Privacy Preserving Image Registration

Riccardo Taiello

Supervisors:
Marco Lorenzi, Melek Önen, Olivier Humbert

Epione Team, Inria Sophia Antipolis
Eurecom, Sophia Antipolis

3iA Côte d'Azur
Institut interdisciplinaire
d'intelligence artificielle

Inria

Introduction

Image Registration (IR)

Image registration goal: spatially align imaging features between two or multiple images.

Image Registration (IR)

Image registration goal: spatially align imaging features between two or multiple images.

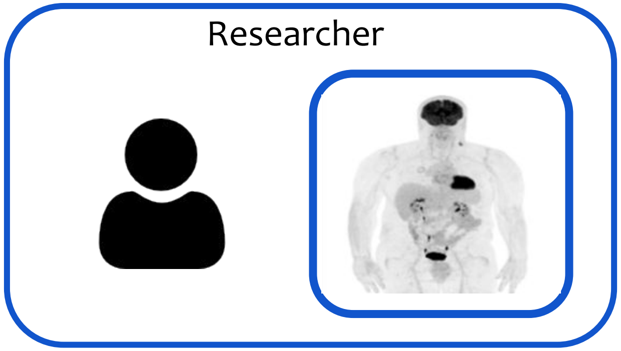


Image Registration (IR)

Image registration goal: spatially align imaging features between two or multiple images.

Researcher

Hospital

Image Registration (IR)

Image registration goal: spatially align imaging features between two or multiple images.

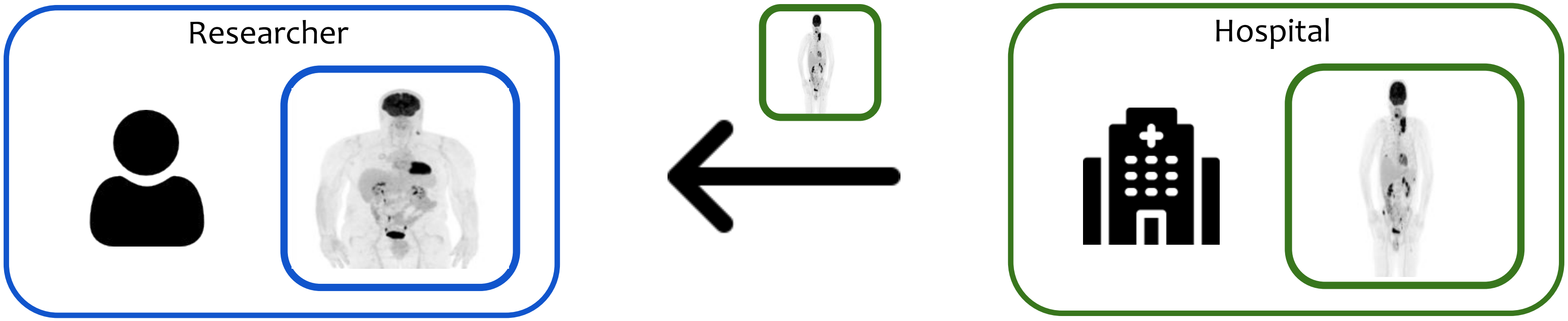
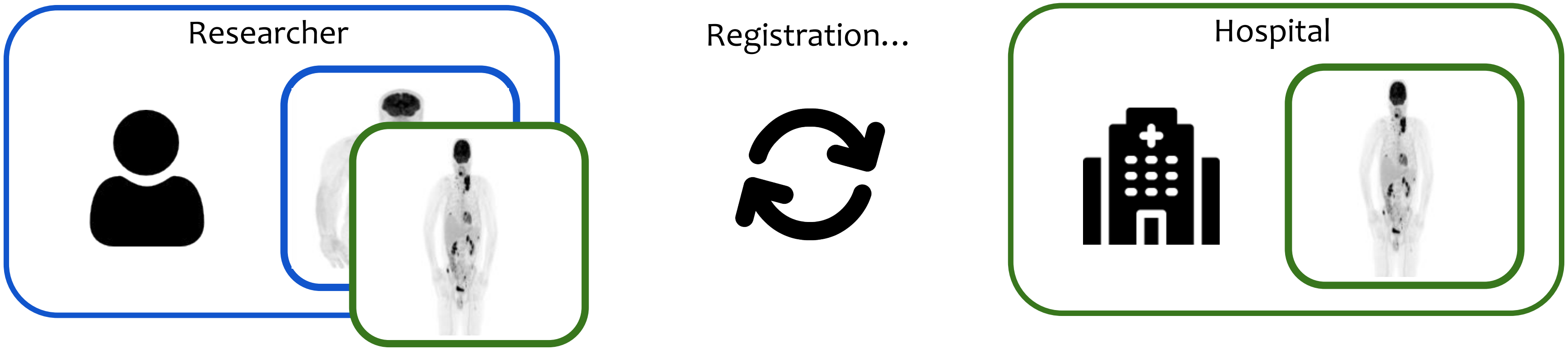


Image Registration (IR)

Image registration goal: spatially align imaging features between two or multiple images.



