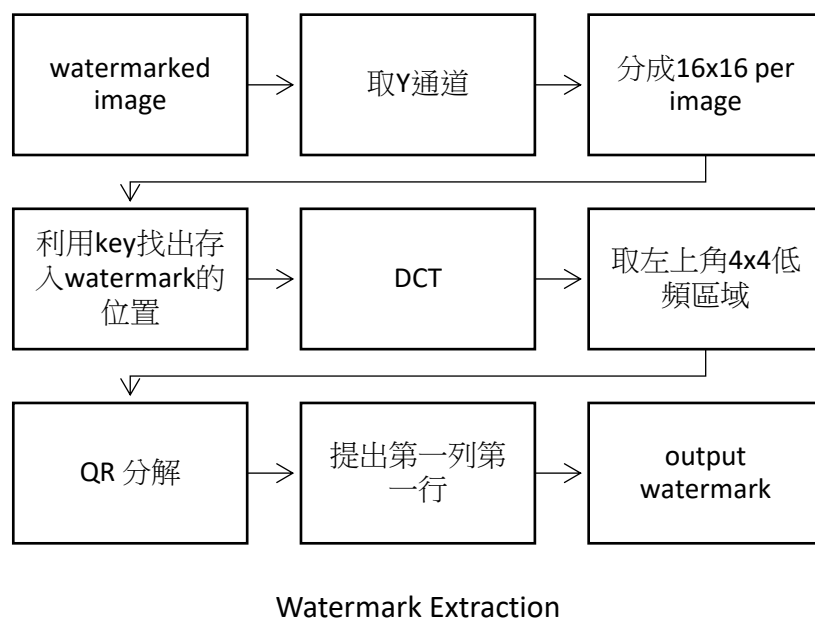
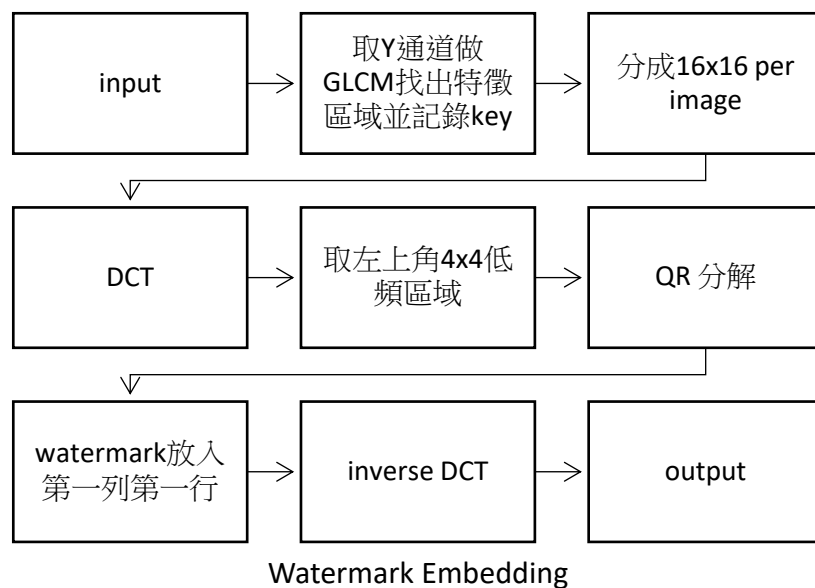


HW4

Title : Image blind watermarking scheme based on DCT-QR decomposition

Introduction :

經過查閱相關 paper 發現，基於 SVD 分解的隱藏浮水印技術已經相當成熟，且搭配 DCT 或 DWT 把浮水印隱藏在低頻區域有相當不錯的效果。但 SVD 分解需要較大的計算資源 ($11n^3$ flops for a $n \times n$ matrix) 且在提取浮水印時需要使用原本的影像。本次作業我們使用基於 QR 分解的隱藏浮水印技術，降低了計算上所需要的資源 ($O(n^2)$ flops) 且搭配 DCT 在隱藏 QR code 上有不錯的成效。本篇的重點是將 Lena 做 DCT 後選取左上角的 4X4 低頻區域，接著將浮水印資訊藏在第一列的第一個元素裡面。在提取浮水印方面，不須使用原本的影像且在各種攻擊下都有良好的表現。



一、 選出儲存浮水印的位置 (compute texture regions)

The entropy value based on the gray-level co-occurrence matrix improves the division of complex texture regions.^[1]

1. Input : 1024 X 1024
2. 裁切圖片每 8 X 8 為一張
3. 取每張圖的 GLCM 後計算 entropy
4. 將所有 entropy 取總和後平均，選出大於平均的 image 並標註
5. 將 8 X 8 的 image 互相結合為 16 X 16
6. 這些 16 X 16 的 image 內有標註 entropy 大於平均的 8 X 8 image，選出標註數量大於平均的 16 X 16 image
7. 隨機從選出的 texture region 中挑選儲存浮水印的位置



