頭資訊與偽裝影像

輸出檔頭資訊（Head information）二對峰值 (PH, NH, PZ, NZ)、眾數索引表 (MT)與藏入浮水印之偽裝影像 I'，檔頭資訊需利用索引表記錄傳送至接收方，此資訊可以為解開機密資訊的金鑰。

隱藏演算法設計上，利用大小 3×3 影像區塊當作預測，將會與二階段直方圖位移技術產生類似問題，當影像大小 M,N 非 3 的倍數時，造成剩餘像素不知該如

何進行嵌入計算，因此若有相同情形發生，剩下的像素本研究不進行像素預測與產生差值統計直方圖運算。再者，區塊內可能會統計出多個相同次數的眾數，預測值不知該如何抉擇時，本方法利用數值最小的眾數當作預測，如此一來，隱藏的混淆的情況將不會發生。

4.2 應用影像區塊眾數資訊取出與影像還原

為取出偽裝影像之機密資訊時，首先要取出峰點值、零點值與眾數索引表，以還原回完整的機密資訊及無失真之原始影像，機密資料的取出與影像還原的程序，可視為藏入資訊的反向流程，擷取出機密資訊與回復原始影像流程。機密資訊擷取與還原影像演算法敘述如下：

【應用影像區塊眾數資訊取出與影像還原演算法】

輸入：偽裝影像、峰點值、零點值、眾數索引表

輸出：原始影像，浮水印

【Step1】輸入偽裝影像

輸入一張大小為 $M \times N$ 且已藏有機密資訊之偽裝影像 I，並讀取眾數索引表 MT、檔頭資訊之峰點值與零點值 (PH, NH, PZ, NZ)。

【Step2】影像分割

將輸入之偽裝影像 I 切割成 B_k 個大小為 3×3 且不重疊的區塊，其中 $\{B_k \mid k = 1,2,...,T\}$，且 $\mathrm{T} = \dfrac{M \times N}{3 \times 3}$，總共可分割成 T 個區塊數量，每個區塊 B_k，$\{b_i \mid i \in 1,2,...,9\}$ 均有九個像素值。

【Step3】計算預測差值影像

將每個區塊進行預測編碼的演算，首先依序掃描區塊 B_k，並讀取索引資訊 MT 所對應之區塊參照值 m_k，將參照值減去該區塊內之像素值 $b_i, i = 1,2,...,9$，得到預

測差值 $d_i, i=1,2,...,9$，計算所有區塊 B_k，$k=1,2,...,T$ 之預測差值後，即產生預測差值影像 D，區塊預測差值之像素值 d_i 計算公式如下：

$$d_i = m_k - b_i \text{，} \quad i=1,2,...,9 \text{，} \tag{4.6}$$

【Step4】統計預測差值影像之直方圖

計算預測差值影像 D 之直方圖，統計預測差值影像之像素值 d_i 出現的次數，繪製成預測差值影像之直方圖 HD，預測差值像素值 d_i，$d_i \in D$，其中預測差值會介於-255 至 255 之間，即 $d_i \in \{-255,-254,...,255\}$ 。

【Step5】取出機密資訊

取出預測差值之正數群組（$0 \le d_i \le 255$）與負數群組（$-255 \le d_i \le -1$）中之峰點 PH、NH 資訊，計算機密資訊 *Secret* 及還原影像像素值。依序掃描整張預測差值影像 D，讀取像素值 d_i，若 $d_i = PH \text{ or } NH$，則取出所藏入之機密資訊 *Secret*=$(0)_2$，像素值保持不變動；另一方面，若 $d_i = PH+1$ 或 $d_i = NH-1$，則取出之機密資訊 *Secret* 為 1，且將該像素值 d_i 回復成預測峰點值 $d_i = PH$ 或 $d_i = NH$，其他之像素值則表示沒有藏入任何機密資訊，該像素值不做任何改變。還原預測差值之像素值及取出機密資訊公式如下：

$$d'_i = \begin{cases} d_i, if\ d_i = PH \mid d_i = NH \\ PH, if\ d_i = PH+1 \\ NH, if\ d_i = NH-1 \end{cases} \text{，} \tag{4.7}$$

$$Secret = \begin{cases} (0)_2, if\ d_i = PH \mid d_i = NH \\ (1)_2, if\ d_i = PH+1 \mid d_i = NH-1 \end{cases} \text{，} \tag{4.8}$$

重複執行上述步驟直到全部機密資訊取出為止，並還原的預測差值影像 D'。將所取出之機密資訊依順序排列，即可得到傳送端所藏入之完整機密資訊 *Secret*。

【Step6】位移直方圖以復原預測差值

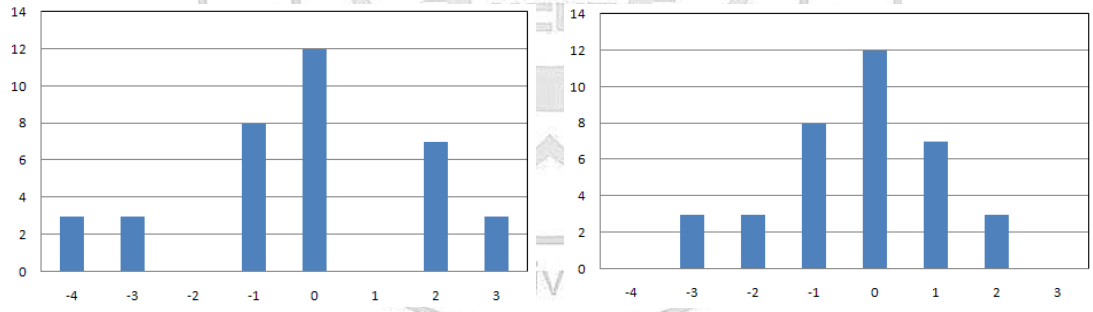
利用峰點與零點資訊作為復原預測差值使用，將正數群組（$0 \le d_i \le 255$）與

負數群組（$-255 \le d_i \le -1$）的峰點與零點之間的像素分別向左位移及向右位移一位元，即預測差值像素 d'_i 介於此區間 $[PH+1, PZ]$，則預測差值減 1，即 $d''_i = d'_i - 1$；另一方面，若預測差值像素 d'_i 介於此區間 $[NZ, NH-1]$，則預測差值加 1，$d''_i = d'_i + 1$，其位移預測差值公式如下：

$$d''_i = \begin{cases} d'_i, if\ d'_i = PH \mid d'_i = NH \\ d'_i - 1, if\ PH+1 \le d'_i \le PZ \\ d'_i + 1, if\ NZ \le d'_i \le NH-1 \end{cases}, \quad (4.9)$$

經由位移後，可得預測差值影像 D''，及對應之直方圖 HD'。

以圖 4-5(a)說明，假設得到的正數群組的預測差值直方圖峰點為 $PH=0$、零點為 $PZ=3$；負數群組的預測差值直方圖峰點為 $NH=-1$、零點為 $NZ=-4$，即在直方圖正數區間[1,3]中，像素值減一位元，即向左位移一單位；在直方圖負數區間[-2,-4]中，像素差值加 1，即向右位移一個單位，之後產生還原位移之預測差值直方圖如圖 4-5(b)。



(a) (b)

圖 4-5 取出機密資訊之直方圖與還原直方圖位移

【Step7】還原原始影像

將預測差值影像還原回原始影像，需對整張預測差值影像 D'' 做預測編碼的演算，將影像 D'' 切割成大小為 3×3 且不重疊的區塊，依序選取區塊 B_k，$k=1,2,...,T$ 及讀取區塊預測眾數 m_k，$k=1,2,...,T$，並將該區塊之眾數參照值 m_k 減去區塊內所有像素值 $d''_i, i=1,2,...,9$，計算如下：

$$b_i = m_k - d''_i, \ i=1,2,...,9, \quad (4.10)$$

依序將每個區塊內之像素值完成還原編碼，即可回復為無失真之原始影像。

在資訊取出及還原流程中，只須將還原資訊輸入於演算法中，當接收方收到偽裝影像、索引表與峰值資訊可進行機密資訊取出，擷取資訊為隱藏的反向流程，機密資訊取出後，位移差值需回復成原始差值，將預測值減去原始差值即可取得原始影像，且為無失真之原始影像。因此，本方法為一可逆式資訊隱藏技術。

4.3 範例說明

為說明隱藏及擷取程序流程，假設原始影像 I 其大小為 6×6 的矩陣，如圖 4-6(a)，利用本文所設計之隱藏演算法將一機密資訊 *Secret* 藏入影像，隱藏程序敘述如 4.3.1 與擷取程序如 4.3.2。

4.3.1 機密資訊隱藏流程

將原始影像 6×6 分割成大小為 3×3 且不重疊之區塊 B_k，$k=1,2,3,4$，找出每個區塊內的眾數 m_k，$k=1,2,3,4$ 當做預測值並且記錄成索引表 MT 如圖 4-6(b)。

