有意義且不擴展分享影像之漸進式視覺密碼

侯永昌
淡江大學資訊管理學系

官振宇
淡江大學資訊管理學系

摘要

視覺密碼是一種資料加密的方法，其作法是將機密資訊分散為 n 張雜亂的 (noise-like) 分享影像 (shares)，讓每一個參與機密分享的人都分別持有一張分享影像，其目的是希望透過分享影像間的疊合，並藉由人類的視覺系統即可直接對加密資訊進行解讀。當要還原機密影像時，假如有超過 k ($k \leqq n$) 位參與者共同參與即可解譯機密資訊，否則就無法在疊合影像上察覺任何機密資訊，這就稱為 (k, n) 門檻機制的視覺機密分享 (visual secret sharing，VSS) 。漸進式視覺密碼不同於傳統視覺密碼，它的概念是透過疊合 2 張以上的分享影像，即可逐步地還原機密資訊，當疊合的分享影像愈多，所還原的機密資訊會愈來愈清晰。

在現行的漸進式視覺密碼研究中，其分享方法仍是以像素擴展為基礎，因此分享影像的大小會擴展為機密影像的 m 倍。當分享影像疊合時，機密影像上的黑點部分，在疊合影像不保證是全黑，白點的部份也不保證是半黑半白，這將會造成疊合影像的還原品質不佳。此外，在分享影像上的偽裝樣式只有一種，管理者無法得知有哪些參與者共同參與解密，這將會造成管理上的問題。

為了解決上述的問題，本研究將以漸進式視覺密碼為基礎，提出一個像素不擴展且有意義分享影像的視覺密碼分享方法，並且將分享影像的樣式擴充為多張偽裝影像。隨著疊合的分享影像增加，機密資訊的輪廓將愈來愈清晰，並且機密影像上的黑點部分，在疊合影像上一定會是全黑，白點的部份也一定是半黑半白，可以產生較佳的色差對比和視覺品質。在分享影像與疊合影像的品質上，每一張分享影像和疊合後的還原影像上分別有 $(i-1)/(n+i)$ 與 $(i-1)/(n+i)$ 的色差對比，可以清楚地顯示出偽裝影像與機密影像的內容。此外，本研究的分享矩陣設計是可以擴充與變動的，使用者可以根據需要來調整分享與疊合影像的色差對比。

關鍵字：視覺密碼、漸進式視覺密碼、機密資訊分享、不擴展分享影像、有意義的分享影像

Friendly and Unexpanded Progressive Visual Cryptography

Young-Chang Hou
Department of Information Management, Tamkang University

Zen-Yu Quan
Department of Information Management, Tamkang University

Abstract

Visual cryptography (VC) is a kind of data encoding method, which is encoding a secret image into *n* pieces of noise-like shares and distributing them to *n* participants. As long as we gather over *k* participants's share, the secret content can be revealed by human eyes through stacking those shares, while less than *k* participants cannot get any information about the secrets. This is called (*k, n*) -threshold visual secret sharing (VSS) scheme. Progressive VC (PVC) is dfferent from traditional VSS, which recovers the secret gradually. That's means, as more shares are being stacked, the outline of the secret image will be getting more clearer.

The previous studies of PVC were all based on pixel-expansion, therefore the size of shares are *m* times larger than the original ones. While recovering a secret image, they would cause a poor visual quality because the black pixels on the restored image might not be fully reconstructed to be black and white pixels might not be 50% of black. Besides, they used one kind of the camouflage image to produce all shares, supervisors might be able to know which participants had actually involved in, and it might bring about some management problems.

In this paper, we propose a novel PVC scheme to produce non-expansion and meaningful shares; and the number of the camouflage images can be extended from single-meaningful image to multiple-meaningful images. As the number of stacking shares increases, the contour of the secret image will be more obvious on the stacked shares. Our research can ensure the black pixels on the restored image to be fully black, and white pixels to be 50% black and 50% white which will cause better contrast, $(i - 1) / (n + i)$ and $(n - 1) / (n + i)$, on both shares and restored image, respectively, which can display the content of the camouflage and secret images more clearly. Moreover, our dispatching matrices are flexible which can be used to adjust the contrast based on user needs.

Key words: Visual Cryptography, Progressive Visual Cryptography, Secret Sharing, Unexpaned Share, Meaningful (Friendly) Share

壹、前言

在歷史的演進過程中，秘密通訊一直是個令人感興趣的議題，例如戰爭期間的情報掌握，是主宰戰局勝敗的關鍵因素。人們為了能安全地傳輸機密資訊，因而發展出密碼學 (Cryptography) 與藏密學 (Steganography) 的技術。密碼學是將機密資訊轉換成一串無意義的訊息，藉以達到隱藏資訊內容的目標，但是無意義的資訊外觀常常引起竊取者的注意，反而引發他試圖破解的意願。而藏密學則是發送方為了降低機密資訊被截獲或被破壞的機會，將機密資訊夾帶在不易被懷疑的物件中，藉此來掩飾機密資訊的存在，提供另一層的安全保障。

在影像隱藏的方法中，最容易實作的技術是最低位元隱藏法 (Least Significant Bit，LSB) 。藉由更改最低位元值對於像素的灰階值影響有限的特性，將機密資訊藏入偽裝影像灰階值的最低的幾個位元內，以達到藏密的目的。不過當偽裝影像藏入機密資訊後，將會對偽裝影像造成破壞，而降低偽裝影像的品質與安全性。因此 Wang 等 (2001) 利用基因演算法 (Genetic Algorithm) 找出置換機密資訊的最佳近似解，因此能夠有效地降低偽裝影像的失真程度。但是 LSB 法所能藏入的資料量通常都不大，藏入的資料也很容易受到影像處理軟體的破壞，這些都是它的主要缺點。

傳統的密碼學或藏密學都將加解密的資訊交由一人所掌管，如果他心懷不軌，機密資訊就沒有任何安全性可言，所以在資訊安全的研究領域中又發展出機密分享機制 (secret sharing scheme) 。機密分享是將重要的機密資訊分給多位參與者，機密資訊的解密必須整合多位參與者所提供的部分資訊才能進行解讀。這個概念首先是由 Shamir (1979) 所提出，其做法是將機密資訊分解成 n 個部份，每一位參與者都擁有一部份的資訊，當要還原機密資訊時，假如有超過 k ($k \leqq n$) 位參與者共同參與，即可解譯機密資訊，否則就無法進行解密，這個方法就稱為 (k, n) 門檻機制 ((k, n) - threshold))。

在 Shamir 的機密分享方法中，是透過 k-1次多項式 (polynomial of degree k-1) 運算，並將機密影像的像素值藏在 k-1次多項式的常數項中，當得到大於 k 張分享影像時，就可以列出 k 個以上的方程式，因此可以解出多項式中的常數項而還原機密影像。不過該方法只有在多項式中隱藏一個像素值，所以產生的分享影像大小與機密影像相同。Thien 與 Lin (2002) 延伸 Shamir 的概念，將機密影像上的 r 個像素值分別填入 r-1 次多項式的 r 個係數上，因此分享影像的大小會是原始機密影像的 1/r。Chen 與 Lin (2005) 採用 Thien 與 Lin 的做法，並利用重組灰階影像位元平面值的方式，進行機密影像的漸進式傳輸。Wang 與 Shyu (2007) 則是運用 Thien 與 Lin 的模型，提出三個適用於漸進式機密影像分享的方法。上述的四篇文章中，在加解密過程中皆需要複雜的數學運算，必須倚賴電腦設備的輔助才能進行，因此限制了資訊分享的應用範圍。Naor 與 Shamir (1995) 提出一個應用在影像資料上的新密碼學方法，稱為視覺密碼 (Visual Cryptography) ，其方法是將機密資訊分散為多張雜亂 (noise-like) 的分享影像 (shares) ，其目的是希望透過分享影像間的疊合，並藉由人類的視覺系統即可直接對加密資訊進行解讀。

雖然傳統視覺密碼具備很多優點，不過仍有一些問題需要解決。首先，分享影像的產生通常是透過像素擴展的方式，使得分享影像擴展為原圖的 m 倍，造成浪費儲存空間等問題。因此 Ito 等 (1999) 採用機率的概念，提出一個適用於黑白影像的像素不擴展加密法，所產生的分享影像與機密影像大小相同。Tu 與 Hou (2007) 則提出多點同時加密的方式，來解決 Ito 等人因為隨機性而造成影像雜亂的問題。Shyu (2007) 則利用隨機網格 (random grid) 的概念來製作分享影像，並提出三種適用於灰階與彩色影像的不擴展加密法。

其次，傳統視覺密碼的分享機制只適用於黑白兩色的影像上。Hou (2003) 首先提出以色彩分解與合成的概念，將彩色影像分解為三原色（青、洋紅、黃）的單色影像，並以半色調技術來模擬影像的連續調變化，將連續調影像轉換為二元影像，然後利用視覺密碼的特性來產生分享影像，因而發展出適用於分享灰階與彩色影像的視覺密碼技術。