Fig 1. compute texture regions

二、 Discrete cosine transform

$$\begin{cases} D(i, j) = \frac{1}{2\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos \frac{(2x+1)i\pi}{2N} \cos \frac{(2y+1)j\pi}{2N} \\ f(x, y) = \frac{1}{2\sqrt{2N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} C(i)C(j) D(i, j) \cos \frac{(2x+1)i\pi}{2N} \cos \frac{(2y+1)j\pi}{2N} \end{cases}$$

1. 將隨機挑選的 texture region 取 DCT
2. 取左上角低頻區域 4 X 4

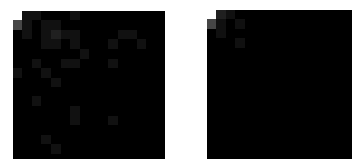


Fig 2. DCT and masked

三、 QR 分解

1. 根據 Reference [3] 提出的基於 Gram-Schmidt 正交化法改進的 QR 分解方法計算 R
2. Q 可從 R 由 Gram-Schmidt 正交化法得到
3. 若 A 為 full column rank 且 R 對角線元素為正，則 QR 分解唯一
4. 優點：只需計算 r_{11} 即可算出剩餘元素，浮水印資料也將存於 r_{11} 中

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} = QR$$

$$= \begin{bmatrix} q_{11} & q_{12} & q_{13} & q_{14} \\ q_{21} & q_{22} & q_{23} & q_{24} \\ q_{31} & q_{32} & q_{33} & q_{34} \\ q_{41} & q_{42} & q_{43} & q_{44} \end{bmatrix} \begin{bmatrix} r_{11} & r_{12} & r_{13} & r_{14} \\ 0 & r_{22} & r_{23} & r_{24} \\ 0 & 0 & r_{33} & r_{34} \\ 0 & 0 & 0 & r_{44} \end{bmatrix}$$

$$M = A^T A = (QR)^T QR = R^T R$$

$$\begin{bmatrix} m_{11} & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \\ m_{31} & m_{32} & m_{33} & m_{34} \\ m_{41} & m_{42} & m_{43} & m_{44} \end{bmatrix} = \begin{bmatrix} r_{11} & 0 & 0 & 0 \\ r_{12} & r_{22} & 0 & 0 \\ r_{13} & r_{23} & r_{33} & 0 \\ r_{14} & r_{24} & r_{34} & r_{44} \end{bmatrix} \begin{bmatrix} r_{11} & r_{12} & r_{13} & r_{14} \\ 0 & r_{22} & r_{23} & r_{24} \\ 0 & 0 & r_{33} & r_{34} \\ 0 & 0 & 0 & r_{44} \end{bmatrix}$$

根據計算可得：

$$R = \begin{bmatrix} \sqrt{m_{11}} & \frac{m_{12}}{r_{11}} & \frac{m_{13}}{r_{11}} & \frac{m_{14}}{r_{11}} \\ 0 & \sqrt{m_{22} - r_{12}^2} & \frac{m_{23} - r_{12}r_{13}}{r_{22}} & \frac{m_{24} - r_{12}r_{14}}{r_{22}} \\ 0 & 0 & \sqrt{m_{33} - r_{13}^2 - r_{23}^2} & \frac{m_{34} - r_{13}r_{14} - r_{23}r_{24}}{r_{33}} \\ 0 & 0 & 0 & \sqrt{m_{44} - r_{14}^2 - r_{24}^2 - r_{34}^2} \end{bmatrix}$$

在計算 R 的對角線 r_{ii} 時，為了避免根號內 ≤ 0 (這樣會造成同一 row 的值計算成無窮大)，所以當根號內 ≤ 0 時對角線該值設為 1。

四、 Watermark Embedding

1. Watermark input：290 X 290，並縮小成 29 X 29
2. 利用下列公式組成長度為 841 的 sequence

$$w_i = 0, \quad R'(1,1) = \begin{cases} R(1,1) + \frac{q}{4} - z & \text{if } z < 3\frac{q}{4} \\ R(1,1) + \frac{5q}{4} - z & \text{if } z > 3\frac{q}{4} \end{cases}$$

$$w_i = 255, \quad R'(1,1) = \begin{cases} R(1,1) - \frac{q}{4} - z & \text{if } z < \frac{q}{4} \\ R(1,1) + \frac{3q}{4} - z & \text{if } z > \frac{q}{4} \end{cases}$$

3. Update A by $A' = QR'$

五、 Watermark Extraction

$$R(1,1) = \sqrt{A(1,1)^2 + A(2,1)^2 + A(3,1)^2 + A(4,1)^2}$$
$$z = R(1,1) \bmod q$$

$$\left(z < \frac{q}{2}\right) \Rightarrow w = 0 \text{ else } w = 255$$

Result :

設置 q 的大小會影響 invisibility 和 robustness，當 q 越大，浮水印的 invisibility 就越弱，PSNR, SSIM 效果越差，但是 robustness 就越強。

