

Visual Cryptography

Team 18

任祖頤 p11922004

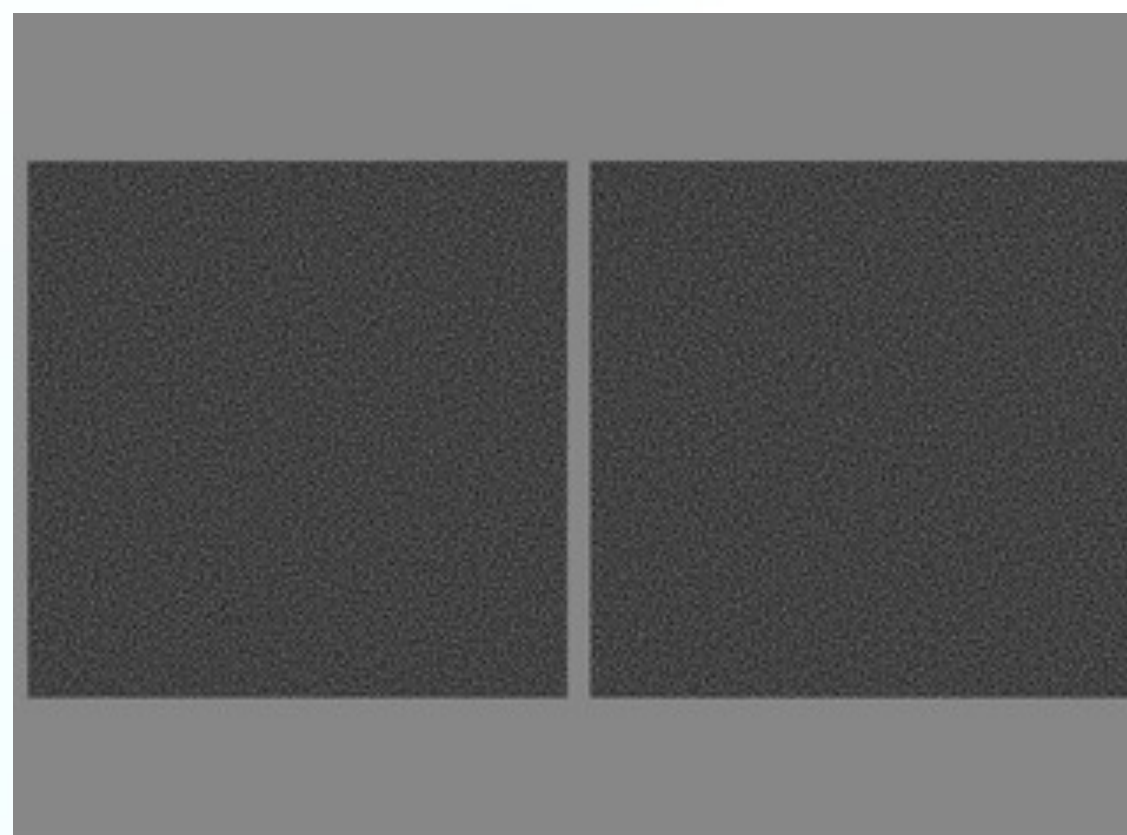
林晨煦 b07902038

張正源 b08902074

2023/5/22

Motivation

- Lecture 6 Digital Halftoning 的課堂上看到 2 張圖片疊合出隱藏圖片的技術，覺得很酷
- 想在實作的過程中，了解這項技術的原理
- 可用於電腦中以圖片形式保存秘密訊息，藉此保護隱私



share 1

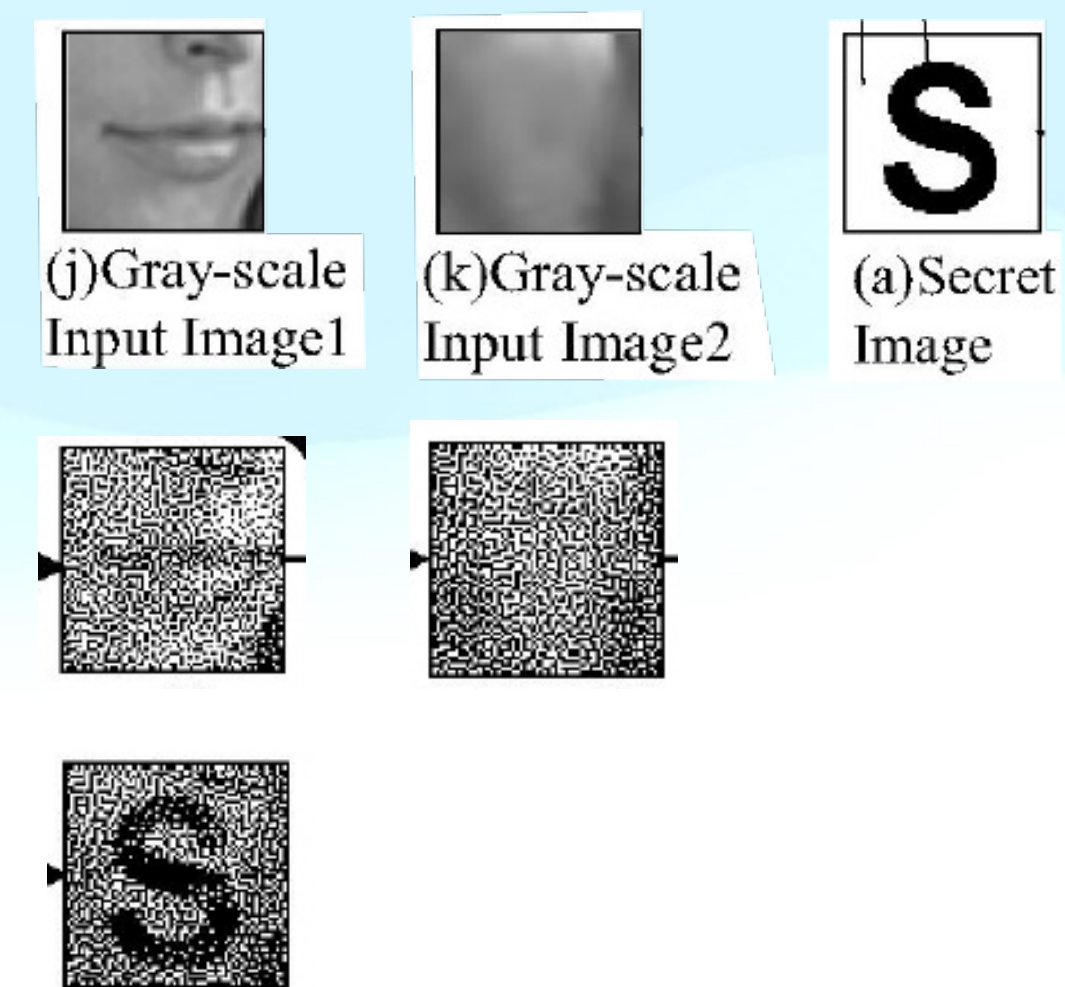


share 2



Problem Definition

- 給予兩張灰階圖片與一張目標黑白圖片
- 將兩張灰階圖片經 halftoning 處理，再進行疊合
- 疊合後可辨認出目標黑白圖片
- 使用 thresholding 進行 halftoning
 - Threshold arrays 是經由 VAC-operation 所產生的 2D 閾值



