# 新的機密高動態範圍影像分享技術
# A Novel Secret High Dynamic Range Image Sharing

王宗銘 鄭友銘 曾宇田 陶嘉瑋 廖彥凱
國立中興大學資訊科學系
E-mail: cmwang, s9156048@cs.nchu.edu.tw;
s9356034, s9356031, s9356045@mail.cs.nchu.edu.tw

## 摘要

近年來廣受討論之高動態範圍影像包含高範圍的色彩顯示能力，相較於傳統低動態範圍影像更能有效地呈現自然世界的真實色彩。鑒於高動態範圍影像之趨勢，本文首創機密高動態範圍影像分享演算法，將機密資訊分享為 $n$ 筆影子資訊，並藉由其中任意 $r$ 筆影子資訊($r \le n$)恢復完整之機密高動態範圍影像。我們根據高動態範圍影像的特性，重新調整影像並以自適應模型的算數編碼方法壓縮，有效縮減影子資訊。為了進一步增進影子資訊在網際網路傳遞的隱密性及完整性，我們更提出植基於邊緣吻合的認證型高動態範圍影像資訊隱藏演算法，以雜湊函數對偽裝影像進行認證，產生不易為人們察覺有異的偽裝高動態範圍影像。實驗結果顯示：我們的技術首開先例，成功提供機密資訊更為隱密、認證、可靠又安全的分享方式。

**關鍵詞**：高動態範圍影像、機密影像分享、資訊隱藏、認證。

## Abstract

High dynamic range (HDR) images which have received much discussion in recent years present real world colors more effectively than conventional low dynamic range (LDR) images. We propose a novel secret high dynamic range image sharing algorithm based on the tendency of HDR image. It shares a secret HDR image into $n$ shadow data, and any $r$ shadow data ($r \le n$) can be used to restore the whole secret HDR image. We make an adjustment in each channel value with respect to the characteristics of HDR image and then compress it by the adaptive arithmetic code. We also propose a HDR image data hiding method with authentication for security and integrality during the transmission on the Internet. It is based on the modified side match scheme and the hash function. Our method makes it hard for the stego HDR image to perceive differences. Experimental results demonstrate that our algorithm provides a way for the secret information to be shared in a private, authentic, reliable and secure way.

**Keywords**: high dynamic range image, secret image sharing, steganography, authentication.

## 1. 簡介

隨著數位科技的蓬勃發展，越來越多人習慣藉數位化的方式保存機密資訊。然而，若機密資訊集中保管，一旦遭受破壞或遺失，機密資訊亦同時損失。另一方面，若機密資訊複製多份，則亦呈倍數提高被破解及遭到解密的可能性[3, 9, 11]。

機密影像分享(secret image sharing)[3, 5, 9, 12, 13]和視覺密碼學分享(visual secret sharing)[2, 4, 11]即為保存機密資訊一個兩全其美的解決方法，提供機密資訊一個可靠安全的分散保存方式。

高動態範圍(high dynamic range, HDR)影像是近年來廣受討論及使用的影像格式，保存的色彩變化範圍遠超過低動態範圍影像，相較之下，更可有效呈現自然世界的真實色彩。本文針對最常見的光輝(radiance)RGBE 影像提出機密影像分享演算法。

我們首先根據高動態範圍影像的特性進行前置處理並以自適應模型的算數編碼方法壓縮，隨後，以多項式的分解取得較小的影子資訊(shadow data)。另一方面，再使用高動態範圍影像資訊隱藏演算法提高秘密傳遞影子資訊的安全性[6]，透過植基於邊緣吻合的方法，將不同數量的訊息分別嵌入於掩護(cover)高動態範圍影像的平滑像素(smooth pixels)與邊界像素(edge pixels)內，取得不易為人們察覺有異的偽裝(stego)高動態範圍影像。此外，我們更以雜湊函數(hash function)對偽裝影像進行認證加密，提供偽裝影像之完整性與正確性的認證。總結本研究：我們提出一個有效的機密高動態範圍影像分享技術，提供機密高動態範圍影像一個隱密、認證、可靠又安全的分享方式。

本文結構如下：第二節說明相關文獻；第三節敘述我們提出的演算法；第四節說明實驗結果。最後，第五節提出結論與未來工作。

## 2. 相關文獻

鑒於目前仍無高動態範圍影像之機密影像分享演算法，此節我們探討傳統低動態範圍影像之機密影像分享演算法及高動態範圍影像之特性為主。

機密影像分享和視覺密碼學分享為保存機密資訊提供一個兩全其美的解決方法，透過機密分享的資訊不再是一份完整的複本，取而代之的是 $n$ 份擁有 $1/r$ 權限的影子資訊[3, 5, 9, 12, 13]。透過 $n$ 份

