Abstract

Evolution of information technology has led to creation of tremendous amount of digital data. The major part of the digital data is multimedia data. The multimedia data is often exchanged over internet. So security of this data is very important. Cryptography is one of the ways to ensure security. In recent years much research has taken place to secure digital images. A digital image is a collection of intensity values of the pixels arranged in the form of a two dimensional matrix. It has been observed that the intensity values of the nearby pixels are strongly related. In this paper an image cryptosystem is proposed that encrypts the digital images by first dividing them into blocks, then the pixel values of the blocks are scrambled. Then the scrambled blocks are randomly passed to the AES algorithm. It is hoped that the proposed method decreases the correlation among the nearby pixels and helps to secure the digital images.

References

- Seyed Hossein Kamali, Reza Shakerian, Mayson Hedayati, Morisen Rahmarn, &quot; A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption&quot; International Conference on Electronics & Information Engineering (ICEIE 2010), (VI 141-VI 145), IEEE, 2010

**Index Terms**

Computer Science  
Security

**Keywords**

Advanced Encryption Standard (AES)  
Cryptography  
Image scrambling  
Security analysis  
entropy  
correlation  
image encryption