ABSTRACT

In general, there are 3 techniques for securing data, that is cryptography, steganography and watermarking. In cryptography, data or information will be secured by encoding the information so that the original meaning cannot be interpreted directly by people. The resulting data can be seen visually by the human eye, but the original meaning is unknown. That's why suspicion will arise for people who see cryptographic results. Steganography technique will secure the original data by hiding data on certain objects so that data cannot be seen visually. Different from cryptography, stored data using steganography techniques will not cause suspicion due to data hiding on other media. The media can be an image, audio or video. Both of these techniques applied to an Android-based application so that they are easy to use. In the application that is applied, the user enters the data or information that he wants to secure. Then the data is given a password which will then be encoded by cryptographic techniques. The cryptographic results are then wrapped in an image so that the data is not suspicious. In this application, the user can also restore the data that was previously secured by entering the password that previously entered on the steganography image. In this research, there are several factors that influence cryptographic and steganographic performance, such as device specifications, image quality, and also the length of messages inserted in the image.

Keywords: Cryptography, Steganography, Android