第三，傳統視覺密碼所產生的分享影像是雜訊式影像，容易引起竊取者試圖破解的意願。因此，Ateniese 等 (2001) 提出一個新的分享技術，不僅能在個別分享影像上看到偽裝影像的內容，降低分享影像被攻擊的機會，也無法由單一分享影像上看到機密內容，而達到安全性的要求。不過在 Ateniese 等人的分享方法中，所能隱藏的機密資訊只侷限於黑白影像，因此侯永昌與吳佳鴻 (2001) 利用分色與半色調技術，將 Ateniese 等人的分享模型延伸至有色階變化的機密影像，而完成彩色影像之擴充型視覺密碼。

最後，傳統視覺密碼是一種非有即無 (all-or-nothing) 的做法，當疊合的分享影像張數少於門檻值（k 張）時，疊合影像上無法顯示機密資訊的內容，只有當疊合的張數等於或大於門檻值時，才能顯示出機密影像的訊息。因此在疊合影像上只會顯示雜訊或機密影像兩種結果，所以視覺密碼無法進行漸進式的機密資訊分享。Fang 與 Lin (2006) 提出一個漸進式 (progressive) 視覺密碼的分享方法，其概念是將機密影像分為多張雜訊式的分享影像，不過在疊合的過程中並非傳統視覺密碼的非有即無，而是隨著疊合的分享影像增加，機密影像的內容將會愈來愈清晰。Fang (2008) 進一步將分享影像上的內容，由雜訊影像轉換成有意義的偽裝影像 (stego-image) ，藉此提升分享影像的安全性。不過在 Fang 的分享方法中，所產生的分享影像大小都是機密影像的 2×2 倍，而且在分享影像上也會顯示出機密影像的輪廓，造成安全上的漏洞。並且當分享機密資訊的人數較少時，機密影像上的黑點和白點部份都可能無法完全被還原，因而降低疊合影像的視覺效果。

本研究將改善上述幾個問題，提出一個非擴展且有意義分享影像的漸進式分享方法，並將分享影像上的樣式擴展為多張不同的偽裝影像。在下面章節中，第二章將簡單說明視覺密碼的製作、半色調技術、像素不擴展技術、藏密學技術與漸進式視覺密碼。第三章是提出本研究的單一與多張有意義視覺密碼模型，並介紹其他分享矩陣的設計方法，第四章則是實驗結果與分析討論，最後在第五章是本研究的結論。

貳、文獻探討

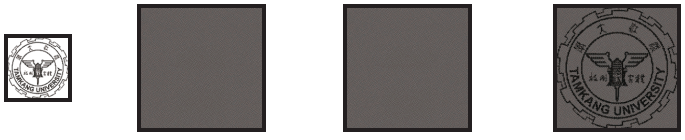
一、 視覺密碼的基本原理

視覺密碼是將機密影像分解成多張分享影像，每一位參與機密分享的參與者都擁有一張分享影像，當要還原機密影像時，藉由疊合 k 張以上的分享影像，疊合影像上就會顯現機密資訊的內容。

在進行機密影像加密前，首先設計兩個 $n \times m$ 的分享矩陣 (C_0、C_1)，分別是代表機密影像上白色或黑色部份的分享影像矩陣，其中 n 是代表參與機密分享的人數，m 則是表示像素擴展的倍數。以分享兩張影像且像素擴展 4 倍為例，機密影像上的每一個像素點會被擴展為兩個由兩白兩黑所組成的影像區塊（如表1所示）。由表1的分享模型中可以發現，無論機密影像的內容為黑為白，所挑選的影像區塊皆是兩白兩黑，加上影像區塊是隨機挑選，因此無法從任一張分享影像上的影像區塊中，解譯出機密影像的內容，也不會顯露出機密影像的輪廓，因而達到機密資訊分享的安全性。當疊合兩張分享影像時，機密影像的黑點部份會被疊合出全黑的區塊，而白點部份則是疊合出半黑半白的區塊，因此在疊合影像上產生 50% 的色差對比。以圖1為例，將一張淡江大學的校徽當成機密影像（圖1.a），製作成兩張視覺密碼的投影片（圖1.b、c），當重疊兩張投影片即可還原淡江校徽（圖1.d）。

表1：2×2擴展視覺密碼分享模型

Pixel	$Share_1$	$Share_2$	Stacked	Pixel	$Share_1$	$Share_2$	Stacked
□	▚	▚	■	■	▚	▟	■
	▞	▞	■		▞	▟	■
	▚	▚	■		▚	▟	■
	▞	▞	■		▞	▟	■
	▙	▙	■		▙	▙	■
	▟	▟	■		▟	▜	■



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

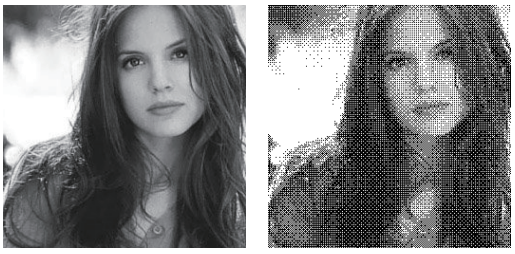
圖1：視覺密碼的分解與疊合

二、 半色調 (Halftone) 技術

每一種影像輸出設備都有特定的方法來呈現影像的色階變化，例如在電腦螢幕上是

利用電流的強弱來控制像素的光量，然後產生不同的色階；而在列印設備上則是利用半色調技術，來模擬連續調影像的色階變化。半色調是一種傳統的印刷技術，是將影像從較多色階轉換為較少色階的一種方法。列印設備藉由控制某一點是否著墨，並將墨點調整為不同形式、大小與疏密程度，便可以間接模擬出連續調影像的色調層次。於是半色調技術就可以藉由單一墨點的印（黑點）或不印（白點），將一個灰階影像轉換成二元影像。

以灰階影像 Mena 為例（圖2.a），轉換後的半色調影像（圖2.b）的每一個像素只會出現黑點或白點。雖然轉換後的半色調影像只有黑白兩色，但是人類視覺系統卻無法分辨過小的網點，而會將附近網點的顏色也納入視網膜的同一個成像位置，於是利用網點排列的疏密，人類視覺系統就可以在半色調影像中模擬出不同色階的感覺。雖然傳統的視覺密碼模型只能應用於黑白影像上，但是轉換後的半色調影像也就是一張黑白影像，因此 Hou (2003) 首先以色彩分解與合成的概念，將彩色影像分解為三張原色（青、洋紅、黃）的單色影像，並運用半色調技術，將灰階或分解後的單色影像轉換為二元影像，再藉由傳統黑白視覺密碼的方法，就可以製作出灰階與彩色影像的分享影像。



(a) (b)

圖2：半色調影像

三、像素不擴展的灰階視覺密碼加密

傳統視覺密碼的分享是以像素擴展為前提，因此機密影像上的每一個像素點，在分享影像上都是由一個影像區塊來代表，並且不論它是由機密影像上的白點或黑點擴展而來，每一個區塊內黑點與白點的比例都相同，藉此保證分享影像上不會暴露出機密影像的資訊。當要還原機密影像時，機密影像的黑點部分在疊合影像上的對應區塊中，被疊合出黑點的比例會比白點部分高（如表1所示），所以在疊合影像上會產生對比色差，而顯現出機密影像的內容（如圖1所示）。

雖然 Naor 與 Shamir (1995) 所提出的概念十分簡單，並且具有高度的安全性，不過像素擴展的結果，將會造成機密影像變形與儲存空間浪費等問題。因此 Ito 等 (1999) 從機率的角度出發，提出一個針對黑白影像的不擴展加密方法。其做法是：當機密影像的像素點是白色時，從表2的前兩列隨機任選一列作為分享的方式，使得兩張分享影像上的像素點顏色相同；反之，當機密影像的像素點是黑色時，則從表2的後兩列隨機任選，使得分享影像上的像素點顏色相異。在疊合分享影像時，機密影像上的黑點部分，疊合後

一定都是黑色的，而白點部分則是黑白出現的機率各半，因而產生出所需要的色差。Ito 等的方法雖然能避免像素擴展的問題，不過隨機挑選的分享方式，可能會破壞影像的網點分佈規則，而造成疊合影像上的凌亂視覺效果。因此 Tu 與 Hou (2007) 提出了多點加密法，即是一次選取機密影像上連續的 m 個白點（黑點）作為加密對象，使得每 m 個白點（黑點）的區域中出現黑色的機率都相等，確保在分享影像上的亂度會受到控制，因此，在疊合影像上可以得到較佳的視覺效果。

表2：Ito 的分享模型

機密影像	分享影像1	分享影像2	還原影像
□	□	□	□
	■	■	■
■	□	■	■
	■	□	■

Shyu (2007) 利用隨機網格 (Random grid) 來製作分享影像，其作法是先在分享影像 1 上設定一個隨機網格R_1，所謂隨機的意思就是網格的內容可以隨機挑選，各有50% 的機率在R_1中出現 0（白色）或1（黑色）；在分享影像 2 上的隨機網格，Shyu 提出三種不擴展的加密方法（如表3所示）。這三種分享方式在疊合影像上分別可以產生50%、25%、25%的色差，因此能夠藉由目視的方式來解讀所隱藏的機密資訊，達成不需要藉助電腦設備來解密的目標。Shyu 的作法雖然可以達到分享影像不擴展的目標，但是他的作法只能適用於 (2, 2) 門檻機制的情況，無法擴展到從 n 個參與者中，任取 k 人都可以還原機密影像的 (k, n) 門檻機制。

