像素無擴展的彩色連續調影像視覺密碼研究

朱正民[1]　邱創標[2]　黃賦宇[3]

[1]中州科技大學機械與自動化工程系

[2]中州科技大學機械與自動化工程系

[3]中州科技大學工程技術研究所研究生

摘要

視覺密碼（Visual Cryptography，又稱視覺秘密分享）是在 1995 年由 Naor 及 Shamir 所提出的一種極為便利的資訊隱藏技術，其中最主要的精神是利用影像重疊來解讀秘密內容，且在解讀秘密過程中不需利用電腦來執行複雜的運算。

而至今的研究中，不管是灰階影像或是彩色影像，都必需先將連續調影像轉換成半色調影像來製作，卻沒有直接採用連續調影像所製作的視覺密碼。

我們針對連續調影像重疊進行深入探討，推導了一個出符合視覺密碼重疊概念的重疊公式。此公式不僅可在電腦上模擬影像的類比重疊，亦可將一張灰階或是彩色的連續調影像不需要經過半色調處理，影像亦不需要經過擴展，便可直接製作成視覺密碼之分享影像。有效的保留連續調影像經過半色調處理或擴展處理後，所失去的影像品質。

關鍵字：視覺密碼、影像重疊、連續調影像

通訊作者
姓名：朱正民
E-mail：chucm@dragon.ccut.edu.tw

壹、前 言

自從 1995 年 Naor 及 Shamir[5]兩位學者提出了一種可直接用數張影像疊合出藏在影像中的秘密而不需藉助任何電腦運算的視覺密碼，最初是應用在黑白機密影像的分享上，稱為（*k*, *n*）-threshold 視覺式秘密分享機制（visual secretsharing scheme, VSS），意即 *n* 張分享影像中至少任取 *k* 張影像加以疊合，即可解晰出機密影像[2, 3]。至今已有不少學者發表相關之研究，方法也不斷地創新，而這些研究大部分都集中在黑白與灰階影像上。

目前視覺密碼在彩色影像上的研究僅占少數。且這些方法都必需將一張連續調影像，利用分色半色調技術，來轉換成半色調影像才能製作。如: 1997 年 Verheul 與 van Tilborg [6] 提出有關彩色視覺密碼的研究，稱 *k* out of *n* *c*-color VSS 機制，也就是具有 *c* 種顏色的機密影像，分解成 *n* 張分享影像，取其中 *k* 張加以疊合，便可還原機密影像。2003 年 Y. C. Hou[7] 也提出了一種以彩色的視覺密碼，它是先將一張彩色影像經過分色處理轉換成分色半色調影像，再經由擴展及編碼，將一張機密影像分解成數張分享影像，將全部的分享影像重疊後即可得到，彩色的機密影像。2008 年 H.C.Wu、H.C.Wang 與 R.W.Yu[4]提出了具有偽裝影像的有意義的彩色視覺密碼。它是取出彩色半色調影像中的，奇數行或偶數行的像素，來做擴展及編碼後重新組合成分享影像，在分享影像上可看到偽裝用的彩色影像，當分享影像重疊後，便會呈現出機密影像。

貳、相關研究

2008 年，Hsien-Chu Wu、Hao-Cheng Wang 與 Rui-Wen Yu[4]提出了，一種具有偽裝影像的有意義的彩色視覺密碼。其作法主要可分為下列三個部分:

