以物件為基礎的高動態範圍機密圖像分享研究
An Object-based High Dynamic Range Secret Image Sharing Method

黃金本　蘇昱軒　許孟妤　曾奕傑　徐竹君
銘傳大學 資訊傳播工程學系
hcptw@mail.mcu.edu.tw ;
{ gary_82002, winnie93, yes_man0913, juntain1211 }@hotmail.com.tw

摘要

隨著網際網路的普及,如何安全地傳輸、保存、與有效率的存取多媒體資料,成為非常重要的議題;而高動態範圍圖像為未來的潮流,目前已廣泛的受到重視。本文提出以物件為基礎的高動態範圍機密圖像分享方法。我們的方法包括三個步驟:首先,將HDR 圖像分割成幾個重要的物件和記錄物件的坐標及相關資訊。第二,使用機密圖像分享方法,對生成的物件和記錄資訊採用不同重要性的方式進行分享。第三,利用拉格朗日內插法重建各個物件。我們的方法具高安全性,且為使用者提供非常方便和有效的重要物件重建方法。實驗結果證實所提出的方法的有效性。

關鍵詞：高動態範圍圖像、圖像分享、分存圖像

Abstract

With the popularity of the Internet, how to securely transmit and store multimedia data, and effectively access them has become an issue of great concern. The high dynamic range (HDR) image as a trend of the future has been extensive attention. In the paper, we propose an object-based secret HDR image sharing method. Our scheme includes three stages. First, we segment an HDR image into several important objects and record related coordinates of the objects in a header file. Second, we employ the secret image sharing method to share with a unequal importance way for the produced objects and the header file. Third, the object can be reconstructed using Lagrange interpolation method. As a result, our method is highly secure and provides users a very convenient and effective reconstruction way for the important object. Experimental results illustrate the effectiveness of the proposed method.

Keywords: high dynamic range image, image sharing, shadow image

1. 前言

近年來，隨著科技的發展，資訊保存及傳送方式從以前的紙筆、留聲機等類比的方式轉變成現在的數位化；且越來越多人喜歡透過電腦、手機等資訊設備來進行資料保存及傳輸。然而，這些保存的資料，若是集中保管，一旦遭到破壞或是遺失，那資料將嚴重的受損，甚至可能全部被破壞而無法再度被取回。同時在這資訊時代，資訊安全顯得格外重要，當數位的機密圖像在傳遞時，為了避免被竊取或攔截，必須採取一些保護措施，例如將資訊隱藏、加密或資訊偽裝等，其中「機密圖像分享」也是保護機密的一種方法，就像某個行政單位在傳送機密文件時，在傳送文件的過程中，資料可能會遭到竊取、竄改、偽造等等的情形，一旦發生這些情形，對該公司或該行政處的危害是非常大的，所以確保資料安全的問題已不容小覷。

在這個資訊化的時代，犯罪方式層層多變，保護這些機密資料實在是非常的不容易，所以必須要加強它的安全性，通常會對這些機密資料做加密，以及資料隱藏的動作，但是在隱藏的資料當中，有時只需要整份資料中的一小部分，卻因為這一小部分，使得我們必須將整份機密文件完全取出，才可以得到想要的部分，這造成使用的不便，而在本專題針對這點力求突破，提出以物件為基礎的概念，發展機密圖像分享的方法，希望能在這方面有所進展，可以將過程簡化，不必將整份文件取出，就可以得到我們所需要的部分。

近年來，關於圖像分享的研究非常多，大多數的研究都是出自於加強機密文件的安全性，進而開始研究這個領域，本文要做的研究是除了可以保有機密文件的安全性之外,再增加它的方便性,例如：對偷窺者而言，以物件為基礎的分享概念就如盲人摸象，大象的各部位為機密圖像的物件，必須得到全部的部位才能得知完整的物體為大象，而得到部分的部位，則只能對原始之樣貌進行猜測。如盲人摸到的部位為腿，偷窺者可能以為這個物體為樹幹；又或者摸到的部位為耳朵，可能被認為是畚箕，如此一來套用在機密物件的分享當中，若只知道其中一個物件只能了解一小部分，則機密性便增加許多。對系統使用者而言，物件分享可以提供很方便的介面，僅針對所需要的部份進行解碼，得到所需要的物件。而高動態範圍圖像為未來的潮流，此種格式的圖像可以保存真實的色彩圖像，目前已廣泛的受到重視。

