DEVELOPMENT OF A CHOAS BASED IMAGE ENCRYPTION AND DECRYPTION ALGORITHM FOR RGB IMAGES

N.W.K.D.V.P. Opatha

Postgraduate Institute of Science, University of Peradeniya, Peradeniya, Sri Lanka

Image encryption and decryption is an important aspect in secure transmission and storage of digital images. The goal of this research study is to evaluate the differences between various encryption and decryption algorithms which basically fall into three categories as traditional ciphers, chaos based techniques and visual cryptography, and to implement an encryption and decryption algorithm by using the chaos based techniques to encrypt RGB images efficiently. In the recent years, chaos based techniques have been developed to encrypt and decrypt images rather than other algorithms, due to the characteristics of the algorithm itself and the digital images. Prior research studies have highlighted many ways in using chaos, along with keys to encrypt digital images by proposing different steps and procedures. Even though the suitability of chaos based techniques to encrypt and decrypt images are high over traditional ciphers and other related encryption and decryption techniques, still chaos based techniques have problems in managing keys, pixel replacement and scrambling when they were used. At the same time, 60% of the studies have implemented encryption and decryption algorithms which are suitable for gray images.

This research study was conducted as an experimental study and algorithm was implemented by using MATLAB 8.1.0.604. A new technique was introduced in key generation and management which generated a key file in binary format by using random mathematical permutation. Red, Green and Blue panels had separate keys in single key file. To improve the security and efficiency, further a block rotation for different color panels was introduced, rather than scrambling the pixels individually. In considering the results, the algorithm was able to overcome the aforementioned issues in many algorithms. Image histogram, correlation coefficient, noise removal filters, key space and time on encryption and decryption were the validation techniques used. Results of the proposed algorithm demonstrated satisfactory results, when compared with existing algorithms. This study enhanced the knowledge by adding a new methodology to the context of chaos based image encryption and decryption.