漸進式機密高動態範圍影像分享演算法
A Progressive Sharing Algorithm for Secret HDR Image

王宗銘 鄭友銘 吳國禎 陶嘉瑋 曾宇田 廖彥凱 林彥宏 陳沛敬 柏傑
國立中興大學資訊科學與工程學系
E-mail: cmwang, s9156048@cs.nchu.edu.tw;
s9356031@mail.cs.nchu.edu.tw

摘要

高動態範圍影像能夠較傳統低動態範圍影像提供更寬容的曝光範圍，因此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，本文首創漸進式的機密高動態範圍影像分享演算法，將機密的高動態範圍影像分享為 n 份影子資訊，藉由其中任意 r 份影子資訊($r \le n$)即可恢復完整之機密高動態範圍影像，若所取得影子資訊未達 r 份仍可恢復部份之機密高動態範圍影像。我們將機密高動態範圍影像的 R、G 及 B 通道分為貝爾圖形資訊及剩餘資訊，並對 E 通道進行無失真壓縮；然後利用漸進式機密分享演算法對壓縮後的 E 通道、貝爾圖形資訊及剩餘資訊分別產生不同機密分享權限的影子資訊，再重新組合成 n 份影子資訊；最後再將 n 份影子資訊分別嵌入掩護的高動態範圍影像中。我們的技術首開先例，成功提供機密資訊一個隱密、可靠、安全的分享方式。

關鍵詞：高動態範圍影像、漸進式機密分享、認證。

Abstract

High dynamic range (HDR) images allow a greater dynamic range of exposures than traditional low dynamic range images. HDR image is more effective to present the realistically colors of the real world. This paper is a pioneer to propose a incremental secret HDR image sharing algorithm. It shares a secret HDR image into n shadow data, and for giving any n shadow data ($r \le n$) can be used to restore the whole secret HDR image, if the number of shadow data obtained is less than r, the secret HDR image could still be restored partially. Our method first splits the R, G and B channel information of the secret HDR image into the Bayer pattern information and remaining information, and the E channel information is compressed by a lossless method. Afterwards, we use a progressive secret sharing algorithm for the compressed E Channel, Bayer pattern information and remaining information to generate shadow data for various authority secret sharing and combine them into n shadow data. Finally, we embed each shadow data into individual cover HDR image. Our algorithm provides a way for sharing secret information privately, reliably, and securely.

Keywords: high dynamic range image, progressive secret sharing algorithm, authentication.

1. 簡介

隨著網路的快速發展，如何在網路上安全的存取機密資訊是一個相當重要的課題，無論是將單份機密資料集中存放，或將其複製多份分開存放，都有其缺點。前者如遭到破壞或遺失，則機密資訊則同時遺失。後者則大幅提升了遭到竊取或破解的可能性[3, 9, 11]。

機密分享(secret sharing)[2-5, 9, 11-15]為一兩全其美的解決方法，其主要概念由權限分享衍伸而來，機密資訊(secret data)透過機密分享產生 n 份影子資訊(shadow data)，只要取得其中門檻值 r 份的影子資訊($r \le n$)，即可還原完整原始機密資訊。

傳統的機密影像分享，若拿到的影子資訊數量小於門檻值 r，則無法窺見機密影像的任何一個部份。漸進式(progressive)機密影像分享改良僅有單一門檻值的缺點，藉由多重的門檻值，即使取得的影子資訊數量未達最高門檻值，仍然可以還原機密影像的整體輪廓。取得越多的影子資訊，還原的機密影像亦越接近原圖，最後，當取得最高門檻值的影子資訊後即可還原完整的原始機密影像。因此，機密影像可隨著影子資訊的逐漸取得，漸漸恢復原貌，此外，若部分影子資訊不幸遺失或遭受破壞，仍可還原部份的機密影像。

高動態範圍(high dynamic range)影像相較於傳統的低動態範圍(low dynamic range)影像，色彩表示能力遠遠超過低動態範圍影像，可更有效的呈現自然世界的真實色彩[8, 10]。

