邱佩玲、李開暉（2013），『以自然影像為基礎的彩色機密影像分享機制』，
資訊管理學報，第二十卷，第一期，頁77-96。

以自然影像為基礎的彩色機密影像分享機制

邱佩玲
銘傳大學風險管理與保險學系

李開暉*
銘傳大學資訊工程學系

摘要

傳統視覺機密分享機制產生雜點分享圖，藉以安全地分享機密影像。但雜點分享圖的外觀難以辨識，造成管理分享圖困難。此外，雜點分享圖傳遞過程中，極容易招致被偵測與攔截的風險。前人所提擴充型視覺機密分享機制，在雜點分享圖上添加有意義的偽裝圖，以解決管理困難的問題，但是大都伴隨更嚴重的像素擴張現象，且無法有效降低被偵測與攔截的風險。因此，本文提出以自然影像為基礎的機密分享機制，以數張任意選取的自然影像和 1 張傳統視覺密碼的雜點分享圖為媒介，傳遞 1 張全彩的數位形式機密影像。本文所提機制具有極高的友善度，同時在加密的過程不需竄改自然影像內容，能有效的降低傳輸風險且無像素擴張，解密時該彩色機密影像也可以完全還原。

關鍵詞：視覺機密分享、擴充型視覺機密、自然影像、傳輸風險

* 本文通訊作者。電子郵件信箱：plchiu@mail.mcu.edu.tw
2011/08/12 投稿；2012/02/07 修訂；2012/06/13 接受

Chiu, P.L. and Lee, K.H. (2003), 'A Color Secret Image Sharing Scheme Based on Natural Images', *Journal of Information Management*, Vol. 20, No. 1, pp. 76-96.

A Color Secret Image Sharing Scheme Based on Natural Images

Pei-Ling Chiu
Department of Risk Management and Insurance, Ming Chuan University

Kai-Hui Lee*
Department of Computer Science and Information Engineering, Ming Chuan University

Abstract

Conventional visual secret sharing (VSS) schemes generate noise-like random pixels on shares to hide secret images. However, these schemes suffer from two problems, one related to security and one related to management. First, the noise-like shares arouse suspicion, which leads to security problems for participants who are involved in a VSS scheme. Second, participants cannot visually identify each share, especially if they hold more than one share simultaneously, which leads to the management problem. To address the management problem, previous researchers developed extended visual cryptography schemes that add a meaningful cover image on each share. Generally, however, these approaches introduce a more serious pixel expansion problem than conventional VSS schemes. In addition, there are still many noise-like pixels on the shares, which do not effectively reduce the security problems. This paper proposes a natural-image-based VSS scheme that can share a color secret image over n-1 arbitrary natural images and one noise-like share image. Instead of altering the contents of the natural images, the encryption process extracts feature images from each natural image. Then, the encryption process divides and distributes the color secret image among these feature images and generates a noise-like share. In such a way, the unaltered natural images are innocuous, thus greatly reducing the security problem. When the n-1 natural images and the share image are received, the n-1 feature images can be extracted and the secret image can be recovered completely by combining the feature images and the share image. Experimental results indicate that the proposed approach is an excellent solution for solving the security and management problems. Moreover, the proposed approach avoids the pixel expansion problem and makes it possible to totally recover the secret images.

Keywords: Visual secret sharing, Extended visual cryptography scheme, Natural images, Transmission risk

* Corresponding author. Email: plchiu@mail.mcu.edu.tw
2011/08/12 received；2012/02/07 revised；2012/06/13 accepted

壹、導論

視覺密碼（Visual Cryptography Scheme, VCS）可以將機密影像加密成 n 張分享圖，一群參與者分別持有 1 張或多張分享圖，沒有人可以從任意 k（$1 \le k < n$）張分享圖取得訊息，但當 n 張分享圖疊合，即可還原機密影像（Naor & Shamir 1995）。而機密本身也可以定義為許多種類，如影像、手寫文件或相片等。此種分享與傳遞機密的方法也稱為視覺機密分享機制（Visual Secret Sharing Scheme, VSSS）。

傳統的視覺密碼學所產生的分享圖，由一些隨機且無意義的像素組成，雖符合安全性的需求，但也帶來兩個顯著的缺點：首先是傳輸的風險極高。攜帶與傳遞隨機且無意義的分享圖，極易招致懷疑與攔截，導致傳遞者與分享圖本身的風險，增加傳遞機密的失敗機率。其次是友善程度不足。由於分享圖上無任何可供辨識的資訊，會導致分享圖的持有者在管理上的極大不便，尤其是當所持有的分享圖數量較多時。

針對友善程度不足的問題，已有學者提出一些解決方案（Ateniese et al 2001; Fang 2008; Klein & Wessler 2007; Wang et al 2009; Yang & Chen 2008）。這些研究除了在分享圖上分享機密影像外，並為每 1 張分享圖加上不同偽裝影像（cover images）以利於辨識，可以解決分享圖友善程度不足的問題，增加管理上的便利性。例如，Ateniese 等（2001）學者發展了適用於一般存結構（General Access Structures, GASs）的擴充型視覺密碼機制（Extended Visual Cryptography Scheme，EVCS）。Klein 與 Wessler（2007）也提出一個可在給定對比值的情況下，建構擴充型視覺密碼機制的簡單方法。Wang 等（2009）則提出一個較一般化的 (k, n)－EVCS 建構方法。以上這些學者除了 Wang 等之外，所提的方法都是針對黑白二元的機密影像，雖能解決分享圖管理不便的問題，卻也帶來了像素擴張與機密影像還原品質不佳的缺點。Hou（2003）提出將彩色影像分離成不同的色平面，再使用傳統視覺密碼的編碼方式，建構(2, 2)彩色視覺機密分享機制。爾後，Shyu（2009）和 Yang 與 Chen（2008）等分別提出適用於(n, n)與(k, n)彩色視覺機密分享機制。Fang（2008）和 Chen 與 Lee（2009）的研究分別針對灰階與彩色的數位型式機密影像，發展出加入偽裝影像的方法，增加分享圖管理的便利性。

為了進一步改善分享圖的友善度，Tsai、Chen 與 Horng（2008）等提出將無意義分享圖轉為灰階或彩色的有意義分享圖的方法，可以適用於以密碼本為核心技術的傳統視覺密碼學，該方法可以運用於現存的視覺機密分享。但美中不足的是，黑色機密像素無法完全還原，還原影像還留下清晰的偽裝影像痕跡。為了讓偽裝影像不要干擾還原影像品質，Chen 與 Tsao（2011）利用互補的偽裝影像使得還原影像不留有偽裝影像痕跡，其缺點是對偽裝影像的限制以及還原影像品質還有待

