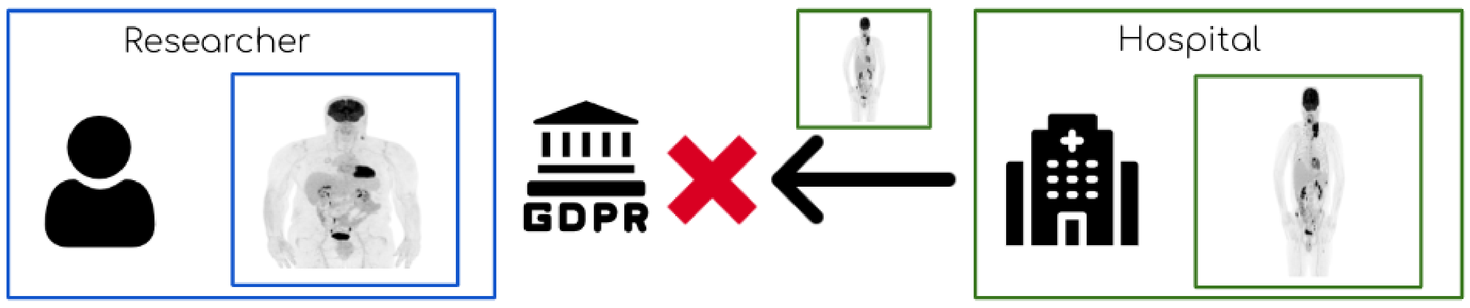
PRIVACY PRESERVING IMAGE REGISTRATION

RICCARDO TAIELLO, MELEK ÖNEN, OLIVIER HUMBERT AND MARCO LORENZI
Epione Research Project, Inria Sophia Antipolis, France - EURECOM, Sophia Antipolis, France - Université Côte d'Azur, Nice, France
GitHub
riccardo.taiello@inria.fr

1.INTRODUCTION

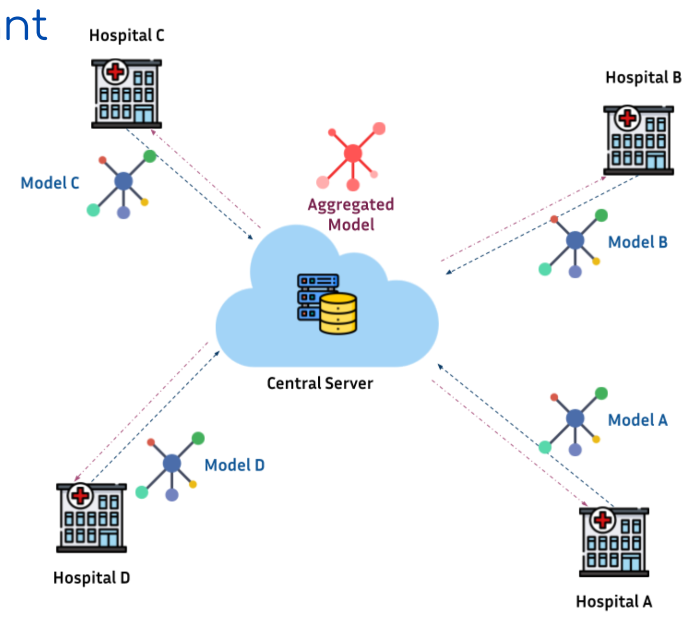
Image registration (IR) is the workhorse of many real-life medical imaging software and applications:

- Public web-based services for medical images segmentation [1];
- Federated Learning (FL) [2] where medical images can be jointly analyzed in multi-centric scenarios.



PROBLEM

Medical imaging information falls within the realm of personal health data and its sensitive nature, these applications of image registration are no longer compliant with regulations currently existing in many countries, such as the GDPR [3], or HIPAA [4].

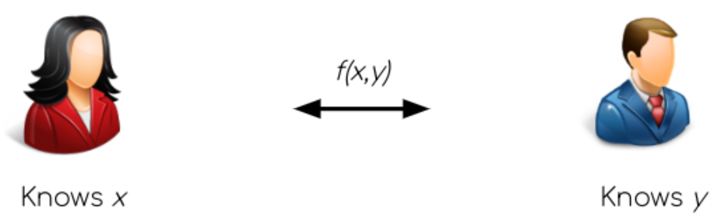


CONTRIBUTION

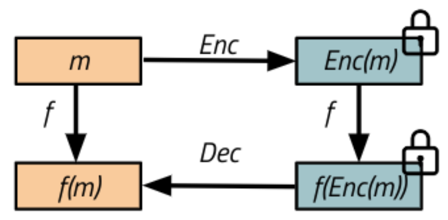
We formulate the problem of IR under a privacy preserving regime, where images are assumed to be confidential and cannot be disclosed in clear.

