Abstract

Exchanging confidential information through a commonly used media such as internet is a risky thing to do. One of the solutions to deal with the problem is steganography, which is the embedding of secret message into digital media such as image, audio, or video so that the exchanged information become unsuspicious. One of the good method which has large capacity is *Bit-Plane* Complexity Segmentation (BPCS). Steganography will be better when we combine it with encryption technique, such as Advance Encryption Standard (AES).

The results shows that the embedding capacity of BPCS Steganography method is large, reaching 47% of the size of the *vessel image*. The quality of *stego image*s are good with PSNR value above 30 dB, although there are some *stego image*s which have PSNR value below 30 dB for using 87-90% of maximum embedding capacity. MOS value of all the tested *stego image*s are above 4,12, indicating good quality. But, this method is not robust to a little change, so that when we add *Gaussian Noise* onto a *stego image*, the decoded message tremendously changes. It provides benefit for message sender and receiver to destroy the evidence. The use of AES encryption reduces the number of the conjugated blocks in the process of BPCS Steganography. Although it requires a little extra time, but the use of AES encryption along with BPCS Steganography will certainly complicate the eavesdroppers to detect and retrieve confidential message.

Keywords: steganography, BPCS, *vessel image*, *stego image*, encryption, AES.