四、藏密學技術

藏密學 (Steganography) 是應用於傳遞機密資訊時，傳送方因擔心機密資訊遭人竊取，所以將機密資訊隱藏在其它有意義影像中的一種學問。在外觀上，這張做為偽裝的影像看起來就是一張普通影像，因此就算被人截獲，人們通常也不會懷疑其中還藏有重要的機密資料，藉此提升傳遞機密資訊的安全性。

在資訊隱藏的方法中，最低位元隱藏法 (Least Significant Bit，LSB) 是最常用的技術之一。其作法是將機密資訊藏入偽裝影像灰階值的最低的一個、或幾個位元內。由於最低位元值的變動對於影像灰階值的改變很小，人類的視覺系統並不容易察覺到偽裝影像上變化。再加上它不需要複雜的運算，因此，使得最低位元隱藏法成為最容易實作的方法。不過在偽裝影像中藏入機密資訊後，將會對偽裝影像造成破壞，並且可能會洩漏出被修改的蛛絲馬跡，降低機密資訊的安全性。因此 Wang 等 (2001) 提出一個最低位元的最佳化置換技術。其做法是利用基因演算法來找尋置換機密資訊的最佳近似解，並將置換後的近似解藏入偽裝影像的最後的 k 個位元中，因而能有效地降低偽裝影像的失真程度，提高資訊隱藏的安全性。最低位元隱藏法主要的缺點是它所能藏入的資料量通常都

不大，以避免嵌入過多的資料，導致偽裝影像品質不佳的問題。此外，最低位元的資料也很容易受到影像處理軟體的破壞，造成機密資訊遺失的問題。

Ateniese 等 (2001) 首先提出應用於視覺密碼的偽裝技術，如表4所示。其分享模型使得在分享影像上有黑白色差，所以在每一張分享影像上皆會顯示偽裝影像的內容，不過卻無法由單一分享影像來獲得機密影像資訊。當疊合分享影像後，由於疊合影像上的黑點密度不同而產生色差對比，因此能夠辨別出機密影像的內容。不過在 Ateniese 等人的分享方法中，所能隱藏的機密資訊只侷限於黑白影像。侯永昌與吳佳鴻 (2001) 則利用色彩分解與半色調技術，將彩色機密影像分解為三張分色（青、洋紅、黃）的半色調影像，並且應用 Ateniese 等人的擴充視覺密碼模型，製作出有意義的彩色偽裝分享影像。

表3：Shyu的分享模型

Method	b	prob	r_1	r_2	$r_1 \otimes r_2$	$prob(s=0)$
Algorithm 1	□	1/2	□	□	□	1/2
		1/2	■	■	■	
	■	1/2	□	■	■	0
		1/2	■	□	■	
Algorithm 2	□	1/2	□	□	□	1/2
		1/2	■	■	■	
	■	1/4	□	□	□	1/4
		1/4	□	■	■	
		1/4	■	□	■	
		1/4	■	■	■	
Algorithm 3	□	1/4	□	□	□	1/4
		1/4	□	■	■	
		1/4	■	□	■	
		1/4	■	■	■	
	■	1/2	□	■	■	0
		1/2	■	□	■	

表4：Ateniese的視覺密碼分享模型

Pixel	$Share_1$		$Share_2$		Stacked	Pixel	$Share_1$		$Share_2$		Stacked
□	W		W			■	W		W		
	W		B				W		B		
	B		W				B		W		
	B		B				B		B		

五、漸進式視覺密碼

傳統機密資訊的傳輸模式是以門檻值為基礎，當取得的分享影像張數大於或等於門檻值（k 張）時，即可進行機密資訊解密；反之，則無法解譯機密資訊。而漸進式傳輸模式則是隨著取得分享影像張數的增加，所能解譯機密資訊的內容愈為完整。Chen 與 Lin (2005) 利用重組灰階影像位元平面值的方式，首先提出一個適用於機密資訊的漸進式分享方法。其作法是先設定多個門檻值 r_j ($r_1 \leqq r_2 \leqq \cdots \leqq r_i$) ，並且一次同時取出機密影像上的 r (Σr_j) 個像素點，將這些像素值依照位元平面 ($b_7b_6b_5b_4b_3b_2b_1b_0$) 的先後順序，重組為 r 個新的像素，最後將重組後的像素值填入 i 個多項式中的 r 個係數上。當取得較少的分享影像時，只能解譯出每一個原始像素的較高位元平面值，而看到失真的機密影像。隨著分享影像的增加，機密影像將會愈來愈清晰，當取得 r_i 張以上的分享影像後，將可解譯出無失真的機密影像內容。不過 Chen 與 Lin 的做法需要電腦的幫助才能還原機密資訊，無法利用疊合、目視的方式來解密。

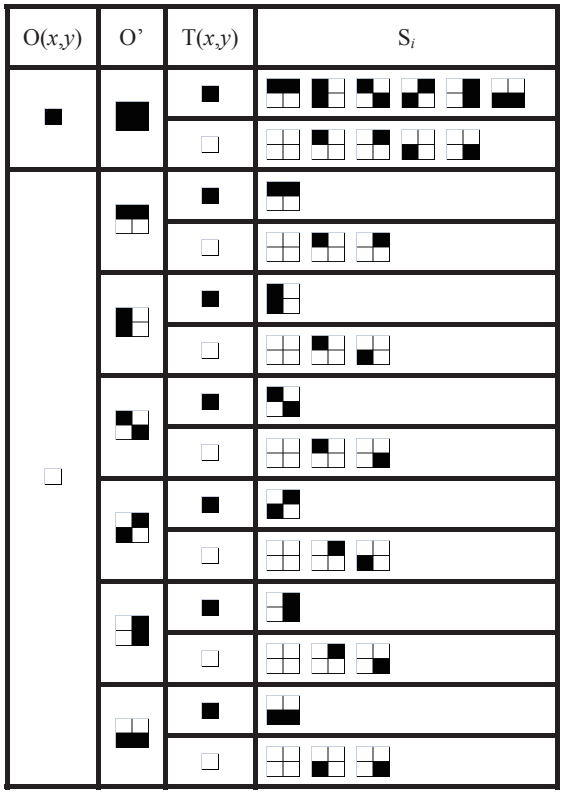
Fang 與 Lin (2006) 提出一個應用於視覺密碼的漸進式分享方法，他們的作法雖然可以直接透過分享影像的疊合來解密，不過所產生的分享影像是雜訊影像 (noise-like image)。雜訊式分享影像的外觀相似，因此當一個人擁有多張不同機密的分享影像時，他將很難挑出正確的分享影像來參與解密的過程。為了解決上述管理上的困難，Fang (2008) 延伸他 2006年的做法，提出一個有意義的漸進式機密分享方法。其做法是輸入一張經半色調處理的機密影像，將機密影像上的每一個像素點擴展成 2×2 的影像區塊，當機密影像上的像素點為黑色時，擴展為全黑的影像區塊；如果像素點為白色時，則隨意擴展為兩白兩黑的影像區塊，擴展後的影像稱之為基底影像，而分享影像 (S_i) 的內容是根據機密影像 (O) 、偽裝影像 (T) 與基底影像 (O') 的區塊內容來決定（如表5 所示）。

在 Fang (2008) 所提出的分享模型中，雖然分享影像由雜訊式轉變為有意義的偽裝影像，不過其方法仍有幾個缺點需要改善。首先，該模型是以像素擴展為基礎，因此分享影像的大小會被擴展為機密影像的 4 倍。第二，在偽裝影像的內容是白色的情況下，當機密影像為黑點時，每一個像素點被分配到 0 和 1 個黑點的機率分別為 1/5 和 4/5；而機密影的白點被分配到 0 和 1 個黑點的機率則是 1/3 和 2/3，於是在每一個 2×2 的白色影像區塊中，出現黑點的期望值分別為 4/5 和 2/3，因此會在偽裝影像的白點部分產生 2/15 (0.133) 的色差。由於黑點出現的機率並不一致，因此在分享影像上會顯露出機密影像的輪廓，因而降低分享影像的安全性。第三，當分享影像疊合後，由於分享影像上的影像區塊是隨機挑選，所以不能保證基底影像上的全黑區塊，在疊合影像上也會被疊合成全黑；同理，基底影像上的兩黑兩白區塊，也無法保證在疊合影像上可以累積到足夠的黑點，使得機密影像的白點部分都會被疊合成半黑白（50% 的黑），因此無法抹掉偽裝影像的影像輪廓。也就是說，在疊合影像上會同時具有偽裝與機密影像，導致兩個影像相互干擾，使得管理者無法輕易分辨何者為機密影像，因而造成疊合影像品質不佳的問題。最後，其分享模型的偽裝影像樣式只有一種，於是管理者無法得知有哪 k 個人參與解密的過程，而造成管理不便的問題產生。

