

ABSTRACT

Steganography is a technique in communication system, where information is concealed into a carrier media, such as image, voice and video, without making significant changes to the cover media. Different from steganography which hides information in plain sight, cryptography applications are used to encrypt information so that only the sender and recipient can understand it. Both of these techniques can be combined so that the information can be more difficult to be broken. This system is designed using image steganography with a text file (.txt) as hidden information that was encrypted before using the DES algorithm.

SSIS is using the spread spectrum method, where information that will be embedded into the cover image is spread within noise that has a wide band frequency. This noise is added then to the cover image. To anticipate an error along the transmission process, SSIS uses Error Control Coding (ECC) with a convolutional encoder in the transmitter and decoder using the Viterbi algorithm in the receiver.

From this simulation I (for storage), the imperceptibility level of the stego image is confined by the number of embedded bits in every pixel of the cover image. The image criteria is not determining the imperceptibility level. In simulation II, the maximum capacity is determined by the size of the cover image itself, the code rate of the convolutional encoder and the level of quantization. Image criteria (low detail, medium detail, high detail), the size of the text file, and the number of embedded bits in every pixel of the cover image are the parameters that determine the imperceptibility level of the stego image in simulation II. MOS subjective values with 30 samples show that the received image has high quality (fine category) in a multipath fading+AWGN channel with SNR upper than 22 dB.