有鑒於高動態範圍影像與低動態範圍影像的先天差異，及其趨勢與重要性，本文提出漸進式機密高動態範圍影像分享演算法。由於高動態範圍影像存在著許多不同的格式，本文針對較常見的光輝(radiance) RGBE 格式進行研究。

首先，我們將高動態範圍影像的 R、G 及 B 以貝爾圖形(Bayer pattern)的方式進行排列，將其用於低階門檻值的機密分享，產生低階門檻值的影子資訊，剩餘的像素資訊則以高階門檻值做機密分享，產生高階門檻值的影子資訊，最後再把低階與高階門檻值的影子資訊重新排列，產生漸進式還原的影子資訊。若只取得低階的門檻值數量的影子資訊進行還原，即可得到以貝爾圖形排列的高動態範圍影像，我們利用影像內插法對影像進行修補，重建每個像素所欠缺的色彩元素，使圖片品質提升。若取得的影子資訊數量，高於最高門檻值，則有足夠的資訊還原完整的機密資訊。此外，由於影子資訊以雜訊方式儲存，在傳輸過程中，容易遭到有心人士的注意甚至進而竄改或破壞，故我們利用高動態範

圖影像資訊偽裝演算法[6]，將影子資訊嵌入高動態範圍影像的平滑像素與邊界像素中，使人不易察覺影子資訊的存在。

本文架構如下：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

本節簡介傳統低動態範圍影像的機密分享演算法，並介紹目前在低動態範圍影像上的漸進式影像分享演算法。

Blakley[7]和 Shamir[1]最早提出機密分享的概念，即所謂的 $(r\ ;\ n)$ 門檻法（$(r\ ;\ n)$ threshold scheme）。$(r\ ;\ n)$門檻法係利用多項式將機密資訊分為 n 份影子資訊，影子資訊內容皆為多項式分解結果，所以看似雜訊，不具有意義。另外，r 則為還原的門檻值($r \le n$)，必須取得至少 r 份影子資訊，才可透過解方程式取得原始的完整機密資訊。

Thien 和 Lin 改良 Blakley 和 Shamir 的$(r\ ;\ n)$門檻法[3]，將方程式中的係數皆以機密影像的像素值代入。由於門檻值為 r 的方程式中，會有 r 個係數，故影子資訊的大小可有效降至原始機密影像的 $1/r$，大幅降低空間與頻寬的需求。

Chen 和 Lin 以 Thien 和 Lin 的方法為基礎，提出了漸進式的機密影像分享技術[13]，除了原始的 r 和 n 門檻之外，加入了 k 門檻值，k 即為多重門檻值的數量，亦即可分為門檻值 $r_1, r_2, \ldots, r_k$，且 $r_1 \le r_2 \le \ldots \le r_k = r$，其中 $r_k = r$ 即為最高門檻值。他們隨後將機密影像分為若干區塊，每個區塊有 $RSUM$ 個像素值($RSUM = r_1+r_2+\ldots+r_k$)，每個區塊中的像素值皆由最高位元至最低位元依序重新排列。最後，將取得的特徵值分別以多重門檻值 r_1 至 r_k 分別進行機密分享。例如，當 $k = 3$，三個門檻值分別為 2，3 及 4，故 $RSUM = 2+3+4 = 9$。隨後，每 9 個像素視為一個區塊，假設取得的 9 個像素值分別為 166，167，164，166，168，165，163，166，168，由最高位元至最低位元依序重新排列即可取得新的特徵值，如圖 1 所示。順著箭頭方向從最高位元起，每 8 個位元為一組重新排列位元即可得到 9 個新的特徵值，分別為 255，128，63，224，0，143，171，76，140。將前 2 個數值代入門檻值為 2 的分享方程式，中間 3 個數值代入門檻值為 3 的分享方程式，最後面 4 個數值也同樣帶入門檻值為 4 的分享方程式。如此一來，即使只拿到 2 份影子資訊，也可先解開機密影像重要的最高位元，即可恢復影像輪廓，隨著取得越多的影子資訊，即可慢慢還原像素值的低位元資訊，進而還原影像細節。

