Assignment 08: Integrated Message Embedding and Encryption Algorithm

授課教師：王宗銘

2023/12/20

1. 請撰寫
   (1) 1 個[偽裝加密與嵌密程式](學號-ass08-FCUE.py)
   (2) 1 個[偽裝解密與取密程式](學號-ass08-BDIX.py)
   影像符號說明與詳細流程，請參考下方流程圖。

2. FCUE 程式

Input:

1. a grayscale image, I_{GC}.
2. secret message {S}.
3. secret keys, [HK], [PK], and [EK]

Processes:

1. GMWRDH Embedding: Applying GMWRDH(n, M, Z, I_{GC}) to produce $I'_{G1}, I'_{G2}, I'_{G3}$.
2. Channel Composition: Compositing $I'_{G1}, I'_{G2}, I'_{G3}$ to form I'_{PC}.
3. Channel Permutation: Random permutation with [PK] to produce I'_{PMC}.
4. RT Encryption: Applying RT Encryption on I'_{PC} using [EK] to produce I'_{EC}.

Output:

1. an encrypted marked color image, I'_{EC}.

3. BDIX 程式

Input:

1. an encrypted marked color image,I'_{EC}
2. secret keys, [DK], [PK], [XK]

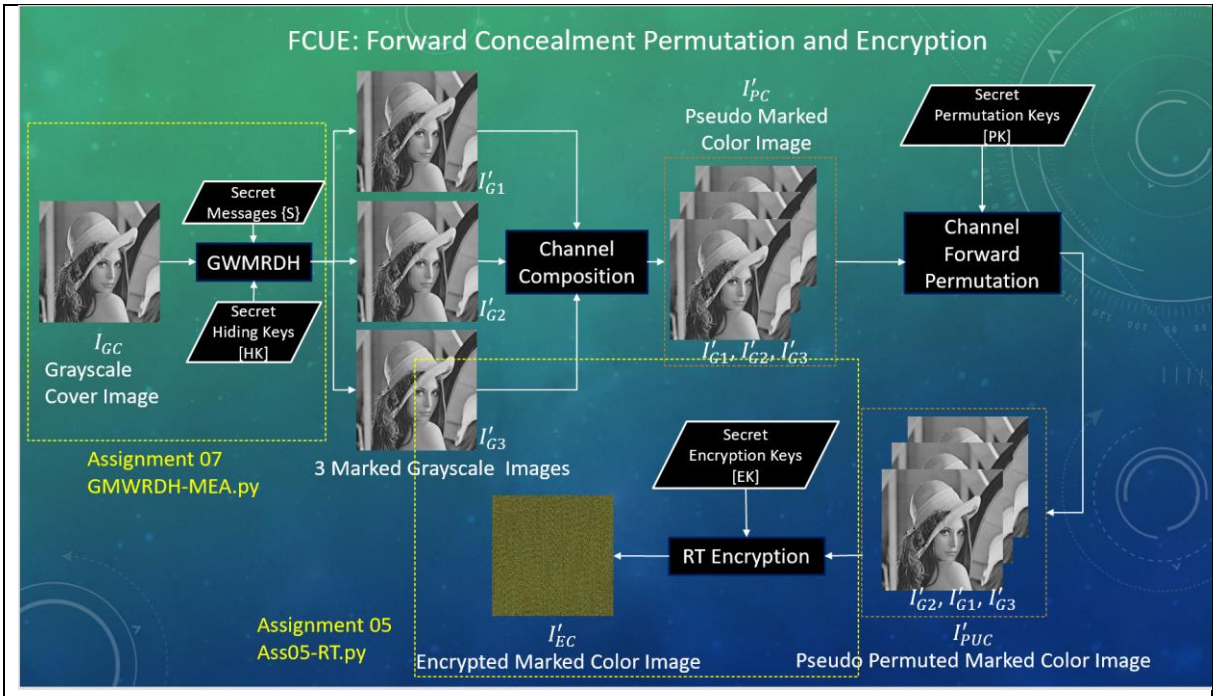
Process:

1. IRT Decryption: Applying IRT with [DK] to decrypt I'_{EC} and produce I'_{PUC}.
2. Channel Inverse Permutation: Applying inverse permutate with [PK] on I'_{PUC} to produce I'_{PC}.
3. Channel Decomposition: Retrieve three marked grayscale images $I'_{G1}, I'_{G2}, I'_{G3}$ from I'_{PC}.
4. Message extraction: Extract secret message {S} using [XK] from $I'_{G1}, I'_{G2}, I'_{G3}$.
5. Restoring image: Using $I'_{G1}, I'_{G2}, I'_{G3}$ to produce I_{RG}.

