Abstract

This paper describes a novel approach for image encryption using stream cipher algorithm based on nonlinear combination generator. This work aims to enhance the security of encrypted image. The work is based on the use of several linear feedback shift registers whose feedback polynomials are primitive and of degrees are all pair wise coprimes combined by resilient function whose resiliency order, algebraic degree and nonlinearity attain Siegenthaler’s, Sarkar and al.’s bounds. This proposed approach is simple and highly efficient. The proposed algorithm was evaluated through a set of tests. In order to have a global idea of the whole performance of system, our tests included visual tests, histogram analysis, key space analysis, Berlekamp-Massey attack, correlation attack and algebraic attack. The results of the experimental tests demonstrate that the proposed system is highly key sensitive, highly resistant to noises and shows a good resistance against brute-force, statistical attacks, Berlekamp-Massey attack, correlation attack and algebraic attack. The system is robust which makes it a potential candidate for image encryption.


- Jolfaei, A. and Mirghadri, A. 2010 A Novel Image Encryption Scheme Using Pixel Shuffler and A5/1; Proceedings of The 2010 International Conference on Artificial Intelligence and Computational Intelligence (AICI10), Sanya, China.
- Carlet, C. 2001 On the cost weight divisibility and non linearity of resilient and correlation immune functions; Proceeding of SETA’01 (Sequences and their applications 2001), Discrete Mathematics, Theoretical Computer Science, Springer p 131-144.

**Index Terms**

Computer Science
Security

**Keywords**

Cryptosystem  Image correlation  Image encryption and decryption  Key stream  Non linear combination generator resilient function

LSFR