行政院國家科學委員會專題研究計畫期中報告
影像分享:基礎、技術與應用(第二年期)
Image Sharing: fundamentals, techniques, and applications

計畫編號：NSC 92-2213-E-009-032
執行期限：92 年 8 月 1 日　93 年 7 月 31 日
主持人：林志青 交通大學資訊科學系所
計畫參與人員：陳尚寬、張御傑、洪國賢
交通大學資訊科學系所

一、　中文摘要

本計畫在第二年裡共有四個主題，第一個主題是藉由改良機密影像分享的方法，使其能隱藏重要的資料；而且是在不增加額外空間的前提下(例如512×512機密影像藏在 4 張256×256的 Host 影像)，達成資料隱藏的目的。在第二個主題中，我們將浮水印的技術以兩種不同的風貌在分存中出現，除了機密影像分享本身具有的容錯性、傳輸效率性等等之外，也因這些浮水印的使用而達到智慧財產權的認證，並增加安全性。第三個主題是針對分存可能在各分存所在地（各子公司）被施以影像處理，如均化、銳化或影像強化等，因而須做出一些保護的措施，使得影像處理過後的分存還是可以湊齊足夠份數後就仍能還原回原來影像。在第四個主題中，我們提出一個新的嘗試，讓機密影像分享的機制在頻域空間上操作。

關鍵詞：影像分享；數位浮水印；資料隱藏；強固性影像分享；頻域空間

Abstract

There are four topics in the second year. The first topic is to design some image sharing methods so that we can embed important data, after sharing, in the shadow stego images. The purpose of data hiding is achieved in the premise that the methods do not need additional storage space. In the second topic, we investigate two watermarking techniques suitable to embed watermarks in shadows. In addition to the advantage that the secret image sharing itself already has failure-tolerance and transmission efficiency, this extension enforces the image sharing methods applicable to various practical applications, including property rights. The third topic considers the cases in which the shadows might be processed using certain image processing steps (e.g. equalization, sharpness, and image enhancement). We intend to propose a protection method which makes the secret image can be recovered. In the fourth topic, we try to design secret image sharing methods in the frequency domain.

二、　計畫緣由與目的

在我們之前所作的一年期計畫（影像分享之初步研究 NSC 90-2213-E-009-131，90/8~91/7）主要是發展一套分享的演算法，其處理對象是一張機密影像，經過此分享方法產生多份分存，儲存在各個分散式資料庫當中；收集 t 份正確分存，即可還原出機密影像。然而，在真實世界中，影像可能會被經過各種處理（例如：均化、壓縮、雜訊)、或者是要加

入一些資料安全訊息（例如：資料隱藏、數位浮水印）；因此，目前之計畫的第二年就是要將機密影像分享法與各種處理機制相結合，主要目的是探討經過各種影像處理機制後，原始影像與各個分存之間的影響與關連。在第二年計畫的第一個主題中，資料隱藏的觀念，就像某些動物的保護色一樣，牠們巧妙地將自己隱藏於環境中，免於被天敵發現而遭受攻擊。若我們是將機密影像利用分享機制打散為各分存，則會對每份分存亦希望加以保護。因為敵人若只盜少數幾份分存，那倒不會洩露出機密影像。但若被盜取夠多份分存，則機密不保。因此各分存仍須加以隱藏以保護之。

第二個主題是數位浮水印的觀念，主要是在著作權的保護。數位浮水印可分成可視和不可視兩類，其做法也各不相同。前者最常見的例子，就是有線電視頻道上所傳送的視訊資料，角落通常會有屬於該頻道所特有的半透明商標（logo），其最主要目的乃在於嚇阻作用，防止非法的使用，雖然減低了該資料的商業價值，卻無損於擁有人的使用。相反的，不可視的數位浮水印藉由將屬於原創作者的數位浮水印嵌入於影像資料中的不顯眼處，做為將來起訴非法使用者的舉證，因此其最主要的目的乃是增加起訴非法使用者的成功率，以保障原創作者的權利。我們希望在我們的影像分存裡能擁有浮水印，以宣示分存的版權。設計上，不論是可視或不可視浮水印，我們都希望能各設計出一套。

在第三個主題中，我們知道雜訊與各種影像處理對於一般的影像有時候雖是具有某種破壞程度，但是仍有可能屬於可以辨識的範圍。然而對於機密影像的分存所做之影像處理或破壞，卻會有更大的衝擊，因為會對還原影像品質造成非常大的影響。所以我們須特別的機制來防止此類施諸於分存之衝擊。

而本計畫的第四主題在探討頻域空間的分享法。處理影像通常分為在值域空間（spatial domain）與頻域空間（frequency domain）的操作兩種。目前存在的機密影像分享法（包括前一年所發展的機密影像分享法）都是針對值域空間；但是，根據以往的經驗，例如數位浮水印，在頻域空間的表現較值域空間為佳。因此，在目前機密影像分享皆在值域空間的研究上來看，在頻率空間的研究便是一個新的而且值得去開發的領域。

目的:

本計畫的研究目的分述如下：

1. 擴充機密影像分享法則，使其能夠與目前的資料隱藏相結合，以達到更進一步的資料安全性與智慧財產權的保護。
2. 設計一套適合機密影像分享的數位浮水印機制，使得在影像分存也能抽取出隱藏式數位浮水印，或是影像分存上直接有可視的浮水印，因而達到保護影像智慧財產權的目的。
3. 設計一套具有自我驗證與修復能力的影像分存 – 能夠偵測各分存是否受到竄改；並且容忍分存受基本的影像處理所造成的破壞，順利的自我修復。
4. 由值域空間機密影像分享法的概念出發，發展出對於頻域空間的機密影像分享法。以適應各種影像壓縮格式。

