行政院國家科學委員會專題研究計畫成果報告
影像分享
Image Sharing

計畫編號:NSC 90-2213-E-009-131
執行期限: 90 年 8 月 1 日～91 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、方文聘、陳尚寬、巫玉珊
交通大學資訊科學系所

一、 中文摘要

本計畫擬藉由機密分享的機制，開發出適用於影像題材的分享系統。計畫包括四個主題:[一] 機密影像分享、[二]非機密影像之分離式容錯資料庫設計、[三] 機密影像的隱藏式分存產生法、[四]具自我修復能力之影像分存設計。第一個主題是藉由對分享方法核心的改良，以達成機密影像在進行分享方法時，其每份分存的資料量能夠大大減少，進而可以進行有效率的傳輸或儲存。在第二個主題中，我們擬設計一種新型的影像資料庫系統：分離式容錯資料庫。這個系統在網路的環境中，發揮兼具傳輸效率與容錯的功能：允許網路在部分線路斷線情況下，仍可合成所要影像。這個主題亦強調分存影像必須要與合成影像近似，以方便子資料庫管理員的識別與管理。分離式影像資料庫可以進一步發展成為分離式影片資料庫，而分存影片的概念可以應用於隨選視訊的研發上，更別具意義。主題三則是藉由對機密影像的分存，加以適當的包裝，避免引人注意，增加分存在使用時的安全性。最後，在主題四，我們則是設計具備有驗證與還原能力的影像分存。在這個方法中，我們擬將每個分存動態分割成大小不一的區塊，並在每一個區塊中嵌入一個特定的性質，藉以用來檢測其正確性。同時，我們也會在每個分存當中隱藏一些資訊，使其具備自我修復之能力。主題四是用來讓系統在將數份分存合成影像時，能測出分存是否遭竄改，並將竄改的分存加以修復。

關鍵詞：機密影像分享；影像之分離式容錯資料庫；隱藏式分存；自我驗證與修復

Abstract

In this project, we will develop an image sharing system. There are four topics in the project. The first topic is the design of some secret image sharing methods, the second one is the design of the distributed fault-tolerant database system for general images, the third one is the generation of the hidden shadows for secret images, and the last topic is the self verification and reparation of the shadows. In the secret image sharing methods, we reduce the shadow size by improving the kernel of some sharing methods. The size reduction of the shadow has the advantage for effective transmission or storage. This is particularly important for images because image data are often big in size. In the second topic, we will develop a new type of image database system -- the distributed fault-tolerant image database system. The system could be effective in time-saving, and have the fault-tolerant ability in Internet. Moreover, we also emphasize the similarity between the shadow images and the original image. With this property, the managers of the subsystems of database could manage the subsystem easily. Note that we may extend the concept of distributed fault-tolerant image database to developing the distributed fault-tolerant video database. The concept of shadow video could also be applied to the study of VOD (video on demand). In the

third topic, we will hide the shadows of the secret image for the security and effectiveness. We plan to make a tight combination of sharing method and data hiding. It means that the data hiding method will be mingled with the progress of secret image sharing method directly. Finally, in the fourth topic, we plan to incorporate the verification and recovery ability to the shadows of a secret image. We plan to split a shadow into multiple variable-size blocks, and maintain a predefined property in each block during the shadow generation process to serve as the attestations for the correctness of the shadow. Some recovery information will also be embedded in a shadow to enable its recovery ability. The fourth topic is to make the system, when used to generate the desired image by combining several shadows, can not only identify which shadows have been modified by intruders, but also recover the modification to get the right shadows.

Keywords： Secret Image Sharing, Distributed Fault-Tolerant Image Database, Hidden Shadow, Self Verification and Reparation.

