行政院國家科學委員會專題研究計畫 成果報告

視覺密碼的應用－利用統計特性守恆的參數來保護數位影像
研究成果報告(精簡版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 97-2221-E-032-024-
執 行 期 間 ：97 年 08 月 01 日至 98 年 07 月 31 日
執 行 單 位 ：淡江大學資訊管理學系

計畫主持人：侯永昌

計畫參與人員：碩士班研究生-兼任助理人員：官振宇
碩士班研究生-兼任助理人員：廖欣音

報 告 附 件 ：出席國際會議研究心得報告及發表論文

處 理 方 式 ：本計畫可公開查詢

中 華 民 國 98 年 12 月 30 日

行政院國家科學委員會補助專題研究計畫成果報告

※※※

行政院國家科學委員會專題研究計畫成果報告

視覺密碼的應用－利用統計守恆的參數來保護數位影像
Applications of Visual Cryptography – Copyright Protection by Using Conservative Parameters from Digital Image

計畫編號：NSC97-2221-E-032-024
執行期限：97 年 8 月 1 日至 98 年 7 月 31 日
主持人：侯永昌　淡江大學資訊管理學系

一、中文摘要

隨著電腦與網際網路持續的發展創新，科技帶給人們的便利便不斷的衝擊人類社會，人與人之間資訊的交流比早期電腦還未發展時來的更加的容易且頻繁。但也因為如此，竊取、修改他人資訊也變得比以往簡單太多，不肖人士利用電腦及網路即可非法取得資料，因此如何防堵資料被偷竊與竄改就顯得非常重要。數位浮水印技術是一種將個人資訊加入到欲保護的媒體中的方法，日後受保護媒體產生爭議時，便可取出以證明其所有權，達到保護資產與驗證所有權目的。本研究以視覺密碼為基礎，應用統計學中的守恆特性產生視覺密碼所需要的分享影像。本研究的優點有三個：一，我們的方法以頻率域的方式嵌入浮水印，產生不擴展的分享影像，降低了像素值易受攻擊的影響。二，驗證所有權的過程不需要原圖的輔助即可取出浮水印。三，解決了保護影像被攻擊後的浮水印視覺效果不佳的問題。實驗結果證明，本研究對於 dark, light, blur, sharpen, noise, wave, jitter, jpeg 等攻擊有優異的抵抗性。

關鍵詞：視覺密碼、不擴展分享影像、浮水印技術、統計守恆

二、緣由與目的

由於數位時代的來臨、網路頻寬快速發展，資訊傳播比以往簡單方便得多，即使是一般民眾也能利用網路隨時得到自己想要的資訊。但換個層面思考，資訊取得容易固然是優點之一，但如果沒有對資訊做適當的保護，則資訊很容易會被別人竊取、竄改，所有權人對這些攻擊束手無策，毫無抵抗性。

為了保護重要的數位資產，許多保護機制相繼被提出，而數位浮水印技術即為其中一種。數位浮水印主要用途是保護資產的所有權，可用在不同型態的多媒體資料上。只要在資料上加入一組特別的訊號，它可能是原著的商標、或個人資訊等等；當需要驗證資料之所有權時，只要取出這組訊號，即可宣稱這個資訊是由某人所有，而達到保護智慧財產權之目的。這組訊號便稱之為數位浮水印。

目前已有許多研究將視覺密碼結合於數位影像浮水印領域。浮水印的嵌入方式大約可分為空間域、以及頻率域兩種處理方式。空間域的優點是計算上較簡化，因此沈昌興等人[1]便利用機密影像最高位元平面結合浮水印產生兩張分享影像，但缺點是分享影像比原圖擴展了兩倍。Hsu(2005)[14]根據統計之中央極限定理，抽樣分配求出樣本均數(Sampling Distribution of Means; SDM)，求出樣本平均數藉以產生分享影像。但缺點是樣本數量要大，樣本分布才會趨近於常態，且分享影像及還原影像皆擴展至原圖的四倍。黃培修(2007)[5]改進 Hsu 缺點，利用統計大數法則之特

性，以隨機樣本比大小的方式，產生非擴展式的分享影像。但是在受保護影像遭遇攻擊時，原本像素值不等的像素配對可能會變成相等，或原本像素值相等的像素配對可能會變成不等，造成兩個像素比較的結果也會跟著改變，使得產生分享影像過程會有誤差。

本研究旨在改進上述缺點，以影像頻率域的方式，並利用即使影像遭受攻擊、統計特徵仍然不會大幅改變的特性，與視覺密碼結合，以應用在數位財產的保護上。我們的研究將採用分享影像不擴展的技術，並期望產生出對於攻擊抵抗性佳的分享影像，即使受保護影像在遭受攻擊後，取出的浮水印仍有良好的視覺效果。

