以半色調技術製作彩色視覺密碼

Visual Cryptography for Color Images Based on Halftone Technology

侯永昌 張兆源 林芳助
Hou, Young-Chang Chang, Chao-Yuan Lin, Franz

國立中央大學資訊管理學系 智慧型資訊系統實驗室
Intelligent Information Systems Laboratory
Department of Information Management, National Central University
e-mail: ychou@im.mgt.ncu.edu.tw

摘 要

視覺密碼學這個新興的密碼學領域，利用了人類視覺系統的特性直接對重疊的影像進行解密，它不須要任何密碼學的知識，也沒有複雜的計算過程。在安全性上，也可以確保截取者無法從這些個別的分享影像中察覺到任何與機密影像相關的紋理。

自從 Naor 及 Shamir 在 Eurocrypt'94 論文中提出了基本的視覺密碼模型後，陸續有不少學者發表了相關的研究。然而這些研究大部份集中在黑白影像的討論上，少有針對灰階及彩色影像提出作法。本篇論文，我們將根據以往視覺密碼的研究，加上半色調技術及分色原理，提出幾種灰階影像和彩色影像的視覺密碼的作法。我們的作法不但延續了黑白視覺密碼直接利用視覺系統解密，無須大量運算的優點，對於先前有關黑白視覺密碼學的研究（如 t out of n Threshold Scheme）亦可以輕易的套用在我們的方法上，而應用在灰階及彩色影像的製作上。

關鍵詞：視覺密碼、半色調技術、色彩分解、影像分享

Abstract

Visual Cryptography, which is an emerging cryptography technology, uses the characteristics of human vision to decrypt the overlapping images. It needs neither cryptography knowledge nor complex computation. In the regard to the safety, it ensures that hackers can't perceive any clues about the secret image on each cover image.

Since Naor and Shamir proposed the basic model of visual cryptography in the Eurocrypt'94, several researchers published their related researches continually. Most of these studies, however, concentrated on black-and-white images; few of them proposed methods for processing gray-level and/or color images. In this paper, we will propose several methods for gray-level and color visualization cryptography based on the past studies of black-and-white visual cryptography and the halftone technology and color decomposition

method. Our approaches do not only keep the advantage of black-and-white visual cryptography, which exploits the visual system to decrypt the secret image without huge computing, but also have the backward compatibility with the previous studies of black-and-white visual cryptography, such as t out of n threshold scheme can also be able to apply to gray-level and color images easily.

Keyword**:** Visual Cryptography, Halftone Technology, Color Decomposition, Images Sharing.

壹、前言

近年來，在網際網路中傳送多媒體資料已經非常普遍，而隨著電子商務時代的來臨，如何在開放的網路環境中，確保這些資料的安全，就成了目前急待解決的問題。

傳統密碼學中的加密技術是目前普遍被用來保護資料安全的方法。經過加密的資料形成亂碼，必須透過正確的鍵值（Key）才能將亂碼還原成原始資料。因此當資料加密後，即使被未經授權者所盜取，也因為沒有可以解密的鍵值，而無法得到原始資料的內容，也因此可以達到資料安全的目的。

Naor 及 Shamir 在 1994 年提出了一個新的密碼學領域，即所謂的視覺密碼學(Visual Cryptography)[9]。其最大的特色在於還原機密影像時不需做任何的計算，而直接利用人類的視覺系統從重疊的分享投影片（Share）中將機密訊息解讀出來，改進了傳統密碼學在解密過程中須大量複雜計算的缺點。而門檻機制(threshold scheme) [9-10, 15]使得視覺密碼學的應用變得更為靈活。針對 t out of n 門檻機制而言($t \le n$)，管理者可將機密影像分解成為 n 張投影片，並分別授權于 n 個成員，每人一張。只要有 t 個以上的成員，將所持有的投影片重疊起來，便可解讀出機密影像的內容；相反的，在小於 t 張投影片的情況上，無論如何都無法讀出機密影像的內容。

目前已有許多視覺密碼學相關的研究成果被公開發表[6-15]，然而這些研究大部份都集中在黑白影像的討論，少有灰階及彩色影像的視覺密碼作法。在 Naor 和 Shamir[10]的文章中所提出的模型，能夠隱藏紅色，黃色和透明色，也就是說他們所提出的彩色視覺密碼，能夠隱藏三種顏色，但其方法所產生的分享投影片有 2C 張之多，兩個人每人各持有 C 張分享投影片，其中 C 代表一個像素（pixel）所分解的子像素（subpixels）數目。在現今多媒體的世界中，對於彩色的影像來說，只能藏三種顏色是太少了一點，而且每個人持有多張分享投影片，也太過麻煩。

Rijmen 及 Preneel[12]曾提出一個彩色影像視覺密碼的作法，他是將一張彩色機密影像中的每一個像素，擴展成兩張分享影像上的 2*2 區塊，而每個區塊分別填入紅、綠、藍及白（透明）四種顏色。Rijmen 及 Preneel 認為這四個顏色在區塊中排列順序的不同會有 24 種可能的組合，當兩張分享影像上對應的區塊重疊後就會有 24^2 的變化。因為人類的視覺系統無法分辨過小色點，而會將區塊內四個像素顏色以平均色看待的情況下，因此就形成了具有不同色彩變化的影像。Rijmen 及 Preneel 的作法的確可以製作出彩色影像視覺密碼，但是無論以色彩學中的「增色」或「減色」模型〔2〕來看，以紅、綠、藍及白（透明）當成四個填入區塊的顏色，似乎並不恰當。另外，若以重疊後區塊內四個像素顏色的平均來表示原始影像中對應的像素顏色，那麼不同區塊在具有相同四個顏色，而排列不同的情況下（如：紅→綠→藍→白與藍→白→紅→綠），所得的平均色應該也會相同，因此並不如作者所說的 24^2 種顏

