

行政院國家科學委員會專題研究計畫 期中進度報告

影像分享：基礎、技術與應用(1/3)

計畫類別：個別型計畫

計畫編號：NSC91-2213-E-009-097-

執行期間：91年08月01日至92年07月31日

執行單位：國立交通大學資訊科學學系

計畫主持人：林志青

計畫參與人員：田智青、陳尚寬、方文聘

報告類型：精簡報告

處理方式：本計畫涉及專利或其他智慧財產權，2年後可公開查詢

中 華 民 國 92 年 6 月 2 日

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(第一年期)
Image Sharing: fundamentals, techniques, and applications

計畫編號：NSC 91-2213-E-009-097
執行期限：91年8月1日~92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：田智青、陳尚寬、方文聘
交通大學資訊科學系所

一、 中文摘要

本計畫為一個三年期的計畫，我們希望藉由三年的時間，把影像分享做全面性的研究以及擴展。第一年有四個主題，第一個主題為漸進式影像分享，主要是希望讓分存 (shadow) 影像在還原時具備漸進還原的特性。第二個主題則是快速的分存檢驗，我們擬設計出一個能即時且快速偵測分存正誤的方法來。第三個主題為具辨識偽造者並修復分存的設計，其主要的功能是在進行分存修復，並且可以結合第二個主題的方法，組成一個能即時偵測並快速修復分存的系統。第四個主題是抗雜訊的強固性影像分享，我們將研究如何使分存影像本身也能具備有強固性，增加分存影像的實用性。

關鍵詞：影像分享；數位浮水印；資料隱藏；錯誤偵測；漸進式影像分享

Abstract

This project is a three-year project. We intend to investigate and extend image sharing thoroughly in three years. We begin with the fundamentals and techniques in the first two years. Besides developing some basic methods for image sharing, including progressive method, we will also discuss how to reduce the impact of some

commonly-seen image processing operations on image sharing, and the technology of combining digital watermarking and data hiding techniques with image sharing. There are four topics in the first year. The first topic is progressive image sharing, the goal of it is to make the shadow images have the progressive recovery property in the recovery processing. The second topic is fast shadows detection, hence we will develop a fast method useful in detecting whether all shadows obtained are true or not. The third topic is a design of faker identification and repairing the damage shadows. The major function of this topic is to repair the damage shadows. Combining with the method of the second topic, we obtain an immediate detection and fast repair system. The fourth topic is a robust image sharing method against noise. We will investigate how to make the shadow images being robust, and hence enlarge the possibility of practical use of the shadow images.

Keywords : Image Sharing, Digital Watermarking, Data Hiding, Error Detection, Progressive Image Sharing.

二、 計畫緣由與目的

這個計畫的主要目的是希望將影像分享作全面性的研究與擴展。第一年計畫的第一個主題是：漸進式影像分享 (progressive image sharing)。

以往對於影像分享的研究多半把主題放在門檻值式 (threshold scheme) 的影像分享；所謂門檻值式的影像分享指的是，分存影像的回收份數需要達到某個預設的門檻值 (例如 t 份) 以上，才能夠還原出原始影像；否則只要回收份數低於門檻值，就無法進行還原的動作，即使強迫還原，其影像品質多半粗糙得無法辨識。在影像分享的領域中，我們發現如果還原的過程中可以採漸進式的還原方式，那麼就可以更加擴充影像分享的應用領域並增添其與網路環境結合的功能性。關於漸進式的還原方式 (以下稱為漸進式影像分享)，所指的是隨著所獲得分存份數的增加，還原的影像品質也隨之增高；最後，回收到某個份數以後，就可以完全無失真地還原出原始影像。例如利用任二份的分存影像還原出的影像品質，必須要比由任一份分存影像還原出的影像品質更好才行，而任三份的還原品質要比任二份更好...依此類推，直到 t 份分存被回收時，就可以得到原來無失真的影像。這樣的漸進式影像分享，在結合網路的運用時，可以增添其應用性。例如藉由控制分存影像的份數來掌握影像品質的輸出，並且擁有影像分享的基本優點。而在頻寬有限的情況下依然可以發揮漸進式還原的優點，仍可看到在有限頻寬能承載的資訊，不至於僅處於影像全無或全有的狀態。

