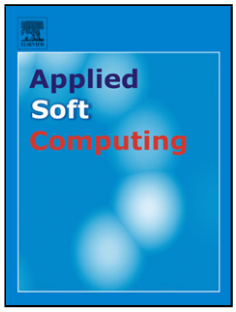

Title: Key Generation for Plain Text in Stream Cipher via Bi-Objective Evolutionary Computing

Authors: Gutha Jaya Krishna, Vadlamani Ravi, S. Nagesh Bhattu

PII: S1568-4946(18)30298-9
DOI: https://doi.org/10.1016/j.asoc.2018.05.025
Reference: ASOC 4891

To appear in: *Applied Soft Computing*

Received date: 3-9-2017
Revised date: 13-4-2018
Accepted date: 15-5-2018

Please cite this article as: Gutha Jaya Krishna, Ravi Vadlamani, S.Nagesh Bhattu, Key Generation for Plain Text in Stream Cipher via Bi-Objective Evolutionary Computing, Applied Soft Computing Journal https://doi.org/10.1016/j.asoc.2018.05.025

Key Generation for Plain Text in Stream Cipher via Bi-Objective Evolutionary Computing

Gutha Jaya Krishna[1,2], Vadlamani Ravi[1*] and S. Nagesh Bhattu[1]

[1]Center of Excellence in Analytics,
Institute for Development and Research in Banking Technology,
Castle Hills, Road No.1, Masab Tank, Hyderabad - 500057, India
padmarav@gmail.com; nageshbhattu@gmail.com

[2]School of Computer and Information Sciences,
University of Hyderabad, Hyderabad-500046, India, krishna.gutha@gmail.com

[*] Corresponding Author; Phone: +914023294042; FAX: +914023535157

Highlights

- We developed a key generation algorithms using NSGA-II in the bi-objective optimization framework and Improved Modified Harmony Search + Differential Evolution (IMHS+DE), Differential Evolution (DE) and Improved Modified Harmony Search (IMHS), in the single objective optimization framework.
- For encoding we employed the Mutated Huffman Tree Coding algorithm.
- We encrypted the encoded key stream as well as the encoded plain text in order to generate the cipher text.
- We then decrypted the cipher text using the encoded key stream followed by the decoding of the deciphered text using the code tables.
- The proposed algorithms are compared with the extant methods.
- Of particular significance is the highest entropy value yielded by the NSGA-II based algorithm, which in turn indicates the strength of the key generated

ABSTRACT

Evolutionary algorithms are widely used to solve a wide variety of continuous, discrete and combinatorial optimization problems. Evolutionary multi-objective optimization problems seek Pareto front in order to negotiate the trade-off amongst various objective functions present in the problem. Much of the literature on cryptography focuses on making the inference problem harder, for securing the content. In this paper, we developed key generation algorithms using Non-Dominated Sorting Genetic Algorithm-II (NSGA-II) in the bi-objective optimization framework and Improved Modified Harmony Search + Differential Evolution (IMHS+DE), Differential Evolution (DE) and Improved Modified Harmony Search (IMHS), in the single objective optimization framework. For encoding the keystream thus generated as well as the plain text we employed the Mutated Huffman Tree Coding algorithm. In the next phase, we encrypted the encoded keystream