

行政院國家科學委員會專題研究計畫期中報告
視覺型、多項式型、與向量量化型的影像分享及應用(第三年期)
Image Sharing using Visual-Cryptography, Polynomials, and
Vector-Quantization Approaches (with Applications in Image Recovery)

計畫編號：NSC 96-2221-E-009-039
執行期限：95 年 8 月 1 日～96 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：張御傑、林憲正、陳李書勝

交通大學資訊科學系所

一、 中文摘要

本計畫為期三年，其目的是針對不同類型的影像或需求，做各型的分享及應用。本年(第三年)的主題是向量量化型影像分享，及影像分享技術在回復被竄改影像之應用。主要是將前二年的分享技術加上以往本實驗室所做的研究，配合影像壓縮的性質，做技術上與應用上的擴充，以期能發揮影像分享的潛能。所以第三年處理的對象從低階影像到高階影像都有。第三年第一個主題為向量量化(Vector Quantization, 簡稱 VQ)型影像分享之可容錯版。在本主題中，我們希望設計一個 VQ 型影像分享技術，其兼具兩種傳統的 VQ 型影像分享技術[1-2]的優點-還原影像的視覺品質令人滿意，並具有容錯的功能。第二個主題為漸進式的向量量化型影像分享。在某些網路頻寬較不足的環境中，使用者可能無法收集到足夠份數的分存，因而導致還原的動作受阻，在這個主題中，主要是希望設計一個直接在索引域空間上操作的可漸進式還原的影像分享技術，使得使用者收集到的份數達到最低門檻時，便能看到最粗糙的影像顯示。第三個主題為向量量化

式的無失真影像分享機制。我們根據前兩個主題的研究成果加以延伸，設計一個能無失真的可漸進式還原的影像分享技術，且產生的分存其大小與原始影像相當。第四個主題是基於影像分享而得的影像修復技術(image recovery technology)。我們根據之前影像分享的研究成果，設計一個具有影像修復能力的影像驗證系統，使得在偵測的過程中，不但可以標示出遭到竄改的位置，並可以針對遭到竄改的區域進行修復，以期望保有原始影像的視覺效果。第五個主題是基於跨影像的交叉分享而得的多張影像修復技術。本主題是應用於多張影像傳輸時，可能會有因網路不穩定而導致某些影像遺失的情形。因此，我們設計了一個具有交互修復能力的影像驗證系統，使得影像本身除了原有的驗證功能之外，還能與其它殘存的影像互相合作來修復那些遺失影像。

關鍵詞：向量量化型影像分享；漸進式還原；無失真還原；影像驗證；竄改偵測；影像修復。

Abstract

This project is the 3rd part of a

three-year project. The goal of the 3-year project is to use three major styles of image sharing techniques to share different kinds of images and meet different needs. There are five topics in the third year. The first topic is the fault-tolerant version of the VQ-style image sharing, and the goal of it is to design a VQ-style image sharing technique with fault-tolerant function and the visual quality of its recovered image is acceptable. The second topic is the progressive VQ-style image sharing. In the network environment with narrow bandwidth, a user may not receive the shares enough to reconstruct the secret image. Therefore, in this topic, we want to design a progressive VQ-style image sharing technique, which works in the index domain, and the quality of the recovery image is progressive according to the amount of the received shares. The third topic is the lossless-recovery version of VQ-style image sharing. We plan to propose a VQ-style image sharing approach to have fast and lossless retrieval in the secret image. The shadows generated by the proposed approach have the same size of the secret image. The fourth topic is an image recovery technology based on image sharing. We design an image authentication system whose features include: 1) detecting whether the authenticated image is tampered; 2) indicating the locations of the tampered area; 3) self-recovering the tampered portion; 4) maintaining the quality of the

authenticated image. The fifth topic is the recovery of several damaged images using the sharing across images, i.e. if r images of the n images are not damaged, then the $n-r$ damaged images can be recovered using the r images. We design a system with image authentication and cross-recovery ability to protect a group of digital images; and its goal is that if some images in the group are tampered or lost, these images can be identified and reconstructed by the mutual support of the survived members.