第一年的第二個主題是：快速的分存檢驗法。由於機密影像分存在傳輸與儲存的過程中，可能遭遇到破壞，(這些破壞可能是傳輸或儲存過程中所產生的雜訊，或是遭受到人為的蓄意破壞)，而喪失其組合出正確機密影像之能力。這時，對影像分存是否全部為真之判斷，也就成為當務之急。因此，我們擬設計一個分存檢驗法，來驗證是否所蒐集到的分存均為正確無誤的，以確保組合出我們所要的機密影像。速度對於現今的網路應

用上是一項相當重要的要求，因此當使用者端欲組合出數量相當多的機密影像時，檢驗速度是重要的考量，因此在此主題中，我們強調此檢驗法的快速。

第一年的第三個主題是：具辨識偽造者並修復分存的設計。在此主題中我們將要求系統不但具有檢驗分存的功能，同時能辨識偽造者，找到藏於分存中的偽造者，並將這些偽造者列於黑名單，下次便不會再將分存交由其保管。更重要的是此方法能達到修復被破壞分存的功能，使其仍能順利的組合出正確機密影像。由於在主題二中，我們強調其能夠快速的檢驗分存 (主題三則強調「修復」，而不強調「快速」)，因此我們可將主題二與主題三相互結合，使其在平常一般情況時，我們利用主題二的快速分存檢驗法，來檢測在網路上大量傳送的分存，一旦發現分存遭受到破壞時，我們可利用主題三的方法，找出所有的偽造者，並修復被破壞的分存，使得機密影像仍能被還原。如此能使此系統變得更加的完備。

第一年的第四個主題是：抗雜訊的強固性影像分享 (robust image sharing)。過去所做的影像分享研究中，分享的資料多半是不容許破壞的，即一旦有些許的變動，也容易會造成還原資料嚴重的誤差。也就是說，分存影像對雜訊干擾十分的敏感。事實上，強固性影像分享在現實的應用上，有其一定的必要性，譬如分存影像在傳輸品質較不穩定的網路中進行傳送時，如果有一些的小雜訊，就容易造成巨大的影像誤差，而使得還原影像的內容失去辨識的功用。當然，我們可以藉由錯誤偵測與還原來回復影像的真實內容；但是，在某些實際的應用領域中，接收端 (例如手機或 PDA) 未必具備夠快的計算能

力（可能因為成本的考量）可以即時地一邊還原，一邊還肩負著檢測與復原的工作；且在這些應用中，還原影像也未必要毫無失真的傳送，只要在容許的誤差內即可（譬如，利用手機利用基地台平行地接收即時分存影像或分存圖片）。有鑑於此，抗雜訊的強固性影像分享的研究是十分需要的。

目的:

1. 設計出漸進式影像分享機制，使得影像品質的好壞與分存份數的多寡成正相關，直到還原出原始影像的品質為止。而同份數但不同分存影像合成的還原影像不必相同，只要品質相當即可。
2. 設計出一個能快速檢驗所取得的數張分存，是否每張均為正確的即時方法。以確保組合出我們所要的機密影像。
3. 設計一個仍然具檢測功能，並對藏有偽造者的一群分存中，揪出這些偽造者。由於所取得的分存若藏有偽造者，或者在傳輸過程中受到干擾，則所重組得到的機密影像將可能會產生雜訊（或甚至看不出任何影像），而我們的目標要能重組回機密影像，即使所取得的分存是有誤的。
4. 設計出能容許雜訊及非惡意性破壞之影像處理的強固性影像分享方法。這樣的方法可以使得分存影像在經過非惡意性破壞之影像處理或雜訊干擾時，其所得的還原影像誤差仍然不會太大，而內容依然可以辨識。

三、 結果與討論

在第一個主題：漸進式影像分享，我們將影像透過 DCT 的轉換後所得到的頻率域的影像分成低頻、中

頻、與高頻三個部分，再透過機密影像分享，根據收到分存的數量，而獲得不同的還原後的影像品質。我們在圖例一展示了根據收到分存數量，所還原的機密影像。在第二主題：快速的分存檢驗法，我們利用多項式的特性和再加上額外檢驗站提供的 1 張支援分存，來設計出一計算量小，速度快的除差形式的檢驗法。我們在圖例二展示了三張分存，其中一張有經過修改。藉由一張支援分存，我們可以偵測到所蒐集到的分存有錯誤的發生。在第三主題：具辨識偽造者並修復分存的設計，我們利用所取的 t 張分存，再加上額外檢驗站提供的 u 張支援分存，經由排列組合的原理，將此 $(t+u)$ 張分存組出 w 組，再利用分存產生逆運算以及分存產生運算，來找出偽造者，並修復遭到破壞的分存。我們在圖例三的三張分存，其中一張有經過修改，而藉由兩張支援分存，我們可以偵測到所蒐集到的分存有錯誤的發生，並且加以修復。在第四個主題：強固性影像分享分存影像強固性要求，我們利用採用擴充資訊載體的方式，來增加對雜訊或非惡意破壞的緩衝空間，並且將編碼方式設計成對誤差敏感度低的形式，以期望分存遭受的破壞（誤差），在還原時，不擴充誤差程度甚至縮小誤差差距。

