Abstract Details

Title: Data Security Management Using Message Encoding and Covert Communication

Authors: Dr. Grima Dhingra, Ms. Sumity

Abstract: Secure data exchange between two parties over the internet is one of the major issues. In this paper approach is used to provide the security to key exchange over internet by implementing all the security methods collectively. The complete procedure is divided in different stages and these all stages are used sequentially to make a true method of data key security. These methods include: key Encoding, key Compression and key Steganography. In first phase the message encoding method is used to generate the 128 bit key which is thus compress in next phase so as to reduce its length. This form is such smaller one that can be used bit by bit in out next phase. The final phase includes the phenomenon of hiding the encoded compressed data in an image through Steganography. To perform this Steganography the task in again divided in sub stages. At first we have to find the areas from the image that have higher density, thus we have to compare each pixel with all its surrounding pixels. As each pixel is in touch of 8 surrounding pixels, we have to find pixels that have maximum no. of different pixel around it. As we get some areas the next work is to find the bit pattern of that pixel. Next work is to replace the LSB (least significant bit) of each such pixel by the bit that we get in term of compressed bit pattern. This process is repeated for all pixels obtained from the compressed key. Finally we get the image with data behind it.

Keywords: Encryption, Compression, Steganography, Least Significant Bit, pixel.