ABSTRACT

Problems related to confidentiality in information exchange are crucial in the digital computer era. There are many methods that can be used to solved it. Audio steganography is the one-form of solution that embed the information into digital audio and utilizing the limitations of the human auditory system in perceiving and detecting soundwave. The kind of embedded information is binary image.

The steganography system implements compressive sampling (CS) for the acquisition process and bit compression on the binary image and also adding the encryption algorithm who created by Rivest, Shamir and Adleman (RSA) as a information securing system of the binary image by generating encryption and decryption key pair before the embeddeding process. The embedding method uses statistical mean manipulation (SMM) in wavelet domain and low frequency sub-band by dividing the audio frequency sub-band using discrete wavelete transform (DWT) first. The steganography system performance is optimized by evaluating parameters that cause a high rate of bit error (BER) after an audio being attacked.

The optimal results of simulation by using this system are the signal to noise ratio (SNR) above 45 decibel (dB) and 5.3833 bit per second (bps) of capacity. This system is on average robust to filtering, noise, resampling and compression attacks with the mean value of BER is equal to 0.28, but this system is not robust with attack that perform pitch shifting, time and speed modification in audio signal resulting in mean value of BER is equal to 0.49.

***Keywords**: Audio Steganography, Statistical Mean Manipulation (SMM), Discrete Wavelete Transform (DWT), Compressive Sampling (CS), RSA Encryption.*