改善等。

最近有一些視覺機密分享相關文獻探討有意義的半色調分享圖（De Santis & Masucci 2007; Kang et al 2011; Lou et al 2011; Nakajima & Yamaguchi 2002; Wang & Arce 2010; Wu et al 2008; Zhou et al 2006），強調分享圖的視覺品質甚於還原影像的品質。灰階或彩色的偽裝影像必須先轉換為半色調，每個原始像素編碼為 m 個次像素的半色調細胞（halftone cells），m 是半色調像素擴張（halftone pixel expansion）因子。Nakajima 與 Yamaguchi（2002）率先提出用兩張自然影像當分享圖，疊合成為另 1 張自然機密影像的(2, 2)-VCS。他們利用可以隨意安排次像素（sub-pixel）位置的半色調演算法設計編碼矩陣，使之疊合產生機密影像。接著，Zhou 等（2006）人將 1 張二元機密影像的分享像素，利用 void and cluster 演算法藏於兩張互補的半色調分享圖的半色調次像素中。並利用參與者可能須攜帶 1 張以上的分享圖而擴展到一般化存取結構（GASs）。Liu 與 Wu（2011）提出嵌入式擴充型視覺密碼機制，不須使用互補的偽裝影像。Kang 等（2011）人將研究延展到彩色的半色調分享圖。這些文獻所發展的半色調化與編碼演算法，必須在分享圖品質與像素擴張之間，或者在分享圖品質與還原機密影像品質之間做取捨。

此外，Tsai、Chen 與 Horng（2009）和 Wu、Thien 與 Lin（2004）分別使用灰階（半色調）/ 全彩影像作為偽裝影像，透過資訊隱藏技術（Steganography）將機密影像隱藏偽裝影像中，雖然增加分享圖的友善度，但依舊無法避免分享圖被偵測的風險。

上述研究雖然能使分享圖變得更友善，更易於管理，但一方面友善的分享圖帶來像素擴張與還原影像品質降低的缺點，另一方面這些高品質的分享圖仍有著被偵測的風險，對於保護傳遞機密影像的人或機密本身，仍有改進的必要。換言之，現存的研究仍無法有效的降低傳輸風險。因此本文提出一個以自然影像為基礎的視覺密碼分享機制（Natural-image-based VSS scheme, NVSS scheme），希望能以 $n-1$ 張完全未經竄改的全彩自然影像和 1 張傳統視覺密碼的分享圖為媒介，傳遞 1 張數位形式的全彩機密影像。本文所提的機制具有極高的友善度，能提高管理的便利性，並可降低傳輸風險，有效地保護傳遞機密者與機密本身。同時解決了像素擴張的問題，且彩色的機密影像得以完全還原。

本文其餘章節安排如下：第貳節介紹所提的 NVSS 方案與演算法。第參節將透過實驗評估所提方案的安全性與演算法的效能。第肆節總結本文。

貳、NVSS 機制

一、$((n-1, 1), n)$–NVSS 模型

本研究以降低分享圖傳輸風險為主要目標，基本假設如下：

(1) 分享圖的數量愈多，傳輸風險愈高。
(2) 具偽裝影像的分享圖，比雜點分享圖有著較低的傳輸風險。
(3) 偽裝影像的品質越高，分享圖的傳輸風險越低。
(4) 無失真的全彩影像比半色調影像具有更高的顯示品質。
(5) 完全未經竄改的自然影像具有最低的傳輸風險。

基於以上假設，本文提出一個以自然影像為基礎的視覺密碼分享機制，記為 $((n-1,1),n)$－NVSS 架構，此架構包含任意選取的 $n-1$ 張自然影像與 1 張傳統視覺密碼的雜點分享圖，為分享全彩機密影像的媒介。這些自然影像可以是彩色或灰階的風景相片、家庭生活相片、廣告圖片，甚至是網際網路上公開可以取得的圖片，加密的過程僅萃取自然影像中的特徵，而不會變更任何自然影像的內容。這些未經任何變更的自然影像分享圖，可透過不知情的第三者、自然影像所有人或藉由網際網路公開傳遞，因此極不容易招致懷疑，即便被攔截，在未達解密門檻的情況下，也無從證實這些自然影像的可疑性，具有非常高的安全性。另 1 張傳統視覺密碼的雜點分享圖，係根據 $n-1$ 張自然影像的特徵與機密影像產生，可交由訓練有素的人員或一個高度安全的傳輸通道傳遞。

當分享的數量 n 增加，依據假設(1)，傳統 (n,n)－VCS 機制的傳輸風險將隨之急劇升高。反觀本文所提模型，當分享的數量 n 增加時，雜點分享圖仍只有 1 張，未經竄改的自然分享圖數量雖與 n 成正比，但因自然影像具有非常高的安全性，所以分享數量 n 增加，此模型的傳輸風險增加仍極為有限。

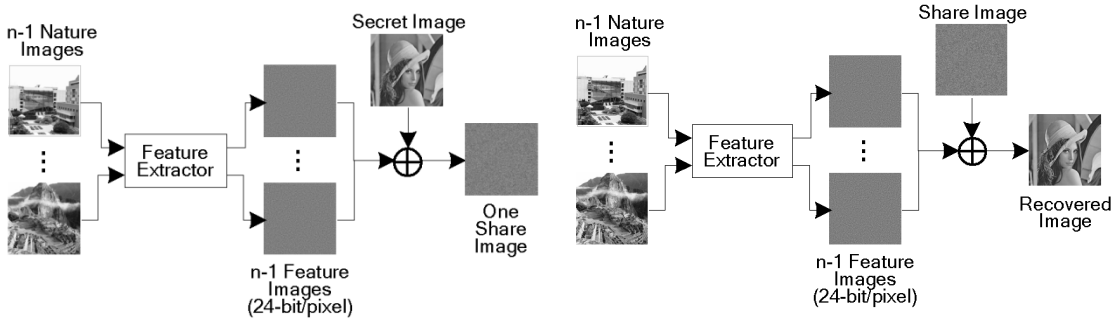
現有的視覺機密分享機制採用的分享圖，大致包括雜點分享圖、二元偽裝影像分享圖以及半色調偽裝影像分享圖等三類，又以半色調偽裝影像的品質最佳。而本研究提出以全彩自然影像為分享圖，其影像品質更勝於半色調偽裝影像分享圖。依據假設(2)與(3)，全彩自然影像分享圖的傳輸風險顯然低於現有的三種分享圖。依據假設(4)與(5)，此研究所提 $((n-1,1),n)$－NVSS 模型傳遞 $n-1$ 張未經竄改的自然影像的風險極低，使得傳輸成本大大降低。唯有另 1 張傳統雜點分享圖須藉由高度安全的傳輸通道傳遞。當傳輸成本有限之下，相較於現有傳統 VCS 機制，所提 NVSS 模型因具有未竄改之自然分享圖，可有效降低機密影像分享機制的傳輸風險。

二、加 / 解密流程

本文所提的 $((n-1,1),n)$－NVSS 方案的加密流程（如圖 1(a)所示），主要分為自然影像的特徵萃取（feature extraction）與加密（encryption）兩個階段。影像特徵萃取階段係將 $n-1$ 張自然影像分別萃取出 24 個二元的特徵矩陣（feature matrices），並將其組合成 1 張 24-bit/pixel 的特徵影像（feature image），爾後在加

密階段根據這$n-1$張特徵影像與機密影像作互斥或（XOR）運算，便可產生 1 張 24-bit/pixel 的雜點分享圖。這$n-1$張的自然影像分享圖（以下簡稱自然分享圖）與經運算產生的 1 張雜點分享圖，即為$((n-1,1),n)$－NVSS 方案的n張分享圖。