2	5	3	1	3	3
2	1	4	1	2	5
3	1	2	2	2	5
1	3	2	4	2	2
5	3	3	4	3	5
4	4	5	4	3	5

(a)

k	m_k
1	2
2	2
3	3
4	4

(b)

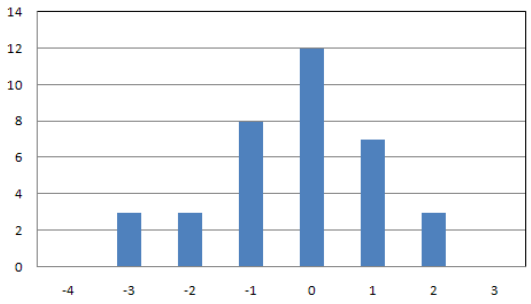
圖 4-6　原始影像與索引表

計算預測差值影像 D 時，將預測值 m_k 減去區塊內各個像素值 b_i，$i=1,2,...,9$，產生預測差值 d_i，$i=1,2,...,9$，以第一個區塊 B_1 說明，區塊 B_1 之預測值即眾數 $m_1=2$，針對區塊內 9 個像素值進行相減運算，區塊 B_1 之預測差值 $d_i=m_k-b_i$ 計算如下：$d_1=2-2=0$、$d_2=2-5=-3$、$d_3=2-3=-1$、$d_4=2-2=0$、$d_5=2-1=1$、$d_6=2-4=-3$、$d_7=2-3=-1$、$d_8=2-1=1$、$d_9=2-2=0$。依序執行完四個區

塊之預測差值計算，形成一張預測差值影像 D 如圖 4-7(a)所示。計算預測差值影像 D 之像素值出現次數，並統計輸出直方圖，即差值影像之直方圖 HD，如圖 4-7(b)。

0	-3	-1	1	-1	-1
0	1	-2	1	0	-3
-1	1	0	0	0	-3
2	0	1	0	2	2
-2	0	0	0	1	-1
-1	-1	-2	0	1	-1

(a)



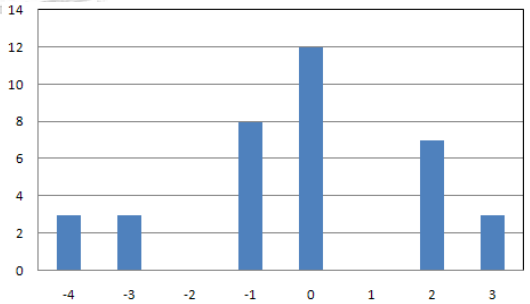
(b)

圖 4-7　預測差值影像與預測差值之直方圖

統計預測差值影像之直方圖後，從正數群組之預測差值和負數群組之預測差值中各找尋一對峰點值與零點值，由圖 4-7(a)可得知正數群組預測差值之峰點像素值 $PH=0$、零點像素值 $PZ=3$；負數群組預測差值之峰點像素值 $NH=-1$、零點像素值 $NZ=-4$。本方法利用峰點像素出現較高之次數予以將隱藏機密資訊於峰點中。為隱藏機密資訊，將正數與負數兩群組之峰點與零點間的預測差值分別往右與左各位移一位元，即在正數群組區間[1,2]中，預測差值加一，即向右位移一個單位；在負數群組區間[-3,-2]中，預測差值減一，即向左位移一個單位，產生預測差值的位移影像 D'，如圖 4-8(a)，及其位移直方圖 HD'，如圖 4-8(b)。

0	-4	-1	2	-1	-1
0	2	-3	2	0	-4
-1	2	0	0	0	-4
3	0	2	0	3	3
-3	0	0	0	2	-1
-1	-1	-3	0	2	-1

(a)



(b)

圖 4-8　預測差值位移影像與位移直方圖

欲將機密資訊 *Secret* 隱藏於預測差值位移影像中，假設機密資訊為 $Secret=(10101010111001100000)_2$，掃描整張預測差值影像圖 4-8(a)，由左到右，從上至下，當藏入機密資訊 *Secret* 為 $(1)_2$ 時，若預測差值像素值 $d_i^{'}=PH$，則 $d_i^{''}=d_i^{'}+1$；若 $d_i^{'}=NH$，則 $d_i^{''}=d_i^{'}-1$，如圖 4-9(a)紅色的差值；當藏入機密資訊 *Secret* 為 $(0)_2$ 時，若預測差值像素值 $d_i^{'}=PH$ 或 $d_i^{'}=NH$ 時，則 $d_i^{'}$ 維持不變，其他不等於 PH、NH 之像素值 $d_i^{'}$ 也保持不變動，藏入機密資訊後之嵌入影像 $D^{''}$ 如圖 4-9(a)。將藏有機密資訊預測差值影像與索引表之預測值運算，即可求得到一張完整且藏有機密資訊之偽裝影像，其中計算是將影像 $D^{''}$ 切割成3×3不重疊之區塊，並依影像區塊 B_k，k=1,2,3,4，順序找尋索引表 MT 之預測值 m_k， k=1,2,3,4 作相減運算，即 $b_i^{'}=m_k-d_i^{''}$，$i=1,2,...,9$，即可產生一張藏有機密資訊的偽裝影像，如圖 4-9(b)。

1	-4	-1	2	-2	-1
1	2	-3	2	0	-4
-2	2	0	1	1	-4
3	1	2	0	3	3
-3	0	1	1	2	-1
-1	-1	-3	0	2	-1

(a)

1	6	3	0	4	3
1	0	5	0	2	6
4	0	2	1	1	6
0	2	1	4	1	1
6	3	2	3	2	5
4	4	6	4	2	5

(b)

圖 4.9　嵌入機密之差值影像與偽裝影像

4.3.2 機密資訊擷取與影像還原流程

影像擷取過程中，假設一張已藏有機密資訊之偽裝影像，取出其檔頭資訊，包含有峰點值、零點值、機密資訊長度大小及索引表，經由檔頭資訊還原成原始影像。

首先輸入一張已藏有機密資訊偽裝影像 I，如圖 4-10(a)，將影像切割成3×3大小且不重疊之區塊 B_k，k=1,2,3,4，進行預測差值演算，將索引表之預測值 m_k，k=1,2,3,4 與對應區塊之像素值 b_i，$i=1,2,...,9$，作相減運算，預測差像素值

$d_i = m_k - b_i$ ，$i=1,2,...,9$，對每個區塊相減完後，即得到一張預測差值影像 D，如圖 4-10(b)。

1	6	3	0	4	3
1	0	5	0	2	6
4	0	2	1	1	6
0	2	1	4	1	1
6	3	2	3	2	5
4	4	6	4	2	5

(a)

1	-4	-1	2	-2	-1
1	2	-3	2	0	-4
-2	2	0	1	1	-4
3	1	2	0	3	3
-3	0	1	1	2	-1
-1	-1	-2	0	2	-1

(b)

圖 4.10 偽裝影像與嵌入機密之差值影像

統計預測差值影像 D，計算差值像素值出現次數，產生一預測差值之直方圖 HD 方式，如圖 4-11。

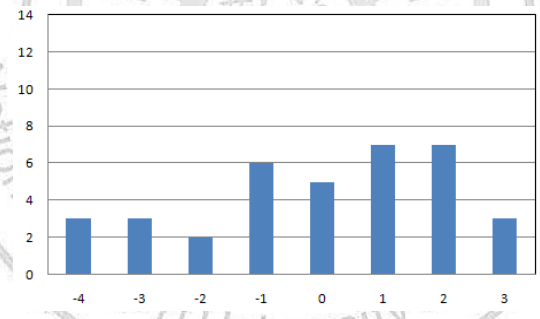
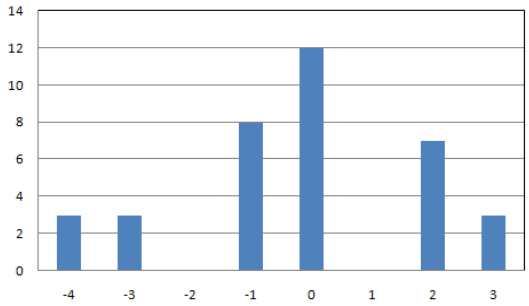


圖 4-11 預測差值之直方圖 HD

利用峰點 PH、NH 資訊取出機密資訊及還原影像像素值，由檔頭資訊得知 $PH=0$ 、 $NH=-1$。依序掃描整張預測差值影像 D ，讀取像素值 d_i ，若 $d_i = PH \ or \ NH$，則取出所藏入之機密資訊 $Secret=(0)_2$，像素值保持不變動；若 $d_i = PH+1$ 或 $d_i = NH-1$，則取出之機密資訊 $Secret$ 為 $(1)_2$，且將該像素值 d_i 回復成預測峰點值 $d_i' = d_i - 1 = PH$ 或 $d_i' = d_i + 1 = NH$，其他之像素值則表示沒有藏入任何機密資訊，該像素值不做任何改變，還原的預測差值影像 D'，取出機密資訊後之影像如圖 4-12(a)。

