ABSTRACT

The need for information security, particularly for confidential data information, is heightened by the rapid exchange of information. Confidential data can be secured using the steganography technique by inserting the data into a media cover. In this case, media cover is in the form of video. This video becomes a medium for sending a message in real-time, or it can commonly be known as video streaming. However, video streaming has the possibility of packet loss. Video streaming is an identical data transmission medium that uses the User Datagram Protocol (UDP) in transmitting the data. The UDP protocol is connectionless, which means that UDP is a protocol that prioritizes delivery time (speed) and ignores lost packets (packet loss). This study proposes a fault tolerant scheme in steganographic video streaming by using repetition code for ensuring the reception of hidden information in a noisy channel such as packet drop in video streaming. This idea comes from the simplest error correction that can minimize errors in the transmission process of data information with the aim of finding the best fault-tolerant value for video steganography. The method used in this study during video streaming is repetition code with n = odd and multiples of 3. This study describes the embedding and extraction process using the DWT method on the YUV color space especially Y channel. The measurement of packet loss effect is done by using PSNR calculation, in which the higher the PSNR value, the higher the quality of the reconstruction. The use of the DWT method which offers high resolution at low frequencies provides a PSNR value of 131.49dB with the use of the H.265 codec when the packet drop is at a percentage of 15%, as well as message insertion and code repetition in every odd frame (1,3, 5,7,..853).

Keywords: Fault tolerant, Steganography, Repetition code, Packet loss.