雖然上述之方法可在傳統低動態範圍影像得到漸進式的效果，然而，目前尚未有人提出高動態範圍影像的漸進式機密分享技術。由於高動態範圍影像具有較高的色彩範圍，勢必需要利用不同的技巧達到還原品質良好且檔案大小合宜的漸進式分享。鑒於高動態範圍影像的優點及未來趨勢，本文根據高動態範圍影像的格式及特性，首創漸進式機密高動態範圍影像分享技術。

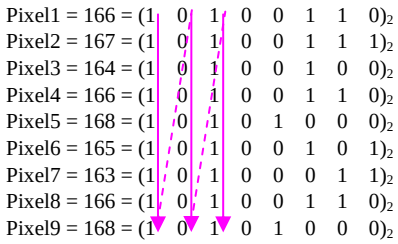


圖 1. 漸進式分享分組示意圖。

光輝 RGBE[8]為高動態範圍影像最常見的格式之一。光輝 RGBE 將原本各以 32 位元浮點數表示的 RGB 轉換為 RGB 各以 8 位元表示並共用一個 8 位元的指數 E，共 32 位元的整數格式，雖然此舉會造成些微影像精細度的損失，但卻可大幅降低所需的儲存空間，故其儼然成為高動態範圍影像的主流格式之一。是故，本論文針對此最常見的高動態範圍影像格式提出漸進式機密高動態範圍影像分享技術。