俟收到 n 張分享圖後，解密端便可同樣地將$n-1$張自然影像分別萃取出 24-bit/pixel 的特徵影像，再將這$n-1$張特徵影像與收到的 1 張雜點分享圖進行解密，便可還原機密影像，解密流程則如圖 1(b)所示。自然影像特徵萃取方法以及加 / 解密演算法，分別說明於後。



(a) 加密流程 (b) 解密流程

圖 1：$((n-1,1),n)$－NVSS 加 / 解密流程

三、自然影像特徵萃取

首先介紹如何從自然影像中萃取出一個二元的特徵矩陣。為了便於說明，以下先定義一些符號。令自然影像、機密影像的影像大小為$w\times h$，自然影像切割區塊大小為8×8 pixels。

- N_α表示自然分享圖α，$1\le\alpha<n$。
- (x,y)表示像素座標，$1\le x\le w$，$1\le y\le h$。
- (x_β,y_β)表示在區塊β的左上角像素座標。
- $p_{\alpha,\varphi}^{x,y}$表示自然分享圖α，在(x,y)座標顏色φ的像素值，$\varphi\in\{R,G,B\}$。
- $H_\alpha^{x,y}$為N_α中(x,y)座標的 RGB 像素值總和，其中

$$H_\alpha^{x,y}=p_{\alpha,R}^{x,y}+p_{\alpha,G}^{x,y}+p_{\alpha,B}^{x,y} \tag{1}$$

- M_α^β表示區塊β中所有像素值（即$H_\alpha^{x_\beta,y_\beta},\ldots,H_\alpha^{x_\beta+7,y_\beta+7}$）的中位數值（median）。
- F_α為N_α的特徵矩陣，元素$f_\alpha^{x,y}$為(x,y)座標的特徵值，$f_\alpha^{x,y}=1$表示N_α在(x,y)座標的像素特徵被解釋為黑像素（black pixel），$f_\alpha^{x,y}=0$則為白像素。

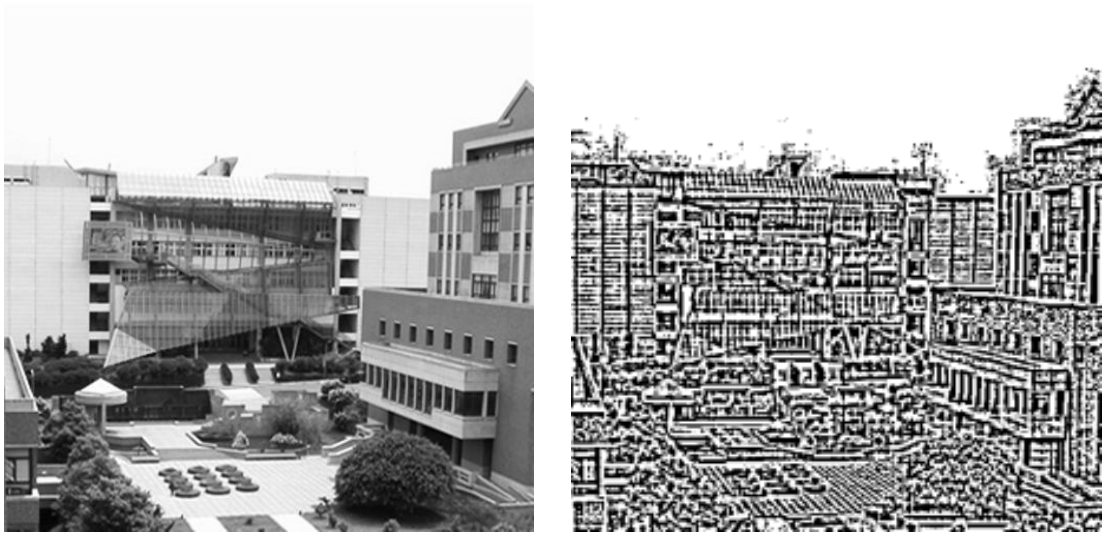
特徵值 $f_{\alpha}^{x,y}$ ，$x_{\beta} \le x \le x_{\beta}+7$ ，$y_{\beta} \le y \le y_{\beta}+7$ ，的萃取方法如下：

$$f_{\alpha}^{x,y} = \begin{cases} 1, & H_{\alpha}^{x,y} < M_{\alpha}^{\beta} \\ 0, & otherwise. \end{cases} \tag{2}$$

表 1：特徵值萃取演算法-FE1

Procedure FE1 ( )
Input: $N_1, ..., N_{n-1}$
Output: $F_{\alpha}, 1 \le \alpha < n$
1. $\forall 1 \le \alpha < n$, divide N_{α} into t blocks with 8×8 pixels
2. $\forall 1 \le \alpha < n$, $\forall 1 \le \beta \le t$, repeat Steps 3~5
3. $\forall x_{\beta} \le x \le x_{\beta}+7$, $y_{\beta} \le y \le y_{\beta}+7$, calculate $H_{\alpha}^{x,y}$ by Equation (1)
4. Calculate M_{α}^{β}
5. $\forall x_{\beta} \le x \le x_{\beta}+7$, $y_{\beta} \le y \le y_{\beta}+7$, calculate $f_{\alpha}^{x,y}$ by Equation (2)
6. $\forall 1 \le \alpha < n$ ，output F_{α}

表 1 為本文第一個自然影像特徵萃取方法-FE1 演算法。演算法的步驟 2 是加總一個區塊中的所有像素值，步驟 4 計算此區塊的像素中位數值，步驟 5 求此區塊的每一像素的特徵。步驟 2～5 是 FE1 演算法的主迴圈，對輸入影像的每一像素進行評估，並決定其特徵值，因此演算法 FE1 的時間複雜度為 $O(nhw) \approx O(hw)$ 。



(a) 自然影像 N_1　　(b) N_1 的特徵影像

圖 2：FE1 所萃取出的影像特徵

我們先以圖 2(a)的自然影像當作輸入 N_1，觀察 FE1 的效果。圖 2(b)是由 N_1 的特徵矩陣 F_1 所得的黑白特徵圖。圖 2(b)的結果顯示，單純以方程式(1)為判別影像特徵基準，會造成特徵圖上的黑像素分布不均勻。進一步分析可知黑像素分布不夠隨機的原因有二：其一，自然影像經常會有大片區域出現相同（或相近似）像素值的情形，如 N_1 的天空部分出現大面積的白色像素，因此導致特徵圖上也出現相同面積的白色特徵像素。其次，由於自然影像像素值會發生叢集的現象，使得特徵圖上容易出現紋理。透過互斥或的加密運算，這些特徵圖上的紋理可能出現在雜點分享圖上，為了安全上的理由，本文發展第二個特徵值萃取演算法-FE2，來解決上述兩個問題。

特徵值萃取演算法二（FE2）將特徵萃取階段分成三個模組（如圖 3 所示），分別對 1 張自然影像進行像素重新排列（permutation）、像素特化（specialization）和特徵萃取等程序，以萃取出一個不具原始自然影像紋理，且黑 / 白像素分布均勻的二元特徵影像。為達此目的，FE2 引入一個虛擬隨機函數 G，函數 G 所使用的隨機數產生器及隨機數種子皆為機密的一部分。