影子資訊的分散保存及任意 $r$ 份影子資訊即可還原完整資訊的能力提供機密資訊一個可靠又安全的分享方式。儘管部份影子資訊已遭受破壞或遺失，只要仍保有任意 $r$ 份影子資訊即可順利還原回原始的機密資訊，達到容錯的可靠保存方式。此外，以往機密資訊只儲存於單一載體(single carrier)之中，若機密資訊被第三者攔截，仍有被解開的風險。藉由機密分享技術則可避開此風險，即使第三者已攔截 $r$-1 份影子資訊亦完全無法窺見原始機密資訊的一角，有效提升機密資訊安全的分散保存。

Blakley[7]及 Shamir[1]分別最早提出機密分享概念：$(r; n)$門檻法(threshold scheme)。$(r; n)$門檻法利用多項式的分解將機密影像分成 $n$ 張看似雜訊的影子影像，只有同時取得其中的 $r$ 張影子影像才能順利還原回原始的機密影像。但是，由於其提出的多項式一次僅輸入一個影像像素值並產生一個影子影像的數值，造成儲存空間大小的需求甚高。

Thien 及 Lin 則進一步改良 Blakley 及 Shamir 的$(r; n)$門檻法，縮小影子影像的儲存大小，降低需嵌入掩護影像的資訊量[3]。其提出的方法可一次輸入 $r$ 個影像像素值於多項式並僅輸出一個影子影像的數值，所以其影子影像大小僅為原始影像的 $1/r$，有效降低影子影像的儲存需求。

傳統低動態範圍影像使用 R、G 及 B 各 8 位元記錄紅、綠及藍三原色的變化程度，故每一原色僅有 0~255 的變化範圍。高動態範圍影像將其擴充，各以 32 位元的浮點數表示三原色的變化程度，大幅提升每一原色的變化範圍為 $0\sim2^{127}$，是故能更真實地記錄自然世界的真實色彩。

高動態範圍影像擁有許多儲存格式，其中最常見的為 Greg Ward 等學者提出的光輝 RGBE 格式[8]。光輝 RGBE 格式將原始每個像素為 96 位元表示的浮點數格式，以指數與尾數替換的方式，降低為 R、G 及 B 各 8 位元並共用 8 位元指數值 E，共 32 位元的整數格式。其中，E 值為利用原始 R、G 及 B 中最大的數值求出。雖然經過此舉轉換之後的高動態範圍影像會有些許失真，但在大幅降低所需儲存空間的前提之下，此失真仍在容許範圍之內，是故此壓縮方式成為高動態範圍影像採用的主流檔案格式之一。因此，我們針對此型態之之高動態範圍影像提出機密影像分享演算法。

## 3. 新的機密高動態範圍影像分享演算法

本論文提出一個新的機密高動態範圍影像分享演算法，分享及隱藏的流程如圖 1 所示。

演算法區分為六個步驟：1.頻道分解、2.頻道壓縮、3.機密分享、4.頻道重組與打散、5.高動態範圍影像資訊隱藏、6.影像認證。首先，輸入機密的高動態範圍影像，將 R、G、B 及 E 各頻道的資料值從原始的機密影像中取出；接著分別對各頻道從事無失真壓縮演算法，產生壓縮後的 $R_c$、$G_c$、$B_c$ 及 $E_c$ 資料值；再對各頻道進行機密分享演算法，產生各頻道分享後的影子頻道 $S_{R_c}$、$S_{G_c}$、$S_{B_c}$ 及 $S_{E_c}$ 資訊，將其重新組合成 $n$ 筆影子資訊(shadow data)，並分別對各影子資訊加入密鑰進行打散，以增加各影子資訊的安全性；再者，利用高動態範圍資訊隱藏演算法，將影子資訊藏入掩護影像，輸出 $n$ 張含有 $1/r$ 權限的偽裝影像；最後，對各偽裝影像進行影像認證的處理，以確保偽裝影像的正確性。

以下，3.1 節將說明機密高動態範圍影像產生 $n$ 筆影子資訊的方法；3.2 節詳細說明將影子資訊藏入掩護影像產生偽裝影像並對其嵌入影像認證資訊的過程；最後，3.3 節說明藉由取得的 $r$ 張偽裝影像，重新還原原始的機密高動態範圍影像。

