

## 視覺密碼學分享模型之新設計法<sup>1</sup>

侯永昌<sup>a</sup> 廖欣音<sup>a</sup> 官振宇<sup>b,\*</sup>

<sup>a</sup>淡江大學資訊管理學系 <sup>b</sup>國立中央大學資訊管理學系

### 摘要

有別於傳統密碼學 (cryptography)，視覺密碼學 (visual cryptography) 是由 Naor 和 Shamir (1995) 所提出的一項與影像分享相關的加解密技術。此項技術結合密碼學與資訊分享的概念，將機密影像經加密為  $n$  張雜亂無章 (noise-like) 的分享影像 (share)，並且將分享影像分配給  $n$  個參與者，每人一張。視覺密碼學主要的精神在於解密時，毋需倚賴任何複雜的數學計算以及大量的電腦運算能力，亦不需任何密碼學知識，僅需將  $k$  張或  $k$  張以上的分享影像重疊，並利用人類視覺系統即可辨識、解碼，重建出原始影像，進而取得所需的機密訊息。

本研究是透過藏密學 (steganography) 的技術，將一張機密影像嵌入到兩張分享影像中。在分享影像上所看到的內容是偽裝影像的資訊，無法直接辨識出機密影像。當分享影像疊合時，將會凸顯出機密影像的內容，而偽裝影像反而會隨著疊合而消失。在實做上，本研究針對  $2 \times 2$  的擴展模型提出四個類型、16 種不同的分享新模型。並且無論在分享影像或疊合影像上，都能夠產生出 25% 或 50% 的黑白色差，因此可以輕易且清楚地辨別出偽裝影像或機密影像的內容。最後，本研究的分享模型的概念簡明且容易實作，使用者可以根據需求來調整影像的黑白色差，以及藏入偽裝影像與機密影像的位置。而在  $(4, 2) / (4, 2)$  分享模型中，分享影像和疊合影像的黑白色差皆為 50%，這個結果優於其他學者的研究成果。

關鍵詞：秘密分享、視覺密碼學、藏密學

<sup>1</sup> 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，並竭誠感謝 M. C. Liao 於論文初稿期間提供寶貴意見，使得本論文更臻完美，謹此致謝。

\* 通訊作者

電子郵件：984403005@cc.ncu.edu.tw



# New Designs for Visual Secret Sharing

Yaung-Chang Hou<sup>a</sup> Hsin-Yin Liao<sup>a</sup> Zen-Yu Quan<sup>b</sup>

<sup>a</sup> Department of Information Management, Tamkang University

<sup>b</sup> Department of Information Management, National Central University

## Abstract

Visual secret sharing (VSS) is a kind of image cryptography, proposed by Naor and Shamir (1995), which integrating the concepts of the cryptography and the information sharing. It encodes a secret image into  $n$  pieces of noise-like shares and dispatches these shares to the corresponding participants. The main advantages of VC is that it no longer needs complicated computation and specialized knowledge to decrypt the secret, the hidden message will be revealed by naked eyes after superimposing  $k$  or more than  $k$  pieces of shares.

In this paper, we embedded two camouflage images into shares according to the theory of steganography, each share's profile is meaningful and it has no way to reveal secret. Besides, the outline of stacked image will be the secret content and the camouflage images were disappeared along with it. In practice, we proposed four approaches (16 models) to implement it. On the other hand, the black-white contrast of shares and stacked image is either 25% or 50%, that's means that the camouflage images and secret image is easy to recognition. Lastly, our proposed models are easy to implement, and the contrast and embedded location can be adjust according to users need; moreover, both the contrasts of shares and stacked image are better than other researches in the  $(4, 2)/(4, 2)$  model.

*Key Words: Secret Sharing, Visual Cryptography, Steganography*

## 1. 前言

隨著資訊科技的蓬勃發展，電腦之使用已相當普遍，網際網路更成為生活中不可或缺的一部份。透過網際網路來進行文字、影像、音訊和影片等數位內容（digital content）的分享，或利用網路相簿、部落格來紀錄生活點滴及分享經驗等行為，業已成為數位化時代中一項重要的活動。資訊科技為人類帶來便利的數位環境，但同時也對網路安全、資訊安全、個人隱私、智慧財產權、…等相關議題造成重大的衝擊。數位內容在網路上分享、傳遞的過程中，容易遭受駭客攻擊、擷取或未經授權者的複製、盜取。因此，如何利用相關技術來保護數位內容，藉此提升數位資料於網際網路上傳輸



的安全性，已經成為現今最重要的研究課題之一，其中以密碼學（cryptography）與藏密學（steganography）為兩個研究主軸。

密碼學是一種運用金鑰（key）機制的加解密演算法，可以分為「對稱式」、「非對稱式」與「混合式」三種方法。對稱式演算法是傳送方利用秘密金鑰（secret key），將明文（plaintext）透過加密動作轉換成密文（ciphertext），然後將密文傳輸至接收方，而接收方收到後再以相同的秘密金鑰進行解密動作。雖然對稱式演算法具有較佳的運算效率，不過這個機制卻有傳送與管理秘密金鑰的問題。非對稱式演算法則是通訊雙方各自持有一對加解密的私鑰（secret key）與公鑰（public key），以公鑰（私鑰）加密的資訊只能用對應的私鑰（公鑰）解密，這樣不僅可以達成秘密通訊與身分驗證的目的，也解決了秘密金鑰傳送與管理的問題。不過非對稱演算法會產生運算效率不彰的問題，於是延伸出同時採用這兩種密碼機制的混合式加解密演算法。混合式的做法是傳送方先以對稱式密碼機制來加密訊息（速度快），然後再利用接收方的公鑰，將對稱式密碼機制所需要的秘密金鑰做加密（秘密金鑰在完成訊息交換後就丟棄，避免金鑰管理的問題），這個動作有一點像將金鑰放入信封中，使他人無法窺伺（這個技術也稱為數位信封，digital envelope），接收方再以自己的私鑰解密，就可以得到這一次的秘密金鑰，解開機密訊息（Diffie and Hellman, 1976; Bellare and Rogaway, 1995; Cramer and Shoup, 1998; Fujisaki and Okamoto, 1999）。由於加解密過程需透過大量且複雜的數學運算，除非破解者取得金鑰，否則在時間及資源有限的狀況下，破解者幾乎不可能破解密文，將它還原成原始資料，因此加密動作可達到保護機密資訊的目的。但是密碼學在加密、解密過程中皆需仰賴電腦的協助，且需經歷複雜的數學運算，耗費大量的時間成本方可完成，對使用者也會造成某種程度的不便。