二、計畫緣由與目的

本計畫是一個為期三年的計畫，藉由延伸前一個三年期的影像分享計畫所得到的成果，來針對不同的影像類型特性與需求，做適合的分享，然後邁向應用。本年度(第三年)的第一個主題是：向量量化 (Vector Quantization, 簡稱 VQ) 型影像分享之可容錯版。傳統的 VQ 型影像分享大致上有兩種方法，第一種方法[1]是將編碼簿(codebook)利用 (r, n) 門檻值的方享方法將編碼簿分享成 n 個分存，而索引檔則存放在本地端，如此一來只要收集到其中 r 份的編碼簿分存，便可得到原本的編碼簿，再利用存放在本地端之索引檔，即可還原出機密影像。優點是只要損壞的編碼簿分存不超過 $n-r$ 份，編碼簿皆可被還原出來，以達到容錯(fault-tolerant)效果，但在應用上仍須從本地端索取索引檔，較不切實際，且還原的影像品質比起第二種方法則較不理想。第二種[2]主要是以每張宿主影像的前 7 個位元層為基礎，訓練成一本編碼簿，

而機密影像便以此編碼簿編碼而得 VQ 索引檔。此索引檔可利用分享機制產生各個分存，再將各個分存藏到各張宿主影像的最後一個位元層中，形成 stego imagea。而還原機密影像時，必需收集到所有的 stego imagea，才能計算出 VQ 索引檔，然後再進行 VQ 的解壓縮過程而還原出機密影像。第二種方法的優點是各張 stego image 的影響不會過大，且還原出來的機密影像也不差，但缺點是若某一張 stego image 損毀，則機密影像將無法還原出。綜合上述兩種方法的優點，我們欲設計一種 VQ 型影像分享法，其 stego image 與還原影像的品質還不錯，並且具有容錯的能力。

本年度(第二年)的第二個主題是：漸進式的向量量化型影像分享。漸進式的影像處理，例如漸進式壓縮、傳輸、分析等在影像界已經有了廣泛的研究；主要是因為漸進式的處理方式在實際的用途上有不錯的功效，並且漸進式的處理一向很適合於在網路的環境上使用，尤其在網路頻寬較不足的環境中，使用者可能無法收集到足夠份數的分存，因而導致還原的動作受阻。所以很自然的，VQ 型影像分享的技術也希望能夠有漸進式的版本，如此，在一些適合漸進式處理的應用上，VQ 型影像分享也可能適用而增加其應用範圍。

本年度(第二年)的第三主題是：向量量化式的無失真影像分享機制。傳統的投影片式機密分享，其每張分存大小常是原始機密影像的至少四倍大。(雖有少數作者做到分存大小維持跟原圖一樣，但其還原的機密影像並不是無失真)。另一方面，多項式的影

像分享雖可做到分存較小且無失真還原機密影像，但其計算較複雜因而較費時。因此，我們希望提出某種向量量化式的影像分享的技術，使得以此機制所產生的分存大小不會擴張，並且可以快速且『無失真』的還原影像，以兼具上述兩種型式的優點。這個機制所產生的分存其大小與原始影像相當。而本主題所設計的 VQ 型影像分享技術也是綜合前兩個主題的優點：容錯、漸進式，並增加無失真的還原功能，成為一個功能完整的 VQ 型影像分享技術。

