Reduction-by-percentage compression technique for reducing sizes of plaintext prior to encryption algorithm

ABSTRACT

Other than security, another major concern in cryptography is efficiency to ensure cryptosystem could be embedded and deployed in various communication devices. Encrypting high numbers of data would consume high computational and storage capacity costs. These issues could affect the efficiency of cryptosystem. One of the approaches to overcome these issues is by integrating data compression technique into cryptosystem. To avoid any encryption and decryption error, lossless compression techniques are deployed in cryptography. The compression techniques are deployed to reduce either the size or number of plaintexts prior to encryption algorithm. Nevertheless, the sizes of the compressed plaintext are still large. To deal with this issue, we proposed a simple technique with ability for reducing the sizes of the compressed plaintext. The inverse of this technique is able to recover the original value of the data without any loss or difference compared to the original data. With smaller sizes, the encryption algorithm would process inputs with smaller sizes, and these could potentially make the encryption algorithm be executed in cheaper computational and storage capacity costs.