ABSTRACT

In this era of digitalization, information security has become a concern due to the widespread use of communication media over the Internet. Some information contained on the Internet can be downloaded for free, and data transmitted over the Internet, such as images, audio, or video, contains a collection of bits that can be further translated into secret messages. Therefore, steganography is used to increase security and reduce misuse, such as modifying information without permission when sending confidential messages.

In this final project, we will implement compression and steganography on a .avi format video host using a data insertion method in the frequency domain called Multibit Spread Spectrum (SS). In this system, Compressive Sampling (CS) is applied to the data compression process, and then bits of information is distributed to the video host and embedded in the video host using the Multibit SS method. With a combination of these methods, CS and the Multibit SS offers the benefits of resource savings, transfers, and smaller data storage capacity, and the benefits of a larger insert data capacity that cannot be upgraded from previous methods.

Results obtained from video steganography systems using compressed .avi format video show that they are resistant to attack. Benchmarking is done by performing attacks in the form of geometric transformations, filtering, format transformations, and noise additions. The simulation implies good results. These results are shown with BER values of 0-7% in noise addition attacks, scaling, and sharpening.

Keywords : *Video Steganography*, *Watermarking*, *Compressive Sampling*, *Spread Spectrum*, *Multibit SS*.