Filière Métiers de la Recherche

IA confidentielle

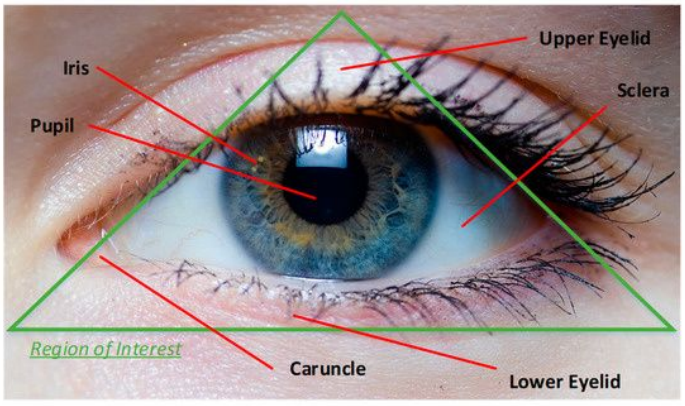
Fabien Imbault

- Contexte de l'étude

L'intelligence artificielle permet de répondre à de nouveaux cas d'usages. Néanmoins, la question de la confidentialité des données personnelles ou de la protection des données sensibles reste une problématique ouverte. On s'intéressera notamment à une technique appelée **confidentialité différentielle**.

- Objectif

L'objectif est de tester de nouvelles méthodes intégrant dès leur conception les enjeux de confidentialité. On prendra le cas de l'identification des personnes par des données biométriques (popularisés par apple faceID/touchID par exemple). On souhaite notamment garantir qu'en cas d'attaque informatique, un potentiel attaquant ne puisse pas récupérer les données individuelles.



Exemple de donnée biométrique qu'on souhaite protéger

- Déroulement

a) Analyse de l'état de l'art (bibliographie critique)
b) Focalisation sur une technique (differential privacy) et une problématique spécifique: la reconnaissance faciale (pour avoir un cas où de nombreuses données existent). Si le temps le permet on pourra tester avec ou sans des masques (problématique actuelle avec le covid)

- Outils et méthodes

Programmation: python
Framework:
https://github.com/opendifferentialprivacy/
https://projects.iq.harvard.edu/files/opendp/files/opendp_programming_framework_11may2020_1_01.pdf
L'avantage de cette méthode est de ne pas nécessiter de matériel spécifique (ex: intel SGX) ou d'algorithme cryptographique complexe (ex: crypto homomorphique). Par conséquent l'étude en sera facilitée.

- Livrables attendus

a) Rédiger un projet d'article scientifique (en anglais), accompagné du projet logiciel (sur github: code et documentation) visant à tester la (ou les) méthode(s) évaluées sur des données simulées ou réelles.
b) Présentation d'un poster.

- Références bibliographiques

En lien direct avec le cas d'usage:

- Chamikara et al., *Privacy Preserving Face Recognition Utilizing Differential Privacy*, 2020 (v2), https://arxiv.org/abs/2005.10486

Articles scientifiques:

- Cammarota et al., *Trustworthy AI Inference Systems: An Industry Research View*, 2020 (v1), Retrieved from https://arxiv.org/abs/2008.04449
- Chamikara et al., *PPaaS: Privacy Preservation as a Service*, 2020(v1), https://arxiv.org/pdf/2007.02013.pdf
- Kaissis et al., *Secure, privacy-preserving and federated machine learning in medical imaging*, Nature Machine Intelligence (2), p.305–311, 2020, Retrieved from https://www.nature.com/articles/s42256-020-0186-1
- Rocher et al*., Estimating the success of re-identifications in incomplete datasets using generative models*, Nature Communications, (10):3069, 2019, https://www.nature.com/articles/s41467-019-10933-3
- Salem et al., *Utilizing Transfer Learning and Homomorphic Encryption in a Privacy Preserving and Secure Biometric Recognition System*, Computers, 8(1):3, 2019, https://www.mdpi.com/2073-431X/8/1/3/htm
- Wood et al., *Differential Privacy: A Primer for a Non-Technical Audience*, Vanderbilt Journal of Entertainment & Technology Law 21 (1):209. 2018, Retrieved from https://dash.harvard.edu/handle/1/38323292

Projets:
Pour donner quelques exemples de projets visant à répondre aux enjeux de confidentialité:

- aggrégation de statistiques sur les navigateurs https://crypto.stanford.edu/prio/
- calcul sur des données médicales encryptées (par ex https://rise.cs.berkeley.edu/projects/opaque/)