Abstract

To send multimedia data over an insecure communicational network with limited bandwidth, we need an organized management for creating and sending information. So far, there have been a few methods proposed from the combination of compression with symmetric encryption, for sending these files. In this paper, using pipeline compression with implementation upon Huffman algorithm, instead of usual compression, is proposed. Moreover, instead of utilizing symmetric encryption algorithms with a low level of security, the public key encryption algorithms are used. The chosen asymmetric encryption algorithm, for implementing some operations on multimedia data, is similar to RSA encryption and uses the $ab \mod m$ expression to generate the key. Moreover, in this paper there has been a circuit proposed with the goal of increasing the speed of the located multiplier in this mathematical expression. Also, considering
the existence of the adder in encryption multiplication circuit, and compression circuit, the use of an special adder is recommended for improving the speed of these parallel multimedia computations.

References


Index Terms
Computer Science
Security

Keywords
Multimedia data multiplication compression asymmetric encryption coding