色變化，而是更少。

最近張真誠等人[3]提出一種彩色影像隱藏的技術，其隱藏演算法是針對所給定的一張機密影像 S，再任選兩張大小與機密影像同樣大小的掩蓋影像(O^1，O^2) 。然後計算機密影像所出現的顏色數量，假設為 CI，並且將所用到的 CI 個顏色的色盤資料建立一個 CIT 表格，並對機密影像所用到的各種顏色指定一個唯一的編碼值，假設就是它在 CIT 的位置。接著對兩張掩蓋影像中的每一像素分別擴展成一個由 M(=k*k)個子像素組成的區塊，使得偽裝影像放大為原來的 k 倍，其中 M 與 k 必需滿足下列的不等式 CI ≦⌊M/2⌋+1。在分享機密影像方面，對機密影像中的每一個像素 S_{ij}，由 CIT 表格中取得顏色值編號 n，然後利用兩張掩蓋影像中對應的顏色值 $O^{1C}{}_{ij}$ 與 $O^{2C}{}_{ij}$，將兩張掩蓋影像中的每一像素所擴展的區塊，隨機分別填入⌊M/2⌋+1 個顏色值為 $O^{1C}{}_{ij}$ 與 $O^{2C}{}_{ij}$ 的像素，並且讓這兩個擴展區塊所填入的位置有 n 個是重疊的，而剩餘的像素則填入透明色。重複這些步驟直到所有像素均處理完畢。而其復原只要從這兩張偽裝影像對每個 k*k 的區塊算出重疊的 n 值，再由 CIT 表格的第 n 個位置求出原來機密影像的顏色值即可復原。

侯永昌等人[1, 2]針對上述的缺點提出了一個改良的方法，去除了每個區塊都有固定的⌊M/2⌋+1 個掩蓋影像顏色值的限制，而是有『隨機個數』的掩蓋影像顏色值。其次隨機的利用交集(AND)和聯集(OR)的觀念，來計算掩蓋影像中每一個擴展區塊中顏色重疊的子像素的二元編碼值，使需要隱藏的機密影像的顏色可以達到 256 色、甚至是全彩影像。最後利用亂數與遮罩(MASK)的技巧，解決了彩色影像因為色彩的連續性和每個擴展區塊中沒有相同數目的顏色子像素，所造成在偽裝影像上顯露出機密影像區塊的邊界問題。

張真誠與侯永昌等人[1-3]雖然也達成了某種程度的彩色影像資料的分享，但是他們做法的最大缺點在於解密時必須透過電腦運算才可取得機密影像，不僅需要大量的運算，而且無法直接重疊出機密影像，違背了視覺密碼直接利用人類視覺來解密的原則。

侯永昌等人[4]利用色彩的累加與分解和降低影像對比與亮度的方法，完成彩色影像視覺密碼的製作，使機密影像可以直接由人的視覺系統所辨識出來，達到視覺密碼學的基本需求。但是所產生的兩張分享影片無法完全摒除影像邊界的感覺，因而尚無法達到安全性的要求。

本篇論文，我們將根據以往視覺密碼的研究，加上半色調技術及分色原理，提出灰階及彩色影像的視覺密碼作法。我們提出的方法延續了統傳視覺密碼的優點，可以不須任何密碼學的運算，直接利用人類視覺系統將機密影像解密出來。在安全性上，同樣可以確保截取者無法從這些個別的分享影像中察覺到任何與機密影像相關的紋理。對於彩色機密影像，我們的作法可以不受限於影像的格式與顏色數，將機密影像中的色彩從重疊的分享影像中表現出來。

貳、灰階影像視覺密碼製作

一、視覺密碼的基本原理

視覺密碼的輸出媒體為透明的投影片，所以在黑白影像上的白點我們以透明看待，因此像素之間的重疊具有以下的特性：黑＋黑＝黑，黑＋白＝黑，白＋黑＝黑，白＋白＝白。常見的黑白視覺密碼作法，是將機密影像上的每一個像素，依據圖 2.1 的方法分解成兩張投影片上的 2*2 區塊。當像素為白點時，以二選一的方式從圖 2.1 前兩列組合中決定兩張投影片中的區塊內容，如果為黑點則從後兩列的組合中挑選。在安全性上，投影片中的每一個區塊都只有兩種可能的型態（黑白黑白，白黑白黑），而且它們是以隨機的方式來決定，所以從單張投影片上是無法分辨出機密影像的原貌，但是當兩張投影片重疊時，原機密影像中的黑點會組合出全黑的區塊，而白點則組合出半黑半白的區塊（可以看成 50%的灰點）。以圖 2.2 為例，一張「中央資管所」字樣的機密影像(a)，製作成兩張視覺密碼投影片（b, c），當我們把這兩張投影片重疊後可以得到（d）的結果。雖然得到的是一張對比降低 50% 的影像, 但是人類的視覺系統還是很容易分辨出機密影像的內容。

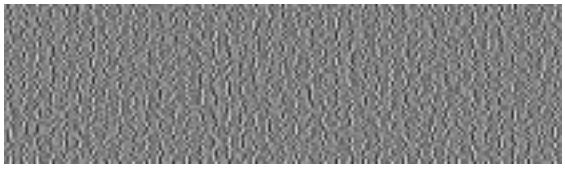
機密影像	投影片 1	投影片 2	重疊影像
□	▚	▚	▚
□	▞	▞	▞
■	▚	▞	■
■	▞	▚	■

