國立成功大學
National Cheng Kung University

古典密碼學 補充2

計網中心 網路與資訊安全組

李南逸

National Cheng Kung University

視覺密碼 Visual cryptography

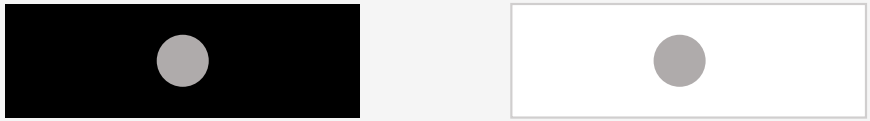
- Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decrypted information appears as a visual image.
- One of the best-known techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994.

視覺密碼 Visual cryptography

- 黑白視覺密碼技術：
  1. 將黑或白的像素點組成的機密影像經特殊處理後，產生n張看似由亂點組合而成的黑白投影片
  2. 這n張投影片可以分別由多位具有管理機密資訊權限的成員所持有，若是成員將其中k張以上(k≦n)的投影片正確的重疊後，就可以將原先的機密資訊直接由人的視覺系統給判讀出來，而不須運用到額外設備及運算 ㄐ零k人才能看到
  3. 如果少於k張，所重疊出來的為雜亂無意義的影像，從影像中也無法取得機密資訊，這就是視覺密碼中典型的n中取k的門檻機制(k out of n threshold scheme)

黑白視覺密碼原理

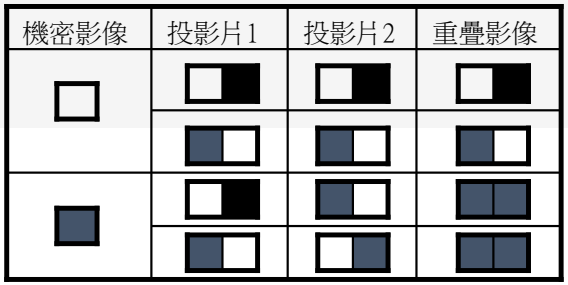
- 一個在黑紙上的灰點一定比放在白紙上的同樣灰點看起來比較亮 (白)



- 視覺密碼這個技術可以將幾張雜亂的影像經重疊以取得機密影像，其主要的原因在於人類視覺系統在辨識物體時，會依據物體和週遭環境之間所產生的對比效果來進行解讀

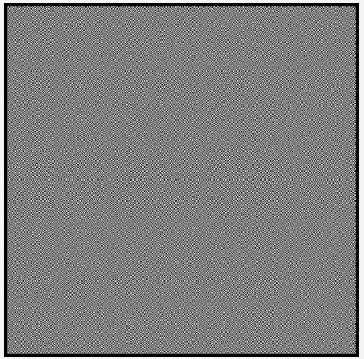
2 out of 2 黑白視覺密碼

- 投影片上黑點、白點的重疊會有下列的特性：
  - 黑＋黑＝黑，黑＋白＝黑，白＋黑＝黑，白＋白＝白

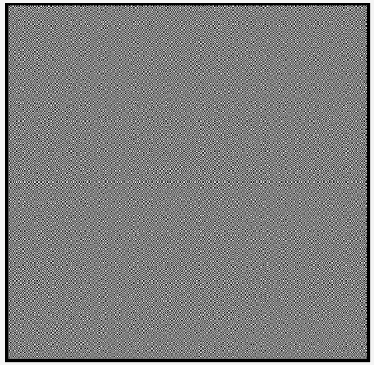


- 若不幸其中一張投影片為非法者所截取，則他必須對投影片上的每一個區塊進行解密，而每一個區塊可能猜對的比率為二分之一，所以如果一張N*M 大小的機密影像要被猜對的機會為2^{-N*M}，機率是非常低的。

灰階與彩色影像視覺密碼

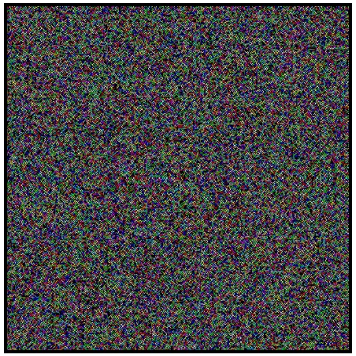


(A) SHARE 1

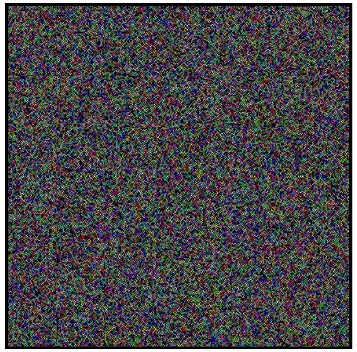


(B) SHARE 2

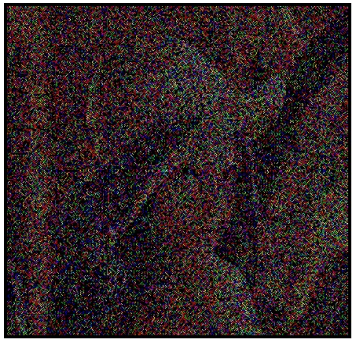
(C) 疊合後的密圖



(A) SHARE 1



(B) SHARE 2



(C) 疊合後的密圖

作業2

- 請利用古典密碼技術設計一套加密器
  - 須包含藏入、取出機密訊息之過程或方式，以及範例
  - 繳交
    1. Pdf檔案（可用手寫方式）
    2. 兩週內繳交
    3. 一人一組

01101001
01101100
01101111
01110110
01100101
01111001
01101111
01110101