藏密學是另一種機密資訊傳輸的技術，這個機制也是透過機密金鑰來加密資訊，不過它的加密技術是將機密資訊嵌入文字或圖形等有意義的偽裝物件中，再將這一份偽裝物件傳送給接收方。當接收方收到這份訊息後，就如同密碼學的解密方法，必須再透過對應的解密金鑰來還原機密資訊，否則將無法得知機密資訊的內容。由於偽裝物件的外觀是有意義的內容，使得機密資訊在傳輸的過程不易被他人發覺，因此達成機密資訊傳輸的安全性。

傳統的密碼學或藏密學都是將加解密的資訊（密文和金鑰）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（Shamir, 1979; Thien and Lin, 2002; Wang and Shyu, 2007）。機密分享的概念是將重要的機密資訊分給  $n$  個參與者，每一個參與者都擁有一部份的資訊，但是這個分享內容是經過加密處理過後雜亂無章的內容，所以單一參與者亦無法解讀出機密資訊之原貌。當要還原機密資訊時，假如有  $k$  位或超過  $k$  ( $k \leq n$ ) 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，藉此達到多人共享、風險分散與



提升安全性等目的。

視覺密碼學 (visual cryptography) 是由學者 Naor 和 Shamir (1995) 所提出的一項與影像分享相關的加解密技術。此項技術結合傳統密碼學與資訊分享的概念，將機密影像經加密後得到  $n$  張分享影像 (share)，每一位參與者所拿到的是一張雜亂無章 (noise-like) 且無法顯現出任何原始影像資訊的分享影像，因此又稱之為視覺秘密分享 (visual secret sharing, VSS)。視覺秘密分享主要精神在於解密時，毋需倚賴任何複雜的數學計算，亦不需任何密碼學知識，僅需將  $k$  張分享影像重疊，並利用人類視覺系統即可以肉眼辨識和解譯，重建出原始影像，進而取得所需的機密訊息。

雜訊式的分享影像雖然可以防止機密內容的外洩，但若在傳輸過程中遭有心人士擷取，容易引起擷取者懷疑其中藏有隱密的資訊，而提升嘗試破解的機率，因此產生有意義分享影像 (meaningful shares) 的概念。此概念主要是將機密影像隱藏在另一張偽裝影像中，縱使分享影像在傳輸過程中被擷取，較不易引起擷取者的疑心，以及降低嘗試破解的機率，因此可以提供另外一層的安全保障。另外，當使用者擁有多個機密的多張分享影像時，有意義的分享影像能為使用者在管理及使用的層面上帶來更大的便利，不會產生難以分辨和管理上的困擾。

本研究著重於有意義的視覺秘密分享，將機密影像嵌入兩張偽裝的分享影像中，在分享影像上所看到的內容是偽裝影像資訊，人類的肉眼無法直接辨識出機密影像的資訊。當分享影像疊合時，將會凸顯出機密影像的內容，而分享影像的資訊會隨疊合而消失。在下面章節中，第二章將簡單說明視覺密碼學與擴充型視覺密碼學的相關研究，第三章說明本研究所提出的四種有意義分享影像的視覺密碼學模型，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。

## 2. 文獻探討

### 2.1 視覺密碼學的基本原理

有別於傳統密碼學於加解密時需透過複雜且大量的電腦運算方可完成，視覺密碼學是結合傳統密碼學與資訊分享的概念，將機密影像經加密後得到多張雜亂無章的分享投影片，並將這些分享投影片分給對應的參與者。視覺密碼學的優點是解密過程中，毋需倚賴任何複雜的電腦運算與專業的密碼學知識，僅需將  $k$  張以上的分享影像重疊在一起，再透過肉眼即可解譯機密資訊。

在進行機密影像加密前，首先需要設計出兩個  $n \times m$  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 2 倍為例，機密影像

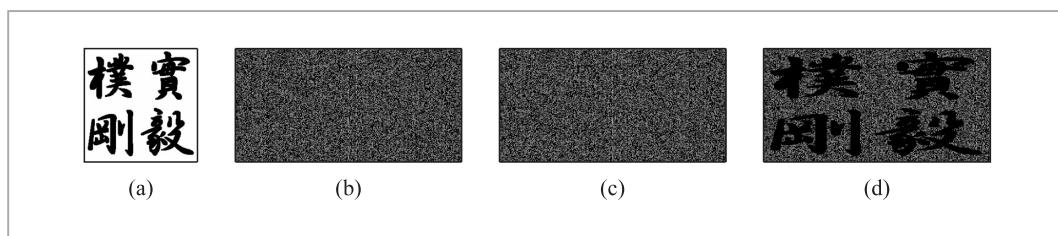




上的每一個像素點會被擴展為兩個由一白一黑所組成的影像區塊，這個分享模型稱之為(2, 2)-threshold 門檻機制（如表 1 所示）。在機密影像中表示白點的部分，兩張分享影像上所分配到的黑點與白點的位置相同，因此重疊分享影像後仍是呈現一黑一白的樣式（如表 1 的左半部）。反觀黑點的部分，兩張分享影像內上所分配到的黑點與白點位置相反，於是疊合影像上會呈現出全黑的樣式（如表 1 的右半部），因此在疊合影像上會產生 50% 的黑白色差。以圖 1 為例，將一張淡江大學的校訓當成機密影像（圖 1(a)），製作成兩張視覺密碼學的投影片（圖 1(b)、(c)），當重疊兩張投影片即可還原淡江校訓（圖 1(d)）。

▼ 表 1 (2, 2)-threshold 擴展型視覺密碼學分享模型

機密影像	分享影像 1	分享影像 2	疊合結果	機密影像	分享影像 1	分享影像 2	疊合結果



▲ 圖 1 視覺密碼學的分解與疊合

## 2.2 擴充型視覺密碼學

傳統視覺密碼學所產生的分享影像是雜訊式內容，這樣雖然可以防止機密內容外洩，不過卻也會引起有心人士的注意與擷取，因而提升攔截者嘗試破解機密資訊的機率。為了解決這個缺點，Ateniese et al. (2001) 應用藏密學概念來設計出一個新分享模型，使得「分享影像」與「疊合影像」都能夠藉由黑白色差，產生出足以讓人類視覺系統直接辨識的影像內容，而這個分享模型稱之為擴充型視覺密碼學（Extended Schemes for Visual Cryptography）。由於分享影像從雜訊式內容轉換為有意義的偽裝圖像，因此即使機密資訊在傳輸過程中遭到有心人士的截取，也會因為分享影像是有意義的圖像，而比較不容易引起截取者的疑心，於是在安全性上提供了另一層的保護。此外，如果參與者參與了多項機密資訊的分享，有意義的分享影像也讓參與者更容易管理大量的分享影像。