為了解決上述問題，本研究將以漸進式視覺密碼為基礎，提出一個像素不擴展且有意義分享影像的視覺密碼分享方法，即是每一張分享影像皆是有意義的偽裝影像，偽裝

影像的樣式也由單張擴展為多張。並且機密影像的黑點部分，在疊合影像上將會被疊合成全黑，白點部分也會被疊合成半黑半白，以產生較佳的色差對比和視覺品質。

表5：Fang的視覺密碼分享模型



參、非擴展且有意義分享影像之漸進式視覺密碼

一、單一有意義視覺密碼

如果分享影像是一張雜訊影像，攔截者雖然無法從中獲得機密影像的訊息，不過這將會引發其中藏有機密資訊的聯想，因而增加攔截者嘗試攻擊的可能性。因此，當分享影像由一張雜訊影像轉變為有意義的偽裝影像時，將可以提供雙重的保護機制。第一層安全性來自於攔截者不易察覺其中藏有機密資訊，因而降低分享影像遭受攻擊的可能性。第二層安全性則來自視覺密碼的機制本身，攻擊者無法由單一分享影像來猜測出機密影像的訊息。所以採用有意義的分享影像，將可以提高機密資訊的安全性。

在雜訊式的分享影像上，每一個單位面積中出現黑點的機率皆相同，在分享影像上沒有明顯的色差對比，因此不會顯示出任何影像的輪廓。不過在有意義的分享方法中，分享影像上必須要有偽裝影像的輪廓，即是在偽裝影像上比較黑的部份，在分享影像上必須比較黑；反之，在偽裝影像上比較白的部份，在分享影像上也要比較白，因此在分

享影像上的黑色與白色區域，出現黑點的機率將會不同，因而產生色差的區別。機密影像上的黑點或白點，可能是由分享影像上的白點所疊合而成，也可能是由分享影像上的黑點所疊合，因此需要四種分享矩陣 (M^0～M^3)，來代表機密影像與偽裝影像的像素分別為（白，白）、（白，黑）、（黑，白）、（黑，黑）四種可能的分享機制。

本研究使用四個 $n \times n$ 的基本分享矩陣 (C_0～C_3)，C_0 矩陣中的第一列全部設為 1（黑色），其餘的全部設為 0（白色）；而 C_1 和 C_2 矩陣相同，都是在矩陣的主對角線上設為 1，其餘的全部設為 0；C_3 矩陣則是矩陣內所有的值都設為1，如表6所示。矩陣中的每一列都代表一種分享方式，每一行則是代表每一位參與者所被分配的內容。在 C_0 矩陣中，每一行都只有一個 1，代表以 C_0 矩陣來產生分享影像時，每一位參與者都只有 $1/n$ 的機率被分配到黑色，而且這些黑點都出現在每一張分享影像上的相同像素位置上。因此，當分享影像疊合時，這些像素點也是只有 $1/n$ 的機率會疊合出黑色。在 C_1 和 C_2 矩陣中，每一位參與者也都是只有 $1/n$ 的機率被分配到黑色，只不過它們都出現在不同的分享影像上的不同的像素位置上。當分享影像疊合時，這些像素點出現黑色的機率將會逐漸增加，當疊合所有的分享影像後，出現黑點的機率將會達到100%。C_3 矩陣則是代表每一位參與者都有100%的機率被分配到黑色，當分享影像疊合時，這一個像素點自然會保持100%的機率會被疊合出黑色。

四個分享矩陣 (M^0 ～ M^3) 皆是由 C^0～C^3 所組合而成，矩陣的大小皆為 $2n \times n$（表7）。為了能夠清楚辨識偽裝影像的內容，所以偽裝影像的黑色部分，在分享影像上出現黑色的機率將會高於白色部分。因此我們將 C_2 放置在偽裝影像為白色的相關矩陣 (M^0, M^2) 中，將 C^3 放置在偽裝影像為黑色的相關矩陣 (M^1, M^3) 中，利用矩陣 C_2 和 C_3 來控制偽裝影像上的色差。因此，當偽裝影像上的像素為白色時，每一張分享影像上出現黑色的機率都保持 $2/2n$；當偽裝影像上的像素為黑色時，出現黑點的機率將增加為 $(n + 1)/2n$，因此在每一張分享影像上產生 $(n\text{-}1)/2n$ 的色差對比。使得分享影像上白的地方比較白、黑的地方比較黑，顯露出偽裝影像的輪廓。

表6：4個 n×n 的基本分享矩陣

$C_0 = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{n \times n}$	$C_1 = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}_{n \times n}$
$C_2 = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}_{n \times n}$	$C_3 = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 1 & 1 & \cdots & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & \cdots & \cdots & 1 \end{bmatrix}_{n \times n}$

表7：4個 2n×n 的機密影像分享矩陣

		偽裝影像	
		白	黑
機密影像	白	$M^0 = \begin{bmatrix} C_2 \\ C_0 \end{bmatrix}_{2n \times n}$	$M^1 = \begin{bmatrix} C_3 \\ C_0 \end{bmatrix}_{2n \times n}$
	黑	$M^2 = \begin{bmatrix} C_2 \\ C_1 \end{bmatrix}_{2n \times n}$	$M^3 = \begin{bmatrix} C_3 \\ C_1 \end{bmatrix}_{2n \times n}$

為了能清楚看到機密影像的內容，在疊合影像上的黑色區域出現黑色的機率也要比白色區域要高。因此我們將 C_0 放置在機密影像為白色的相關矩陣 (M^0, M^1) 中，將 C_1 放置在機密影像為黑色的相關矩陣 (M^2, M^3) 中，利用矩陣 C_0 和C_1 來控制疊合影像上的色差。因此，當疊合 k 張分享影像後，機密影像中的白點部份有 $(k + 1)/2n$～ $(n + 1)/2n$ 的機率出現黑色，而黑點部份則有 $2k/2n$～ $(n + k)/2n$的機率出現黑色。隨著疊合的分享影像張數增加，機密影像的黑色區域變黑的速率將大於白色區域，使得黑白之間的色差對比愈來愈明顯。當疊合所有分享影像時，疊合影像上的白點將有 $(n + 1)/2n$ 的機率出現黑色，而黑色部分則是全黑，於是在疊合影像上出現 $(n\text{-}1)/2n$ 的黑白色差。使得疊合後的還原影像，在機密影像的黑色部分會顯得比較黑、白色部分則是比較白，藉以顯露出機密影像的輪廓。

在產生分享影像時，由隨機亂數取得一個 1～$2n$ 的亂數值 t。當機密影像與偽裝影像為 (白，白) 時，取出 M^0 矩陣中第 t 列的列向量，將第一個值 $M^0(t, 1)$ 分配給第 1 張分享影像，第二個值 $M^0(t, 2)$ 分給第 2 張分享影像，…，依序將第 n 個值 $M^0(t, n)$ 設給第 n 張分享影像。同理，如果機密影像和偽裝影像依序為（白，黑）、（黑，白）與（黑，黑）等組合時，只要由隨機亂數值取出對應矩陣 (M^1, M^2, M^3) 中的列向量，依序將其值分配給對應的分享影像即可。

在每一次的影像內容分配時，由於每一張分享影像都只被分配到一個像素，因此本研究所產生的分享影像大小將會與機密影像相同，而能夠避免像素擴展所造成的問題。在安全性的考量上，矩陣 M^0 與 M^2 中的每一行皆是兩個 1，而矩陣 M^1 與 M^3 中的每一行則是皆為 $n + 1$ 個 1，因此無論機密像素的顏色是黑或是白，在分享影像上只要是白色的區域都有 $2/2n$ 的機率被分配到黑點，而黑色的區域則有 $(n + 1)/2n$ 的機率被分配到黑點，完全不會洩露出機密影像的蛛絲馬跡，所以分享影像可視為是安全的。而且分享影像上顯示的內容就是偽裝影像，攔截者可能會誤以為是一般的圖片，不易察覺其中還藏有部份機密影像的資訊，因而降低了試圖攻擊的可能性，使得機密影像的安全性大為提高。在疊合影像上，不論機密影像的白點部份是由偽裝影像上的黑點或是白點所疊合而成，都有 $(n + 1)/2n$ 的機率被疊合出黑色，而黑點的部分則一定是全黑，所以在疊合影像上不僅看不到偽裝影像的邊緣輪廓，還可以達到 $(n\text{-}1)/2n$ 的高色差對比，產生良好的

