

ABSTRACT

In this era, technology has grown rapidly especially in telecommunication field to exchange information in form of voice or data. The more technology grow, the smaller private space. That is why steganography, a technique to insert hidden information into a media including voice, video, or data that can send information without being known by anyone else appears. In the other side, steganography has a negative impact in which some people misuse it to send information in purpose of criminality. Based on that reason, steganalysis appears to attack steganography by knowing whether hidden message does exist or not in a media. In this research, the steganalysis is in Domain Discrete Multiwavelet Transform (DMWT) with K-NN classification method on image. From the test result based on DMWT level usage, the accuracy result is 58,75% for level 1 DMWT, 54,58% for level 2 DMWT, 53,16% for level 3 DMWT, 51,58% for level 4 DMWT, 51,24% for level 5 DMWT. While the effect of image size to the image performance accuracy is 49,83% for 128, 60,41% for 256, 56% for 512. The effect of K value used in K-NN to the accuracy is 83,75% for K=1, 82,5% for K=3, 86,25% for K=7, 81,25% for K=9. The effect of sort of K-NN used to the performance accuracy is 78% for Euclidean K-NN, 86% for Cityblock K-NN, 74% for Cosine K-NN, and 96% for Correlation. The effect of image size to performance accuracy is 63,33% for 1KB message insertion, 61,66% for 3KB message insertion, 70% for 5KB message insertion, and 73,33% for full message.

Keyword : Steganalysis, Discrete Multiwavelet Transform (DMWT), K-Nearest Neighbor (K-NN)