Ateniese et al. (2001) 所提出的擴充型視覺密碼學，是將機密影像上的每一個像素點擴展成一個大小為  $2 \times 2$  的區塊，並根據表 2 的分配規則來進行編碼。在這一個分享模型中，偽裝影像中的黑點是以 3 黑 1 白（75% 黑）的區塊來表達，而白點則是被表示為 2 黑 2 白（50% 黑）的區塊。因此，在任何一張分享影像上，偽裝影像的黑色區域與白色區域有 25% 的黑白色差。另外，針對重疊後的結果而言，若機密影像像素為白點，在疊合影像上會被疊合為 3 黑 1 白（75% 黑）的區塊；若機密影像像素為黑點，則是被疊合為 4 黑（100% 黑）的區塊，因此疊合影像上的機密內容也會有 25% 的黑白色差。

▼ 表 2 Ateniese et al. (2001) 所提出的編碼模型

機密影像	偽裝影像 1	偽裝影像 2	分享影像 1	分享影像 2	疊合結果	機密影像	偽裝影像 1	偽裝影像 2	分享影像 1	分享影像 2	疊合結果
□ 白	白	白			 黑色佔 75%	■ 黑	白	白			 黑色佔 100%
	白	黑					白	黑			
	黑	白					黑	白			
	黑	黑					黑	黑			

當機密像素為白點時，依照兩張偽裝影像上的像素顏色，由模型的左半部中取出合適的組合；而機密影像像素為黑點時，則是由模型的右半部中取出合適的組合。當機密影像中的所有像素皆處理完畢後，就可以產生偽裝分享影像 1（圖 2(a)）及偽裝分享影像 2（圖 2(b)）。雖然利用人類視覺系統即可以辨識出偽裝影像和機密影像的內容，但是比起傳統視覺密碼學有 50% 的黑白色差（圖 1），25% 的黑白色差（圖 2）是比較差的。



▲ 圖 2 擴充型視覺密碼學的實驗結果



### 2.3 視覺密碼學的相關研究

視覺密碼學的研究起源於機密分享的議題，如果所有的機密資訊都交由一人所掌管，一旦他心懷不軌，機密資訊就沒有任何安全性可言。因此視覺密碼學將機密影像分解成多張分享影像，讓每一個參與者都分別持有一張分享影像，一定要有  $k$  位或超過  $k$  ( $k \leq n$ ) 位的參與者共同參與，才可解譯機密資訊，否則就無法進行解密。藉此可以達到多人共享、風險分散與提升安全性等目的。

在 Naor and Shamir (1995) 提出了視覺密碼學的模型後，陸續有很多學者針對這個模型提出進一步的修正建議。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 et al. (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 and Hou (2007) 則提出多點同時加密的方式，來解決 Ito et al. (1999) 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。

Naor and Shamir (1995) 只有提出了黑點與白點的分解規則，對於具有多色階的灰階或彩色影像卻束手無策，使得視覺密碼學的研究在 2000 年以前一直只侷限於黑白影像，而無法應用在現今豐富多彩的多媒體世界，因而降低了視覺密碼學的應用領域。半色調 (halftoning) 是一種模擬連續調影像的技術，它是透過不同大小與疏密的黑 (白) 點的排列，使得只需要黑點或白點兩種顏色，就能表現出灰階影像的色彩濃淡變化。當機密影像為彩色影像時，透過色彩分解與合成技術，可以將彩色影像分解為 3 個單色的灰階影像；每一個灰階影像再透過半色調技術，轉換成不同疏密程度的黑白影像，使得視覺密碼學的應用得以進入灰階與彩色機密影像的領域 (e.g., Hou et al., 2001; Hou, 2003; Shyu, 2006)。而侯永昌與吳佳鴻 (2001) 利用色彩分解、合成與半色調技術，將 Ateniese et al. (2001) 的擴充型分享模型延伸至有色階變化的機密影像。

傳統視覺密碼學是一種非有即無 (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，因此衍生出漸進式 (progressive) 視覺密碼學的研究 (Fang and Lin, 2006; Fang, 2008)。不過他們所產生的分享影像大小都是機密影像的  $2 \times 2$  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。為了改善這些問題，Hou and Quan (2011)，以及侯永昌與官振宇 (2010) 分別提出了「雜訊式分享影像」與「有意義分享影像」的研究，並且在分享影像的大小、安全性與疊合影像品質等衡量指標上，都優於 Fang (2006; 2008) 所提出的模型。



由於視覺密碼學具有安全性佳和解密容易的優點，因此可以應用於電子商務流程中關於資訊安全的部份。例如：應用視覺密碼學的概念於視覺訊息驗證與視覺身分識別等應用（e.g., Naor and Pinkas, 1997; Hu and Tzeng, 2007）。此外，如果可以從我們所擁有的智慧資產中產生一張分享影像，配合我們手中當成身分認證的另外一張分享影像，只要這兩張分享影像疊合後，能夠顯現出我們所需要的數位浮水印，就可以達成驗證智慧財產權的目的（e.g., Hou and Chen, 2000; Hsu and Hou, 2005）。

### 3. 有意義分享影像之視覺密碼學

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，但是卻可能會引發其中藏有機密資訊的聯想，因而增加攔截者嘗試破解的可能性。反之，當分享影像轉變為有意義的偽裝影像時，將可以提供雙重的安全保護。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學本身的機制，使得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。

因此本研究採用有意義分享影像之視覺密碼學的作法，將一張偽裝影像嵌入兩張分享影像中，在分享影像上所看到的內容是偽裝影像資訊，看不到機密影像的資訊。反之，當分享影像疊合時會凸顯出機密影像的內容，而分享影像的資訊會隨疊合而消失。主要的核心概念是將分享影像奇數區塊的像素值交由「偽裝影像」上對應的像素來決定，而偶數區塊的像素值則交由「機密影像」的像素決定。換句話說，是在分享影像的奇數區塊藏入了有關「偽裝影像」的資訊，而在偶數區塊則藏入「機密影像」的資訊。

在分享影像上需顯示「偽裝影像」的資訊，所以在分享影像上對應偽裝影像的像素區塊中出現黑點、白點的機率會有所不同，藉以產生足夠的明暗色差之對比。但是在疊合結果上不能顯示出偽裝影像的資訊，因此在疊合影像上的奇數像素區塊需是呈現相同的黑點／白點的比例，以避免出現偽裝影像的資訊，干擾到機密影像的呈現。在分享影像上，由於不能顯示「機密影像」的資訊，所以對應機密影像像素區塊的黑點／白點的比例必需一樣，不能在像素區塊間產生黑白色差，才不致於在分享影像中透露出任何與機密影像相關之蛛絲馬跡；而這部份的疊合結果反而需呈現明顯之黑白色差，方能凸顯機密影像的內容。

