植基於視覺秘密分享技術之敏感性資料顯示

Demonstration of Sensitive Material Based on Visual Secret Share Technology

陳金鈴
朝陽科技大學
clc@mail.cyut.edu.tw

詹進科
中興大學
jkjan@cs.nchu.edu.tw

陳文虎
中興大學
w9656004@cs.nchu.edu.tw

摘要

本文提出一種安全傳遞敏感性資料的方法，此方法利用視覺秘密分享技術建構兩張分享圖像，一張依原始圖像產生具有原始圖像視覺意義的分享圖像，另一張依上述分享圖像及敏感性資料圖像產生不具任何視覺意義的分享圖像，當我們要顯示隱含之敏感性資料時，只須將兩張分享圖像疊合即可得知。我們的方法具有以下三種效益：(1)不須藉由電腦輔助計算，便可直接由人眼辨識出內含之資料，故具有計算及執行上的效益；(2)通常敏感性資料之顯示只會局限於文件的一小部份，不會因像素擴展之因素造成分享圖像過大，故具有實用性上的效益；(3)根據實驗結果顯示，原始圖像及敏感性資料圖像皆與他人相同時，互相交換分享圖像亦無法得知內含之圖像意義，且傳遞之分享圖像其顯示黑色及白色的相對對比為零，具有安全性上的效益。

關鍵詞：秘密分享技術、視覺密碼、敏感性資料、視覺秘密分享、有意義分享圖像

Abstract

In this paper, we proposed a secure method of transmission sensitive material. This method constructs two share images using the visual secret share technology, one share image is generated from the original image that the meaning in a vision coordinates the original image, and the other share image is generated according to the above share image and the sensitive material image that does not have any meanings in a vision. When the owner needs to reveal the hidden sensitive material, we can superimpose these two share images to recognize the hidden sensitive material. Our method has the following three kind of benefits: (1) To recognize the hidden message via human visual system does not need the computer auxiliary computation, will therefore have in the computation and the execution benefits; (2) In general, sensitive material will only occupy small part of a document that the factor of the pixels expansion will not cause the share image to be oversized, will therefore have in the usable benefit; (3) According to the experimental result that the original image and the sensitive material image all when is the same with other people, mutually exchanges the share image to be also unable to know the hidden sensitive material, and meaningless share image in a visual

demonstrating the black and the white relative contrast is zero, has in the secure benefit.
Keywords: Secret share technology; Visual cryptography; Sensitive material; Visual secret share; Meaningful share

1.簡介

視覺密碼的觀念是由 Naor 與 Shamir [4]首先提出來的，它與傳統密碼學的主要差異在於解密過程的不同，傳統密碼學方面不論使用對稱式加密法[8]或非對稱式加密法[3]之加密與解密過程均須利用相關密碼學知識與計算機資源方能達成，而視覺密碼學的主要精神在於解密的方法是透過人類視覺系統，不須藉由電腦輔助計算，便可直接由人眼辨識出來。因此，在一些無法使用電腦解密的情況下，視覺式的秘密分享方法是一個很好的解決方案，在視覺密碼的研究中，像素擴展技巧[1-2, 4-6, 9-12]與提高對比技巧[2, 4, 6, 7, 9]是兩個重要的應用主題，雖然大部分的視覺密碼方法的產出都是雜亂無章的分享圖像，然而，有一些視覺密碼方法的產出卻是有意義的圖像[1, 5, 12]，雜亂無章的分享圖像雖然可以確保安全性，但是卻容易遭受懷疑與破壞。因此，分享圖像本身為有意義的圖像的秘密分享方式，有其實際的應用價值。

在書面資料傳遞過程中，有些敏感性的內容並不希望由非相關人員知悉，如學生的操行成績或公司的人事考績等等。基於此，本文利用上述視覺秘密分享技術達成敏感性資料之安全傳遞，直接透過人類視覺來辨識出機密訊息，其運作原理是配合機密訊息分解成數張分享圖像，欲讀取藏入之機密訊息時，只需將這些分享圖像部分疊合或全部疊合，不須藉由電腦輔助計算，便可直接由人眼辨識出來。

本文提出之方法是利用視覺秘密分享技術產生兩張分享圖像，疊合後顯示內含之敏感性資料。首先，定義各個分享圖像及疊合圖像每個區塊依其顯示為黑色或白色決定黑點數目及白點數目。接著，一張分享圖像依據原始圖像(如姓名圖像)並配合其黑點及白點定義製作而成，所顯示之圖像其視覺上和原始圖像相同，且每個區塊其黑點及白點分佈之位置由亂數決定；另一張分享圖像是依據上述所產生之分享圖像及敏感性資料圖像並配合其每個區塊的黑點及白點定義製作而成，其顯示之圖像不具任何視覺上的意義，疊合該兩張分享圖像即可顯示內含敏感性資料。本論文之其他章節敘述如下：第 2 節為相關文獻介紹，第 3 節描述我們所提出的方法，第 4 節為實驗結果及安全性分析，最後，我們在第 5 節做個結論。