本文於第二節探討相關文獻；第三節提出研究方法；第四節為實驗結果。最後，第五節提出結論。

2. 文獻探討

本章介紹機密分享相關的文獻，對幾種基本機密分享方法進行詳細探討。首先，介紹高動態範圍圖像格式[1]，再介紹兩個具影響力之機密分享方法：Shamir[2]所提出之(r,n)門檻機制及 Thien 及 Lin 機密圖像分享方法[3]，最後介紹小分存機密圖像分享與應用分享技術的圖像認證方法。

高動態範圍圖像演算法的特性是它的頻道不同於以往的低動態，高動態範圍的照片是由 R.G.B.E.的四個頻道所組成的，而以往的一般照片則是由 R.G.B.三個頻道所組成，其中 E 頻道是代表 RGB 像素值中的指數部分，為區隔出和一般照片不同的地方。高動態範圍能夠將圖片色彩更完整的呈現出來，清晰度提升，模糊不清或感光度低的圖片，經過 Photoshop 軟體加工後，更加明亮清晰，讓人看得更清楚，但也因為這樣，色彩範圍變得更大，在處理時間上會比較久一些。

在 Shamir 所提出的其中一項資料分享技術為(r,n)門檻理論，其技術原理是將一份重要資訊 D，利用分享方程式將資料分存成n份(D1,D2,…,Dn)，使用者必須收集r份分存資料或r份以上時，才能將重要資訊 D 重建，反之則無法將資料還原。

根據此理論，要將重要資訊 D 分成n份分存資料，要先取一個質數 p 以及一個$r-1$次的多項式：

$$q(x)=(a_1+a_2x+\cdots+a_rx^{r-1})\ mod\ p$$

其中，a_0=D，$(a_1,a_2,\dots,a_r)$為介於 0 到(p-1)之間隨機所產生的亂數。在資料還原階段，當我們從n份分存資料中取得任意 r 份分存資料與對應之鍵值時便可帶入重組方程式中得到r個含有r個未知數的多項式，$(a_1,a_2,\dots,a_r)$可以利用拉格朗日內插法(Lagrange interpolation) [4]依序求出其解，而a_0便是原本的重要資料。

Thien 及 Lin 以 Shamir 的(r,n)門檻理論為基礎提出一個機密圖像分享方法，將一張機密圖像先做像素調整，像素值大於 250 以上得像素點(251~255)改成 250 計算。接著將圖像分成多個分享區塊，每一個包含 r 個像素。對每一個分享區塊（以第 j 個區塊為例），將其像素值分別代入下列方程式的係數a_0,a_1,...,a_r中，來得到這個區塊的分享方程式：

$$q_j(x)=(a_1+a_2x+\cdots+a_rx^{r-1})\ mod\ 251$$

在建立一個區塊的分享方程式後，我們可分別帶入n個鍵值 k_1,k_2,...,k_n來得到產生$q_j(k_1),\dots,q_j(k_n)$，得到n個像素，這些像素即分別儲存到n張分存圖像中的地j個位置點。根據上述方式將整張圖像的所有區塊處理完，我們便可得到n張分存圖像，而產生的每張分存圖像為原機密圖的 1/r倍。當使用者收集到分享階段所建立r張時，便可依序從每張分存圖像中取得一個點，如同 Shamir 的方法，將得到的r個[鍵值,點資料]配對代回至方程式中來得到一個包含r個方程式的方程組，這個方程組得每一個方程式都有r個未知數a_0,a_1,...,a_r。利用拉格朗日內插法再重複上述步驟將分存圖像中所有點處理完，即可以還原出整張原機密圖像。小分存機密圖像分享與應用分享技術的圖像認證方法[5]，文獻中主要分為兩部分：

第一部分提出小分存機密圖像分享技術，將一張圖像分成n張較小的圖像分存，這些分存圖像被分開傳輸與儲存。當使用者收集到n張分存圖像中的r張或以上時，即可重建出原圖像，否則無法得到圖像中的任何資訊。

