文字型視覺機密分享

方文聘
元培科技大學
wpfang@mail.ypu.edu.tw

許佳豪
元培科技大學
pt7922310@gmail.com

王德順
元培科技大學
wangts@mail.ypu.edu.tw

摘要

本論文提出文字型式之視覺機密分享，不同於傳統視覺密碼學單純對影像進行處理，本論文提出方法是對純文字檔案進行分享，將文字檔案列印在投影片後，進行疊合，可以出現機密資訊，同樣的方法可以將視覺分享的特性，全部套用在文字型視覺分享上，且因為文字檔案特性，本文方法已經具有友善視覺分享的特性，且又有安全與不易攻擊之特性。

關鍵詞：視覺分享、文字格式、友善分享

Abstract

This paper proposed a text form visual sharing scheme. Different from traditional visual sharing scheme which handle with image, the proposed method shares text file. Secret information revealed after users stack two or more transparencies which print texts. The advantages of proposed method include not only the advantages of traditional visual sharing method, but also have the characteristic of friendly visual sharing method.

Keywords: Visual secret sharing, text format, friendly sharing.

前言

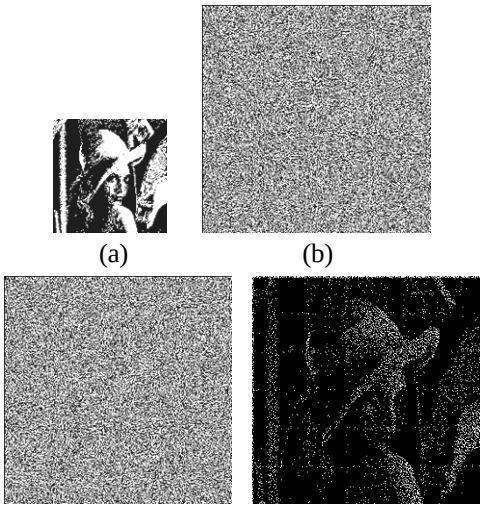
目前資訊技術日益發達，資訊交流頻繁，因此安全的傳遞資訊非常重要，常見傳遞方法有數位浮水印、密碼學等方法，近年來，許多人開始探討視覺機密分享方法，視覺機密分享的特色是不需要電腦即可進行解碼，在分存數量不足的情況下不易被破解。但是，視覺機密分享的解碼影像品質相對於影像分享方法差，且分存不易管理，相關研究如下一段說明。

為了解決影像分享的分存管理不易的問題，本論文提出文字型之視覺機密方分享方法，有可以容易管理分存，且不易被攻擊的優點，更重要的是可以擁有大多數視覺機密分享的特色。

本論文其他部分包括第二段介紹視覺密碼學，第三段說明提出方法，第四段說明實驗結果，第五段討論與結論。

視覺密碼學

視覺密碼學最早由 Naor 與 Shamir[1]提出，最簡單的版本為產生兩張投影片，皆為亂碼型式，每格點為黑色或是白色的機率都是 50%，對於單獨一張投影片皆無法猜測出原始影像內容，但是如果將兩張投影片直接疊合，則可以還原出原始的影像內容，如圖 1 所示，原理是利用人眼對於深色與淺色的認知是相對的，因此，同一區塊黑點較對會被人眼視為黑色，反之則是為白色，方法是先建立一個基本矩陣，如表 1 所示，兩個相對應的點會擴張成區塊，如果原始影像是黑色，則區塊內黑點位置會剛好相反，反之，則相同，所以疊合後會產生擴張，但是和原始影像接近的疊合結果。



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

圖 1. 傳統視覺密碼學例子(a)為原圖(b)(c)為分存，(d)為疊合(b)與(c)之結果。

表 1、視覺密碼學方法說明

原始影像	相對區塊 s		疊合結果
	分存 1	分存 2	
□	■□ □■	□■ ■□	■■ ■■
■	■□ □■	□■ ■□	■■ ■■

近年來，有許多學者開始對視覺影像分享進行研究，包括 Ateniese 等人[2]提出通用存取結構，設計不同分存結合可以得到不同的結果、或是不同的幾何關係可以得到不同的疊合結果[3-7]，也有人設計出另外的不擴張的影像機密分享方法，包括隨機網格方法[8-10]與機率方法[11]，也有學者對將視覺機密分享與數位媒體特性結合，讓資料可以透過直接視覺解碼或是經由機器進行解碼[12-14]。

提出方法

本文提出文字型式之視覺機密分享方法，流程如圖 2 所示，方法首先讀取要作為基底的文字檔，再讀取要分享的機密影像(本論文實驗以文字為例)，讀取後，計算顯示文字位置，與機密影像所要顯示的位置，再將第一張投影片文字每個字以隨機方法決定位置畫於投影片，而第二張投影片的文字繪製方法則是將相對應機密影像位置進行隨機移動，如此即完成編碼。