圖 2.1 黑白像素的分享與重疊

(a) 機密影像

(b) 分享影像 1

(d) 分享影像 1 與分享影像 2 重疊結果



(c) 分享影像 2

圖 2.2 機密影像視覺密碼製作

二、半色調(Halftone)技術

每一種用來呈現影像的媒體，都因其物理特理而有不同表現色階的方法。在電腦螢幕裡，利用電流的強弱來控制像素發出的光

量，這些光量的不同產生了各種不同的色階；而一般列印設備（如點陣、雷射、噴墨列表機等），只能控制單一墨點的印（黑點）或不印（白點），而不能直接顯現出原影像的灰度或色調（tone）。因此必須利用網點的疏密來表現影像的色階，如亮部網點較疏，暗部網點較密（圖 2.3），這種利用網點疏密來模擬色階的方法，我們就稱之為半色調技術[6]。利用半色調技術我們可以將具有色階之影像轉換成二元影像，以灰階影像為例（圖 2.4a），轉換後的半色調影像（圖 2.4b），每一個像素只有兩種可能的色階（黑色或白色）。雖然轉換後的影像只有黑白兩色，但是在人類視覺系統無法分辨過小網點，而將附近的網點也參考進去的情況下，利用網點排列的疏密，仍然可以模擬出各種不同的色階感覺。

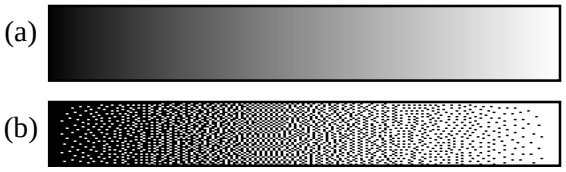


圖 2.3 (a) 連續調 (b) 半色調

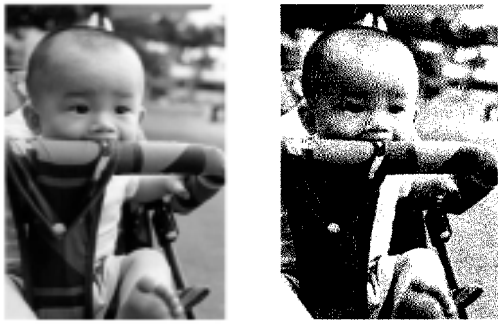


圖 2.4 (a) 連續調 (b) 半色調

三、灰階視覺密碼的製作

既然大部份的列印設備在列印灰階影像前都必須經過半色調的轉換，而轉換後的半色調影像又是一個黑白影像，這樣的影像格式便非常適合利用傳統黑白視覺密碼方法（圖 2.1）來製作視覺密碼。所以本篇文章即利用轉換後的半色調影像來製作灰階影像的視覺密碼，其演算法描述如下：

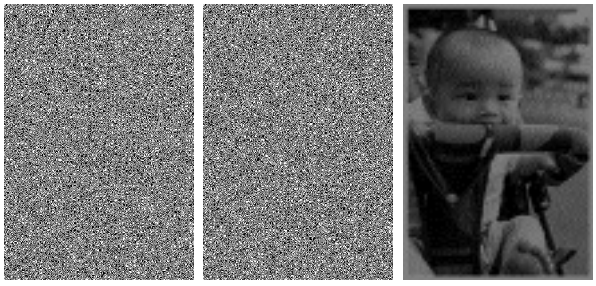
(1) 將灰階影像轉換成黑白半色調影像。

(2) 對於半色調影像上的每一個黑點或白點，我們依據圖 2.1 的方法分解成兩張投影片上的 2*2 區塊。當像素為白點時，以隨機的方式從圖 2.1 前兩列的組合中，隨機的挑選其中一列，做為投影片 1 和投影片 2 上區塊內容的組合；如果為黑點，則從後兩列的組合中挑選其中的一列，做為兩張投影片的內容。

(3) 重覆步驟（2），直到半色調影像上的每一個像素均被分解完成為止，就可以得到兩張分享機密影像的視覺密碼投影片。

四、實驗與討論

圖 2.4 中我們依據上述提出的方法對一張灰階影像(圖 2.4a)，經過半色調的處理後(圖 2.4b)，製作成兩張視覺密碼的投影片（圖 2.5a，圖 2.5b），從這兩張分享投影片中我們確實無法得知任何與機密影像相關的訊息，但是當我們將這兩張投影片重疊在一起時，便形成圖 2.5c 的結果，結果中我們可以清楚的分辨出是一張小女孩的圖片。



(a) 投影片 1 (b) 投影片 2 (c) 投影片 1+2

圖 2.4 灰階視覺密碼的製作與重疊

參、彩色影像之視覺密碼

一、色彩的基本原理

色彩的構成我們常用「增色」、「減色」二種模型（圖 3.1）來加以描述[6]。其中「增色」模型是利用不同的色光加以混合來呈現所要的色彩，對於任何射入眼中的可見光都可以用紅（Red）、綠（Green）、藍（Blue）三種色光組合而成，色光混合愈多，光度愈增加，愈近於白色光，故稱之為「增色」。而紅、綠、藍則稱為色光三原色，電腦螢幕就是一個增色模型的最好例子；「減色」模型則是利用物體表面反射的色光組合來呈現色彩（因為大部份的物體無法自發光源）。以一個放在自然光下的蘋果為例，蘋果的表面吸收了自然光中的綠光及藍光，而反射紅光至人的視覺系統，就形成了紅色的蘋果。在顏料中青（Cyan）、洋紅（Magenta）、黃（Yellow）可以混合出各種不同的顏色，顏料的混合愈多，光度愈減少，愈近於黑色，故稱之為「減色」。而青、洋紅、黃則稱為顏料三原色，這三種顏色是無法由其他顏色組合出來，彩色列表機就是利用減色模型的原理來列印彩色圖片。