二、 計畫緣由與目的

近年來許多針對機密數位影像所做相關的資料安全技術紛紛被提出，如影像隱藏(data hiding)，數位浮水印(digital water marking)等等。然而這些技術本身隱含著先天性上缺點:其資訊集中於一個資訊載體，所以一但這個資訊載體遭破壞或整個遺失，機密亦即損失。但在另一方面，若複製多份，則被盜取破解的機率亦會增加。為能解決這樣一個問題，資訊分散(分享)是個很好的解決方式。

因為數位影像的資料量很大，且有固定的值域範圍，所以須要發展針對數位影像性質設計的機密影像分享方法。我們今年所提的第一個主題，即是將數位影像的兩項特性：1.資料量大、2.值域固定(灰階值都在 0~255 之間)，加以考量，進而創造出有別於密鑰分享的機密影像分享方法。我們將對分享方法的內部核心加以改良，以達成機密影像分享的輸出分存可以既安全又可以使其資料量大大減少。

本計畫的第二個主題是：非機密影像之分離式容錯資料庫的設計。第一主題中的影像分享，在其本體上可視為一種將資料透過分散而防止資料會因單一機器損壞而無法救回的安全性處置機制；而這樣的機制(分享機制)事實上適合於建構一個新型態的影像資料庫，我們稱之分離式影像資料庫。這種新型態的影像資料庫在網路應用上非常具有發展性，我們在此粗略的說明如下：分離式影像資料庫，可以提供需要資料影像傳輸的應用(如 WWW)的背後設施。其本體由幾個分散式的資料庫構成，各個分散式的資料庫儲存的是影像的分存(shadow)；應用時，各個資料庫同時平行傳輸至接收端，由於分存資料量小於原始影像的資料量，所以傳輸的時間會減少，達成加速的效果。此外，更重要的一個特性是：由於資訊分享的性質，接收端可以只要接收到一定門檻值份數的分存即可還原出原始影像，故此機制先天上就具備有『容錯』的性質。這樣的性質對於在網路上進行傳輸更有幫助。因此我們不會因某一時刻在某條線路上忽然的斷線就無法即時取得重要影像。

有關分離式影像資料庫的設計，雖然可以直接使用我們在第一主題所提出的機密影像分享方法，然而，真正在商業用途上卻有不便之處。主要是因為第一主題所產生的分存，在各個子系統裡，呈現的是看起來很像一堆 random noise 的圖像。所以在資料庫的管理上，如果子系統管理員面對的是一個個 random noise 式的分存,子系統管理員將不容易區分分存的『身份』(屬於哪一個原始影像)，十分不便。於是我們需要針對分離式影像資料庫需求，研究出一種方法，使得產生的分存可以看起來像原始影像的縮影，而不要只是像一堆 random noise。

本計畫的第三個主題是：機密影像的隱藏式分存產生法。當我們產生機密影像的分存後，尤其是需要特別強調其安全性之時，我們需要對分存加以適當的包裝，

如此在儲存或傳輸時才有安全的保障。資料隱藏(Data hiding)是個適用的方法，可以拿來『包裝』分存。我們當然可以直接利用已有的資料隱藏方法來『包裝』分存，然而我們發現，目前的資料隱藏方法藏資料後的輸出的影像資料量通常會大於所藏入的資料的資料量，我們好不容易將分存資料的資料量降低，當然不希望因為『包裝』而增加資料量，所以我們希望，最好能夠加『包裝』，而資料量卻不增加，也就是說要達成隱蔽後之影像(stego image)資料量與分存(即是 embedding image)資料量的比例是 1:1。

本計劃的第四個主題是：具自我驗證與修復能力之影像分存設計。由於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影像之能力。此外，若一個使用者已經蒐集到足夠組合出正確影像的分存份數，組合出的影像卻是沒有意義的圖像(例如一張雜訊影像)，這時，對一份影像分存的真偽之判斷，也就成為一項挑戰。因此，我們擬設計一個正確分存性質分配與驗證法則，必要時並根據其檢查碼，將錯誤自動更正，確保組合出我們所要的影像。

目的：

1. 改良多種機密分享的核心方法，建立其核心的數學模式，使其各輸出分存的資料量可以小於原始的資料量，而且還能具有相當程度的安全性，因而適用於影像資料之分享。
2. 設計出一種非機密影像的分散式容錯資料庫，使其在每個子庫的分存影像能與原始影像相似，以方便於分離式影像資料庫的管理與運作；而資料庫的母庫在合成影像時，又具容錯之功能，所以不要求每個子資料庫之間(或與母庫之間)的連線永遠二十四小時隨時暢通。
3. 設計出能夠隱藏機密影像的高效率影像分存方法(須有 1:1 的隱藏效果，不能因隱藏而使分存影像尺寸變大而浪費儲存空間或傳輸時間)。
4. 設計出具有自我驗證與修復能力之影像分存，使得各個影像分存在遭遇到破壞後，能夠正確的自我驗證此影像分存的正確性；如果所遭遇的破壞在系統所能容忍的範圍內，則系統能夠成功的自我修復，以確保組合出我們所要的影像。

