### Assignment 08: Integrated Message Embedding and

### Encryption Algorithm

授課教師：王宗銘

2023/12/20

1. 請撰寫
2. 1個[偽裝加密與嵌密程式](學號-ass08-FCUE.py)
3. 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,

2. secret message {S}.

3. secret keys, [HK], [PK], and [EK]

Processes:

1. GMWRDH Embedding: Applying GMWRDH(n, M, Z, ) to produce , .

2. Channel Composition: Compositing , to form .

3. Channel Permutation: Random permutation with [PK] to produce .

4. RT Encryption: Applying RT Encryption on using [EK] to produce .

Output:

1. an encrypted marked color image, .

3. BDIX程式

Input:

1. an encrypted marked color image,

2. secret keys, [DK], [PK], [XK]

Process:

1. IRT Decryption: Applying IRT with [DK] to decrypt and produce .

2. Channel Inverse Permutation: Applying inverse permutate with [PK] on to produce .

3. Channel Decomposition: Retrieve three marked grayscale images , from.

4. Message extraction: Extract secret message {S} using [XK] from , .

5. Restoring image: Using , to produce .

Output:

1. secret message, {S}.

2. restored image, .

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,

2-marked: 嵌密影像, , .

3-channe: 構建影像, .

4-permut: 排列影像,

5-encry: 加密影像, .

6-decry: 解密影像, .

7-invmut: 逆排列影像,

8-decom: 解構影像, , .

9-restor: 恢復影像, .

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,

2-marked: 嵌密影像, , .

3-channe: 構建影像, .

4-permut: 排列影像,

5-encry: 加密影像, .

6-decry: 解密影像, .

7-invmut: 逆排列影像,

8-decom: 解構影像, , .

9-restor: 恢復影像, .

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)