Neural Computing and Applications (2023) 35:10449–10471
https://doi.org/10.1007/s00521-023-08243-3

ORIGINAL ARTICLE

# Exploring a Q-learning-based chaotic naked mole rat algorithm for S-box construction and optimization

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

Received: 27 June 2021 / Accepted: 6 January 2023 / Published online: 30 January 2023

## Abstract

This paper introduces a new variant of the metaheuristic algorithm based on the naked mole rat (NMR) algorithm, called the Q-learning naked mole rat algorithm (QL-NMR), for substitution box construction and optimization. Unlike most competing works (which typically integrate a single chaotic map into a particular metaheuristic algorithm), QL-NMR assembles five chaotic maps (i.e., Chebyshev, logistic, circle, Singer, and sinusoidal) as part of the algorithm itself. Using a Q-learning table, QL-NMR remembers the historical performance of each chaotic map during the S-box construction process allowing just-in-time adaptive selection based on its current performance. Experimental results for 8 × 8 S-box generation demonstrate that the proposed QL-NMR gives competitive performance against other existing works, particularly in terms of nonlinearity and strict avalanche criteria. To further demonstrate the effectiveness of our proposed work, we have subjected the QL-NMR for image segmentation using multilevel thresholding. The results confirm that QL-NMR gives better performance than its predecessor NMR. Finally, QL-NMR S-box also outperformed NMR S-box in image encryption.

**Keywords** Naked mole rat · Chaotic maps · Substitution-box

## 1 Introduction

Cryptography involves protecting and securing critical data and information being transferred over nonsecure channels so that it could reach the desired destination without leakage. A block cipher is one of the most critical components of cryptography. Based on Shannon's principles of confusion and diffusion [1], block ciphers, e.g., Data Encryption Standard (DES) [2] and Advanced Encryption Standard (AES) [3], have come into existence. Confusion refers to the practice of obscuring the correlation between the ciphertext text and the key making it as complex as possible via substitution. Meanwhile, diffusion relates to the process of disseminating the influence of one plaintext bit on multiple ciphertext bits to obscure its statistical dependencies via permutation.

Substitution-box (S-box) is the only dynamic component of the block ciphers that provides confusion through the nonlinear mapping of inputs and outputs. More precisely, S-box is a nonlinear substitution mapping from $S(x) : GF(2^n) \rightarrow GF(2^m)$ via the Boolean function formulation $f(x) = (f_1(x), f_2(x), \ldots f_m(x))$. The nonlinearity

✉ Kamal Z. Zamli
kamalz@ump.edu.my

Fakhrud Din
fakhruddin@uom.edu.pk

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

[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 Science and IT, Faculty of Information Technology, University of Malakand, Chakdara, Dir Lower, Khyber Pakhtunkhwa, Pakistan

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

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