第六章　結論與貢獻

本研究所提出的浮水印加密方法是以視覺密碼與離散小波轉換這二種技術為主，利用視覺密碼分享的特性，將影像所有權分享給合法的擁有者，當要驗證擁有者的合法性時，只要取出疑似非法影像中的 share 與影像所有者手中的 share 重疊，便可確認此擁有者是否有侵權的嫌疑。本論文的貢獻條列如下：

一、有別於一般複雜的加密方法，本方法在藏入與取出浮水印的過程中相當簡易。

二、結合頻率域的方法找出影像中的高頻帶來藏入浮水印，並應用模數的運算，只需一個小波係數便能藏入一個分解影像的位元。

三、在取出浮水印的過程中不需要原始影像的輔助即可取出受攻擊影像中的浮水印。

四、具有與視覺密碼相等的安全性，任何單一張分享影像上皆不會洩露有關浮水印的資訊。

根據實驗結果顯示，在經過一般的影像攻擊後仍然能夠取出人眼能夠辨識的浮水印影像，確實能達到數位浮水印技術的強韌性要求。

未來本研究除了能採用其他不同類型的影像來做實驗之外，希望能夠結合其他領域的方法來加強本研究抵抗攻擊的強韌性，例如使用基因演算法(genetic algorithm, GA)來計算出模數 R 值及 α 值之間的最佳化，以滿足先前在第一章第一節所提到一個好的浮水印所需滿足條件之平衡。另外，本研究在藏入浮水印時，由於

浮水印是以 0 或 1 的形式來判斷該使用何種模數運算，所以任何數位形式的資料皆可做為本研究在保護智慧財產權時所使用的浮水印，並不只侷限於黑白影像，因此本研究未來希望能更靈活地利用其他的數位資料來做為浮水印，以增加本研究方法在應用上的多樣化。