Image Encryption Using Circular-Shifting, Permutation Expansion and XOR

By

Qasem Hasan Yousef Makki

Supervisor

Dr. Ayman Mahmoud Aref Abdalla

Co-supervisor

Dr. Mustafa Mohd Hussien Al Rifaee

Al-Zaytoonah University of Jordan, 2023

Abstract

With the development of technology and its extension on a large scale, and the increase in the number of internet users, in addition to the importance of transferring data, images, video, text, and audio, as well as image protection, it has been essential to protect data in general and images in particular. Many researchers in this field have developed different algorithms for this purpose. Therefore, this thesis presents three new schemes for lossless encryption of Bitmap images (color and grayscale). These schemes apply confusion and diffusion by using Permutation Expansion and circular shift, in addition to creating XOR, BitXOR, and flip operations. Furthermore, the schemes aim at generating keys with high sensitivity and large keyspace. Implementation and analysis of the results using various quality measures demonstrated the efficacy of the proposed schemes. When

the three proposed schemes were applied to benchmark images of different sizes, they were robust and resistant to statistical, differential, and brute force attacks. The entropy values of the encrypted images were close to 8, the correlation values between pixels were close to zero, and the histogram distribution was uniform. In addition, the NPCR and UACI values were close to the standard values, SSIM values were as very low, and MSE and PSNR values were very high.

Keywords: image encryption, permutation expansion, circular shift, XOR.