還原影像品質。因此，本研究的分享模型中，在分享影像的大小、安全性與疊合影像品質等衡量指標上，都將優於 Fang (2008) 所提出的模型。

單一有意義視覺密碼演算法

Input：兩張寬和高分別為 W、H，且經半色調處理的影像，一張為機密影像 P，一張為偽裝影像 C

Output：n 張相同內容的分享影像 S^m，$m = 1, 2, \ldots, n$

Process：

1 隨機取得一個 $1 \sim 2n$ 的 t 值

2 針對機密與偽裝影像的每一個像素 $P(i, j)$ 與 $C(i, j)$，$1 \le i \le W$，$1 \le j \le H$

針對每一張分享影像 S^m，$m = 1, 2, \ldots, n$

2.1 if $P(i, j) = 0$ and $C(i, j) = 0$ then $S^m(i, j) = M^0(t, m)$

2.2 else if $P(i, j) = 0$ and $C(i, j) = 1$ then $S^m(i, j) = M^1(t, m)$

2.3 else if $P(i, j) = 1$ and $C(i, j) = 0$ then $S^m(i, j) = M^2(t, m)$

2.4 else $S^m(i, j) = M^3(t, m)$

3 重複執行步驟 1、2，直到整張機密影像 P 上的每一個像素都被處理完畢為止

二、分享矩陣的其它設計

矩陣 $M^0 \sim M^3$ 的上半部 (C^2 和 C^3) 主要是控制分享影像上的黑白色差，除了表6的設計以外，也可以運用其它設計方式（表8）來獲得不同程度的色差對比。假設新的分享矩陣 C_2^i 和 C_3^i 的大小都是 $i \times n$，i 為介於 $2 \sim n$ 之間的整數。在矩陣 C_2^i 中，將矩陣依行數切割成 i 個區間，每個區間都擁有 n/i 行（如果 n/i 除不盡時，則有些區間會多分到一行，成為 $\lceil n/i \rceil$ 行，有些區間會少一行，成為 $\lfloor n/i \rfloor$ 行）。第一列在第一個區間內的值皆設為 1，第二列在第二個區間內的值皆設為 1，…，第 i 列在第 i 個區間內的值皆設為 1，其餘位置的值都設為 0。而矩陣 C_3^i 則是將矩陣內的值全部設為 1。也就是根據矩陣 C_3^i 所分配的分享影像都只有一個機會出現黑點，而根據 C_3^i 所分配的分享影像則有 i 個機會出現黑點，因此可以得到一個新的分享矩陣設計（表9），其矩陣大小為 $(i + n) \times n$。

根據表9的設計，偽裝影像上的白點部分有 $2/(n + i)$ 的機率會被分配到黑點，而黑點的部分則是有 $(i + 1) / (n + i)$ 的機率會被分配到黑點，因此在每一張分享影像上的黑白色差是 $(i\text{-}1) / (n + i)$ ，$i = 2, 3, ..., n$。當 i 值愈大時，在分享影像上的黑白色差愈大，黑白區域的輪廓將更加明顯；反之，分享影像上的黑白色差會降低，黑白區域的輪廓將會比較不清楚，因此分享影像的品質較差。當疊合 n 張分享影像後，機密影像的白點部分有 $(i + 1) / (n + i)$ 的機會出現黑點，而黑點部分則是100%的黑，因此疊合影像上的黑白色差對比是 $(n\text{-}1) / (n + i)$ ，$i = 2, 3, ..., n$，因此，當 i 值愈小時，疊合影像上的黑白色差愈大，也就是機密影像的還原品質也愈好。

表8：2個 $i \times n$ 的基本分享矩陣

$$C_2^i = \begin{bmatrix} 1\cdots1 & 0\cdots0 & \cdots & \cdots & 0\cdots0 \\ 0\cdots0 & 1\cdots1 & 0\cdots0 & \cdots & 0\cdots0 \\ \vdots & 0\cdots0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0\cdots0 & \cdots & \cdots & 0\cdots0 & 1\cdots1 \end{bmatrix}_{i\times n}$$

$$C_3^i = \begin{bmatrix} 1 & 1 & \cdots & \cdots & \cdots & \cdots & \cdots & 1 \\ 1 & 1 & \cdots & \cdots & \cdots & \cdots & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & \cdots & \cdots & \cdots & \cdots & \cdots & 1 \end{bmatrix}_{i\times n}$$

表9：4個 $(i + n) \times n$ 的新機密影像分享矩陣

		偽裝影像	
		白	黑
機密影像	白	$M^0 = \begin{bmatrix} C_2^i \\ C_0 \end{bmatrix}_{(i+n)\times n}$	$M^1 = \begin{bmatrix} C_3^i \\ C_0 \end{bmatrix}_{(i+n)\times n}$
	黑	$M^2 = \begin{bmatrix} C_2^i \\ C_1 \end{bmatrix}_{(i+n)\times n}$	$M^3 = \begin{bmatrix} C_3^i \\ C_1 \end{bmatrix}_{(i+n)\times n}$

三、多張有意義視覺密碼

在3.1節中，所產生的分享影像都是有意義的偽裝影像，攔截者不易察覺其中是否藏有機密訊息，因而降低被攻擊的機會，擁有較高的安全性保護。但是在這個分享機制下，每一張分享影像上的內容皆相同，當有事後稽核 (audit) 的需要時，就比較難透過「以圖追人」的方法，辨識出這些分享影像是屬於哪些參與者。因此由單張偽裝影像延伸至多張有意義的偽裝影像後，將能有效地解決上述的問題。

利用多張有意義的偽裝影像來產生對應分享影像的過程中，疊合影像上的每一點像素內容（黑色或白色），是由不同分享影像上的黑點（白點）所疊合而成，每一張分享影像在同一個像素位置上的像素值可能不同，例如：第一張是白色，第二、三、四張是黑色等情況。因此，在產生分享影像時，不能像單張偽裝影像的作法，只是取得對應矩陣中的某一列，並將列向量值分配給每一位參與者，而是要依據每一張偽裝影像與機密

影像上的顏色，分別取不同矩陣 (M^0、M^1 或 M^2、M^3) 中的值來進行分享。

在產生分享影像時，首先由隨機亂數取得一個 $1\sim2n$ 的 t 值。當機密影像是白色時，取出 M^0 與 M^1 矩陣中的第 t 列，如果第 m 張偽裝影像是白色，將矩陣 M^0 的第 m 個值 $M^0(t, m)$ 分配給第 m 個參與者；如果第 m 張偽裝影像是黑色，將矩陣 M^1 的第 m 個值 $M^1(t, m)$ 分配給第 m 個參與者。反之，當機密影像是黑色時，則是取出 M^2 與 M^3 矩陣中的第 t 列，根據第 m 張偽裝影像的內容，將矩陣 M^2 或 M^3 的第 m 個值取出，分配到第 m 張分享影像中。

根據這種方式，就可以依照不同的偽裝影像來產生不同內容的分享影像，達到易於管理的目的。在每一張分享影像上，白色區域與黑色區域出現黑點的機率都分別是 $2/2n$ 與 $(n + 1)/2n$，因此每一張分享影像上都有相同的色差，不會有不同的分享影像對比差異懸殊的問題發生。

多張有意義視覺密碼演算法

Input：$n + 1$ 張寬和高分別為 W、H，且經半色調處理的影像，一張為機密影像 P，其它為偽裝影像 C_m，$m = 1, 2, \ldots, n$

Output：n 張分享影像 S^m，$m = 1, 2, \ldots, n$

Process：

1 隨機取得一個 $1\sim2n$ 的 t 值

2 針對機密影像的每一個像素 $P(i, j)$，$1 \le i \le W$，$1 \le j \le H$

針對每一張偽裝與分享影像 C_m 與 S^m，$m = 1, 2, \ldots, n$

2.1 if $P(i, j) = 0$ and $C_m(i, j) = 0$ then $S^m(i, j) = M^0(t, m)$

2.2 else if $P(i, j) = 0$ and $C_m(i, j) = 1$ then $S^m(i, j) = M^1(t, m)$

2.3 else if $P(i, j) = 1$ and $C_m(i, j) = 0$ then $S^m(i, j) = M^2(t, m)$

2.4 else $S^m(i, j) = M^3(t, m)$

3 重複執行步驟 1、2，直到整張機密影像 P 上的每一個像素都被處理完畢為止

肆、實驗結果與分析討論

實驗環境的 CPU 是 AMD Athlon (tm) XP 2600+ 1.91GHz，記憶體 256 MB，作業系統是 Windows XP，開發軟體是使用 Java (JDK 1.6.0) 。並利用上述提出的兩個方法進行實驗，實驗的影像依序是八卦、太極、文字 1、文字 2、唐老鴨、木蘭、水滴、Mena 等八張經半色調處理的影像（圖3）。

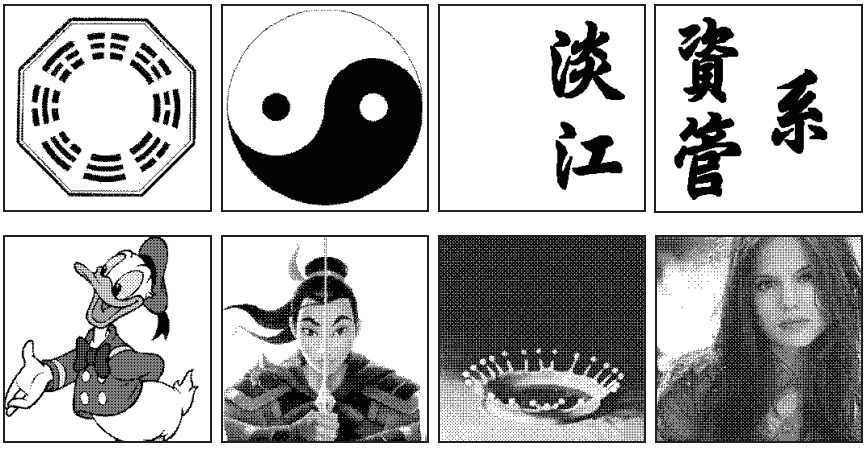


圖3：實驗影像

一、實驗一：單張有意義的分享影像

圖4～圖5是根據 3.1 節的方法所產生的分享影像，分享的影像張數分別設定為 6、7 張，採用的機密分享矩陣如表7 所示，程式執行的時間分別為 1.244、1.375 秒。

