

Annnonce de sujet de thèse 2025-2028

Inférence et explicabilité en mode confidentiel : vers l'autodiagnostic via l'image

Mots-clés :

Cryptographie appliquée, Apprentissage automatique, Vision par Ordinateur, Apprentissage profond, Préservation de la vie privée, Explicabilité.

Description du sujet :

Ce sujet de thèse vise à aborder conjointement la confidentialité et l'explicabilité d'une décision obtenue par analyse d'image au moyen d'un réseau de neurones. Dans un contexte de classification effectuée à partir d'un serveur distant, l'objectif est de développer des approches permettant de préserver la confidentialité de l'image en entrée, celle (le cas échéant) de la prédiction mais aussi celle de son explication. Protéger le caractère privé des données [1] tout en assurant la transparence du modèle [2] constitue un enjeu crucial, notamment dans des domaines tels que la santé. L'objectif est aligné avec le cadre réglementaire qui se met en place en matière d'IA à l'échelle européenne (AI Act). Si ces questions font séparément l'objet d'importants travaux en cryptographie et en apprentissage automatique, l'explicabilité sous contrainte de confidentialité s'inscrit comme une nouvelle problématique [3].

Le projet cherchera à identifier des méthodes d'explicabilité locale tirant partie d'informations ou de concepts visuels pouvant être adaptées à un mode confidentiel. La confidentialité pourra être abordée sous l'angle du calcul multipartite sécurisé [4] et/ou de chiffrement homomorphe [5]. Grâce à une collaboration avec le CHU de Saint-Etienne, il sera possible d'ajuster le système d'IA sécurisé et de procéder à une expérimentation supervisée sur des données de santé, en direction d'un autodiagnostic. L'expérimentation pourra être étendue aux dimensions éthique et juridique dans le cadre d'un partenariat Auvergne - Rhône-Alpes - Canada sur l'Intelligence Artificielle.

Références :

- [1] Akram, A., Zimmer, P., Gritti, C., Karame, G., & Önen, M. (2025). Fundamentals of privacy-preserving and secure machine learning. In *Trustworthy AI in Medical Imaging* (pp. 385-409). Academic Press.
- [2] Patrício, C., Neves, J. C., & Teixeira, L. F. (2023). Explainable deep learning methods in medical image classification: A survey. *ACM Computing Surveys*, 56(4), 1-41.
- [3] Nguyen, Thanh Tam, et al. Privacy-preserving explainable AI: a survey. *Science China Information Sciences* 68.1 (2025): 111101.
- [4] Li, Yong, et al. Privacy-preserving federated learning framework based on chained secure multiparty computing. *IEEE Internet of Things Journal* 8.8 (2020): 6178-6186.
- [5] Pulido-Gaytan, B., & Tchernykh, A. (2024). Self-learning activation functions to increase accuracy of privacy-preserving Convolutional Neural Networks with homomorphic encryption. *Plos one*, 19(7), e0306420.

Résultats attendus :

- Identification de méthodes d'explicabilité locale pour la classification d'images pouvant être réalisées en mode confidentiel
- Définition d'un ou plusieurs cadres de mise en œuvre de méthodes de classification explicables.
- Proposition et implémentation de méthodes d'explicabilité confidentielle issues du/des cadres proposés.
- Expérimentations sur une tâche en santé et positionnement par rapport aux dimensions éthiques et juridiques en IA.

Localisation de la thèse :

[Laboratoire Hubert Curien](#) (LabHC), Université Jean Monnet - Saint-Etienne
(réunions régulières au [Laboratoire CITI](#) de l'INSA de Lyon)

Début de la thèse : 1^{er} octobre 2025

Environnement de la thèse :

Thèse s'inscrivant au sein d'un bouquet de thèses autour des *Data et IA dans une démarche durable et responsable*, se déroulant au sein du Collège d'Ingénierie Lyon - Saint-Etienne et de l'Université Jean Monnet.

Support de financement :

Contrat Ecole Doctorale Sciences Ingénierie Santé (ED 488) d'une durée de 3 ans.