原圖為"lena.bmp" size=1024x1024，浮水印為"watermark.png" size=290x290

以下展示三種 q : $q=150$, $q=250$, $q=350$ 受助教提供的三種攻擊方式的結果：

$q=150$









PSNR = 45.208

SSIM = 0.994999

Extract watermark without attack BER = 0%



Fig 3. Extract watermark

q=150	Noise ($\mu=0, \sigma=0.1$)	Blur (ksize=(7,7) $\sigma=2$)	Compress Resize to (200,200)
Host image			
浮水 印			
BER	11.5338%	4.1617 %	16.1712%

結果：都無法用手機辨識出 QR code

q=250



PSNR = 41.7095322

SSIM = 0.99113066

Extract watermark without attack BER = 0%



Fig 4. Extract watermark

q=250	Noise ($\mu=0, \sigma=0.1$)	Blur (ksize=(7,7) $\sigma=2$)	Compress Resize to (200,200)
Host image			
浮水 印			
BER	0.9512%	0.5945 %	7.6099%

結果：前兩者可以用手機辨識出 QR code，compress 則不行。

q=350



PSNR = 38.8268

SSIM = 0.985079

Extract watermark without attack BER = 0%



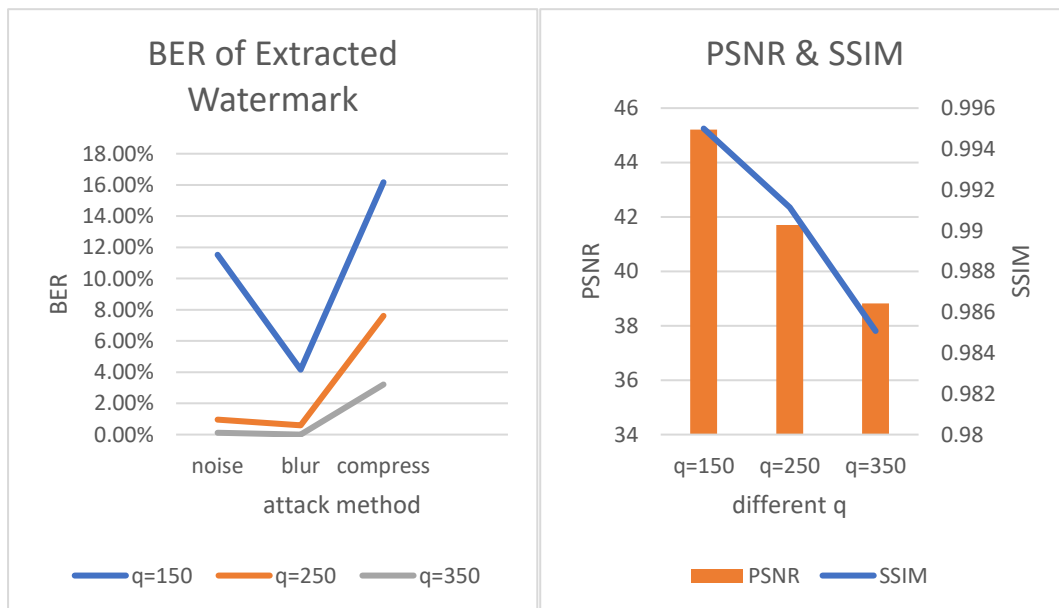
Fig 5. Extract watermark

q=350	Noise ($\mu=0, \sigma=0.1$)	Blur (ksize=(7,7) $\sigma=2$)	Compress Resize to (200,200)
Host image			
浮水 印			
BER	0.1189%	0.0 %	3.2104%

結果：三者都可以用手機辨識出 QR code，只是 compress 辨識的有點困難。

註：相同程式每次測試取出的浮水印圖案都不同，BER 也會略為浮動。以 q=350 為例，曾測出過 noise 攻擊後的 BER=0.0%，compress 攻擊後的 BER=3.8%。

整理成圖表如下：



可以觀察到我們的做法對於 gaussian blur 的抵抗性最好，其次為 noise，最差為 compression。

References

- [1] Zhao Xiaolei, Wang Guangqin, and Xu Xibin. 2020. Robust Digital Watermarking Algorithm Based on DCT-SVD and QR Code. In Proceedings of the 2020 3rd International Conference on Artificial Intelligence and Pattern Recognition (AIPR 2020). Association for Computing Machinery, New York, NY, USA, 186–190.
- [2] Qingtang Su, Yugang Niu, Gang Wang, Shaoli Jia, Jun Yue. Color image blind watermarking scheme based on QR decomposition, Signal Processing, Volume 94, 2014, Pages 219-235, ISSN 0165-1684.
- [3] P. T. Nha, T. M. Thanh and N. Huynh, "An improved QR decomposition for color image watermarking," 2018 10th International Conference on Knowledge and Systems Engineering (KSE), 2018, pp. 56-60, doi: 10.1109/KSE.2018.8573423.
- [4] Phuong Thi Nha, Ta Minh Thanh, "A Combination of DWT and QR Decomposition for Color Image Watermarking", 2021 13th International Conference on Knowledge and Systems Engineering (KSE), pp.1-6, 2021.