PRIVACY PRESERVING TOOLS

Multi Party Computation (MPC)



Fully Homomorphic Encryption (FHE)



2.BACKGROUND

We consider a scenario with two parties, $party_1$, and $party_2$, whereby $party_1$ owns image I and $party_2$ owns image J .
The cost function to optimize the registration problem is the sum of squared intensity differences (SSD):

$$\mathrm{SSD}\left(I, J, \mathbf{p}\right) = \arg\min_{\mathbf{p}} \sum_{\mathbf{x}} \left[I\left(W_{\mathbf{p}}\left(\mathbf{x}\right)\right) - J\left(\mathbf{x}\right) \right]^2$$

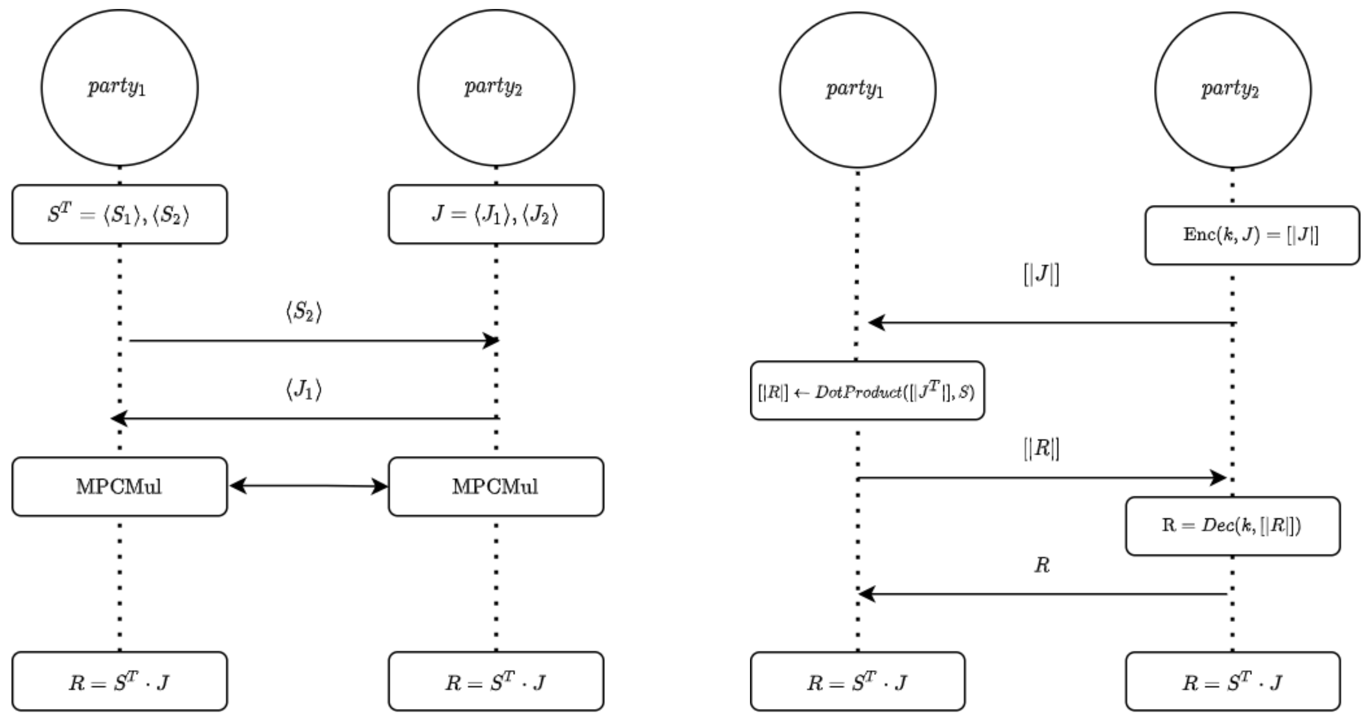
Under Gauss-Netwon optimization scheme, the parameters of the spatial transformation can be computed as:

$$\Delta\mathbf{p} = \underbrace{H^{-1}}_{party_1} \cdot \sum_{\mathbf{x}} \underbrace{S\left(\mathbf{x}\right)}_{party_1} \cdot \left(\underbrace{I\left(\mathbf{W}_{\mathbf{p}}\left(\mathbf{x}\right)\right)}_{party_1} - \underbrace{J\left(\mathbf{x}\right)}_{party_2} \right)$$

To compute the registration update the only operation requiring the joint availability of information from both parties is the term $R = \sum_{\mathbf{x}} \underbrace{S\left(\mathbf{x}\right)}_{party_1} \cdot \underbrace{J\left(\mathbf{x}\right)}_{party_2}$, in vectorized form $R = \underbrace{S^T}_{party_1} \cdot \underbrace{J}_{party_2}$

3.PRIVACY PRESERVING IMAGE REGISTRATION (PPIR)

MPC FHE



Scalability of privacy preserving tools is achieved using gradient approximations, i.e. Uniformly Random Selection (URS) [5] and Gradient Magnitude Selection (GMS) [6].