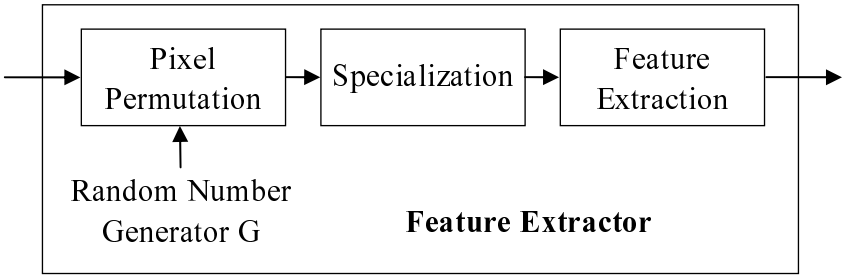


圖 3：修正後的特徵萃取器包含三個模組

以像素重新排列為基礎的方法（permutation-based methods）已經成功的運用到影像的加密（Jeyamala et al 2010; Liu & Wang 2010; Xinpeng 2011）。本文所提的 NVSS 機制藉助像素重新排列方法來改善特徵萃取流程，以取得虛擬隨機化（pseudo-randomized）的特徵影像。對於原始的自然影像的像素在空間上具有的叢集現象，特徵萃取流程以像素重新排列模組來消除此現象。假設所採用的原始自然影像是全彩影像，每個像素以 24 位元深度表紅、綠、藍（RGB）三元素。加解密階段，像素交換模組分別針對 R、G、B 三個色平面，隨機挑選成對的像素位置，互換自然影像像素元素。而交換像素的隨機序列是由亂數產生器 G 決定，交換次數與隨機數種子皆為機密的一部分。若交換次數夠多，處理過的自然影像紋理可完全消失，就像 1 張無意義雜點圖，消除與原始影像的關聯。

此外，只要加 / 解密雙方約定，本機制可使用在公眾領域（public domain）任意取得的自然影像進行加密。為降低攻擊者使用外觀相似的自然影像攻擊此機制，本研究進一步提出一個像素特化（specialization）的程序，加強自然影像相鄰像素的關聯性，使自然影像更具特殊性，以提高本機制的安全性。自然分享圖 N_α 在顏色 φ 平面上，座標 (x, y) 的像素值 $p_{\alpha,\varphi}^{x,y}$ 可依序被特化如下：

$$p_{\alpha,\varphi}^{x,y} \leftarrow p_{\alpha,\varphi}^{x-1,y} \oplus p_{\alpha,\varphi}^{x,y}, \tag{3}$$

亦即透過簡單的互斥或運算，建立相鄰像素的關聯。

自然影像經重新排列像素與像素特化（specialization）程序後，再使用演算法 FE1 即可萃取出每 1 張自然影像的二元像素特徵矩陣。

表 2：特徵值萃取演算法-FE2

Procedure FE2 ( )
Input: $N_1, \ldots, N_{n-1}, t_p$
Output: F_α, $1 \le \alpha < n$。
1. $\forall 1 \le \alpha < n$, $\forall \varphi \in \{R, G, B\}$, repeat Steps 2~4 t_p times
2. Randomly select the first coordinates (x_1, y_1), $x_1 \in [1, w]$, $y_1 \in [1, h]$.
3. Randomly select the second coordinates (x_2, y_2), $x_2 \in [1, w]$, $y_2 \in [1, h]$.
4. Exchange values of $p_{\alpha,\varphi}^{x_1,y_1}$ and $p_{\alpha,\varphi}^{x_2,y_2}$
5. $\forall 1 \le \alpha < n$, $\forall \varphi \in \{R, G, B\}$, perform Steps 6~9
6. $p_{prev} \leftarrow 0$
7. $\forall 1 \le y < h$, $\forall 1 \le x < w$, perform Steps 8 and 9
8. $p_{\alpha,\varphi}^{x,y} \leftarrow p_{prev} \oplus p_{\alpha,\varphi}^{x,y}$
9. $p_{prev} \leftarrow p_{\alpha,\varphi}^{x,y}$
10. Call procedure FE1 ( )

特徵值萃取演算法-FE2，如表 2 所列。FE2 的步驟 1~4 是對每 1 張自然影像的 R、G、B 三個顏色平面各隨機進行 t_p 次的像素值交換，亦即圖 3 中的 pixel permutation 程序。步驟 6~9 進行像素特化。步驟 10 是呼叫 FE1 程序，進行一個位元的特徵萃取。

演算法 FE2 步驟 2~4 的時間複雜度是 $O(t_p)$。步驟 6~9 的時間複雜度是 $O(hw)$。步驟 10 的時間複雜度也是 $O(hw)$。因此演算法 FE2 的時間複雜度為 $O(hw + t_p)$。

四、加 / 解密演算法

本文所提$((n-1,1),n)$–NVSS 方案可透過$n-1$張自然影像與 1 張雜點分享圖加密 1 張 24 位元全彩機密影像。假設對一影像我們稱此影像所有像素的同一位元為一位元平面（bit-plane），則 24 位元全彩影像共有 24 個位元平面。因此對全彩影像加密，每 1 張特徵影像與雜點分享圖都需擴充為 24-bit/pixel。特徵影像的每個位元平面都是相對於彩色機密影像同一位元平面的二元特徵矩陣。對於機密影像的每一位元平面，在加密（解密）前，均須先萃取$n-1$張自然影像的特徵矩陣，再將機密圖（分享圖）的該位元平面與所萃取出的$n-1$特徵矩陣作 XOR 運算（以下以運算子$\oplus$表示之），便可產生此位元平面的分享圖（還原影像）。因此，要加密（解密）1 張全彩的機密影像，就必須分別對 24bits 的像素值進行加密（解密）。

加 / 解密演算法如表 3 所列，$((n-1,1),n)$–NVSS 加 / 解密演算法所使用的影像均為 24-bit/pixel 的全彩影像。演算法所使用的符號定義如下：

- S為輸入影像，S_φ表示S在顏色φ平面的影像元件，$\varphi \in \{R,G,B\}$。
- $\overline{S}$為輸出影像，$\overline{S}_\varphi$表示$\overline{S}$在顏色φ平面的影像元件，$\varphi \in \{R,G,B\}$。
- FI_α為自然影像N_α的一個二元特徵影像，$FI_{\alpha,\varphi}$表示在顏色φ平面所有二元特徵影像之集合，$\varphi \in \{R,G,B\}$。$FI_{\alpha,\varphi,i}$表示$FI_{\alpha,\varphi}$中i–th 位元的二元特徵影像，$0 \le i \le 7$，$FI_{\alpha,\varphi,i} \in \{0,1\}$。
- ρ為隨機數產生器 G 所使用的隨機數種子。