以上的描述，說明了 Rijmen 及 Preneel 作法中以紅、綠、藍及白（透明）當成四個填入區塊的顏色並不恰當，若以「增色」的角度來看，任何的色彩加上白色後應仍為白色，因此以紅、綠、藍及黑為填入區塊的四個顏色，似乎較為合理；另外，若以「減色」的角度來看，紅、綠、藍任兩種顏色的組合，所得的結果皆為黑色，所以紅、綠、藍及白中任兩種顏色的組合只可能得到 4 種結果：紅＋白＝紅、綠＋白＝綠、藍＋白＝藍及黑色，此時應以青、洋紅、黃及白為填入區塊的四個顏色應該較為恰當。

在電腦系統中，大部分的影像處理軟體及目前普遍被使用的 Windows 作業系統，其所提供的 API（Application Interface）皆以 RGB 做為色彩表示的基礎，主要的原因在於我們大部份都以螢幕做為輸出的媒體，而螢幕是利用發射 RGB 光源至人的視覺系統來產生彩色影像。在表現 1677 萬色變化的全彩模式中，R、G、B 各以 8bits 來表示，因此 R、G、B 中的每一單色皆有 0 255 的色階變化。也就是說，當我們以（R，G，B）來描述一個色點時，（0，0，0）表示最黑點，而（255，255，255）則表示最白點。

在視覺密碼中，我們是以分享影像（投影片）做為解密的工具，也就是最終輸出物為投影片。由於投影片上的色彩比較適合以「減色」模型來描述，因此接下來我們所提的彩色視覺密碼作法中，皆以 CMY 的減色

模型來描述色彩。由於 R、G、B 相對於 C、M、Y 為互補色，因此在全彩的模式下對於描述同一種顏色，（R，G，B）及（C，M，Y）具有下列的關係，C=255-R，M=255-G，Y=255-B。在（C，M，Y）表示法裡，（0，0，0）表示最白點，而（255，255，255）則表示最黑點。

二、彩色影像列印

彩色印表機大多利用青、洋紅、黃三種色墨來表現色彩，因此在彩色影像列印前必須進行分色處理。所謂分色原理主要是從影像中每一個像素的色彩中，分離出所含的青、洋紅、黃三個色彩成為 3 張分色影像（由於色墨成份的關係，有些青，洋紅，黃色墨混合後並無法表現出純黑色，所以有些印表機的分色處理會加上黑色的分色影像，成為 4 個分色影像）。這些分色影像就像是單一的灰階影像一樣，每一個像素仍具有不同的色階，因此仍須借助半色調技術，將分色影像轉換成印表機用來表現色階的分色半色調影像。這三張分色半色調影像分別為（青，白）、（洋紅，白）及（黃，白）的兩色影像，這些影像疊合後就可以表現出原始影像上的各種不同色彩。一個列印彩色影像的程序，可以圖 3.2 來描述。

接下來我們利用將彩色影像分解為三張分色半色調影像的方法，提出三種彩色視覺密碼的作法。在想法上，我們可以把一張經由圖 3.2 的步驟所處理過的彩色組合影像 P 上的每一個像素 P_{ij} 的顏色，看成是一個由 C（青）、M（洋紅）、Y（黃）三張分色半色調影像圖中，相對應網點的顏色(C_{ij}，M_{ij}，Y_{ij})所組合成。其中 C、M、Y 影像皆為二元影像，所以對於任何一個像素 C_{ij}、M_{ij} 或 Y_{ij} 只有空白及不是空白這兩種可能。我們以 0 表示空白，1 表示包含顏色，則 P_{ij} 具有下列八種可能的組合：(0，0，0)，(1，0，0)，(0，1，0)，(0，0，1)，(1，1，0)，(1，0，1)，(0，1，1)，(1，1，1)，其中 P_{ij}（0，0，0）代表為白點，而（1，1，1）則為黑點。由於青、洋紅、黃為顏料三原色，因此它在透明媒體上重疊時仍有青＋青＝青，青＋白＝青及白＋白＝白…的特性。接下來我們就一一介紹我們所提的三種彩色視覺密碼的作法。

三、作法一

我們提出的第一個作法是將彩色機密影像利用圖3.2所示的步驟，轉換成C、M、Y三個分色的半色調組合影像後，將影像中的每一個像素擴展成2*2的區塊，並將它的顏色分別分配到青、洋紅及黃三張分享影像上。這些分享影像上的每一個區塊皆為二點透明及二點含分色的顏色，因此可以達到最大的亂度，清除影像紋理的目的。另外，我們再設計一張半黑白的遮罩，遮罩影片的目的是當這四張分享影像重疊時，遮罩可以遮掉了一些我們不希望出現的顏色，而表現出我們要的顏色。

以圖3.3為例，如果組合影像上的像素P_{ij}為（0，0，0），則三張分享影像上色點的分佈即如圖3.3之第一列，因為加上Mask重疊

後，三張分享影像露出來的部份都是"白色"的部份，形成白色的感覺；如果組合影像上的像素P_{ij}為（1，1，0），則只有C及M的分量可以顯露出來，Y的分量被Mask遮蔽，表示在三張分享影像上色點的分佈即如圖3.3之第五列，形成藍色（青＋洋紅）的感覺；如果組合影像上的像素P_{ij}為（1，1，1），則C、M及Y的分量都可以顯露出來，重疊在一起以後就形成黑色，再加上Mask的黑色，整個區塊就都是黑色，表示在三張分享影像上色點的分佈即如圖3.3之第八列。利用這樣的方法，我們就可以將組合影像中三個分色的八種組合以圖3.3的方式來表示。