4.EXPERIMENTAL RESULTS

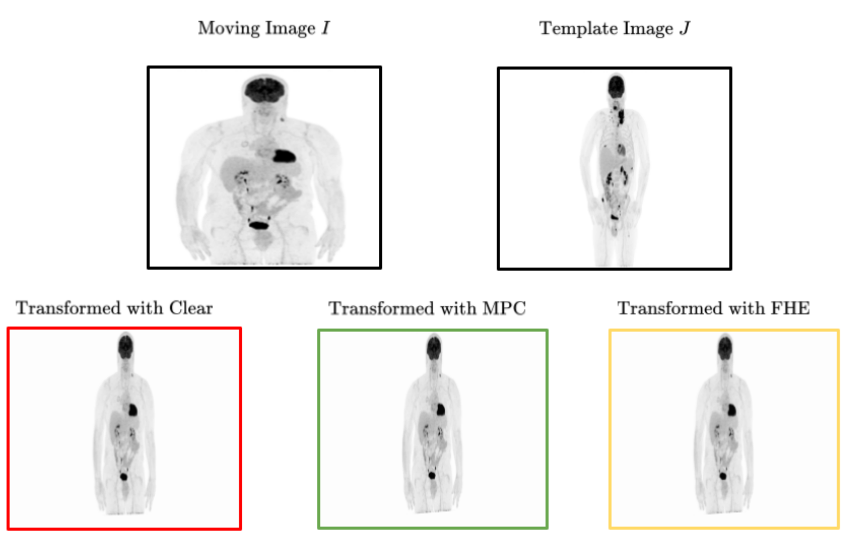


Figure 1: qualitative results for affine registration

We demonstrate and assess PPIR based on linear (Figure 1) and non-linear registration, by comparing the registration results with respect to the ones obtained with standard registration on clear images (Clear). Table 1 (Affine registration metrics) shows that PPIR through MPC and FHE leads to negligible differences with respect to Clear. Table 1 (Affine efficiency metrics) reports that MPC demands higher communication and slower time execution, while FHE has lower communication but higher time execution.

Affine registration metrics			
Solution	Intensity Error (SSD)	Num. Interation	Displacement RMSE CLEAR vs PPIR (mm)
CLEAR	4.34 ± 0.0	118 ± 0.0	-
SPDZ	4.34 ± 0.0	114.8 ± 4.0	1.81 ± 0.02
CKKS	✗	✗	✗
CLEAR + URS	4.38 ± 0.0	61 ± 0.0	-
SPDZ + URS	4.34 ± 0.0	60.4 ± 6.85	16.49 ± 3.74
CKKS ($D = 128$) + URS	4.34 ± 0.10	61.80 ± 4.82	23.31 ± 2.72
CLEAR + GMS	4.34 ± 0.0	63 ± 0.0	-
SPDZ + GMS	4.34 ± 0.0	59.80 ± 6.20	6.21 ± 1.49
CKKS ($D = 128$) + GMS	4.34 ± 0.05	60.4 ± 5.12	5.17 ± 1.40

Affine efficiency metrics				
Solution	Time $party_1$ (s)	Time $party_2$ (s)	Comm. $party_1$ (MB)	Comm. $party_2$ (MB)
CLEAR	0.0	0.0	-	-
SPDZ	0.13	0.13	1.54	1.54
CKKS	✗	✗	✗	✗
CLEAR + URS	0.0	0.0	-	-
SPDZ + URS	0.02	0.02	0.20	0.20
CKKS ($D = 128$) + URS	2.55	0.02	0.06	0.01
CLEAR + GMS	0.0	0.0	-	-
SPDZ + GMS	0.02	0.02	0.20	0.20
CKKS ($D = 128$) + GMS	2.51	0.02	0.06	0.01

Table 1: quantitative results for affine registration, where SPDZ = MPC and CKKS = FHE

5.CONCLUSION & FUTURE EXTENSIONS

This work introduces PPIR, a novel framework to allow IR when images cannot be disclosed in clear. Future extensions are:

- Improve FHE time complexity;
- Apply to others cost function, i.e. Mutual Information.

6.REFERENCES

[1] Shattuck et al. : Online resources or validation of brain segmentation methods. NeuroImage45(2), 431–439 (2009)
[2] McMahan et al. : Communication-efficient learning of deep networks from decentralized data. In: AISTATS. pp. 1273–1282. PMLR (2017)
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council.
[4] Health Resources and Services Administration. Health insurance portability and accountability act, 1 (1996).
[5] Mattes et al. : Pet-ct image registration in the chest using free-form deformations. IEEE transactions on medical imaging 22(1), 120–128
[6] Sabuncu et al. : Gradient based non-uniform subsampling for information-theoretic alignment methods. In: The 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society. vol. 1, pp. 1683–1686. IEEE (2004)