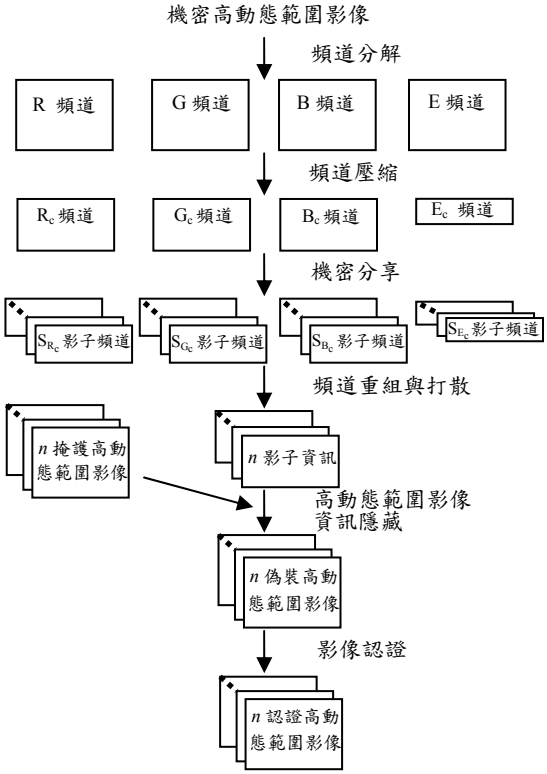



**圖 1 機密高動態範圍影像之分享與隱藏流程圖**

### 3.1 影子資訊產生技術

由於高動態範圍影像與低動態範圍影像的差異，我們首先根據高動態範圍影像的特性將 RGBE 拆解為 4 個分離的頻道，亦即 R、G 及 B 各佔 8 位元/像素及共享 8 位元/像素指數值 E，再就此整數型態四頻道之特性提出適用的無失真壓縮演算法。

由於高動態範圍影像中的 E 值在分佈上擁有相同數值緊鄰的特性，故使其擁有較高的壓縮效率；然而，R、G 及 B 的數值分布特性較傳統的低動態範圍影像有更高的差異性，是故我們根據其特性提出前置差異處理，降低其數值變化差異，提高數值重複機率，藉此提升壓縮效率。

考慮一張解析度為 $x\times y$ 之機密高動態範圍影像 $S=\{s_{ij}|\ 1\le i\le x \text{ and } 1\le j\le y\}$，其中 $s_{ij}$ 為影像上相對座標的像素值。我們透過方程式 1 求得像素差異值 $s_{ij}'$。

$$s_{ij}' = \begin{cases} s_{ij} & if\ i=0\ \ and\ \ j=0 \\ s_{ij} - s_{(i-1)j} & if\ i \neq 0\ \ and\ \ j=0 \\ s_{ij} - s_{i(j-1)} & otherwise \end{cases} \qquad (1)$$

藉由方程式 1 取得之像素差異值有較低的變化量及較高的重複性，見圖 2，故可提升其壓縮效率。

| | | | |
|---|---|---|---|
| 100 | 110 | 120 | … |
| 110 | 125 | 130 | … |
| 120 | 125 | 140 | … |
| … | … | … | … |

⇨

| | | | |
|---|---|---|---|
| 100 | 10 | 10 | … |
| 10 | 15 | 5 | … |
| 10 | 5 | 15 | … |
| … | … | … | … |

**圖 2** 像素差異變化範例

為了縮減分享後產生的影子資訊量，我們對 R、G 及 B 的各像素差異值及 E 頻道值分別使用自適應模型的算數編碼(adaptive arithmetic coding)進行壓縮，各輸出一個介於 0 和 1 之間的二進位制小數。其壓縮方法為給定一個位元組 0~255 的概率分布表，初始化每個數字出現的概率為 1/256。每輸入一個數值就調整概率分佈表，並將要輸出的小數限定在某個越來越小的區間內。處理完所有的數值之後便得到所要輸出的二進制小數值，如圖 3 所示。

