Abstract

RC6 is a symmetric block cipher that possesses remarkable features, e.g., simple structure, Feistel structure and supporting for different block size, key length and number of rounds. However, some recent studies show that this cipher is subject to several cryptanalyses such as statistical attack, linear cryptanalysis, correlation attack and brute force attack. This paper proposes an enhancement version dubbed Chaotic Key Based RC6 (CKBRC6) that makes use of the Logistic map to generate round keys. Comprehensive assessments for the security of our proposal and fair comparisons between it and RC6 demonstrate the outperformance of the former in the domain of image encryption.

References


27. strong attacks”.


Index Terms

Computer Science Security

Keywords

RC6, Logistic map, Chaotic encryption key.