第一章　緒論

第一節　研究背景

隨著電腦的普及化及網路科技的進步，過去以紙本形式為主的資料已經不能夠滿足現代人講求方便快速的需求，多數的資料已能夠運用電腦處理的方式由紙本資料轉換成數位資料，再透過網路科技將資料做最快速的傳送。由於資料的數位化，要經由網路來取得資料是相當容易的事，且在取得資料時，存在有許多便利的複製方法來提供使用者去複製、重製資料，當使用者在享受科技給予便利的同時，對於多數數位原創者或是企業來說，如何預防智慧財產權的侵犯及保障合法的所有權是相當重要的問題。因此，許多關於智慧財產權保護的機制相繼被提出，數位浮水印(digital watermarking)就是一種能夠保護數位資料的方法，其做法是隱藏一個有意義的簽章或是浮水印到原始影像當中，來做到版權的保護、圖片的認證以及防止複製品的發生。

數位浮水印的概念於 1990 年首次被提出，該技術是將與版權相關的浮水印資訊嵌入數位媒體中，以保障所有權及合法的擁有權(婁德權，張明昌，2004)。一般而言，數位浮水印依其使用目的可分為易碎型浮水印(fragile watermarking)及強健型浮水印(robust watermarking)(陳文淵，卓江南，2003)。易碎型浮水印主要是應用於影像的竄改偵測上，當影像遭受到竄改時，可藉由易碎型浮水印偵測出受到竄改之處，並進而達成修復的目的；強健型浮水印則是應用於所有權的保護，當影像的版權受到侵害時，作者可從影像中取出嵌入的浮水印，以證明其所有權，因此強健型浮水印在嵌入影像後不能輕易被移除，如此才能在影像被盜用時仍然能夠取出證明所有權的浮水印。若依嵌入浮水印後的影像上是否可

看見浮水印來做分類依據，則浮水印技術可分為可視浮水印(visible watermarking)與不可視浮水印(imperceptible watermarking)(陳文淵，卓江南，2003)。不可視的強健型浮水印通常應用於所有權的保護，而本研究所提出的方法即屬於此類浮水印技術。一個完整的浮水印機制通常包含兩個階段：一為浮水印藏入階段；另一為浮水印取出階段，其程序分別如圖 1-1 及圖 1-2 所示(Katzenbeisser and Petitcolas, 2000)。圖 1-1 為藏入浮水印到原始影像的過程，在輸入的部份包含原始影像 I、浮水印 W 及一份秘密的 key 值，其中秘密的 key 值為原始影像所有者持有，為日後在取出浮水印時所需的金鑰；輸出的部份則為經過藏入浮水印程序後所產生的被浮水印影像 I'。圖 1-2 為從被浮水印影像中取出浮水印的過程，在輸入的部份包含原始影像 I、被浮水印影像 I'、浮水印 W 及一份秘密的 key 值，其中原始影像 I 及浮水印 W 會依照不同的浮水印方法，視其所需來決定是否有存在的必要；輸出的部份則為經過浮水印取出程序後，產生用來驗證所有權的浮水印影像 W'。