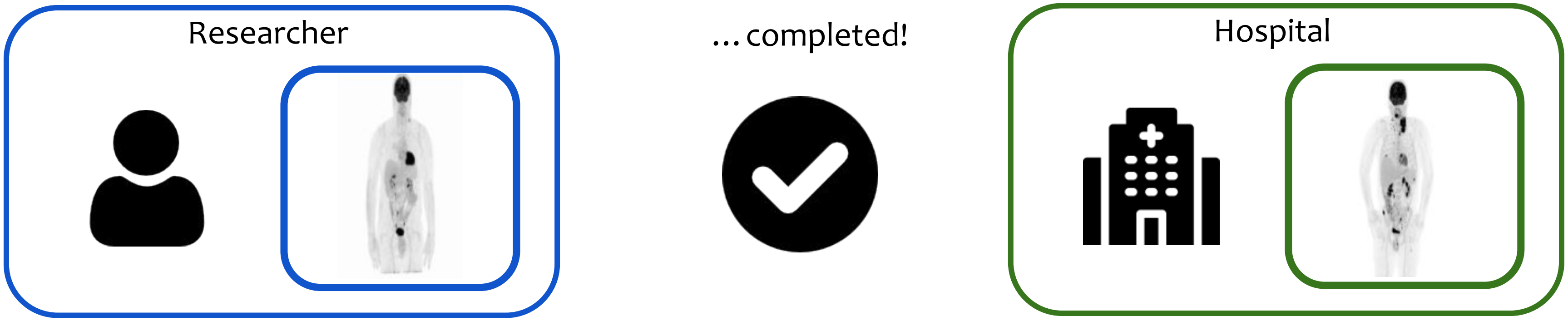
Researcher

Registration…

Hospital

Image Registration (IR)

Image registration goal: spatially align imaging features between two or multiple images.



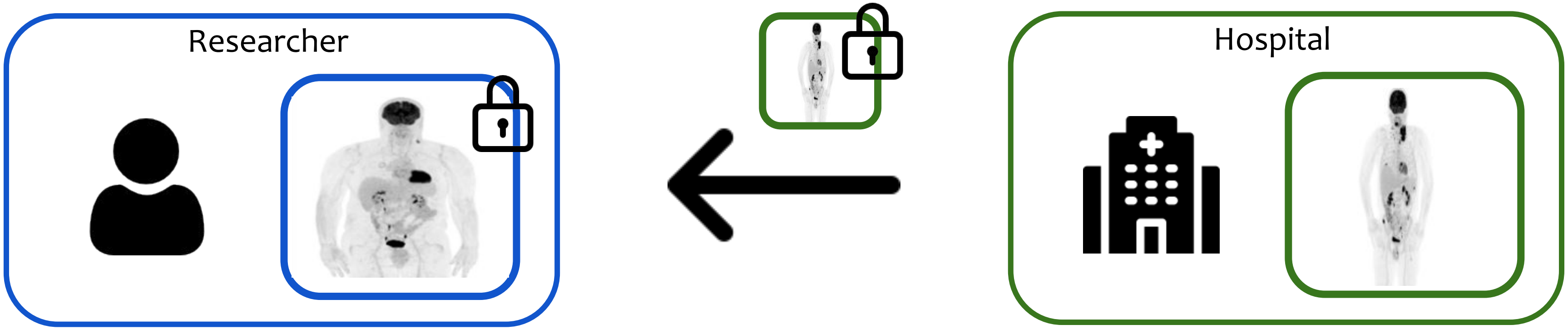
Researcher

…completed!

