Abstract

Steganography is the art of secretly transferring of data and steganalysis is the art of detecting that hidden data embedded in cover media. In the past years many powerful and robust methods of steganography and steganalysis have been reported in the literature. In this present work, a Steganalysis technique for Histogram-Shifting Based Data Hiding is designed to detect hidden data by using spike generation and template matching. The proposed work analyzes the characteristics of histogram changes during data hiding procedure, and then uses these features to distinguish between stego and original image. The presented work perform the steganalysis in four steps: First, an input image is filtered by using perwitt operator for edge detection. Second, the spike image is divided into 8x8 blocks and then histogram is generated for each block. Third, histogram of each block of stego-image and original image is compared by using 5 similarity measures (norm distance, cosine distance, Euclidean distance, Chi-squared distance, Entropy distance). Fourth, Neural Network (NN) is trained as a classifier to discriminate stego image from original image. Experimental results indicate that the proposed steganalysis method is better than the method proposed by Der-Chyuan Lou et. al. [1] and can effectively detect stego image at low bit rates.
References


**Index Terms**

Computer Science

Artificial Intelligence

**Keywords**

Steganography; Steganalysis; Spikes; Neural Network (NN).