2.相關文獻介紹

2.1. Naor 和 Shamir 方法

Naor 和 Shamir[4]在 1995 年所提出的視覺密碼技術是依據自定之 m×m 像素擴展機制，將欲處理之二元圖像 N×M 像素大小擴展成 mN×mM 像素大小，並設定每個區塊大小為 m×m。接著，定義分享圖像及疊合圖像每個區塊顯示黑色及白色的黑點及白點數目，如表 1 所示。最後，參照機密圖像及表 1 所定義疊合後每個區塊顯示黑色及白色的黑點及白點數目，產生數張不具任何意義的二元分享圖像，將這些分享圖像部分疊合或全部疊合後，便可直接由人眼辨識出內含之機密訊息。

由上述程序可知，Naor 和 Shamir 方法所產生之分享圖像不具任何視覺上之意義，故適合成為公開傳遞之圖像，但也因不具視覺上之意義，所以，管理上將產生相當的困擾。

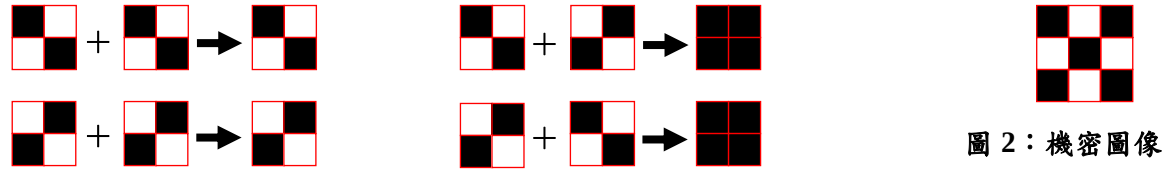
表 1：Naor 和 Shamir 提出方法的黑點及白點定義

項　目 / 圖 像 別	每個 m×m 區塊之黑色定義	每個 m×m 區塊之白色定義	備　註
分享圖像	a(黑),m×m-a(白)	b(黑),m×m-b(白)	a = b a, b, m ∈ N
疊合圖像	p(黑),m×m-p(白)	q(黑),m×m-q(白)	p > q p, q, m ∈ N

我們舉一簡單範例說明其實作方式如下：首先，我們使用 2×2 像素擴展機制並設定兩張分享圖像每個區塊之黑點及白點數目皆為{2(黑), 2(白)}，再設定兩張分享圖像疊合後每個區塊之黑色定義為{4(黑), 0(白)}及白色定義為{2(黑), 2(白)}，圖 1(a)為其疊合出的機密圖像像素為白色的狀態，圖 1(b)為其疊合出的機密圖像像素為黑色的狀態。接著，我們將如圖 2 的機密圖像中每一個像素所對應於兩張分享圖像的區塊放入相對應的黑點及白點數目，以符合疊合後每個區塊顯示黑色及白色的黑點及白點數目，完成所有區塊後即產生如圖 3(a)的分享圖像(一)及圖 3(b)的分享圖像(二)，而該兩張分享圖像並不具任何視覺上之意義。最後，疊合前述之分享圖像(一)及分享圖像(二)即可顯示視覺上如圖 2 之機密圖像，其疊合圖像如圖 3(c)所示。

2.2. Hwang 和 Chang 方法

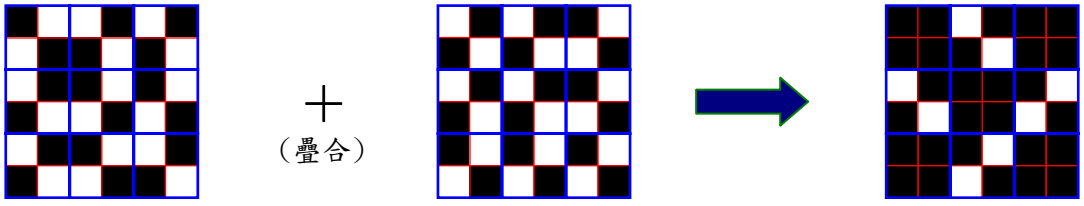
Hwang 和 Chang[5]在 2001 年所提出的視覺密碼技術是依據自定之 m×m 像素擴展機制，將欲處理之二元圖像 N×M 像素大小擴展成 mN×mM 像素大小，並設定每個區塊大小為 m×m，接著，定義分享圖像及疊合圖像每個區塊顯示黑色及白色的黑點及白點數目，如表 2 所示，配合表 2 之分享圖像每個區塊顯示黑色



(a)　　(b)

圖 1：(a)疊合後為白色的狀態 (b)疊合後為黑色的狀態

圖 2：機密圖像



(a)　　(b)　　(c)