一、抽取機密影像及偽裝影像的奇數行（或偶數行）之像素。如圖 2.1。

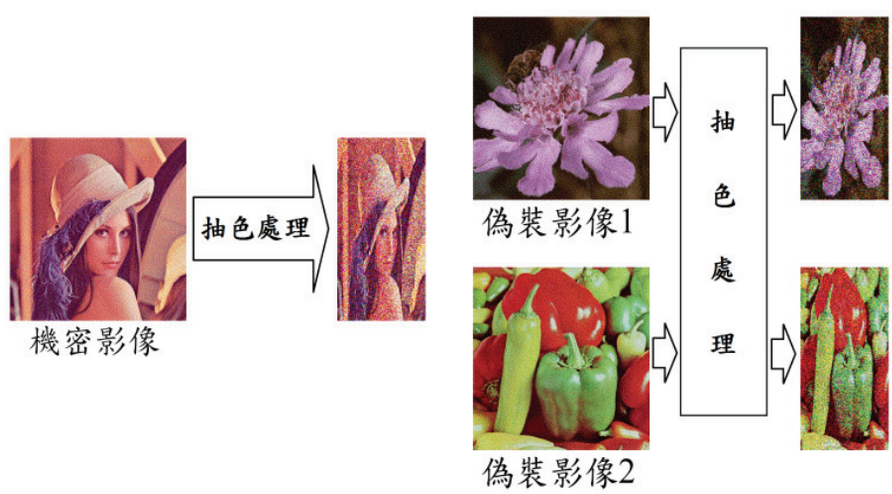


圖 2.1 抽取奇數行（或偶數行）之像素的影像

二、將機密影像依進行機密影像編碼處理，偽裝影像進行偽裝影像編碼處理。其編碼方式分為機密影像編碼（如表 2.1）與偽裝影像編碼（如表 2.2）兩種。

表 2.1　機密影像編碼對照表

機密影像像素	□	■	■	■	■	■	■	■
分享影像區塊1	■	■	■	■	■	■	■	■
分享影像區塊2	■	■	■	■	■	■	■	■
重疊影像區塊	■	■	■	■	■	■	■	■

表 2.2　偽裝影像編碼對照表

偽裝影像1 / 偽裝影像2	□	■	■	■	■	■	■	■
□	■	■	■	■	■	■	■	■
■	■	■	■	■	■	■	■	■
■	■	■	■	■	■	■	■	■
■	■	■	■	■	■	■	■	■
■	■	■	■	■	■	■	■	■
■	■	■	■	■	■	■	■	■
■	■	■	■	■	■	■	■	■
■	■	■	■	■	■	■	■	■

三、經過編碼處理後的機密影像與偽裝影像的每個像素會被擴展成一個 2×2 區塊，最後再將此 2×2 區塊組合成一個 4×2 區塊。組合方式如圖 2.2。而圖 2.3 為該 4×2 區塊的重疊示意圖。

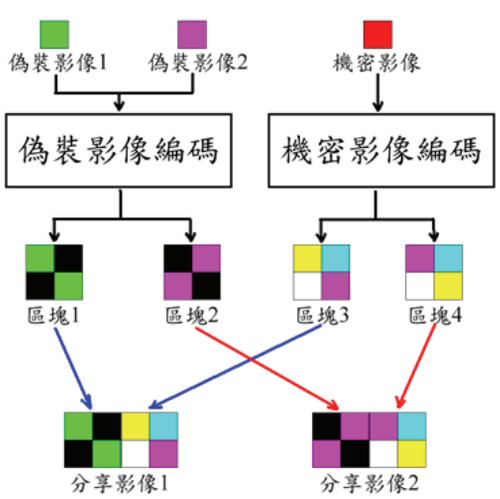


圖 2.2　Hsien-Chu Wu 等人的組合方式

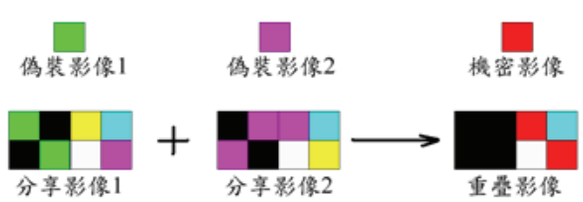
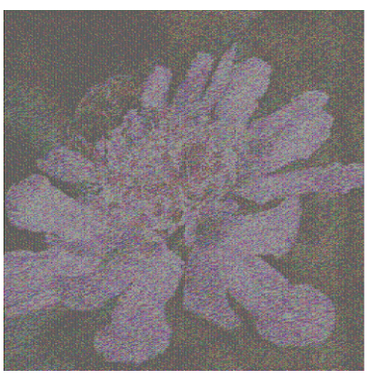
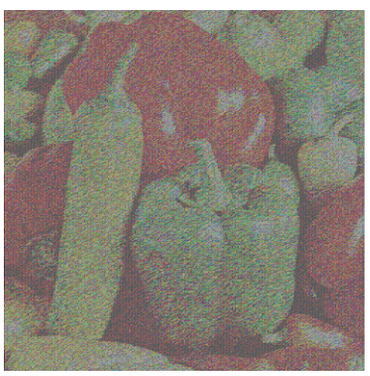