0	-4	-1	2	-1	-1
0	2	-3	2	0	-4
-1	2	0	0	0	-4
3	0	2	0	3	3
-3	0	0	0	2	-1
-1	-1	-3	0	2	-1

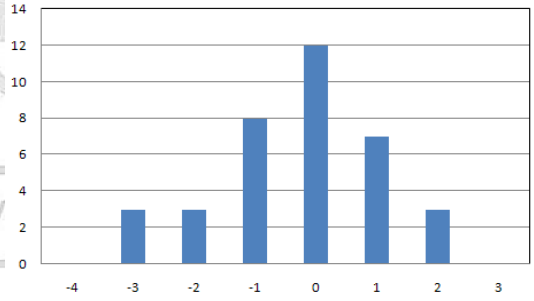


(a) (b)

圖 4-12 取出機密之預測差值影像 D' 與直方圖

將機密資訊取出之後，預測差值影像直方圖如圖 4-12(b)，利用已知峰點 $PH=0$ 、$NH=-1$，零點 $PZ=3$ 、$NZ=-4$ 進行位移直方圖，即將正數群組與負數群組之峰點與零點間的預測差值分別往左與右各位移一位元，在直方圖正數群組區間[1,3]中像素值減 1，$d_i''=d_i'-1$ ，即向左位移一單位；在直方圖負數群組區間[-4,-2]中，像素差值加 1，$d_i''=d_i'+1$ ，即向右位移一個單位，產生還原位移之預測差值影像如圖 4-13(a)，而位移還原之預測差值直方圖如圖 4-13(b)。

0	-3	-1	1	-1	-1
0	1	-2	1	0	-3
-1	1	0	0	0	-3
2	0	1	0	2	2
-2	0	0	0	1	-1
-1	-1	-2	0	1	-1



(a) (b)

圖 4-13 還原位移之預測差值影像與直方圖

最後將各區塊預測值 m_k ， k=1,2,3,4，與位移後影像區塊像素值 d_i ，i=1,2,…,9，作相減運算，即 $b_i=m_k-d_i''$ ，i=1,2,…,9，即可回復成原始影像且像素值並無失真，如圖 4-14。

2	5	3	1	3	3
2	1	4	1	2	5
3	1	2	2	2	5
1	3	2	4	2	2
5	3	3	4	3	5
4	4	5	4	3	5

圖 4-14 原始影像

本範例詳細描述隱藏、擷取資訊及還原影像的實作，利用大小 6×6 的原始影像矩陣說明，以 3×3 大小切割成 4 個區塊，其預測值為 4 個區塊眾數，該區塊眾數減去區塊內像素可能預測差值，之後就可以進行藏匿秘密資訊流程，此外索引表需要記錄當作還原資訊的金鑰。欲獲得機密資訊與還原影像時，偽裝影像及索引表輸入演算法，經過七個步驟萃取與還原運算即可完成。由簡單範例說明了應用影像區塊眾可逆隱藏演算流程與實作相符，達成以高容量且可逆式為設計概念的資訊隱藏技術。

第五章 動態矩陣機密資訊隱藏技術

本章節提出動態矩陣機密資訊隱藏技術，由於資訊隱藏技術需提升大量容量又不失其影像品質，本方法利用動態矩陣隱藏大幅提升前兩章直方圖修改之資訊隱藏技術的容量，影像品質也較第三、四章的隱藏技術更為良好。此技術不僅考量資訊隱藏後的安全性，還可以提升隱藏容量與保持藏入後的影像品質，最主要設計屬於可逆式資訊隱藏技術，除了可以取出隱藏的機密浮水印資訊，尚可將偽裝影像還原成原始影像。在 5.1 節為資訊隱藏流程，利用亂數設計一個小型的動態矩陣，將動態矩陣對應影像餘數進行修改像素值完成藏匿流程。5.2 節為資訊取出與還原，機密餘數影像透過動態矩陣的對應萃取出機密資訊，再利用最初的餘數影像與機密餘數影像將偽裝影像回復至原始影像。5.3 節為本方法的範例說明，詳細的資訊隱藏、擷取與影像還原流程時做如以下小節所述。

5.1 動態矩陣資訊隱藏

本方法利用動態矩陣進行機密資訊的隱藏，首先設計一動態矩陣，利用二個亂數產生大小 3×3 的矩陣，其中亂數一為決定動態矩陣中心值，利用中心值遞增並順時針方向排列於矩陣邊緣，亂數二為決定矩陣邊緣排列起始位置。輸入一張原始影像，將原始影像轉換成一張餘數影像 *REMI* ，隱藏資訊時，先將浮水印利用亂數三轉換成雜亂無章的資訊，將此資訊進行轉換為二進制，再以六個位元為一組，轉換成兩個九進制值，而該值為矩陣中的值，X 與 Y 軸決定該矩陣中的值，因此要找出機密資訊對應位置產出機密餘數影像 *NREMI* ，最後要將餘數影像與機密餘數影像進行藏入判斷並藏入資料，藏入完成後將產出偽裝影像以及影像還原資訊。動態矩陣機密資訊隱藏演算法說明如下。

【動態矩陣機密資訊隱藏演算法】

輸入：原始影像，機密資訊

輸出：偽裝影像，餘數影像，*random1*， *random2* 與 *random3*

【Step 1】產生動態矩陣

本系統利用兩個亂數產生一動態矩陣，其亂數為整數目的為產生 0 到 9 的數值，設大小為 3×3 之矩陣 MT ，$MT=\left\{m_{i,j}\left|m_{i,j}\in 0,1,2...,8\right.\right\}, 0\le i,j\le 2$ ，其中 $m_{i,j}$ 值皆不相等。首先，系統產生一亂數種子 *random1*，計算矩陣中心值 $m_{1,1}$ ，$m_{1,1}$ = *random1* mod 9，其 mod 為餘數計算函數，如圖 5-1 矩陣位置 (1,1)，編號為 0，此亂數功能為決定動態矩陣中心值。其次再利用第二個亂數種子 *random2* 決定排列矩陣之起始邊緣位置 $d=random2 \bmod 9$，如圖 5-1 編號 1,2,…,8 邊緣位置，計算起始的邊緣位置值 $m_{i,j}$ ，$i,j\neq 1$，其他邊緣位置值以順時針遞增方式排列，即 $m_{i,j}=m_{i,j}+1$，若排列值為 8，則回到 0 開始再遞增排列，最後形成一動態矩陣。

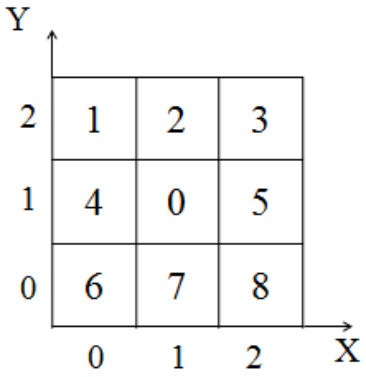


圖 5-1　動態矩陣之位置

【Step 2】輸入原始影像

輸入一張灰階原始影像 $I_{x,y}$ ，其中 $x\in\{1,2,...,M\}$ ， $y\in\{1,2,...,N\}$ ，此影像要當作藏匿資訊的載體又稱負載影像。

【Step 3】產生餘數影像並分組

將負載影像由左至右從上到下掃描，每一個像素值皆除 3，所有餘數存成餘數影像 *REMI*，此影像矩陣可為後續演算流程之判斷及影像還原功能。在餘數影像 *REMI* 中，以四個像素為一組，總共有 $\frac{M \times N}{4}$ 組，每組四個像素數為 rem_i，$rem_i \in \{0,1,2\}$，其中 $1 \le i \le 4$，以 rem_1 與 rem_2 兩個像素為一組作為 X 與 Y 軸查詢對應之動態矩陣值，相同的，像素 rem_3 與 rem_4 為一組，亦產生對應動態矩陣值。

【Step 4】機密資訊利用亂數擬亂

輸入浮水印機密資訊，利用亂數種子 *random3* 擬亂浮水印資訊，即是將完整的浮水印資訊轉換為雜亂無章的資訊，讓有心想取出機密資訊的非法人士無法得知機密訊息的內容。

【Step 5】機密資訊轉換

將打亂後的浮水印資訊轉換成二進制資料，再轉換為九進制資料。首先，將機密資訊以二進制 6 bits 為一組，每一組位轉換成兩個九進制的機密資訊值{t1, t2}，此二個值當為動態矩陣值，分別找尋其對應動態矩陣 X 與 Y 軸之值。