Problem Definition

Example（以下投影片將以此為例子）

- 原始訊息=“NTU_CSIE 臺大資工”（存成 148*105 的 png 檔），如下所示
- 輸入灰階圖片為兩隻狗，大小同為 148*105，如下所示



secret.png



dog1.png



dog2.png

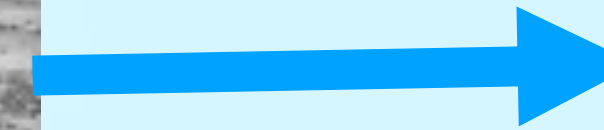
Algorithm

Pre-processing (前處理)

- 準備兩張灰階圖片與一張黑白加密圖片
- 圖片大小皆為 $M * N$
- 確保圖片格式與大小符合需求
- 將兩張灰階圖片，透過 Contrast Manipulation，將 intensity value 的範圍從0~255，縮小成64~191，以改善最終 decode 後的效果（存成 F1.png 及 F2.png）



dog1.png



F1.png



dog2.png

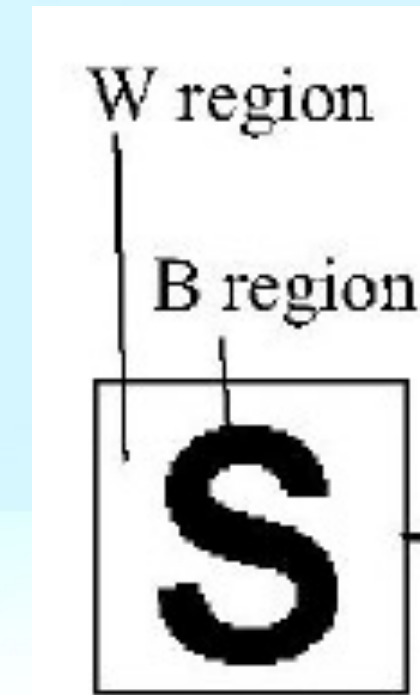


F2.png

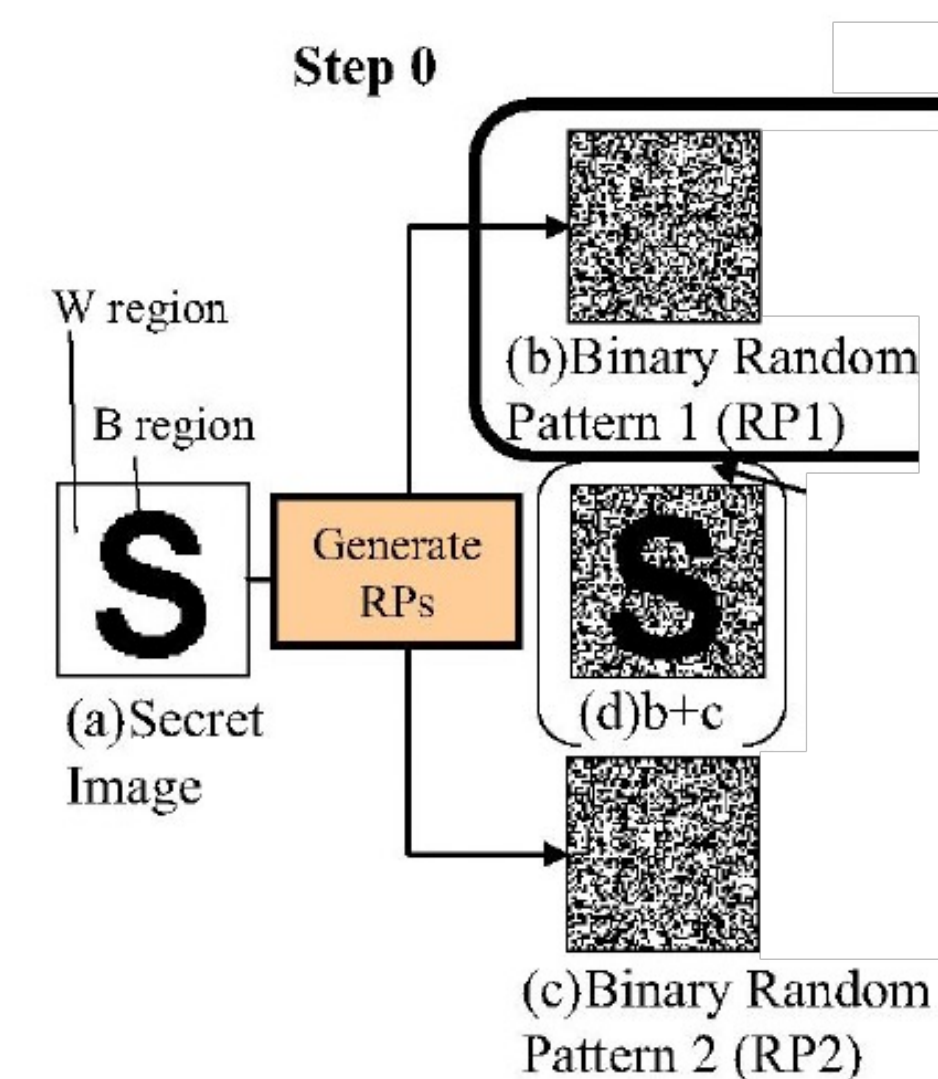
Algorithm

Step 0: Generating RPs (Random Binary Pattern Shares)