3. 漸進式高動態範圍影像分享演算法

本論文提出一個漸進式機密高動態範圍影像分享技術，其流程如圖 2 所示。

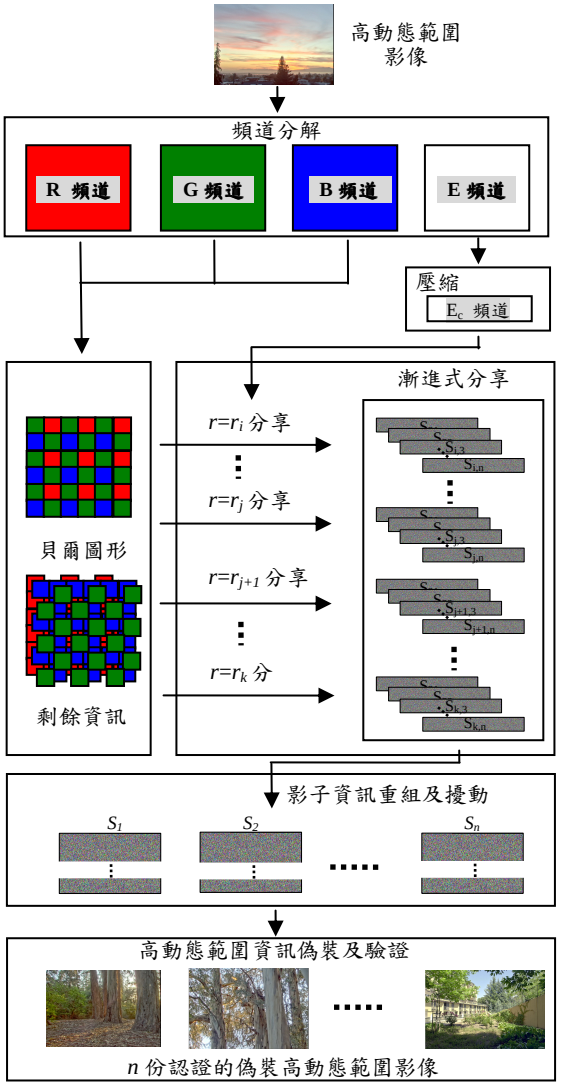


圖 2. 機密高動態範圍影像之分享與偽裝流程圖

演算法區分為六個步驟：1. 頻道分解、2. E 頻道壓縮、3. 貝爾圖形濾波、4. 漸進式分享、5. 影子資訊重組及擾動、6. 高動態範圍影像資訊偽裝及驗證。首先，輸入機密的高動態範圍影像，將 R、G、B 及 E 各頻道的數值從原始的機密影像中取出；接著對 E 頻道從事無失真壓縮演算法，產生壓縮後的 E_c 資料串；隨後，利用貝爾圖形濾波器對 R、G 及 B 三頻道進行過濾，使其分為貝爾圖形及剩餘資訊；接著，以漸進式機密分享演算法，對 E_c 資料串、貝爾圖形資料串及剩餘資訊資料串做不同權限的機密分享，產生各權限分享的影子資訊，其中，$r=r_i$ 時為對 E_c 資料串、貝爾圖形資料串做分享，$r=r_{j+1\sim k}$ 時為對剩餘資訊資料串分享， i 為最小的權限分享，k 為最大的權限分享值，即擁有 k 份可完全還原原始資訊，並將其重新組合成 n 筆影子資訊，並分別對各影子資訊加入密鑰進行擾動，以增加各影子資訊的安全性；再者，利用高動態範圍資訊偽裝演算法，將影子資訊藏入掩護影像，輸出 n 張含有影子資訊的偽裝影像；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 節說明機密高動態範圍影像經由漸進式分享技術產生 n 筆影子資訊的方法；3.2 節詳細說明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 節說明如何藉由取得的偽裝影像，漸進式還原原始機密高動態範圍影像，並利用貝爾圖形及影像內插法達到更高的影像還原品質。

3.1 漸進式高動態範圍影像分享技術

由於高動態範圍影像與傳統低動態範圍影像與生俱來的差異，我們首先需根據高動態範圍影像的特性將 RGBE 拆解為四個分離的頻道，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；並且，為縮減欲分享的資料量，就此整數型態 E 頻道值之特性採用適用的無失真壓縮演算法。高動態範圍影像的 E 值分佈往往擁有相同數值緊鄰集中的特性，故使其具有較高的壓縮效率，在此我們針對 E 頻道使用自適應模型的算術編碼(adaptive arithmetic coding)方法進行壓縮，以減少所需分享的資訊量，使其更能夠有效的藏入偽裝影像中。

隨後，為了在漸進式分享演算法中，達到在僅獲得到少量資訊時就能夠恢復較高品質的影像效果，在這裡我們提出以貝爾圖形的排列方式，將 RGB 頻道數值加以排列，使其分為貝爾圖形排列的資料串以及剩餘資訊的資料串兩個部份。貝爾圖形的部份，我們在每一個像素中只取出 RGB 其中一個頻道的影像數值，其排列的方式是以紅綠交錯成一列，綠藍交錯成另一列，使三個頻道的數值能均勻的分布在每個區域。其中，由於 G 頻道數值包含了大部分的亮度資訊，而人眼對亮度的變化比色彩的變化來的敏感，是故，在此保留 G 頻道的數值比 R 及 B 頻道數值多了一倍，使其能夠在保有少量資訊的前提下，擁有更好的影像效果，如圖 3 所示。

