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

cryptography. The CRC Press series on discrete mathematics and its applications. CRC
- C. Adams and S. Lloyd, Understanding PKI: Concepts, Standards, and Deployment
(Person Education), 2003].
- C. C. Lu and S. Y. Tseng, Integrated Design of AES (Advanced Encryption
Standard) Encrypter and Decrypter, in Proceedings of the IEEE International Conference
- R. Hashemian, Design and Hardware Implementation of a Memory Efficient
Huffman Decoding, in Proceedings of the IEEE Conference on Consumer Electronics,
- G. Engels and S. Sauer, Object-oriented Modeling of Multimedia Applications,
- G. Boato, N. Conci, V. Conotter, F. G. B. De Natale, and C. Fontanari,
Multimedia Asymmetric Watermarking and Encryption, Electronics Letters, Vol. 44,
No. 9, PP. 601-602, April 2008.
- H. D. Lin and D. G. Messerschmitt, Designing a High –Throughput VLC Decoder
PartII-Parallel Decoding Methods, In Proceedings of the IEEE Transactions on Circuits
- H. Park and V. K. Prasanna, Area Efficient VLSI Architectures for Huffman
Coding, in Proceedings of the IEEE Transactions on Circuits and Systems, Analog and
- J. Kim, J. Kim, and C. M. Kyung, A Lossless Embedded Compression Algorithm
for High Definition Video Coding, in Proceedings of the 2009 IEEE International
Conference on Multimedia and Expo, ICME 2009, PP. 193-196, New York City, NY, USA,
2009.
- L. Y. Liu, J. F. Wang, R. J. Wang, and J. Y. Lee, Design and Hardware
Architectures for Dynamic Huffman Coding, IEEE Proceedings, Computers and Digital
- M. Benes, S. M. Nowick, and A. Wolfe, A Fast Asynchronous Huffman Decoder
for Compressed-Code Embedded Processors, in Proceedings of the 4th International
Symposium on Advanced Research in Asynchronous Circuits and Systems (ASYNC ’98),
Encryption of Compressed MultiMedia Data


Index Terms

Computer Science
Security

Keywords
Multimedia data multiplication compression asymmetric encryption coding