三、研究方法

（一）視覺密碼：

視覺密碼的概念最初是由Noar & Shamir[19]提出，相較於傳統密碼學在加解密的過程中都需要複雜的數學運算，視覺密碼的概念是：在加密的過程中，藉由一定的加密規則來打亂機密影像的像素分布，將機密影像加密成為n張分享影像，讓分享影像看起來是雜亂無章、無法顯示出任何有關原始影像的蛛絲馬跡。在解密的過程中完全不需要複雜的數學運算，只要有k張($k \le n$)或k張以上的分享影像疊合，即可還原機密影像，利用人類視覺來辨識機密影像的內容；反之，如果分享影像疊合張數少於k張，機密影像就無法還原，也就是無法在疊合影像上顯示機密影像的內容，此即為所謂的(k, n)門檻值(k-out-of-n threshold)。

（二）視覺密碼應用於浮水印技術：

視覺密碼的概念最初是由Noar & Shamir[19]提出，相較於傳統密碼學在加解密的過程中都需要複雜的數學運算，視覺密碼的概念是：在加密的過程中，藉由一定的加密規則來打亂機密影像的像素分布，將機密影像加密成為n張分享影像，讓分享影像看起來是雜亂無章、無法顯示出任何有關原始影像的蛛絲馬跡。在解密的過程中完全不需要複雜的數學運算，只要有k張($k \le n$)或k張以上的分享影像疊合，即可還原機密影像，利用人類視覺來辨識機密影像的內容；反之，如果分享影像疊合張數少於k張，機密影像就無法還原，也就是無法在疊合影像上顯示機密影像的內容，此即為所謂的(k, n)門檻值(k-out-of-n threshold)。

視覺密碼的概念就是利用機密影像產生出兩張半黑白的分享影像，當分享影像疊合在一起時，就可以顯示出機密影像內容。如果可以從我們所擁有的智慧資產中產生一張分享影像，配合我們手中當成身分認證的另外一張分享影像，只要兩張分享影像疊合之後能顯現出我們所需要的浮水印，就可以達成驗證智慧財產權的目的。

視覺密碼所產生的每一張分享影像上都有50%的黑點和50%的白點，從編碼的理論上來看，每張分享影像就是一連串0和1的組合。如果我們能從原圖中產生隱含原圖資訊的0、1串列，就可以產生出我們所需要的一張分享影像(master share)(如圖1所示)。有了master share和浮水印的資訊，透過視覺密碼的加密規則，就能製作出另一張分享影像(ownership share)。Master share可以丟棄不要，ownership share需要保存下來，代表我們身分認證的憑證，日後可以用它來驗證智慧財產權。

往後若智慧財產所有權發生爭議時，只需要從爭議影像中產生出mater share’，和我們手中的身分憑證ownership share疊合，如果能顯現出浮水印的資訊，表示這項資產的所有權歸我們所有，而達到驗證所有權的目的。

視覺密碼運用在浮水印機制時，由於浮水印並不會實際嵌入至原圖中，因此不會破壞原圖，取出浮水印時亦不需要參考原圖，並且只要將分享影像互相疊合，即可利用人類視覺解密，不需要複雜的數學運算就能辨到。因此，視覺密碼與浮水印技術結合的研究重點就在於：如何從原圖中取出隱含原圖資訊的0、1串列並產生出分享影像。

（三）統計守恆：

我們發現一張影像遭受影像處理軟體攻擊後，通常都還能保持一定的影像品質。也就是影像中原來的山還是山、海還是海；影像中紅色的部份仍然要保持比較紅、綠色的部份仍然要保持比較綠；被攻擊影像的像素值雖然都有所更改，但它的外觀仍然與未受攻擊前差不多。因此，不難發現像素的分配仍然能維持一定的規律。

影像皆由一個個像素所構成，將這些像素以數值量化之後，這些像素值就代表了這個數位影像。通常一張數位影像上有為數眾多的像素，因此統計學就成了幫助我們了解這群資料特性的工具。一般來說，由於母體數量可能過於龐大，計算上太複雜，因此通常會以抽樣的樣本來代表母體，並以統計量(statistic)來表現出樣本資料的特性[2, 6]。統計量可分為兩種：一是代表資料集中趨勢的算術平均數、中位數；另外一類是代表資料離散趨勢的變異數、四分位差等。

在觀察中，我們發現一張圖像中可以保持穩定的性質大致可歸類於以下三種：最高位元平面、常態分配、大數法則。

一、最高位元平面：在影像遭受攻擊時，外觀卻不會有大幅的改變，這是因為最高位元通常最不容易被更改到，所以才能保留最大多數的影像外觀，因此我們可以說最高位元平面對於影像攻擊擁有最佳的強固性。沈昌興[1]就是利用這個特性，以最高位元平面製作出具強固性的分享影像。

二、常態分配：根據中央極限定理(Central Limit Theorem)，一個自母體抽出的樣本所計算出的樣本平均值，只要樣本的抽樣數夠大($n > 30$)，樣本平均值會趨近於以母體平均值為中心的常態分配(Normal Distribution)；且樣本平均值大於母體平均值的機率會與小於母體平均值的機率相當，也就是$Pr(x_t \geq \mu)=Pr(x_t \leq \mu) = 0.5$ [7]；因此Hsu [14]便以此特性來產生驗證浮水印所需的master share。但是，當數據中出現異常的極大值或極小值時，算術平均數有可能會偏離正常的中心位置，產生誤差，因而影響其代表性。