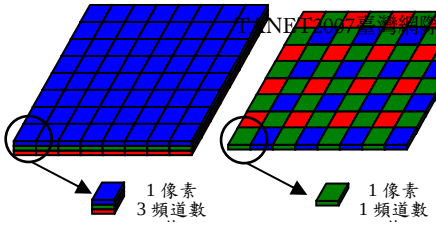


圖 3.貝爾圖形排列示意圖

除了用以構成貝爾圖形的 RGB 像素值外，其餘的部份即為剩餘資訊的資料串，如圖 4 所示。

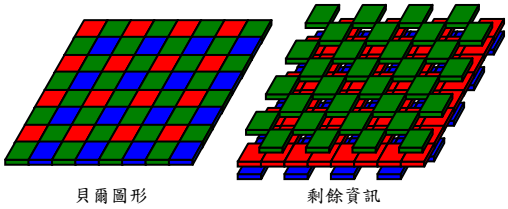


圖 4.貝爾圖形與剩餘圖形。

在此論文中，如何在僅取得少量影子資訊的前提下，即可達到高品質的漸進式高動態範圍影像效果是我們的主要研究議題之一。因此，我們在提出的漸進式機密高動態範圍影像分享演算法，首先針對 E 頻道及貝爾圖形的資料串從事低階門檻值的機密分享，產生低階門檻值 i 的影子資訊，亦即在 n 份影子資訊中，只要取得 i 份的影子資訊($i<r<n$，i>=最低門檻值)，即可還原高動態範圍影像的部分重要資訊，得到良好的視覺效果。其中，由於 E 值在高動態範圍影像中為決定 R、G 及 B 各頻道真實像素值的重要參考依據，是故，我們必須使 E 頻道值可在取得最少門檻值的影子資訊時即可完全還原。

為了簡化說明我們提出的演算法，在這裡我們假設 $k=3$，並且以 $r_1=2$，$r_2=3$、$r_3=4$ 為例，亦即取得四份影子資訊時即可完全還原原始的高動態範圍影像；首先，我們將貝爾圖形的資料串重新排列，得到我們期望的漸近式還原效果，這裡我們假設在 r_1 的部份，可以還原貝爾圖形資料串每個數值的前三個位元，因此我們將貝爾圖形資料串每個數值的前三個位元取出，且由於 r_1 為最低門檻值，所以必須將壓縮後的 E 頻道數值一併取出，並以八個位元為一組得到 r_1 的資料串 D_{r1}；在 r_2 的部份，我們假設可以還原貝爾圖形的剩餘部份，所以我們將貝爾圖形資料串中每個數值的後五個位元取出，以八個位元為一組得到 r_2 的資料串 D_{r2}；在 r_3 的部份，我們假設可以完全還原原始影像，所以我們將剩餘圖形的資料串取出，並以八個位元為一組得到 r_3 的資料串 D_{r3}，如圖 5 所示。

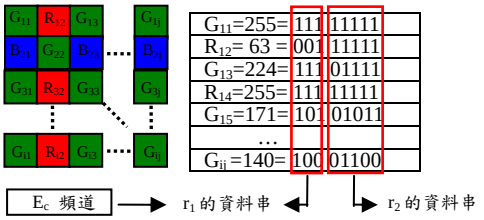


圖 5 r_1 及 r_2 分享資料串示意圖。

由於經過重新排列後所得到的資料串在使用分享演算法做分享時，需模一個質數。然而，因為

251 為不超過 255 的最大質數，但是，其資料串內的數值分佈目前仍介於 0 到 255 之間，若直接將數值模 251 則會造成部分的失真，為了確保分享後資料的正確性，故我們需先以方程式 1 將數值展開，令數值分佈範圍重新落於 0 到 250 之間，得到無失真處理後的資料串 D_{r1}'、D_{r2}'及 D_{r3}'。藉由此法，我們可以無失真地將其再逆推回原始的資料串 D_{r1}、D_{r2}及 D_{r3}。

$$D' = \begin{cases} D & if \quad D < 250 \\ (250,\ D-250) & if \quad D \geq 250 \end{cases} \qquad (1)$$

接著，將資料串 D_{r1}' 、D_{r2}' 及 D_{r3}'切割成數個區段，每個區段分別含有 r_1、r_2及 r_3個值，且資料串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，其中 *r* 分別為 r_1、r_2及 r_3的門檻值，如方程式 2。

$$q^r{}_s(x) = (a_0 + a_1 x + ... + a_{r-1}x^{r-1}) \bmod 251 \qquad (2)$$

其中，$a_0, a_1, \ldots, a_{r-1}$ 為各區段的 *r* 個數值，*s* 為區段的編號，藉此方程式可計算出 r_1、r_2及 r_3的影子數值 $q^r{}_s(1), q^r{}_s(2), \ldots, q^r{}_s(n)$，亦即 r_1、r_2及 r_3的各 *n* 個影子資訊。

最後，將 D_{r1}'、D_{r2}'及 D_{r3}'這三個資料串經過分享演算法產生的各 *n* 個影子資訊，隨即重新加以組合，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擾動的動作，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偽裝