圖 2.3　重疊示意圖

經過組合後會得到兩張影像分享影像如圖 2.4，從圖 2.4 中我們可以看到兩張不同的偽裝影像。當我們把分享影像重疊後，偽裝影像的像素便會被黑色的像素所覆蓋，而機密影像的像素則會顏色的混合而變色，進而呈現出機密影像，如圖 2.5。



a. 分享影像 1



b. 分享影像 2

圖 2.4 Hsien-Chu Wu 等人的分享影像

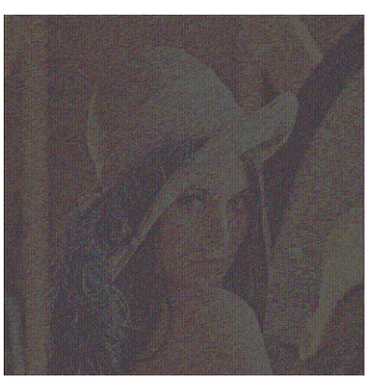


圖 2.5 Hsien-Chu Wu 等人的重疊影像

參、影像種類與重疊探討

一、 連續調影像與半色調影像

（一）連續調影像（Continuous-tone Image）

在黑色至白色中，仍有許多種灰色，如接近黑色的灰色、接近白色的灰色，連續調影像即是以連續的方式來呈現由黑色到白色的影像，如圖 3.1（a）、圖 3.2（a）。也是我們比較熟悉的數位影像，可分為灰階與全彩兩種。它會依不同的位元數，會有不同的色階。我們一般的數位相機所拍攝之影像，大部分為 24 位元及 32 位元。

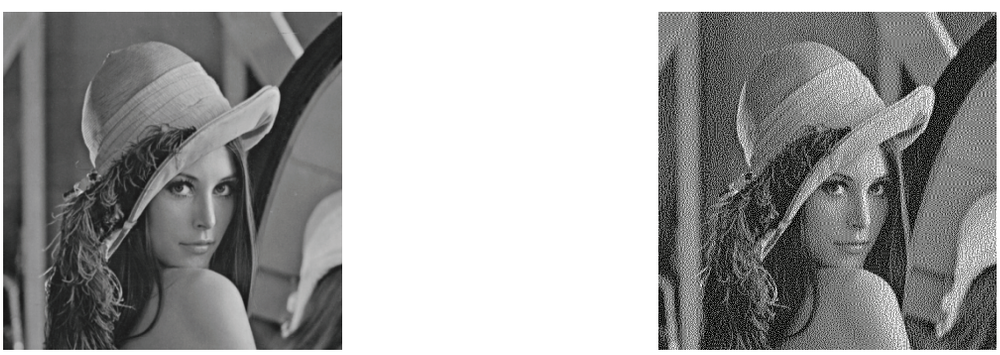
（二）半色調影像（Half-tone Image）

二元影像的一種，它是利用黑點與白點的分佈比例，來呈現不同的影像色階，若

一區塊中，僅有白點無任何黑點時，則該區塊為白色。若一區塊中，僅有少數黑點時，則該區塊為接近白色的灰色。若一區塊中，僅有少數白點時，則該區塊為接近黑色的灰色。若一區塊中，僅有黑點無任何白點時，則該區塊為黑色。如圖 3.1（b）、圖 3.2（b）。