我們採用將每一個像素擴展為  $2 \times 2$  區塊的做法，因此在分享影像上，每一個區塊中可以有 0~4 個黑點或白點，他們的分配方式和對應的編碼如表 3 所示。為了後續說明的方便性，我們將影像區塊依其出現之黑點數分為 5 個子集合，其中， $X_0 = \{0\}$ ， $X_1 = \{1, 2, 4, 8\}$ ， $X_2 = \{3, 5, 6, 9, 10, 12\}$ ， $X_3 = \{7, 11, 13, 14\}$ ， $X_4 = \{15\}$ 。



▼ 表 3 影像區塊中黑點之分配方式和對應編碼表

區塊 內容	二進位 編碼	十進位 編碼	區塊 內容	二進位 編碼	十進位 編碼	區塊 內容	二進位 編碼	十進位 編碼	區塊 內容	二進位 編碼	十進位 編碼
	0000	0		1000	8		1001	9		1011	11
	0001	1		0011	3		1010	10		1101	13
	0010	2		0101	5		1100	12		1110	14
	0100	4		0110	6		0111	7		1111	15

為了在分享影像上顯示「偽裝影像」的資訊，所以只要能在分享影像上對應偽裝影像的黑色像素區塊中出現黑點的機率比較高、對應白色像素區塊中出現黑點的機率比較低的設計，都足以產生足夠的明暗色差之對比，顯示出「偽裝影像」的資訊。因此以  $2 \times 2$  的擴展區塊而言，擴展區塊中出現黑點個數分別為  $(2, 1)$ 、 $(3, 2)$ 、 $(4, 3)$  或  $(4, 2)$  都可以用來代表分享影像中的黑色區塊或白色區塊。不同排列方式的分享區塊疊合後，又可以在疊合影像上排列出不同黑白分配組合。因此，我們根據排列組合結果而提出四個類型、16 種不同的分享新模型。

### 3.1 類型 A： $(3, 2) / (4, 3)$ 模型

在分享影像上的影像區塊中，我們以出現 3 個黑點來代表偽裝影像上的黑色，出現 2 個黑點來代表偽裝影像上的白色，以產生 25% 的黑白色差；而在疊合影像上我們以出現 4 個黑點來代表機密影像上的黑色，出現 3 個黑點來代表機密影像上的白色，這樣可以產生 25% 的黑白色差。我們簡稱這個作法為  $(3, 2) / (4, 3)$  模型（表 4）。

(1) 當分享影像所要決定的像素區塊為奇數時，區塊內的像素值是由偽裝影像上的像素值來決定。

- ① 當兩張偽裝影像的像素值均為黑色時：隨機於  $X_3$  中任選一個編號  $S_1$ ，作為分享影像 1 和分享影像 2 的像素區塊組合，此時兩個分享區塊內的黑白分布相同，黑色佔像素區塊的比率為 75%。
- ② 當兩張偽裝影像的像素值均為白色時：隨機於  $X_2$  中任選兩個編號  $S_1$  和  $S_2$ ，分別作為分享影像 1 與分享影像 2 的像素區塊組合，使得兩者之區塊組合不能相同，且  $S_2 \neq 15 - S_1$ 。此時，兩個分享區塊內黑色分布的比率都是 50%。
- ③ 當兩張偽裝影像上的像素為一黑一白時：對應黑色像素的分享區塊 ( $S_b$ ) 由  $X_3$  中選擇其一，而對應白色像素的分享區塊 ( $S_w$ ) 則由  $X_2$  中選擇，但是  $S_w$  中的黑點必須與  $S_b$  中的黑點重疊，也就是  $S_b \text{ OR } S_w = S_b$ 。此時， $S_b$  中黑色的比率為 75%，而  $S_w$  中的比率為 50%。





(3, 2) / (4, 3) 模型的設計對於單一的像素區塊而言，分享影像上代表偽裝影像的黑色部份確實比較黑（75% 的黑），而白色部份比較白（50% 的黑），因此有了黑白顏色的差異，使得整張分享影像會呈現出偽裝影像的輪廓。而這部份的疊合結果皆屬於  $X_3$  中的某一種形態，使得無論偽裝像素點為黑或白，在疊合後的像素區塊中皆呈現 75% 的黑。因此，在這部份的疊合結果中無法顯示出偽裝影像的輪廓。

(2) 當分享影像所要決定的像素區塊為偶數時，區塊內的像素值是由機密影像上的像素值來決定。

- ① 當機密影像的像素值為黑色時：隨機於  $X_2$  中任選一個編號  $S_1$ ，作為分享影像 1 的像素區塊組合，而分享影像 2 的像素區塊組合  $S_2$  與分享影像 1 互補，也就是  $S_2 = 15 - S_1$ 。此時，兩個分享區塊內黑色分布的比率也是 50%。
- ② 當機密影像的像素值為白色時：隨機於  $X_2$  中任選兩個編號  $S_1$  和  $S_2$ ，分別作為分享影像 1 與分享影像 2 的像素區塊組合，使得兩者之區塊組合不相同，且  $S_2 \neq 15 - S_1$ 。此時，兩個分享區塊內黑色分布的比率都是 50%。

▼ 表 4 (3, 2) / (4, 3) 模型的編碼

偽裝影像 1	偽裝影像 2	分享影像 1	分享影像 2	疊合結果	機密影像	分享影像 1	分享影像 2	疊合結果
■	■	$S_1 \in X_3$	$S_2 = S_1$	$(S_1 \text{ OR } S_2) \in X_3$	■	$S_1 \in X_2$	$S_2 = 15 - S_1$	$(S_1 \text{ OR } S_2) \in X_4$
■	□	$S_1 \in X_3$	$S_2 \in X_2,$ $(S_1 \text{ OR } S_2) = S_1$	$(S_1 \text{ OR } S_2) \in X_3$				
□	■	$S_1 \in X_2$	$S_2 \in X_3,$ $(S_1 \text{ OR } S_2) = S_2$	$(S_1 \text{ OR } S_2) \in X_3$	□	$S_1 \in X_2$	$S_2 \in X_2,$ $S_2 \neq S_1,$ $S_2 \neq 15 - S_1$	$(S_1 \text{ OR } S_2) \in X_3$
□	□	$S_1 \in X_2$	$S_2 \in X_2,$ $S_2 \neq S_1,$ $S_2 \neq 15 - S_1$	$(S_1 \text{ OR } S_2) \in X_3$				