依 3.1 節之方法產生的影子資訊，是以雜訊的方式儲存，為了降低被有心人士察覺的風險，提升傳輸的安全性。故我們提出藉由單向雜湊函數(one-way hash function)確認偽裝影像之正確性。

認證型高動態範圍影像資訊偽裝演算法共可分為三個步驟:1. 像素分類、2. 區塊處理以及 3. 邊界處理。

像素分類：高動態範圍影像中，E 值為決定 R、G 及 B 浮點數數值的共用指數數值，所以相鄰的像素其 E 值通常相同或相近，根據此一特性可推論出，像素相鄰且 E 值相同稱之為區塊；反之，若像素相鄰但 E 值相異，則稱之為邊界。

區塊處理：區塊的部分使用雙邊界(two - sided)的區塊相配演算法，根據被指定之像素的上方像素與左方像素之間的差異，決定嵌入的資訊量。像素處理方向如圖 6 所示：灰色部份為參考像素，都使用最低有效位元取代的方法嵌入一個位元。白色部份則是以區塊相配演算法根據影像之間的變異程度嵌入不定量的資訊。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 86 個像素暫時保留，不予嵌入影子資訊，如圖 6 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我們僅以最低有效位元取代法嵌入 1 位元，如圖 6 標記為 LSB 之綠色區塊。

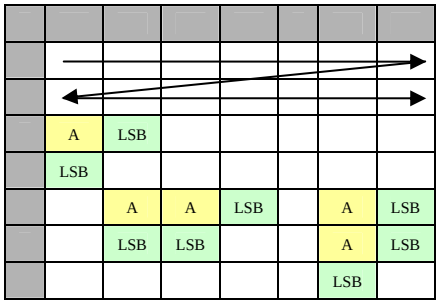


圖 6 雙邊界區塊相配演算法之像素處理方向圖

邊界處理：相鄰的像素 E 值若不相同，在影像中是屬於邊界的的像素，所以無法直接使用區塊相配演算法嵌入資訊。嵌入資訊之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 轉為相同的數值，但 E 值轉換後，R、G 及 B 也要隨之調整，使其浮點數值接近轉換 E 值前的數值，但如果轉換後 R、G 及 B 超過 255，必須強迫轉換為 255。

待影子資訊已全數嵌入完畢後，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 86 個像素，並將其餘的影像像素值以雜湊函數 SHA-256(secure hash algorithm)產生認證碼。根據 SHA-256 演算法之特性：無論待認證資訊之長度為何，我們最終皆可得到 256 位元的認證碼。此外，我們將此 256 位元之認證碼除以 4 後取其餘數，再將此 2 位元之數值，置於 256 位元認證碼之後，故我們共可得到 258 位元之偽裝影像認證碼，如圖 7 所示。最後，我們將此 258 位元的認證碼以密鑰產生的亂數拆成 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 86 個像素的 R、G 及 B 之中

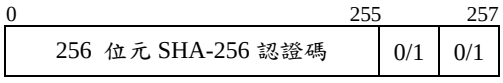


圖 7 偽裝影像認證碼示意圖

取出資訊時，先以密鑰找出原先嵌入偽裝影像認證碼的 86 個像素，並從中取出認證碼，隨後以 SHA-256 之演算法判斷偽裝影像之完整性，若通過認證，開始擷取已嵌入偽裝影像中之影子資訊。

3.3 漸進式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，從內嵌有影子資訊的偽裝高動態範圍影像中，透過嵌入之認證碼確認該偽裝高動態範圍影像之正確性與完整性，若該偽裝影像通過認證則可確保其未遭受惡意地竄改，故可順利從中取出內嵌的影子資訊，並藉由密鑰還原原始影子資訊的排列順序，並將其拆解為各門檻值的影子資訊。其中，若取得的影子資訊份數不足以完全還原原始高動態範圍影像，則在這裡我們可以藉由漸進式的還原取得高品質的近似原始影像。首先，若我們可以得到低階門檻值的影子資訊份數，則可以取得完整的 E 頻道數值，以上述 *k*=3 之例而言，其中 r_1=2，r_2=3、r_3=4，我們可以在取得 r_1 門檻值之影子資訊時，同時藉由機密解分享得到貝爾圖形資料串的前三個