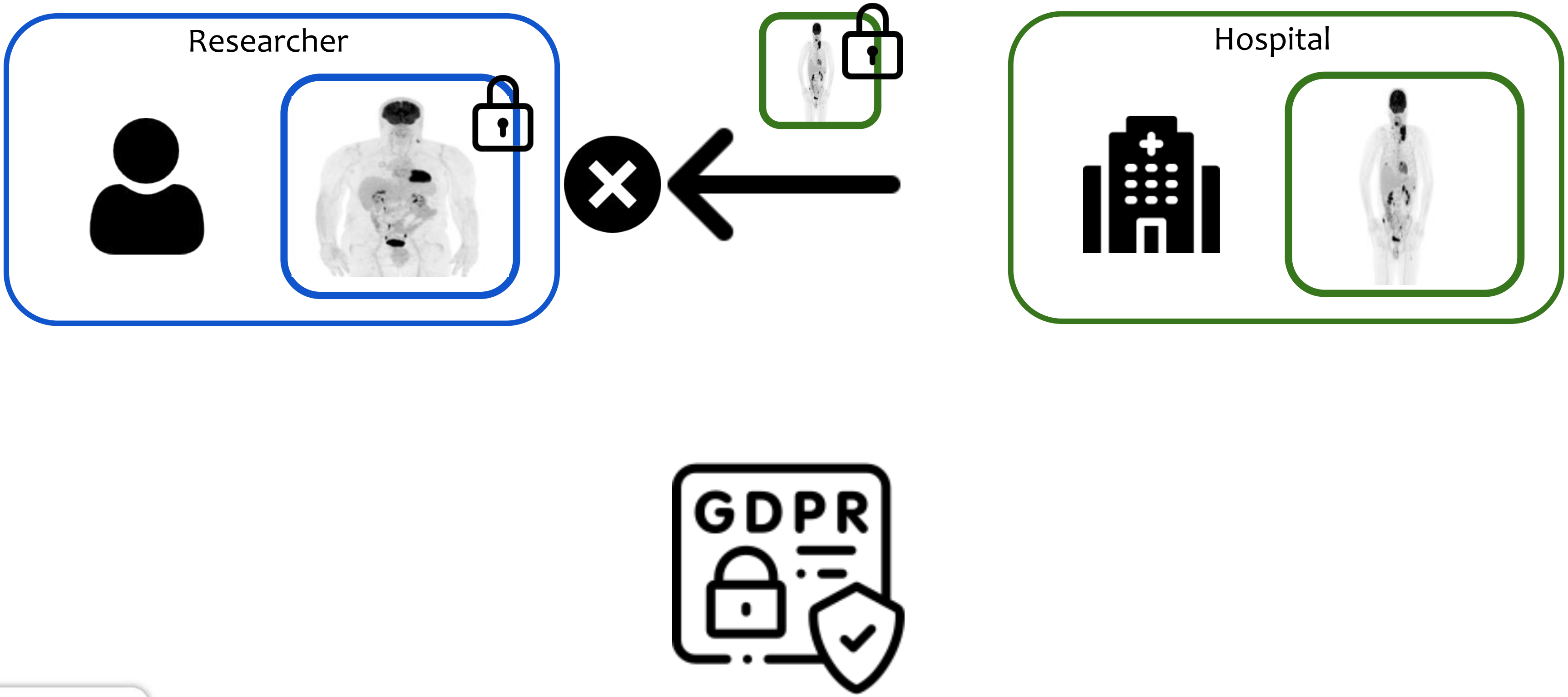
Hospital

Problem

Privacy Concerns



Privacy Concerns



Background

Optimization problem - IR [Baker et al.]

$$\mathrm{SSD}(I, J, \mathbf{p}) = \arg\min_{\mathbf{p}} \sum_{i,j} \Big[(I(W_{\mathbf{p}}(i,j))) - J(i,j) \Big]^2$$

$$\Delta\mathbf{p} = H^{-1} \cdot \sum_{i,j} S(i,j) \cdot (I(\mathbf{W}_{\mathbf{p}}(i,j)) - J(i,j))$$

$$S(i,j) = \nabla I(i,j) \frac{\partial\, \mathbf{W}_{\mathbf{p}}(i,j)}{\partial \mathbf{p}}$$

$$H = \sum_{i,j} \left(\nabla I(i,j) \frac{\partial\, \mathbf{W}_{\mathbf{p}}(i,j)}{\partial \mathbf{p}} \right)^T \left(\nabla I(i,j) \frac{\partial\, \mathbf{W}_{\mathbf{p}}(i,j)}{\partial \mathbf{p}} \right)$$

Method

Privacy Preserving Image Registration (PPIR)[Taiello et al.]