a.連續調　　b.半色調

圖 3.1　連續調與半色調的灰階漸層影像

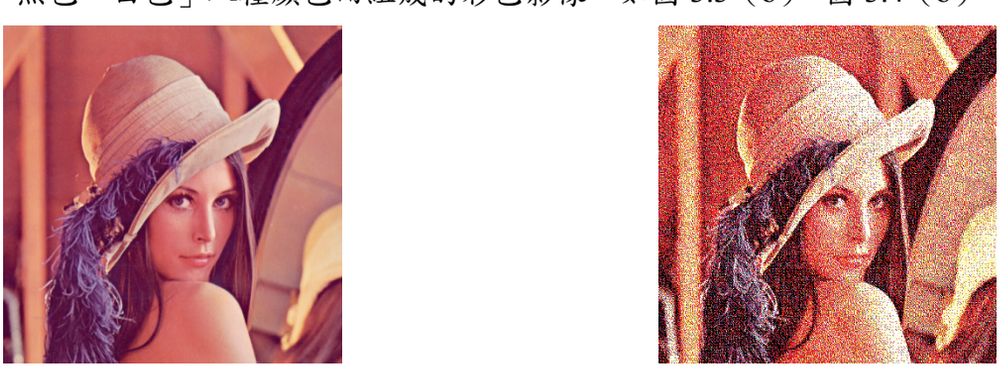


a.連續調　　b.半色調

圖 3.2　連續調與半色調的 Lenna 灰階影像

（三）彩色半色調影像（Half-tone Color Image）

一般的半色調影像，都是由灰階影像直接產生，它僅有黑與白兩種色彩，而彩色連續調影像並無法直接使用相同的方法來轉換成半色調影像。它需先做分色處理，將影像分成青色（Cyan）影像、洋紅色（Magenta）影像、黃色（Yellow）影像三張影像，再把該三張影像轉換成半色調影像，最後再重新合成為一張新的影像，即為彩色半色調影像。它是僅有「紅色、黃色、綠色、青色、藍色、洋紅色、黑色、白色」八種顏色而組成的彩色影像，如圖 3.3（b）、圖 3.4（b）。



a.連續調　　b.半色調

圖 3.3　連續調與半色調的 Lenna 彩色影像

a.連續調

b.半色調

圖 3.4 經過放大後的圖 3.3

二、影像重疊的變化

一般的灰階半色調影像與單純的黑白影像僅只有黑色與白色兩種顏色。依視覺密碼的重疊概念，黑色會覆蓋白色。而彩色半色調影像是由「黑色、白色、青色、洋紅色、黃色、紅色、綠色、藍色」，共八種顏色所組成。依視覺密碼的重疊概念，黑色會覆蓋所有顏色，白色會被所有顏色覆蓋，青色與洋紅色重疊會變為藍色，青色與黃色重疊會變為綠色，洋紅色與黃色重疊會變為紅色，青色、洋紅色及黃色重疊會變為黑色，如圖 3.5。

圖 3.5 CMY 混色圖

而連續調影像上的色彩相當繁多，以一般常見的 8 位元灰階影像就有 2^8 種顏色，24 位元的彩色影像也有 2^{24} 種顏色，這類影像經過重疊後的變化是相當複雜的。也因此至今視覺密碼的研究中，並沒有直接採用連續調影像的研究。

三、連續調影像重疊方程式

朱正民等人[1]曾提過，連續調影像中，有著多種色階。以一張 8 位元灰階影像色來說。若 1 色階為白色，256 色階為黑色，而 128 色階與 128 色階重疊後，並非會得到 256 色階的黑色。它是有一個規則性的變化。

假設有一張像素值為 a 的透明影像，而我們眼睛接收到的則是一光線經過透明影像後，所剩餘的光線。因此我們假設把 x_i 當作光線未經過透明影像前的光線強度，而 x_o 為光線經過透明影像後所剩餘的強度。則：

$$x_o = x_i - \frac{x_i}{1} \times \frac{pixel}{2^n}, 0 < x_i \le 1, 0 \le x_o \le 1 \qquad (1)$$

其中 $pixel$ 為影像像素值，n 為影像色階的位元數。

若光線穿過影像前的強度 x_1 為最強的強度 1，當光線經過透明影像後剩餘的強度 x_2 ，此時我再將另一張像素值為 b 的透明影像與像素值為 a 的透明影像重疊，則我們眼睛接收到的則是一光線經過兩張透明影像後，所剩餘的光線 x_3 。而兩張透明影像的重疊像素值 c 則為：

$$c = 2^n - x_3 \times 2^n, 0 \le c \le 2^n, 0 \le x_3 \le 1$$

因：

$$x_1 = 1$$

$$x_2 = x_1 - \frac{x_1}{1} \times \frac{a}{2^n} = 1 - \frac{a}{2^n}$$

$$x_3 = x_2 - \frac{x_2}{1} \times \frac{b}{2^n} = \left(1 - \frac{a}{2^n}\right) - \left(1 - \frac{a}{2^n}\right) \times \frac{b}{2^n}$$

$$\therefore c = 2^n - \left[1 - \frac{a}{2^n} - \left(1 - \frac{a}{2^n}\right) \times \frac{b}{2^n}\right] \times 2^n \quad (2)$$