本年度(第二年)的第四主題是：基於影像分享而得的影像修復技術 (image recovery technology)。影像資料在經過網路傳遞或電腦被入侵後，我們很難保證其仍完整，因此保護影像資料的完整性便成為一個重要的議題。影像驗證就是為了防止攻擊者蓄意竄改影像內容所發展出來的技術。而大部份的影像驗證方法都具有偵測竄改是否發生與標示遭到竄改的區域的能力，卻較少有進一步地修復工作。影像修復則是針對遭到竄改的區域進行修復，以期望能重建原始影像的風貌。至今為止，本實驗室已對機密影像分享與關於其分存的錯誤控制提出過一連串的方法與實驗結果，而我們希望將這些技術應用至影像驗證之修復功能這主題之中，以獲得一個功能強大的影像驗證暨修復系統，來提升影像在網路傳輸及儲存的安全性。

本年度(第二年)的第五主題是：基於跨影像的交叉分享而得的多張影像修復技術。前一主題(主題四)是基於單張影像的修復，必須在該影像未被

完全破壞的前提下才能進行修復的動作。倘若整張影像被完全破壞或遺失，則主題四的修復機制將宣告失敗。如果我們現在擁有的是 2 張以上的影像，則我們可以將每張影像的回復資訊藏入其他影像之中。如此一來就算某幾張影像被完全破壞了，我們依然能利用其他未被破壞的影像資訊還原出被破壞的影像。再者，在許多 channels 下，攻擊者難以同時對所有影像進行攻擊。因此我們以這樣的假設為開端，為了保護多張影像資料的完整性的需求，結合機密影像分享的技術，來設計一套能利用群體的影像資訊來修復個別影像的機制。在這個主題之中，我們使用 n 張影像，這 n 張影像經過本機制處理後，只要有 r 張影像未被破壞，就可以利用這 r 張影像重現全部的 n 張影像，如此可以提升多張影像在傳輸時的可靠度。

目的：

1. 設計出一種 VQ 型影像分享法，使得 stego image 和還原影像的品質還不錯，並且具有容錯的能力。
2. 設計出在索引域空間上操作的可漸進式還原的影像分享技術。若收到的分存張數不足最低門檻時，則完全看不出原機密影像的任何資訊。但從收到的分存達到最低門檻開始，就可以約略看到原始機密影像，且還原的影像品質的好壞與收集到的分存份數的多寡成正相關。
3. 設計出一種向量量化式的影像分享機制，使得以此機制所產生的分存可以快速且『無失真』的還原影像。這個機制所產生的分存其大小與原始影像相當。

4. 建構一個基於影像分享而得的影像修復的機制，使得一張影像遭受惡意竄改的程度在一定量下，仍能藉由同一張影像的殘餘部份修復回類似原本的樣貌。
5. 利用跨影像的交叉分享技術，建構一套多張影像交叉修復的機制，使得經過本機制前處理過的 n 張影像，只要有任意 r 張影像未被破壞，我們就可以利用這 r 張影像還原出全部的影像。

三、 結果與討論

在第一主題：向量量化(Vector Quantization, 簡稱 VQ)型影像分享之可容錯版，首先我們先選定所需要的宿主影像之數目，即 (r, n) 門檻值中的 n ，然後取 n 張宿主影像中的 r 張來產生各自的編碼簿，並對所欲分享的機密影像，進行向量量化的壓縮[3]，接著將所得到的索引檔作 (r, n) 門檻值的分享處理，並將所產生的 n 份索引檔分存藏於 n 張宿主影像中。最後利用未參與向量量化的 $n-r$ 張宿主影像來攜帶有關 r 張編碼簿之間的重要資訊，以達成我們的容錯目的，使得當收集到任 r 張 stego image 即可重建出以向量量化壓縮的機密影像。如圖例一，本實驗所設定的門檻值是 $(3, 5)$ ，(a)-(e) 為五張本實驗用的 512×512 宿主影像，(k) 為 1024×1024 機密影像，(f)-(j) 為經過嵌入索引檔分存與編碼簿間相關資訊後的宿主影像(即 stego image)，可以看出其影像品質令人滿意(PSNR 值附於下方括號內)；(l) 為是收集到任三份 stego image 所還原的機密影像。

