Abstract

With the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. Because of widely using images in industrial process, it is important to protect the confidential image data from unauthorized access. This paper presents the design of a 128 bit encoder using AES Rijndael Algorithm for image encryption. The AES algorithm defined by the National Institute of Standard and Technology (NIST) of United States has been widely accepted. Optimized and Synthesizable VHDL code is developed for the implementation of 128-bit data encryption and process.
ISE9.2i software is used for synthesis. Timing simulation is performed to verify the functionality of the designed circuit.

Reference

- M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki “A Modified AES Based Algorithm for Image Encryption” World Academy of Science, Engineering and Technology 27, 2007
- Alireza Hodjat, Student Member, IEE, and Ingrid Verbauwhede, Senior Member, IEEE “Area-Throughput Trade-Offs for Fully Pipelined 30 to 70 Gbits/s AES Processors” IEEE Transactions on Computers, Vol.55, no.4, April 2006
- Pawel Chodowiec and Kris Gaj “Very compact FPGA implementation of the AES Algorithm”, in Proc. Of Cryptographic hardware and embedded system workshop, pp.319-333, 2003

Index Terms

Computer Science Image Processing
Key words

Rijndael
S-box

Advanced Encryption Standard