【Step 6】尋找機密資訊之矩陣位置，產生機密餘數影像

設定一大小為空白影像 (Null image)，每組機密資訊 {t1, t2}，以此二值 t1 與 t2 當為動態矩陣中的值，分別找尋動態矩陣對應的 X 與 Y 軸之位置值，設 t1 的 X 軸對應 $nrem_1$ 與 Y 軸對應 $nrem_2$，t2 的 X 軸對應 $nrem_3$ 與 Y 軸對應 $nrem_4$，其中對應值為 $nrem_i$，$nrem_i \in \{0,1,2\}$，$1 \le i \le 4$。將 $nrem_i$，$1 \le i \le 4$ 儲存至空白影像之對應位置，成為影像像素值，計算完機密資訊像素值，形成一機密餘數影像 *NREMI*。

【Step 7】藏入機密資訊

由左至右且從上到下掃描整張影像 $I_{x,y}$、餘數影像 *REMI* 與機密餘數影像

$NREMI$，以四個像素值為一組進行藏入判斷，每組rem_i與$nrem_i$，$1 \le i \le 4$，進行條件判斷，修改原始像素值$I_{x,y}$，以藏入機密資訊，資訊藏匿總共有三種情況，像素值加一、像素值不變與像數值減一，嵌入如公式 5.1。

$$I'_{x,y} = \begin{cases} I_{x,y}+1, & if((rem_i == 2 \& nrem_i == 0) | (rem_i == 1 \& nrem_i == 2) | (rem_i == 0 \& nrem_i == 1)) \\ I_{x,y}, & if((rem_i == 2 \& nrem_i == 2) | (rem_i == 1 \& nrem_i == 1) | (rem_i == 0 \& nrem_i == 0)) \\ I_{x,y}-1, & if((rem_i == 2 \& nrem_i == 1) | (rem_i == 1 \& nrem_i == 0) | (rem_i == 0 \& nrem_i == 2)) \end{cases}, \quad (5.1)$$

其中 $1 \le i \le 4$，重複執行直到機密資訊藏入整張影像為止。

【Step 8】輸出偽裝影像與還原資訊

機密資訊隱藏後產出偽裝影像$I'_{x,y}$、餘數影像$REMI$、亂數種子$random1$、$random2$與$random3$，偽裝影像及其還原資訊需傳送給接收方，方便日後機密資訊的取出與原始影像還原。

動態矩陣資訊隱藏流程設計以四個像素為一組嵌入，當影像大小不為四的倍數時，造成剩餘像素無法進行對應，因此若有此情形發生，剩下的像素本研究不進行隱藏流程，但對於整張影像最多只有兩個像素無法進行預測，像素使用效率影響不大，本技術在動態矩陣隱藏技術中，增加了隱藏的安全性與減少了記憶體對矩陣計算的負擔，此方法為無失真的隱藏技術，達成本研究的資訊隱藏目標。

5.2 動態矩陣機密資訊取出與還原

機密資訊取出與偽裝影像的還原流程相似於機密資訊藏入流程，首先，利用二個亂數計算出動態矩陣，輸入偽裝影像計算機密餘數影像，機密餘數影像以四個值為一組，每一組可以利用動態矩陣配合機密餘數即可取出兩個九進位機密資訊，將機密資訊轉換成二進制後，透過亂數三將打亂的浮水隱轉換成原始浮水印機密資訊，即完成浮水印機密資訊影像。影像還原時，需利用機密餘數影像與餘數影像進行判斷，將偽裝影像的餘數修改成餘數影像的值，最後修改像素值即還原完成流程。

【動態矩陣機密資訊取出與影像還原演算法】

輸入：偽裝影像，餘數影像，*random1*， *random2* 與 *random3*

輸出：原始影像，機密資訊

【Step 1】動態矩陣產生

動態矩陣產生方式如同資訊隱藏之第一步驟，輸入二個亂數種子 *random1*及 *random2* 進行動態矩陣的製作。首先， *random1* 決定動態矩陣中心值，利用 *random2* 決定排列矩陣之邊緣位置值 $m_{i,j}$，$i, j \neq 1$ 形成一動態矩陣。

【Step 2】輸入偽裝影像

輸入一張偽裝影像 $I'_{x,y}$，其中 $x \in \{1,2,...,M\}$， $y \in \{1,2,...,N\}$，此影像要取出機密資訊並利用餘數影像還原成原始影像。

【Step 3】產生機密餘數影像並分組

將偽裝影像由左至右從上到下掃描，各別像素值除以 3，將餘數存成機密餘數影像矩陣 *NREMI*，此矩陣為當初利用動態矩陣位置對應的 X 與 Y 軸之值，產出 *NREMI* 後，將四個像素分成一組，總共有 $\frac{M \times N}{4}$ 組，其餘數為 $nrem_i$，$nrem_i \in \{0,1,2\}$，其中 $1 \leq i \leq 4$，每兩個值可決定動態矩陣的值，也就是機密資訊值。

【Step 4】取出機密資訊

獲取 *NREMI* 後，將每組的 $nrem_1$ 與 $nrem_2$ 對應動態矩陣的 X 與 Y 軸，查詢動態矩陣對應值，也就是機密資訊以九進制呈現的 t1 值，另外 $nrem_3$ 與 $nrem_4$ 對應動態矩陣的 X 與 Y 軸，亦九進制機密資訊 t2 值，t1 與 t2 組合後，轉換成一組 6 bits 的二進制機密資訊，重複此流程至整張影像取出結束。

【Step 5】還原機密資訊

將每組二進制值資訊集合後，利用 *random3* 將打亂後的浮水印機密資訊轉還原

成原始浮水印機密資訊，將產出完整的浮水印機密資訊。

【Step 6】還原影像

由左至右且從上到下掃描整張偽裝影像 $I'_{x,y}$ 、機密餘數影像 *NREMI* 與餘數影像 *REMI* ，以四個值為一組進行還原判斷，每組 $nrem_i$ 與 rem_i ，$1 \le i \le 4$ ，進行條件判斷，修改偽裝像素值 $I'_{x,y}$ ，總共有三種情況，像素值加一、像素值不變與像數值減一，影像還原如公式 5.2。

$$I_{x,y} = \begin{cases} I'_{x,y}+1, if\ ((nrem_i == 2 \,\&\, rem_i == 0) \mid (nrem_i == 1 \,\&\, rem_i == 2) \mid (nrem_i == 0 \,\&\, rem_i == 1)) \\ I'_{x,y},\ if\ ((nrem_i == 2 \,\&\, rem_i == 2) \mid (nrem_i == 1 \,\&\, rem_i == 1) \mid (nrem_i == 0 \,\&\, rem_i == 0)) \\ I'_{x,y}-1, if\ ((nrem_i == 2 \,\&\, rem_i == 1) \mid (nrem_i == 1 \,\&\, rem_i == 0) \mid (nrem_i == 0 \,\&\, rem_i == 2)) \end{cases}, \quad (5.2)$$

其中 $1 \le i \le 4$，重複執行直至整張影像還原為止。

【Step 7】輸出原始影像與機密資訊

機密資訊由上述流程擷取後將獲取完整的機密資訊，以及將偽裝影像還原至原始影像 $I_{x,y}$ ，取出與還原流程就此結束。

資訊取出及還原流程中，將還原資訊如餘數影像與亂數等輸入於演算法中，即可萃取出浮水印資訊，最終將偽裝影像回朔至最初原始影像。本方法設計可逆資訊隱藏設計，在動態矩陣資訊隱藏技術中，有具體且明確的做法與流程，達成機密資訊傳遞與原始資訊共存的研究目標。

5.3 範例說明

本節將以例題闡述說明資訊隱藏、取出資訊與還原影像流程，首先，設計一個大小為 3x3 動態矩陣 *MT* ，如圖 5-2，並輸入一張大小為 4x4 的原始影像矩陣 *I* ，如圖 5-3，計算機密餘數影像，動態矩陣之機密資訊的藏入、取出與還原原始影像，機密資訊隱藏流程與影像還原流程說明如 5.3.1 與 5.3.2。

5.3.1 機密資訊隱藏流程

動態矩陣產生為先製作大小為 3×3 矩陣，再著利用兩個亂數種子 *random1* 與 *random2*，動態矩陣中心位置值為 *random1* mod 9 = 4，而 *random2* mod 9= 7，如圖 5-1 邊緣位置 7 開始排列，順時針以中間值為 4 開始遞增方式排列，當遇到矩陣位置 2 且排列值大於 8 時，排列值則從 0 開始遞增排列，動態矩陣產生如圖 5-2 所示。

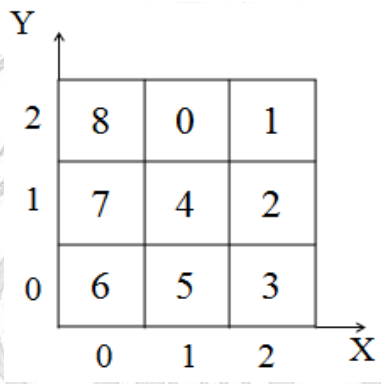


圖 5-2 動態矩陣 *MT*

假設輸入一張大小為 4×4 的原始影像矩陣 *I*，如圖 5-3，由左至右由上到下掃描整張影像，將每個像素值分別除以 3，得到一張餘數影像 *REMI*，如圖 5-4。以四個像素為一組，可得到四組值，第一組值：rem_1=1、rem_2=2、rem_3=0 與 rem_4=2；第二組值：rem_1=0、rem_2=1、rem_3=0 與 rem_4=0；第三組值：rem_1=0、rem_2=2、rem_3=1 與 rem_4=1；第四組值：rem_1=2、rem_2=1、rem_3=0 與 rem_4=0。

