Neural Computing and Applications (2023) 35:4051–4071
https://doi.org/10.1007/s00521-022-07899-7

ORIGINAL ARTICLE

Utilizing the roulette wheel based social network search algorithm for substitution box construction and optimization

Kamal Z. Zamli[1,2] · Hussam S. Alhadawi[3,4] · Fakhrud Din[5]

Received: 2 November 2021 / Accepted: 27 September 2022 / Published online: 19 October 2022

Abstract

This paper introduces a new variant of a recent metaheuristic algorithm based on the Social Network Search algorithm (SNS), which is called the Roulette Wheel Social Network Search algorithm (SNS). As the name indicates, the main feature of RWSNS is the fact that the algorithm allows proportionate selection of its search operators (i.e., from imitation, conversation, disputation and innovation) through exploiting the roulette wheel. Additionally, RWSNS also incorporates the Piecewise map as replacement for the pseudo random generator during the population initialisation to ensure high nonlinearity and allow further solution diversification. Finally, unlike its predecessor, RWSNS also permits the systematic manipulation of candidate solutions around the global best agent through the swap operator to boost its search intensification process, as the global best candidate solution is often clustered and always lurking around the current local best. Results based on the construction of 8 × 8 substitution-box demonstrate that the proposed RWSNS exceeds other competing metaheuristic algorithms in two main S-box criteria, namely, the average nonlinearity score and strict avalanche criteria (i.e., SAC offset), whilst maintaining a commendable performance on bits independence criteria, differential approximation probability and linear approximation probability.

Keywords Social network search algorithm · Substitution-box · Optimization

1 Introduction

Many real-world problems in science and engineering can be formulated as optimization problems to ensure good returns on investment from either maximation or minimization perspective. To date, metaheuristic algorithms have often been sought after to address these problems owing to their inherent generality and problem independence. Metaheuristic algorithms often excel when compared with general heuristic or exhaustive search algorithms in terms of efficient computational resource utilisation, as well as obtaining a sufficiently good solution within a reasonable execution time, especially for large scale optimization problems.

Substitution-box (S-box) presents a major milestone in modern cryptographic applications, that is, to provide confusion (i.e., hiding the relationship between ciphertext and the key) and diffusion (i.e., hiding the cipher text with the plain text). S-box is a nonlinear substitution mapping from $S(x) : GF(2^n) \rightarrow GF(2^m)$ via Boolean function formulation $f(x) = (f_1(x), f_2(x), \ldots f_m(x))$. In fact, S-box is

✉ Kamal Z. Zamli
kamalz@ump.edu.my

Hussam S. Alhadawi
hussam.alhadawi@duc.edu.iq

Fakhrud Din
fakhruddin@uom.edu.pk

[1] Faculty of Computing, College of Computing and Applied Sciences, Universiti Malaysia Pahang, 26600 Pekan, Pahang, Malaysia

[2] Faculty of Science and Technology, Universitas Airlangga–C Campus, JI. Dr. H. Soekamo, Mulyorejo, Surabaya 60115, Indonesia

[3] Department of Computer Techniques Engineering, Dijlah University College, Baghdad, Iraq

[4] College of Engineering, University of Warith Al-Anbiyaa, Karbala, Iraq

[5] Department of Computer Science and IT, Faculty of Information Technology, University of Malakand, Chakdara, Khyber Pakhtunkhwa, Pakistan