Abstract

Steganography is the art of hiding messages in another media so that the existence of a message is unknown. Similarity level of the container before and after the message is inserted also become a consideration, because if the difference is clear enough it would arouse suspicion.GIF Format limits the number of the color in 256 colors and is a lossless multimedia file format that is suitable for steganography media. Steganography in GIF image use gifshuffle algorithm.

Another way that can be used to secure message is to use cryptography. Cryptography scramble the message so that the message can not be read except by the recipient. AES is able to process a plaintext into ciphertext with a minimum size. It is suitable to use in steganography that has limited storage space.

This study tested by combining these two ways of securing delivery of message in a single package. Before the message inserted in into the container, the message will be encrypted first. Limitations of storage capacity in GIF encourages compression performed on the message. Huffman is used because it has a compression ratio that is large enough.

From the test results, obtained the conclusion that the AES was able to secure the data well when tested on a variety of other cryptographic algorithm. Gifshuffle capable of storing messages in GIF with a ratio in PSNR above 23 dB. In addition, the limited capacity of the message in the GIF can be enlarged with Huffman compression. Messages that can be stored increased to more than 50% from its original size.

Keywords: Steganography, Gifshuffle, AES, Huffman, PSNR.