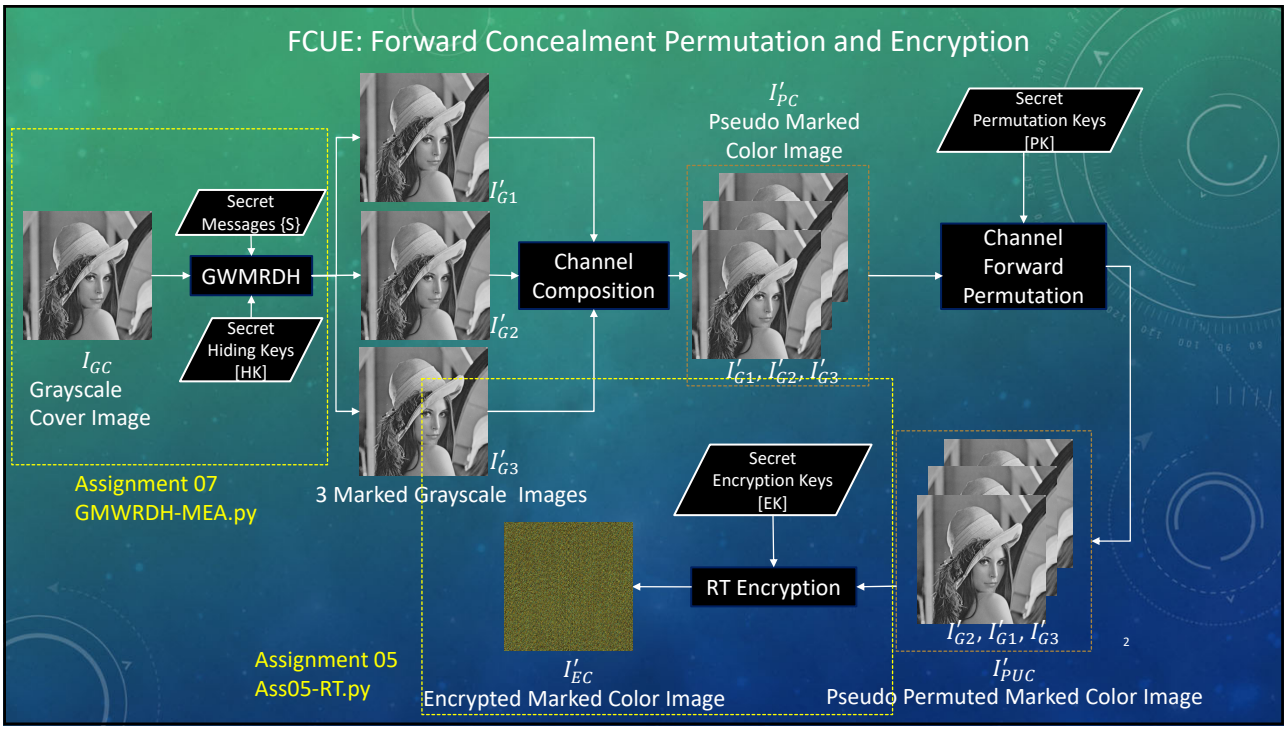
FCUE: FORWARD CONCEALMENT PERMUTATION AND ENCRYPTION

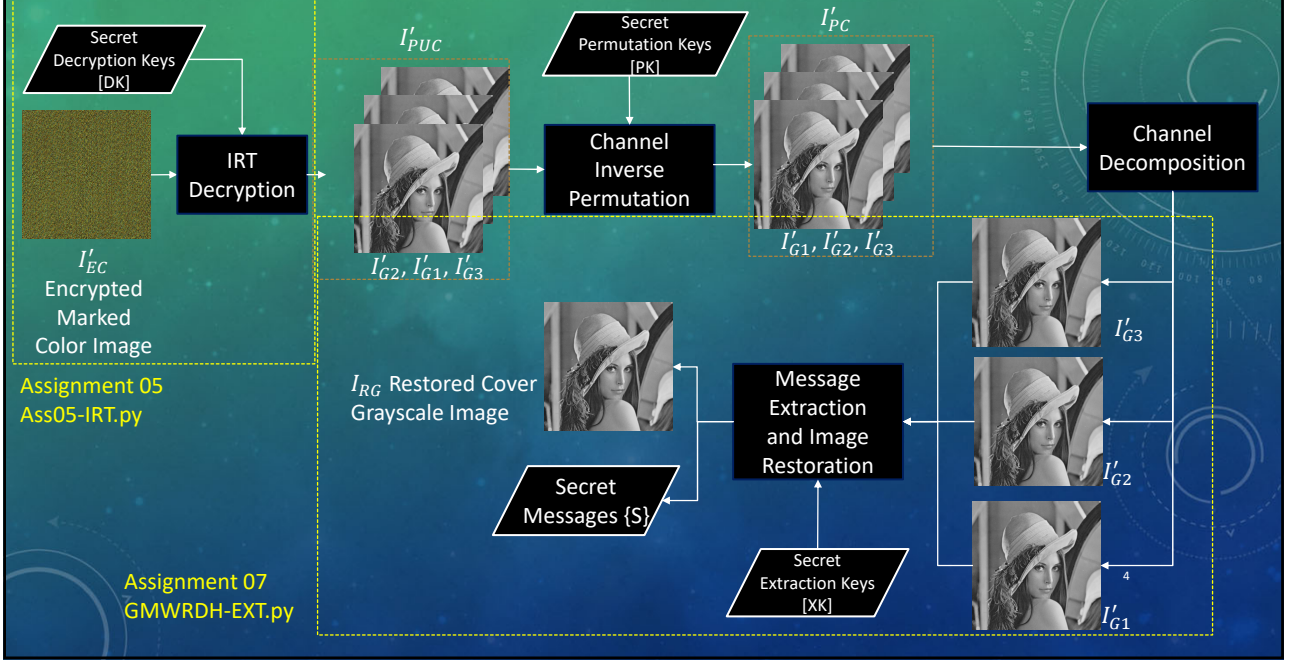
- Input:
  - 1. a grayscale image, I_{GC} ,
  - 2. secret message {S},
  - 3. secret keys, [HK], [PK], and [EK]
- Processes:
  - 1. GMWRDH Embedding: Applying GMWRDH(n, M, Z, I_{GC}) to produce $I'_{G1}, I'_{G2}, I'_{G3}$.
  - 2. Channel Composition: Compositing $I'_{G1}, I'_{G2}, I'_{G3}$ to form I'_{PC}.
  - 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}.