圖 3：(a)分享圖像(一)　(b)分享圖像(二)　(c)疊合圖像

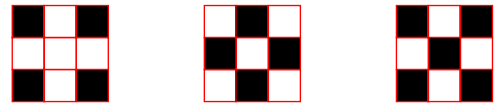
表 2：Hwang 和 Chang 提出方法的黑點及白點定義

項　目 / 圖 像 別	每個 m×m 區塊之黑色定義	每個 m×m 區塊之白色定義	備　註
分享圖像	a(黑), m×m-a(白)	b(黑), m×m-b(白)	a > b a, b, m ∈ N
疊合圖像	p(黑), m×m-p(白)	q(黑), m×m-q(白)	p > q p, q, m ∈ N

及白色的黑點及白點數目，分別產生視覺上具有其原來圖像意義的分享圖像。最後，依據表 2 所定義疊合後每個區塊顯示黑色及白色的黑點及白點數目，參照機密圖像調整部份或全部分享圖像的某些黑點及白點數目後，即完成分享圖像之製作，經調整後之所有分享圖像依然具有其原來之圖像意義，將這些分享圖像部分或全部疊合後，便可由人眼直接辨識出內含之機密訊息。

由上述程序可知，Hwang 和 Chang 方法所產生之分享圖像，視覺上都具有其原來圖像之意義，這將使得管理者方便管理各式各樣的分享圖像，但因分享圖像具有視覺上之意義，使得分享圖像擴展 m×m 倍的大小，換言之，將會浪費相當多的儲存空間且實用性將大為降低。

我們舉一簡單範例說明其實作方式如下：首先，我們先準備三張皆有意義的圖像，一張為圖 4(a)的 LOGO-1 圖像、一張為圖 4(b)的 LOGO-2 圖像及圖 4(c)的機密圖像。其次，我們使用 3×3 像素擴展機制並設定兩張分享圖像每個區塊之黑色定義為{6(黑), 3(白)}及白色定義為{4(黑), 5(白)}，再設定兩張分享圖像疊合後每個區塊之黑色定義為{8(黑), 1(白)}及白色定義為{6(黑), 3(白)}，圖 5(a)為其分享圖像依其 LOGO-1 圖像或 LOGO-2 圖像像素為黑色時每個區塊之其中一種圖例、圖 5(b)為其分享圖像依其 LOGO-1 圖像或 LOGO-2 圖像像素為白色時每個

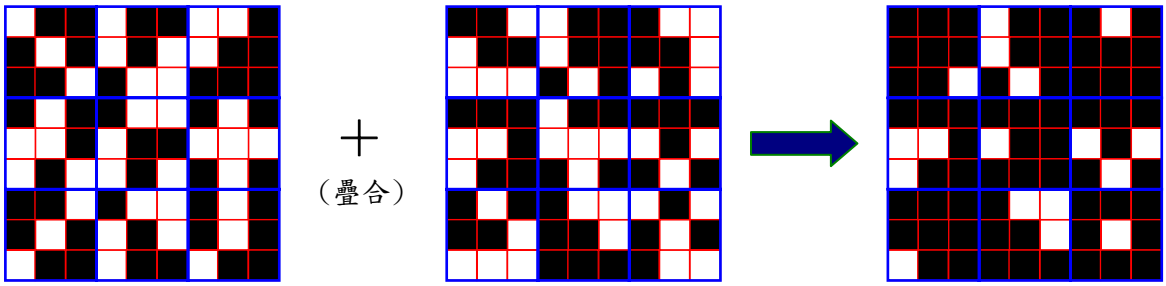


(a)　(b)　(c)

圖 4：(a) LOGO-1 圖像
(b) LOGO-2 圖像
(c)機密圖像

(a)　(b)　(c)　(d)

圖 5：(a)分享圖像為黑色時每個區塊之其中一種圖例
(b)分享圖像為白色時每個區塊之其中一種圖例
(c)疊合圖像為黑色時每個區塊之其中一種圖例
(d)疊合圖像為白色時每個區塊之其中一種圖例



(a) (b) (c)

圖 6：(a)分享圖像(一) (b)分享圖像(二) (c)機密圖像

區塊之其中一種圖例、圖 5(c)為其疊合圖像為黑色時每個區塊之其中一種圖例及圖 5(d)為其疊合圖像為白色時每個區塊之其中一種圖例。接著，將 LOGO-1 圖像及 LOGO-2 圖像每一個像素分別依上述分享圖像顯示黑色或白色的定義放入相對的黑點及白點數目，並將兩張分享圖像相對的區塊疊合後，其中一張分享圖像每個區塊的黑點及白點數目依機密圖像之像素值並配合另一張分享圖像相對區塊的黑點及白點數目加以調整，使其符合前述疊合圖像顯示黑色或白色的定義，完成所有區塊後即產生分享圖像(一)及分享圖像(二)，而其分享圖像依然分別具有其原來之圖像意義。最後，疊合前述之分享圖像(一)及分享圖像(二)即可顯示視覺上如圖 4(c)之機密圖像，其疊合圖像如圖 6(c)所示。