在第二主題：漸進式的向量量化

型影像分享，首先，針對參與編碼過程的編碼簿進行相似度的排序，使得鄰近的碼語區塊(codeword)極為相似。接著，針對所欲分享的機密影像，進行向量量化的壓縮[3]，然後將所得到的索引檔以深度的角度來作切割，也就是針對各索引值的位元層作(r, n)門檻值的分享處理。所得到的分存大小，由於索引檔已經是很小的檔案，再經過(r, n)門檻式的分享，將會變得很小；再者，由於具有漸進式的還原功能，因此本系統有利於頻寬較小或連線狀況不穩定的網路環境使用。如圖例二，本實驗所設定的門檻數列是(3, 4, 5)共三階門檻，機密影像為「F-16」。(a)是收集任兩份分存所重建的影像，由於未達到最低門檻，所以看不到任何有關機密影像的資訊；(b)和(c)是收集到任三和四份分存之結果，很明顯地看得出來隨著收集的份數越多，重建的影像品質越來越好；(d)當收集到最高門檻五份分存的時候，即可還原出以傳統的向量量化編碼的機密影像。

在第三主題：向量量化式的無失真影像分享機制，針對所欲分享的機密影像，我們將向量量化後的影像與原始影像的差值及所得到的索引檔，進行(r, n)門檻值的分享處理，並將所得到的分存利用以前我們研發的模組隱藏法[5]藏於n張與機密影像同樣大小的宿主影像中，即成為 stego image，使得當收集到的 stego image 份數越多，則得到越多關於機密影像的資訊，當收集到的 stego image 份數達到一個設定的門檻值，即可無失真的重建原始機密影像。因為索引檔與差值所產生的分存都非常的小，所

以 stego image 的影像品質並不會與宿主影像差距太大，因此也較不易引起攻擊者的注意。如圖例三，本實驗所設定的門檻數列是(2, 3, 4, 5)共四階門檻，機密影像為「F-16」。(a)-(e)為五張 stego image，可以看出其影像品質令人滿意；(f)是收集任兩份宿主影像所重建的影像，這是最低門檻，所以只能看到非常粗糙的原始影像；(g)和(h)是收集到任三份跟任四份宿主影像之結果，很明顯地看得出來隨著收集的份數越多，重建的影像品質越來越好；(i)當收集到最高門檻五份的時候，即可還原出無失真的原始影像。

在第四主題：基於影像分享而得的影像修復技術(image recovery technology)。我們利用某些相關於影像區塊的性質產生驗證資料，並嵌入影像區塊中，用來檢測影像的完整性。同時，為了使影像本身除了能偵測是否遭到惡意的竄改之外，還具有修復被破壞區域的能力。我們利用向量量化編碼產生關於影像的修復資料，並搭配(r, n)門檻式分享方法平均分散地藏於影像本身中，使其容錯的特質來達成修復的能力。如圖例四，(a)-(d)是四張經過影像驗證處理後的加工影像，其影像品質令人滿意，皆能維持在 44 db 的水準；(e)和(f)是針對「Lena」這張圖所進行的切割破壞，分別是 25%與 50%；(g)和(h)是對「Lena」和「F-16」這兩張圖進行偽造；(i)-(l)是針對各個破壞進行驗證的結果，可以看出明確的偵測出破壞的區域；(m)-(p)是針對遭到破壞的區域進行修復的結果，可以看出修復的結果令人滿意。當然，破壞的區