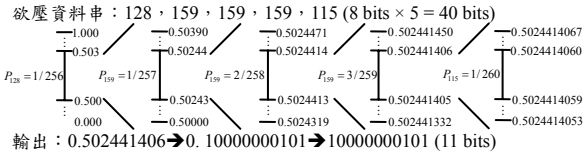



**圖 3 算數編碼示意圖**

本論文使用 3 階的上下文模型，即在概率分佈表中，對下一個讀入的數值，概率的調整不僅考慮單一數值的出現機率，是考慮連續四個數值出現的概率。由於壓縮前對概率表的初始化動作，會造成需要對幾乎不出現的上下文進行編碼，所以使用了轉義碼的概念。轉義碼是混在壓縮數據中的特殊記號，用於通知解壓縮程序的下一個上下文，在此之前從未出現過，需要使用低階的上下文進行編碼。如果轉入最低的 0 階上下文表仍未出現過此輸入的資料值，則轉到一個特殊的轉義上下文表中，該表內含 0~255 所有的符號。每個符號的計數都為 1，且永不更新，任何高階上下文皆沒有出現的符號將退到這裡按照 1/256 的頻率進行編碼。此舉可有效根據輸入數據的變化快速調整到最佳位置，並迅速減少對高概率數值編碼所需要的位數。

因為四頻道皆以相同方式產生影子頻道，所以下述僅以 R 頻道為例；經過壓縮後的 $R_c$ 頻道欲使用分享演算法做頻道分享時，需模一個質數。然而，因為 251 為不超過 255 中的最大質數，但是，其頻道內的數值分布仍介於 0 到 255 之間，若直接將數值模 251 則會造成部分的失真，故我們需先以方程式 2 將數值展開，令數值分布範圍重新落於 0 到 250 之間，並儲存於於陣列 $R_c'$。藉由此法，我們可以無失真地將 $R_c'$ 的數值再逆推回原始的 $R_c$ 數值。

$$R_{c_i}' = \begin{cases} R_{c_i} & if\ R_{c_i} < 250 \\ (250,\ R_{c_i} - 250) & if\ R_{c_i} \geq 250 \end{cases} \qquad (2)$$

接著將 $R_c'$ 陣列切割成數個區段，每個區段皆含有 $r$ 個 $R_c'$ 頻道值，且 $R_c'$ 頻道中的每個值都屬於且僅屬於一個區段，對每個區段我們可定義一個 $r$-1 階的多項式，如方程式 3。

$$q_j(x) = (a_0 + a_1 x + ... + a_{r-1} x^{r-1}) \bmod 251 \qquad (3)$$

其中，$a_0$, $a_1$, …, $a_{r-1}$ 為此區段的 $r$ 個 $R_c'$ 頻道值，藉此方程式可計算出下列數值：$q_j(1)$, $q_j(2)$, …, $q_j(n)$，亦即 $n$ 個影子數值。緊接著，利用上述方法分別求得 $G_c$、$B_c$ 及 $E_c$ 的各 $n$ 個影子頻道。

最後，將四個頻道經過分享演算法產生的各 $n$ 個影子頻道重新加以組合，即可得到所需要的 $n$ 個影子資訊，並藉由給予一個密鑰進行影子資訊打散的動作，提高影子資訊的安全性及隱密性。

## 3.2 高動態範圍影像之資訊隱藏及影像認證

依本文上述方法產生影子資訊後，由於其為雜訊影像，為了提升其傳輸之安全性，本節使用高動態範圍影像資訊隱藏演算法將其嵌入普通的高動態範圍影像中。此外，為了避免偽裝影像之內嵌資訊遭到破壞，造成機密影像還原失敗，我們認為仍須針對該偽裝影像進行影像認證，故我們提出藉由單向雜湊函數(one-way hash function)確認偽裝影像正確性，避免取出錯誤的影子資訊。

認證型高動態範圍影像資訊隱藏演算法共有三個步驟：1.像素分類、2.區塊處理與 3.邊界處理。

像素分類：高動態範圍影像中，相鄰的像素其指數值 E 皆相同或相近，根據此特性，像素相鄰且 E 值相同稱之為區塊；反之，則稱為邊界。

區塊處理：區塊部份使用雙邊界(two-sided)之區塊相配演算法，根據該像素與上方及左方像素之差異決定可嵌入之資訊量。像素處理方向如圖 4 所示：灰色部分為參考像素，故先以最低有效位元取代法嵌入 1 位元；白色部分則以區塊相配演算法根據其影像變異程度嵌入不定量之資訊。此外，為了最後可嵌入認證影像所需的資訊，我們先以密鑰決定 43 個像素暫時不嵌入影子資訊，如圖 4 標記為 A 之黃色區塊。由於雙邊界之區塊相配演算法需參考該像素之上方及左方像素，故已決定保留為嵌入認證影像資訊的下方及右方像素僅以最低有效位元取代法嵌入 1 位元，如圖 4 標記為 LSB 之綠色區塊。