三、大數法則：在一個龐大的群體中，若將每個個體獨立看待，則每個個體的出現都是看似隨機且不相關連的存在。但是若將這些個體加以歸類，便可發現這些個體都是依據某種規律性而出現，這種規律性的特性便是機率理論中的大數法則。依照大數法則的定理，只要實驗的次數夠多，那麼每種結果所出現的機率會趨近於理論值[7]。黃培修[5]便利用大數法則的性質，每次取出成對的樣本(a, b)加以比較，預期a比b大的機率應該與b比a大的機率相當。若將這種規律性應用在分享影像的像素分配上，則可預期分享影像上黑色與白色像素出現的機率將趨近於各50%，而產生隨機且雜亂無章的分享影像。

由以上可知，即使影像遭到攻擊，像素整體的分配仍會因為統計的守恆而不會被輕易的改變。因此將視覺密碼的概念配合統計特性所產生的Master share與Ownership share應具有相當好的保守性。當智慧資產的身分需要驗證時，先從資產中產生Master share’，再配合我們手中所握有的Ownership share，如能疊合出浮水印的字樣，就可宣稱該資產所有權為我們所有，達到智慧資產身分驗證的目的。

（四）改良式像素配對：

Hsu和黃培修在處理影像時皆採用空間域的做法，也就是以像素值為處理的主要對象。但是像素值容易受到攻擊或影像處理的影響，而發生改變，使得因此而產生的Master Share也容易發生變化，造成在驗證浮水印時NC值不佳的結果。本研究則採用頻率域的做法，先將受保護影像進行三階的小波轉換，因為LL3低頻帶中的每一個係數都濃縮了許多像素的像素值，也就是它保有原影像最多的資訊，如果利用LL3的係數來代替原影像，必定可以減少個別像素的影響，降低Master Share發生改變的機率。以512*512大小的影像為例，進行三階小波轉換後的LL3頻帶大小仍然有64*64，樣本的數量大小已非常充足。因此我們取出LL3頻帶中的像素，每次隨機選取兩個像素來進行比較，依據大數法則，我

們可以預期比較結果會具有大小機率各半的特性，我們利用這個特性來產生分享影像，使得分享影像上的黑點與白點能夠平均分佈；而且當受保護的影像遭受攻擊後，仍能因為大數法則定理的作用，使得像素配對的結果仍具有守恆特性的關係，讓我們可以取出正確的master share，達成驗證數位資產所有權的目的。

我們的浮水印將以不可見的強固型為主，由於取出時不需要原圖，也不需要原浮水印的輔助，因此屬於半盲型的浮水印，並且嵌入浮水印的方式為頻率域。我們的實驗以512*512大小的灰階影像為對象，保護影像的過程可分為兩個部份：第一部分為嵌入數位浮水印，產生出兩張分享影像Master share和Ownership share；第二部分為數位資產所有權的驗證過程。

一、浮水印嵌入步驟：

第一部分為將浮水印嵌入於分享影像而產生出Master share及Ownership share。產生Master share和Ownership share的步驟如圖2所示。

輸入：受保護影像(大小為H_1*W_1)、浮水印(大小為H_2*W_2)、種子(S)

輸出：分享影像Master share及Ownership share。

步驟一：對受保護的影像做三階的Haar離散小波轉換，並取出LL3的區塊中的所有像素值。

步驟二：利用亂數S產生一序列種子S = {s_1, s_2, s_3, …, s_n | $n = 2(H_2*W_2)$}個位址，接著利用這序列S逐一定出經過三階Haar小波轉換後LL3區塊的所有位址後，取出這些位址的像素值。

步驟三：接著每次從LL3並經過亂數定址的位置中，每次選取兩個像素以比較像素值的大小。

若是前一個像素大於後一個像素，則設定像素為白色；若是前一個像素小於後一個像素,則設定像素為黑色。若前一個像素等於後一個像素，則用樣本的座標來決定像素為黑或白；若座標取mod 2等於0，就設定像素為白色；若座標取mod 2等於1，則設定像素為黑色。

步驟四：Ownership share的產生必須配合浮水印的像素和Master share來決定。若浮水印像素為白色，則選擇與Master share相同的像素；若浮水印像素為黑色，則選擇相反的像素，因此兩張分享影像疊合後，浮水印白色部份在疊合影像上將呈現半黑半白，而黑色部份則為全黑。

步驟五：重複步驟三和步驟四直到每一個浮水印的像素都被分解成Master Share和Ownership Share上的像素為止。這樣兩張分享影像Master share和Ownership share就產生出來了。

