

Development of A Chaos Based Image Encryption and Decryption Algorithm for Color Images

N. W. K. D. V. P. Opatha^{1*}

Image encryption and decryption are important in secure transmission and storage of digital images. Image encryption and decryption algorithms are basically categorized into three categories, i.e., traditional ciphers, chaos based techniques and visual cryptography. The goal of this research is to implement an efficient image encryption and decryption algorithm for color (RGB) images, by using chaos based techniques, while analyzing the issues prevailing in the existing chaos based algorithms. In recent years, many chaos based algorithms have been developed, as their suitability in image encryption and decryption is significant. Prior research studies have highlighted the different methodologies in using chaos based techniques, to encrypt and decrypt images, while identifying the issues in them.

The research study was conducted as an experimental study. A new technique was proposed to generate the key, which was based on random mathematical permutation. The proposed key was a combination distinct keys for red, green and blue panels of an image. Pixel intensity values were replaced separately in the three panels, based on the key that was generated. Moreover, block transformation was introduced, to be performed, subsequently after replacing the pixel intensity values. The block transformation had three different patterns for three color panels. Finally, encrypted image was received by combining these three layers. Decryption was the reverse process of the encryption process. The algorithm was tested for its accuracy and its validity. Encrypted images provided a flat histogram, which demonstrated the validity. Application of noise removal filter on the encrypted image, did not provide the plain image. Key space of the proposed method was $8.578177753 * 10^{506}$ for one panel, and the key file was a combination of 3 distinct keys of the given nature, which was larger and complex than the other methods. Average execution time (in seconds) for encryption and decryption are 0.012 and 0.014 respectively, which is lower than the other methods. Correlation coefficient between the plain image and cipher image were lower than the existing techniques, and thus this method demonstrated satisfactory results compared with the existing chaos based image encryption and decryption algorithms.

Keywords: *Image encryption, Image decryption, Chaos, RGB images, Block transformation*

¹ University of Peradeniya, Sri Lanka *v.opatha@gmail.com