第二部分是自動修復破壞的圖像驗證技術，文中利用(r,n)門檻理論，將區塊量化後的索引值分散並隱藏到其他區塊中，來增強圖像自動恢復的能力。然而他的優點是可以將分存圖像較小，利於網路上傳輸儲存，亦可分散儲存，即使有遺失仍可從其他圖片中取得，還具有較高的容錯性，即使圖像自動修復後的圖像品質與原圖以肉眼幾乎看不出有明顯差異;反之缺點則是不易分析出資料嵌入所有區塊的規則性。

經研究了許多相關文獻後，我們發現，過去的研究都選擇以整個圖像進行分享，會造成使用者的不方便，若不是整張圖像都為重要機密的部分，資料的傳送與儲存將占用許多記憶體空間。在本專題，我們提出以物件為基礎的概念，將使用者認為極為重要或機密的部分，分別視為物件，更能節省許多傳送與存取的記憶體，更可以有效率的重建想要的機密圖像，使重建過程更簡化，方便使用者，且更能提升分享之機密性。

3. 研究方法

我們提出的研究方法包括三個步驟：首先，進行系統所需之前置工作。將 HDR 圖像分割成幾個重要的物件和記錄物件的坐標與重建所需的資訊標頭檔。第二，進行圖像分享。使用機密圖像分享方法對生成的物件和記錄資訊採用不同重要性的分享方式。第三，進行圖像重建。利用拉格朗日內插法對及各個物件所需的分存圖像進行重建物件。研究方法的流程如圖 1，詳細的技術說明如下。

3.1 前置工作

如圖 2 所示，在本次研究中採用文獻探討中提到的高動態範圍圖片(HDR)，它能夠凸顯比傳統低動態圖像還要更鮮明的色彩顯示能力，如此一來便可以將各物件的輪廓清楚的呈現出來。

首先要做的動作是製作 HDR 圖片，使用的軟體為光影魔術手以及 Photoshop，以下為製作 HDR 的步驟：

步驟 1：先開啟光影魔術手軟體。

步驟 2：開啟三張或三張以上欲製作成高動態範圍的照片，禁止使用曝光值一樣的照片，曝光值一樣將無法製作 HDR。

步驟 3：使用軟體中的「批次處理」功能，將圖片中的些許位移誤差去除。

步驟 4：接著開啟 Photoshop，加入已做完批次處理

的照片。

步驟 5：軟體參考加入之三張照片製作出 HDR，最後輸出，而存取必須使用 32 位元儲存。圖 3 之各圖片((a), (b), (c), (d))根據原圖之比例呈現，採用前述步驟所建立起來的高動態範圍(HDR)的圖像，可以將一般正常相片無法清楚呈現出來的文字圖像部分清楚顯示出來。

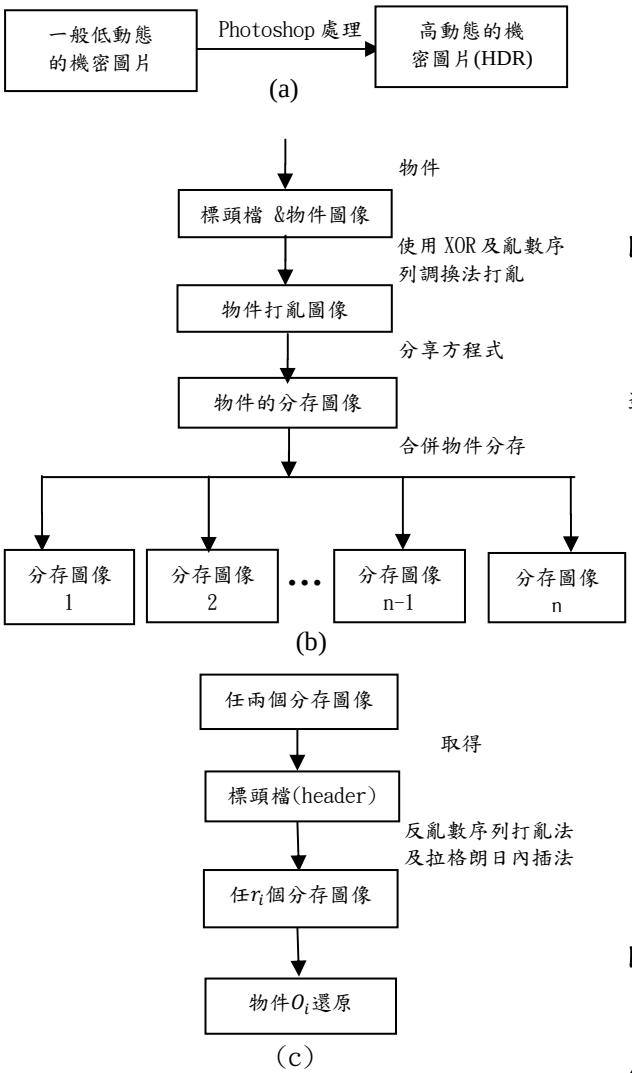
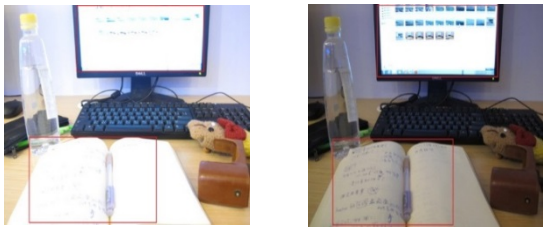