為了達到驗證身份的目的，兩張分享影像產生後，我們保留Ownership share以及種子S以作為日後身分認證用，而Master share就可丟棄不用。

一、資產所有權驗證步驟：

第二部份的數位資產所有權的驗證過程，如圖3所示。

步驟一：需要驗證受爭議影像(O')之所有權時，先對受爭議影像進行三階的Haar離散小波轉換，再以手中所握有的亂數種子(S)逐一定址LL3區塊的所有位址。

步驟二：每次取出兩個像素依像素分享規則進行比較，若是前一個像素大於後一個像素，則設定像素為白色；若是前一個像素小於後一個像素,則設定像素為黑色。若前一個像素等於後一個像素，則用樣本的座標來決定像素為黑或白；若座標取mod 2等於0，就設定像素為白色；若座標取mod 2等於1，則設定像素為黑色。

步驟三：重複步驟二直到取出H_2*W_2個像素為止，即可產生相對應的master share'。

步驟四：將master share'與自己手中所握有的ownership share進行疊合，如能取出代表數位財產權的浮水印，就表示這項資產的所有權已被驗證。

四、結果與討論

（一）實驗環境

作業系統環境為windows XP service pack 3，Intel Core2 Duo處理器，記憶體為2GB，以Java 6.0做為程式開發工具。實驗對象分別以lena、food、flower、mario等四張受保護影像做實驗(圖4)，每張大小皆為512*512、並經過灰階處理；浮水印為256*256的”淡江資管”黑白影像(圖5)。

（二）攻擊實驗

下面將以Photoshop CS4為工具，對受保護影像lena, food, flower 和mario分別進行light, dark, blur, sharpen, noise, wave, jitter, crop, jpeg等攻擊，再利用NC值檢驗經過攻擊後受保護影像所產生的浮水印與原浮水印的相似程度(圖6)。

Light攻擊是將受保護影像調亮20%的亮度，Dark攻擊是將受保護影像調暗20%的亮度，Blur攻擊是將受保護影像作高斯模糊的處理，Sharpen攻擊是將受保護影像做更銳利化的處理，Noise攻擊是將受保護影像加入12.5%的雜訊，Wave攻擊是將受保護影像做漣漪效果的扭曲，Jitter攻擊是將受保護影像的左邊剪下六個像素寬的長方形，再貼到右邊，Jpeg攻擊是壓縮受保護影像。

的優點，以Haar小波轉換為基礎，並將統計學的守恆特性應用在數位財產的保護中，製作出黑白像素出現機率各半且分布均勻的分享影像。分享影像疊合後浮水印字樣仍為全黑，而浮水印字樣以外所出現的黑與白機率各為1/2，因此浮水印字體顯而易見。即使當受保護影像經過dark, light, blur, sharpen, noise, wave, crop, jitter, jpeg等攻擊，所產生出的Master share’也能夠發揮統計學守恆的作用，使得像素比較的結果不易受更改，也就是Master Share’與Master Share更為近似，因此疊合出的浮水印NC值仍能保持在90%以上，顯示我們的方法對於攻擊的抵抗性佳。

本研究所提出的方法，相較於Hsu以樣本平均數進行比較，我們的方法需要的樣本數較少，計算量因此降低；而和黃培修以空間域的方式進行像素比對相比，以小波轉換後的LL3係數來當作母體，可以減少單一像素的變動性。並且以像素的統計特性比較的結果相對穩定，所以即使受保護影像遭遇攻擊，像素比較結果也不易被改變。我們的方法不僅將浮水印嵌入於不擴展的分享影像，在驗證所有權的過程也不需要原圖的輔助；並且也解決了保護影像被攻擊後的浮水印視覺效果不佳的問題。