4	5	3	2
3	4	3	3
6	5	4	4
5	4	3	6

圖 5-3　原始影像 *I*

1	2	0	2
0	1	0	0
0	2	1	1
2	1	0	0

圖 5-4　餘數影像 *REMI*

假設欲隱藏之符水印機密資訊轉換成二進制，若轉換後機密資訊為 $(111111010010101011011101)_2$，將每六個位元為一組，轉換成九進制資訊，如第一組為 $(111111)_2$ 轉換成 $(70)_9$，t1=7 與 t2=0；第二組為 $(010010)_2$ 轉換成 $(20)_9$，t1=2 與 t2=0；第三組為 $(101011)_2$ 轉換成 $(47)_9$，t1=4 與 t2=7；第四組為 $(011101)_2$ 轉換成 $(32)_9$，t1=3 與 t2=2。

機密資訊轉換完成後，要找出各組對應於矩陣的位置，第一組 t1=7 對應的矩陣位置為 $nrem_1$=0 與 $nrem_2$=1，t2=0 對應的矩陣位置為 $nrem_3$=1 與 $nrem_4$=2；第二組 t1=2 對應的矩陣位置為 $nrem_1$=2 與 $nrem_2$=1，t2=0 對應的矩陣位置為 $nrem_3$=1 與 $nrem_4$=2；第三組 t1=4 對應的矩陣位置為 $nrem_1$=1 與 $nrem_2$=1，t2=7 對應的矩陣位置為 $nrem_3$=0 與 $nrem_4$=1；第四組 t1=3 對應的矩陣位置為 $nrem_1$=2 與 $nrem_2$=0，t2=2 對應的矩陣位置為 $nrem_3$=2 與 $nrem_4$=1，因此也產生機密餘數影像 *NREMI*，如圖 5-5。

0	1	1	2
2	1	1	2
1	1	0	1
2	0	2	1

圖 5-5　機密餘數影像 *NREMI*

獲取機密餘數影像 *NREMI* ，利用公式 5.1 進行藏入流程。第一組藏入流程判斷，當 rem_1=1 且 $nrem_1$=0，則該像素減一，*I'*=*I*-1=4-1=3；當 rem_2=2 且 $nrem_2$=1，則該像素要減一，*I'*=*I*-1=5-1=4；當 rem_3=0 且 $nrem_3$=1，則該像素加一，*I'*=*I*+1=3+1=4；當 rem_4=2 且 $nrem_4$=2，則該像素不變，*I'*=*I*=2。第二、三、四組依上述藏入流程判斷並藏入機密資訊，即可得偽裝影像 *I'*，如圖 5-6 所示。最後，將輸出偽裝影像 *I'*、餘數矩陣 *REMI* ，亂數一 *random1*、亂數二 *random2* 。

3	4	4	2
2	4	4	2
7	4	4	3
5	3	2	7

圖 5-6　偽裝影像 *I'*

5.3.2 機密資訊擷取與影像還原流程

當接收到偽裝影像 *I'*、餘數矩陣 *REMI* ，二個亂數 *random1*、*random2* 時，即可進行機密資訊取出與還原流程。首先，利用二個亂數計算動態矩陣，產生大小為 3x3 矩陣，利用亂數一計算矩陣中心值：*random1* mod 9 = 4，而亂數二計算

矩陣位置起始值 $random2 \mod 9 = 7$，得到動態矩陣如圖 5-2 所示。

取出機密資訊時，將偽裝影像 I' 各像素值除以 3，取得機密餘數影像 *NREMI* 後如圖 5-5，各組分別取出動態矩陣之兩個九進制值，由 $nrem_1$ 與 $nrem_2$ 找出 t1 及 $nrem_3$ 與 $nrem_4$ 找出 t2，再將 t1 與 t2 結合轉換成六個二進制的值，機密資訊取出之第一組，$nrem_1$=0 與 $nrem_2$=1 則 t1=7，$nrem_3$=1 與 $nrem_4$=2 則 t2=0，結合成$(70)_9$，轉換成二進制$(111111)_2$；第二組，$nrem_1$=2 與 $nrem_2$=1 則 t1=2，$nrem_3$=1 與 $nrem_4$=2 則 t2=0 結合成$(20)_9$，轉換成二進制$(010010)_2$；第三、四組依次轉換轉換成二進制，將各組機密資訊結合起來，即可取出機密資訊為$(111111010010101011011101)_2$。

影像還原流程是將偽裝影像的機密餘數影像 *NREMI* 及餘數影像 *REMI* 進行影像還原，還原流程如公式 5.2。還原影像之第一組為 $nrem_1$=0 且 rem_1=1，則該像素不變，$I=I'+1=3+1=4$；$nrem_2$=1 且 rem_2=2，則該像素要加一，$I=I'+1=4+1=5$；$nrem_3$=1 且 rem_3=0，則該像素減一，$I=I'-1=4-1=3$；$nrem_4$=2 且 rem_4=2 則該像素不變，$I=I'=2$；第二、三、四組依次取出流程，還原得到原始影像 I，如圖 5-3。

範例詳細描述資訊隱藏整個流程，利用餘數對應動態矩陣概念，由兩個亂數製作一個大小 3×3 之動態矩陣，輸入一張大小為 4×4 原始影像將四個像素為一組分成四組，進行對應動態矩陣並寫入機密訊息。欲擷取機密資訊與影像還原時，偽裝影像需進行餘數運算對應動態矩陣，可完整取出機密資訊，再利用原始餘數影像將偽裝影像還原至初始狀態。藉由範例說明，動態矩陣資訊隱藏實做確實可行，並可達成資訊隱藏且影像無失真的目標。

第六章 實驗結果與討論

本節將針對實驗結果提出討論與分析，包括實驗中所使用掩護影像、浮水印影像、藏入量以及影像品質數據與相關文獻的比較。本研究主要使用六張大小為512x512 灰階影像，分別為 Lena、Jet、Boat、Baboon、Barbara 與 Goldhill 作為原始影像，影像是從 USC-SIPI 影像資料庫取得並作為本實驗影像，如圖 6-1 所示。機密資訊為大小 800x800 的浮水印，隱藏時由使用者自行調整欲藏入的機密資訊大小，如圖 6-2 所示。在 6.1 節為 PSNR 值計算公式，6.2 節為二階段直方圖位移之高容量可逆性影像隱藏容量比較，6.3 節為應用影像區塊眾數之高容量可逆式隱藏技術容量比較，6.4 節為動態矩陣機密資訊隱藏容量與影像品質比較，6.5 節為可逆式資訊隱藏之影像品質與隱藏容量討論。

6.1 PSNR 值計算公式

本研究使用峰值訊號雜訊比 PSNR(Peak Signal to Noise Ratio)評估隱藏後的偽裝影像品質，公式定義如下：

$$\mathrm{PSNR} = 10 \times \log_{10} \frac{255^2}{\mathrm{MSE}} (\mathrm{dB}) \text{，} \tag{6.1}$$

其中 MSE(Mean square error)表原始影像與偽裝影像像素之均方差，其計算如下：

$$\mathrm{MSE} = \frac{1}{\mathrm{M} \times \mathrm{N}} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(\mathrm{P}_{i,j} - \mathrm{P}'_{i,j} \right)^2 \text{，} \tag{6.2}$$

$M \times N$ 代表著影像大小，$P_{i,j}$ 為原始數位影像(i,j)位置上的像素值，$P'_{i,j}$ 則是代表偽裝影像(i,j)位置上的像素值。

6.2 二階段直方圖位移之高容量可逆性影像隱藏技術容量比較

本論文所提二階段直方圖位移之高容量可逆性影像隱藏演算法可以依據不同

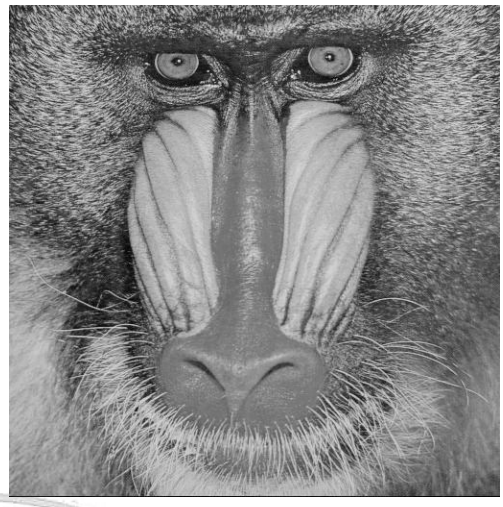
層級的設定而有不同的嵌入量，這種可調式動態嵌入機密資訊可依據不同的浮水印大小進行隱藏，以適應機密資訊大小之負載容量，並可增加隱藏之負載空間容量。表 6-1 為本方法定義不同層級的隱藏容量，層級由兩個峰值大小決定，以容量大小依序排列層級，層級越低容量越少，層級越高容量就越高。因此，本方法可依據浮水印機密資訊大小決定所需隱藏層級。另外，亦可在負載容量與影像品質之間決定所需隱藏層級。表 6-2 為本研究依不同層級計算各影像之隱藏容量及其 PSNR 值，若考慮隱藏容量就以較高之層級隱藏方法，若考慮影像品質就以較低之層級隱藏。即使是層級不同，隱藏機密資訊所產生偽裝影像如圖 6-3 所示，實驗顯示本方法之偽裝影像有良好之影像品質。。

