ABSTRACT

Steganography is misused by unresponsible people nowadays. This technique is always used to hide crime message (such as terrorist community) and being sent to their teammate to attack another community. Their message probably can make a negative effect not only for their target but also public. For anticipating that problem, we can use a technique for detection secret message called steganalysis.

Steganalysis is a technique used to detect specific file, which is being hidden with secret message or not. This final project use steganalysis in DCT(Discrete Cosine Transform) domain and spatial domain, and file, which is being researched, is RGB image with .jpg format.

The results of this final project are size of the image testing affecst the performance of the system which the details in the image with 100KB capacity has an accuracy of 70.37%, *image with 150KB capacity has an accuracy of* 62.96%, *image with a capacity of 200KB has an accuracy of* 59.26%,, *with a capacity of 300KB image has an accuracy of* 55.55%, *image with 400KB capacity has an accuracy of* 51.85%, and *image with 500KB capacity has an accuracy of* 48.15%. *The larger size of the secret message , the greater the result of accuracy . Details of accuracy are message with a capacity of 1KB has* 54.17%, *of accuracy ,capacity of 2KB has* 56.25%,*of accuracy, and capacity of 3KB has* 69.44%.*of accuracy . The system is able to detect the presence of secret message embedded using steganography applications SilentEye with* 58.33% of *accuracy even if not trained . The system can also detect the presence of secret message embedded using steganography applications Steghide and Jphide with accuracy respectively* 62.50% *and* 66.67%. *From the results of tests performed, the accuracy of the data obtained domain feature extraction based on DCT domain only amounted to* 64.58%, 43.75% *on spatial domain only , and* 66.67% *on DCT and spatial domain.*

Keywords: Steganalysis, Digital Image, DCT (Discrete Cosine Transform), JPEG