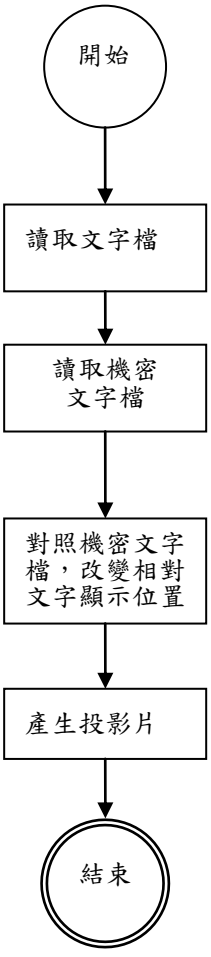


圖 2.流程圖。

演算法如下所示

演算法

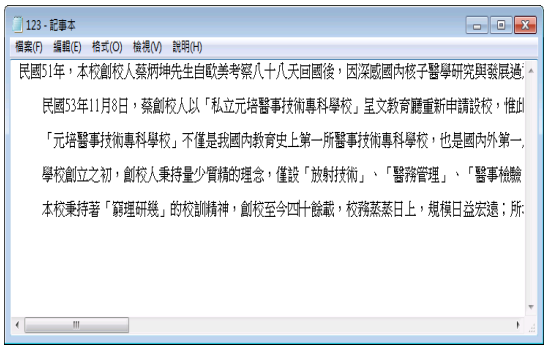
輸入：分存文字檔 F(長度 N)、機密資料座標 H、
分存文字長寬 WxH、字大小 a×b

輸出：分存 S_1、S_2(長度 N)

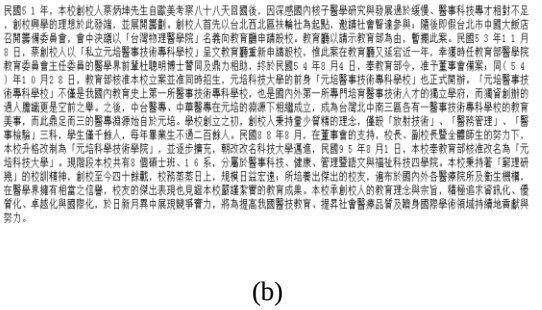
j=0
For i=1 to N
x= (i MOD W) ×a
$y=\left\lfloor \frac{i}{W} \right\rfloor \times b$
Δx = 隨機選擇-1、0、1
Δy =隨機選擇-1、0、1
If i=H(j) then
在 S_1 座標(x+Δx,y+Δy)畫 F(i)
在 S_2 座標(x-Δx,y-Δy)畫 F(i)
j=j+1
Else
在 S_1 座標(x+Δx,y+Δy)畫 F(i)
在 S_2 座標(x+Δx,y+Δy)畫 F(i)
End if
End For

實驗結果

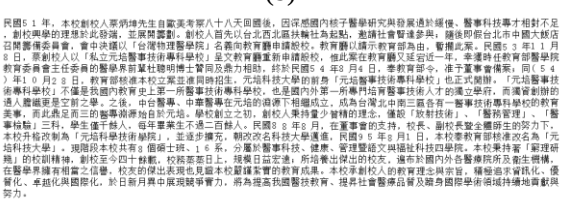
實驗結果如圖 3 所示，圖 3(a)為原始文字檔資料，圖 3 (b)與(c)為分存,圖 3(d)為疊合後的結果，疊合後可以看到所隱藏的資訊。



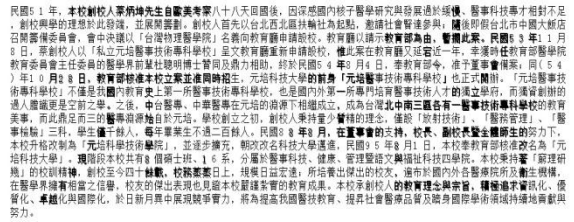
(a)



(b)



(c)