位元，藉由貝爾圖形之特性，在這裡我們使用方程式 3 的影像內插法對所得到的漸進式還原影像作影像修補，藉由既有的影像資訊內插取得未知的影像資訊，其中 C 為欲修補的頻道值，C_1~C_8 為其四周的頻道值，N 為 C_1~C_8 中有數值的個數，如圖 8 所示。

$$C = \sum_{i=1}^{8} C_i / N \qquad (3)$$

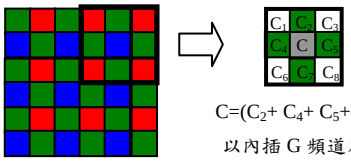


圖 8. 利用內差法求得未知的影像資訊。

影像內插後，由於我們所得到的影像只有貝爾圖形的前三個位元為真實資訊，因此後面五個位元仍然為未知的資訊，是故我們以五個位元所能表示數值的中間數來作為未知的影像數值，如方程式 4，以達到更高品質的漸進式高動態範圍影像。其中，*m* 即為尚未還原的位元數。而若我們可以得到更高門檻值份數的影子資訊，則藉由機密解分享，可以得到更趨近於原始的機密高動態範圍影像。

$$V = V + 2^{m-1} - 1 \qquad (4)$$

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漸進分享的過程。

圖 9(a)為欲分享的機密高動態範圍影像，圖 9(b)至圖 9(e)為將分享後的影子資訊嵌入四張高動態範圍偽裝影像的結果，其偽裝影像與原圖的 PSNR 介於 29.5 至 36.2 之間，擁有不錯的相似度。一般來說以肉眼難以察覺其變化。

圖 10(a)至圖 10(c)為由最高位元開始還原相同比例的 R、G 及 B 的高動態範圍影像結果，由於圖中每個像素的 R、G 及 B 的資料量皆相等，所以無法進行內插。圖 10(d)至圖 10(f)則是在還原時，以貝爾圖形的概念進行 R、G 及 B 不同比例的還原，由於每個像素都只有 R、G 或 B 其中一個頻道的資訊，所以使用內插的方式取得像素中沒有的頻道資訊，由圖中可看出以貝爾圖形的排列進行還原並內插的效果明顯就優於 R、G 及 B 的等量還原，而圖片說明的 *PSNR*（peak signal to noise ratio）定義為方程式 5。

$$PSNR = 10 \log\left(\frac{255^2}{MSE}\right) \qquad (5)$$

其中，*PSNR* 越高則代表嵌入前後的失真越少。表 1 則說明了兩種還原方式的 *PSNR* 比較，從表中也可清楚發現，在相似的還原比例下，還原順序貝爾圖形排列並進行內插後的 *PSNR* 值比還原等量比例的方法明顯較高。

由實驗結果可發現，在拿到未達到最高的門檻值的影子資訊時，若資訊還原的順序是以貝爾圖形的方式進行排列並且進行內插，其影像品質比從最高位元等量還原 R、G 及 B 明顯較佳。

5.結論與未來工作

鑒於高動態範圍影像的發展，本文首創了漸進式機密高動態範圍影像分享演算法，並以貝爾圖形的方式對機密影像像素進行排列後再進行分享，以此增加影子資訊未達到最高門檻時的還原品質，並使用認證型高動態範圍影像資訊偽裝演算法將分享後的影子資訊嵌入掩護影像中，使其傳送時不易遭到察覺其存在，也以 SHA-256 認證的方式確保影子資訊完整性，以免由錯誤的偽裝影像中取出影子資訊，總結本研究：我們提出一個有效的漸進式機密高動態範圍影像分享演算法，即使影子資訊未達到最高門檻值，依然可還原機密高動態範圍影像的部分資訊，其還原的資訊順序在以貝爾圖形排列並進行影像內插，增加影像品質，並透過資訊偽裝產生視覺效果良好的偽裝影像，達到隱密、可靠且安全的分享。

未來工作上，我們將朝下列方向研究：第一、減少影子資訊量：目前本方法只針對 E 頻道進行壓縮，希望將來能對其餘頻道有效進行壓縮，減少影子資訊量。第二、增加其廣泛性：目前本文只針對光輝 RGBE 的高動態範圍影像進行分享，未來希望能延伸到其他的高動態範圍影像格式繼續研究。

致謝

本研究承蒙國科會之經費補助(96-2815-C-005 -053 -E、96-2815-C-005 -054 -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.