- 將黑白圖片的每個像素分為W（白色），B（黑色）兩種
- 對於圖中每一像素點 (i, j)：



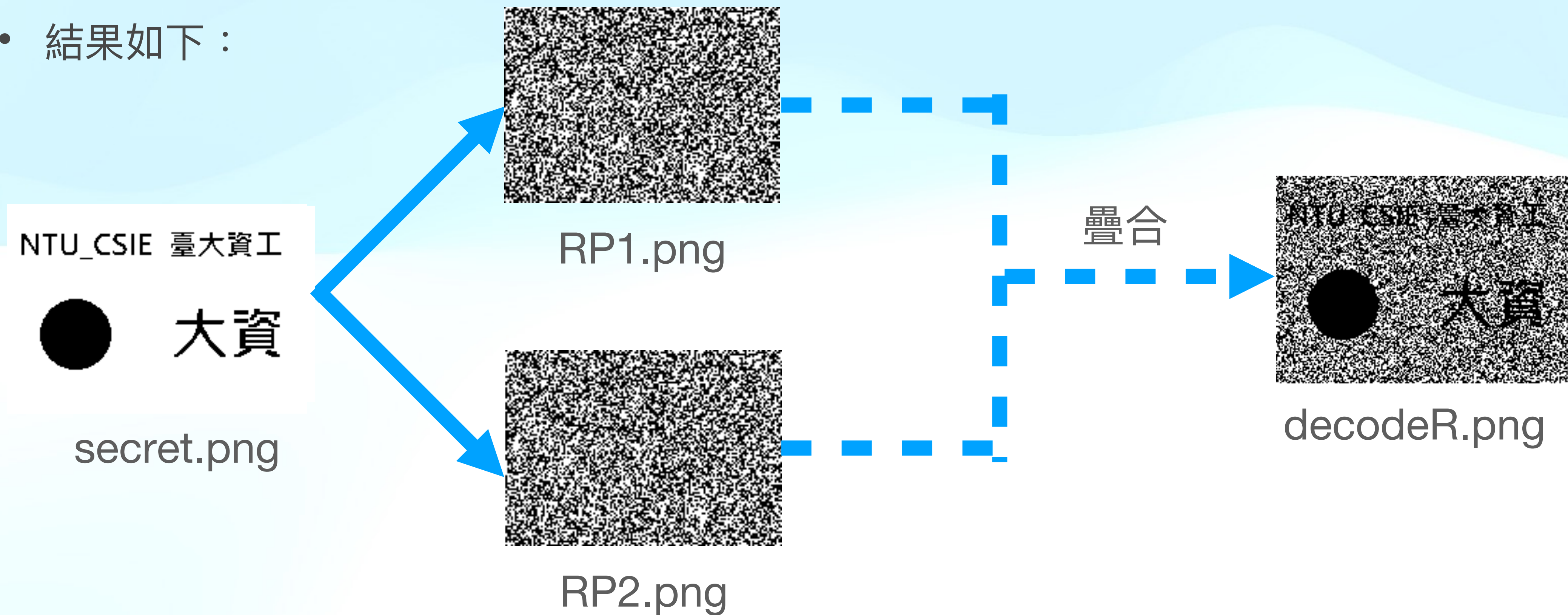
- 根據黑白圖片是 W 或 B，給對應位置的像素對 (RP1_{ij}, RP2_{ij}) 隨機賦值 $\begin{cases} W \text{ pixel } (RP1, RP2) = (0,1) \text{ or } (1,0). \\ B \text{ pixel } (RP1, RP2) = (0,0) \text{ or } (1,1). \end{cases}$
- 由上述方法，產生 RP1 和 RP2
- RP1, RP2 疊合後，可獲得右圖中(d)的圖案



Algorithm

Step 0: Generating RPs (Random Binary Pattern Shares)

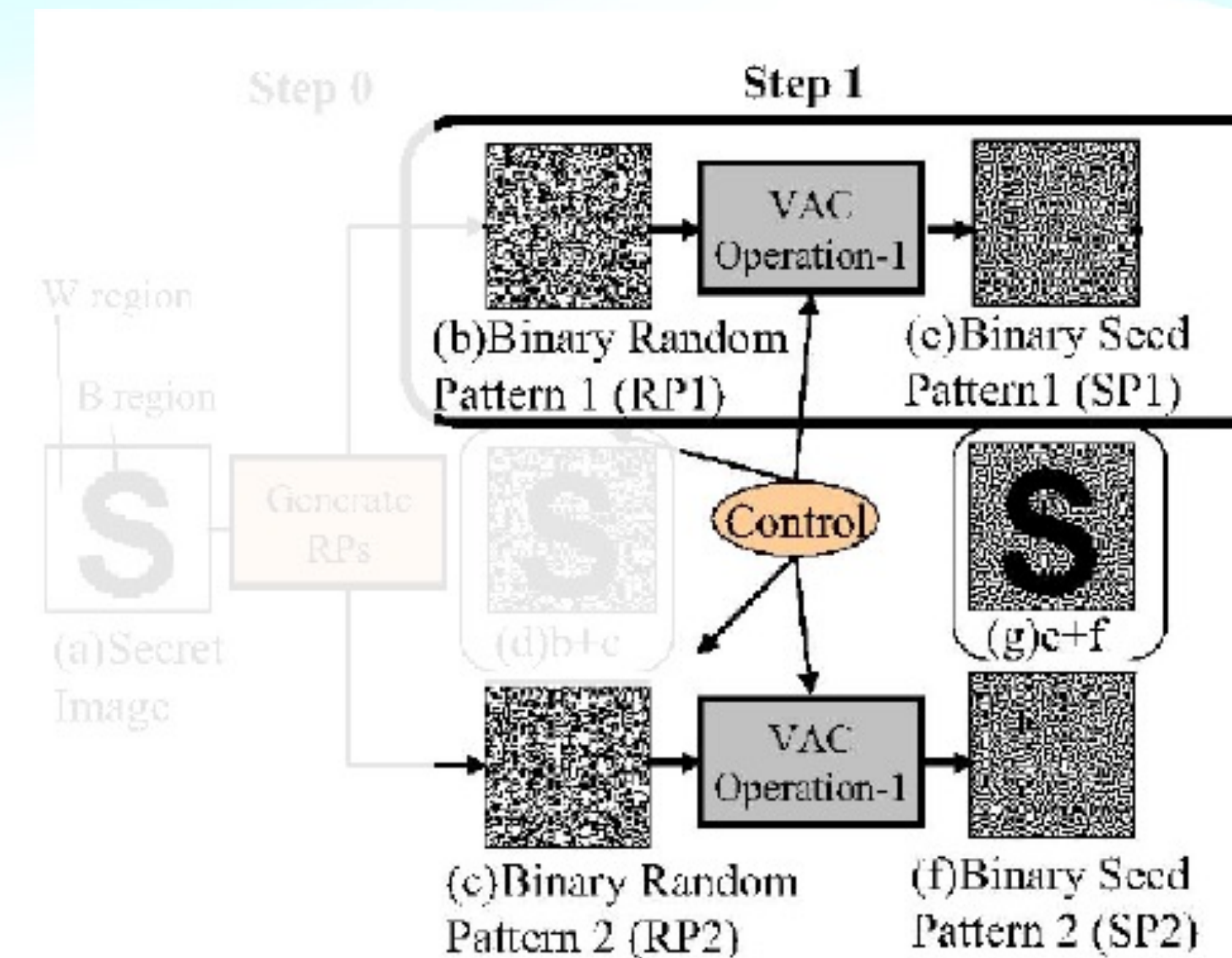
- 結果如下：



Algorithm

Step 1: Generating SPs (Binary Seed Pattern Shares)