步驟 1 使用隨機數種子ρ初始化隨機數產生器 G，加 / 解密端均需使用相同的種子，以便得到相同的虛擬隨機序列。步驟 2 初始化特徵影像。步驟 3~14 是主要迴圈，用以對每 1 張自然影像進行 24 個二元特徵值的萃取。每一次萃取特徵值，均須呼叫程序 FE2，重新排列（re-permute）自然影像上的像素，使得 24 個二元特徵矩陣皆不相同。步驟 15 即加 / 解密階段，直接使用互斥或運算疊合輸入影像 S 與所得的特徵影像FI_1、…、FI_{n-1}。對全彩影像而言，加 / 解密演算法的主迴圈呼叫演算法 FE2 共 24 次，因此演算法的複雜度是$O(24(hw+t_p)) \approx O(hw+t_p)$。

$((n-1,1),n)$–NVSS 架構加 / 解密演算法適用於加密與解密，加解密流程的參數可設定如下：

- 加密流程：輸入影像為$n-1$張自然影像與 1 張機密影像，輸出則為分享圖。
- 解密流程：輸入影像為$n-1$張自然影像與 1 張分享圖，輸出則為還原影像。

從上述的演算法可發現，加密的過程中，自然影像上每一像素的資料，僅被萃取成一個位元的特徵值，用以加密一個機密位元；而分享圖上的每一像素，則是根據機密影像上的每一像素與特徵矩陣上相對的特徵值，直接運算而得。因此不論是特徵圖或分享圖，均無像素擴張問題。同理，解密的過程也不會引起任何的擴張。從以上討論可知，本文的$((n-1,1),n)$–NVSS 方案，並不會帶來像素擴張。

表 3：$((n-1,1),n)-$NVSS 架構之加 / 解密演算法

Input: S, $N_1, \ldots, N_{n-1}$, ρ

Output: $\overline{S}$

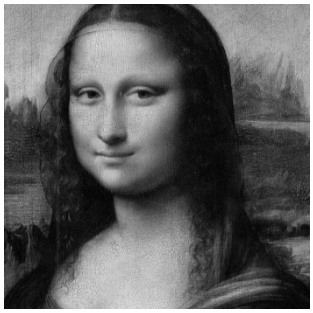
1. Initialize the random number generator G by the seed ρ
2. $\forall 1 \le \alpha < n$, $\forall \varphi \in \{R, G, B\}$, $\forall 0 \le i \le 7$, $FI_{\alpha,\varphi,i} \leftarrow 0$
3. **For** $i \leftarrow 0$ to 7
4. **Begin**
5. **Call** procedure FE2 ( )
6. **For** $\alpha \leftarrow 1$ to $n-1$
7. $FI_{\alpha,R,i} \leftarrow F_\alpha$
8. **Call** procedure FE2 ( )
9. **For** $\alpha \leftarrow 1$ to $n-1$
10. $FI_{\alpha,G,i} \leftarrow F_\alpha$
11. **Call** procedure FE2 ( )
12. **For** $\alpha \leftarrow 1$ to $n-1$
13. $FI_{\alpha,B,i} \leftarrow F_\alpha$
14. **End For**
15. $\forall \varphi \in \{R, G, B\}$, $\overline{S}_\varphi \leftarrow S_\varphi \oplus FI_{1,\varphi} \oplus \ldots \oplus FI_{n-1,\varphi}$
16. **Output** $\overline{S}$

參、實驗結果與討論

本節將以實例展示所提$((n-1,1),n)-$NVSS 方案與加 / 解密演算法的效能。我們以$((4,1),5)-$NVSS 方案為例，4 張 24 位元的全彩自然分享圖（圖 4(a)~(d)所示）與 1 張 24 位元的全彩機密影像（圖 4(e)）為實驗標的。實驗所用的自然分享圖及機密影像大小為512×512像素。

(a)自然分享圖 N_1

(b)自然分享圖 N_2



(c)自然分享圖 N_3

(c)自然分享圖 N_4

(d)機密影像

圖 4：((4, 1), 5) – NVSS 方案實驗用的自然分享圖與機密影像

一、實驗 I：特徵影像的觀察

本節透過實驗，觀察在不同的像素交換次數（t_p）下，像素重新排列後自然影像的像素之隨機程度，以驗證演算法 FE2 的效能。圖 5 是使用 FE2 所得特徵影像 FI_1 上相鄰像素的垂直相關性（correlation）分析的結果。圖 5 顯示像素的垂直相關性會隨著排列次數的增加而迅速降低，亦即自然影像的紋理愈顯模糊。當 $t_p = 0.1A$，$A = h \times w$，垂直相關性約為 0.63，$t_p = A$ 時，像素間的相關性就已低於 0.02，重新排列後的自然影像的像素已顯得相當地隨機。特徵影像 FI_1 上相鄰像素數的水平相關性與圖 5 的結果幾乎是一致的。

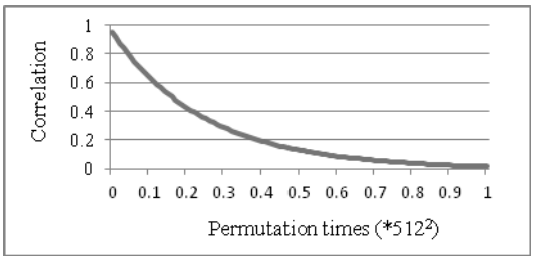
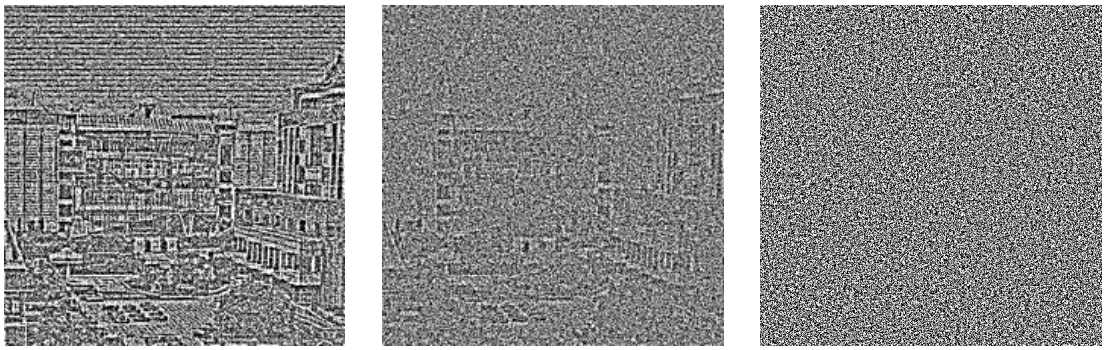