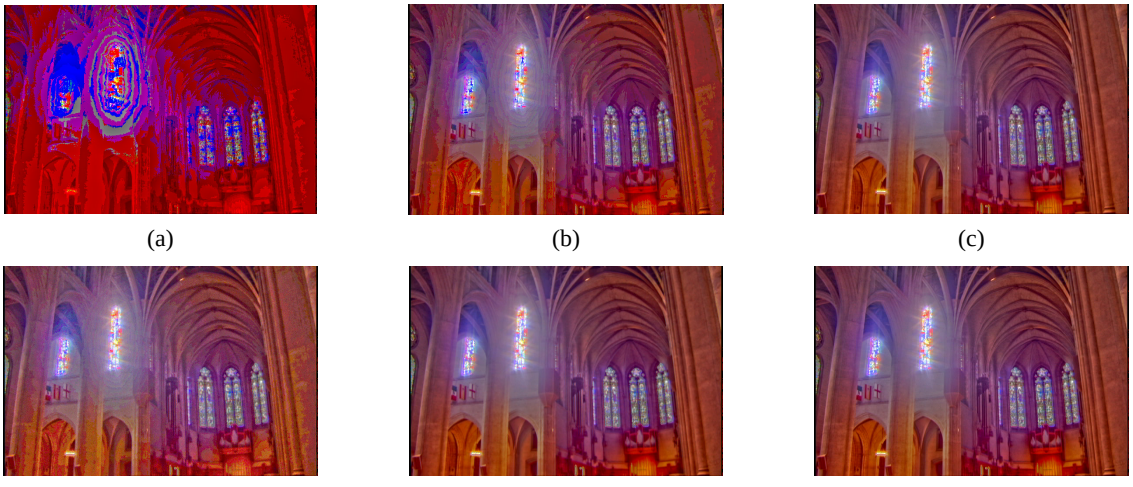
[6] C. M. Wang, Y. M. Cheng, Y. P. Tzeng, H. W. Kan, Y. H. Huang, P. Y. Leu, Y. S. Hsieh, “A Novel Data Hiding Algorithm for High Dynamic Range Image,” Taiwan Network Conference, 2005.

[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] Y. C. Hou, “Visual cryptography for color images,” Pattern Recognition Vol. 36, pp.1619-1629, 2003.
[15] Y. S. Wu, C. C. Thien, and J.C. Lin, “Sharing and hiding secret images with size constraint,” Pattern Recognition Vol. 37, pp.1377-1385, 2004.

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

圖 9 (a)為欲分享的高動態範圍影像教堂；(b)至(e)為將影子資訊嵌入後的四張偽裝影像，其 PSNR 介於 29.5 至 36.2 之間。



(a) (b) (c) (d) (e) (f)

圖 10 教堂的實驗結果:(a)~(c)為還原順序非貝爾圖形排列也無內插，(d)~(f)為還原順序為貝爾圖形排列並且內插。其中(a)及(d)為兩份影子資訊的還原結果；(b)及(e)為三份影子資訊的還原結果；(c)及(f)為四份影子資訊的還原結果(無失真)。

表 1 有無使用貝爾圖形及內插的還原之 PSNR 的比較。

		兩份影子資訊還原影像		三份影子資訊還原影像		四份影子資訊還原影像	
		還原比例	PSNR	還原比例	PSNR	還原比例	PSNR
教堂	非貝爾圖形無內插還原	30.5%	13.36	53.1%	26.68	100%	Lossless
	貝爾圖形內插還原	30.5%	24.55	50.0%	33.06	100%	Lossless