World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:10, No:09, 2016

Creation of S-Box in Blowfish Using AES

Authors : C. Rekha, G. N. Krishnamurthy

Abstract : This paper attempts to develop a different approach for key scheduling algorithm which uses both Blowfish and AES algorithms. The main drawback of Blowfish algorithm is, it takes more time to create the S-box entries. To overcome this, we are replacing process of S-box creation in blowfish, by using key dependent S-box creation from AES without affecting the basic operation of blowfish. The method proposed in this paper uses good features of blowfish as well as AES and also this paper demonstrates the performance of blowfish and new algorithm by considering different aspects of security namely Encryption Quality, Key Sensitivity, and Correlation of horizontally adjacent pixels in an encrypted image.

Keywords : AES, blowfish, correlation coefficient, encryption quality, key sensitivity, s-box
Conference Title : ICCSIT 2016 : International Conference on Computer Science and Information Technology
Conference Location : San Francisco, United States
Conference Dates : September 26-27, 2016