圖 5：特徵影像 FI_1 垂直相鄰像素關聯性



(a) $FI_1(t_p = 0.1A)$ (b) $FI_1(t_p = 0.5A)$ (c) $FI_1(t_p = A)$

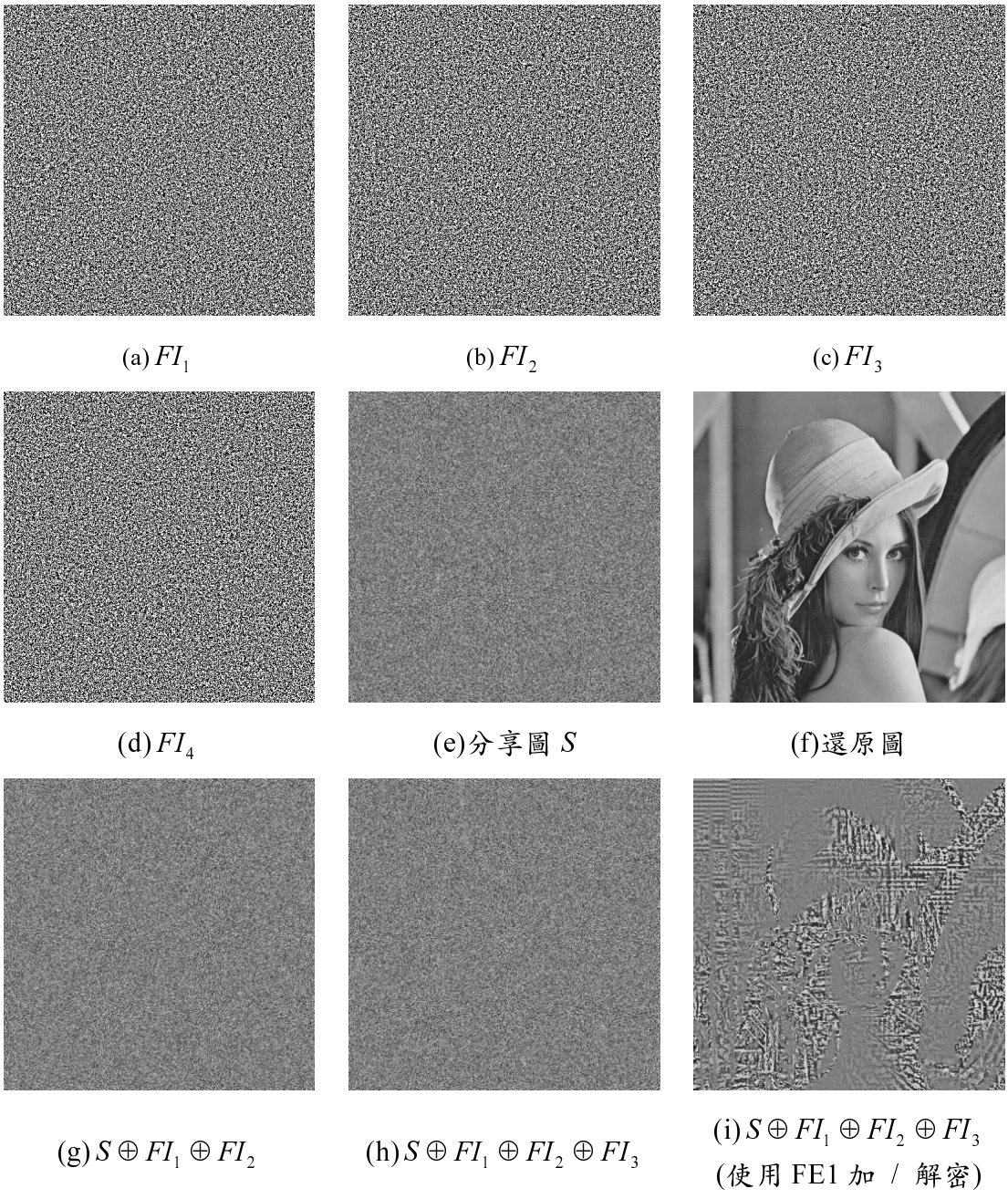
圖 6：FE2 所萃取出 N_1 的特徵影像。($A = h \times w$)

圖 6 為圖 2(a)的自然影像使用演算法 FE2 所萃取出的二元特徵影像。圖 6 顯示隨著像素交換次數的增加，所萃取出的特徵影像就顯得愈隨機。尤其是，原本圖 2(b)的特徵影像上方的大片白色像素，在圖 6(b)與(c)中已被隨機的黑點所取代，顯見演算法 FE2 的有效性。

二、實驗 II：加解密結果展示

圖 7 為使用圖 4 的 4 張自然影像與機密影像加 / 解密的部分結果，像素交換次數（t_p）設為 $h \times w$ 次。圖 7(a)~(d)為 4 張自然分享圖的特徵影像。圖 7(a)~(d)的特徵影像顯得相當隨機，可見演算法 FE2 對任何自然影像均為有效。從這些隨機的特徵影像所產生的分享圖（圖 7(e)）上，無法以肉眼看出任何規則或與機密圖有關的紋理，可印證分享圖的安全性。圖 7(f)則為被完美還原的還原圖。

圖 7(g)與(h)為未達解密條件的解密結果，因限於篇幅我們僅列出一部分。圖 7(g)與(h)的疊合影像中，完全無任何紋理出現。反觀圖 7(i)的疊合圖可發現，由於使用演算法 FE1 加密，無法完全消除特徵圖的紋理（如圖 2(b)所示），使得圖 7(i)的疊合圖在未達解密條件的情況下，即呈現部分紋理，造成洩密風險，而圖 7(h)的疊合圖則無此顧慮。此一對照進一步的印證，所提演算法 FE2 的安全性。



(a) FI_1 (b) FI_2 (c) FI_3

(d) FI_4 (e)分享圖 S (f)還原圖

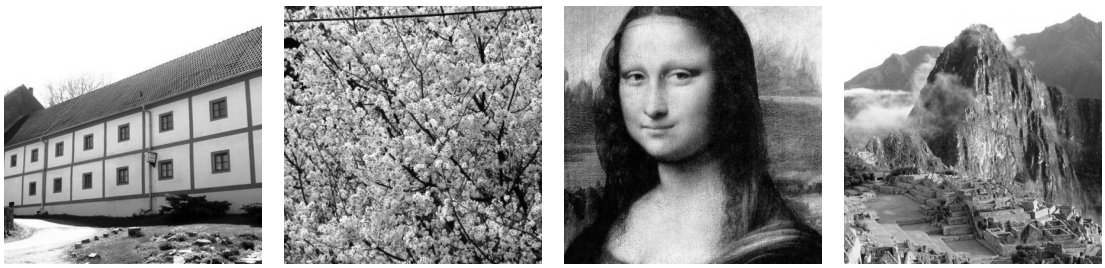
(g) $S \oplus FI_1 \oplus FI_2$ (h) $S \oplus FI_1 \oplus FI_2 \oplus FI_3$ (i) $S \oplus FI_1 \oplus FI_2 \oplus FI_3$ (使用 FE1 加 / 解密)

圖 7： 使用 4 張自然影像實驗結果。(a)~(d)自然分享圖 $N_1 \sim N_4$ 的二元特徵影像（1-bit/pixel），(e)分享圖（24-bit/pixel），(f)還原圖，(g)與(h)為 S 與部分特徵影像（24-bit/pixel）疊合結果，(i)是使用演算法 FE1 加 / 解密的結果。