(3, 2) / (4, 3) 模型的設計對於單一的像素區塊而言，不管機密像素點為黑色或白色，在分享影像上的像素區塊中皆呈現半黑半白的狀態（50% 的黑），因此在分享影像中無法透露出與機密影像相關的資訊。但是在疊合後，當機密像素點為黑色時，在疊合區塊中會比較黑（100% 的黑）；反之，當機密像素點為白色時，在疊合區塊中確實比較白（75% 的黑），因此會產生機密影像的輪廓，顯示出與機密影像相關的資訊。

(3, 2) / (4, 3) 模型在分享影像上是以出現 3 個黑點來代表偽裝影像上的黑色，2 個黑點來代表偽裝影像上的白色；在疊合影像上則是以出現 4 個黑點和 3 個黑點，分別代表機密影像上的黑色與白色。這個做法無論在分享影像或疊



合影像的影像區塊中，顏色的分布都與 Ateniese et al. 的擴充型視覺密碼學作法相同，只能在分享影像和疊合影像上產生 25% 的黑白色差，因此是屬於比較差的設計法。此外，同樣可以產生 25% 黑白色差的設計法還有  $(2, 1) / (2, 1)$  模型、 $(2, 1) / (3, 2)$  模型、 $(2, 1) / (4, 3)$  模型、 $(3, 2) / (2, 1)$  模型、 $(3, 2) / (3, 2)$  模型、 $(4, 3) / (2, 1)$  模型、 $(4, 3) / (3, 2)$  模型和  $(4, 3) / (4, 3)$  模型等八種設計法，有興趣的讀者可以自行嘗試推導它的編碼方式。不過這九個設計法所產生的視覺效果，都比不上後面三個類型的分享法。

### 3.2 類型 B： $(2, 1) / (4, 2)$ 模型

在分享影像上的影像區塊中，我們以出現 2 個黑點來代表偽裝影像上的黑色，出現 1 個黑點來代表偽裝影像上的白色，以產生 25% 的黑白色差；而在疊合影像上我們以出現 4 個黑點來代表機密影像上的黑色，出現 2 個黑點來代表機密影像上的白色，這樣可以產生 50% 的黑白色差。我們簡稱這個作法為  $(2, 1) / (4, 2)$  模型（表 5）。

(1) 當分享影像所要決定的像素區塊為奇數時，區塊內的像素值是由偽裝影像上的像素值來決定。

- ① 當兩張偽裝影像的像素值均為黑色時：隨機於  $X_2$  中任選一個編號  $S_1$ ，作為分享影像 1 和分享影像 2 的像素區塊組合，此時兩個分享區塊內的黑白分布相同，黑色佔像素區塊的比率為 50%。
- ② 當兩張偽裝影像的像素值均為白色時：隨機於  $X_1$  中任選兩個編號  $S_1$  和  $S_2$ ，分別作為分享影像 1 與分享影像 2 的像素區塊組合，使得兩者之區塊組合不能相同，黑色佔像素區塊的比率為 25%。
- ③ 當兩張偽裝影像上的像素為一黑一白時：對應黑色像素的分享區塊 ( $S_b$ ) 由  $X_2$  中選擇其一，而對應白色像素的分享區塊 ( $S_w$ ) 則由  $X_1$  中選擇，但是  $S_w$  中的黑點必須與  $S_b$  中的黑點重疊，也就是  $S_b \text{ OR } S_w = S_b$ 。此時， $S_b$  中黑色的比率為 50%，而  $S_w$  中的比率為 25%。

$(2, 1) / (4, 2)$  模型的設計對於單一的像素區塊而言，分享影像上代表偽裝影像的黑色部份確實比較黑（50% 的黑），而白色部份比較白（25% 的黑），因此有了黑白顏色的差異，使得整張分享影像會呈現出偽裝影像的輪廓。而這部份的疊合結果皆屬於  $X_2$  中的某一種形態，使得無論偽裝像素點為黑或白，在疊合後的像素區塊中皆呈現半黑半白的狀態（50% 的黑）。因此，在這部份的疊合結果中無法顯示出偽裝影像的輪廓。

(2) 當分享影像所要決定的像素區塊為偶數時，區塊內的像素值是由機密影像上的像素值來決定。



- ①當機密影像的像素值為黑色時：隨機於  $X_2$  中任選一個編號  $S_1$ ，作為分享影像 1 的像素區塊組合，而分享影像 2 的像素區塊組合與分享影像 1 互補，也就是  $S_2 = 15 - S_1$ 。此時，兩個分享區塊內黑色分布的比率也是 50%。
- ②當機密影像的像素值為白色時：隨機於  $X_2$  中任選一個編號  $S_1$ ，作為分享影像 1 和分享影像 2 的像素區塊組合，此時兩個分享區塊內的黑白分布相同，黑色佔像素區塊的比率為 50%。

(2, 1) / (4, 2) 模型的設計對於單一的像素區塊而言，不管機密像素點為黑色或白色，在分享影像上的像素區塊中皆呈現半黑半白的狀態（50% 的黑），因此在分享影像中無法透露出與機密影像相關的資訊。但是在疊合後，當機密像素點為黑色時，在疊合區塊中會比較黑（100% 的黑）；反之，當機密像素點為白色時，在疊合區塊中確實比較白（50% 的黑），因此會產生機密影像的輪廓，顯示出與機密影像相關的資訊。其他類似的設計還有 (3, 2) / (4, 2) 模型和 (4, 3) / (4, 2) 模型，也是可以在分享影像上產生 25% 的黑白色差，在疊合影像上產生 50% 的黑白色差設計，有興趣的讀者可以自行嘗試推導它的編碼方式。

▼ 表 5 (2, 1) / (4, 2) 模型的編碼

偽裝影像 1	偽裝影像 2	分享影像 1	分享影像 2	疊合結果	機密影像	分享影像 1	分享影像 2	疊合結果
■	■	$S_1 \in X_2$	$S_2 = S_1$	$(S_1 \text{ OR } S_2) \in X_2$	■	$S_1 \in X_2$	$S_2 = 15 - S_1$	$(S_1 \text{ OR } S_2) \in X_4$
■	□	$S_1 \in X_2$	$S_2 \in X_1,$ $(S_1 \text{ OR } S_2) = S_1$	$(S_1 \text{ OR } S_2) \in X_2$				
□	■	$S_1 \in X_1$	$S_2 \in X_2,$ $(S_1 \text{ OR } S_2) = S_2$	$(S_1 \text{ OR } S_2) \in X_2$	□	$S_1 \in X_2$	$S_2 = S_1$	$(S_1 \text{ OR } S_2) \in X_2$
□	□	$S_1 \in X_1$	$S_2 \in X_1,$ $S_2 \neq S_1$	$(S_1 \text{ OR } S_2) \in X_2$				