3.我們提出的方法

我們提出的方法是利用 Hwang 和 Chang 方法產生視覺上具有其原來圖像意義的分享圖像，除適合做為個人之識別分享圖像外，亦方便管理者管理各式各樣的分享圖像，接者，利用 Naor 和 Shamir 方法產生不具任何視覺上意義的分享圖像，而這將適合成為公開傳遞之圖像。我們結合兩者之優點製作一張視覺上具有原來圖像意義的分享圖像，稱之為原始圖像擴展之分享圖像；另一張不具任何視覺上意義的分享圖像，稱之為特徵化分享圖像。疊合該兩張分享圖像後，顯示內含之敏感性資料圖像。其處理流程圖如圖 7。

3.1.初始程序

步驟 1：採用 m×m 像素擴展機制，將欲處理之二元圖像 N×M 像素大小擴展成 mN×mM 像素大小，並稱 m×m 像素為一個區塊。

步驟 2：分別定義原始圖像擴展之分享圖像、特徵化分享圖像及疊合圖像每個區塊顯示黑色或白色的黑點及白點數目，如表 3 所示，其定義之黑點或白點數目須符合如下規則：

(1)p(黑)≧b(黑)＋d(黑)，以確保疊合圖像顯示黑色的黑點和白點數目。

(2)q(黑)≧max{a(黑), c(黑)}，以確保疊合圖像顯示白色的黑點和白點數目。

(3)p(黑)－q(黑)差距愈大愈好，以確保疊合圖像能得到較佳的人眼辨識效果。

3.2.產生原始圖像擴展之分享圖像程序

輸入：(1)N×M 像素大小的原始圖像。

(2)依 3.1.節之步驟 2 所定義原始圖像擴展之分享圖像每個區塊

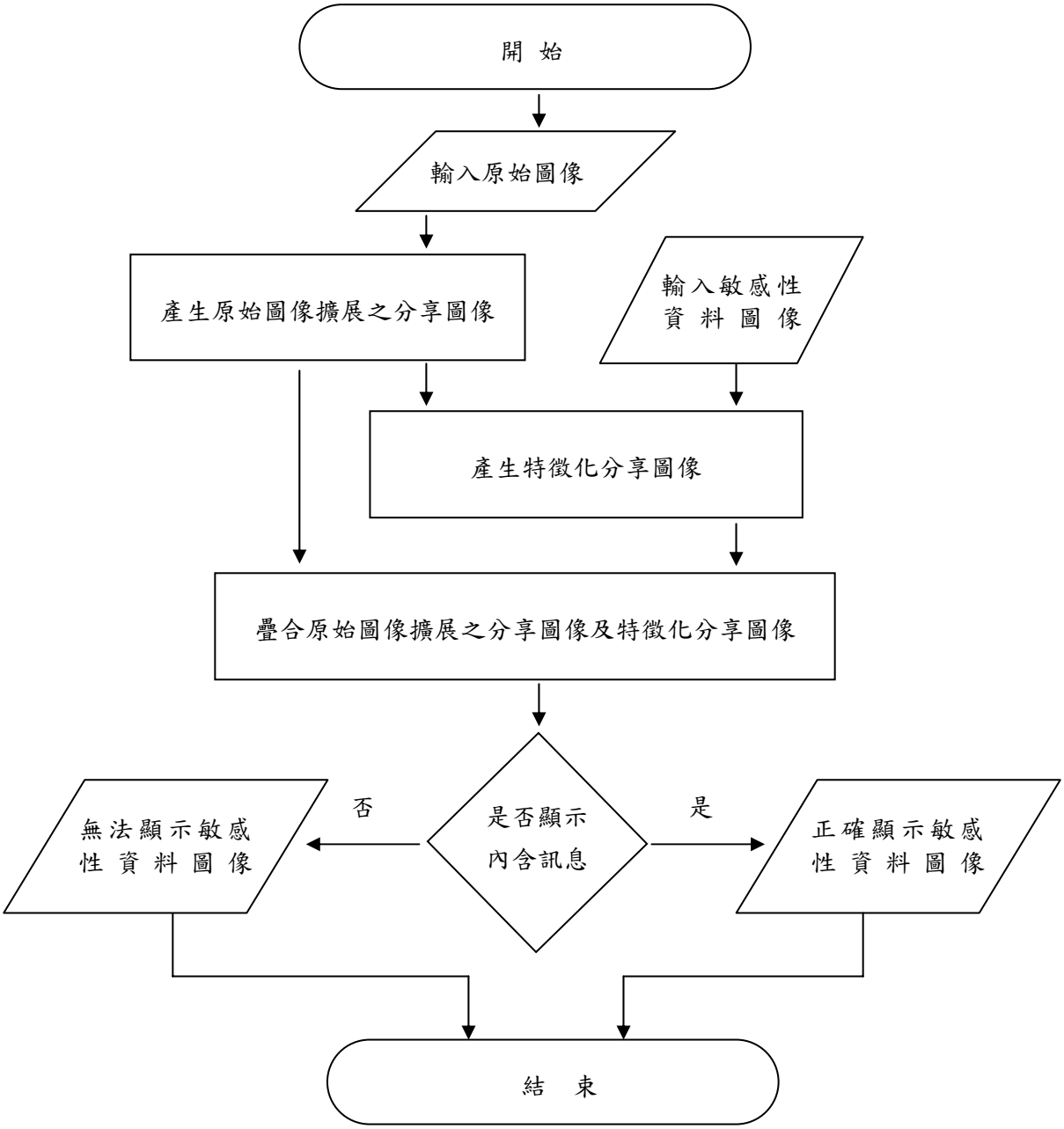


圖 7：我們提出方法的處理流程圖

表 3：我們提出方法的黑點及白點定義

項目 / 圖像別	每個 m×m 區塊之黑色定義	每個 m×m 區塊之白色定義	備註
原始圖像擴展之分享圖像	a(黑), m×m-a(白)	b(黑), m×m-b(白)	a > b a, b, m ∈ N
特徵化分享圖像	c(黑), m×m-c(白)	d(黑), m×m-d(白)	c = d c, d, m ∈ N
疊合圖像	p(黑), m×m-p(白)	q(黑), m×m-q(白)	p > q p, q, m ∈ N