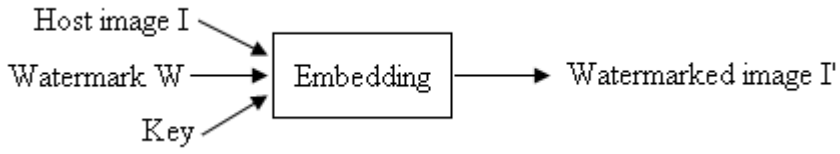

圖 1-1　浮水印之藏入程序

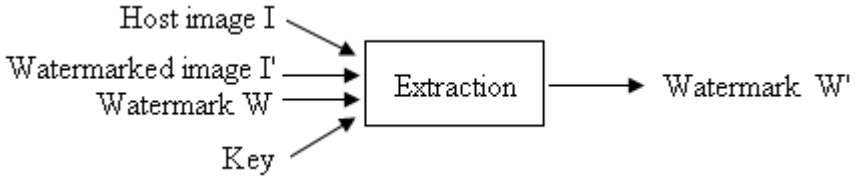

圖 1-2　浮水印之取出程序

一般在設計不可視的強健型浮水印時，有下列幾項應考慮的條件(Katzenbeisser and Petitcolas, 2000；王旭正，柯宏叡，2003)：

一、不可察覺性(imperceptibility)：

對於資料的價值來說，為了防止資料被複製而使其附帶有明顯的浮水印，是會造成一定程度的破壞。因此，在設計一個浮水印時，最基本要求就是藏入浮水印後的資料不能被人眼察覺到與原始資料有任何的不同。

二、強韌性(robustness)：

對於一般資料處理的攻擊要有相當的抵抗能力，即便是受到攻擊後也要能夠取出高辨識度的浮水印。

三、盲目性(blindness)：

為了增加在驗證所有權時的便利性且減少不必要的儲存原始資料的空間，一個實用的浮水印在取出時，應該不需要原始資料的輔助就可以順利取出。

四、明確性(unambiguity)：

為了保障所有者的權益，藏入的浮水印必須含有特定的意義，且在取出後能夠讓人很明確的辨識出浮水印的內容，不容許有模稜兩可的情況發生。

五、安全性(security)：

需考量藏入浮水印的區域是否會被攻擊者所推測出來，更不能讓浮水印被攻擊者任意移除，且浮水印在透過 key 值來藏入資料後，在沒有 key 值的情況之下，任何人皆無法讀取資料中的浮水印資訊。

六、負載量(payload)：

指浮水印機制所能隱藏的浮水印資料量，通常所隱藏的資料量愈多，浮水印被察覺出來的可能性愈大。

對於現今的研究來說，要同時滿足這些條件是具有相當大的挑戰，況且某些條件之間會互相抵觸，例如為了加強浮水印的強韌性來抵抗各種影像攻擊及避免浮水印被移除情形發生，勢必會對原始影像有所更動，通常修改的幅度愈大，浮水印的強韌性愈佳，但相對地愈容易被人眼察覺到浮水印的存在，使得不可察覺性的要求愈無法被滿足。因此，在針對不同的目的及需求的情況下，在設計浮水印時，如何去達到上述這些條件的平衡是我們需要去努力的目標。

第二節　研究動機

1995 年，Naor 與 Shamir 提出一種不需經過複雜的計算就能做到影像分享及保密的方法，稱為視覺密碼(visual cryptography, VC)，其作法是將機密影像分解成 n 份(shares)，讓 n 位合法的擁有者各持有一份，而每一份分解影像在外觀上看起來都是亂碼，解密時只需將至少 k ($k \leq n$)份的分解影像重疊在一起，就能以人眼看到機密影像，由於視覺密碼又是一種祕密分享的方法，因此又可稱為(k,n)-threshold 視覺式秘密分享(visual secret sharing)。

由於視覺密碼的加解密方法簡單，且具有無條件安全性，因此近年來有一些應用視覺密碼的數位浮水印技術相繼被提出(侯永昌，沈昌興，2000;Chang and Chuang, 2002;Chang and Wu, 2001;Chen and Hou, 2001;Hou and Chen, 2000;Hsu and Hou, 2005;Hwang, 2000；Lou, Tso, and Liu, 2007)。其中有多篇方法未真正將浮水印藏入原始影像中，而是根據原始影像的特徵與一張代

表符水印的影像，依視覺密碼的機制共同產生一張用以驗證所有權的影像，因此若有兩張特徵相似的影像，有可能會產生誤認所有權的情況。

此外，有些方法使用空間域的技術，對抗攻擊的效果較不如頻率域的技術，尤其如侯永昌與沈昌興(2000)及 Hwang (2000)的方法，以原始影像的最高位元平面做為影像的特徵圖，當影像的像素值在 127 附近，便很容易因為像素值些微的變化，導致最高位元平面有大幅度的變動，進而影響浮水印的強韌性。此外，利用最高位元平面依視覺密碼的機制所產生的另外一張分享影像，並不符合視覺密碼的安全條件。