三、實驗 III：替代攻擊

由於所提的 NVSS 機制，係使用任取的自然影像為傳密的媒介，本小節將驗證本機制承受替代攻擊的能力。實驗假設下列嚴峻的情境：加解密採用 $((4,1),5)$ – NVSS 方案，攻擊者已正確攔截 3 張加密用的自然分享圖與 1 張雜點分享圖，且已取得解密程式，在仍缺乏 1 張自然分享圖的情況下，企圖使用任意自然影像解密。本實驗並且進一步假設攻擊者在很偶然的情況下，得知所缺自然分享圖的主題，因此可採用 1 張極類似的影像進行替代攻擊。

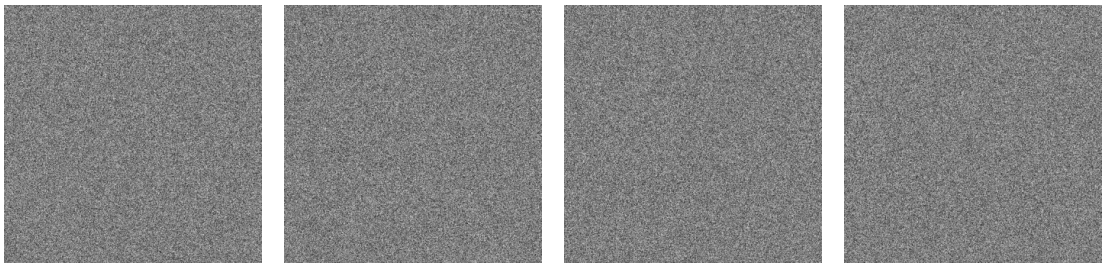
圖 8 是自然影像 N_1、N_2、N_3 與 N_4 的替代影像，分別記為 FN_1、FN_2、FN_3 與 FN_4。這些替代影像是以圖 4 的自然影像透過 Google 的圖形搜尋引擎搜尋，在 Internet 公開領域中所搜尋到最相似的影像，再經過人工調整成與原自然影像相同大小。用肉眼觀之，這些替代影像與原自然影像具有極相似的特徵。



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

圖 8： 4 張用來進行替代攻擊的影像：(a) $FN_1 : N_1$ 的替代影像，(b) $FN_2 : N_2$ 的替代影像，(c) $FN_3 : N_3$ 的替代影像，(d) $FN_4 : N_4$ 的替代影像

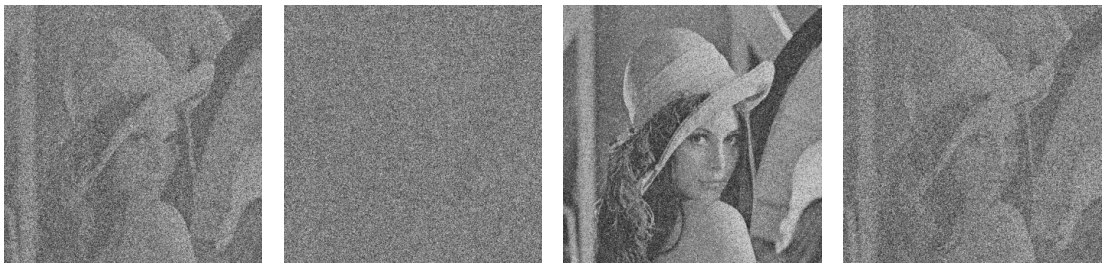
圖 9 展示上述實驗架構的攻擊結果。實驗結果顯示，使用替代影像無法還原機密影像。尤有甚者，也沒有任 1 張疊合圖能顯示出與機密影像相關聯的紋理。因此，可驗證本機制能有效抵擋替代攻擊。



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

圖 9：使用 1 張替代影像攻擊的實驗結果（使用 specialization 模組）：(a)~(d)分別是使用 $FN_1 \sim FN_4$ 替代 $N_1 \sim N_4$ 進行攻擊所產生的疊合結果

接著，我們使用驗證所提的特徵萃取演算法中 Specialization 模組的效能。圖 10 的實驗中，加 / 解密演算法進行特徵萃取時，略去圖 3 中的像素特化步驟；實驗結果顯示，未經像素特化的自然分享圖可能無法抵擋替代攻擊，尤其是當加密者使用極具特徵的自然分享圖（如 N_1），或是極容易取得於公開領域取的知名影像（如 N_3 名畫蒙娜麗莎的微笑與 N_4 知名旅遊景點祕魯馬丘比丘）。但圖 10(b)也顯示，對於較複雜的自然分享圖（如 N_2），雖然使用外觀極為相似的影像進行攻擊，仍無法一窺機密影像內容。反觀圖 9 的結果可證實，本文所提的像素特化策略，的確能夠使自然分享圖產生特殊性，可有效抵擋替代攻擊，消除加密者可能須慎選自然分享圖的困擾，增加本機制的使用彈性。



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

圖 10：使用 1 張替代影像攻擊的實驗結果（不使用 specialization 模組）：(a)~(d) 分別是使用 $FN_1 \sim FN_4$ 替代 $N_1 \sim N_4$ 進行攻擊所產生的疊合結果

四、與其他研究比較

本節從不同特性的觀點，提出本研究與現存研究的比較。從表 4 中可觀察出，雖然前人的研究致力改善機密影像的品質，但有些研究僅能加密顏色十分有限的機密影像（如 Hou 2003; Yang & Chen 2008; Shyu 2009），有些研究雖可加密半色調彩色影像，但有些研究會引起像素擴張（如 Wu et al 2008; Kang et al 2011），有些研究僅能支援（2, 2）的加密方案（如 Wu et al 2008; Lou et al 2011）。其中，Lou 等（2011）的方法雖可還原較高品質的半色調機密影像，但疊合圖上會殘留非常清楚的掩護影像（cover images），嚴重干擾還原機密影像的辨識，使該機制所能分享的機密影像內容受限。本研究具有能加密全彩機密影像，且能達到還原全彩機密影像，不會造成任何失真與像素擴張的優點。此外，不論參與分享的人數（n）有多少，本研究均能使用 $n-1$ 張任選的自然影像，在完全不竄改影像內容的情況下，分享機密影像，這些自然分享圖的友善程度，遠高於其他機制的分享圖。

表 4：本研究與前人研究成果比較

特質	本研究	前人的研究					
		Hou (2003)	Wu et al (2008)	Yang & Chen (2008)	Shyu (2009)	Lou et al (2011)	Kang et al (2011)
可支援方案	(n, n)	(2, 2)	(2, 2)	(k, n)	(n, n)	(2, 2)	(k, n)
機密影像品質	全彩	顏色有限	半色調	顏色有限	顏色有限	半色調	半色調
還原影像品質	全彩 [a]	可辨識	可辨識	可辨識	可辨識	可辨識 [b]	可辨識
像素擴張因子	1	4	4	3	1	1	4
外觀有意義的分享圖	是（$n-1$ 張） 否（1 張）	否	是	否	否	是	是
分享圖品質	($n-1$ 張)全彩 [a] +(1 張)雜點	雜點	半色調 （品質差）	雜點	雜點	半色調 （品質佳）	半色調 （品質差）
可被偵測的分享圖數量 / 分享圖總數量	$1/n$	1	1	1	1	1	1
分享圖傳輸風險	低	極高	高	極高	極高	中	中
加密演算法複雜度	$O(hw)$ [c]	$O(hw)$	$O(hw)$	$O(hw)$	$O(hw)$	$O(hw)$	$O(hw)$
解密演算法複雜度	$O(hw)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$

a：本研究的還原影像與有意義的分享影像的品質都是全彩且無失真。

b：Lou et al（2011）的還原影像仍殘留有非常清楚的掩護影像。

c：符號 h 與 w 分別表示機密影像高與寬的像素數量。

傳統機密分享機制所使用的 n 張分享圖或為雜點、或經竄改，每一張都有被偵測的可能性。反觀本機制傳遞的 n 張分享圖中，僅包含 1 張雜點分享圖，此分享圖雖然仍存在傳輸風險，但另外的 $n-1$ 張自然分享圖，因未經竄改，攔截者也就難以偵測，因而本機制傳輸 n 張分享圖的風險將被降低到 $1/n$。據此而論，本機制確實提供了一個具有極低傳輸風險的機密分享機制。