### 3.3 類型 C：(4, 2) / (4, 3) 模型

在分享影像上的影像區塊中，我們以出現 4 個黑點來代表偽裝影像上的黑色，出現 2 個黑點來代表偽裝影像上的白色，以產生 50% 的黑白色差；而在疊合影像上我們以 4 個黑點來代表機密影像上的黑色，3 個黑點來代表機密影像上的白色，這樣可以產生 25% 的黑白色差。我們簡稱這個作法為 (4, 2) / (4, 3) 模型（表 6）。

- (1)當分享影像所要決定的像素區塊為奇數時，區塊內的像素值是由偽裝影像上的像素值來決定。



- ①當兩張偽裝影像的像素值均為黑色時：選擇編號 15 作為分享影像 1 和分享影像 2 的像素區塊組合，也就是  $S_1 = S_2 = 15$ 。此時，兩個像素區塊均為全黑。
- ②當兩張偽裝影像的像素值均為白色時：隨機於  $X_2$  中任選一個編號  $S_1$ ，作為分享影像 1 的像素區塊組合，而分享影像 2 的像素區塊組合與分享影像 1 互補，也就是  $S_2 = 15 - S_1$ 。此時，兩個分享區塊內黑色分布的比率也是 50%。
- ③當兩張偽裝影像上的像素為一黑一白時：對應黑色像素的分享區塊 ( $S_b$ ) 為全黑，而對應白色像素的分享區塊 ( $S_w$ ) 則由  $X_2$  中選擇。此時， $S_b$  中黑色的比率為 100%，而  $S_w$  中的比率為 50%。

(4, 2) / (4, 3) 模型的設計對於單一的像素區塊而言，分享影像上代表偽裝影像的黑色部份確實比較黑 (100% 的黑)，而白色部份比較白 (50% 的黑)，因此有了黑白顏色的差異，使得整張分享影像會呈現出偽裝影像的輪廓。而這部份的疊合結果皆屬於全黑的形態，使得無論偽裝像素點為黑或白，在疊合後的像素區塊中皆呈現 100% 的黑。因此，在這部份的疊合結果中無法顯示出偽裝影像的輪廓。

- (2)當分享影像所要決定的像素區塊為偶數時，區塊內的像素值是由機密影像上的像素值來決定。它的產生方式是採用 (4, 3) 模式，因此它與 (3, 2) / (4, 3) 模型中針對偶數像素區塊的操作方式是相同的，因此我們就不再說明它顏色分派的方式，請自行參考 (3, 2) / (4, 3) 模型中的說明。

其他類似的設計還有 (4, 2) / (2, 1) 模型和 (4, 2) / (3, 2) 模型，也是可以在分享影像上產生 50% 的黑白色差，在疊合影像上產生 25% 的黑白色差設計，有興趣的讀者可以自行嘗試推導它的編碼方式。

▼ 表 6 (4, 2) / (4, 3) 模型的編碼

偽裝影像 1	偽裝影像 2	分享影像 1	分享影像 2	疊合結果	機密影像	分享影像 1	分享影像 2	疊合結果
■	■	$S_1 \in X_4$	$S_2 = S_1$	$(S_1 \text{ OR } S_2) \in X_4$	■	$S_1 \in X_2$	$S_2 = 15 - S_1$	$(S_1 \text{ OR } S_2) \in X_4$
■	□	$S_1 \in X_4$	$S_2 \in X_2$	$(S_1 \text{ OR } S_2) \in X_4$				
□	■	$S_1 \in X_2$	$S_2 \in X_4$	$(S_1 \text{ OR } S_2) \in X_4$	□	$S_1 \in X_2$	$S_2 \in X_2,$ $S_2 \neq S_1,$ $S_2 \neq 15 - S_1$	$(S_1 \text{ OR } S_2) \in X_3$
□	□	$S_1 \in X_2$	$S_2 = 15 - S_1$	$(S_1 \text{ OR } S_2) \in X_4$				

### 3.4 類型 D：(4, 2) / (4, 2) 模型

在這個模型中，不論是在分享影像或疊合影像上的影像區塊中，我們都以出現 4 個黑點來代表黑色，出現 2 個黑點來代表白色，這樣可以產生 50% 的黑白色差。我們



簡稱這個作法為  $(4, 2) / (4, 2)$  模型 (表 7)。

- (1) 當分享影像所要決定的像素區塊為奇數時，區塊內的像素值是由偽裝影像上的像素值來決定。它的產生方式是採用  $(4, 2)$  模式，因此它與  $(4, 2) / (4, 3)$  模型中針對奇數像素區塊的操作方式是相同的，因此我們就不再說明它顏色分派的方式，請自行參考  $(4, 2) / (4, 3)$  模型中的說明。
- (2) 當分享影像所要決定的像素區塊為偶數時，區塊內的像素值是由機密影像上的像素值來決定。它的產生方式是採用  $(4, 2)$  模式，因此它與  $(2, 1) / (4, 2)$  模型中針對偶數像素區塊的操作方式是相同的，因此我們就不再說明它顏色分派的方式，請自行參考  $(2, 1) / (4, 2)$  模型中的說明。

▼ 表 7  $(4, 2) / (4, 2)$  模型的編碼

偽裝影像 1	偽裝影像 2	分享影像 1	分享影像 2	疊合結果	機密影像	分享影像 1	分享影像 2	疊合結果
		$S_1 \in X_4$	$S_2 = S_1$	$(S_1 \text{ OR } S_2) \in X_4$		$S_1 \in X_2$	$S_2 = 15 - S_1$	$(S_1 \text{ OR } S_2) \in X_4$
		$S_1 \in X_4$	$S_2 \in X_2$	$(S_1 \text{ OR } S_2) \in X_4$				
		$S_1 \in X_2$	$S_2 \in X_4$	$(S_1 \text{ OR } S_2) \in X_4$		$S_1 \in X_2$	$S_2 = S_1$	$(S_1 \text{ OR } S_2) \in X_2$
		$S_1 \in X_2$	$S_2 = 15 - S_1$	$(S_1 \text{ OR } S_2) \in X_4$				

