

## MULTIMEDIA SECURITY, PRIVACY AND ANONYMITY, COPYRIGHT PROTECTION OF DEEP MODELS

**Supervisor Name:** Prof. Dr. Fernando Pérez González

**Email:** fperez@gts.uvigo.es

**Research Group:** Signal Processing in Communications Group

The Signal Processing in Communications Group (GPSC) is specializing in the theoretical foundations and practical applications of statistical signal processing. Our core expertise lies in developing mathematical models and algorithms to solve complex problems in two main areas: digital communications - including satellite systems and 5G/6G - and multimedia security. The group's activity is characterized by a balance between fundamental research and technology transfer, supported by a portfolio of over €9 million in competitive funding.

Within the scientific community, GPSC is internationally recognized for its contributions to multimedia security, having authored foundational works that bridge information theory and data security. For a postdoc, GPSC offers a high-performance environment with a proven track record of high-impact journal publications and a global network of collaborators. We are currently shifting the boundaries of digital trust by applying our expertise in detection and estimation to Privacy-Enhancing Technologies (PETs) and the IP protection of machine learning models, ensuring that signal processing remains at the heart of secure and private data computation.

**Keywords:** Multimedia Forensics | Watermarking | Privacy-enhancing technologies | Homomorphic signal processing

### Research Focus:

Research in this area focuses on the security, privacy, and forensic analysis of digital information by combining information theory with statistical signal processing to ensure the integrity and traceability of data in adversarial environments. A primary pillar involves Multimedia Forensics and Security, addressing both passive and active protection through source identification via sensor noise (PRNU), deepfake detection, and the design of watermarking schemes developed to remain detectable even after sophisticated AI-driven manipulations and generative editing. Parallel to this, the group advances Privacy-Enhancing Technologies (PETs), with a focus on Signal Processing with Encrypted Data to execute complex operations (such as biometric matching) while maintaining data confidentiality.

A core and expanding component of our work is Federated Learning, where we are highly active in developing frameworks that ensure both privacy-preserving computation and the Copyright Protection of Deep Models. This involves pioneering "model watermarking" and fingerprinting techniques that embed cryptographic signatures into neural network parameters, enabling the tracking of unauthorized redistribution and the verification of model ownership even in decentralized training environments. These integrated lines of inquiry provide a rigorous framework for postdocs to address the critical challenges of intellectual property and privacy in modern AI-driven ecosystems.