本機制的加密演算法的時間複雜度，在像素交換次數設為 $h \times w$ 次的情況下，與其他研究相同，均為 $O(hw)$。但本研究所提方案在解密的階段，仍需對自然分享圖進行特徵萃取，因此會比其他機制耗時。

肆、結論

本文提出以自然影像為基礎的視覺密碼加密機制—$((n-1,1),n)$–NVSS 方案。此機制使用$n-1$張自然影像與 1 張傳統的雜點分享圖加密全彩機密影像。相對於現存的機密分享機制，本研究所提演算法來自於使用任何自然影像的資訊作特徵萃取，過程不會對影像進行任何的修改，不但有效地增加了分享圖的友善程度，同時也更能保護傳遞機密者與機密本身。實驗結果顯示，所提的演算法不會引起分享圖的像素擴張，能抵擋替代攻擊，且機密影像還可完美地被還原。未來，本研究考慮將本機制擴展到門檻型的機密分享機制。

致謝

本文作者由衷地感謝兩位審查委員所提出的寶貴意見，使得本文若干疏漏之處得已修正，大大地提高本文的品質。此外，本文接受國科會計畫資助（計畫編號：NSC 101-2410-H-130-001 與 NSC 101-2221-E-130-018），特此一併致謝。

參考文獻

Ateniese, G., Blundo, C., Santis, A.D. and Stinson, D.R. (2001), 'Extended capabilities for visual cryptography', *Theoretical Computer Science*, Vol. 250, No. 1-2, pp. 143-161.

Chen, T.H. and Tsao, K.H. (2011), 'User-friendly random-grid-based visual secret sharing', *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 21, No. 11, pp. 1693-1703.

Chen, T.H. and Lee, Y.S. (2009), 'Yet another friendly progressive visual secret sharing scheme', *Proceeding of the Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP '09)*, Kyoto, Japan, September 12-14, pp. 353-356.

De Santis, A. and Masucci, B. (2007), 'New results on non-perfect sharing of multiple secrets', *Journal of Systems and Software*, Vol. 80, No. 2, pp. 216-223.

Fang, W.P. (2008), 'Friendly progressive visual secret sharing', *Pattern Recognition*, Vol. 41, No. 4, pp. 1410-1414.

Herranz, J. (2009), 'On the transferability of private signatures', *Information Sciences*, Vol. 179, No. 11, pp. 1647-1656.

Hou, Y.C. (2003), 'Visual cryptography for color images', *Pattern Recognition*, Vol. 36,

No.7, pp. 1619-1629.

Jeyamala, C., GopiGanesh, S. and Raman, G.S. (2010), 'An image encryption scheme based on one time pads - A chaotic approach', *Proceeding of the International Conference on Computing Communication and Networking Technologies (ICCCNT 2010)*, Chettinand, India, July 29-31, pp. 1-6.

Kang, I., Arce, G.R. and Lee, H.K. (2011), 'Color extended visual cryptography using error diffusion', *IEEE Transactions on Image Processing*, Vol. 20, No. 1, pp. 132-145.

Klein, A. and Wessler, M. (2007), 'Extended visual cryptography schemes', *Information and Computation*, Vol. 205, No. 5, pp. 716-732.

Liu, F. and Wu, C. (2011), 'Embedded Extended Visual Cryptography Schemes', *IEEE Transactions on Information Forensics and Security,* Vol. 6, No. 2, pp 307-322.

Liu, H. and Wang, X. (2010), 'Color image encryption based on one-time keys and robust chaotic maps', *Computers & Mathematics with Applications*, Vol. 59, No. 10, pp. 3320-3327.

Lou, D.C., Chen, H.H., Wu, H.C. and Tsai, C.S. (2011), 'A novel authenticatable color visual secret sharing scheme using non-expanded meaningful shares', *Displays*, Vol. 32, No. 3, pp. 118-134.

Nakajima, M. and Yamaguchi, Y. (2002), 'Extended visual cryptography for natural images', *Journal of WSCG*, Vol. 10, No. 2, pp. 303-310.

Naor, M. and Shamir, A. (1995), 'Visual cryptography', *Advances in Cryptology: Eurprocrypt'94*, Vol. 950, pp. 1-12.

Shyu, S.J. (2009), 'Image encryption by multiple random grids', *Pattern Recognition*, Vol. 42, No.7, pp. 1582-1596.

Tsai, D.S., Chen, T.H. and Horng, G. (2008), 'On generating meaningful shares in visual secret sharing scheme', *The Imaging Science Journal*, Vol. 56, No.1, pp. 49-55.

Tsai, D.S., Horng, G., Chen, T.H. and Huang, Y.T. (2009), 'A novel secret image sharing scheme for true-color images with size constraint', *Information Sciences*, Vol. 179, No. 19, pp. 3247-3254.

Wang, D., Yi, F. and Li, X. (2009), 'On general construction for extended visual cryptography schemes', *Pattern Recognition*, Vol. 42, No. 11, pp. 3071-3082.

Wang, Z. and Arce, G.R. (2010), 'Halftone visual cryptography by iterative halftoning', *Proceeding of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2010)*, Dallas, Texas, USA, March 14-19, pp. 1822-1825.

Wu, H.C., Wang, H.C. and Yu, R.W. (2008), 'Color visual cryptography scheme using

meaningful shares', *Proceeding of the Eighth International Conference on Intelligent Systems Design and Applications*, Kaohsiung City, Taiwan, November 26-28, pp. 173-178.

Wu, Y.S., Thien, C.C. and Lin, J.C. (2004), 'Sharing and hiding secret images with size constraint', *Pattern Recognition Letters*, Vol. 34, pp. 1377-1385.

Xinpeng, Z. (2011), 'Lossy compression and iterative reconstruction for encrypted image', *IEEE Transactions on Information Forensics and Security*, Vol. 6, No. 1, pp. 53-58.

Yang, C.N. and Chen, T.S. (2008), 'Colored visual cryptography scheme based on additive color mixing', *Pattern Recognition*, Vol. 41, No. 10, pp. 3114-3129.

Zhou, Z., Arce, G.R. and Crescenzo, G.D. (2006), 'Halftone visual cryptography', *IEEE Transactions on Image Processing*, Vol. 15, No. 8, pp. 2441-2453.