ABSTRACT

Encryption is the process of digital image using an algorithm to transform the information from being read by an unwanted party. The algorithm developed is popular chaotic algorithms that use randomization method image.

The final task is to discuss the comparative analysis algorithm Rubik's Cube and modified Arnold's Cat Map algorithm on digital image encryption. In a previous study, a comparison Rubik's Cube algorithm with Arnold's Cat Map that lead to the conclusion that the Rubik's Cube is better than Arnold's Cat Map. However, in that study, the Arnold's Cat Map is just a standalone algorithm, which for the decryption process is very easy to do. It just repeats the iterations to get the original image. Therefore, it created a modification of Arnold's Cat Map algorithm with Chaotic Map.

After testing the two of algorithms, it showed that for the computational time, the process of encryption and decryption of modified ACM algorithm is shorter than the Rubik's Cube. For the analysis of histograms test, both have uniformly distributed cipher image but modified ACM algorithm is constant for all tested image. The correlation coefficient of the two algorithms is close to 0 which means that all the pixels have been scrambled with the Rubik's Cube that is categorized as weak correlated, while modified ACM is very weak correlated. The avalanche effect value of the two algorithms are low, Rubik's Cube has 10.9375% and 0.71825% for modified ACM algorithm. Modified ACM algorithm is more resistant to attack noise while Rubik's Cube is better for brute force attack. Based on the performance parameter, in the experiment, the modified ACM algorithm is better than Rubik's Cube algorithm.

Keywords : *Rubik's Cube, Arnold's Cat Map, Chaotic Map*