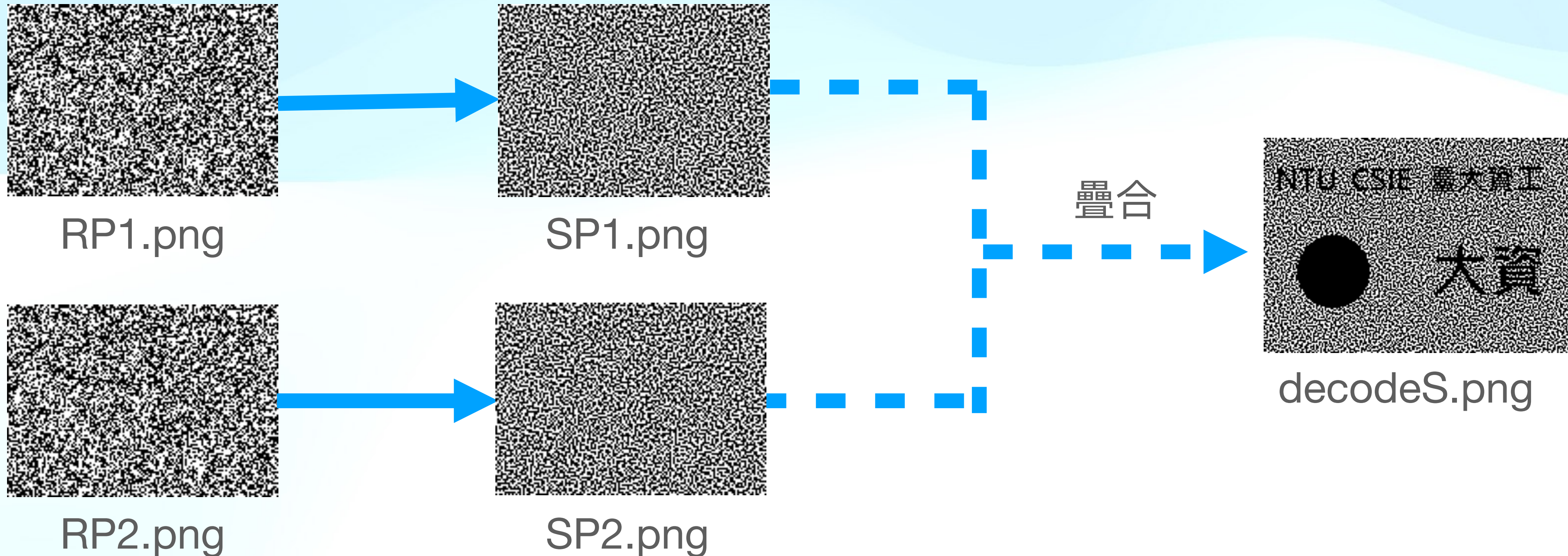
- 使用 VAC Operation-1 演算法
- 對 RP1 和 RP2，分別生成 SP1 和 SP2
- 生成後的結果，如右圖(e), (f), (g)所示



Algorithm

Step 1: Generating SPs (Binary Seed Pattern Shares)