圖 1. 研究方法流程圖(a)圖片製作流程圖，(b)分享階段流程圖，(c)還原階段流程圖



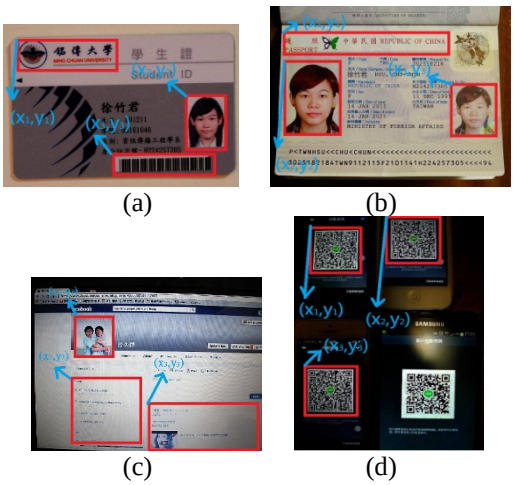
(a) (b)

圖 2 高低動態範圍圖片(a) 傳統低動態範圍，(b) 高動態範圍(HDR)

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

圖 3 HDR 圖片：(a) 學生證(尺寸:441×640)，(b) 護照(尺寸:509×682)，(c) 網頁個人資料(尺寸:514×680)，(d) QR code(尺寸:697×520)

為確定讀入程式之圖片中有多少個物件，須先進行分割，圖 4.為一例：



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

圖 4 物件切割示意圖： (a) 學生證，(b) 護照，(c) 網頁個人資料，(d) QR Code

本文將背景亦視為一個物件，因此圖象中有四個物件。切割原則是將物件區隔開來，將這些區塊視為物件處理，其處理步驟如下：

步驟 1：根據分割物件的長和寬及左上角的座標(x_i,y_i)來清楚地描述物件之位置。

步驟 2：若將一個物件內的所有數值放進一個矩陣當中，則 t 個物件就會有 t 個對應的矩陣。將這些資訊儲存在標頭檔中，以為重建時使用。

3.2 圖像分享

圖像分存階段的最主要工作，是將一張欲保護的高解析度機密圖像，透過分享方法來建立n張的物件分存圖像，這些物件分存圖像可以被分開儲存與傳送，來提高機密圖像資料的安全性與方便性。於本研究，對各個物件採用不同重要性的分享方式，

即採用(r_i, n)門檻機制，而$2 \le r_i \le n$，各個r_i分別為標頭檔與各物件的重建時所需要的分存圖像數，以下為分享步驟：

步驟 1：選擇一張欲分享的機密 HDR 圖片。

步驟 2：選定欲隱藏之機密物件範圍，假設物件分割成O_1，O_2，…，O_m四個物件的圖片，若 m=4 則結果如圖 4，並記錄物件之座標資料成標頭檔。

步驟 3：將圖片像素值使用mod 251，大於 250 像素值展開並且重新排列。

步驟 4：將展開後的物件及標頭檔採用不同的r_i值(像素個數值)代入公式(1)。

$$q_j(x) = \left(a_1 + a_2 x + \cdots + a_{r_i} x^{r_i - 1}\right) mod\ 251 \quad (1)$$

