

IMAGE ENCRYPTION USING RANDOMIZED ITERATIVE SCRAMBLING & PER-PIXEL SINGLE BIT INVERSION

Flow of Encryption

Pseudo Random Number Matrix Generation

Generation of a 1-D random number array (RN[]) of size equal to the longer dimension of the image with user key as initial seed.

Scrambling Phase

- Iterative
- Iteration involves row-wise and column wise shuffling
- Makes use of the random number matrix

Per-Pixel Single Bit Inversion

Mod 8 of RN[] calculated to decide the pixel position to be inverted

XOR Operation

Image pixels XORed with RN[] in alternating L-R and R-L manner

Flow of Decryption

Pseudo Random Number Matrix Generation

XOR Operation

Per-Pixel Single Bit Inversion

Scrambling Phase

Experimental Validation

Quantitative Evaluation

- Correlation b/w original and encrypted images ranged between $0.0001 - 0.01$
- Horizontal and vertical correlations in encrypted image ranged between $0.0001-0.01$
- NPCR values always $> 99.5\%$
- UACI values in range $30\% - 33\%$
- Entropy consistently >7.9

Other Significant Features

- High Key Sensitivity
- Resistant against cropping attacks
- Produces extremely close results to those desired across **ALL** the standard metrics

Qualitative Evaluation

- A great amount of visual degradation observed across a variety of test cases
- Almost uniform histograms generated after encryption