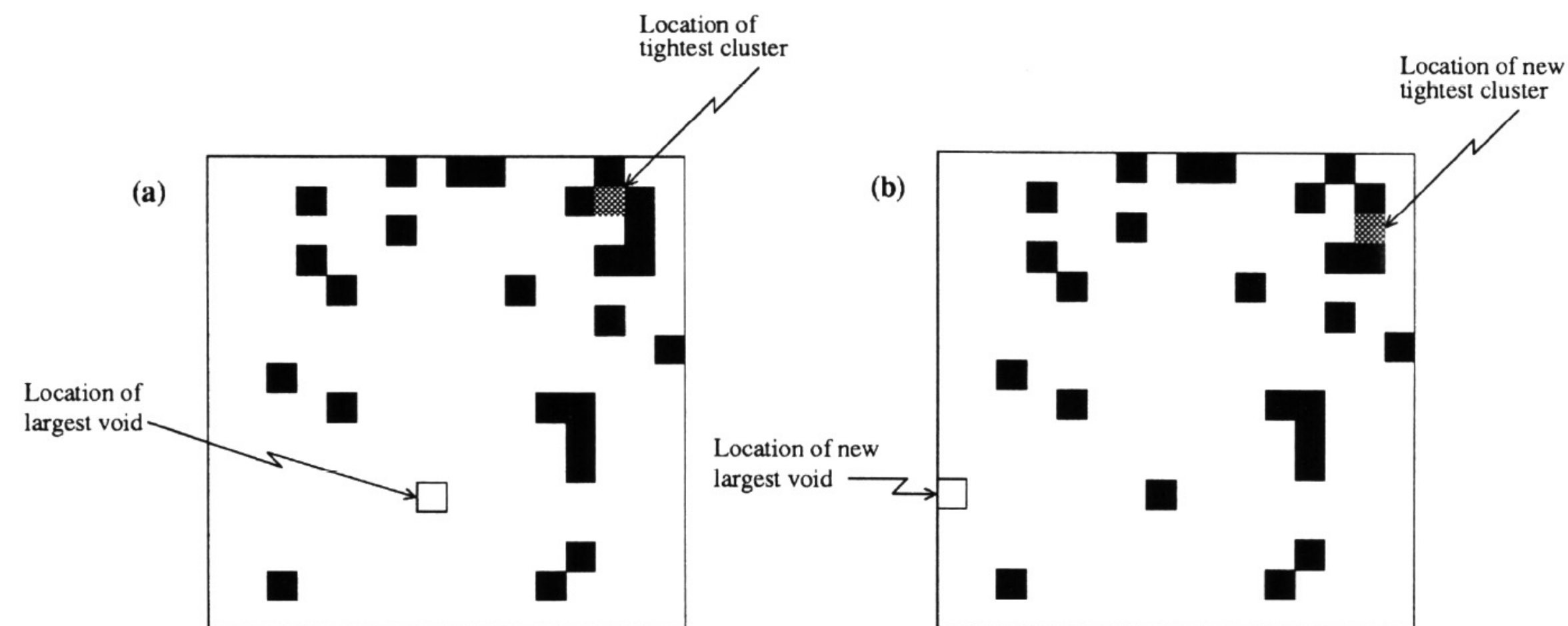
- 結果如下：



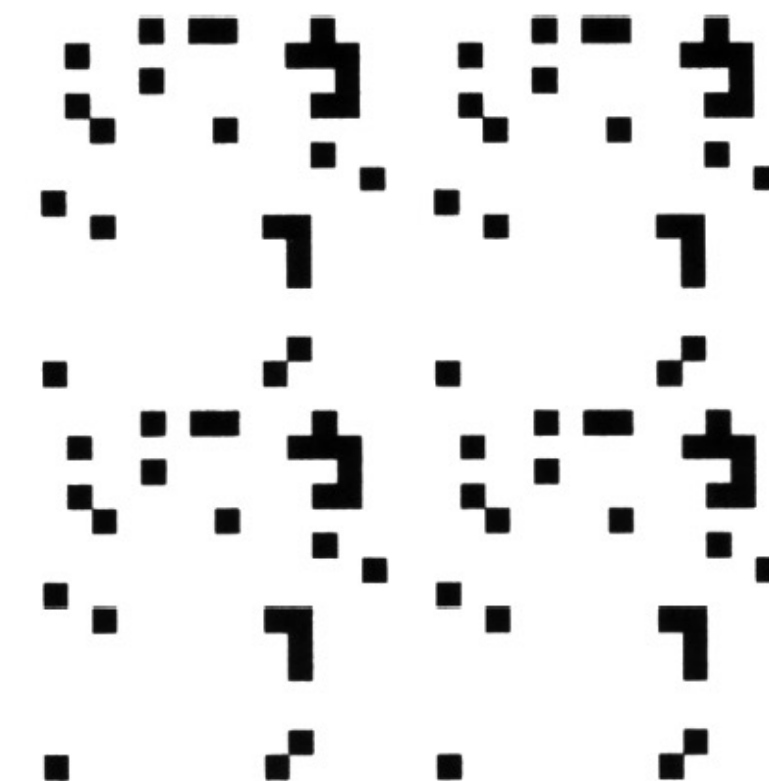
Algorithm

About VAC Operation

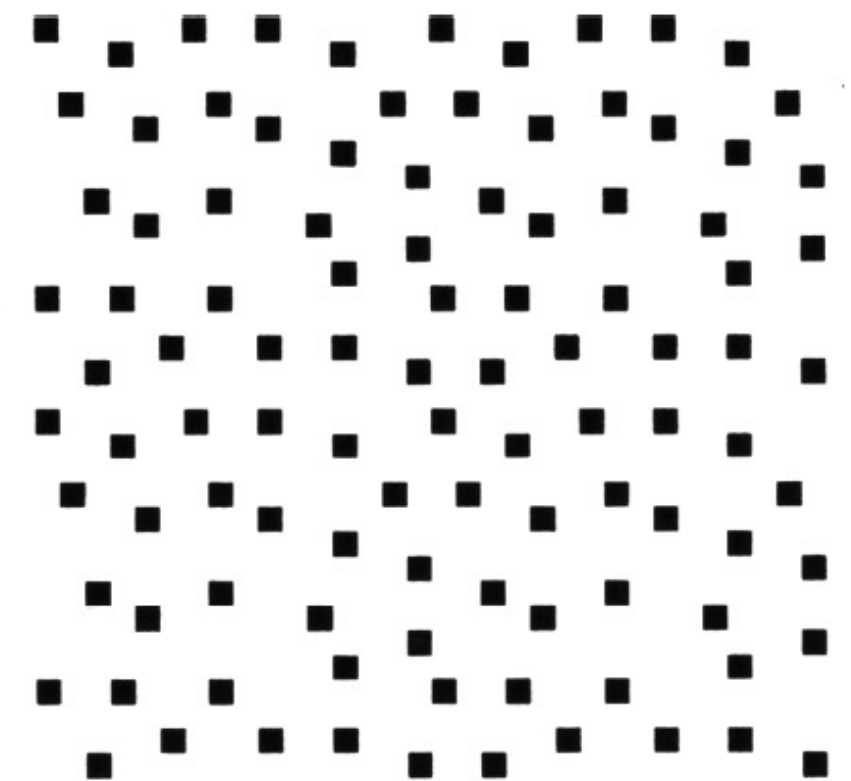
- "The void-and-cluster method for dither array generation", 1993. R. A. Ulichney, 1993.
- 反覆計算 pixel 的叢集與空間區域，利用刪除叢集 pixel 並添加空間 pixel 的方式來讓 halftoning 的 pixel 分佈逐漸均勻化



(a) Input Pattern



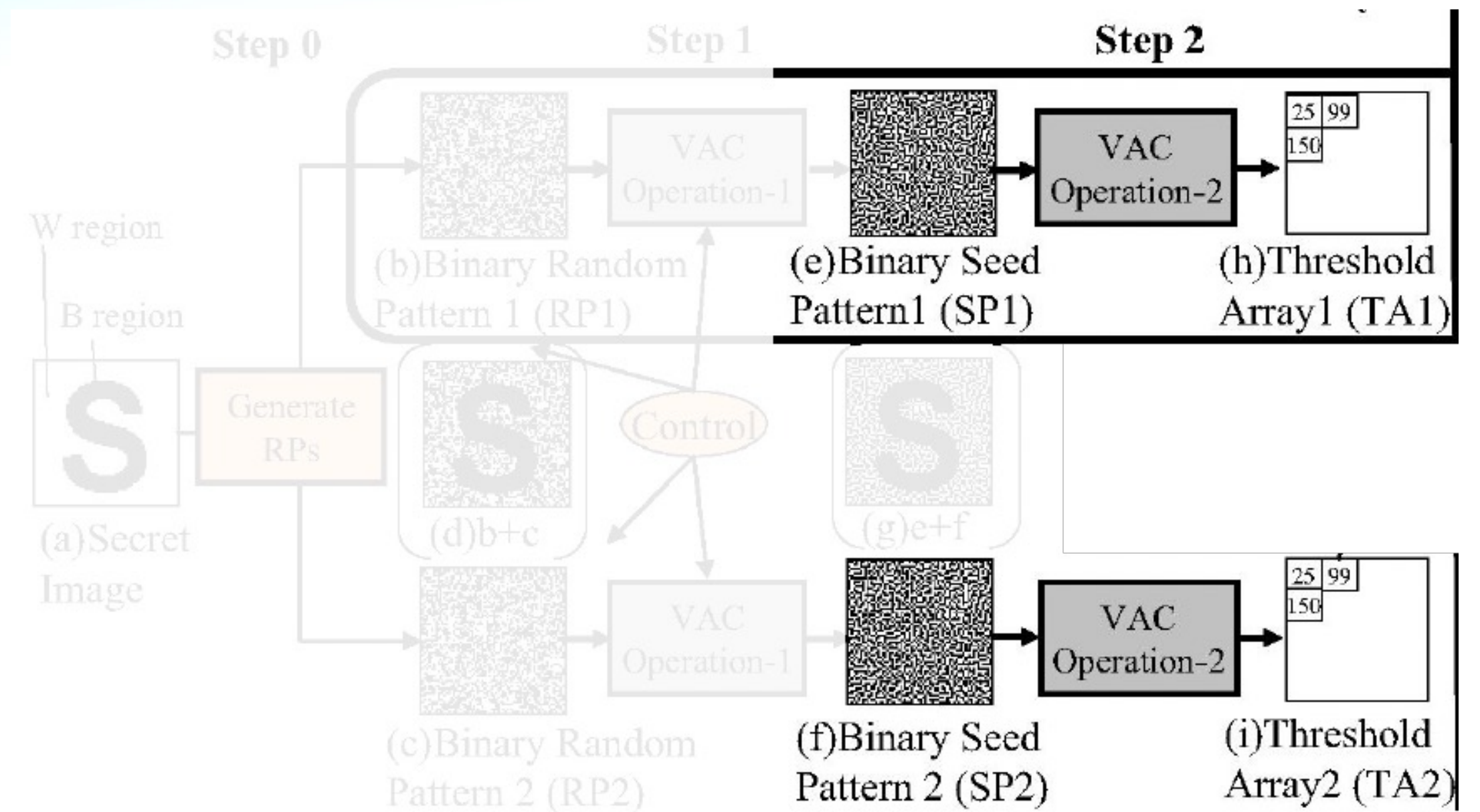
(b) Rearranged Pattern



Algorithm

Step 2: Generating TAs (Threshold Arrays)