令 $n=0$ 或將（2）式除以 2^n 可得：

$$c = a + b - ab, 0 \le a \le 1, 0 \le b \le 1 \quad (3)$$

由（3）式可得：

$$b = \frac{c - a}{1 - a}, 0 \le a \le 1, 0 \le b \le 1 \quad (4)$$

依視覺密碼的製作原理，c 即為秘密影像的像素值，因此若我們可以採取某些方式來設定其中一張分享影像的像素值，便可利用公式（4）來推算出另一張分享影像的像素值。

肆、研究方法與實驗結果

一、研究方法

實驗我們採用最常見的 24 位元的彩色連續調影像，我們先將影像分解成三張僅有 C：青色、M：洋紅色、Y：黃色的單一種色素的連續調影像。該三張影像則分別為「青色連續調影像、洋紅色連續調影像、黃色連續調影像」，再將三張影像的顏色做交錯處理，其方法如表 4.1，經過交錯處理後產生三張基準影像，如圖 4.1。

表 4.1 基準影像顏色交錯方案對照表

方案	基準影像 1	基準影像 2	基準影像 3
方案 1	C	M	Y
方案 2	C	Y	M
方案 3	M	C	Y
方案 4	M	Y	C
方案 5	Y	C	M
方案 6	Y	M	C

