Call for Papers
Themed Series of APSIPA Trans. on Signal and Information Processing on
"Deepfakes, Unrestricted Adversaries, and Synthetic Realities in the Generative AI Era"

Introduction

The rise of generative AI has led to a notable increase in the use of deepfake technology, accompanied by a concerning surge in unrestricted adversarial examples. This trend has posed significant concerns in the signal and information processing community. Initially limited to visual media, deepfakes have evolved to include multimodal elements, seamlessly integrating audio, text, and imagery to create elaborate narratives. This advancement has given rise to synthetic realities where distinguishing between authentic and manipulated content poses an increasingly formidable challenge.

Moreover, the proliferation of deepfakes has coincided with unrestricted adversaries, which exploit inherent vulnerabilities in machine learning models and intensify existing challenges. While much research has concentrated on defending against norm-constrained unimodal attacks, it is crucial to address unrestricted adversaries, which pose significant risks to the reliability and safety of AI systems across various domains. Expanding research efforts to encompass uni- and multi-modal adversaries is vital for developing robust defenses and ensuring the integrity of AI-driven technologies in real-world applications.

This themed series addresses the two sides of the coin - generation and defense against deepfakes, unrestricted adversaries, and synthetic realities. We welcome researchers and innovators to contribute their original work and help shape the future of information forensics in the generative AI era. Submissions are invited to explore a broad spectrum of topics, including but not limited to the following.

Topics of Interest:

- Uni- or multi-modal deepfake generation and detection
- Deepfake attribution and source identification techniques
- Explainable AI methods for understanding and interpreting deepfake models
- Ethical and societal implications of deepfake technologies
- Applications of deepfakes in creative industries (e.g., film, advertising, entertainment)
- Generation and detection of uni- or multi-modal unrestricted adversaries
- Theoretical analysis of unrestricted adversaries
- Transferability of unrestricted adversaries across different models and domains
- Realistic threat models and defenses
- Benchmarking and evaluation methodologies and datasets
- Human perception and cognitive aspects

Each paper submitted to this series will be reviewed using the first-come-first-serve principle. The target of the first round of decision-making is 5 weeks, and the period of the first round of revision is 2 weeks. The paper will be accepted between 8-12 weeks (depending on 1 or 2 revisions). Once the submission window has closed, accepted papers ready for publication will be published online. The series will be accompanied by an editorial written by the guest editorial team. If a paper cannot be accepted within the publication window, it will be considered as a regular paper.

If you are interested in paper submission, please refer to:
https://nowpublishers.com/Journal/AuthorInstructions/SIP

If you have any questions, please contact Dr. Isao Echizen (iechizen@nii.ac.jp) and Dr. Minoru Kuribayashi (kminoru@tohoku.ac.jp).

Submission Window: August 1 to October 31, 2024
Publication Window: January 2025

Guest Editorial Team

- Isao Echizen (Co-lead), National Institute of Informatics, Japan
- Minoru Kuribayashi (Co-lead), Tohoku University, Japan
- Yuhong Liu, Santa Clara University, USA
- Huy H. Nguyen, National Institute of Informatics, Japan