$$\Delta\mathbf{p} = H^{-1} \cdot \sum_{i,j} \overset{\text{Researcher (party}_1\text{)}}{\boxed{S(i,j)}} \cdot \left(I(\mathbf{W}_\mathbf{p}(i,j)) - \overset{\text{Hospital (party}_2\text{)}}{\boxed{J(i,j)}}\right)$$

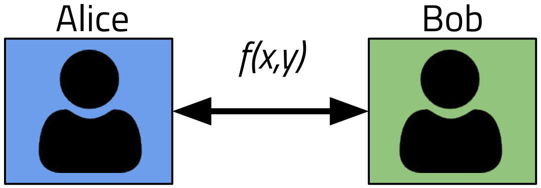
$$R = \sum_{i,j} \overset{\text{Researcher (party}_1\text{)}}{\boxed{S(i,j)}} \cdot \overset{\text{Hospital (party}_2\text{)}}{\boxed{J(i,j)}}$$

In a vectorized form:

$$R = \overset{\text{Researcher (party}_1\text{)}}{\boxed{S^T}} \cdot \overset{\text{Hospital (party}_2\text{)}}{\boxed{J}}$$

Privacy Preserving Techniques

Multi Party Computation (MPC)



Knows *x*

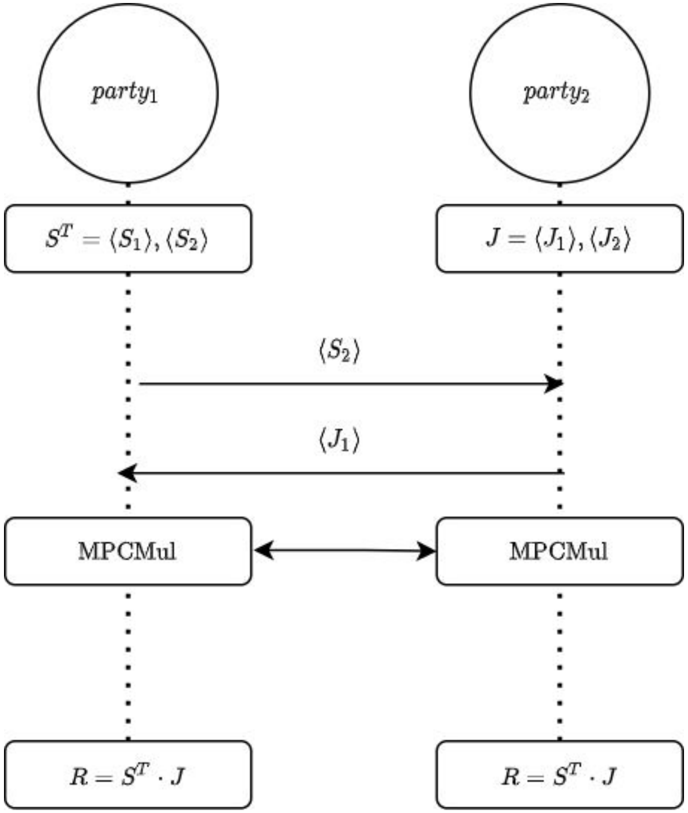
Knows *y*

Fully Homomorphic Encryption (FHE)

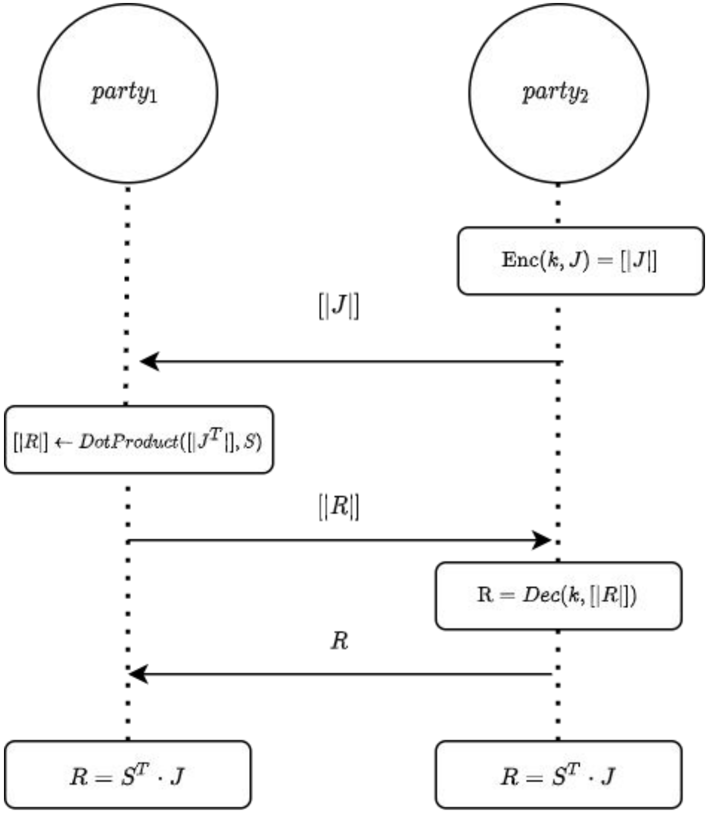
$$\begin{tikzcd} m \arrow[r, "Enc"] \arrow[d, "f"'] & Enc(m) \arrow[d, "f"] \\ f(m) & f(Enc(m)) \arrow[l, "Dec"'] \end{tikzcd}$$

