



## AI Security and Safety

Guest Editor:

**Prof. Dr. Xianglong Liu**

School of Computer Science and  
Engineering, Beihang University,  
Beijing 100191, China

Deadline for manuscript  
submissions:

**closed (15 March 2024)**

### Message from the Guest Editor

Dear Colleagues,

In this Special Issue, we aim to bring together researchers from the fields of adversarial machine learning, model robustness, model privacy, and explainable AI to discuss recent research and future directions for AI security, in particular, computer vision and pattern recognition. We invite submissions on any aspect of the security in deep learning systems (particularly computer vision and pattern recognition). We welcome research contributions related to, but not limited to, the following topics:

- Adversarial attacks and defenses for deep learning systems;
- Backdoor attacks and mitigations for deep learning models;
- Model stealing for AI applications and systems;
- Understanding the uncertainty and vulnerabilities of DNNs;
- Deepfake techniques on images and videos;
- Robustness of compact models and systems;
- Privacy-preserved deep learning;
- Explainable AI.





an Open Access Journal by MDPI

## Editor-in-Chief

### Prof. Dr. Flavio Canavero

Department of Electronics and  
Telecommunications,  
Politecnico di Torino, 10129  
Torino, Italy

## Message from the Editor-in-Chief

*Electronics* is a multidisciplinary journal designed to appeal to a diverse audience of research scientists, practitioners, and developers in academia and industry. The journal is devoted to fast publication of latest technological breakthroughs, cutting-edge developments, and timely reviews of current and emerging technologies related to the broad field of electronics. Experimental and theoretical results are published as regular peer-reviewed articles or as articles within Special Issues guest-edited by leading experts in selected topics of interest.

## Author Benefits

**Open Access:** free for readers, with article processing charges (APC) paid by authors or their institutions.

**High Visibility:** indexed within Scopus, SCIE (Web of Science), CAPlus / SciFinder, Inspec, and other databases.

**Journal Rank:** JCR - Q2 (*Physics, Applied*) / CiteScore - Q2 (*Control and Systems Engineering*)

## Contact Us

---

Electronics Editorial Office  
MDPI, St. Alban-Anlage 66  
4052 Basel, Switzerland

Tel: +41 61 683 77 34  
[www.mdpi.com](http://www.mdpi.com)

[mdpi.com/journal/electronics](http://mdpi.com/journal/electronics)  
[electronics@mdpi.com](mailto:electronics@mdpi.com)  
[X@electronicsMDPI](https://x.com/electronicsMDPI)