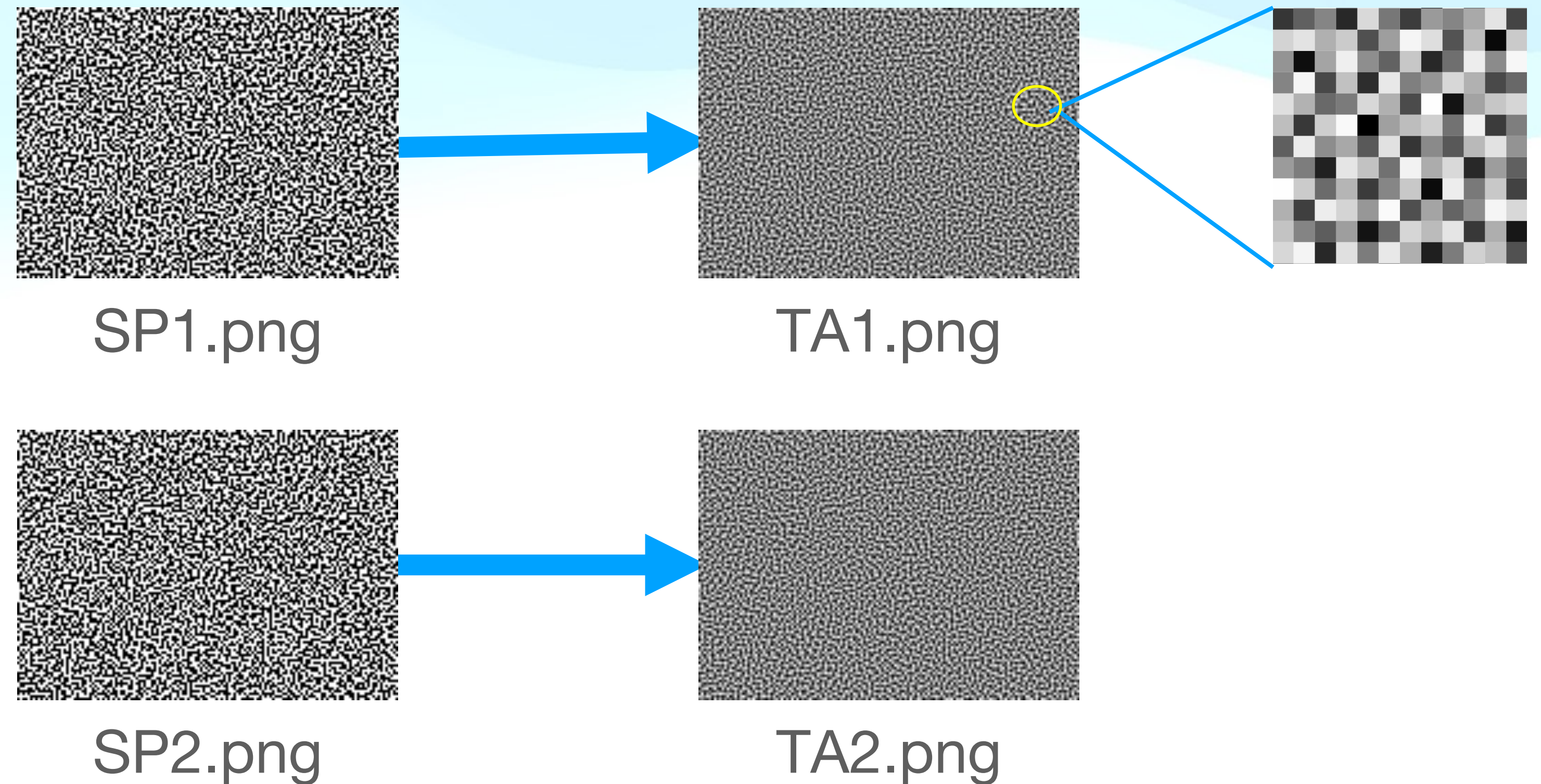
- 對 SP1 和 SP2 使用 VAC Operation-2 演算法
- 依照 SP1, SP2 每個 window 裡面的 pixel 分佈計算出 threshold array 分別生成 TA1 和 TA2
- 生成後的結果，如右圖(h), (i)所示



Algorithm

Step 2: Generating TAs (Threshold Arrays)

- 結果如下（下圖 TA1.png, TA2.png 是將 threshold arrays 視為 image，存成 png 檔後的樣子）：



Algorithm

Step 3: Generating Xs (Binary Share Images)

- 將 2 張灰階圖片 F1, F2

依照 TA1 和 TA2 提供的 threshold 來進行 Halftoning 轉換
$$\begin{cases} \text{Pixel} = 0 & \text{if } F1(j,k) < TA1(j,k) \\ \text{Pixel} = 1 & \text{if } F2(j,k) \geq TA2(j,k) \end{cases}$$

- 產生 binary share images X1, X2

- 疊合 X1 和 X2

可得目標黑白圖片中的訊息

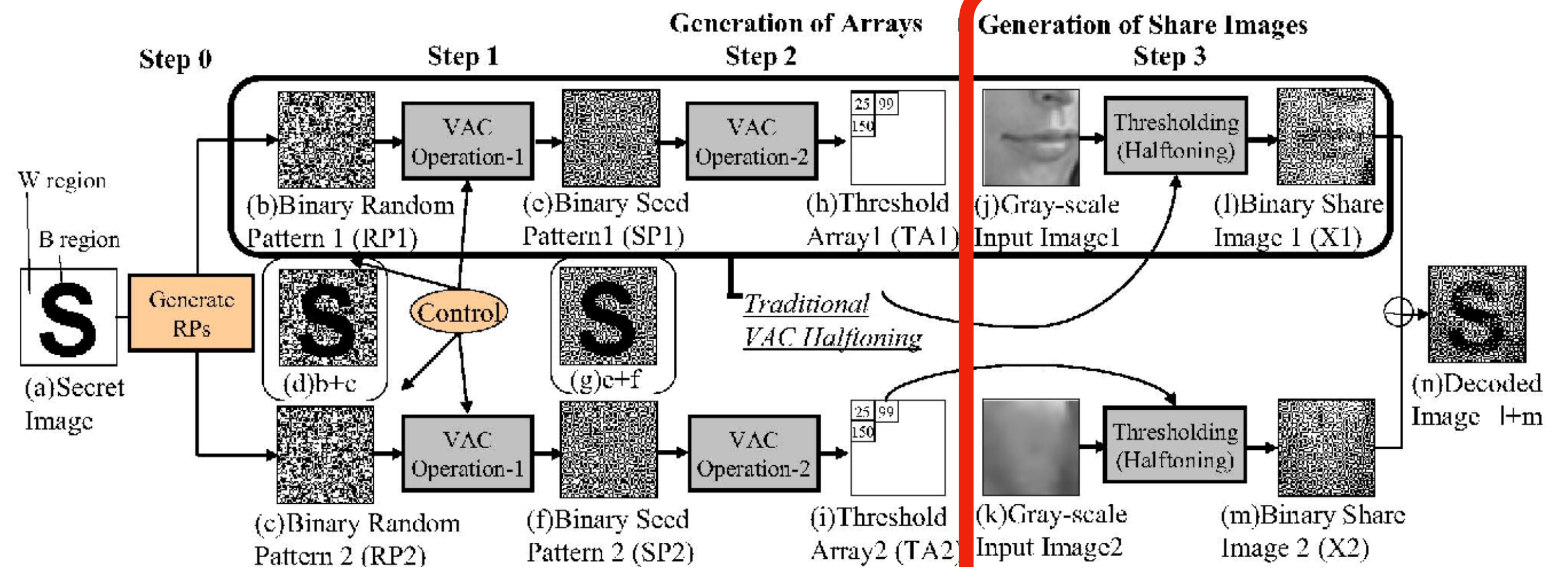
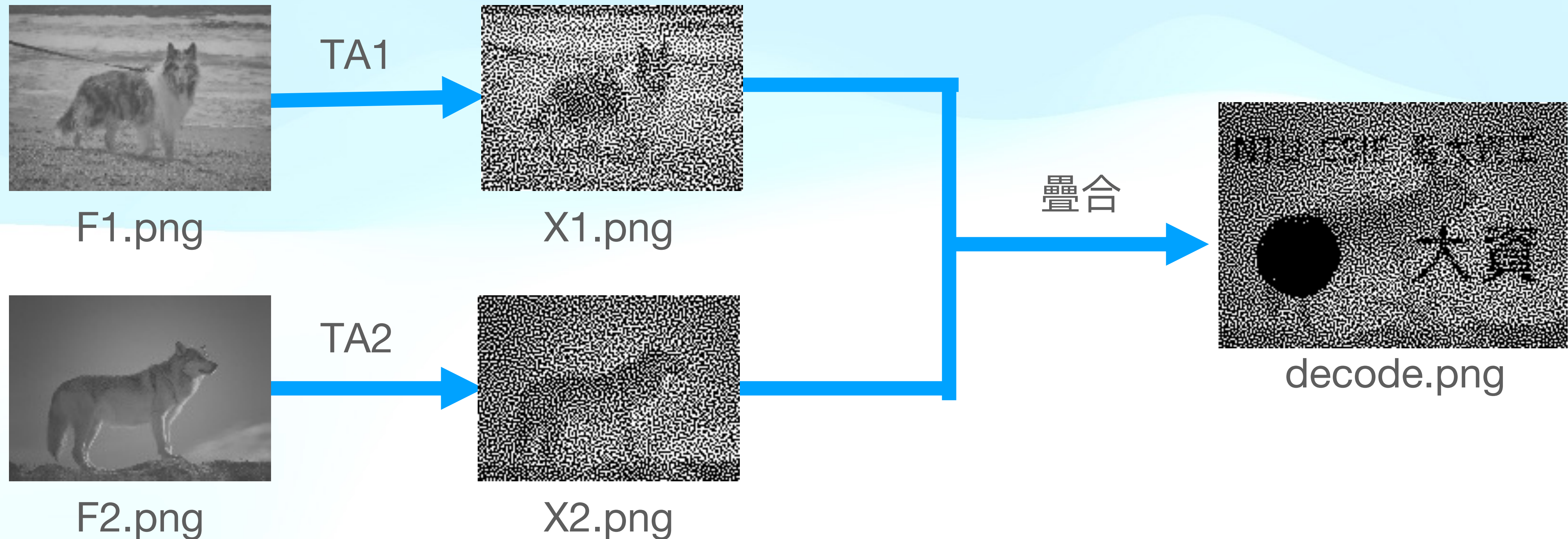