本方法使用二階層式雙直方圖隱藏方式，在負載影像隱藏容量上均會向上提升，產生較佳之效果。在實驗上首先使用四張影像 Lena、Jet、Boat 與 Baboon 進行實驗，並且將層級設為 L=4 與 Hong 等人所提方法比較如表 6-3，實驗顯示在隱藏容量方面，均較 Hong 等人所提方法[17]為佳。另一方面，再以影像 Lena、Jet、Barbara 與 Goldhill 進行實驗，層級設為 L=2 與 Zhao 等人所提方法[42]比較，實驗結果在隱藏容量方面如表 6-4，實驗顯示有更好之隱藏效果。

(a) Lena

(b) Jet

(c) Boat



(d)Baboon

(e) Barbara

(f)Goldhill

圖 6-1　實驗影像

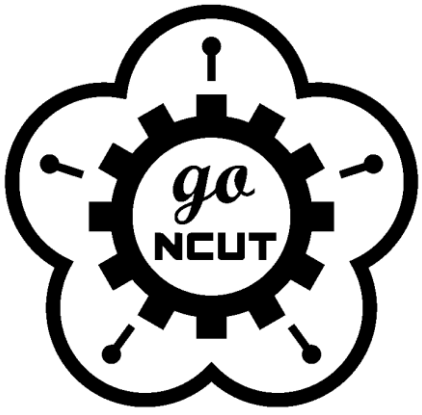


圖 6-2　浮水印之機密資訊

表 6-1　不同層級對應的容量計算

Level	容量
L=1	PH_1+PH_2
L=2	$PH_1+PH_2+PL_2$
L=3	$PH_1+PL_1+PH_2$
L=4	$PH_1+PL_1+PH_2+PL_2$

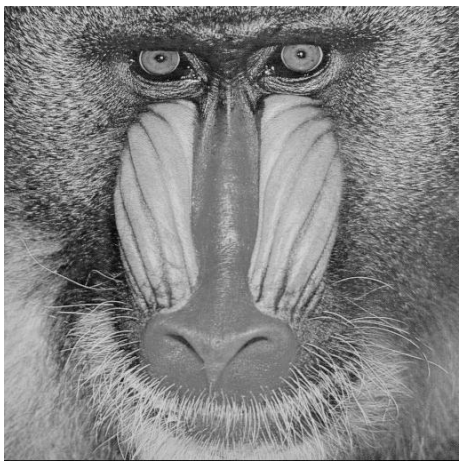
表 6-2　不同層級容量之 PSNR 比較

Image	L=1		L=2		L=3		L=4	
	容量	PSNR	容量	PSNR	容量	PSNR	容量	PSNR
Lena	28479	51.4341	30084	50.5772	50081	49.4428	54686	48.8829
Jet	37727	51.5861	44344	50.7882	62293	49.6231	68910	49.0966
Boat	15175	51.3497	19296	50.4607	27199	49.0879	30780	48.5405
Baboon	7641	51.3505	9173	50.3109	13655	48.9604	15187	48.331
Barbara	16765	51.4328	20107	50.4274	29729	49.2021	33071	48.5725
Goldhill	16835	51.7718	20277	50.8132	29571	49.1224	33313	48.575

(a) Lena，PSNR=48.8829

(b) Jet，PSNR=49.0966

(c) Boat，PSNR=48.5405



(d) Baboon，PSNR=48.331

(e) Barbara，PSNR=48.5725

(f) Goldhill，PSNR=48.575

圖 6-3　L=4 之偽裝影像

表 6-3　隱藏容量與 Hong et al.比較

Image	隱藏容量			
	本研究 L=4	Hong et al.[17]	增量	增量比
Lena	54686	46839	7847	16.75%
Jet	68910	64863	4047	6.24%
Boat	30780	29824	956	3.21%
Baboon	15187	14154	1033	7.30%

表 6-4　隱藏容量與 Zhao et al.比較

Image	隱藏容量			
	本研究 L=2	Zhao et al.[42]	增量	增量比
Lena	30084	24976	5108	20.45%
Jet	44344	39621	4723	11.92%
Barbara	20107	16845	3262	19.36%
Goldhill	20277	18233	2044	11.21%

6.3 應用影像區塊眾數之高容量可逆式隱藏技術容量比較

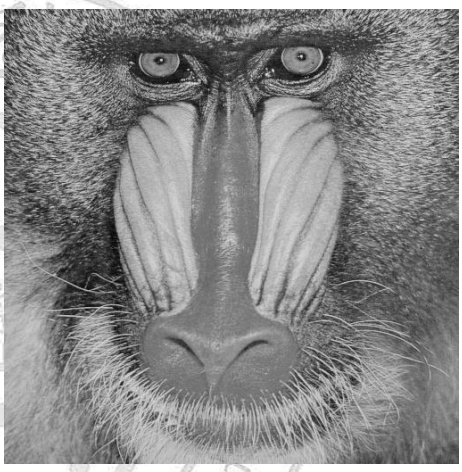
本方法利用影像區塊眾數當成預測值，由於眾數之像素具有像素相似高的特性，其預測差值計算結果會趨近於零，因此在藏入機密資訊之負載影像容量可提升很多，而以 LSB 嵌入機密資訊後之偽裝影像亦能維持有良好之影像品質，其偽裝影像與原始影像之 PSNR 值都能保持在 48 dB 以上，在這種影像品質下，對於人類的視覺上是不易察覺有改變的，偽裝影像及 PSNR 值如圖 6-4。本實驗所提方法與 Hong 等人[17]及 Zhao 等人[42]之方法進行比較，在藏匿後的負載容量及影像品質 PSNR 值如表 6-5 與 6-6 說明。

在表 6-5 中，本方法與 Hong 等人方法相較下，在負載影像隱藏容量方面，本方法之可藏入資訊量均大幅提高，以 Baboon 而言，本方法之藏入容量遠大於 Hong 等人方法之藏入量兩倍之多。以實驗之四張影像的平均值而言，可以明顯地的說明本方法的藏入容量是 Hong 等人方法的一倍以上。另一方面，本方法與 Zhao 等人所提方法進行比較，如表 6-6，以 Barbara 與 Goldhill 而言，本方法容量高於 Zhao 等人三倍以上之藏入容量。以實驗之四張影像的平均值而言，本方法隱藏容量較 Zhao 等人方法提高達到兩倍以上的容量。在影像品質方面，本方法的 PSNR 亦皆高於 Zhao 等人所提出的方法，由本實驗結果顯示，本方法在影像的隱藏容量與影像品質均呈現良好之成效。

(a) Lena，PSNR=48.9295

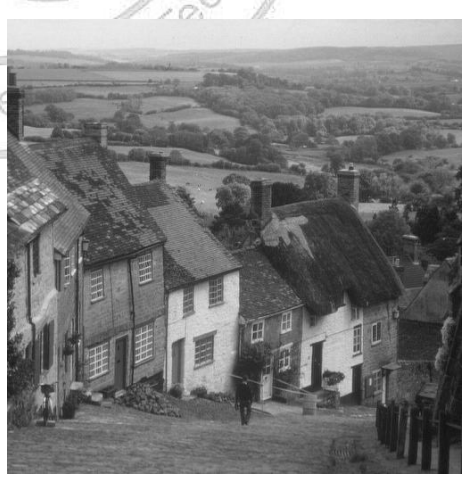
(b) Jet，PSNR=49.0446

(c) Boat，PSNR=48.7361



(d) Baboon，PSNR=48.5624

(e) Barbara，PSNR=48.7287



(f) Goldhill，PSNR=48.7403

圖 6-4　偽裝影像

表 6-5　隱藏容量與 Hong et al.比較

Image	隱藏容量			
	本研究	Hong et al.[17]	增量	增量比
Lena	94145	46839	47306	101.00%
Jet	105379	64863	40516	62.46%
Boat	71960	29824	42136	141.28%
Baboon	52978	14154	38824	274.30%