顯示黑色或白色的黑點和白點數目分別為{a(黑), m×m-a(白)}及{b(黑), m×m-b(白)}。

輸出：原始圖像擴展之分享圖像。

步驟 1：將 N×M 像素大小的原始圖像擴展成 mN×mM 個像素大小，並將擴展之圖像以每個區塊為 m×m 個像素大小加以分割。

步驟 2：原始圖像中每一個像素所對應的區塊依表 3 原始圖像擴展之分享圖像所定義的黑點和白點數目，放入相對的黑點及白點，其區塊中黑點及白點分佈之位置由亂數決定，完成所有區塊後即形成原始圖像擴展之分享圖像，而其圖像視覺上之意義和輸入之原始圖像相同。

3.3.產生特徵化分享圖像程序

輸入：(1)N×M 像素大小的敏感性資料圖像。

(2)mN×mM 像素大小的原始圖像擴展之分享圖像。

(3)依 3.1.節之步驟 2 所定義特徵化分享圖像每個區塊顯示黑色或白色的黑點和白點數目分別為{c(黑), m×m-c(白)}及{d(黑), m×m-d(白)}。

(4)依 3.1.節之步驟 2 所定義疊合圖像每個區塊顯示黑色或白色的黑點和白點數目分別為{p(黑), m×m-p(白)}及{q(黑), m×m-q(白)}。

輸出：特徵化分享圖像。

步驟 1：將 N×M 像素大小的敏感性資料圖像擴展成 mN×mM 個像素大小，並將擴展之圖像以每個區塊為 m×m 個像素大小加以分割。

步驟 2：敏感性資料圖像中每一個像素所對應的區塊依表 3 特徵化分享圖像所定義的黑點和白點數目，放入相對的黑點及白點，且與原始圖像擴展之分享圖像相對的區塊疊合，並比較敏感性資料圖像加以調整，直至符合表 3 疊合圖像所定義的黑點和白點數目，完成所有區塊處理後即形成特徵化分享圖像，而其顯示之圖像並不具任何視覺上之意義。

3.4.疊合原始圖像擴展之分享圖像及特徵化分享圖像程序

輸入：(1)依 3.2.節所產生的原始圖像擴展之分享圖像。

(2)依 3.3.節所產生的特徵化分享圖像。

輸出：敏感性資料圖像。

步驟：將原始圖像擴展之分享圖像和特徵化分享圖像加以疊合，透過人類視覺予以判讀，如為正確的分享圖像疊合將顯示內含之敏感性資料圖像；反之，則無法顯示內含之敏感性資料圖像。