BDIX: BACKWARD DECRYPTION INVERSE-PERMUTATION AND EXTRACTING

- 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}.

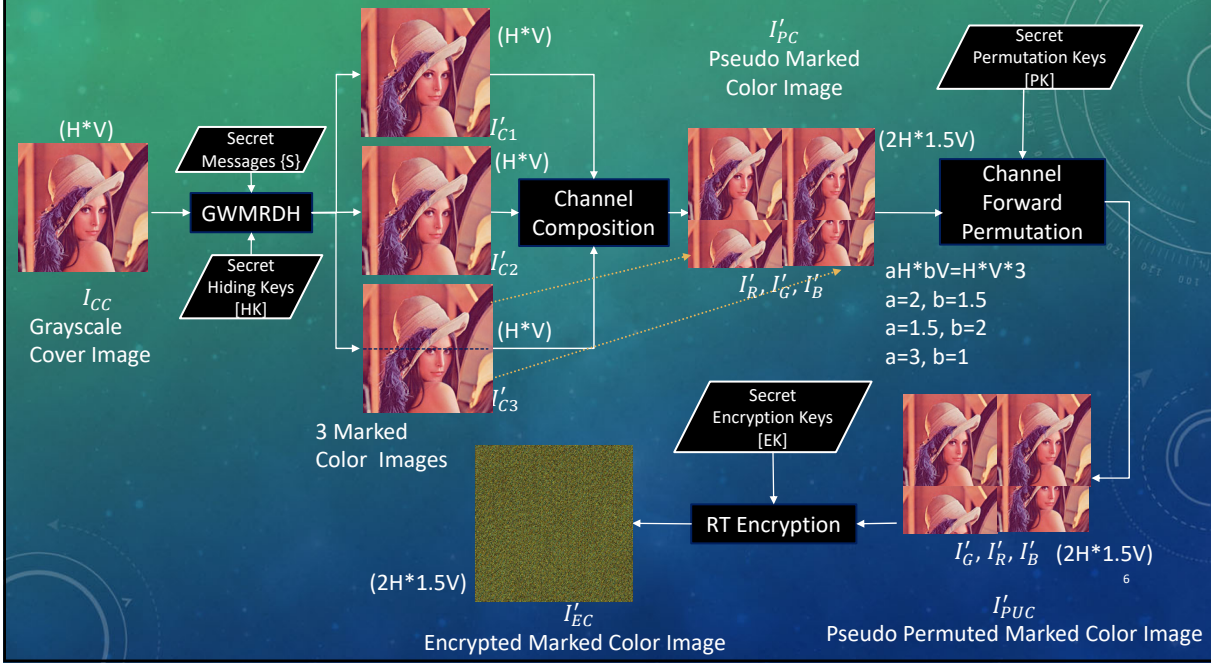
BDIX: Extracting Secret Messages and Restoring Cover Image



FCUE: FORWARD CONCEALMENT PERMUTATION AND ENCRYPTION (COLOR IMAGES)

- Input:
  - 1. a color image, I_{CC} ,
  - 2. secret message {S},
  - 3. secret keys, [HK], [PK], and [EK]
- Processes:
  - 1. GMWRDH Embedding: Applying GMWRDH(n, M, Z, I_{CC}) to produce $I'_{C1}, I'_{C2}, I'_{C3}$.
  - 2. Channel Composition: Compositing $I'_{C1}, I'_{C2}, I'_{C3}$ 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}.