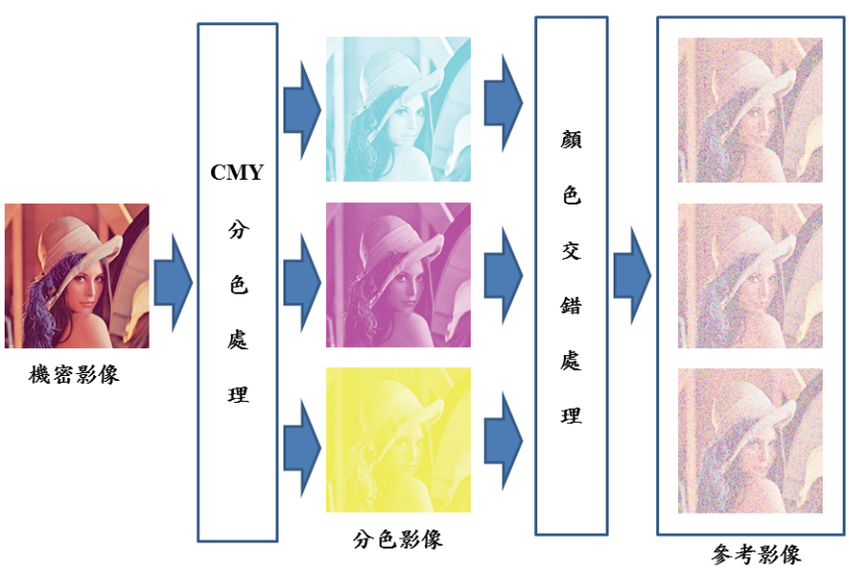


圖 4.1 產考影像製作流程

產生基準影像後，我們分別將三張基準影像來進行像素分解，而每張基準影像產生 4 張分享影像，其基準影像像素分解分產生享影像的方法如下：

1. 讀取基準影像之像素值，做為 c 值。
2. 隨機產生 1 個 50~100 的亂數，做為 a 值。
3. 當 c 值小於 a 值時。

則隨機選取一張分享影像存入 c 值，其餘三張分享影像，皆存入 255。

當 c 值大於 a 值時。

則將 a 值與 c 值同代入公式（3），計算 b 值。隨機選取兩張分享影像分別存入 a 值與 b 值，其餘的 2 張分影像則存入 255。

重復 1~3 的動作至結束。

由於直接產生的分享影像仍可查覺到 Lenna 的影像（如圖 4.2（a））。

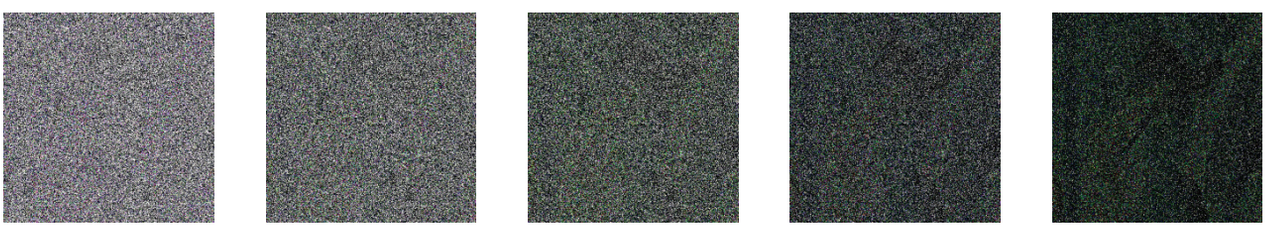
因此我們必需加入雜訊，其加入雜訊規則如下：

1、 讀入所有分享影像 C、M、Y 值。

2、 以自訂的機率產生雜訊。雜訊像素我們以分享影像的該位置的像素值之補色（即 255 減去原像素值）。

由於加入雜訊，雖會提高安全性，但也會降低還原影像的影像品質。因此，我們依不同的雜訊機率，分別為加入約 10%、20%’、30%、40%、50%“60%、70%、80%、90%雜訊。再加上無加入雜訊的分享影像，共 10 組分享影像（如圖 4.2），來探討安全性問題。

a. 無雜訊　b. 10%雜訊　c. 20%雜訊　d. 30%雜訊　e. 40%雜訊



f. 50%雜訊　g. 60%雜訊　h. 70%雜訊　i. 80%雜訊　j. 90%雜訊

圖 4.2　實驗的分享影像

二、安全性分析

由於我們所使用的影像為連續調影像，並無法像使用半色調技術所製做的分享影像一樣，直接去計算分享影像上的黑點與白點的分佈比例，來分析安全性。因此我們先將 Lenna 影像轉換成黑白影像，區分成黑色區域與白色區域（如圖 4.3），來計算兩個區域的像素平均值，統計後整理成表 4.2。

圖 4.3　Lenna 的黑白影像

表 4.2 區塊像素平均值分析表

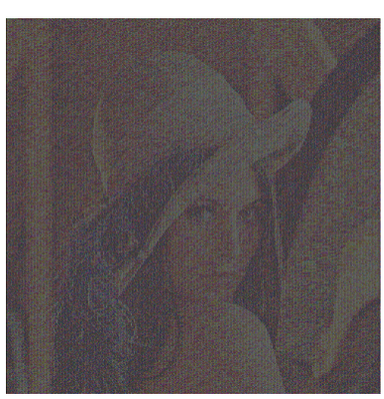
影像	無雜訊			約 10%雜訊			約 20%雜訊			約 30%雜訊			約 40%雜訊		
色層	C	M	Y	C	M	Y	C	M	Y	C	M	Y	C	M	Y
白色區域	250	241	241	223	219	213	198	193	193	174	173	168	149	147	147
黑色區域	239	230	235	214	212	208	192	188	190	170	171	164	147	147	147
色差值	11	11	6	9	7	5	6	5	3	4	2	4	2	0	0
影像	約 50%雜訊			約 60%雜訊			約 70%雜訊			約 80%雜訊			約 90%雜訊		
色層	C	M	Y	C	M	Y	C	M	Y	C	M	Y	C	M	Y
白色區域	124	125	124	100	102	102	75	79	79	51	56	57	26	31	36
黑色區域	125	125	126	103	104	104	80	83	82	58	63	61	35	38	42
色差值	1	0	2	3	2	2	5	4	3	7	7	4	9	7	6

依照正常人的視覺來看，在 8 位元的灰階影像或 24 位元的彩色影像上，像素值只要差距 8 以上，我們便可以感覺到色差，在表 5.1 中，無加入雜訊的分享影像，僅有 Y 色層（黃色色層）的像素值在 8 以下，因此我們可以在分享影像上輕易察覺到機密影像的輪廓。加入 10%雜訊後，各色層的色差值即有明顯的下降，但色差值仍接近 8，故我們在分享影像上雖無法輕易查覺到機密影像的輪廓，但若集中注意力仍可被察覺。而隨著雜訊的增加，各色層的色差也愈來愈折近 0，但雜訊從 60%開始，色差值又有增加的現像。因我們的雜訊並非是黑點或白點，而是該像素值的補色，也因此在雜訊機率大於 50%後，像素值的差距又會開始逐漸的增大，直到 90%的像素值色差又會與 10%的相近，也因此我們可以在 90%雜訊的分享影像上察覺到與 10%雜訊的分享影像相反色調的影像。