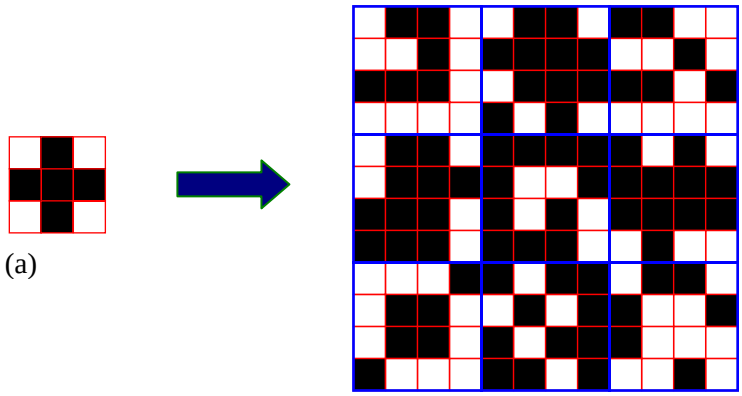
由上述程序可知，我們提出的方法所產生的原始圖像擴展之分享圖像具有原始圖像所代表的圖像意義，故可做為個人之識別分享圖像，另一張特徵化分享圖像則不具任何視覺上之意義，故適合成為公開傳遞之圖像，兩者相互配合，將使敏感性資料得以安全傳遞及顯示。我們舉一簡單範例說明其實作方式，首先，我們先準備兩張圖像，一張為如圖 8(a)的原始圖像，另一張為如圖 8(b)的敏感性資料圖像。其次，我們使用 4×4 像素擴展機制並定義原始圖像擴展之分享圖像、特徵化分享圖像及疊合圖像每個區塊顯示黑色及白色的黑點及白點數目，如表 4 所示。再者，依據 3.2.節程序產生圖 9(b)的原始圖像擴展

(a) (b)

圖 8：(a)原始圖像 (b)敏感性資料圖像

表 4：我們提出方法的黑點及白點定義(實驗)

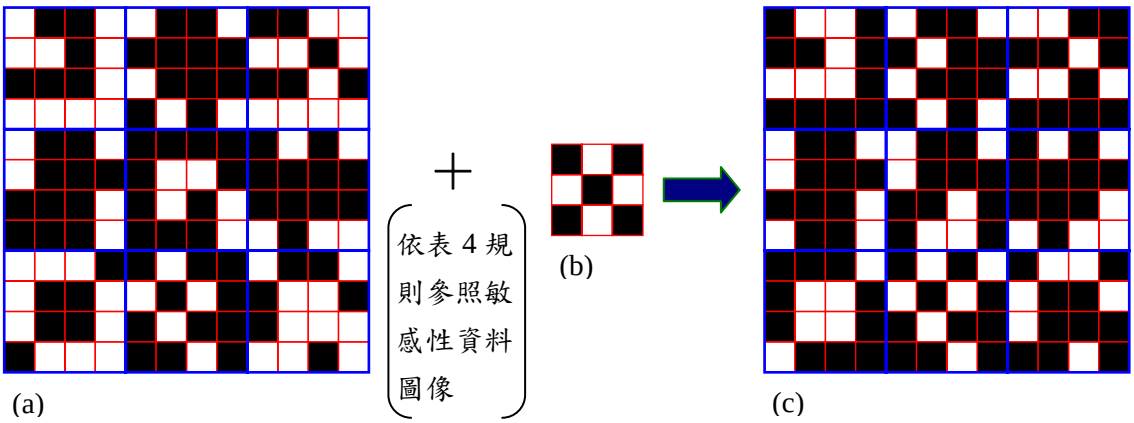
項　目 / 圖像別	每個 4×4 區塊之黑色定義	每個 4×4 區塊之白色定義
原始圖像擴展之分享圖像	11(黑), 5(白)	6(黑), 10(白)
特徵化分享圖像	10(黑), 6(白)	10(黑), 6(白)
疊合圖像	16(黑), 0(白)	11(黑), 5(白)



(a)

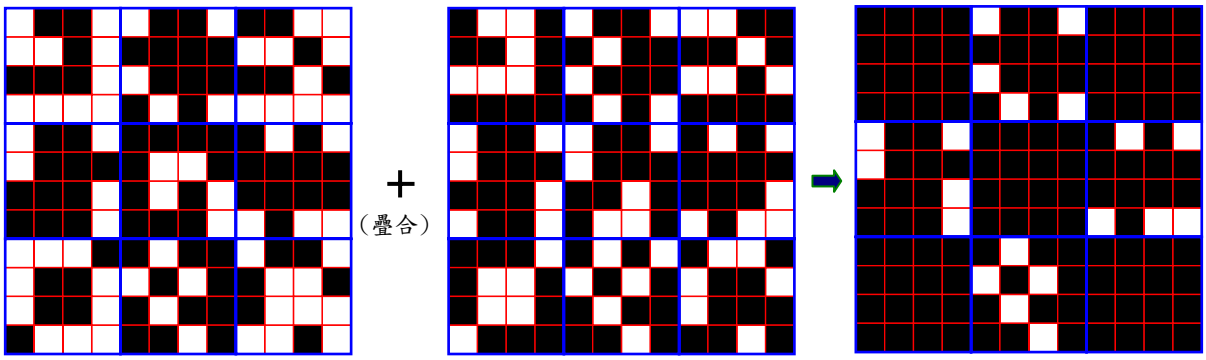
(b)

