Abstract

Today sharing of a digital images over network is growing in huge numbers. The security of network is becoming more significant as the quantity of data being exchanged on the internet rises. Apart from this, the data that is relevant for the image is also transmitted with it. Therefore, the privacy and data integrity entails protecting against illegal access and utilization. Thus these actions have resulted in enormous growth of the field of securing the data. Information ciphering is a method which is utilized for hiding data in the digital files likes- audio, images and video etc. This method is also referred to as steganography. Here the data is hidden in the image. The data may be the information about the image.

To calculate and estimate the performance of the proposed algorithm, a set of test were done which were quite successful and promising. These assessments were comprised of histogram analysis, correlation analysis, differential analysis, information entropy. Results of assessments displayed that the new integration method has a promising security features and it is more efficient than AES algorithm alone, without the shifting technique which enables it becoming a
Modified AES Algorithm Integrating IBDP (Image Block Displacement Procedure) for Data Encryption

decent method for ciphering the digital data. The results exhibited that histogram of a ciphered image made a uniform distribution which is quite unique different from the histogram of the plain image and the correlation of pixels of the image was dramatically decreased by utilizing the integration method, thus higher entropy results were achieved.

References

2. E.Kavitha, “FPGA implementation of area optimized AES Algorithm for secure communication applications” (IJARCET), Volume 5, Issue 4, April 2016

Index Terms

Computer Science Security
Keywords

PFAK, Data Encryption, Modified Algorithm PCA, Noise, Block Cipher, NC, Noise.