ABSTRACT

In developments in this modern era, what is desired can already be sought through various sources of information. There are still many types of information that can be accessed that have a good level of security. To overcome the problems that occur, we need a technique called steganography, where this technique is used to overcome information or secret messages into the data cover. Types of data cover can be video, audio, and also image. With the steganography technique, so that it can happen to restore, one of which is by inserting certain messages on the information used for criminality needs. Therefore, steganalysis is needed where this technique is used to attack steganography in order to find out whether the media in it has a message insertion or not.

This steganalysis research analyzes the Discrete Wavelet Transform (DWT) method and Support Vector Machine (SVM) for the classification process of the staged images from the android Steganography application. Although steganography techniques that use these methods are increasingly developed and widely used by the public to maintain confidentiality, the accuracy parameters are the most considered. So, this research not only detects whether there are hidden text messages or not, but also knows the position of the existence of secret messages with the best accuracy.

The parameters such as Mean, Variance, Standard Deviation, Skewness, Kurtosis, and Entropy used to produce the best level of accuracy and can facilitate analysis. The results of this study indicate that the accuracy level is equal to 95% in the steganalysis system with the number of insertion messages as many as 108 characters and 128x128 images were decomposed with Level-3 DWT on the Gaussian Kernel. For the position and volume detection system which is based on the inserted block id in both the original and the original image obtained an accuracy of 90%.

Keywords: *Steganography, Steganalysis, Discrete Wavelet Transform* (DWT), *Support Vector Machine* (SVM).