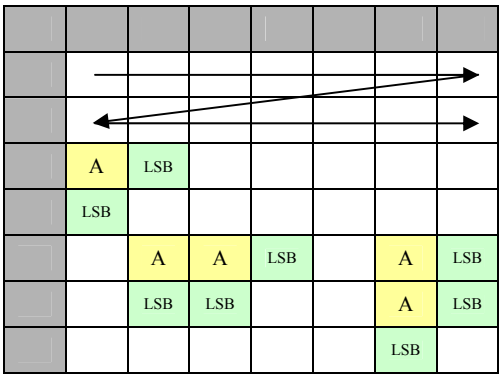



**圖 4 雙邊界區塊相配演算法之像素處理方向圖**

由於高動態範圍影像之指數值 E 為影像像素值最終亮度的決定關鍵，故我們僅嵌入資訊於高動態範圍影像之 R、G 及 B 頻道。鑒於 RGBE 的 R、G 及 B 的處理方式相同，故以下皆以 R 為例說明。假設欲處理的像素為 $R_x$，其上方像素 R 值為 $R_u$，左方像素 R 值為 $R_l$，則差異值 $d$ 可由方程式 4 所得。

$$d = (R_u + R_l) / 2 - R_x \quad (4)$$

當 $|d| \leqq 1$，以最低有效位元取代法嵌入資訊，若 $|d| > 1$，則以方程式 5 求得最適的嵌入量 $a$。

$$a = log_2 |d|, \text{ if } |d| > 1 \quad (5)$$

求出最適嵌入量 $a$ 後，再使用嵌入資訊值 $b$，由方程式 6 算出新的差異值 $d'$。

$$d' = \begin{cases} 2^a + b, & if \quad d > 1 \\ -(2^a + b), & if \quad d < 1 \end{cases} \quad (6)$$

最後再使用方程式 7 取得嵌入資訊後的 $R_x'$ 值，其中，$R_x'$的範圍為 0~255。

$$R_x' = (R_u + R_l) / 2 - d' \quad (7)$$

為了確保嵌入後的數值在 0~255 之間，在嵌入之前再用方程式 8 及方程式 9 檢查，若其中一式成立，代表嵌入的值不在 0~255 之內，故不嵌入資訊。

$$d > 1 \ \cap \ (R_u + R_l) / 2 < 2^{a+1} - 1 \quad (8)$$

$$d < 1 \ \cap \ (R_u + R_l) / 2 + 2^{a+1} > 256 \quad (9)$$

邊界處理：影像之中屬於邊界的像素，由於其 E 值與相鄰像素並不相同，無法直接用區塊相配演算法嵌入資訊。嵌入資訊前必須先根據本身像素的指數值 E，將相鄰像素的指數值 E 轉換成相同的數值，當 E 值改變後，需藉由方程式 10 轉換 RGBE 數值，其中 R'及 E'為轉換後的 R 值及 E 值。如果轉換後的數值超過 255，需強迫降為 255。

$$R' = R \times 2^{E-E'} \quad (10)$$

當上方及左方像素之 E 值轉換成與本身像素 E 值相同時，即可使用區塊相配演算法嵌入資訊。

待影子資訊嵌入完畢後，我們以單向雜湊函數確認偽裝影像之正確性。首先，我們捨去原先保留為嵌入認證資訊之用的 43 個像素，並將其餘的影像像素值以雜湊函數 MD5(message-digest algorithm)[14]產生認證碼。根據 MD5 演算法之特性：無論待認證資訊之長度為何，最終皆可得到 128 位元認證碼。此外，我們對此認證碼再加上 1 位元之奇同位認證，共可得到 129 位元之偽裝影像認證碼，如圖 5 所示。最後，我們將此 129 位元的認證碼以密鑰產生亂數並拆成 3 份，分別以最低有效位元取代法將此資訊分別嵌入事先保留的 43 個像素的 R、G 及 B 之中。

| 0 ... 127 | 128 |
|---|---|
| 128 位元 MD5 認證碼 | 0/1 |

**圖 5 偽裝影像認證碼示意圖**

取出資訊部分與嵌入方法類似，首先，以密鑰決定原嵌入偽裝影像認證碼的 43 個像素，並從中取出認證碼，隨後以 MD5 演算法判斷偽裝影像之正確性，若通過認證則開始擷取已嵌入之影子資訊。假設欲處理的像素 R 值為 $R_x^*$，上方像素及右方像素為 $R_u^*$及 $R_l^*$，則由方程式 11 求得差異值 $d^*$。

$$d^* = (R_u^* + R_l^*) / 2 - R_x^* \quad (11)$$

當 $|d^*| \leqq 1$，則取出該像素之最後一位元。若 $|d^*| > 1$，則使用方程式 12 求得最適嵌入量 $a$，也就是該像素的原始嵌入量大小。

$$a = log2 |d^*|, \text{ if } |d^*| > 1 \quad (12)$$

最後利用方程式 13 算出原始嵌入資訊 $b$

$$b = \begin{cases} d^* - 2^a, & if \quad d^* > 1 \\ -d^* - 2^a, & if \quad d^* < 1 \end{cases} \quad (13)$$