另外我們也可以從顏色分量的角度來分析重疊影像上的顏色分布。以圖3.3之第一列為例，在組合影像上的2*2區塊中，黑色佔了整個區塊的一半，而黑色可以視為是青＋洋紅＋黃的組合，因此也就相當於(C，M，Y)顏色分量各佔整區塊的一半，亦即（1/2，1/2，1/2）。如果組合影像上色點的分佈即如圖3.3之第五列，只有C及M的分量可以顯露出來，Y的分量被Mask遮蔽，再加上mask的黑色（可以視為是青＋洋紅＋黃），表示在組合影像上的2*2區塊中，青及洋紅可以出現在四個區塊中，而黃色只出現在兩個區塊中，因此(C，M，Y)顏色分量可以用（1，1，1/2）來表示。如果組合影像上色點的分佈即如圖3.3之第八列，四個區塊中都是黑色，因此(C，M，Y)顏色分量可以用（1，1，1）來表示。利用這樣的方法，我們就可以將組合影像中顏色分量的組合以（1/2，1/2，1/2），（1，1/2，1/2），（1/2，1，1/2），（1/2，1/2，1），（1，1，1/2），（1，1/2，1），（1/2，1，1），（1，1，1）來呈現。因此重疊影像中的白色不再是全白（0，0，0），而是半黑白（1/2，1/2，1/2）；重疊影像中顏色的分布不再是由（0，0，0）（1，1，1），而是由（1/2，1/2，1/2）（1，1，1），和傳統黑白視覺密碼的研究一樣，都是藉由降低重疊影像上顏色的對比，來達成分享投影片上的亂度。

此作法，每一個遮罩區塊中的黑點分佈有C(4，2)＝6種組合，每一種組合都有對應的Share1，Share2及Share3的分佈。實作時，可以用隨機的方式取得遮罩及對應的Share分佈，更可增加破解的難度。

1、彩色視覺密碼演算法－作法一

(1) 將彩色影像轉換成3張分色半色調影像C、M、Y。

(2) 針對組合影像中的每一個像素P_{ij}，進行下列處理：

a. 我們先以隨機的方式選出一種2*2大小遮罩，並以隨機的方式在這四點位置中任意加入兩點黑點（形成半黑半白的狀態）。

b. 所以當遮罩選定後，根據a中遮罩裡的黑點位置及C_{ij}決定在區塊中何處填入色點（青色）。當C_{ij}=1（不為白點）時，在區塊中對應於Mask裡不是黑點的位置填入色點；而當C_{ij}=0（白點），則在對應於Mask裡黑點的位置填入色點。最後在將這個區塊加入Share1分享影

像上的對應位置。

c. 依循b的作法，以Mij決定填入Share2區塊中色點（洋紅）的位置；以Yij決定填入Share3區塊中色點（黃）的位置。

(3) 重覆步驟（2），直到組合影像上的每一個像素均被分解完成為止，就可以得到四張（青、洋紅、黃及黑）分享機密影像的視覺密碼投影片。

(4) 只要將這四張分享影像重疊起來，便可直接由人的視覺系統進行解密。

2、實驗與討論

在黑白視覺密碼學的理論中，分享影片上的每一個像素，都以半黑白的方式來呈現，以達到分享影片中的亂度。因此，雖然重疊影像中的黑是全黑，但是白就不再是全白，而是半黑白，因而降低了重疊影像中顏色的對比。在我們的彩色視覺密碼學的研究中也是如此。我們利用圖3.2中的三張分色半色調影像製作分享影片(圖3.4)。在這四張分享影像中完全是亂碼，我們完全無法從其單一的影像上察覺到原始機密影像的紋理，而重疊影像雖然在對比上有些降低（降低50%），但仍然可以輕易的辨別出影像上的內容。

本作法利用Mask來遮住不希望出現在重疊影像中的顏色，造成黑色背景的效果。因此，如果缺少了Mask分享影片，將會造成雜色的出現，因而混淆了機密影像的輪廓，無法顯示出機密影像的內容。因此，我們可以將Mask分享影片交由管理階層保管，讓他有較高的權限，而Share C, M, Y則交由其他三個部屬所保管。就算這三個部屬合謀，沒有主管所擁有的Mask分享影片，也無法竊取機密影像的內容。因此，Mask分享影片就可以提供一層特權（privilege）或稽核的機制。

四、作法二

由於人類的視覺系統無法直接辨識過小的色點，因此會把鄰近的色點一起參考近去感覺出一個區塊內的平均色，這也是經過半色調及分色後的影像可以表現出各種不同色彩的原因。利用這個特性，我們延伸出另一個彩色視覺密碼的模型。本作法主要是將分色半色調影像中的每一個像素展開成兩張分享影像上的 2*2 區塊，而區塊內分別填入青、洋紅、黃及一個透明色，再藉由二張分享影像上對於這四個顏色可以有不同排列方式，經重疊後就可以產生不同的色彩變化。以圖 3.5 為例，第一列中 Share1 與 Share2 上的色彩分佈完全相同，重疊後因為視覺系統會將這四個點(青、洋紅、黃及透明)的效果均化，而得到白色的感覺。從顏色分量的角度去看，青、洋紅和黃各佔整個區塊的四分之一，亦即(1/4，1/4，1/4)。而第二列中的 Share1 及 Share2，青色及透明對調，重疊後在這四點上就含有二個青，一個洋紅及一個黃得到(1/2，1/4，1/4)的結果，而得到青色的感覺。依照組合影像的需要，我們可以利用圖 3.5 上作法欄的指示，選取 Share１及 Share2 上的區塊色彩分佈，就可以完成兩張分享影片的製作。這兩張分享投影片重疊

後，就可以得到顏色分量的分布為（1/4，1/4，1/4）到（1/2，1/2，1/2）的重疊影像。

Share1 上的色彩分佈有 3!=6 的組合，不同的 Share1 也可以產生對應的 Share2，因此，實作時可以隨機的選擇不同的 Share1 以增加破解的難度。