J 表示物件中對應之區塊。

步驟 5：接著進行的就是資料打散，將各物件像素值與金鑰進行 XOR 互斥邏輯打散，XOR 真值表如表 1.。

步驟 6：為了能將各物件圖像分享後之雜訊更為均勻，所以將各個圖像分別再使用亂數序列法[7]重新排序像素值。

步驟 7：最後加入嵌入的概念。將 E 頻道以及標頭資訊分享出來的分存圖像分成三個部分，將它們連同標頭檔分別嵌入到 R.G.B.三層的分存圖像中。

(a)O_1

(b)O_2

(c)O_3

(d) O_4

圖 5 物件示意圖:(a)物件 1，(b)物件 2，(c)物件 3，(d) 物件 4

3.3 圖像重建

在重建圖像時，不需將完整的圖像都找回，可以依據使用者的需求，來決定恢復的物件。在本研究中，根據(r_i, n)門檻機制，$2 \le r_i \le n$，i=0,…,m，m 表物件個數，把機密圖像分存成n個分存圖像，並編號1至n。

以下為重建階段步驟：

步驟 1：取得欲還原之物件所需的分存圖像。

步驟 2:使用拉格朗日內插法(Lagrange interpolation)來將像素值還原回其原來之位置。

拉格朗日內插法公式如下：

$$q_{ij}(x) = [q_j(h_1)\frac{(x-h_2)(x-h_3)\ldots(x-h_{r_i})}{(h_1-h_2)(h_1-h_3)\ldots(h_1-h_{r_i})} + q_j(h_2)\frac{(x-h_1)(x-h_3)\ldots(x-h_{r_i})}{(h_2-h_1)(h_2-h_3)\ldots(h_2-h_{r_i})} + \cdots + q_j(h_{r_i})\frac{(x-h_1)(x-h_2)\ldots(x-h_{r_{i-1}})}{(h_{r_i}-h_1)(h_{r_i}-h_2)\ldots(h_{r_i}-h_{r_{i-1}})}] mod 251$$

步驟 3：使用反亂數序列法將分享階段使用亂數序列法重新排序後像素值之位置還原。

步驟 4：再與金鑰進行 XOR，還原重新排序後像素值之位置。

步驟 5：將mod 251展開過後的資訊合併至原來的像素值，就能完整地還原欲還原之物件。

步驟6：將所有重建物件組合可以重建原機密圖像。

舉例說明，如果使用者只需要編號1的物件，那只需3個分存圖像即可，則無需將六個分存圖像皆運算，如此一來可以減少運算時間，運算方式如下。

n=6，6 個分存圖像；m=4，4 個物件

$r_0 = 2$ => 2 個找到 header file

$r_1 = 3$ => 3 個找到 O_1

$r_2 = 4$ => 4 個找到 O_2

$r_3 = 5$ => 5 個找到 O_3

$r_4 = 6$ => 6 個找到 O_4

表 1. XOR 互斥邏輯真值表

X	Y	X⊕Y
0	0	0
0	1	1
1	0	1
1	1	0

(a)

(b)

(c)

(d)

圖 6 製作 HDR 之圖片: (a)圖片 1，(b)圖片 2，(c)圖片 3，(d) 高動態範圍圖像

4. 實驗結果

本研究的實驗環境為 Intel i5CPU 之 PC 硬體，Windows 7 作業系統，Photoshop 及 Matlab 應用軟體；以第 3 節提出之研究方法的步驟進行實驗，詳細說明於下。

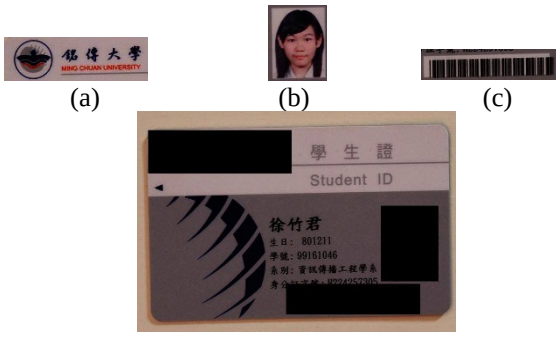
4.1 前置工作實驗

根據第 3 節前置工作的需求，本文製作實驗用之高動態範圍圖片，並進行分割成四個物件以利後續實驗之進行。為展示本文的高動態範圍圖片的製作方法，利用三張大小及拍攝角度相同但曝光值不同之圖像如圖 6 (a), (b), (c)，再利用第 3 節方法處理此三張圖像，製作出的高動態範圍圖像如圖 6 (d)。此結果可以很清楚得顯示製作出來的高動態範圍圖像的特性。