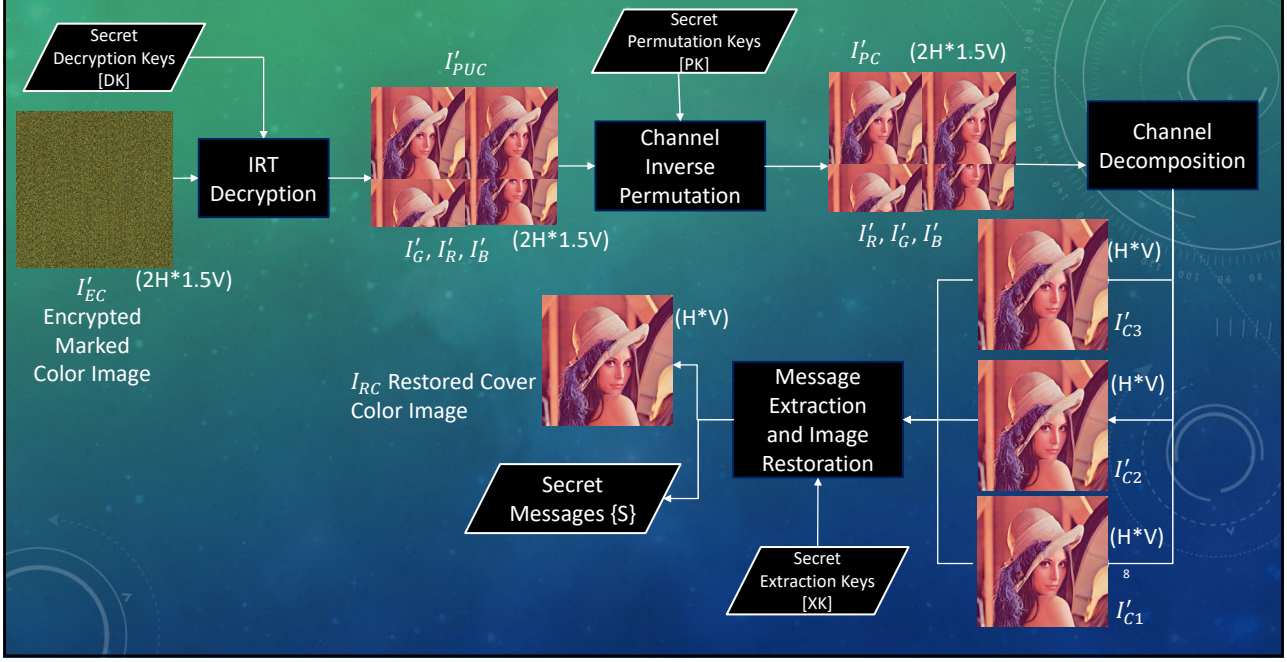
FCUE: Forward Concealment Permutation and Encryption (Color Image)



BDIX: BACKWARD DECRYPTION INVERSE-PERMUTATION AND EXTRACTING (COLOR IMAGE)

- 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 color images $I'_{C1}, I'_{C2}, I'_{C3}$ from I'_{PC}.
  - 4. Message extraction: Extract secret message {S} using [XK] from $I'_{C1}, I'_{C2}, I'_{C3}$.
  - 5. Restoring image: Using $I'_{C1}, I'_{C2}, I'_{C3}$ to produce I_{RC}.
- Output:
  - 1. secret message, {S}.
  - 2. restored image, I_{RC}.

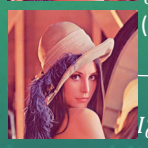
BDIX: Extracting Secret Messages and Restoring Cover Image (Color Image)



Various Resolutions for Channel Composition (Color Image)


(H*V)

I'_{C1}


(H*V)

I'_{C2}

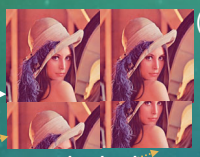

(H*V)

I'_{C3}

3 Marked
Color Images

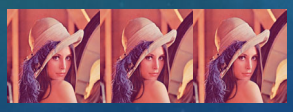
Channel
Composition

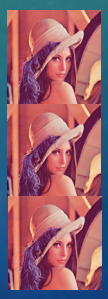
I'_{PC}
Pseudo Marked
Color Image

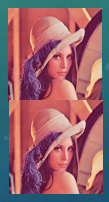

(2H*1.5V)

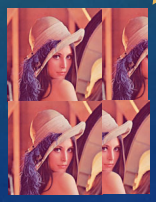
I'_R, I'_G, I'_B

Channel Composition must satisfy: aH*bV=H*V*3
a=2, b=1.5
a=1.5, b=2
a=3, b=1
a=1, b=3
.....


a=3, b=1 →(3H*V)


a=1, b=3 →(H*3V)




a=1.5, b=2 →(1.5H*2V)