表 6-6　隱藏容量與 Zhao et al.比較

Image	隱藏容量			
	本研究	Zhao et al.[42]	增量	增量比
Lena	94145	24976	69169	276.94%
Jet	105379	39621	65758	165.97%
Barbara	72473	16845	55628	330.23%
Goldhill	73078	18233	54845	300.80%

6.4 動態矩陣機密資訊隱藏容量與影像品質比較

本節使用三張大小為 512×512 灰階影像，Lena、Jet 與 Baboon 作為負載影像，如圖 6-1(a)、(b)、(d)所示。機密資訊為矩形浮水印，將影像大小縮小至 627×627，如圖 6-2 所示。將機密訊息透過動態矩陣隱藏演算法藏入於負載影像中，產生偽裝影像如圖 6-5 所示。本方法利用動態矩陣進行機密資訊隱藏，影像中每個像素都可以藏入機密資訊，每四個像素可以被藏匿二個九進制資料或是六個位元的二進制資料，因此負載影像可以藏入大量的機密資訊，但在每個像素只可能被修改一個單位，換句話說，資訊藏匿產生像素值變化可能是加減一個單位或者像素值保持不動，由於像素值變化不大，藏入後的偽裝影像與原始影像的 PSNR 值都可以保持 49.8 dB 以上，對於此種影像品質，人類視覺無法察覺該影像已作改變，由此可見本方法可藏入大量機密資訊並具良好影像品質。偽裝影像及 PSNR 值如圖 6-5，

本實驗所提方法與 Fridrich 等人及 Chang 等人方法進行比較，隱藏後的容量及影像品質 PSNR 如表 6-7。

(a) PSNR=49.8780　　(b) PSNR=49.8906　　(c) PSNR=49.8963

圖 6-5　偽裝影像

在表 6-7 中，本方法與 Fridrich 等人提出的濕紙編碼法[15]及 Chang 等人所提出的魔術矩陣與濕紙編碼法之資料隱藏技術[11]比較，在藏入容量方面，本方法利用影像中各像素藏匿資料，而文獻[11]的方法先預處理影像的乾濕像素，機密資訊只能藏入於乾像素中，濕像素無法寫入，造成隱藏容量降低。本方法的藏入容量為四個像素可以藏入六個位元，以 512×512 灰階影像實驗，則藏入容量可達 $512\times512\times\frac{6}{4}=393216$ bits，此隱藏容量與 Fridrich 等人的 LSB 法， two-LSB 法及 Chang 等人方法比較，容量分別增加了 207.2%、53.6%、77.12% ，顯示本方法大量的增加隱藏容量。在影像品質的比較，本方法三張偽裝影像 PSNR 值均高於 49.8 dB，由於隱藏容量較大，影像品質較 Chang 等人方法稍微降低，但亦優於 Fridrich 等人的 two-LSB 法。由實驗結果得知，本方法所提出的隱藏演算法影像品質達到良好視覺效果，更有效大幅提升負載影像之可隱藏容量。

表 6-7　隱藏容量與影像品質比較

Image / Methods	Lena		Jet		Baboon	
	(bits)	(dB)	(bits)	(dB)	(bits)	(dB)
Fridrich et al. [15](LSB)	128000	54.14	128000	54.16	128000	54.14
Fridrich et al. [15](two-LSB)	256000	47.18	256000	47.15	256000	47.16
Chang et al.[11]	222000	50.33	222000	50.32	222000	50.34
本方法	393216	49.8780	393216	49.8906	393216	49.8963

6.5 可逆式資訊隱藏之影像品質與隱藏容量討論

上述小節的實驗結陳述，本方法於可逆式資訊隱藏不論在影像品質以及影像藏匿機密資訊空間，都較先前學者提出的隱藏技術有良好的改善。影像品質利用 PSNR 計算，目的在於計算影像藏入資訊前後的差異，先前學者[3]提出通常 PSNR 值大於 30(dB)都是讓人眼能夠接受的範圍，經我們實驗結果顯示，本方法 PSNR 值皆高於 48(dB)以上的水準，雖然有些影像品質不比文獻高，但對於人眼已經無法辨識影像是否有所改變，甚至電腦也偵測不到差異所在。因此，現今對於資訊隱藏技術設計方向朝向影像高容量藏匿方式，在直方圖修改藏匿技術中，二階段直方圖修改嵌入方式藏秘容量皆高於兩位學者；另一方法，應用影像區塊眾數隱藏技術，隱藏容量平均高於學者一倍以上至多高達三倍，實驗結果充分顯示嵌入演算法在預測能力有效提升。除此之外，動態機密資訊隱藏技術之影像負載容量也凌駕於直方圖隱藏技術許多，由於四個像素可藏匿六個二進制之值，一張影像可以藏 1.5 倍的二進制的量，與文獻的容量相較下也高達一倍以上。換句話說，本研究設計的可逆式資訊隱藏演算法，影像品質不僅良好，影像的負載容量也大幅提升。

第七章 結論與未來研究方向

本章節將闡述本研究所提之三種空間域影像資訊隱藏研究結論，7.1 節討論設計的方式的優點及具有高容量的藏匿方法，除此之外，將像素做微小修改以至於影像品質維持良好水準，再者，本研究提出的技術皆為可逆式隱藏方法，具有安全及保留原始資訊等特色。7.2 節為未來研究方向，以利用直方圖修改與動態矩陣隱藏方法，提出更新穎且具有貢獻性的資訊隱藏技術。

7.1 結論

本論文提出三種空間域可逆式資訊隱藏方法，首先提出的為二階段直方圖位移之高容量可逆性影像隱藏，本方法使用二階段預測編碼法計算鄰近區塊內像素差值，第一階段產生區塊內像素差值後，尚有一個像素未被利用，因此產生第二階段區塊間像素預測差值之計算，提升像素使用率，使得影像負載容量增大。二階段隱藏的優點為可動態調整機密資訊隱藏容量，所產生二個差值直方圖之雙峰點，有彈性依使用者需求取捨資訊嵌入容量或影像品質，亦即層級大小會影響到藏入容量高低及影像品質的優越。更進一步，本研究為了提升影像的負載容量，提出另一以直方圖為基礎之方法，應用影像區塊眾數可逆資訊隱藏技術，使用預測編碼法計算區塊內的像素差值，本方法的關鍵預測方式為區塊眾數當成預測值，將區塊預測值與像素值做預測差值計算，讓預測差值趨近於零，如此，統計後之預測差值直方圖的峰值次數提升，換句話說，影像可藏容量也跟隨增加，利用雙峰嵌入方式，將有效藏匿大量機密資至影像中。

資訊隱藏主要追求最大的資訊可藏容量及影像嵌入後的影像品質，本論文又提出新型動態矩陣機密資訊隱藏技術，利用兩個亂數產生小型動態矩陣，亂數等同於金鑰分享於傳送與接收雙方，防止有心人士擷取機密資訊並做出攻擊，學者所提 EMD 隱藏方式需產出固定式且龐大的矩陣，本研究設計出作法相同且簡單實作的縮小矩陣，此矩陣具有動態性可提升機密安全性又可降低大型矩陣之記憶體

負擔，本方法不再使用文獻提出濕紙編碼法是為了將影像像素使用率提升，讓整張影像之各個像素皆可藏入機密，大幅增加影像的負載容量。

本論文三種資訊隱藏實驗結果顯示，對影像承載機密資訊的容量均有不錯的成果，所提之三種機密資訊隱藏技術皆為空間域隱藏，當機密資訊寫入像素後，像素最多也只會更動一個單位，也就是像素值加一、減一或不變的特色，影像品質皆維持優異的表現，由實驗結果得知，利用直方圖資訊隱藏技術，PSNR 可以維持 48(dB)以上的水準。然而，利用動態矩陣機進行的密資訊隱藏，PSNR 更可高達 49(dB)以上，達成視覺上的不可察覺性。此外，本研究提出的資訊隱藏皆為可逆式資訊隱藏，換句話說，從偽裝影像取出機密資訊後，亦可回復為無失真之原始影像，本研究可達成在資訊安全保密下且不失去原始資訊共存之特色。

7.2 未來研究方向

本研究所提三種空間域可逆式資訊隱藏方法，經實驗結果顯示，在影像維持良好的品質之下，資訊隱藏容量均能有效提高，在未來階段的研究，事實上還是有可以改善的部分有待繼續發掘，就隱藏容量而言，直方圖隱藏方法有著不錯的成果，但還是可以利用更精準的預測方式，使其峰點出現頻率更多，如朝向 2×2 區塊眾數當作預測，使得預測能力提高並增加藏匿容量，或讓沒藏匿資料卻要位移的像素不要太多，可利用變異數預先處理區塊內或區塊間像素，將複雜的區塊跳過，不進行資訊隱藏等，這些都為藏匿容量增加或不變下，讓影像品質 PSNR 值能夠盡可能的提升。而在動態矩陣藏匿機密資訊的方法，我們可以朝向影像安全的前提下進行發展，例如設計多個動態矩陣，並將原始影像分成多個區塊，影像中每個區塊利用不同的動態矩陣進行資訊的隱藏，這可使影像藏匿的機密性提高，防止有心人士惡意的攻擊，故在未來我們希望進一步去研究空間域可逆資訊隱藏技術，使其能達到高負載量、良好的視覺品質與機密資訊的安全性為目標。

參考文獻

【1】 張真誠，黃國峰與陳同校(2003)，電子影像技術，旗標出版股份有限公司。

【2】 張真誠，黃國峰與陳同校(2003)，數位影像處理技術，旗標出版股份有限公司。

【3】 郭紹宏與席家年(2009)，植基於 EMD 資料隱藏技術之研製，碩士論文，南台科技大學資訊工程系

【4】 粘添壽(2008)，資訊與網路安全技術，旗標出版股份有限公司。

【5】 Ahmed, N., Natarajan, T. and Rao, K. R., "Discrete Cosine Transform," IEEE Transactions on Computers, vol. C-23, no. 1, pp. 90-93, 1974.