本實驗針對護照與學生證二圖像進行分享與還原實驗。利用前述方法得到高動態範圍圖片後，根據欲分享之物件的座標及長與寬，使用 Matlab 軟體將物件依序分割成物件 1 (O_1) ~ 物件 4 (O_4)，護照與學生證圖像分割結果各別如圖 7 及圖 8。

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

圖 7 護照分割後之各物件: (a)物件 1 (O_1)，(b)物件 2 (O_2)，(c)物件 3 (O_3)，(d) 物件 4 (O_4)



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

圖 8 學生證分割後之各物件: (a)物件 1 (O_1)，(b)物件 2 (O_2)，(c)物件 3 (O_3)，(d) 物件 4 (O_4)

4.2 圖像分享實驗

本實驗對圖 7 及圖 8 進行圖像分享，採用(r_i, n)門檻機制，而$2 \le r_i \le n$，i=0,1,⋯,m, m=4 表示有 4 個物件，n=6 表示將各個物件分享成 6 個分存圖像，各個r_i分別為標頭檔與各物件圖像分享時所使用的像素與的重建時所需要的分存圖像數，於本實驗各個r_i對應的像素個數如下: $r_0 = 2$對應 header file，$r_1 = 3$對應物件 1 (O_1)，$r_2 = 4$對應物件 2 (O_2)，$r_3 = 5$ 對應物件 3 (O_3)，$r_4 = 6$對應物件 4 (O_4)，先將圖像的像素值大於 250 像素展開重新排列。再根據對應之物件採用不同之r_i值，將展開圖像像素代入公式(1)。

$$q_j(x) = \left(a_1 + a_2 x + \cdots + a_{r_i} x^{r_i - 1}\right) mod\ 251$$

經此步驟對所有物件進行分享後產生六個分存圖像；各個分存圖像再分別透過使用一次 XOR，金鑰為 64，以及使用亂數序列法重新排序像素值，以增加各個分存圖像的安全性。圖 7 及圖 8 之護照與學生證物件圖像分享實驗結果各別如圖 9 及圖 10。

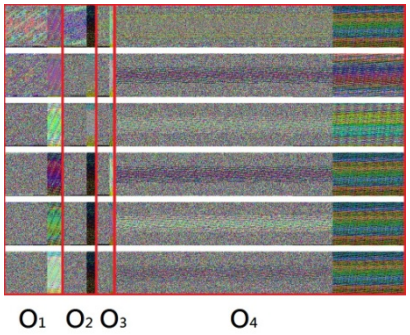


圖 9 護照分享後的六個分存圖像

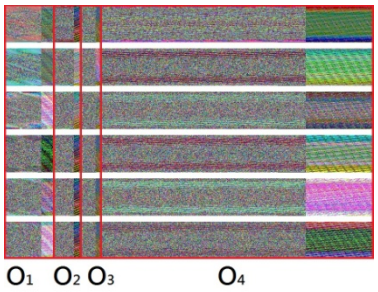


圖 10 學生證分享後的六個分存圖像

4.3 圖像重建實驗

本文以物件為基礎，所以機密圖像的重建是以使用者需求的部分，做為還原之物件的依據，使用者需要哪個物件，則透過各物件設定所需分存圖像之門檻來還原物件。

物件還原的實驗步驟，以反亂數序列法將各像素值重新排列打散前的位置，接著分別將各個像素值以金鑰(本實驗採用為 64)進行 XOR，再將拉格朗日內插法之公式套用於本次實驗加以計算。例如：若$r_1 = 3$，而要還原之資料為$\{q_j(1), q_j(2), q_j(4)\}$，

