عنوان مقاله:

Hardware Implementation of ۱۲۸-Bit AES Image Encryption with Low Power Techniques on FPGA to VHDL

محل انتشار:

مجله مهندسی برق مجلسی, دوره 6, شماره 4 (سال: 1391)

تعداد صفحات اصل مقاله: 10

نویسندگان:

Ali Farmani - *University of Tabriz/Department Electrical and Computer Engineering, Tabriz*

Hossein Balazadeh Bahar - *University of Tabriz/Department Electrical and Computer Engineering, Tabriz*

خلاصه مقاله:

This paper describes the implementation of a low power and high-speed encryption algorithm with high throughput for encrypting the image. Therefore, we select a highly secured symmetric key encryption algorithm AES(Advanced Encryption Standard), in order to decrease the power using retiming and glitch and operand isolation techniques in four stages, control unit based on logic gates, optimal design of multiplier blocks in mixcolumn phase and simultaneous production keys and rounds. Such procedure makes AES suitable for fast image encryption. Implementation of a ۱۲۸-bit AES on FPGA of Altera Company has been done, and the results are as follows: throughput, ۶.۵ Gbps in ۴۴۱.۵ MHz and ۱۳۰mw power consumption. The time of encrypting in tested image with ۳۲*۳۲ sizes is ۱.۲۵ms.

کلمات کلیدی:

prof.koze kanani, en, University of Tabriz, dean of department of electrical and computer engineering