三、重疊影像比較

2008 年，Hsien-Chu Wu 等人[4]所提出的方法，是僅取奇數行或偶數行的像素來制作視覺密碼，因此這種作法本身就已有約 50%的雜訊。再加上加入的雜訊愈高，在分享影像重疊後，所得到的還原影像之影像品質也會隨著下降，甚至使機密影像的像素被雜訊所破壞，而使得重疊後法得到機密影像。基於此，我們僅取雜訊率 50%的重疊影像與 Hsien-Chu Wu 等人的方法來比較。

a. 我們的方法加入 50%雜訊



Hsien-Chu Wu 等人的方法

圖 5.2 重疊影像比較

如圖 5.2 Hsien-Chu Wu 等人[4]的方法所制作的重疊影像，由於雜訊是固定於奇數行或偶數行（機密影像藏於奇數行時，則偶數行為雜訊），因我們眼睛在接收彩色信號會自動補償顏色，而此做法的機密影像洽好皆位於黑色雜訊中間，因此照成重疊影像明顯的偏於灰暗。而我們的做法，雜訊是採用隨機散佈，相對的機密影像亦是隨機散佈，固我們的重疊影像明顯比 Hsien-Chu Wu 等人的重疊影像明亮。

伍、結論

本論文有別於以往的研究，我們直接採用了一般的數位連續影像來製作視覺密碼，有效的保留續調影像經過半色調處理或擴展處理後，所失去的影像品質。並且同時擁有傳統視覺密碼的優點，可直接利用重疊，來解讀秘密內容。不僅如此，連續調影像同時也具有相當大的藏密範圍，因此我們的研究亦可以結合其它的藏密技術來達到驗証或防偽…等功能。

參考文獻

[1] 朱正民，黃立仁，黃賦宇，” 連續調灰階影像視覺秘密分享，”工程應用技術學刊，第一卷，第一期，2012 年 2 月，頁. 53-63

[2] Ateniese, G., Blundo, C., De Santis, A., and Stinson, D. R., “Constructions and Bounds for VisualCryptography”, in *23rd International Colloquium on Automata, Languages and Programming （ICALP ‘96）*, LNCS 1099, 1996a: pp.416-428.

[3] Blundo, C., De Bonis, A., and De Santis, A., “Improved Schemes for Visual Cryptography”, *Designs, Codes and Cryptography* （24）, 2001: pp. 255-278.

[4] H.C.Wu, H.C.Wang and R.W.Yu, “Color Visual Cryptography Scheme Using Meaningful Shares,” Eighth International Conference on Intelligent Systems Design and Applications, 2008.

[5] Naor, M., and Shamir, A., “Visual Cryptography,” in *Advances in Cryptology-EUROCRYPT ’94*, LNCS 950, Springer-Verlag, 1995, pp. 1-12.

[6] Verheul, E. R., and van Tilborg, H. C. A.,“Constructions and Properties of *k* out of *n*Visual Secret Sharing Schemes”, *Designs, Codes and Cryptography* （11:2）, 1997: pp. 179-196.

[7] Y. C. Hou, “Visual cryptography for color images,” *Pattern Recognition*, Vol. 36, pp.1619-1629, 2003.

Journal of Applied Engineering Technology
Vol.1 No.2

The Numerical Simulation for Surface Structure Effect in the anode channel of PEMFC

Chao-Chung Liu[1] Guan-Ru Cheng[2] Chi-Lang Huang[3]

[1]Department of Electrical Engineering and Energy Technology, Chung Chou University of Science and Technology

[2,3]Graduate School of Engineering Technology, Chung Chou University of Science and Technology

Abstract

The main purpose of this study is to calculate the transport phenomena of fuel gas in the anode channel of proton exchange membrane fuel cells （PEMFC）. In this code, the structured single-block and staggered grid system are adopted for discretization of the space domain, while the finite volume method is applied to solve iteratively the governing equations of mass and momentum. The coupling among the velocities and pressure is handled by PISO methods. The transport characteristics of flow field in the anodic Channel are presented with the variant parameter. Furthermore, it is investigated the relation between the electric current density and surface structure effect in anode channel.

Keywords: PEMFC, Anode Channel, Surface Structure