五、結論

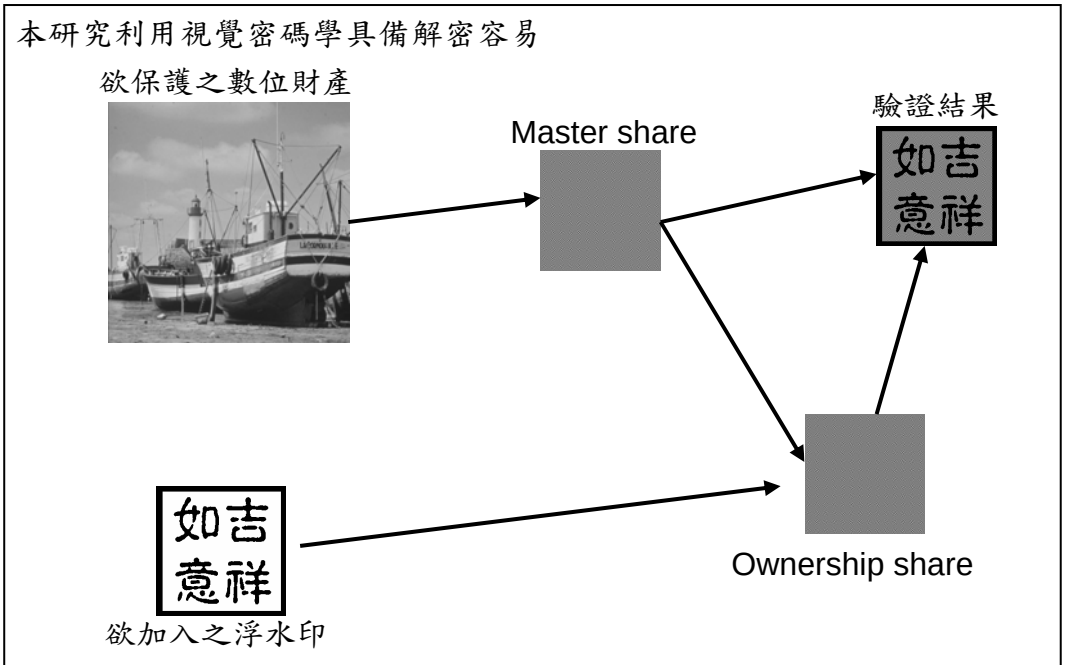


圖 1 視覺密碼應用於浮水印之模型

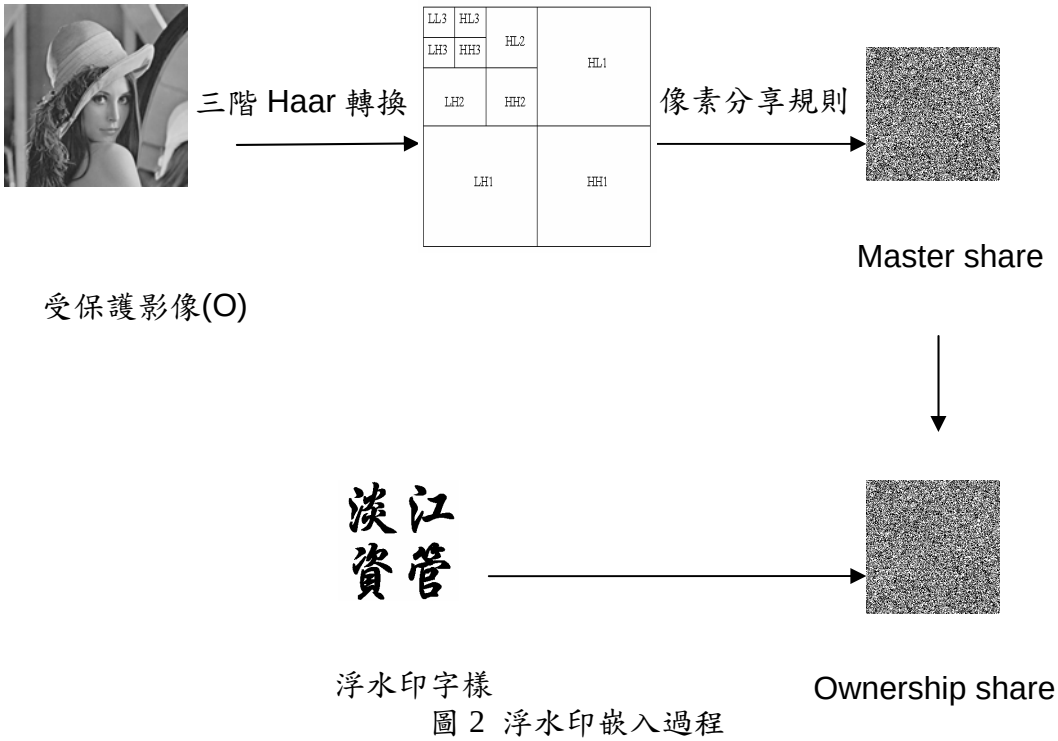


圖 2 浮水印嵌入過程

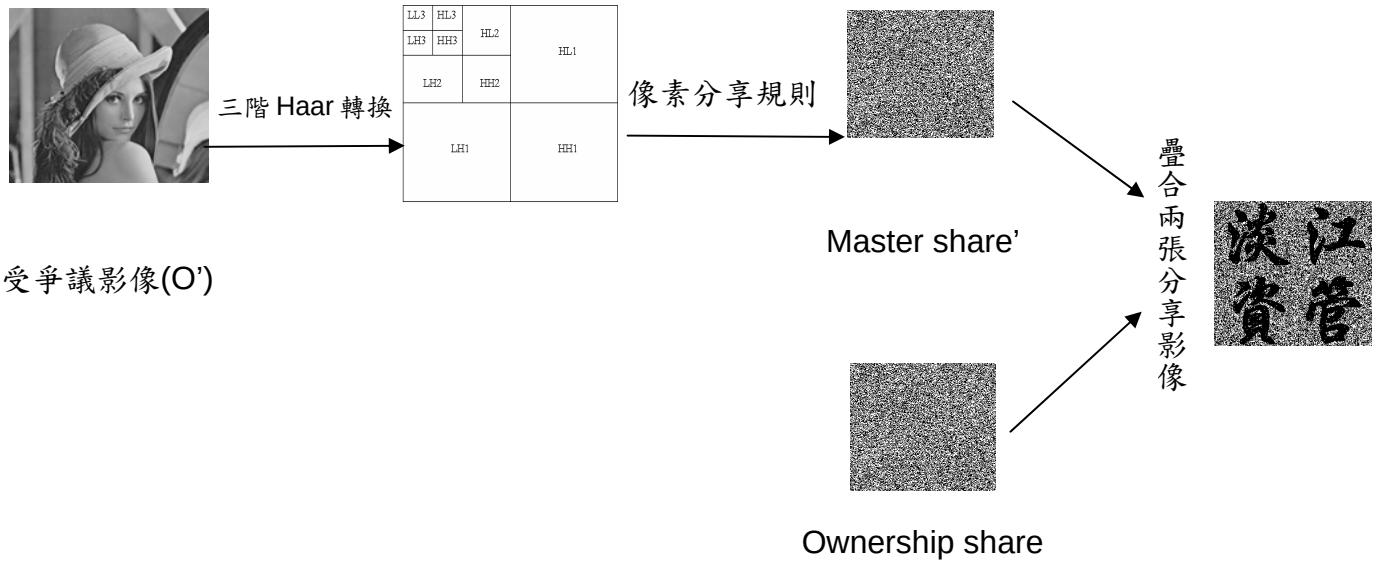
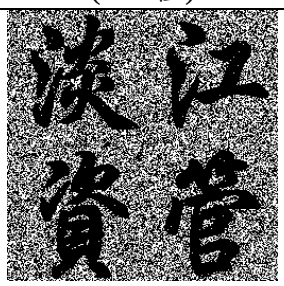
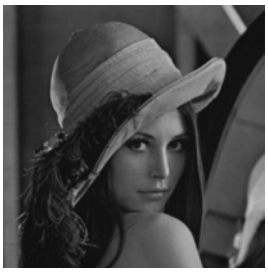
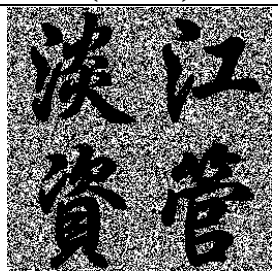
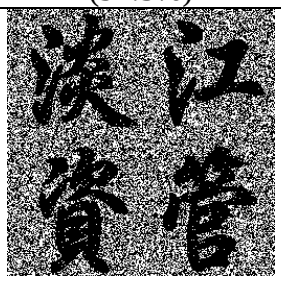
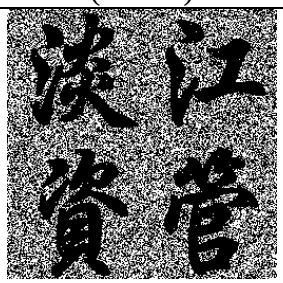