PPIR protocols [Taiello et al.]

Multi Party Computation (MPC)



Fully Homomorphic Encryption (FHE)


$party_1$
$party_2$
$\mathrm{Enc}(k, J) = [|J|]$
$[|J|]$
$[|R|] \leftarrow DotProduct([|J^T|], S)$
$[|R|]$
$\mathrm{R} = Dec(k, [|R|])$
R
$R = S^T \cdot J$
$R = S^T \cdot J$

Optimization

For MPC & FHE:

Large images, solutions:

- Uniformly Random Selection (URS)[Mattes et al.]
- Gradient Magnitude Sampling (GMS)[Viola et al.]

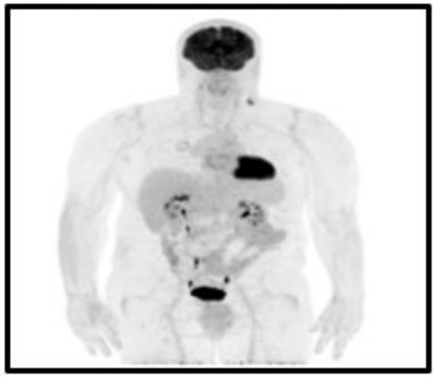
For FHE:

We propose to partition the image I into K sub-arrays, and the matrix S into K submatrices.

