ABSTRACT

storing secret files or sending files without being detected when transmitted is a requirement that is now the most sought after and used in sending secret messages that are safe without being able to be known and attacked by attackers and the secret files can only be opened by the recipient. Steganography is a technique in increasing the security of a data, namely by inserting a secret information or message using a media which is usually called a host or carrier or cover. In the audio signal that has been inserted the message must have a quality SNR value above 30 dB, BER below 30%, and CER also below 30% and when given an attack the value is not much different.

In this Final Project a system is designed to send a secret message in the form of text through audio steganography using LSB insertion method where the secret message is encrypted first using Rivest Shamir Adleman (RSA) and using Iteratively Reweighted Least Square (IRLS) reconstruction as an estimation after an CS attack. . In this research, the writer tries to get a Signal to Noise Ratio (SNR) of 40dB or equivalent to excellent signal (5bars), Character Error Rate (CER) of less than 30%, and a Bit Error Rate (BER) of a limit of 30%. We will also test Compressive Sampling (CS) attacks to test the quality of the system whether the message will be very damaged or not..

The result of this final project is an audio steganography system that has good quality before attack with SNR on the first message has an average of 97 dB, on the second message has an average of 92dB, on the third message has an average of 84 dB, and on the fourth message has an average of 83 dB, and a CER value of 0% is also BER 0%. When given an attack in the form of CS the SNR value of each attack and each message is above 40 dB, the CER value is 8% and the BER is 3.94%.

Keywords: *Signal-to-Noise* (SNR), *Iteratively Reweighted Least Square* (IRLS), *Least Significant Bit* (LSB), *character error rate (CER), Bit Error Rate (BER),Rivest Shamir Adleman* (RSA)