圖 9：(a)同圖 8(a)之原始圖像 (b)原始圖像擴展之分享圖像



(a) (b) (c)

圖 10：(a)同圖 9 (b)之原始圖像擴展之分享圖像 (b)同圖 8 (b)之敏感性資料圖像 (c)特徵化分享圖像



(a) (b) (c)

圖 11：(a)同圖 9 (b)之原始圖像擴展之分享圖像 (b)同圖 10 (c)之特徵化分享圖像 (c)疊合圖像

之分享圖像、依據 3.3.節程序產生圖 10(c)的特徵化分享圖像及依據 3.4.節程序產生圖 11(c)的疊合圖像。

4.實驗結果及安全性分析

4.1.實驗結果：

輸入：(1)圖 12(a)之原始圖像及圖 12(b)之敏感性資料圖像，假設圖像大小均為 30 × 75 像素。

(2)原始圖像擴展之分享圖像、特徵化分享圖像及疊合圖像每個區塊顯示黑色及白色的黑點及白點數目，如表 4 定義所示。

4.1.1.依據我們第 3 節所提出的方法製作如圖 13(a)的原始圖像擴展之分享圖像及如圖 13(b)的特徵化分享圖像，疊合此兩張分享圖像後，即可正確地顯示出如圖 13(c)的敏感性資料圖像。

4.1.2.測試原始圖像及敏感性資料圖像皆與他人相同時，我們提出方法之安全性：同樣使用圖 12(a)的原始圖像及圖 12(b)的敏感性資料圖像，再次產生如圖 14(a)的原始圖像擴展之分享圖像及圖 14(b)的特徵化分享圖像。

(a) (b)

圖 12：(a)原始圖像 (b) 敏感性資料圖像

【假設 1】使用圖 14(a)的原始圖像擴展之分享圖像與圖 13(b)的特徵化分享圖像疊合，其結果並無法得出內含之訊息，圖 14(c)為其疊合圖像。

【假設 2】使用圖 13(a)的原始圖像擴展之分享圖像與圖 14(b)的特徵化分享圖像疊合，其結果亦無法得出內含之訊息，圖 14(d)為其疊合圖像。

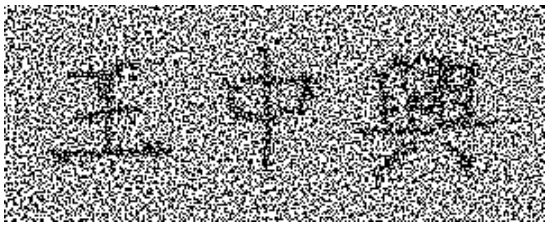
4.2.安全性分析：

4.2.1.原始圖像及敏感性資料圖像皆與他人相同時之安全性分析：

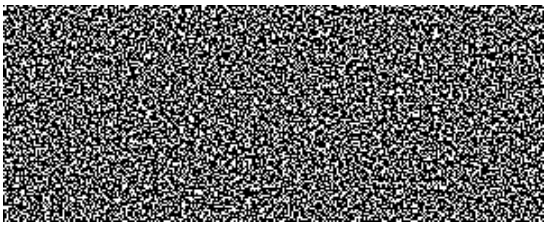
由 4.1.2 節實驗結果得知，原始圖像所建構之原始圖像擴展之分享圖像因其黑點及白點分佈之位置由亂數決定，再加上敏感性資料圖像是隨機位置放置，故可保證敏感性資料圖像只會由正確的原始圖像擴展之分享圖像及特徵化分享圖像疊合後顯示。

4.2.2.敏感性資料在傳遞過程中之安全性分析：

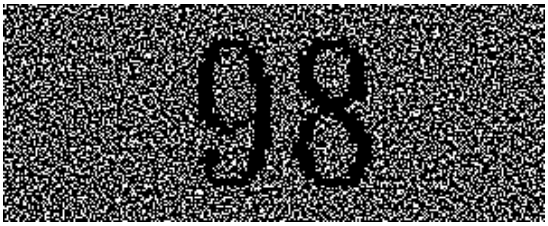
敏感性資料在傳遞過程中其所傳遞之圖像為特徵化分享圖像，如圖 13(b)及圖 14(b)所示。而特徵化分享圖像每個區塊



(a)

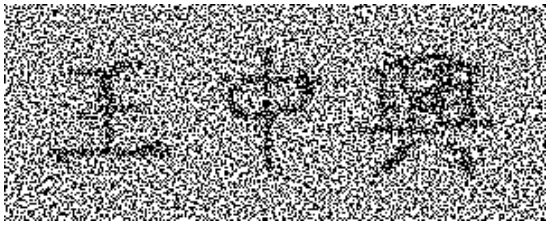


(b)