1、視覺密碼演算法－作法二

(1) 將彩色影像轉換成3張分色半色調影像C、M、Y。

(2) 針對組合影像中的每一個像素P_{ij}，進行下列處理：

a. 我們先在Share1上展開2*2區塊，並以隨機的方式將青、洋紅、黃及透明色填入區塊中。

b. 同樣在Share2中建立一個2*2大小的區塊，根據a中所產生的區塊其四個顏色的排列位置及C_{ij}，M_{ij}，Y_{ij}，並參考圖3.5中的作法欄的作法，決定Share2上對映區塊內，青、洋紅、黃及透明四個顏色的排列方式。以一個像素P_{ij}為(1，1，0)為例，當選定了Share1區塊排列為青→白→洋紅→黃時，將青色與洋紅色位置對調後便成為Share2上對映的區塊排列方式洋紅→白→青→黃。

(3) 重覆步驟（2），直到組合影像上的每一個像素均被分解完成為止，就可以得到兩張分享機密影像的視覺密碼投影片。

(4) 只要將這二張分享影像重疊起來，便可直接由人的視覺系統進行解密。

2、實驗與討論

我們同樣利用圖3.2中的三張分色半色調影像製作分享影片(圖3.6)。其中的分享影像亦無法從單一的影像中察覺原始機密影像的紋理，而重疊影像仍然可以輕易的辨別出影像上的內容。

作法二改善了作法一必須利用四張分享影像才可以重疊出組合影像的不方便之處，只須兩張分享影像即可進行解密，但是，就無法如作法一提供特權或稽核的機制。然而依照圖3.5的作法，重疊影像的顏色分量的分布分別是(1/4，1/4，1/4) (1/2，1/2，1/2)，其中白點的值為(1/4，1/4，1/4)，黑點值為(1/2，1/2，1/2)。也就是說，作法二所得的分享影像經過重疊後，顏色對比的廣度將為原始影像的25%。而以作法一中白點的值為(1/2，1/2，1/2)，黑點的值為(1，1，1)來看，作法一所得的重疊影像對比的廣度則為原始影像的50%。因此，作法二所得的重疊影像對比會比作法一來得差，但是色階的變化在1/4 1/2之間，所以亮度會比較高一些，對於色系太深的機密影像而言，會有較好的合成效果。

五、作法三

為了同時改善作法一須要四張分享影像的麻煩，並解決作法二重疊影像對比不好的問題，我們提出第三種只需兩張分享影像，又不必犧牲太多影像對比的彩色視覺密碼的作法。我們的作法是將彩色機密影像轉換成

的 C、M、Y 三張分色半色調影像，利用 2.3 節中灰階影像視覺密碼作法，分別製作出 C１，C2、M1，M2 和 Y１，Y2 六張分享影像。每一張分享影像都是兩個白點和兩個分色色點，也就是顏色分量都是 2/4。然後將 C1，M1，Y1 三張分享影像組合成 Share1，而將 C2，M2，Y2 組合成 Share2。因此對於 Share1 及 Share2 上的每一個區塊，其顏色分量都是(1/2，1/2，1/2)，而兩者重疊後，就可以得(1/2，1/2，1/2)　(1，1，1)的效果。圖 3.7 中顯示了一個藍色的色點，分解為兩張分享影像的過程，以及重疊後的結果。

1、視覺密碼演算法－作法三

(1) 將彩色影像轉換成3張分色半色調影像 C、M、Y。

(2) 針對組合影像中的每一個像素P_{ij}，進行下列處理：

a. 將C_{ij}、M_{ij}、Y_{ij} 依傳統黑白視覺密碼的作法，分別擴展出C_{ij1}，C_{ij2}、M_{ij1}，M_{ij2} 及Y_{ij1}，Y_{ij2} 六個暫存的2*2大小區塊。

b. 將區塊C_{ij1}、M_{ij1} 及Y_{ij1} 進行組合，並填入對應於P_{ij} 的Share1區塊中。

c. 另外將區塊C_{ij2}、M_{ij2} 及Y_{ij2} 進行組合，並填入對應於P_{ij} 的Share2區塊中。

(3) 重覆步驟（2），直到組合影像上的每一個像素均被分解完成為止，就可以得到兩張分享機密影像的視覺密碼投影片。

(4) 只要將這二張分享影像重疊起來，便可直接由人的視覺系統進行解密。

2、實驗與討論

我們同樣利用圖3.2中的影像製作分享影片(圖3.8)。它也延續了作法一及作法二中無法從單一的分享影像中察覺原始機密影像的紋理，及重疊影像可以輕易的辨別出內容的優點。並且改善了作法一須要四張分享影像的麻煩，及作法二重疊影像對比不好的問題。但是同樣的，本作法無法如作法一提供特權或稽核的機制。

肆、結論

視覺密碼的提出，無疑提供了影像在網路上傳送的另一種安全作法，它的優點在於解密時無需大量的運算，可直接利用人類視覺特性來取得機密。目前關於視覺密碼的研究大多集中在黑白影像的探討上，在本文裡我們利用半色調技術及分色原理為灰階影像及彩色影像的視覺密碼製作提出了完全的解決方法。

利用半色調技術我們可以將具有色階的影像轉換成適合於視覺密碼製作的二元影像，加上分色原理 C，M，Y 顏料三原色可以表現出彩色影像上的各種色彩。和傳統的黑白影像視覺密碼模型一樣，將機密影像上的每一個像素擴展至分享影像上的 2*2 區塊，而區塊中皆保持 2 個色點的狀態，因此非常安全。

我們的作法不但延續了黑白視覺密碼直接利用視覺系統解密，無須大量運算的優點，而且對於先前的相關研究，例如：t out of n Threshold Scheme，亦可以藉由不同的資料