域越大，修復影像的品質影響就越大。

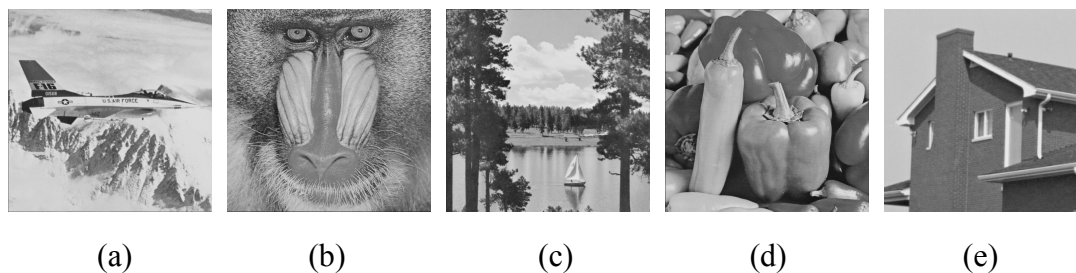
在第五主題：基於跨影像的交叉分享而得的多張影像修復技術。我們利用影像壓縮技術來取得所有影像的修復資料，並利用所設計的雙層式(r, n)分享機制來保存這些修復資訊，最後加入影像驗證所需之資訊而完成整個保護的工作。因此，只要殘存的影像有 r 張(或超過 r 張)，即可互相合作來修復那些遺失的影像。如圖例五，本實驗所設定的門檻值是(2, 4)，即在四張保護影像群組中，只要任兩張影像是完整沒有遭到破壞的，即可修復其他遺失或遭到破壞的影像。(a)-(d)為四張經過處理後的保護影像，可以看出影像品質令人滿意，並不會影響他們的使用價值；(e)-(h)則是當某 2 張影像遭到破壞或遺失時，靠著群組裡別的影像所重建的修復影像。從實驗可以看出修復影像的品質是可以接受的。

四、計畫成果與自評

第三年的第一、二、三、四、五主題，我們均成功的達成預期目標與成果，而其中第一二、三目前正在整理結果即將投稿至國際期刊；第四、五主題已經完成結果文件，並投稿至國際期刊。

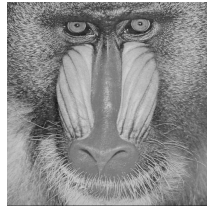
五、參考文獻

- [1] C.C. Chang and R.J. Hwang, "Sharing secret images using shadow codebooks," *Information Sciences*, Vol. 111, pp. 335-345, 1998.
- [2] Tung-Shou Chen and Chin-Chen Chang, "New method of secret image sharing based upon vector quantization," *Journal of Electronic Imaging*, Vol. 10, No. 4, pp. 988-997, 2001.
- [3] R.M. Gray and D.L. Neuhoff, "Quantization," *IEEE Trans. Information Theory*, Vol.44, No. 6, pp. 2325-2383, 1998
- [4] C. C. Thien and J. C. Lin, "Secret image sharing," *Computers & Graphics*, Vol. 26, pp. 765-770, 2002.
- [5] C.C. Thien and J.C. Lin, "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function," *Pattern Recognition*, Vol. 36, No. 12, pp. 2875-2881, 2003.





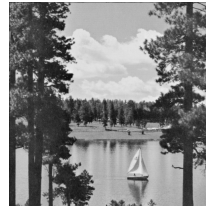
(f) (52.70 dB)



(g) (52.71 dB)



(h) (52.69 dB)



(i) (48.87 dB)



(j) (50.34 dB)

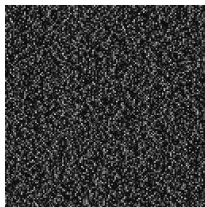


(k)

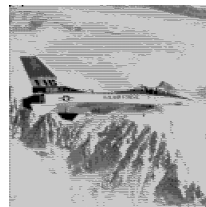


(l) (PSNR=34.01 dB)

圖例一 第一主題一向量量化型影像分享之可容錯版的實驗結果(括號內為其 PSNR 值)。 (a)-(e)為原始的五張 512×512 宿主影像；(f)-(j)為其對應的 stego image；(k)為 1024×1024 機密影像；(l)為收集到任三張 stego image 所還原的機密影像。



(a)



(b) (18.60 dB)

