Abstract

Image steganography is the process of hiding information (a binary sequence) within an image. This is done by altering the least significant bit (LSB) of each pixel value such that it matches the parity of the bit sequence. Two common techniques are used for embedding information in LSB, LSB Replacement and LSB Matching, with the latter offering improved security as it introduces less changes in the statistical distribution of the bytes and thus less susceptible to structural attacks.

To enhance the reliability of information-hiding techniques, we propose the utilization of Gale-Berlekamp Switch Game to minimize the number of changes to the LSBs. Information is arranged in a matrix of binaries, and each row and column are controlled by a switch that toggles the parity of bits across the corresponding row or column. The aim is to find the combination of toggled switches that result in minimal '1's within the matrix.

In the context of image steganography, matrix representing the information to be hidden is first XORed with LSB matrix of the image, to identify mismatches represented in the form of '1's. Gale-Berlekamp Switch Game is subsequently applied to reduce the number of '1's in the resulting matrix. Optimization is done using Python PuLP package. Overall results show promise, images hidden with optimized information are less detectable than the original counterpart, using the chosen image steganography tool Alethia. However, the high complexity of solving the linear optimization problem, particularly for larger datasets, indicates a trade-off between steganographic security and computational efficiency.