Abstract

In the present brutal competitive world, security is prime factor to transmit confidential data over the internet. Cryptographic algorithms play very important role in providing the data security against the various attacks. The specific characteristics of image, like high transmission rate with limited bandwidth, correlation among pixels, redundancy and requirement of high storage capacity makes traditional algorithms unsuitable for image encryption. To cross these boundaries for real time applications, design of new algorithms that require less computational power while preserving a sufficient level of security is always a big challenge for researchers. This paper proposes an algorithm based on block based image transformation using perfect shuffle operation followed by new encryption algorithm. In this paper we compare the generated results with available algorithms like AES, RC6 and BFS on the basis of two parameters entropy and correlation.

References

- D. Coppersmith, "The data encryption standard(DES) and its strength against
A Novel Approach for Image Encryption by New M Box Encryption Algorithm using Block based Transformation along with Shuffle Operation

- Qian Li and Yang Wang “The Performance Analysis of Image Encryption Algorithm...
A Novel Approach for Image Encryption by New M Box Encryption Algorithm using Block based Transformation along with Shuffle Operation Based on Chaotic System; published in IEEE International Conference on Electronic & Mechanical Engineering and Information Technology 12-14 August 2011.

- Schneider, T. D, Information theory primer with an appendix on logarithms, National Cancer Institute, 14 April 2007.

**Index Terms**

Computer Science  Security

**Keywords**

Network Security  Image Encryption  Image Entropy  Image Correlation  Confusion And Diffusion