分享方式[15]，套用我們的方法，而輕易的應用在彩色及灰階影像的製作上。

參考文獻

1. 侯永昌、林芳助、張兆源著，「彩色機密影像分享技術改良與製作」，第五屆資訊管理研究暨實務研討會，世新大學，民國 88 年 11 月，頁 592-597。
2. 侯永昌，林芳助，張兆源，「一種 256 色機密影像分享的新技術」，資管評論，第九期，頁 89-105。
3. 張真誠、蔡垂雄、陳同孝著，「一種用來分享彩色機密影像的技術」，第九屆全國資訊安全會議論文集，台中，pp. LXIII-LXXII，88 年 5 月。
4. 侯永昌，張兆源，林芳助，1999.12，「以色彩分解為基礎的彩色視覺密碼」，第五屆資訊管理研究暨實務研討會論文集，台北，pp. 584-591。
5. 連國珍，「數位影像處理」，儒林圖書有限公司，1992。
6. 羅福林、李興才 著，印刷工業概論，中國文化大學出版部，民 76，頁 121-126。
7. Ateniese, G., C. Blundo, A. De Santis, and D. R. Stinson, “Visual Cryptography for General Access Structures “, Information and Computation, 129（1996）, pp.86-106.
8. Blundo, C. A. De Santis and D. R. Stinson “On the Contrast in Visual Cryptography schemes”, ftp://theory.lcs.mit.edu/pub/tcrypto1/96-13.ps.
9. Naor, M. and A. Shamir, “Visual Cryptography”, Advances in Cryptology: Eurpocrypt’94, Springer-Verlag, Berlin, 1995, pp. 1-12.
10. Naor, M. and A. Shamir, “Visual Cryptography II: Improving the Contrast Via the Cover Base”. Theory of Cryptography Library Report 96-07, ftp://theory.lcs.mit.edu.tw/pub/cryptol/96-07.ps
11. Naor, M. and B. Pinks, “Visual Authentication and Identification”, http://theory.lcs.mit.edu/~tcrypto/
12. Rijmen, V. and B. Preneel, “Efficient Colour Visual Encryption for Shared Colors of Benetton” Presented at Eurocrypto’96 Rump Session Available as http://www.iacr.org/conferences/ec96/rump/preneel.ps.
13. Rubin, A.D. “Independent one-time passwords”, computing Systems Vol.9, 1996, pp.15-27
14. Shamir, A. “Visual Cryptanalysis”, proc of Eurocrypt’98, Espoo, 1998.
15. Stinson, D.R., “An introduction to Visual Cryptography”, http://bibd.unl.edu/~stinson/vcs-pus.ps.

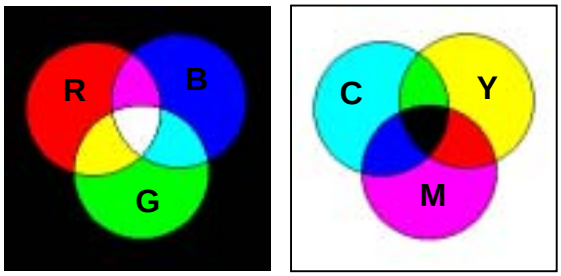


圖 3.1 (a) 增色模型 (b) 減色模型

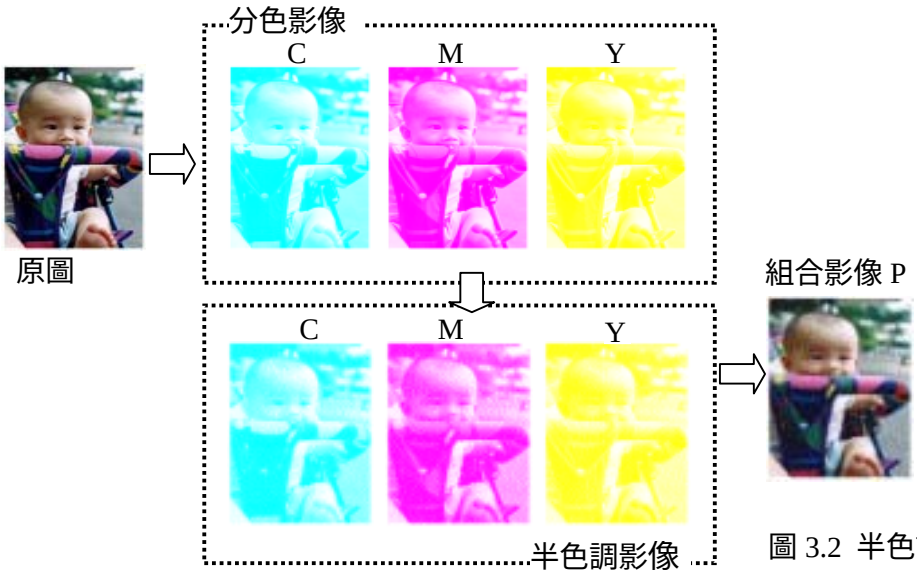
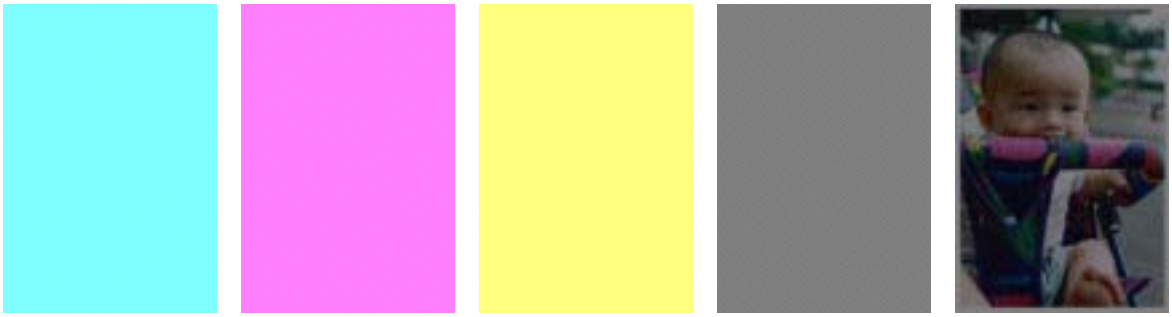