祕密分享演算法：

輸入：2 張大小為  $H \times W$  之黑白偽裝影像和 1 張大小為  $H \times W$  之黑白機密影像。

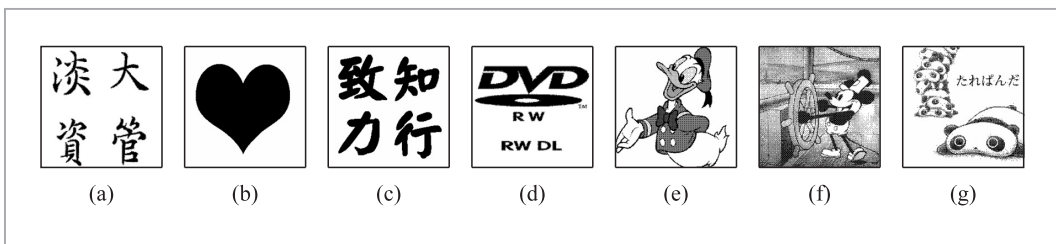
輸出：2 張大小為  $2H \times 2W$  之黑白偽裝分享影像。

- (1) 循序讀取兩張偽裝影像及機密影像上的像素點。
- (2) 依據偽裝影像像素及機密影像像素的像素點內容，執行對應的分享模型。
- (3) 將分享模型中的像素點結果存入兩張分享影像的對應位置上。
- (4) 重覆執行步驟 1~3，直到每一個像素點都被讀取，即可完成分享影像之製作。

#### 4. 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)。在本實驗中，共使用 7 張圖片 (圖 3) 來作為偽裝影像及機密影像之用，其中有 4 張黑白影像 (圖 3(a)~圖 3(d)) 和 3 張經半色調處理後的灰階影像 (圖 3(e)~圖 3(g))，而每張影像大小皆為  $256 \times 256$ 。





▲ 圖 3 實驗用圖

#### 4.1 實驗結果

圖 4~圖 6 分別展示四種類型的實驗結果。在偽裝分享影像上，我們所看到的內容是兩張偽裝影像的資訊，並且無法從任一張分享影像上辨識出機密影像的資訊。當重疊兩張分享影像後，疊合影像上就只能看到機密影像，而偽裝影像的資訊則是會隨之消失，因而不會干擾機密影像的呈現。

	(3, 2) / (4, 3) 模型	(2, 1) / (4, 2) 模型	(4, 2) / (4, 3) 模型	(4, 2) / (4, 2) 模型
偽裝分享影像一				
偽裝分享影像二				
疊合影像				

▲ 圖 4 文字類型實驗結果



	(3, 2) / (4, 3) 模型	(2, 1) / (4, 2) 模型	(4, 2) / (4, 3) 模型	(4, 2) / (4, 2) 模型
偽裝分享影像一				
偽裝分享影像二				
疊合影像				

▲ 圖 5 卡通類型實驗結果

根據圖 4~圖 6 可以發現，當偽裝影像的內容是文字或黑白圖像（圖 4 和圖 5）時，由於這些圖案的結構規律且色塊間區隔明顯，即使分享影像的產生是透過亂數來挑選影像區塊的內容，不過在 (3, 2)、(2, 1) 和 (4, 2) 三個模型的實驗結果，偽裝分享影像都能夠清晰地辨識出偽裝影像的內容。反觀以卡通圖案的灰階影像（圖 6）做為偽裝影像時，色塊間的區別本來就較不明顯，加上亂數挑選區塊內容所帶來的不規則性，使得偽裝分享影像的清晰度較差。此外，無論在偽裝分享影像或機密影像上，挑選高色差值的 (4, 2) 分享模型所得到的影像視覺品質，都會優於低色差值的 (4, 3)、(3, 2) 和 (2, 1) 分享模型所得到的實驗結果。

#### 4.2 分析與討論

視覺密碼學的評比基準在於分享影像的安全性和分享影像與疊合影像的黑白色差。本研究的安全保護機制建立在：





	(3, 2) / (4, 3) 模型	(2, 1) / (4, 2) 模型	(4, 2) / (4, 3) 模型	(4, 2) / (4, 2) 模型
偽裝分享影像一				
偽裝分享影像二				
疊合影像				

▲ 圖 6 灰階影像類型實驗結果

- (1) 藏於分享影像上偶數區塊的機密影像，其黑點與白點出現的機率都相同，都是 2 白 2 黑（參閱表 4 ~ 表 7 的下半部），因此在分享影像中，針對機密影像的黑白色差為 0%，不會露出任何機密影像紋理的。也就是說，當我們看到分享影像上的某一個區塊，發現它是兩個白點兩個黑點時，我們沒有辦法知道它是由機密影像上的黑點所分派出來的，還是由機密影像上的白點所分派出來的。
- (2) 藏於分享影像上奇數區塊的偽裝影像，其黑點與白點出現的機率只與偽裝影像的顏色有關，與機密影像的顏色無關（參閱表 4 ~ 表 7 的上半部）。當偽裝影像是黑點時，分配到的黑點比較多（顯得比較黑）；當偽裝影像是白點時，分配到的黑點比較少（顯得比較白）。因此在分享影像中，可以露出偽裝影像的紋理。因為區塊的顏色分配與機密影像的顏色無關。也就是說，當我們看到分享影像上的某一個區塊，我們是沒有辦法知道它是由機密影像上的黑點所分派出來的，還是由機密影像上的白點所分派出來的。



(3)無論是採用哪一種分享模型，隨機猜測的正確率上限值為 50%，因此要把機密影像上每一個點都猜對的機率趨近於 0 ( $0.5^N$ ，其中  $N$  是機密影像的像素個數)，如此可以達到計算上的安全性 (computational security)。因此，我們可以宣稱本研究所設計的股份模型是安全的。

其次，我們綜合本研究所提出的四種類型和 Ateniese et al. (2001) 的股份模型，將實驗結果整理成表 8。我們可以發現：不論在股份影像上或疊合影像上的黑白色差，本研究都優於 Ateniese et al. (2001) 的做法，並且  $(4, 2) / (4, 2)$  模型是目前已知的最佳結果，使得偽裝影像和機密影像的內容都能夠清楚地為人眼所辨識。

▼ 表 8 Ateniese et al. (2001) 與本研究的黑白色差比較

	分享影像	疊合影像
Ateniese et al.	25%	25%
$(3, 2) / (4, 3)$ 模型	25%	25%
$(2, 1) / (4, 2)$ 模型	25%	50%
$(4, 2) / (4, 3)$ 模型	50%	25%
$(4, 2) / (4, 2)$ 模型	50%	50%

本研究的核心概念是將股份影像的奇數區塊內容，交由「偽裝影像」上對應的像素來決定，而偶數區塊內容則交由「機密影像」的像素決定。藉由這樣的做法，我們就可以在股份影像的奇數區塊中植入了有關「偽裝影像」的資訊，而在偶數區塊中植入「機密影像」的資訊。除了這種做法外，我們也可以利用亂數來隨機指定需要藏入偽裝影像與機密影像的位置，或是調整偽裝資訊與機密資訊的嵌入百分比，藉此調整股份影像（疊合影像）的顯示比例，以及增加作業上的彈性。此外，針對灰階或彩色的偽裝影像與機密影像時，只需要將它們先透過色彩的分解、合成與半色調的技術處理後，就可以直接使用本研究的方法來處理，如同圖 6 的實驗。由於本研究的股份模型都是針對兩張股份影像來設計，因此這就成為本研究的唯一限制。

