# Malware Detection using Deep Learning based Images Analysis

Ipshita Roy Chowdhury and Deepayan Bhowmik

*Division of Computing Science and Mathematics, University of Stirling, Stirling, FK9 4LA, Scotland, United Kingdom.*

***SICSA CONFERENCE 2021: Sustainability and Resilience***

**Abstract**

Malware can compromise a computer system in any form such as Internet worms, viruses, Trojan horses etc. Malware writers always adopt new sophisticated techniques to generate various types of malicious codes which can develop sophisticated anti-detection techniques. Different types of Malware Families have complex, dynamic behaviours and characteristics which can cause a novel and targeted attack in a cyber-system. There are three types of malware depending upon the code structure: Basic, Polymorphic and Metamorphic. Advanced techniques like Camouflage, Packing or code obfuscation are adopted by the malware developers to make the code unreadable and avoid detection. Image and visualization based detection methods are useful to analyze malicious codes. Deep Learning based methods are being widely used to detect malware variants and code visualization. Attention mechanism (CNN and LSTM) and Neural Network based architectures can be effective to detect structural changes of malware and classification from a set of malware images.

*Keywords:* Attention, Camouflage, Deep Learning, Metamorphic, Polymorphic, Packing