Post-doc position

Content-based document signature for IoT security

The L3i laboratory has one open post-doc position in computer science, in the specific field of document image analysis and pattern recognition.

Duration: 12 months
Position available from: April or May 2019
Salary: approximately 2100 €/ month (net)
Place: L3i lab, University of La Rochelle, France
Specialty: Computer Science/ Image Processing/ Document Analysis/ Pattern Recognition
Contact: Mickaël Coustaty (mickael.coustaty [at] univ-lr.fr) and Petra Gomez-Krämer (petra.gomez [at] univ-lr.fr)

Position Description

The L3i is a research lab of the University of La Rochelle. La Rochelle is a city in the south west of France on the Atlantic coast and is one of the most attractive and dynamic cities in France. The L3i works since several years on fraud detection in documents and document security and has become a worldwide reference in this domain.

The work done by the post-doc will take part in the context of the SPIRIT (European funding by the CHIST-ERA program) and SVP-IoT (funding of the Region Nouvelle Aquitaine) projects. As the adoption of digital technologies expands, it becomes vital to build trust and confidence in the integrity of such technology. The SPIRIT and SVP-IoT projects will investigate the proof of concept of employing novel secure and privacy-ensuring techniques in services set-up in the Internet of Things (IoT) environment, aiming to increase the trust of users in IoT-based systems. The proposed system will address distinct issues related to security and privacy, hence, overcoming the lack of user confidence, which inhibits utilization of IoT technology.

The work of the L3i within those projects is to develop a technology based on creating a content-based signature of user data/ documents, in order to ensure the integrity of sent data upon arrival. This technology has also been developed at the University of La Rochelle [1, 2, 3] but has not yet been employed in the IoT domain. The projects aim to build upon the highly significant results produced by the partners and to research the challenges of how these technologies can be adapted for IoT environment.

More specifically, the work done by the post-doc will consist in two main objectives: (1) extracting content from IoT device data by analyzing the input IoT device data in order to prepare the data for analysis and semantics extraction; (2) computing a unique content-based signature to allow authenticating an IoT data object independently of its physical representation.

Hence, this work will consist of two parts: data/ document analysis and signature computation. In the first part, an IoT data object will be analyzed in order to obtain a robust description of the object, which is independent of the acquisition mode and source. The different components of the document and their spatial relationships (for images this would be printed text, tables, graphics, stamps, handwritten signature…) will be extracted. The aim is to obtain a stable decomposition and reliable content extraction, which conforms to the requirements of the subsequent security-assuring tasks.

The signature computation method, which is the second part, combines cryptographic hash algorithms and perceptual hash algorithms. The cryptographic signature is based on the robust description of the IoT data object. This allows authenticating any object even if it has been subjected to minor modifications as long as these modifications do not change any part of the semantic content.

Qualifications

Candidates must have a completed PhD and research experience in image processing and analysis or pattern recognition.

General Qualifications

- Good programming skills mastering at least one programming language like Java, Python, C/C++
- Good teamwork skills
- Good writing skills and proficiency in written and spoken English or French

Applications

Candidates should send a CV and a motivation letter to **mickael.coustaty [at] univ-lr.fr** and **petra.gomez [at] univ-lr.fr**.

References

[1] S. Eskenazi, B. Bodin, P. Gomez-Krämer, and J.-M. Ogier. A perceptual image hashing algorithm for hybrid document security. In *International Conference on Document Analysis and Recognition (ICDAR)*, pages 741-746, 2017.

[2] S. Eskenazi, P. Gomez-Krämer, and J.-M. Ogier. The Delaunay document layout descriptor. In *ACM International Symposium on Document Engineering (DocEng)*, pages 167-175, 2015.

[3] S. Eskenazi, P. Gomez-Krämer, and J.-M. Ogier. When document security brings new challenges to document analysis. In *International Workshop on Computational Forensics (IWCF)*, Lecture Notes in Computer Science (LNCS 8915), pages 104-116. Springer, 2015.