## 5. 結論

在本研究所提出的四個類型的股份模型中，皆是將有意義的偽裝影像嵌入兩張股份影像中，並且在每一張股份影像上都無法辨識出機密影像的內容。當股份影像重疊後，疊合影像上必須要凸顯出機密影像的內容，而偽裝影像的資訊反而要隨之消失，因此不會干擾機密影像的呈現。

為了在股份影像上顯示「偽裝影像」的資訊，以及不會揭露出機密資訊的內容，



於是在代表偽裝影像的像素區塊需要有黑白色差，而在代表機密影像的像素區塊則是不能有黑白色差。在本研究的設計中，我們設定將偽裝影像嵌入在分享影像上的奇數區塊，並且在對應偽裝影像的黑點與白點的影像區塊上，黑點出現個數分別為 (2, 1)、(3, 2)、(4, 3) 或 (4, 2) 四種組合，使得偽裝影像的黑白色差分別為 25% 或 50%，達成凸顯出偽裝影像的目的。然而，在分享影像上的偶數區塊則是不能洩露出機密影像的紋理，所以其黑點／白點出現的機率需要相同，使得在偶數影像區塊上的黑白色差為 0%。由於無法從分享影像中察覺出任何與機密影像相關之紋理，因此可以確保機密資訊的隱密性，進而達到提升機密影像安全性之目的。

同樣的道理，為了在疊合影像上顯示「機密影像」的資訊，本研究設計在對應機密影像的像素區塊內，疊合影像的黑點出現個數分別為 (2, 1)、(3, 2)、(4, 3) 或 (4, 2) 四種組合，使得機密影像的黑白色差也是 25% 或 50%，因此可以凸顯出機密影像的內容。然而藏於奇數區塊的偽裝影像，疊合後的影像區塊內容都會有相同的黑點個數，使得偽裝影像的黑點與白點之間的色差為 0%，因此無法在疊合影像上顯示出任何與偽裝影像相關的資訊。

本研究具備下列幾項優點：(1)本研究的分享模型的概念簡明且容易實作。(2)在 (4, 2)／(4, 2) 分享模型中，分享影像和疊合影像的黑白色差皆為 50%，這個結果優於其他學者的研究，使得偽裝影像和機密影像的內容能清楚地為人眼所辨識。(3)本研究的分享投影片均為有意義的偽裝影像，因此可以提高分享投影片的安全性，也讓參與者更容易管理大量的分享影像。

## 參考文獻

- 侯永昌、吳佳鴻 (2001)，「以彩色明圖為偽裝影像之擴充型視覺密碼」，《第五屆資訊管理學術暨警政資訊實務研討會論文集》，62-69。
- 侯永昌、官振宇 (2010)，「有意義且不擴展分享影像之漸進式視覺密碼」，《資訊管理學報》，17(3)，131-154。
- Ateniese, G., Blundo, C., De Santis, A., and Stinson, D. R. (2001), "Extended schemes for visual cryptography," *Theoretical Computer Science*, 250, 143-161.
- Bellare, M. and Rogaway P. (1995), "Optimal asymmetric encryption," *Lecture Notes in Computer Science*, 950, 92-111.
- Cramer, R. and Shoup, V. (1998), "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," *Lecture Notes in Computer Science*, 1462, 13-25.





- Diffie, W. and Hellman, M. E. (1976), "New Directions in Cryptography," *IEEE Transactions on Information Theory*, 22(6), 644-654.
- Fang, W. P. and Lin, J.C. (2006), "Progressive viewing and sharing of sensitive images," *Pattern Recognition Image Analysis*, 16(4), 638-642.
- Fang, W. P. (2008), "Friendly progressive visual secret sharing," *Pattern Recognition*, 41(4), 1410-1414.
- Fujisaki, E. and Okamoto, T. (1999), "Secure integration of asymmetric and symmetric encryption schemes," *Lecture Notes in Computer Science*, 1666, 537-554.
- Hou, Y. C. (2003), "Visual cryptography for color images," *Pattern Recognition*, 36(7), 1619-1629.
- Hou, Y. C., Chang, C. Y., and Tu, S. F. (2001), "Visual cryptography for color images based on halftone technology," in *Processing of Systems, Cybernetics and Informatics 2001*, Florida, Orlando, 441-445.
- Hou, Y. C. and Chen, P. M. (2000), "An asymmetric watermarking scheme based on visual cryptography," in *WCCC-ICSP 5th International Conference on Signal Processing Proceedings*, 992-995.
- Hou, Y. C. and Quan Z. Y. (2011), "Progressive visual cryptography with unexpanded shares," *IEEE Transactions on Circuits and Systems for Video Technology* 21(11), 1760-1764.
- Hsu, C. S. and Hou, Y. C. (2005), "Copyright protection scheme for digital images using visual cryptography and sampling methods," *Optical Engineering*, 44(7), 1-10.
- Hu, C. M. and Tzeng, W. G. (2007), "Cheating prevention in visual cryptography," *IEEE Transactions on Image Processing*, 16(1), 36-45.
- Ito, R., Kuwakado, H., and Tanaka, H. (1999), "Image size invariant visual cryptography," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E82-A (10), 2172-2177.
- Naor, M. and Pinkas, B. (1997), "Visual authentication and identification," *Lecture Notes in Computer Science*, 1294, 322-336.
- Naor, M. and Shamir, A. (1995), "Visual cryptography," *Lecture Notes in Computer Science*, 950, 1-12.
- Shamir, A. (1979), "How to share a secret," *Communications of the ACM*, 22(11), 612-613.
- Shyu, S. J. (2006), "Efficient visual secret sharing scheme for color images," *Pattern Recognition*, 39(5), 866-880.
- Shyu, S. J. (2007), "Image encryption by random grids," *Pattern Recognition*, 40(3),



1014-1031.

Thien, C. C. and Lin, J. C. (2002), "Secret image sharing," *Computers & Graphics*, 26(5), 765-770.

Tu, S. F. and Hou, Y. C. (2007), "Design of visual cryptographic methods with smooth-looking decoded images of invariant size for gray level images," *Imaging Science Journal*, 55(2), 90-101.

Wang, R. Z. and Shyu, S. J. (2007), "Scalable secret image sharing," *Signal Processing: Image Communication*, 22s(4), 363-373.