則計算方法如下：

$$q_{ij}(x) = [q_j(1)\frac{(x-2)(x-4)}{(1-2)(1-4)} + q_j(2)\frac{(x-1)(x-4)}{(2-1)(2-4)} + q_j(4)\frac{(x-1)(x-2)}{(4-1)(4-2)}] mod\ 251$$

以下為其他物件還原的例子：

$$q_j(x) = (a_1 + a_2x + \cdots + a_{r_i}x^{r_i-1})\ mod\ 251$$

$q_j(x) = (a_1 + a_2x)\ mod\ 251$

=>有 2 個分存圖像才可以找得到 header

$q_j(x) = (a_1 + a_2x + a_3x^2)\ mod\ 251$

=>有 3 個分存圖像才可以找得到 O_1

$q_j(x) = (a_1 + a_2x + a_3x^2 + a_4x^3)\ mod\ 251$

=>有 4 個分存圖像才可以找得到O_2

$q_j(x) = (a_1 + a_2x + a_3x^2 + a_4x^3 + a_5x^4)\ mod\ 251$

=>有 5 個分存圖像才可以找得到O_3

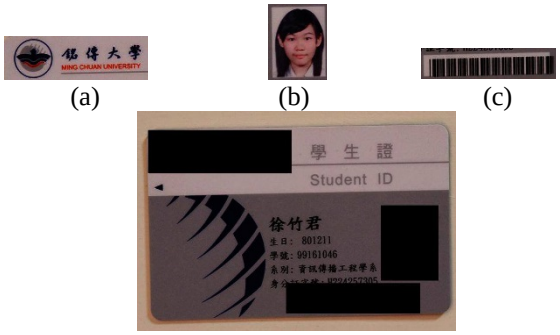
$q_j(x) = (a_1 + a_2x + a_3x^2 + a_4x^3 + a_5x^4 + a_6x^5)\ mod\ 251$

=>有 6 個分存圖像才可以找得到O_4

護照與學生證的各個物件的重建結果各別如圖 11 及圖 12，顯示被還原之物件圖像和原物件圖像在視覺上察覺不出任何差別。

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

圖 11 護照還原後之各物件(a)物件 1，(b)物件 2，(c)物件 3，(d) 物件 4



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

圖 12 學生證還原後之各物件(a)物件 1，(b)物件 2，(c)物件 3，(d) 物件 4

5. 結論

本文已提出以物件為基礎的高動態範圍機密圖像分享方法。該方法的物件被還原後，在圖像的品質可以保持非常清晰，不會產生失真現象；而且必須蒐集達到所需分存圖像，才能重建物件，具有非常高的安全性。透過物件的概念，該方法具有可以將物件各別取出的特性，在還原物件圖像時，只須取得各物件所需的分存圖像門檻值，便可以還原該部分的物件圖像，非常的方便而有效率。實驗結果證實我們所提出的方法之有效性。而由於高動態範圍圖像具又四個通道，於分享出來的分存圖像雖經使用金鑰進行互斥邏輯運算，以及使用亂數序列法重新排序但效果未盡理想，未來將考慮使用資料嵌入法，將分存嵌入自然圖像中，以更進一步提高資料之傳輸或儲存的安全性。

致謝

本研究承蒙國科會計畫編號 102-2815-C-130-038-E 之經費補助，謹此致謝。

參考文獻

[1] http://sts.dhp.ks.edu.tw/andy/2006TANET/F00013.pdf，查閱日期 28. 1. 2013.

[2] A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no.11, 612–613, 1979.

[3] C.C.Thien and J.C.Lin,“Secret image sharing,” Comput. Graphics, 26(5), 765–770, 2002.

[4] C. C. Chang and R. J. Huang, “Sharing secret images using shadow codebooks,” Inf. Sci., 111 (1–4), 335–345 ,1998.

[5] R.Z. Wang, C.H. Su, “Secret image sharing with smaller shadow images,” Pattern Recognition Letters 27 (6), 551-555, 2006。

[6] http://web.ntpu.edu.tw/~ccw/statmath/M_gui.pdf，查閱日期 18. 3. 2013.

[7] 洪宗樺：《在轉換域之影像浮水印機制研究》。銘傳大學資訊工程學系碩士班碩士學位論文，2010。