四、 計畫成果自評

第一年的前三大主題，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。至於最後一個主題，我們已經設計出對誤差敏感度低的編碼方式，目前已在實驗的階段，即將獲得成果。

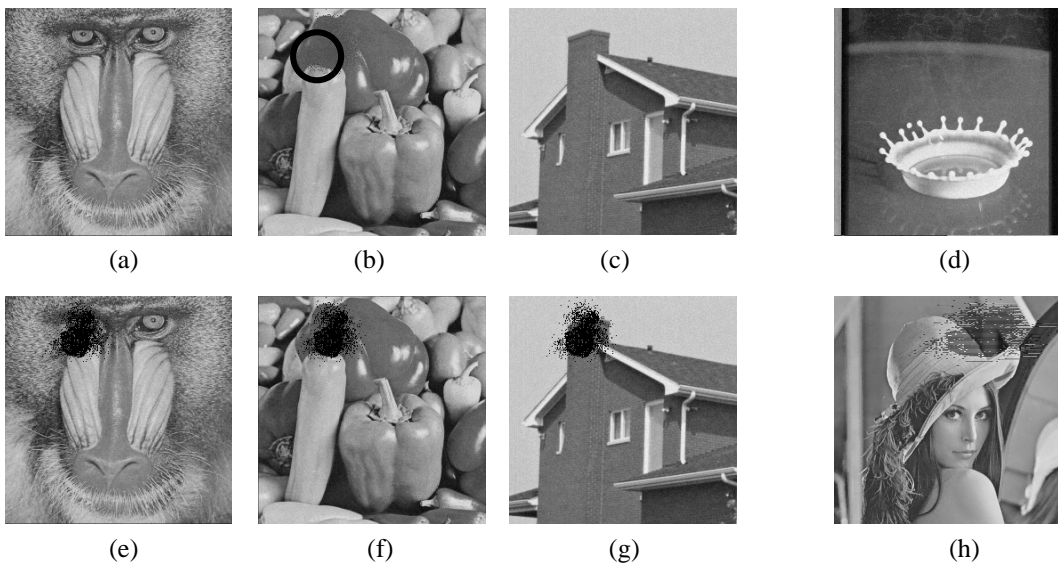
五、 參考文獻

[1]C.C. Chang and C.W. Chan
 “Detecting dealer cheating in secret sharing systems”, Computer Software and Applications Conference, 2000. COMPSAC 2000. The 24th Annual International, 2000
 Page(s): 449 –453

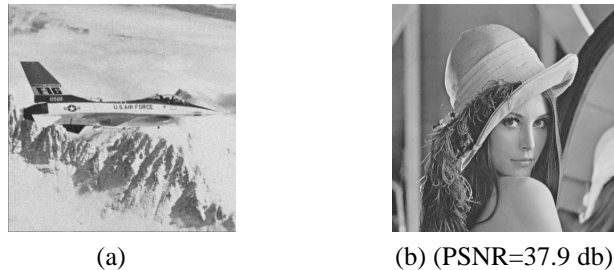
[2]R.J. Hwang, W.B. Lee and C.C. Chang, “A concept of designing cheater identification methods for secret sharing ”, Journal of Systems and Software vol. 46, Issue: 1, April 1, 1999, pp. 7-11



圖例一 第一主題-漸進式影像分享之實驗結果(threshold=5)。 (a)為原圖， (b)~(d)分別為取得分存數量三，四，五所還原的機密影像。



圖例二 第二主題-快速的分存檢驗法之實驗結果(threshold=3)。 (a)~(c)為將分存隱藏於內的影像(stego image)，且(b)為被破壞之分存，(d)為支援分存，(e)~(g)為檢測出有錯誤分存之結果，(h)為由有錯誤分存所還原的影像。(原圖為圖例一(a))



圖例三 第三主題：具辨識偽造者並修復分存的設計之實驗結果。(a)與圖例二(d)為兩張支援分存，(b)為指認出圖例二(b)是錯誤分存後，予以更正後所得的影像。