三、 結果與討論

在第一主題-機密影像分享方法，我們藉由取消隨機參數的方式，產生了資料量只有原影像的 $1/t$ 之分存影像（t 為設定之門檻值)。並且也同時證明了其具有想當高的安全性。我們在圖例一展示了所產生的分存影像及其還原回來的圖形。在第二主題-非機密影像的分散式容錯資料庫，我們成功地利用了影像中相鄰像素相似的特性，來進行圖形不同區域的分類與編碼，並且利用差分法來減低資訊熵，以便減少資料量，利用此方法產生的分存影像與原影像相似，但品質只有約 22 dB，可以避免被直接盜用；而若以足夠的分存加以還原則可以得到約 37 dB 的高品質圖片，符合我們設計的目的。我們在表一列出詳細的實驗數據以供參考。在第三個主題-機密影像的隱藏式分存產生法，我們先將原圖進行量化的前處理，並將還原所需的資訊嵌入量化圖中，接著再以一種簡單的資料隱藏的方法進行影像隱藏；利用上述的方法，我們成功的產生了隱藏式的分存，即分存影像隱蔽在一般影像，而此藏有分存影像的一般影像(stego image)的資料量只有原機密影像的 $1/t$。此方法產生的 stego image 擁有不錯的影像品質：約 34.33 dB，而還原回來的影像則有更高的影像品質，我們將其列於表二。最後一個主題-具自我修復能力的影像分存設計，我們原本計畫利用週期性方程式來當作檢驗的功能，然而發現由於影像像素多為整數值，套用在週期函數上會有超出值域的困擾，於是我們利用各分存是由同一個函數產生的性質，採用分存間的差分法來檢驗分存的正誤。然後再由判斷為正確的數份

分存來組合成機密影像。

四、 計畫成果自評

前三大主題，我們均成功的達成了預期的目標；成果，也已經投稿至 IEEE Transaction 及 PR 等相關期刊上，正在審核中。至於最後一個主題-自我修復能力的影像分存設計，其成果亦正在整理即將投稿至國際期刊。

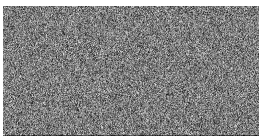
五、 參考文獻

[1] A. Beimel, B. Chor, "Secret Sharing with Public Reconstruction", IEEE Transactions on Information Theory 44 (5) (1998) 1887-1896.

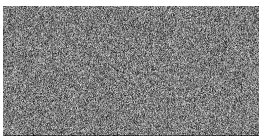
[2] W. Bender, F.J. Paiz, W. Butera, S. Pogreb, D. Gruhl, R. Hwang, "Applications for data hiding", IBM Systems Journal 39 (3-4) (2000) 547-568.

(a)

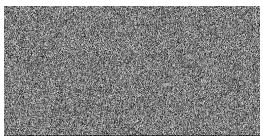
(b)



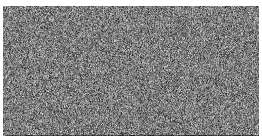
(c)



(d)



(e)



(f)

圖例一 第一主題-機密影像分享方法之實驗結果。(a)為原圖，(b) 為由(c)~(f)任意兩張分享影像還原所得的圖形。

	The revealed images		The expanded shadow images	
	MSE	PSNR	MSE	PSNR
Jet (2,*m*)	6.61	39.93	225.91	24.59
Jet (4,*m*)	9.99	38.14	583.27	20.47
Lena (2,*m*)	10.36	37.98	247.00	24.20
Lena (4,*m*)	15.25	36.30	582.06	20.48
Monkey (2,*m*)	19.08	35.33	632.04	20.12
Monkey (4,*m*)	22.76	34.56	1387.60	16.71

表一 第二主題-非機密影像的分散式容錯資料庫之實驗結果：還原影像及分存影像的 MSE 與 PSNR 之比較。

Recovery secret image	House	Jet	Peppers	Milk	Tiff	Woman
PSNR(dB)	41.64	39.36	37.66	40.74	38.79	40.52

表二 第三個主題-機密影像的隱藏式分存產生法之實驗結果：還原影像之 PSNR 值。