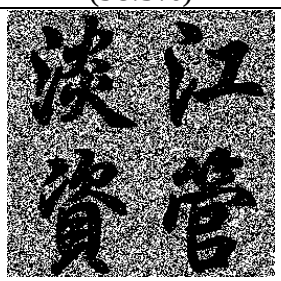
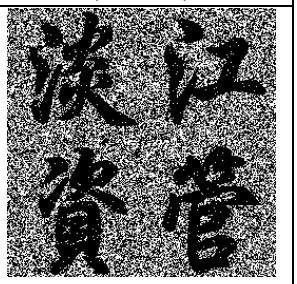
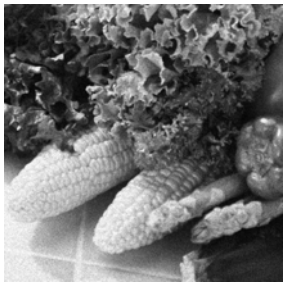
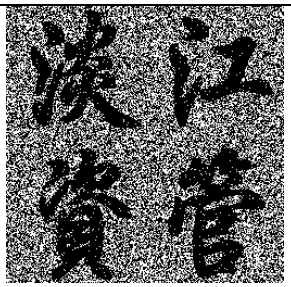
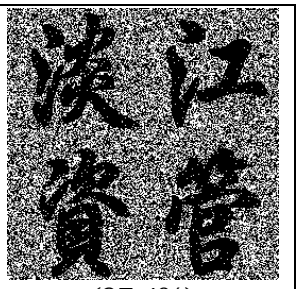
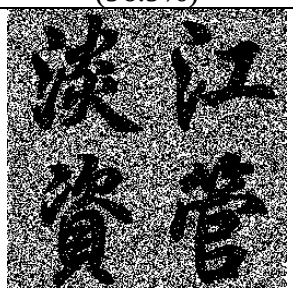


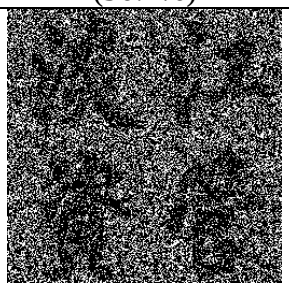
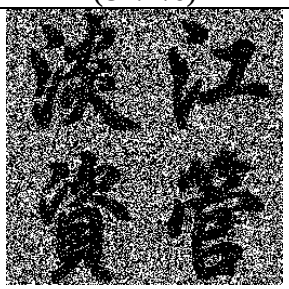
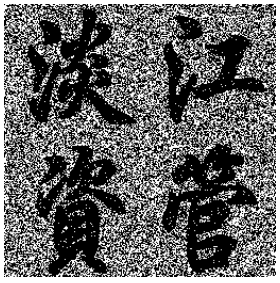
圖 3 影像驗證過程