Lou, Tso, and Liu (2007)的方法雖然是以頻率域的技術為基礎，但他們亦未真正將浮水印藏入影像中，而且他們雖號稱結合視覺密碼的方法，但其還原浮水印時，與視覺密碼的解密方法不同，因此不能算是採用視覺密碼的技術。

總而言之，大部分結合視覺密碼設計所有權保護機制的研究，未將浮水印藏入原始影像中，可能會導致所有權錯認的疑慮，且他們多半以空間域的技術為基礎，使得抵抗攻擊效果不佳，甚至有些方法並未考慮到安全性。因此，一個結合視覺密碼的所有權保護機制，應是必須將浮水印真正嵌入原始影像中，並符合視覺密碼的安全條件與解密的特性，同時，該機制必須能抵抗大部分常見的影像攻擊。

第三節　研究目的

本研究提出一種應用視覺密碼技術並在頻率域藏入浮水印的方法，主要是將浮水印利用視覺密碼分解成兩份，其中一份藏入原始影像的小波係數中，另一份則做為取出浮水印的金鑰，在不

需透過原圖的輔助下就能夠產生浮水印，且在沒有金鑰的情況下，即便是取出藏入原始影像的分解影像也無法得知任何關於浮水印的資訊，而浮水印的分解影像在藏入小波係數時，則是應用模數的運算依分解影像的位元去修改小波係數的值，因此只需一個小波係數便能藏入一個分解影像的位元。在前一節所提到的一些應用視覺密碼的數位浮水印技術絕大部分屬於空間域的方法，而其中的一些方法並未將浮水印藏入影像中，因此會產生誤認所有權的問題，而且有些方法則未充分利用視覺密碼的安全性，因此具有安全上的疑慮。本研究所提出的方法除了能夠解決上述的問題之外，也不會產生因影像太相似所造成誤解的問題，且在應用視覺密碼的方法時，是根據隨機的方式來採用分享的規則，可以避免攻擊者依循一定的規則來猜出所藏的浮水印影像。另外，本研究所使用的頻率域技術雖然在計算的量上較空間域來的多，但是對於抵抗訊號處理的破壞通常較空間域要來的強，因此利用頻率域技術來將浮水印藏入影像中可以使浮水印擁有較佳的強韌性(婁德權，張明昌，2004)。

第四節　研究限制

根據本研究所提出的方法，在藏入及取出浮水印時，對於不可察覺性、強韌性及負載量這三項條件能夠達到一定的平衡，並可在取出浮水印時不需原圖的輔助、取出的浮水印具有相當程度明確性及能夠在安全性上避免攻擊者對影像做非法的修改。

在現今的技術上要同時滿足不同形式浮水印的所有需求是有待繼續努力的，因此，在設計本研究方法時，有以下限制：

一、影像類型：

本研究是採用原圖為灰階影像且浮水印為黑白影像來做設計，其他類型的影像組合暫時不做考慮。

二、多浮水印：

多浮水印的條件主要是能提供合法的第三者也能加上自己的浮水印，且在個別取出浮水印時並不會互相影響，而這項條件將不列入本研究考慮的範圍。

本論文後續的章節架構安排如下：為了讓讀者對於本研究所使用的技術有一初步的了解，因此在第二章會先簡介本研究所使用到的視覺密碼與離散小波轉換的技術；另外會探討一些與本研究相關的文獻，接下來第三章詳細敘述本研究的方法，並在第四章呈現本研究的實驗結果，第五章會介紹一篇與本研究作法相似的論文並針對此篇論文與本研究進行比較；最後第六章則是本論文的結論與貢獻。