Abstract

In this paper, we proposed a model for text encryption using elliptic curve cryptography (ECC) for secure transmission of text and by incorporating the Arithmetic/Huffman data compression technique for effective utilization of channel bandwidth and enhancing the security. In this model, every character of text message is transformed into the elliptic curve points...
Comparative study of Arithmetic and Huffman Compression Techniques for Enhancing Security and Effective Bandwidth Utilization in the Context of ECC for Text

(Xm,Ym), these elliptic curve points are converted into cipher text . The resulting size of cipher text becomes four times of the original text. For minimizing the channel bandwidth requirements, the encrypted text is compressed using the Arithmetic and Huffman compression technique in the following two ways by considering i) x-y co-ordinates of encrypted text and ii) x-co-ordinates of the encrypted text. The results of the above two cases are compared in terms of overall bandwidth required and saved for Arithmetic and Huffman compression.

Reference

- V. Miller, "Uses of elliptic curves in cryptography", Advances in Cryptology--Crypto '85, Lecture Notes in Computer Science, 218
- Fernandes, A. “Elliptic Curve Cryptography”, Dr. Dobb’s journal, December 1999
Comparative study of Arithmetic and Huffman Compression Techniques for Enhancing Security and Effective Bandwidth Utilization in the Context of ECC for Text


Index Terms

Computer Science

Security
Comparative study of Arithmetic and Huffman Compression Techniques for Enhancing Security and Effective Bandwidth Utilization in the Context of ECC for Text

Key words
Elliptic Curve Cryptography (ECC)       Text encryption
Huffman compression
Arithmetic compression