與嵌入時相同，若方程式 14 和方程式 15 成立，則代表未嵌入資訊，所以不需取出。

$$d^* > 1 \cap (R_u^* + R_l^*) / 2 < 2^{a+1} - 1 \quad (14)$$

$$d^* < 1 \cap (R_u^* + R_l^*) / 2 + 2^{a+1} > 256 \quad (15)$$

### 3.3 機密高動態範圍影像還原

此節我們簡述機密高動態範圍影像還原之步驟：首先，從 $n$ 筆偽裝影像中挑選 $r$ 筆偽裝影像並透過嵌入之認證碼確認該偽裝影像之正確性與完整性，若該偽裝影像通過認證則確定其未遭受竄改，故可順利從中取出內嵌的影子資訊。待取得 $r$ 筆影子資訊後，藉由密鑰還原原始影子資訊的排列順序，並將其拆解為 $S_{R_c}$、$S_{G_c}$、$S_{B_c}$ 及 $S_{E_c}$ 各 $r$ 筆影子頻道並帶回方程式 3。其中，$q_j(1), q_j(2), \ldots, q_j(r)$ 為各影子頻道的數值，求得之係數值 $a_0, a_1, \ldots, a_{r-1}$ 即為壓縮後之 $R_c$、$G_c$、$B_c$ 及 $E_c$ 各頻道數值，再經由解壓縮求得各頻道的原始四頻道資料，最後，將其重新合成，即取得原始之機密高動態範圍影像。

## 4. 實驗結果

本節將說明並分析實驗成果。本論文提出的演算法以 C 語言作為開發語言，並以 AMD Athlon64 3000+的 CPU 及 1GB 的記憶體作為測試平台。以下將以實際的圖例說明我們提出的演算法實行機密高動態範圍影像分享的過程。

圖 6 為機密高動態範圍影像分享範例圖，其中，圖 6e 為日落，解析度為 720x480。圖 6f~圖 6i 為其分享出各自擁有 1/3 權限的 4 份影子資訊，每筆影子資訊皆含有 $S_{R_c}$、$S_{G_c}$、$S_{B_c}$ 及 $S_{E_c}$ 全部頻道的資訊，所需儲存空間皆小於原始機密影像，證明我們的分享方式有效縮減了影子資訊的大小。由表 1 可看出，高動態範圍影像在前置差異處理之後，其壓縮完產生的影子資訊大小相較於直接以算數編碼壓縮頻道產生的影子資訊為小。我們對高動態範圍影像進行前置處理提高數值重複機率，因此可得到較佳的壓縮效果及壓縮速率。

圖 7a 為影像原始之 B 值分佈圖，數值範圍分散落於 0~255 之間，造成算數編碼壓縮效率不佳；

然而，經前置處理後的 B 值分佈範圍集中落於 0~127 之間，如圖 7b。由表 1 得知，藉由前置處理可得到較佳的壓縮效果及需求較少的壓縮時間，故可有效減少需要的資訊嵌入量。圖 6a~圖 6d 為已嵌入影子資訊及認證資訊的偽裝高動態範圍影像，我們無法以肉眼查覺其差異性，故我們以 PSNR 顯示偽裝影像與掩護影像的相似度，如表 2 所示。其中，PSNR 數值越大代表相似度越高，一般而言，高於 30 即無法以肉眼察覺差異之處。藉由我們提出的認證型資訊隱藏演算法取得的偽裝影像其 PSNR 值皆高於 35，以肉眼很難分辨差異之處。

對於每張取得的的偽裝影像，在取出內嵌的影子資訊之前，須先認證偽裝影像的正確性。認證失敗即代表偽裝影像已遭變更，還原程序將強制終止。僅有認證通過的偽裝影像才可順利地取出正確的內嵌資訊，取得正確的影子資訊。由於影子資訊事先已由密鑰改變資訊排列方式，故我們隨後必須以正確的密鑰復原影子資訊的排列方式並將其分解為 $S_{R_c}$、$S_{G_c}$、$S_{B_c}$ 及 $S_{E_c}$ 影子頻道。以此例而言，只有同時取得 3 份認證通過的偽裝影像才可順利地取得還原機密高動態範圍影像所需的影子資訊。隨後即透過我們提出的演算法取得 $R_c$、$G_c$、$B_c$ 及 $E_c$ 頻道之資料，並解壓縮取得原始的 R、G、B 及 E 頻道之數值，最後，重組各頻道之值即可得到完整的原始機密高動態範圍影像，如圖 6j。