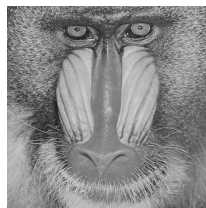
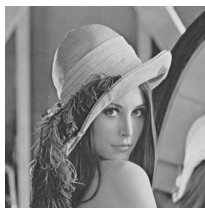


(c) (23.04 dB)



(d) (31.48 dB)

圖例二 第二主題一漸進式的向量量化型影像分享之實驗結果(括號內為其 PSNR 值)。此實驗同時使用三個不同品質的門檻值(3, 4, 5)：(a)為收集到任兩份所還原的影像；(b)為任三份所還原的影像；(c)為任四份所還原的影像；(d)為收集到最高門檻值(五份)所還原的機密影像。



(a) (40.21 dB) (b) (40.41 dB) (c) (40.89 dB) (d) (40.80 dB) (e) (40.87 dB)



(f) (28.00 dB) (g) (32.30 dB) (h) (35.96 dB) (i)

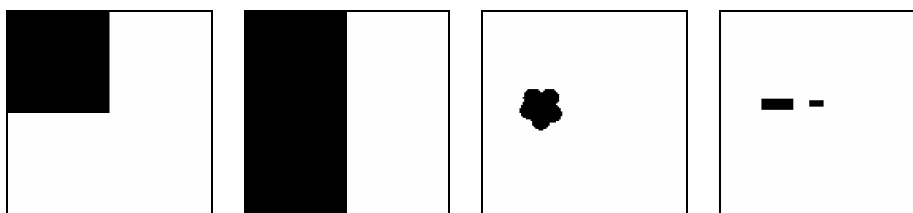
圖例三 第三主題一向量量化式的無失真影像分享機制之實驗結果(括號內為其 PSNR 值)。此實驗同時使用四個不同品質的門檻值(2, 3, 4, 5): (a)-(e)為五張 stego images; (f)為收集到任兩份 stego images 所還原的影像; (g)為收集到任三份 stego images 所還原的影像; (h)為收集到任四份 stego images 所還原的影像; (i)為收集到最高門檻值(五份)所還原的無失真原始影像。



(a) (44.14 dB) (b) (44.13 dB) (c) (44.15 dB) (d) (44.15 dB)



(e) (f) (g) (h)

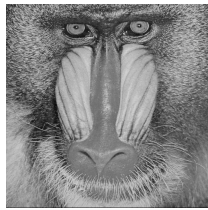


(i) (j) (k) (l)



(m) (38.93 dB) (n) (34.77 dB) (o) (41.58 dB) (p) (42.45 dB)

圖例四 第四主題—基於影像分享而得的影像修復技術之實驗結果(括號內為其 PSNR 值)。(a)-(d)為四張加工影像；(e)-(h)分別為針對(a)切割 25%區域、50%、增加頭飾，與針對(b)修改徽章等不同的破壞所產的結果；(i)-(l)則是其對應的偵測結果；(m)-(p)則是對應的修復影像。



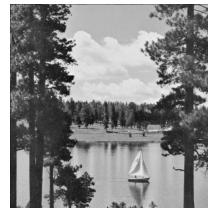
(a) (44.17 dB)



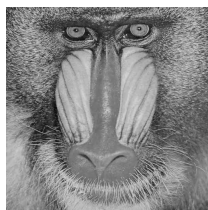
(b) (44.14 dB)



(c) (44.16 dB)



(d) (44.15 dB)



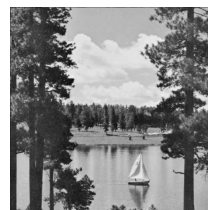
(e) (33.82 dB)



(f) (41.57 dB)



(g) (42.54 dB)



(h) (38.32 dB)

圖例五 第五主題—基於跨影像的交叉分享而得的多張影像修復技術之實驗結果(括號內為其 PSNR 值)。(a)-(b)為四張保護影像；(e)-(h)則為他們的修復影像。