Abstract

Steganography in digital images is a technique to hide secret information in a digital media as an intermediary so as not to look like it should. One method of steganography is Bit Plane Complexity Segmentation (BPCS). BPCS utilize the characteristics of human vision system the human visual do not see the information contained in the noise in the area of an image. The advantages of this method is to have a large insertion ratio compared using Least Significant Bit. Currently BPCS method applied on the document image with a bitmap format at a spatial domain, and not on a compressed image of the document (after embedding secret data, then steganography image is compressed). Compressiom aims to reduce the size of the image data. The problems that arise at this time if lossy compression techniques applied to steganography inserted data will result in loss of information. To overcome this used wavelet-based compression can be used to perform lossy compression and lossles.

In this Final Task will be discussed on steganographic methods Bit-Plane Complexity Segmentation and Compression Embedded Zerotree Wavelet (EZW). EZW aims quantization image while compressing the image. Performance parameters used are Peak Signal to Noise Ratio (PSNR) and compression ratio for image steganography, and Bit Error Rate (BER) for confidential data. Testing is done by analyzing the image quality of the image steganography and steganography extraction result after such an attack given the addition of Gaussian noise and lossless or lossy compression using the EZW.

Results obtained from the implementation using BPCS steganography, data is inserted in the wavelet domain can be compressed using a wavelet-based compression cover image can hold data about 25% of the size of the cover image with a compression ratio of about 20% with a PSNR above 30dB and BER image data 0, the compression ratio can still be increased if the threshold of compression increases.

Keywords: Steganography, BPCS, Compression, Wavelet, PSNR, Ratio, BER.