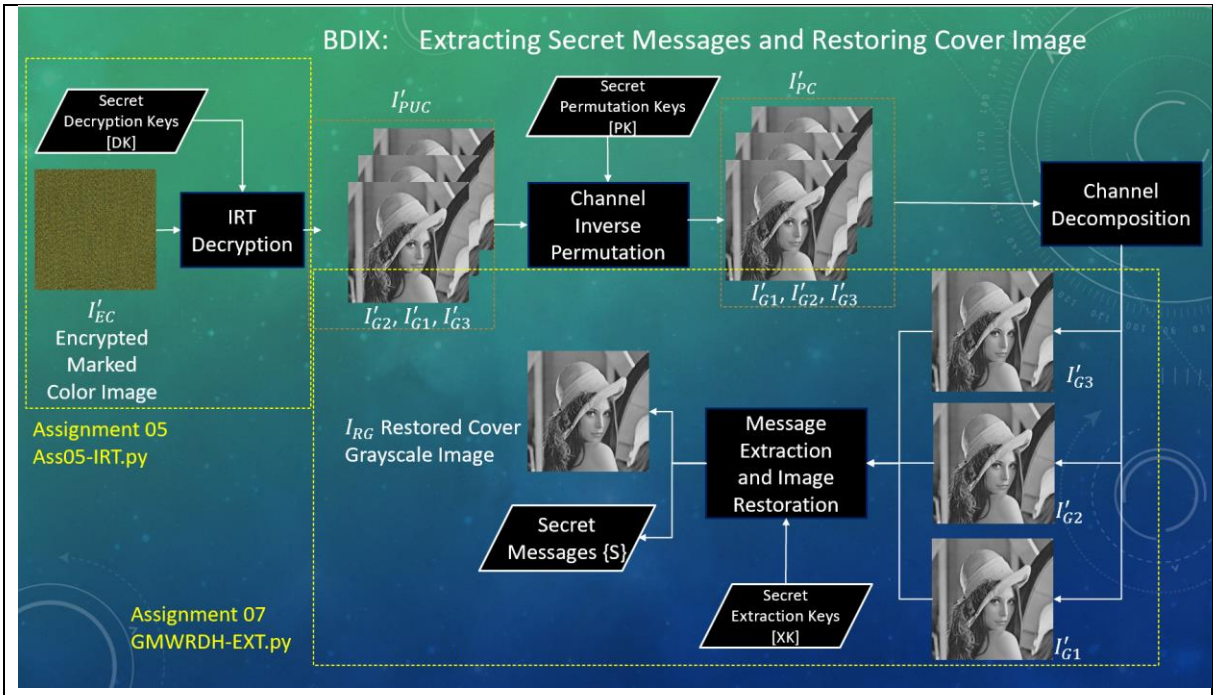
Output:

1. secret message, {S}.
2. restored image, I_{RG}.

4. 使用或儲存結果之檔案目錄，共 15 個目錄，說明如下：
   1-origin: 原始影像, I_{GC}
   2-marked: 嵌密影像, I'_{G1}, I'_{G2}, I'_{G3}.
   3-channe: 構建影像, I'_{PC}.
   4-permut: 排列影像, I'_{PUC}.
   5-encry: 加密影像, I'_{EC}.
   6-decry: 解密影像, I'_{PUC}.
   7-invmut: 逆排列影像, I'_{PC}.
   8-decom: 解構影像, I'_{G1}, I'_{G2}, I'_{G3}.
   9-restor: 恢復影像, I_{RG}.
   10-rpatab: 嵌密參數 (RPA Table 參數檔)
   11-mesmea: 嵌密訊息 (embedding message)
   12-encpar: 加密參數
   13-decpar: 解密參數
   14-mesext: 取密訊息 (extracted message)
   15-imgres: 加密、嵌密、取密、解密、回復數據(quality result)



FCUE:偽裝加密與嵌密 流程



BDIX: 偽裝解密與取密 流程

5. 提供測試：

請使用 Lena.png 與 Baboo.png 測試影像。

提供 LCUE 與 BDIX 流程影像。

6.繳交: 請繳交壓縮檔案，壓縮方式請選 zip 或 rar。

壓縮檔案名稱: 學號-ass08.rar，包含下列 2 個程式、15 個目錄、1 個 readme.txt

(1) 1 個 偽裝加密與嵌密程式 (學號-ass08-FCUE.py)。此程式可由 Assignment 05 與 07 修改之。

(2) 1 個[偽裝解密與取密程式](學號-ass08-BDIX.py)。此程式可由 Assignment 05 與 07 修改之。

(3) 15 個目錄，建議目錄包含數字，可根據流程自動排列。說明如下：

1-origin: 原始影像, I_{GC}

2-marked: 嵌密影像, I'_{G1}, I'_{G2},I'_{G3}.

3-channe: 構建影像, I'_{PC}.

4-permut: 排列影像, I'_{PUC}.

5-encry: 加密影像, I'_{EC}.

6-decry: 解密影像, I'_{PUC}.

7-invmut: 逆排列影像, I'_{PC}.

8-decom: 解構影像, I'_{G1}, I'_{G2},I'_{G3}.

9-restor: 恢復影像, I_{RG}.

10-rpatab: 嵌密參數 (RPA Table 參數檔)

11-mesmea: 嵌密訊息 (embedding message)

12-encpar: 加密參數

13-decpar: 解密參數

14-mesext: 取密訊息 (extracted message)

15-imgres: 加密、嵌密、取密、解密、回復數據(quality result)

(4) 1 個 readme.txt，請放在與 python 程式同目錄層，敘述如何執行 python 程式，載明是否需要額外的套件。(請提供)