由於此例中每張偽裝影像僅持有 1/3 權限的影子資訊，若竊取者無法同時取得 3 份相異的偽裝影像並以正確的密鑰取出影子資訊則無法窺得原始之機密高動態範圍影像。藉由認證型偽裝影像的完整性與不可視性、機密影像分享的權限分散及密鑰的安全性，我們可確保機密高動態範圍影像隱密、認證、可靠又安全的分享。

## 5. 結論與未來工作

鑒於高動態範圍影像之趨勢及重要性，本論文首創一個新的機密高動態範圍影像分享演算法，能夠成功的將機密高動態範圍影像分享為 $n$ 筆擁有 $1/r$ 權限的影子資訊，提供機密資訊更為可靠又安全的分享方式。藉由高動態範圍影像的特性，我們重新調整影像並以自適應模型的算數編碼方法壓縮，有效縮減影子資訊。隨即透過認證型高動態範圍資訊隱藏技術，將影子資訊成功嵌入其他高動態範圍影像，並以單向雜湊函數確認偽裝影像之正確性，除了可產生不易為外人所察覺的視覺效果，更可避免由錯誤的偽裝影像中取出錯誤的影子資訊。

首先，我們根據高動態範圍影像的特性進行前置處理並以自適應模型的算數編碼壓縮，隨後，以多項式的分解取得較小的影子資訊。為了增進影子資訊傳遞的隱密性，我們使用認證型高動態範圍影像資訊隱藏演算法提高秘密傳遞影子資訊的安全性，並透過植基於邊緣吻合的方法，將不同數量的訊息嵌入於掩護高動態範圍影像的平滑像素與邊界像素內，產生不易為人們察覺有異的偽裝高動態範圍影像。最後，以雜湊函數對偽裝影像認證，確保偽裝影像之完整性與正確性。總結本研究：我們的演算法可有效的將機密高動態範圍影像分享成 $n$ 筆擁有 $1/r$ 權限的影子資訊，並透過認證型高動態範圍影像資訊隱藏演算法取得視覺效果良好的偽裝影像，達到隱密、認證、可靠又安全的分享。

未來工作上，我們將繼續朝下列方向研究：第一、縮減隱藏資訊量：透過不同的前置處理或無失真壓縮方式，則可在不損壞影子資訊的正確性及完整性下，減少其資訊量，以利於資訊隱藏。第二、增加廣泛性：由於目前我們僅針對高動態範圍影像主流格式之一的光輝 RGBE 研究，未來將嘗試將其延伸至其他高動態範圍影像格式。


## 致謝

本研究承蒙國科會之經費補助(95-2815-C-005-029-E、95-2815-C-005-028-E、95-2815-C-005-027-E)，謹此致謝。


## 參考文獻


[1] A. Shamir, How to share a secret, Commun. ACM, Vol. 22, No. 11, pp. 612-613, 1979.

[2] C. C. Chang, J. C. Chuang, “An image intellectual property protection scheme for gray-level images using visual secret sharing strategy,” Pattern Recognition Letters Vol. 23, pp.931-941, 2002.

[3] C. C. Thien, J. C. Lin, “Secret image sharing,” Computers & Graphics Vol. 26 , pp.765-770, 2002.

[4] C. C. Lin, W. H. Tsai, “Visual cryptography for gray-level images by dithering techniques,” Pattern Recognition Letters Vol. 24, pp.349-358, 2003.

[5] C. C. Lin, W. H. Tsai, “Secret image sharing with steganography and authentication,” The Journal of Systems and Software Vol. 73, pp.405-414, 2004.

[6] C. M. Wang, Y. M. Cheng, Y. P. Tzeng, H. W. Kan, Y. H. Huang, P. Y. Leu, Y. S. Hsieh, “A Novel Data Hiding Algorithm for High Dynamic Range Image,” Taiwan Network Conference, 2005.

