

Use of new efficient lossless data compression method in transmitting encrypted Baptista symmetric chaotic cryptosystem data

Abstract

A new compression algorithm used to ensure a modified Baptista symmetric cryptosystem which is based on a chaotic dynamical system to be applicable is proposed. The Baptista symmetric cryptosystem able to produce various ciphers responding to the same message input. This modified Baptista type cryptosystem suffers from message expansion that goes against the conventional methodology of a symmetric cryptosystem. A new lossless data compression algorithm based on the ideas from the Huffman coding for data transmission is proposed. This new compression mechanism does not face the problem of mapping elements from a domain which is much larger than its range. Our new algorithm circumvent this problem via a pre-defined codeword list. The purposed algorithm has fast encoding and decoding mechanism and proven analytically to be a lossless data compression technique.