圖4以六張分享影像為例，分享影像（圖4.a）上白色區域與黑色區域出現黑點的機率分別為 2/12 與 7/12，由於黑點的分佈差異（41.67% 的色差對比）而顯示出偽裝影像內容，然而卻無法從某一張分享影像中獲得機密資訊。當疊合 k 張分享影像後，機密影像中的白點部分，疊合出黑點的機率是 $(k + 1)/12$（由分享影像中的白點疊合而來）～ 7/12（由分享影像中的黑點疊合而來）的黑，而黑點部份則是 $2k/12$（由分享影像中的白點疊合而來）～ $(k + 6)/12$（由分享影像中的黑點疊合而來）的黑。因此，在重疊的張數少的時候（圖4.b～c），部份機密影像的黑色部份（由分享影像中的白點疊合而來）還沒有累積出足夠的黑色像素，它顯示黑色的程度，甚至不如分享影像上的黑色部份，因此機密影像的輪廓不明顯。但是，黑色地區累積黑點的速率大於白色地區，隨著疊合張數的增加，漸進式的本質逐漸顯現，機密影像的內容將愈來愈清晰（圖4.d ～ f）。當疊合所有的分享影像以後，在機密影像（圖4.f）中的白色區域，疊合出黑點的機率為 7/12，而黑色區域則是全黑，因此，在疊合影像上出現 5/12 (41.67%) 的色差對比，足以清楚地辨識機密影像的內容。

圖5以七張分享影像為例，分享影像（圖5.a）上白色區域與黑色區域出現黑點的機率分別為 2/14 與 8/14，當疊合所有的分享影像以後，在機密影像（圖5.g）中的白色區域，疊合出黑點的機率為 8/14，而黑色區域則是全黑。因此，不論在分享影像或疊合影像上都出現 6/14 (42.86%) 的色差對比，足以清楚地辨識分享影像或機密影像的內容。

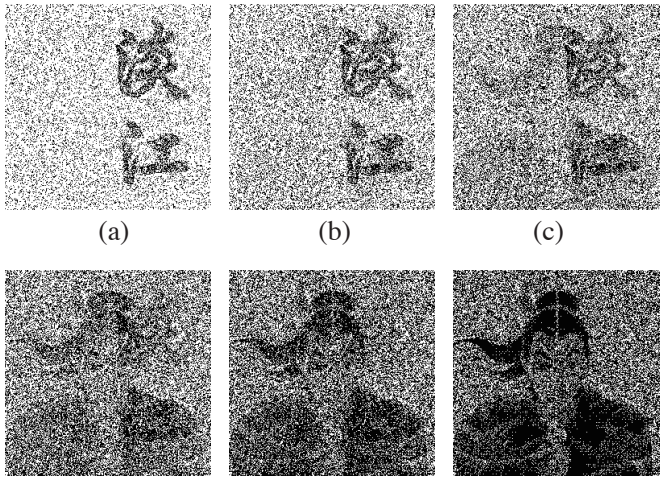


圖4：6張有意義且分享影像內容相同的實驗結果
(a) ～ (f) 任1～6張分享影像疊合

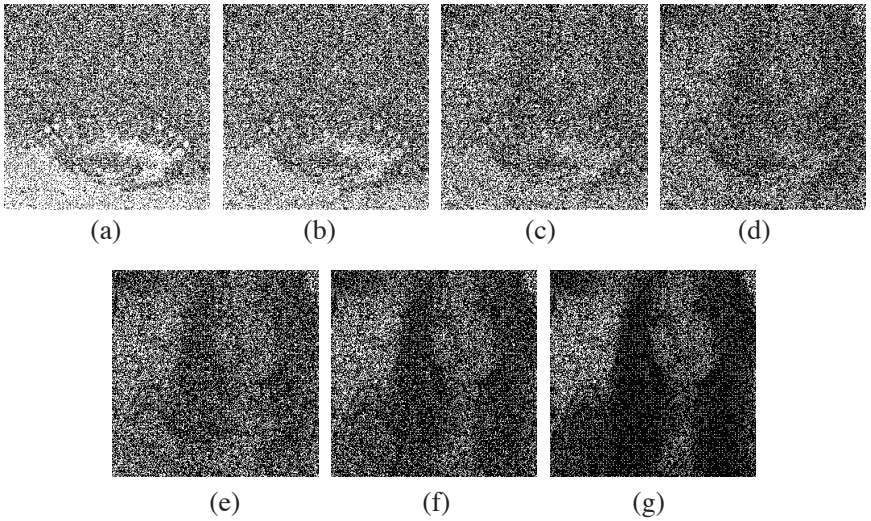


圖5：7張有意義且分享影像內容相同的實驗結果
(a) ～ (g) 任1～7張分享影像疊合

根據實驗結果可以發現，當偽裝影像是文字（圖4）時，因為圖案的結構規律，所以雖然是利用亂數的結果來產生分享影像，其分享影像依然能夠清晰地顯示其圖樣。反觀如果是以灰階影像（圖5）做為偽裝影像，其圖形的輪廓本來就不是那麼明顯，加上亂數所帶來的不規則性，使得分享影像的清晰度比卡通圖案或文字印刷要差。

在還原機密影像時，在機密影像上的黑色部份出現黑點的機率，一定要大於機密影像上的白色部份。但是，機密影像上的白色部份有可能是由分享影像上黑色的部份所疊

合而成（疊合 k 張分享影像後，出現黑點的機率為 $(n+1)/2n$）；反之，機密影像上的黑色部份可能是由分享影像上白色的部份所疊合而成（疊合 k 張分享影像後，出現黑點的機率為 $2k/2n$）。因此，在重疊的張數少的時候，機密影像的黑色部份還沒有累積出足夠的黑色像素，它在部份地區顯示黑色的程度，甚至不如分享影像上的黑色部份，因此機密影像的輪廓不明顯。一直要到 $2k/2n > (n+1)/2n$ 時，也就是疊合的張數 k 大於 $(n+1)/2$ 時，機密影像的內容將愈來愈清晰，漸進式的本質逐漸顯現。這一點由圖4～圖5 中可以得到印證。

我們以偽裝影像與機密影像分別為文字 1 和文字 2 來產生五張有意義的分享影像，並將本研究與 Fang (2008) 的兩個實驗結果整理成表10。從表10 可以得知，由於 Fang 的分享模型是採取像素擴展的方式（表5），因此所分享影像大小將會是機密影像的 4 倍，而本研究則是改進為非擴展式分享，因而可以減少儲存空間與傳輸時間的浪費。

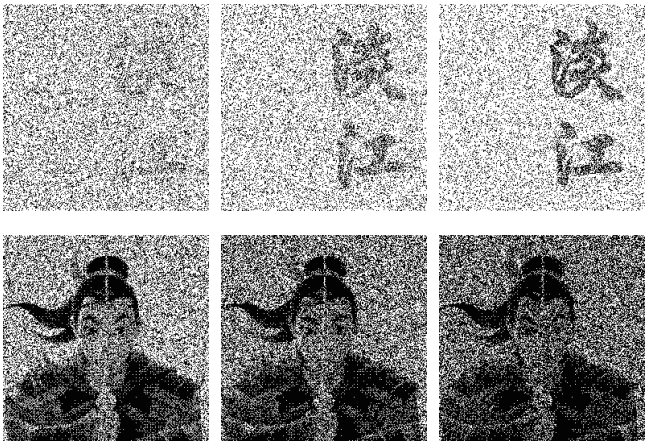
其次是分享模型的內容設計上，無論偽裝影像上的像素點內容是黑色或白色，被分配到黑點的機率分別為 3/5 和 1/5，因此可以保證本研究所產生的每一張分享影像上，都會呈現出有意義的偽裝影像，並且不會洩露出機密影像的邊緣輪廓。然而在 Fang 的模型中，由於偽裝影像的白點部分在分享影像上被分配到黑點的機率不一致，使得在偽裝影像與機密影像的內容為（白，黑）時，被分配到黑點的機率為 4/5，會大於在偽裝影像與機密影像為（白，白）時的機率 (2/3) ，因而出現 2/15 (≒ 13%) 的色差，因此在分享影像上會暴露出機密影像的圖像，而降低分享影像的安全性。以表10.a 為例，分享影像的左方即隱約出現文字 2 的圖像。此外，機密影像為白點部分被分配到黑點的機率也不一致，使得在偽裝影像與機密影像的內容為（黑，白）時，分享影像上被分配到 2 個黑點的機率為 100%，而在（白，白）的狀況下，分享影像上被分配到 0 個和 1 個黑點的機率分別是 1/3、2/3。當重疊五張分享影像後，對應偽裝影像與機密影像的組合為（黑，白）時，每一個 2×2 的區塊都有 2 個黑點，而在（白，白）的組合時，每一個 2×2 的區塊出現 0 個黑點的機率是 1/243，而出現 1 個和 2 個黑點的機率依序是 62/243、180/243，使得每一個 2×2 的區塊中出現黑點的期望值為 422/243 (≒1.74) 。由於這一種黑白的色差，而造成疊合影像上表10.c 可以清楚看到偽裝影像（文字 1）的輪廓，而造成視覺上的混淆。