【6】 Alattar, A. M., "Reversible watermark using the difference expansion of generalized integer transform," IEEE Transactions on Image Process, vol. 13, no. 8, pp. 1147–1156, 2004.

【7】 Chang, C. C., Tai, W. L. and Lin, C. C., "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.

【8】 Chang C. C., Lin C. C., Tseng C. S. and Tai W. L., "Reversible hiding in DCT-based compressed images," Information Sciences, vol. 177, no. 13, pp. 2768–2786, 2007.

【9】 Chang, C. C., Hsieh, Y. P. and Lin, C. Y., "Lossless data embedding with high embedding capacity based on declustering for VQ-compressed images," IEEE Transactions on Information Forensics and Security, vol. 2, no. 3, pp. 341–349, 2007.

【10】 Chang, C. C. and Chou, Y. C., "A Fragile Digital Image Authentication Scheme Inspired by Wet Paper Codes," Fundamenta Informaticae, vol. 90, no. 1-2, pp. 17-26, 2009.

【11】 Chang, C. C., Chen, Y. H., Wang, Z. H. and Li, M. C., "A Data Embedding Scheme Based on a Magic Matrix and Wet Paper Codes," International Conference on Computational Intelligence and Natural Computing (CINC 2009), vol. 2, pp. 303-306, 2009.

【12】 Chang, C. C., Chen, K. N. and Lin, H. C., "Novel Magic Matrices Generation Method for Secret Messages Embedding," International Journal of Computer Sciences and Engineering Systems, vol. 5, no. 3, pp. 235-241, 2011.

【13】 Dejey, D. and Rajesh, R. S., “Robust discrete wavelet-fan beam transforms-based colour image watermarking,” IET on Image Processing, vol. 5, no. 4, pp. 315-233, 2011.

【14】 Demirel, H. and Anbarjafari, G., “Discrete Wavelet Transform-Based Satellite Image Resolution Enhancement,” IEEE Transactions on Geoscience and Remote Sensing, vol. 49, no. 6, pp. 1997-2004, 2011.

【15】 Fridrich, J., Goljan, M., Lisonek, P., and Soukal, D., “Writing on wet paper,” IEEE Transactions on Signal Processing, vol. 53, no. 10, pp. 3923-3935, 2005.

【16】 Hsiao, J. Y., Chan K. F. and Chang J. M., “Block-based reversible data embedding,” Signal Process, vol. 89, no. 4, pp. 556–569, 2009.

【17】 Hong, W. and Chen, T. S., “A local variance-controlled reversible data hiding method using prediction and histogram-shifting,” The Journal of Systems and software, vol. 83, no. 12, pp. 2653-2663, 2010.

【18】 ISO/IEC JTC1 10918-1 (ITU-T Rec. T.81), Information technology – Digital compression and coding of continuous-tone still images: Requirements and guidelines, 1994.

【19】 Jin, H. L., Fujiyoshi, M. and Kiya, H., “Lossless data hiding in the spatial domain for high quality image,” IEICE Trans. Fundamentals, vol. E90-A, no. 4, pp. 771–777,2007.

【20】 Ker, A. D., “Steganalysis of LSB matching in grayscale images,” IEEE Signal Processing Letters, vol. 12, no. 6, pp. 441-444, 2005.

【21】 Kim, H. J., Sachnev, V., Shi, Y. Q., Nam, J. and Choo, H. G., “A novel difference expansion transform for reversible data embedding,” IEEE Transactions on Information Forensics and Security, vol. 3, no. 3, pp. 456–465, 2008.

【22】 Kieu, T. D., Wang, Z. H., Chang, C. C. and Li, M. C., “A Sudoku Based Wet Paper Hiding Scheme, ” International Journal of Smart Home , vol. 3, no. 2, pp. 1-12 , 2009.

【23】 Lee, C. F., Chang, C. C. and Wang, K. H., “An Improvement of EMD Embedding Method for Large Payloads by Pixel Segmentation Strategy,” Image and Vision Computing, vol. 26, no. 12, pp. 1670-1676, 2008.

【24】 Luo, L., Chen, Z., Chen, M., Zeng, X. and Xiong, Z., “Reversible Image Watermarking Using Interpolation Technique,” IEEE Transactions on Information Forensics and Security, vol. 5, no. 1, pp. 187-193, 2010.

【25】 Lee, C. F. and Shin, M. C., “Reversible Data Hiding Based on VQ Compression Code,” International Conference on Genetic and Evolutionary Computing (ICGEC 2011 Fifth), pp. 208-211, 2011.

【26】 Mielikainen, J., “LSB matching revisited,” IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285-287, 2006.

【27】 Ni, Z., Shi, Y. Q., Ansari, N. and Su, W., “Reversible data hiding,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354–362, 2006.

【28】 Petitcolas, F. A. P., Anderson, R. J. and Kuhn, M. G., “Information hiding—a survey,” Proceedings of the IEEE. Special Issue on Protection of Multimedia Content, vol. 87, no. 7, pp. 1062–1078, 1999.

【29】 Provos, N. and Honeyman, P., “Hide and seek: an introduction to steganography,” IEEE Security and Privacy Magazine vol. 1, no. 3, pp. 32–44, 2003.

【30】 Simmons, G. L., “The Prisoners’ Problem and Subliminal Channels,” Proc. Annu. Int. Cryptology Conf., Santabarbara, CA, pp. 51-67, 1984.

【31】 Seki, Y., Kobauashi, H., Fujiyoshi, M. and Kiya, H., “A Data Hiding Method without Specifying Embedded Positions for JPEG Image,” Electronics and Communications in Japan, Part3, vol. 90, no. 11, pp. 21-29, 2007.

【32】 Tian, J., “Reversible data embedding using a difference expansion,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 8, pp. 831–841, 2003.

【33】 Thodi, D. M. and Rodriguez, J. J., ”Expansion embedding techniques for reversible watermarking,” IEEE Transactions on Image Process, vol. 16, no. 3, pp. 723–730, 2007.

【34】 Tseng, H. W. and Hsieh, C. P., “Prediction-based reversible data hiding,” Information Sciences, vol. 179, no. 14, pp. 2460–2469, 2009.

【35】 Tsai, P., “Histogram-based reversible data hiding for vector quantisation-compressed images,” IET on image processing, vol. 3, no. 2, 2009.

【36】 Tsai, P. Y., Hu, Y. C. and Yeh, H. L., “Reversible image hiding scheme using predictive coding and histogram shifting,” Signal Processing, vol. 89, no. 6, pp. 1129–1143, 2009.

【37】 Wang, Z. H., Kieu, T. D., Chang, C. C. and Li, M. C., “A Novel

Information Concealing Method Based on Exploiting Modification Direction," Journal of Information Hiding and Multimedia Signal Processing, vol. 1, no. 1, pp. 1-9, 2010.

【38】 Yang, C. H. and Tsai, M. H., "Improving histogram-based reversible data hiding by interleaving predictions," IET Image Process, vol. 4, no. 4, pp. 223-234, 2010.

【39】 Yin, Z. X., Chang, C. C. and Zhang, Y. P., "An Information Hiding Scheme Based on (7,4) Hamming Code Oriented Wet Paper Codes, " Inter. Journal of Innovative Computing, Info and Control , vol. 6, no. 7, pp. 3121-3130 , 2010.

【40】 Zhang, X. and Wang S., "Efficient Steganographic Embedding by Exploiting Modification Direction," IEEE Communications Letters, vol. 10, no. 11, pp. 781-783, 2006.

【41】 Zeng, B. and Fu, j., "Directional Discrete Cosine Transforms—A New Framework for Image Coding ," IEEE Transactions on Circuits and Systems for Video Technology, vol. 18, no. 3, pp. 305-313, 2008.

【42】 Zhao, Z., Luo, H., Lu, M. Z. and Pan, J. S., "Reversible data hiding based on multilevel histogram modification and sequential," AEU - International Journal of Electronics and Communications, vol. 65, no. 10, pp. 814-826, 2011.