圖 4 受保護影像(512*512) (a) lena (b) food (c) flower (d) mario

受攻擊影像 (Light)	疊合後的浮水印 (NC 值)	受攻擊影像 (Blur)	疊合後的浮水印 (NC 值)
	 (99.4%)		 (98.2%)
	 (99.7%)		 (97.5%)
	 (99.9%)		 (98.3%)
	 (99.8%)		 (99.0%)

受攻擊影像 (Noise)	疊合後的浮水印 (NC 值)	受攻擊影像 (Wave)	疊合後的浮水印 (NC 值)
	 (94.3%)		 (98.0%)
	 (95.5%)		 (97.4%)

	 (96.9%)		 (97.4%)
	 (97.4%)		(98.9%)

受攻擊影像 (Jitter)	疊合後的浮水印 (NC 值)	受攻擊影像 (Jpeg)	疊合後的浮水印 (NC 值)
	(90.1%)		(96.4%)
	 (82.2%)		(96.6%)
	 (93.4%)		(97.0%)
	(92.3%)		 (97.4%)

六、計畫成果自評

本研究利用視覺密碼學具備解密容易的優點，以Haar小波轉換為基礎，並將統計學的守恆特性應用在數位財產的保護中，製作出黑白像素出現機率各半且分布均勻的分享影像。分享影像疊合後浮水印字樣仍為全黑，而浮水印字樣以外所出現的黑與白機率各為1/2，因此浮水印字體顯而易見。即使當受保護影像經過dark, light, blur, sharpen, noise, wave, jitter, jpeg等攻擊，所產生出的Master share'也能夠發揮統計學守恆的作用，使得像素比較的結果不易受更改，也就是Master Share'與Master Share更為近似，因此疊合出的浮水印NC值仍能保持在90%以上，顯示我們的方法對於攻擊的抵抗性佳。

本研究所提出的方法，相較於 Hsu 以樣本平均數進行比較，我們的方法需要的樣本數較少，計算量因此降低；而和黃培修以空間域的方式進行像素比對相比，以小波轉換後的 LL3 係數來當作母體，可以減少單一像素的變動性。並且以像素的統計特性比較的結果相對穩定，所以即使受保護影像遭遇攻擊，像素比較結果也不易被改變。我們的方法不僅將浮水印嵌入於不擴展的分享影像，在驗證所有權的過程也不需要原圖的輔助；並且也解決了保護影像被攻擊後的浮水印視覺效果不佳的問題。

五、參考文獻

[1] 侯永昌，沈昌興，“基於視覺密碼之不可察覺的浮水印技術”，*第六屆資訊管理暨實務研討會論文集*，新竹，F1，民國 89 年十二月。

[2] 林光賢，統計學概念與方法，幼獅文化事業公司，民國 78 年八月出版，pp. 31-54。

[3] 陳同孝，張真誠，黃國峰，數位影像處理技術，旗標出版股份有限公司，民國 95 年九月出版，pp. 1-1 – 1-6, 8-1 – 8-14。

[4] 張明昌，婁德權，劉江龍，“運用影像特徵於浮水印研究”，國防大學中正理工學院國防科學研究所博士論文，民國九十四年八月。

[5] 黃培修，“結合非擴展式視覺密碼與機率理論於數位影像之保護”，淡江大學資訊管理學系碩士論文，九十六年六月。

[6] 趙元甫，“資料隱藏技術之研究”，國立中央大學碩士論文，八十八年六月。

[7] 賴鐵軍，郭祝武，應用統計學，全華科技圖書股份有限公司，民國九十二年三版一刷，pp. 5.1 - 5.29。

[8] Blundo, C. and De Santis, A., “Visual Cryptography Schemes with Perfect Reconstruction of Black Pixels”, *Computer & Graphics* (12:4), 1998: pp. 449-455.

[9] Chang, C.C., Hsiao, J.Y., and Yeh, J.C., “A Colour Image Copyright Protection Scheme Based on Visual Cryptography and Discrete Cosine Transform”, *Imaging Science Journal*, vol.50, 2002, pp.133-140.

[10] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-jeng Wang, Hung-Min Sun, “Adaptive data hiding in edge areas of images with spatial LSB domain systems,” *IEEE Transactions on Information Forensics and Security*, Vol. 3, Issue 3, Sept. 2008, pp. 488-497.

[11] C.S. Pei, Y.C. Zeng, “Temper Proofing and Attack Identification of Corrupted Image by Using Semi-fragile Multiple-watermarking Algorithm,” *ASIACCS*, pp. 166-174, March 2006.

[12] Fridrich, j., Goljan, M., Rui Du, “Detecting LSB steganography in color, and gray-scale imges,” *IEEE Multimedia*, Vol. 8, Issue 4, Oct.-Dec. 2001, pp.22-28.