最後則是針對於疊合影像品質的比較。由於 Fang 的分享模型是基於機率分配，如果機密影像的白點部分是由分享影像的白點部分所堆疊而成，在疊合影像上無法保證一定能夠累積足夠的黑點，因此某些影像區塊無法完全還原成兩黑兩白，而分享影像上的黑點部份一定有兩個黑點，因此無法抹去偽裝影像的內容（見表10.c 的右半部），於是在疊合影像上會同時存在機密與偽裝影像兩者，而造成視覺效果上的混淆。此外，機密影像的黑點部分如果是由分享影像的白點部分所堆疊而成，被疊合出全黑的影像區塊的機率也低於由分享影像的黑點部分所堆疊的區域（見表10.c 的「系」字），這將會造成疊合影像品質不佳的問題。雖然本研究也是採取機率分配的概念，但是從本研究的分享模型可以得知，當重疊所有的分享影像後，機密影像的黑點部分將會被疊合成全黑，而白點部分則是保持60%的黑，因此疊合影像上可以產生40%的色差對比，這都優於 Fang 的實驗結果（25%的色差對比），所以本研究的疊合影像具有較好的還原品質。

二、實驗二：不同的分享矩陣

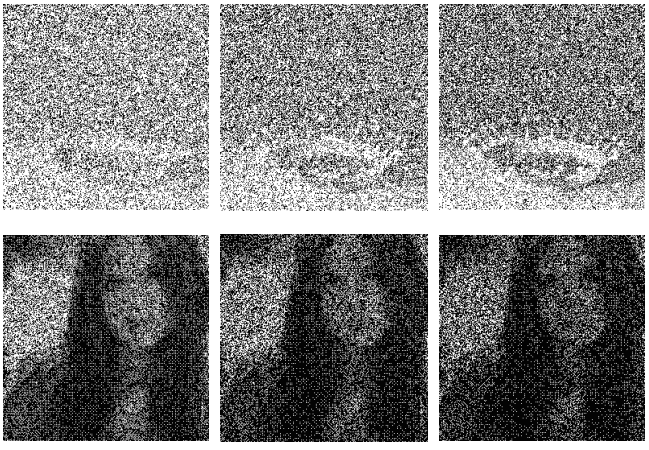
在表9中，主要用來控制分享影像上的黑白色差是 C_2^i 和 C_3^i 的部份，當偽裝影像上的像素為白色時，每一張分享影像上出現黑色的機率都保持 $2/(n+i)$ ；當偽裝影像上的像素為黑色時，出現黑點的機率將增加為 $(i+1)/(n+i)$ ，因此在每一張分享影像上產生 $(i-1)/(n+i)$ 的色差對比。使得在每一張分享影像上，偽裝影像的白色區域會顯得比較白，而黑色區域則是比較黑，因而顯露出偽裝影像的輪廓。其中 i 的值介於 2 到 n 之間。

本實驗主要是想探討不同的 i 值，對於分享影像與疊合後所還原的機密影像的影響。圖6～圖7是根據表9的分享矩陣所產生的分享影像，圖6的分享影像張數設定為 6 張，i 值分別設為 2、4、6。圖7 的分享影像張數設定為 7 張，i 值分別設為 3、5、7。



(a) $i=2$ (b) $i=4$ (c) $i=6$

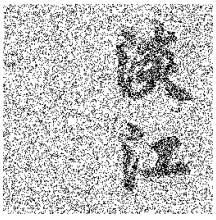
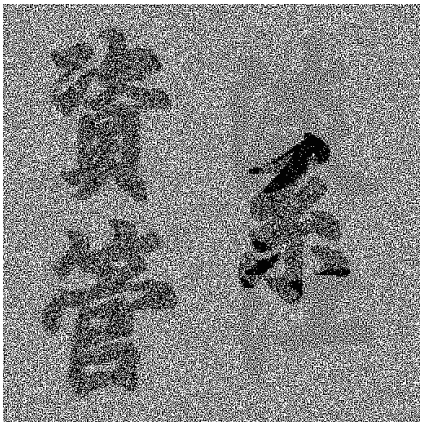
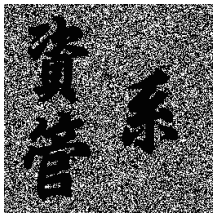
圖6：不同分享矩陣的影像



(a) $i=3$ (b) $i=5$ (c) $i=7$

圖7：不同分享矩陣的影像

表10：本研究與Fang的比較表

	Fang (2008)	本研究
分享影像		
	(a) 在偽裝影像的白色部份有 13% 的色差對比，會隱約洩漏出機密影像 (文字 2)「資管系」的背景字樣	(b) 有意義偽裝影像，不會洩漏出任何機密影像的邊緣輪廓
疊合影像		
	(c) 機密影像的黑點不保證為全黑，白點也不保證為半黑白，在疊合影像上會同時出現偽裝與機密影像，因而造成視覺效果混淆的情況產生	(d) 機密影像的黑點被還原為全黑，且在疊合影像上不會出現偽裝影像
影像大小	512 × 512 (擴展為 4 倍)	256 × 256 (不擴展)

根據圖6～圖7 的結果可以發現，當 i 值愈大時，在分享影像上的黑白色差愈大，黑白區域的輪廓更加明顯，因此分享影像的品質較佳；反之，當 i 值比較小時，分享影像

上的黑白色差就比較低，黑白區域的輪廓比較不清楚，因此分享影像的品質較差。當 i 值比較小時，因為圖6的偽裝影像其圖案結構比較規律，因此所產生的分享影像的效果比圖7 的結果為佳。當疊合 n 張分享影像後，機密影像的白點部分有 $(i+1)/(n+i)$ 的機會出現黑點，而黑點部分則是全黑，疊合影像上的黑白色差對比是 $(n\text{-}1)/(n+i)$ ，$i = 2, 3, ..., n$。因此，當 i 值愈小時，疊合影像上的黑白色差愈大，也就是機密影像的還原品質愈好。

機密資訊的管理者如果是希望分享影像上的色差明顯，i 應該要取比較大的值；反之，如果是希望疊合影像較清晰，則 i 應該要取比較小的值。為了使分享影像與疊合後的機密影像都有足夠的色差，而達到較佳的視覺品質，建議將分享矩陣的大小設定為 $2n \times n$，如表6 與表7所示。

三、實驗三：多張有意義分享影像

圖8是根據 3.3 節的方法所產生的分享影像，分享的影像張數設定為 6 張，程式執行的時間為 3.105 秒。在多張有意義且漸進式的分享方法中，每一張分享影像上的內容都不同，由於分享影像上黑白之間有41.67%的色差對比，因而可以顯示出偽裝影像的內容，並且無法從分享影像中獲得機密內容的蛛絲馬跡。當疊合 k 張分享影像後，機密影像中的白點部分，被疊合出黑點的機率是 $(k+1)/12$～$7/12$ 的黑，而黑點部份則是 $2k/12$ ～ $(k+6)/12$ 的黑。因此，當疊合全部分享影像後，在機密影像中的白點部份，被疊合出黑點的機率為7/12，而黑點部份則是全黑，因此在疊合影像上會出現5/12 (41.67%) 的色差對比，足以清楚地辨識機密內容。