Fig. 3 Proposed VAC-HVC algorithm

Algorithm

Step 3: Generating Xs (Binary Share Images)

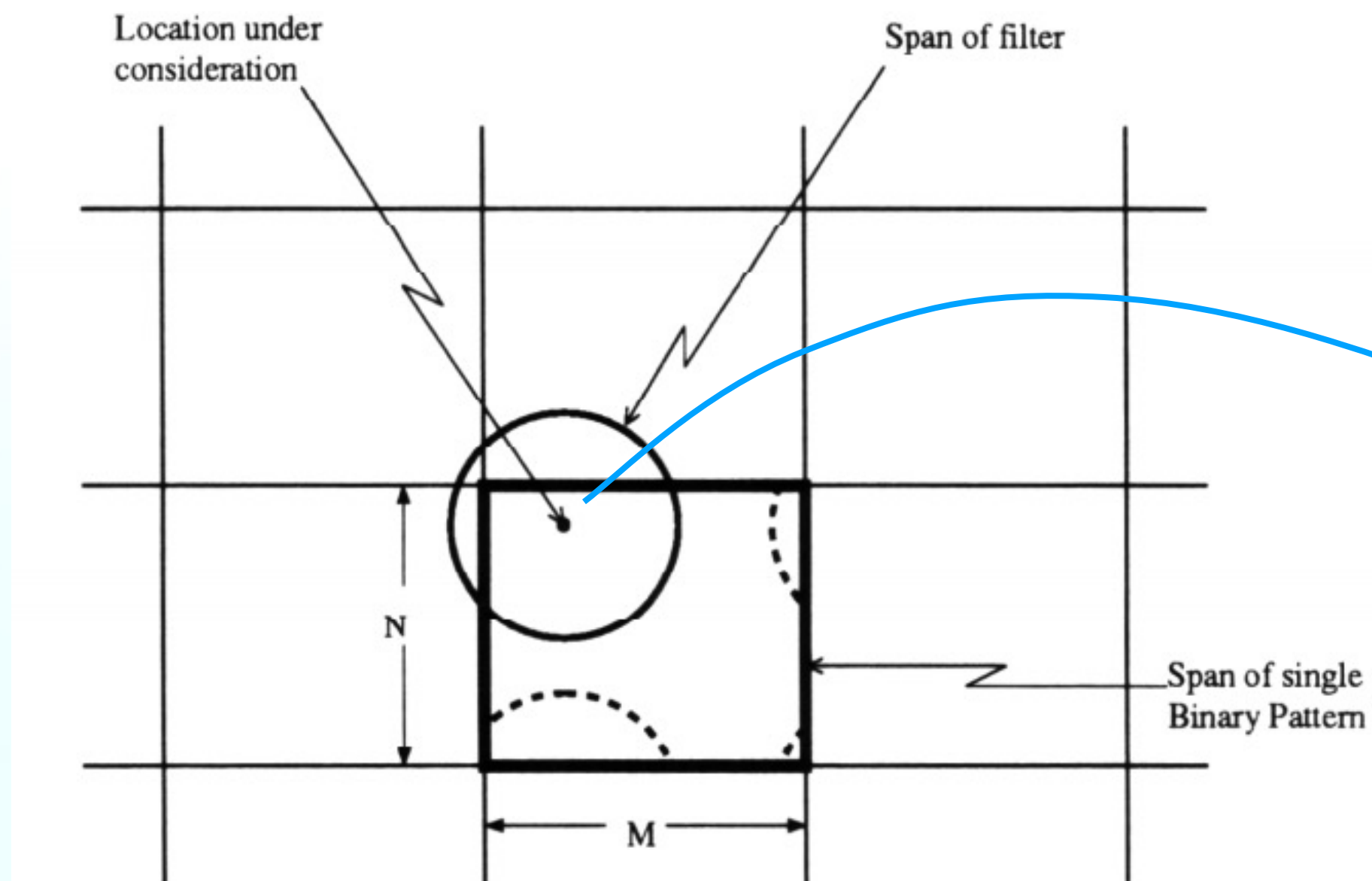
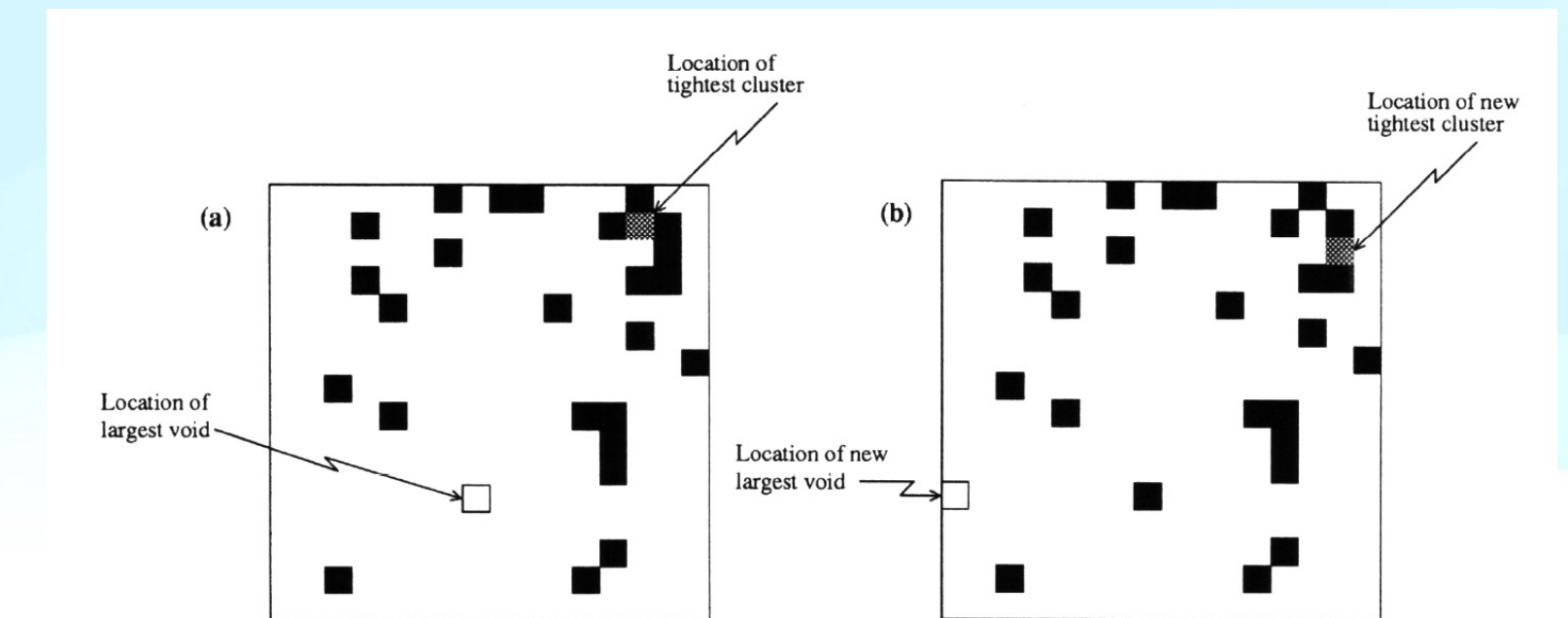
- 結果如下：