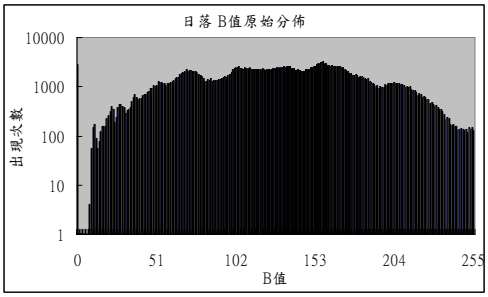
[7] G. R. Blakley, “Safeguarding cryptographic keys,” Proceedings AFIPS 1979 National Computer Conference, Vol. 48, pp. 313-317, 1979.

[8] G. Ward, “Real Pixel,” Graphics Gems II, Ed. by J. Arvo, Academic Press, pp. 80-83, 1992.

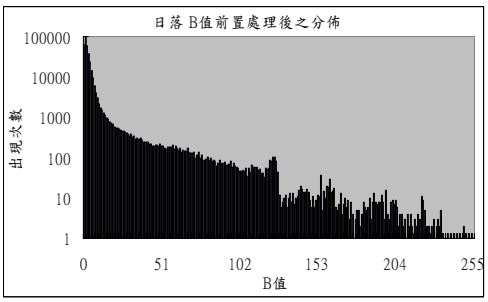
[9] J. B. Feng, H. C. Wu, C.-S. Tsai, and Y.-P. Chu, “A new multi-secret images sharing scheme using Largrange's interpolation,” The Journal of Systems and Software Vol. 76, pp.327-339, 2005.

[10] M. Ashikhmin, “A Tone Mapping Algorithm for

High Contrast Images,"In Proceedings of the 13th Eurographics Workshop on Rendering, pp. 145-156, 2002.
[11] R. Lukac, K.N. Plataniotis, "Bit-level based secret sharing for image encryption," Pattern Recognition Vol. 38, pp.767-772, 2005.
[12] R. Z. Wang, C. H. Su, "Secret image sharing with smaller shadow images," Pattern Recognition Letters Vol. 27, pp.551-555, 2006.
[13] S. K. Chen, J. C. Lin, "Fault-tolerant and progressive transmission of images," Pattern Recognition Vol. 38, pp.2466-2471, 2005.
[14] W. Stallings. Cryptography and Network Security: Principles and Practice. Prentice Hall International, Inc., Second edition, 1999.




(a)




(b)

**圖 7 前置處理前後之影像數值分佈圖：(a)為日落影像原始之 B 值分佈圖，數值範圍落於 0~255 之間；(b)為經前置處理後的 B 值分佈圖，數值範圍落於 0~127 之間，數值重複率大幅提升，有效提升壓縮效果。**

(a)

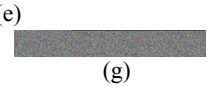
(b)

(c)

(d)

(e)

(f)



(g)

(h)

(i)

(j)

**圖 6 (e)為欲分享的機密高動態範圍影像，藉由分享演算碼產生 4 份影子資訊，分別為(f)~(i)；並透過驗證型資訊隱藏演算法將其嵌入掩護高動態範圍影像，(a)~(d)即為已嵌入影子資訊及認證資訊的偽裝高動態範圍影像；最後，任取通過認證的 3 份偽裝影像皆可還原其對應的完整原始機密高動態範圍影像(j)。**

**表 1 機密影像藉由前置處理前後的比較表，從表中可看出前置處理可有效增加壓縮率及減少壓縮時間。**

| 機密影像 | 解析度 | 壓縮率 | | 壓縮時間 | | 其餘時間 | |
|---|---|---|---|---|---|---|---|
| | | 僅算數編碼 | 含前置處理 | 僅算數編碼 | 含前置處理 | 僅算數編碼 | 含前置處理 |
| 日落 | 720×480 | 53% | 56% | 2.55s | 2.31s | 1.06s | 1.01s |
| 教堂 | 720×480 | 29% | 37% | 51.04s | 3.27s | 1.81s | 1.63s |
| 宮殿 | 660×433 | 29% | 31% | 37.06s | 2.89s | 1.59s | 1.48s |

**表 2 將影子資訊嵌入掩護影像的 PSNR 數據，由圖表可知皆在 35 以上，即肉眼無法分辨與原圖之差異。**

| 機密影像 | 偽裝影像 | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 圖 | 解析度 | PSNR | 圖 | 解析度 | PSNR | 圖 | 解析度 | PSNR | 圖 | 解析度 | PSNR |
| 日落 | 圖 6a | 720×480 | 36.53 | 圖 6b | 720×480 | 39.30 | 圖 6c | 660×433 | 41.09 | 圖 6d | 660×433 | 41.64 |