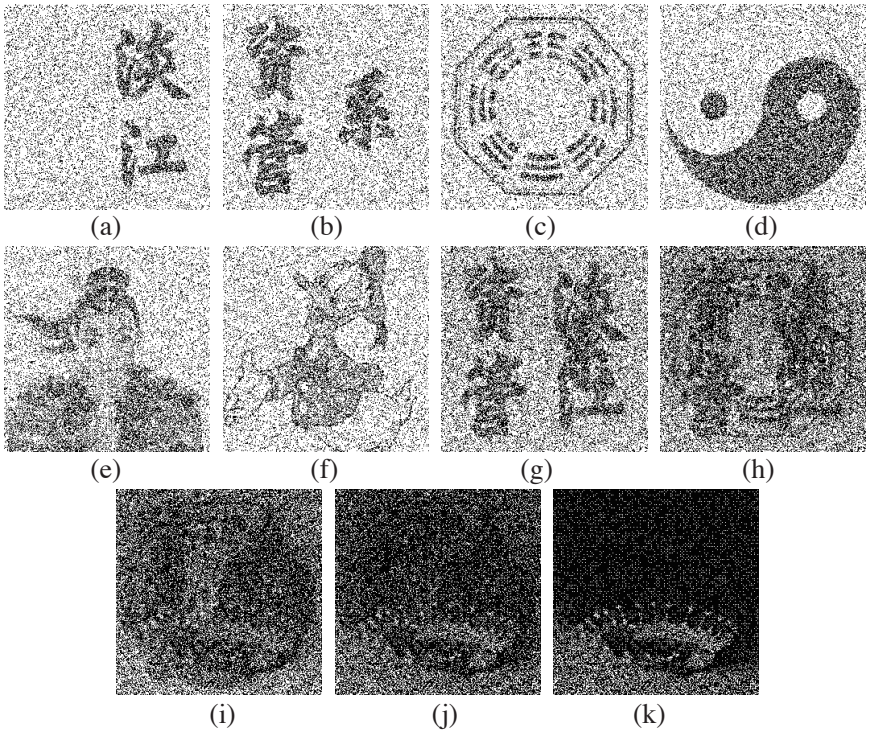


圖8：6張有意義且分享影像內容相異的實驗結果
(a) ～ (f) 任一張分享影像， (g) ～ (k) 依序疊合2～6張分享影像

四、分析與討論

表11是本研究與其他研究的比較。相較於其他研究者的做法，本研究的優點有： (1) 利用非擴展技術進行機密資訊分享，所產生的分享影像大小與機密影像相同，因此可以減少儲存空間與傳輸時間的浪費。 (2) 在分享影像內容上，本研究的分享影像是顯示有意義的偽裝影像，並且分享影像的樣式擴充為多張偽裝影像，可以增加管理的方便性。 (3) 在分享與疊合影像的品質上，每一張分享影像和疊合後的疊合影像上分別有 $(i - 1) / (n + i)$ 與 $(n - 1) / (n + i)$ 的色差對比，可以清楚地顯示出偽裝影像與機密影像的內容。 (4) 本研究的分享矩陣設計是可變動的，其中 $i = 2, 3, ..., n$，使用者可以根據需要來調整分享與疊合影像的色差對比。當 $i = n$ 時，每一張分享影像和疊合影像上都有 $(n - 1) /2n$ 的高色差對比。 (5) 雖然本研究也是採用機率的概念，但是在機密影像上的黑點部份，本研究的結果是會被完全還原，白點的部份也一定會被完全還原成半黑白，所以在疊合影像上可以產生較佳的視覺品質。 (6) 本研究的分享矩陣設計不會在分享影像或疊合影像上洩漏出任何機密影像或偽裝影像的蛛絲馬跡，可以確保機密資訊的安全性。

表11：本研究與其他漸進式研究之比較

作者	分享影像大小	分享影像內容	分享影像樣式	色差對比		分享矩陣的擴充性	疊合品質(黑點還原為全黑、白為半黑白)	分享影像的安全性
				分享影像	疊合影像			
Fang 與 Lin	放大2×2	雜訊	—	—	50%	無	不保證	不安全
Fang	放大2×2	有意義	單一	25%	50%	無	不保證	不安全
本研究	原始大小	有意義	多張	$(i\text{-}1) / (n+i)$	$(n\text{-}1) / (n+i)$	有	保證	安全

伍、結論

傳統視覺密碼是將一張機密影像加密成 n 張分享影像，參與機密分享的 n 個參與者都分別持有一張分享影像，只要疊合 k 張或 k 張以上的分享影像，即可解密機密訊息；相反地，當少於 k 張分享影像時，便無法透過分享影像的重疊來解密機密資訊。視覺密碼的優點在於解密方式是透過人眼完成，不需要借助額外的電腦設備或複雜的解密演算法，也由於這種特殊的解密方式，使得視覺密碼能夠適用於沒有電腦設備的情況。

漸進式視覺密碼不同於傳統視覺密碼，它的概念是透過疊合 2 張以上的分享影像，即可逐步地還原機密資訊，當疊合的分享影像愈多，所還原的機密資訊會愈來愈清晰。這個概念延伸視覺密碼的應用性，使得視覺密碼的解密過程由過去非有即無的模式，轉變為漸進式的傳輸方式，因此增加機密分享機制的彈性。不過現行的漸進式視覺密碼研究皆是利用像素擴展的分享方式，然而像素擴展的結果將會產生分享影像變形、不易攜帶，以及浪費傳輸時間與儲存空間等問題。此外，分享影像上若是顯示雜訊影像，將會

引起攔截者的注意，增加被攻擊的可能性。如果運用藏密學的概念，將分享影像由以往的雜訊影像，轉變成有意義的偽裝影像，使得攔截者不易察覺其中藏有機密資訊，將更可以提高機密資訊的安全性。

因此，本研究是以漸進式視覺密碼為基礎，提出一個非擴展的視覺密碼分享方法，並在分享影像上顯示單張或多張有意義的偽裝影像。為了在分享影像上顯示有意義的偽裝影像，分享矩陣的設計必須讓偽裝影像上的黑點區域，被分配到黑點的機率大於白點區域，使得在每一張分享影像上，都能顯示出偽裝影像的黑白輪廓，而矩陣 C_2 和 C_3 就是用來控制分享影像上的黑白色差。無論機密影像上的像素內容為何，偽裝影像上的白色與黑色區域都是以固定的機率（分別是 $2/2n$, $(n + 1)/2n$）來分配黑點給每一張分享影像，所以分享影像上不會顯露機密影像的資訊，而滿足視覺密碼的精神。因為分享影像上是有意義的內容，可以降低攔截者的懷疑與試圖攻擊的可能性，因此可以保護機密影像的安全性。

為了在疊合影像上顯示有意義的機密影像，分享矩陣的設計也必須讓機密影像上的黑點區域，被疊合成黑點的機率大於白點區域，才能在疊合影像上顯示出機密影像的黑白輪廓，而矩陣 C_0 和 C_1 就是用來控制疊合影像上的黑白色差。在疊合影像上某一個像素可能是由偽裝影像上的黑點或白點所疊合而成，因此在疊合較少張分享影像時，機密影像上某些由分享影像的白色區域所疊合而成的黑色區域，出現黑點的比例，可能會低於某些由分享影像的黑色區域所疊合而成的白色區域，因此使得機密影像的輪廓不明顯。但是疊合影像上黑色區域變黑的速率大於白色區域，隨著疊合的分享影像增加，機密影像上的黑色區域被加速變黑，使得機密資訊的輪廓愈來愈清晰，而達到漸進式視覺密碼的要求。無論偽裝影像上的像素內容為何，當疊合所有的分享影像以後，在機密影像的白點部份被疊合出黑點的機率都是 $(n + 1)/2n$，而黑點部分則是出現全黑，所以在疊合影像上不會出現偽裝影像的輪廓。

本研究的分享矩陣設計不僅不會在分享影像或疊合影像上洩漏出任何機密影像或偽裝影像的蛛絲馬跡，可以確保機密資訊的安全性，還在每一張分享影像和疊合後的疊合影像上產生 $(i\text{-}1)/(n + i)$ 與 $(n\text{-}1)/(n + i)$ 的色差對比，可以清楚地呈現出較高品質的偽裝影像與機密影像的內容。

致謝

本論文為中華民國行政院國家科學委員會補助之研究計畫 NSC97-2221-E-032-024 的部份研究成果，謹此致謝。

參考文獻

1. 侯永昌、吳佳鴻，民90，『以彩色明圖為偽裝影像之擴充型視覺密碼 An Extended

Visual Cryptography Scheme for Concealing Color Images』，第五屆資訊管理學術暨警政資訊實務研討會。

2. Ateniese, G., Blundo, C., De Santis, A., and Stinson, D. R. "Extended Schemes for Visual Cryptography," *Theoretical Computer Science* (250) , 2001, pp. 143-161.
3. Chen, S.K. and Lin, J.C. "Fault-tolerant and progressive transmission of images," *Pattern Recognition* (38:12) , 2005, pp. 2466-2471.
4. Fang, W.P. "Friendly progressive visual secret sharing," *Pattern Recognition* (41:4) , 2008, pp. 1410-1414.
5. Fang, W.P. and Lin, J.C. "Progressive viewing and sharing of sensitive images," *Pattern Recognition Image Analysis* (16:4) , 2006, pp. 638-642.
6. Hou, Y.C. "Visual cryptography for color images," *Pattern Recognition* (36:7) , 2003, pp. 1619-1629.
7. Ito, R., Kuwakado, H., and Tanaka, H. "Image Size Invariant Visual Cryptography," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E82-A (10) 1999, pp. 2172-2177.
8. Naor, M. and Shamir, A. "Visual Cryptography," *In Advances in Cryptology-EUROCRYPT '94, LNCS 950, Springer-Verlag*, 1995, pp. 1-12.
9. Shamir, A. "How to share a secret," *Communications of the ACM* (22:11) , 1979, pp. 612-613.
10. Shyu, S.J. "Image encryption by random grids," *Pattern Recognition* (40:3) , 2007, pp. 1014-1031.
11. Thien, C.C. and Lin, J.C. "Secret image sharing," *Computers & Graphics* (26:1) , 2002, pp. 765-770.
12. Tu, S.F. and Hou, Y.C. "Design of visual cryptographic methods with smooth-looking decoded images of invariant size for gray level images," *Imaging Science Journal* (55:2) , 2007, pp. 90-101.
13. Wang, R. Z. and Shyu, S. J. "Scalable secret image sharing," *Image Communication* (22:4) , 2007, pp. 363-373.
14. Wang, R. Z., Lin, C. F. and Lin, J. C. "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognition* (34:3) , 2001, pp. 671-683.