民國５１年，本校創校人蔡炳坤先生自歐美考察八十八天回國後，因深感國內統子醫學研究與發展過於緩慢，醫事科技專才相對不足，創校興學的理想於此發踐，並展開籌劃。創校人首先以台北西北扶輪社為起點，邀請社會賢達參與；隨後即假台北市中國大飯店召開籌備委員會，會中決議以「台灣物理醫學院」名義向教育廳申請設校。教育廳以請示教育部為由，暫擱此案。民國５３年１１月８日，蔡創校人以「私立元培醫事技術專科學校」呈文教育廳重新申請設校，惟此案在教育廳又延宕近一年，幸獲時任教育部醫學院教育委員會主任委員的醫學界前輩杜聰明博士暨同及鼎力相助，終於民國５４年３月４日，奉教育部令，准予置事會備案；同（５４）年１０月８日，教育部核准本校立案並准同時招生，元培科技大學的前身「元培醫事技術專科學校」也正式開辦。「元培醫事技術專科學校」不僅是我國內教育史上第一所醫事技術專科學校，也是國內外第一所專門培育醫事技術人才的漢立學府，而獲省創辦的過人膽識更是空前之舉。之後，中台醫專、中華醫專在元培的資源下相繼成立，成為台灣北中南三區各有一醫事技術專科學校的教育美事，而此鼎足而三的醫專源源始自於元培。學校創立之初，創校人秉持重少智精的理念，僅設「放射技術」、「醫務管理」、「醫事檢驗」三科，學生僅千餘人，每年畢業生不過二百餘人。民國８８年８月，在董事會的支持，校長、副校長暨全體師生的努力下，本校升格改制為「元培科學技術學院」，並逐步擴充，朝改改名科技大學邁進，民國９５年８月１日，本校奉教育部核准改名為「元培科技大學」，現階段本校共有８個碩士班、１６系，分屬於醫事科技、健康、管理暨語文與福祉科技四學院，本校秉持著「腳理研機」的校訓精神，創校至今四十餘載，校務蒸蒸日上，規模日益宏遠；所培養出傑出的校友，遍布於國內外各醫療院所及衛生機構，在醫學界建有相當之信譽，校友的傑出表現也見證本校辦理紮實的教育成果。本校承創校人的教育理念與宗旨，積極追求資訊化、優質化、卓越化與國際化，於日新月異中展現競爭實力，將為提高我國醫技教育、提昇社會醫療品質及躋身國際學術領域持續地貢獻與努力。

(d)

結論與討論

本論文提出對文字媒體進行影像機密分享，因為分存皆為有意義的文字，所以可以很容易的管理分存，另外，因為每個字的座標變化很小，對於閱讀品質並沒有太大的影響，而且，只擁有單獨一個文字檔並無法知道所隱藏的資料。當疊合後，可以得到欲顯示內容，與傳統視覺密碼學的差別，包括分存格式不同，不需要擴張分存大小，未來，可以設計出(n,r)型分享，或是設計不同的存取結構。

參考文獻

[1] M. Naor and A. Shamir, “Visual Cryptography,” Advances in Cryptogoly --- Eurocrypt ’94, Lecture Notes in Computer Science, vol. 950, 1-12,Springer-Verlag, Berlin,1995

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

[3] H.C. Wu and C.C. Chang, “Sharing Visual Multi-secrets Using Circle Shares,” Computer Standards & Interfaces, Vol. 28, 123-135, 2005

[4] W.P. Fang, “Visual Cryptography in Reversible Style, ”IEEE Proceeding on the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing(IIHMSP2007), Kaohsiung, Taiwan, R.O.C, 2007, 11, 26～2007, 11, 28.

[5] Wen-Pinn Fang, “A Survey for Visual Sharing Scheme with Geometry Property,”Journal of Image Processing and Communication, Vol. 2, No. 1, 2010, 12, pp. 35-39.

[6] W.P. Fang, “Non-expansion Visual Secret Sharing in Reversible Style, ”International Journal of Computer and Network Security, Vol. 9, No. 2, 2009, 2, 204-208

[7] W.P. Fang, “Maximizing the Secret Hiding Ratio in Visual Secret Sharing with Reversible Property,”International Journal of Computer and Network Secur

[8] Kafri and E. Keren, “Encryption of Pictures and Shapes by Random Grids,” Optics Letters, Vol. 12, No. 6, 377 - 379, 1987.

[9] S. J. Shyu, “Image Encryption by Random Grids,” Pattern Recognition, Vol. 40, Issue 3, 1014 - 1031, 2007.

[10] T. H. Chen and K.H. Tsao, “Visual Secret S haring by Random Grids Revisited”, Pattern Recognition, 2008, online(http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6V14-4V1TXMJ-1-1&_cdi=5664&_user=2414342&_orig=mlkt&_coverDate=11%2F30%2F2008&_sk=999999999&view=c&wchp=dGLzVtz-zSkzV&md5=0f9b092b81e841ed86e4a8c6eadd4a22&ie=/sdarticle.pdf)

[11] C. N. Yang, ”New Visual Secret Sharing Schemes Using Probabilistic Method,” Pattern Recognition Letter, Vol. 25 2004, 481 – 494

[12] W.P. Fang, J.C. Lin, 2006, 4, “ Visual Cryptography with Extra Ability of Hiding Confidential Data ” Journal of Electronic Imaging, 15, 023020

[13] R.Lukac and K.N. Plataniotis , “Bi-level Based Secret Sharing for Image Encryption”, Pattern Recognition Vol. 38, 2005, 767–772.

[14] W.P. Fang and J. C. Lin, “Multi-channel Secret Image Transmission with Fast Decoding: by using Bit-level Sharing and Economic-size Shares” International Journal of Computer and Network Security, 6, 2006, 6, 228-234.