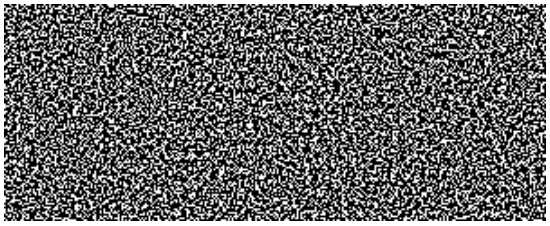


(c)

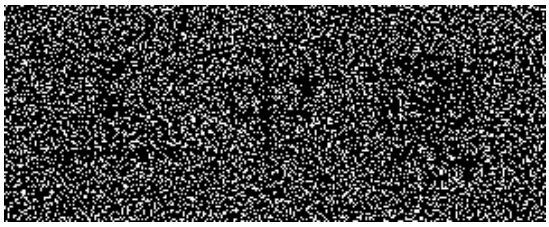
圖 13：(a)原始圖像擴展之分享圖像 (b)特徵化分享圖像 (c)疊合圖像



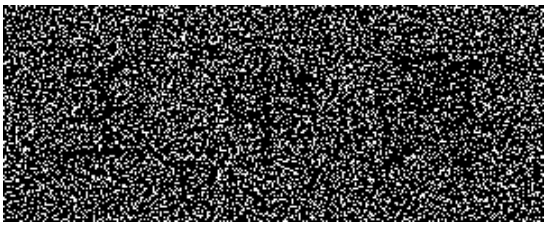
(a)



(b)



(c)



(d)

圖 14：(a)再次產生之原始圖像擴展之分享圖像 (b)再次產生之特徵化分享圖像
(c)【假設 1】之疊合圖像 (d)【假設 2】之疊合圖像

顯示黑色或白色的黑點和白點數目分別為{c(黑), m×m-c(白)}及{d(黑), m×m-d(白)}，因為 c(黑)等於 d(黑)，故相對對比[(c-d)/(m×m)]×100%等於零，故無法由其特徵化分享圖像得知內含之敏感性資料圖像。

5.結論

本文提出以視覺秘密分享技術來顯示敏感性資料具有其安全性及實用性，首先，建構原始圖像擴展之分享圖像每個區塊其黑點及白點分佈之位置由亂數決定且敏感性資料圖像是隨機位置放置，再加上特徵化分享圖像的相對對比為零，故可保證將由正確的原始圖像擴展之分享圖像及特徵化分享圖像疊合後顯示內含之敏感性資料圖像。再者，本文雖採用 4×4 像素擴展機制產生分享圖像，如此將使得分享圖像大小比原始圖像大小擴展 4×4 倍，但疊合出的圖像人眼辨識效果較

佳，且敏感性資料之顯示通常只會局限於文件的一小部份，未來，如學生的操行成績或公司的人事薪資及考績等等，在書面資料傳遞過程中，可利用本文方法避免其內容被非相關人員所知悉。

參考文獻

[1] W.P. Fang, “Friendly progressive visual secret sharing”, Pattern Recognition, Vol. 41, pp. 1410-1414, 2008.

[2] Tzeng, W. G. and Hu, C. M., “A New Approach for Visual Cryptography”, Designs, Codes and Cryptography, Vol. 27, No. 3, pp. 207-227, 2002.

[3] Rivest, R. L. Shamir, A. and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems”, Communications of the ACM, Vol. 21, Issue 2, pp. 120-126, 1978.

[4] Naor, M. and Shamir, A., “Visual cryptography”, Advances in Cryptology-EUROCRYPT’94, LNCS 950, pp. 1-12, 1995.

[5] Hwang, R.J., Chang, C.C., “Hiding a picture in two pictures”, Optical Engineering, Vol. 40, Issue 3, pp. 342-351, 2001.

[6] Hofmeister, T., Krause, M. and Simon, H. U., “Contrast-optimal k out of n Secret Sharing Schemes in Visual Cryptography”, Theoretical Computer Science, Vol. 240, Issue 2, pp. 471-485, 2000.

[7] Eisen, P. A. and Stinson, D. R., “Threshold Visual Cryptography Schemes with Specified Whiteness Levels of Reconstructed Pixels”, Designs, Codes and Cryptography, Vol. 25, No. 1, pp. 15-61, 2002.

[8] “DES Encryption Standard (DES)”, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 46, National Technical Information Service, 1997.

[9] Blundo, C., De Bonis, A. and De Santis, A., “Improved Schemes for Visual Cryptography”, Designs, Codes and Cryptography, Vol. 24, No. .3, pp. 255-278, 2001.

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

[11] Ateniese, G., Blundo, C., De Santis, A. and Stinson, D. R., “Visual Cryptography for General Access Structures”, Information and Computation, Vol. 129, Issue 2, pp. 86-106, 1996.

[12] Ateniese, G., Blundo, C., De Santis, A. and Stinson, D. R., “Extended Capabilities for Visual Cryptography”, Theoretical Computer Science, Vol. 250, Issues 1-2, pp. 143-161, 2001.