[13] Hou, Y.C. and Tu, S.F., “Visual Cryptography Techniques for Color Images without Pixel Expansion”, *Journal of Information, Technology and Society*, 2004(1), pp.95-110.

[14] Hsu C.S. and Hou Y.C., 2005.07, “Copyright protection scheme for digital images using visual cryptography and sampling methods”, *Optical Engineering*, Vol. 44, Issue 7,

pp. 077003 (10 pages).

[15] Ito, R., Kuwakado, H., and Tanaka, H., "Image Size Invariant Visual Cryptography", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science* (E82-A:10), 1999, PP.2172-2177.

[16] Kalantari, N.K., Akhaee, M.A., Ahadi, S.M., Amindavar, H., "Robust Multiplicative Patchwork Method for Audio Watermarking", *IEEE Transactions on Audio, Speech and Language Processing,* Vol. 17, Issue 6, Aug. 2009, pp. 1133-1141.

[17] Lee S.J. and Jung S.H., "A Survey of Watermarking Techniques Applied to Multimedia", *Proceedings of IEEE International Symposium on Industrial Electronics* vol. 1 (2001), pp. 272-277.

[18] Lou, D.C., Tso, H.K., Liu, J.L., "A copyright protection scheme for digital images using using visual cryptography technique," *Computer Standards & Interfaces* 29 (2007) 125–131.

[19] Noar, M. and Shamir, A., "Visual Cryptography", *Advances in Cryptology:Eurpocrypt' 94*, Springer-Verlag, Berlin, 1995, pp.1-12.

[20] Ruanaidh, J.J.K.O., W.J. Dowing and F.M. Boland, "Watermarking Digital Images for Copyright Protection", *IEE Proc. – Vis. Image Signal Process*, Vol. 143, No. 4 August 1996, pp. 250-256.

[21] Sluciak, O., Vargic, R., "An audio watermarking method based on wavelet patchwork algorithm," *15th International Conference on Systems, Signals and Image Processing,* 2008, June 2008, pp. 117-120.

[22] Sureca, B., Dr. Swamy, GN., Dr. Srinivasa Rao, K., A Ravi Kumar, "A Watermarking Technique based on Visual Cryptography," *Journal of Information Assurance and Security* 4 (2009), 470-473.

[23] S.Joo, Y. Suh, J. Shin, H. Kikuchi, S. J. Cho, "A new robust watermark embedding into wavelet DC components," ETRI Journal 24(5) (2002) 401- 404.

[24] Y. Wang, J.F. Doherty, R.E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Transactions on Image Processing* 11 (2) (2002) 77-88.

參加 1st International Conference on Computer Support Education (CSEDU 2009) 心得報告

淡江大學資訊管理系　侯永昌

一、參加會議經過

The 1st International Conference on Computer Support Education (CSEDU 2009) 是由 INSTICC (Institute for Systems and Technologies of Information Control and Communication) 主辦，WfMC (Workflow Management Coalition)、IICREST (Interdisciplinary Institute for Collaboration and Research on Enterprise Systems and Technology)、IEEE Education Society Chapter, Portugal Section、IEEE Portugal Section 所贊助的國際研討會，會議於 2009 年 3 月 23 至 26 日在葡萄牙的里斯本市舉行，，會議場地選在 SANA Metropolitan Hotel。本次大會共有 3 個會場同時舉行，有來自 20 多個國家的學者專家，發表 144 篇研究論文，分為 20 個 oral session 和 3 個 poster session，另外還有 6 場 keynote lecture。會議涵蓋的領域有：Information Technologies Supporting Learning、Learning/Teaching Methodologies and Assessment、Social Context and Learning Environments、Legal and Cultural Management Issues 和 Domain Applications and Case Studies 等多個主題，參加者可以自由選擇有興趣的主題來聽講。此次會議的內容豐富，兼具理論及實務，提供參加人士了解資訊科技在教育支援與學習評估領域中的發展現況及未來發展的趨勢。筆者的論文「LEARNING WITH FUN - An Application of Visual Cryptography」被安排在 3 月 26 日 11:15 – 12:00 的「Information Technologies Supporting Learning」分組中發表，並與數位聽講學者交換意見，研究內容與會人士相當的肯定。

二、與會心得

此次會議是以「資訊科技支援教育工作」(Computer Supported Education)為主

軸，希望藉助學者專家的研討，可以提昇方法論和相關支援教學工具的水準，以幫助人們提升資訊科技在教育支援與學習評估的方面的作用。本次研討會特別強調 new educational environments、best practices and case studies、institutional policies、open and distance education 等議題，在這一次的研討會中，我們可以感覺到資訊科技早已滲透到教育與學習這個領域，而且愈來愈強調實際應用的層面，對於它所造成的衝擊和影響也吸引了很多學者競相投入相關的研究。

三、建議事項

國內學者只有本人參加此次會議，發表論文，但來自大陸的與會者卻有七八位，明顯的多於國內學者。建議教育部或國科會多補助國內有興趣參與國際會議的學者出國參加學術會議，以了解研究的新趨勢和增加與國外學者交流的機會。