Abstract

The paper presents the security and compression of data by Digital Arithmetic coding with AES (Advanced Encryption Standard) algorithm. The basic research is to arithmetically encode the data first and then encrypt it by using AES algorithm then transmits the code. At the receiving end the data is decrypted and decoded to produce the user data. The paper has an advantage of encoding/decoding and compression of data at a time. The input data size is of 128 bits or 256 bits in AES, so the idea is to compress the data before encryption by arithmetic coding. For encoding/decoding use digital arithmetic coding and for encryption/decryption we use AES algorithm. The arithmetic coding is similar to Huffman coding they both achieve their
compression by reducing the average number of bits required to represent the symbol. Arithmetic coding stands out in terms of elegance, effectiveness and versatility, since it is able to work most efficiently in largest number of circumstances and purposes. AES is advanced encryption standard process where deals with substation and permutation of data for proper secure.

References

- Information theory by STEVES RAMEN, 1st edition, springer publications.
- http://www.arturocampos.com/ac_arithmetic.html

Index Terms

Computer Science
Electronic Design And Signal Processing

Keywords
Arithmetic Encoding  Aes Encryption  Aes Decryption  Arithmetic Decoding