School of Computing, Engineering, and the Built Environment
Edinburgh Napier University

PHD STUDENT PROJECT

Funding and application details

Funding status: Self-funded students only

Application instructions:
Detailed instructions are available at https://www.napier.ac.uk/research-and-innovation/research-degrees/how-to-apply

Prospective candidates are encouraged to contact the Director of Studies (see details below) to discuss the project and their suitability for it.

Project details

Supervisory Team:
- DIRECTOR OF STUDY: Dr Jawad Ahmad (Email: J.Ahmad@napier.ac.uk)
- 2ND SUPERVISOR: Professor William J. Buchanan

Subject Group: Cyber-security and system engineering

Research Areas: Computer Science - Cyber Security

Project Title: Substitution Boxes for Image Encryption Applications using Choas

Project description:

Substitution Boxes (S-Boxes) are used to substitute message symbols with predefined values to enhance diffusion in cryptographic systems. While a single S-Box technique is effective for colored and grayscale images, it is less suitable for binary images. The high correlation among pixels in binary images leads to correlated substituted symbols, making them predictable even after encryption. Consequently, relying solely on a single S-Box for substitution renders the encryption vulnerable, allowing potential intruders to exploit various attacks on the encrypted image. It has been proved previously that traditional encryption methods applied to highly correlated images are insecure due to their inherent weaknesses.Chaos-based confusion and diffusion can greatly enhance the

robustness and cryptographic security of an image encryption scheme. The purpose of this research is to delve into chaos theory and investigate its practical application in securing S-Boxes and enhancing image encryption methodologies.

References:

Candidate characteristics

Education:

A second class honour degree or equivalent qualification in Computer Science, Electrical Engineering, Electronics Engineering, Computer Engineering or Mathematics.

Subject knowledge:

- Good knowledge of mathematics and programming.

Essential attributes:

- Experience in fundamental mathematics and cryptography.
- Competent in Good level of implementation skills in one or more programming languages, such as MATLAB, Python and C/C++.
- Knowledge of Mathematics and programming.
- Good written and oral communication skills.
- Strong motivation, with evidence of independent research skills relevant to the project.
- Good time management.

Desirable attributes: