ABSTRACT

Science is evolving rapidly this recently, thus makes information becomes the most valuable thing. People then try to protect it in many different methods. One of the methods is encrypting the information, so that it would not be able to read by others.

One type of information is digital image, which many information/data are within it. Pixels are highly correlated in digital image, so that not all encryption methods can be applied for digital image due to its optimization in regards of time consumption and security. For these reasons, new encryption methods need to be developed. In this final task Cat Map and Baker Map algorithm is used for encrypting digital image.

Output of this final task is building a system that could encrypt digital image with a high security and optimum time consumption. Based on the experiments applied to 800×800 pixels image, Combined Cat Map-Baker Map needs 12.656 seconds, and Baker Map is the fastest with 0.272 seconds to complete.

This final task also demonstrate on how to break Cat Map, Baker Map, Combined Cat Map-Baker Map, DES and RSA using *brute force attack* algorithm (run using specified PC owned by the author) applied to 128×128 pixels image. For *deciphering* encrypted image generated by Cat Map algorithm, the *brute force attack* algorithm needs 1.499×10^{-5} year. It needs 9.909×10^{21} years for Baker Map algorithm, 1.341×10^{14} years for DES algorithm, 0.569 year for RSA algorithm, and 2.289×10^{26} years for Combined Cat Map-Baker Map algorithm which means that this algorithm provide the best security among them.

Keywords: chaotic-map, Arnold's cat map, baker map, digital image encryption.