Open Science Index, Computer and Information Engineering Vol:8, No:12, 2014 publications.waset.org/abstracts/16549.pdf

On Dynamic Chaotic S-BOX Based Advanced Encryption Standard Algorithm for Image Encryption

Authors : Ajish Sreedharan

Abstract : Security in transmission and storage of digital images has its importance in today’s image communications and confidential video conferencing. Due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access. Advanced Encryption Standard (AES) is a well known block cipher that has several advantages in data encryption. However, it is not suitable for real-time applications. This paper presents modifications to the Advanced Encryption Standard to reflect a high level security and better image encryption. The modifications are done by adjusting the ShiftRow Transformation and using On Dynamic chaotic S-BOX. In AES the Substitute bytes, Shift row and Mix columns by themselves would provide no security because they do not use the key. In Dynamic chaotic S-BOX Based AES the Substitute bytes provide security because the S-Box is constructed from the key. Experimental results verify and prove that the proposed modification to image cryptosystem is highly secure from the cryptographic viewpoint. The results also prove that with a comparison to original AES encryption algorithm the modified algorithm gives better encryption results in terms of security against statistical attacks.

Keywords : advanced encryption standard (AES), on dynamic chaotic S-BOX, image encryption, security analysis, ShiftRow transformation
Conference Title : ICCST 2014 : International Conference on Computer Science and Technology
Conference Location : Penang, Malaysia
Conference Dates : December 04-05, 2014