ABSTRACT

As the digital world grows, the use of digital media is also increasing. However, the nature of digital media has a weakness in cases of confidential information exchange. The rise of information theft on the internet is very risky to occur, so that the exchange of confidential information must be done carefully. Therefore, better security technology is needed to balance the current development.

In this study, audio steganography was made using the RC4 encrypted SWT-DST method. The signal is decomposed into low and high frequencies by the Stationary Wavelet Transform (SWT) method. So we can use low frequencies to insert secret messages. After that, the signal is transformed from the frequency domain to the time domain using Discrete Sine Transform (DST). The RC4 algorithm is used to encrypt messages so that those who do not have a stego-key cannot extract the contents of the secret message that is in the audio. After encrypting, the message will be inserted into the audio host using the Quantization Index Modulation (QIM) insertion method.

Based on the results of tests that have been carried out by the SWT-DST-RC4 method show that when the optimal parameters without attacks have an average value of SNR = 48.16; ODG = - 0.39; BER = 0. The effect of quantization bit number and frame length also affects the SNR, ODG, and BER values. The average maximum audio capacity is at nframe = 64 and nbit = 6, has a SNR value of 44.89; ODG = 0.11; and BER = 0. The system is only resistant to Noise attacks (5 dB). Messages that use RC4 and without RC4 have different quality parameters. The number of message characters also greatly influences the system's maximum capacity for performance. The more the number of characters, the quality of the system decreases. By using RC4, the system is able to reduce BER so the performance is getting better.

Keywords: Quantization Index Modulation (QIM), RC4, Discrete Sine Transform (DST), Stationary Wavelet Transform (SWT).