Profil attendu :

Candidat titulaire d'un diplôme d'Ecole d'Ingénieurs ou de Master 2 d'Université en mathématiques appliquées ou en informatique, ayant reçu une formation en cryptographie et/ou en apprentissage automatique, maîtrisant un langage de programmation ainsi qu'une ou plusieurs librairies de développement de référence dans l'un de ces domaines.

Processus de candidature :

- **27/05/2025** : Date limite des candidatures (entretiens au fil de l'eau avec les candidats présélectionnés) ;
- **28/05/2025** : Remise de la liste classée définitive au Collège Ingénierie Lyon-Saint-Etienne - Université Jean Monnet.
- **13/06/2025** : Décision finale sur les candidats sélectionnés par le Collège Ingénierie Lyon-Saint-Etienne - Université Jean Monnet.

Suite au processus de sélection et sans délai, un contrat de doctorat de 3 ans sera établi par l'École Doctorale Sciences, Ingénierie, Santé, ED 488.

Contact : Thierry Fournel (LabHC), Clémentine Gritti (CITI, Inria) et Amaury Habrard (LabHC, Inria)
fournel@univ-st-etienne.fr, clementine.gritti@insa-lyon.fr, amaury.habrard@univ-st-etienne.fr

Envoyer CV, lettre de motivation, relevés de notes de M1&M2 et coordonnées de référents.

Bouquet de thèses 2025

Le sujet de thèse de doctorat décrit ci-après s'inscrit au sein d'un bouquet de thèses dont le but est de construire une approche scientifique pluridisciplinaire pour aborder l'enjeu sociétal « Société numérique responsable » et plus précisément, la thématique spécifique « Data et IA dans une démarche durable et responsable », identifiée comme un enjeu prioritaire par les 4 établissements du Collège d'Ingénierie Lyon Saint-Etienne (Centrale Lyon, ENTPE, INSA Lyon, Mines Saint-Étienne) et par l'Université Jean Monnet Saint-Étienne, qui soutiennent financièrement les thèses formant ce bouquet 2025.

Le bouquet de thèses 2025 regroupe 6 thèses qui couvrent différentes facettes de la science des données et de l'intelligence artificielle en abordant les questions suivantes :

- Monitoring des procédés de cristallisation par émission acoustique assistée par IA
- Conception assistée par IA de biopolymères biodégradables et/ou biosourcés pour la protection durable des cultures agricoles
- Méthodes d'apprentissage automatique pour la prédiction du microclimat urbain
- Identification non-linéaire de structures pilotée par des données
- Inférence et explicabilité en mode confidentiel : vers l'autodiagnostic via l'image
- Vers une certification de la surveillance vibratoire par IA explicative

Ces thèses rassemblent au total 16 encadrants rattachés à 11 laboratoires du site Lyon Saint-Etienne (Centre d'Innovation en Télécommunications et Intégration, Centre SPIN – Génie des Procédés, Ingénierie des Matériaux Polymères, Biologie Fonctionnelle, Insectes et Interactions, Institut Camille Jordan, Laboratoire de Mécanique des Fluides et d'Acoustique, Laboratoire de Tribologie et Dynamique des Systèmes, Laboratoire d'InfoRmatique en Image et Systèmes d'information, Laboratoire Hubert Curien, Laboratoire Vibrations Acoustique, Matériaux : Ingénierie & Science) dont les 5 établissements financeurs sont tutelles. Les 6 doctorants recrutés au titre de ce bouquet seront inscrits dans 3 Écoles Doctorales du site : MEGA, EDML, SIS.

Les équipes (doctorants et leurs encadrants) impliquées dans ces 6 thèses forment une communauté scientifique pluridisciplinaire : des échanges réguliers entre ces équipes se dérouleront tout au long des 3 années du parcours doctoral, notamment sous la forme de séminaires communs permettant de développer l'approche systémique pluridisciplinaire propre au bouquet et d'enrichir les compétences disciplinaires des équipes dans un esprit de partage et d'apprentissage. Les mémoires de thèses produits à l'issue du parcours doctoral reflèteront également le positionnement original des travaux de thèse au sein d'un bouquet en incluant un chapitre qui développera l'analyse de l'impact des travaux réalisés sur l'enjeu « Data et IA dans une démarche durable et responsable ».