三、 結果與討論

在第一個主題：機密影像分享嵌入資料隱藏，我們設計了一個簡單、快速並且適合機密影像分享核心的資

料隱藏演算法。將機密影像分享後所得到分存分別透過此演算法隱藏於一般影像中，由於經過證明隱藏後的影像與原來的一般影像的差異最多只有8(以灰階影像的灰階值而言)，因此在不影響人類視覺的觀念下，將重要的分存資訊藏於一般影像中，而避免被駭客或有心人士發現，因而被取出或被竄改。我們在圖例一展示了 Host 影像和藏入分存後的 stego 影像。原機密影像是 512×512 而各 Host 為 256×256 且只要 4 份 256×256 stego 影像就可組出機密影像。在第二主題：嵌入數位浮水印的機密影像分享，在第一部分(不可視浮水印)，我們將影像經過機密影像分享，產生若干分存後，利用擴增多項式的方法，經由所擴增項數的係數，去調整每一個分存的數值，如此的調整，並不影響還原後的結果，卻同時可以符合內定數位浮水印的規則，使得我們可以直接從任一分存中，取得事先嵌入的數位浮水印，並且可以無失真的還原原始的機密影像。我們在圖例二展示了嵌入前與嵌入後的分存，看起來並沒有什麼不同，但是可以從嵌入後的任一分存中抽取出事先嵌入的浮水印。在第二部分(可視浮水印)，我們在分存中嵌入可視的浮水印，在還原回原影像時，可以有兩種選擇:第一種是在還原的影像中仍然保有可視的浮水印;第二種是在還原的影像中不會看到可視的浮水印。圖例三展示了嵌入有可視浮水印的分存，以及由這些分存還原回的原始機密影像。在第三主題：加強機密影像分享遭影像處理的可還原性，我們將原圖的資訊交錯隱藏在分存中，並且在還原為原始機密影像的過程中，可以自動偵測並修補被損毀的部分，使得原始的機密影像即使在分存被竄改，仍然可以還原回可辨認的原始機密影像。我們在圖例四展示了當分存被破壞時未經修補與經修補過後的還原影像。在第四個主題：機密影像分享的機制在頻域空間上的實行，由於頻域空間的數值比值域空間的範圍較大且不一定為正的浮點數，因此我們必須要透過 JPEG 壓縮和一個分割機制來轉換數值，並且根據頻域空間上的係數的重要性不同(例如，低頻、中頻、高頻)，因此在分割上必須採取適應於不同位置的處理方式，才能將其係數轉換成適合我們的機密影像分享的輸入。

四、 計畫成果自評

第二年的前二大主題，我們均成功的達成預期目標與成果，目前正在整理即將投稿至國際期刊。而第三個主題，對於一般性的破壞(例如：雜訊)，我們均能有效的修補，但對於一些影像處理(例如：均化、銳化)，是我們亟待努力的研究空間。至於最後一個主題，我們已經設計出適合機密影像在頻域空間上操作的機制。實做則仍在進行中。其結果會在期末報告寫入。

五、 參考文獻

[1] C.C. Chang and R.J. Hwang, “Sharing secret image using shadow codebooks,” *Information Science*, Vol. 111, No. 1-4, pp. 335-345, 1998.

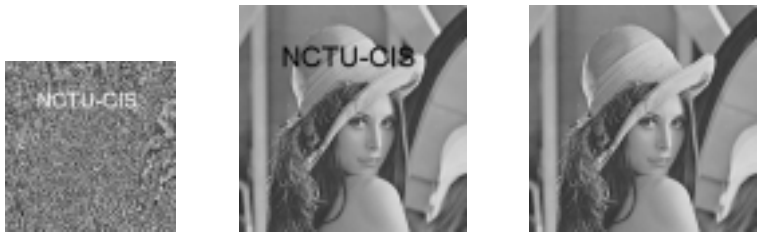
[2] C.C. Thien and J.C. Lin, “Secret image sharing,” *Computers and Graphics*, Vol. 26, pp. 765-770, 2002

(a) (b) (c) (PSNR=52.39 db) (d) (PSNR=52.39 db)

圖例一 第一主題-512×512 機密影像分享嵌入隱藏之實驗結果(每張 Host 影像大小為 256×256)。(a)~(b)為 Host 影像的原圖，(c)~(d)分別為藏入分存後的影像。

(a) (b) (c)

圖例二 第二主題(1)-不可視浮水印。(a) 為其中一個原影像分存，(a) 為其中一個嵌入隱藏式浮水印後的影像分存 (b) 為由該分存抽出的數位浮水印 (c) 為還原後的影像(無失真)。



(a) (b) (c)

圖例三 第二主題(2)-可視浮水印。(a) 為其中一個嵌入可視浮水印後的影像分存 (b) 為還原後的第一種影像，仍可見到可視的浮水印 (c)為還原後的第二種影像 (PSNR = 50.36 db)，並不會見到可視的浮水印。

(a) (b) (c) (d)

圖例四 第三主題-加強機密影像分享遭影像處理的可還原性。(a) 為未經修補的還原影像，(b) 為經過修補的還原影像， (c) 為未經過修補的還原影像，(d)為經過修補的還原影像。