圖 3.2 半色調彩色影像列印

Mask	露出的顏色 (C,M,Y)	Share1(C)	Share2(M)	Share3(Y)	重疊影像	顯示的顏色分量(C,M,Y)
	(0，0，0)					(1/2，1/2，1/2)
	(1，0，0)					(1，1/2，1/2)
	(0，1，0)					(1/2，1，1/2)
	(0，0，1)					(1/2，1/2，1)
	(1，1，0)					(1，1，1/2)
	(0，1，1)					(1/2，1，1)
	(1，0，1)					(1，1/2，1)
	(1，1，1)					(1，1，1)

圖 3.3 彩色視覺密碼模型一



(a) Share1(C) (b) Share2(M) (c) Share3(Y) (d) Mask (e) 重疊影像

圖 3.4 四張分色的分享影片和重疊的效果

露出的顏色(C,M,Y)	Share1	Share2	重疊影像	作法	實際效果	顯示的顏色分量(C,M,Y)
(0，0，0)				Share1, 2 具有相同排列		(1/4，1/4，1/4)
(1，0，0)				青與透明位置對調		(1/2，1/4，1/4)
(0，1，0)				洋紅與透明位置對調		(1/4，1/2，1/4)
(0，0，1)				黃與透明位置對調		(1/4，1/4，1/2)
(1，1，0)				青與洋紅位置對調		(1/2，1/2，1/4)
(0，1，1)				黃與洋紅位置對調		(1/4，1/2，1/2)
(1，0，1)				青與黃位置對調		(1/2，1/4，1/2)
(1，1，1)				兩兩位置對調		(1/2，1/2，1/2)

圖 3.5 彩色視覺密碼模型二

(a) Share1　(b) Share2　(c) 重疊影像

圖 3.6 兩張分享影片和重疊的效果

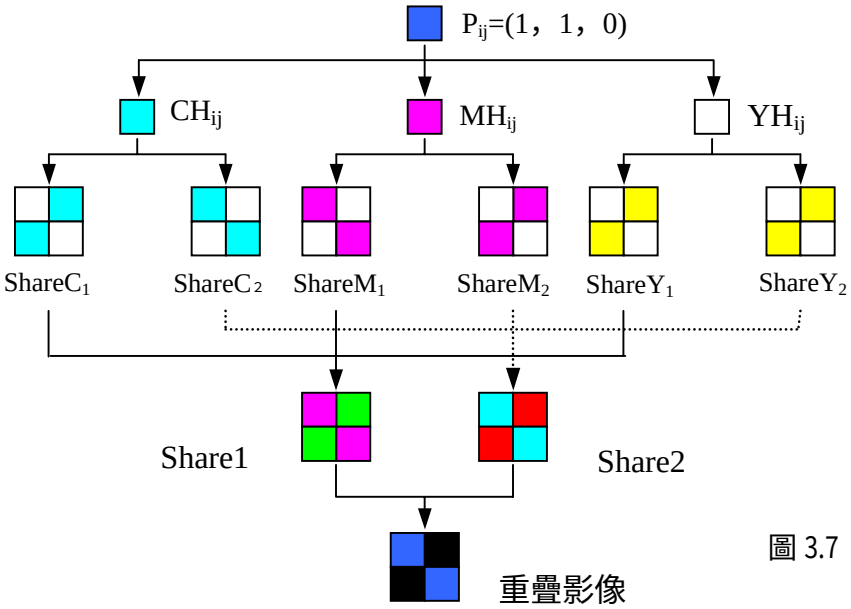
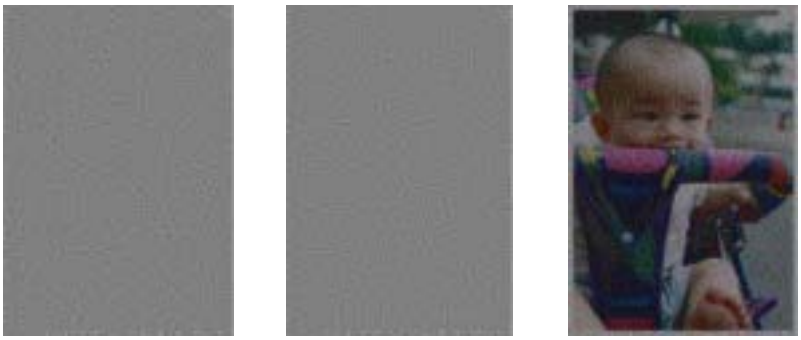


圖 3.7 彩色視覺密碼模型三



(a) Share1　(b) Share2　(c) 重疊影像

圖 3.8 兩張分享影片和重疊的效果

作者簡介

侯永昌
國立交通大學資訊工程研究所博士。現任國立中央大學資訊管理系副教授，兼學生事務處僑外生輔導室組長。研究領域為資訊隱藏、浮水印技術與視覺密碼、模糊理論、軟體工程、演算法則。

張兆源
國立中央大學資訊管理系碩士。研究領域為影像處理、資訊隱藏與視覺密碼。

林芳助
國立中央大學資訊管理系碩士。目前服役軍中，預計民國 90 年底退伍。研究領域為資訊隱藏與浮水印技術。