Title:Enhanced data security with cryptography and steganography

Abstract

For many years, people were concerned with the secure transmission of data.The encryption is used to securely communicate data in open networks. As each type of data has its own structures, different techniques should be used to protect confidential data.The existing algorithms used for encryption in cryptography have some flaws such as easily data can be retrieved using ASCII values for numerical representation. The proposed system combines cryptographic algorithm with steganography to protect data or message overnetwork thereby enhancing the data security.

Problem Definition

Today, to transmit confidential information over the network, security is essential. Cryptographic algorithms play an important role to provide the data security against malicious attacks. Many people think that the efficiency of cryptographic algorithm depends only on its time taken for encryption and decryption.However, the efficiency of cryptographic algorithm also depends on number of stages used to obtain cipher text to maintain data secrecy. The algorithms such as Magic Rectangle, Fisher Yet Shuffle algorithm and Genetic algorithm are designed separately to maintain data secrecy. If one continues to use these algorithms individually, data may be lost as security provided by these algorithms can be easily compromised. To overcome the problem, proposed system combines Magic Rectangle, Fisher Yates Shuffle algorithm and Genetic algorithm to enhance the security by increasing complexity of the encryption process.

As sender gives input, the magic rectangle is constructed based on some constraints such as seed value, min start, max start, column sum. To enhance data security, Fisher Yates shuffle algorithm is applied on constructed Magic Rectangle to shuffle the data. The genetic algorithm hides shuffled data into an image generating a complex ciphertext.