到此，我們已經將原始訊息「NTU_CSIE 臺大資工」，藏在 X1.png 和 X2.png 中。將兩張圖疊合後，可將原始訊息重現

Problems

- Tightest Clusters 與 Largest Void 的計算效能
 - 如果把 $m \times n$ 當成常數，則每次 Dither Array (DA) 更新至少需要 $O(n^2)$
 - 把 $m \times n$ 作為 $O(n^2)$ 來看則需要 $O(n^4)$



$$DA(x, y) = \sum_{p=-M/2}^{M/2} \sum_{q=-M/2}^{M/2} BP(p', q') f(p, q)$$

$$p' = (M + x - p) \text{ modulo } M$$
$$q' = (M + y - q) \text{ modulo } M.$$

Problems

- Tightest Clusters 與 Largest Void 的計算效能難以提升
 - 以 VAC-Operator2 而言至少需要更新 DA $m \times n$ 次，若將 $m \times n$ 視為常數則整個流程跑完需要 $O(n^4)$
 - 若將 $m \times n$ 視為 $O(n^2)$ 則需要 $O(n^6)$
 - 一張 128×128 的照片大約需要 40 分鐘， 200×200 則需要 2 個小時以上
 - 圖片小於 128×128 時，成品的解碼效果不好 (幾乎看不出來加密訊息)
 - 如果放在缺乏運算資源的伺服器上直接算到死機

ABCDEFG



Problems

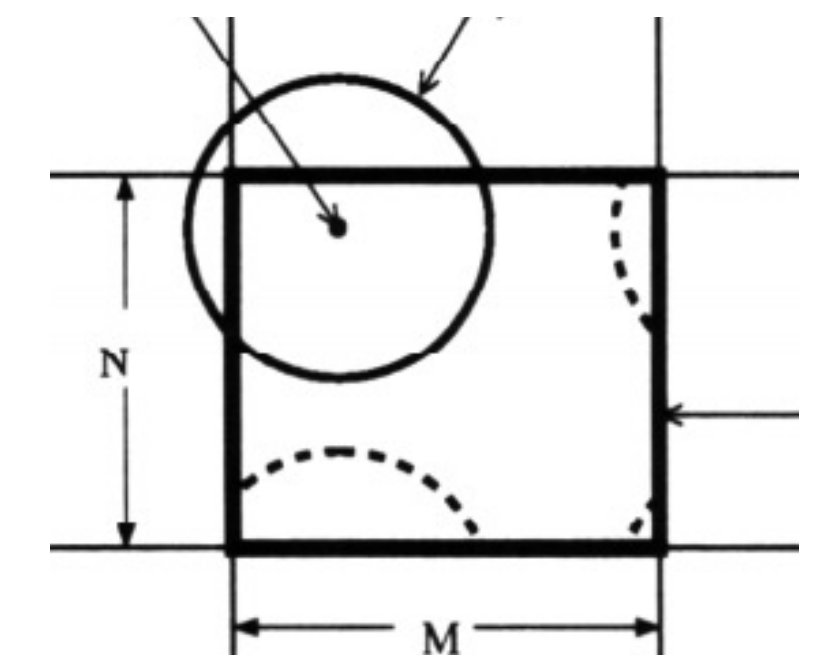
- 優化方式

- VAC-Operator1 將圖片切成多個子塊分別運算
- 事先將所有 weighting function $f(p,q)$ 可能的解都計算出來，用查表的方式使用

$$e^{-\frac{r^2}{2\sigma^2}} \quad r^2 = x^2 + y^2$$

```
Exp = []  
for i in range(0, 100000):  
    Exp.append(np.exp(-i/4.5))
```

- 當 Halftoning Image 有更新時，DA 只更新可能影響到的位置，而不是整張 DA 重新計算
- 運算時間降低為 128x128 大約需要 15 分鐘，200x200 則需要 1 個多小時



Expected Result

- 依照論文中的 Algorithm 進行實作
- 預期可達成「疊合 2 張圖產生原始訊息」的目標
- 完成後預計將結果加框，並印在透明材料上展示
- 設計一個使用者介面，讓使用者可以輸入自己的 crypto message 及圖片，應用會自動產生出兩張加密圖片讓使用者分享留存

References

- *R. A. Ulichney, "The void-and-cluster method for dither array generation", Proc. SPIE, Human Vision Visual Processing, Digital Displays IV, Vol. 1913, pp. 332-343, 1993.*
- *E. Myodo; S. Sakazawa; Y. Takishima, "Visual Cryptography Based on Void-And-Cluster Halftoning Technique", International Conference on Image Processing, 2006*



The end.

Thanks for your listening.