Results

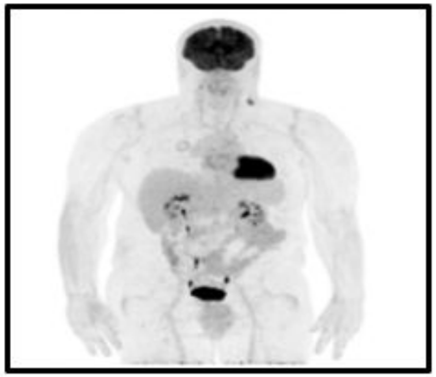
Results

Moving Image I

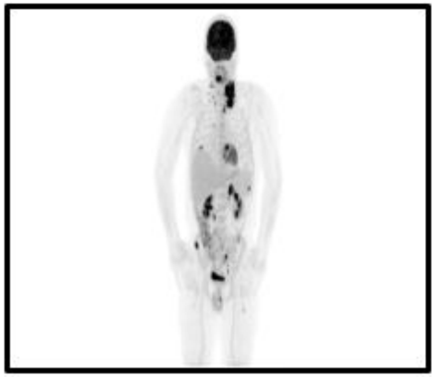


Results

Moving Image I

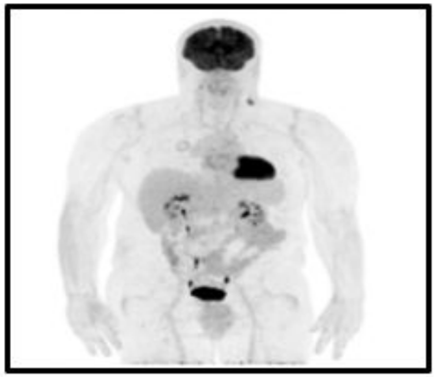


Template Image J

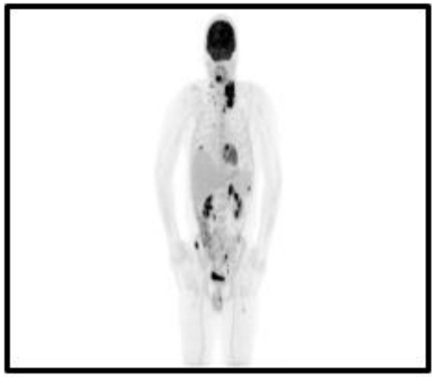


Results

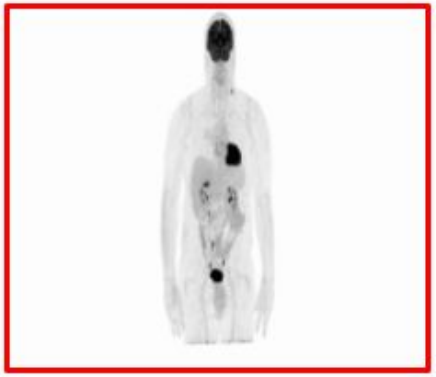
Moving Image I



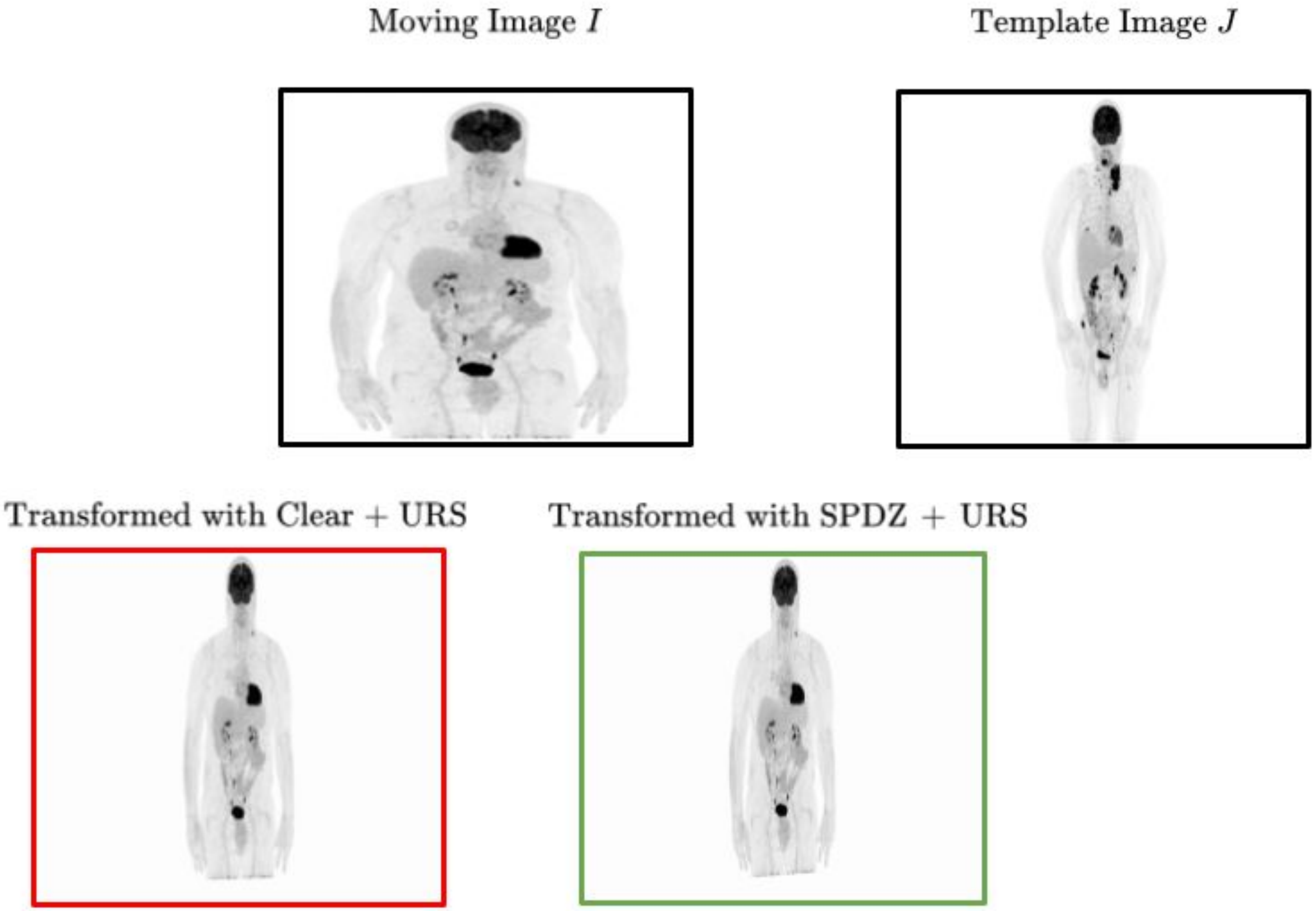
Template Image J



Transformed with Clear + URS



Results



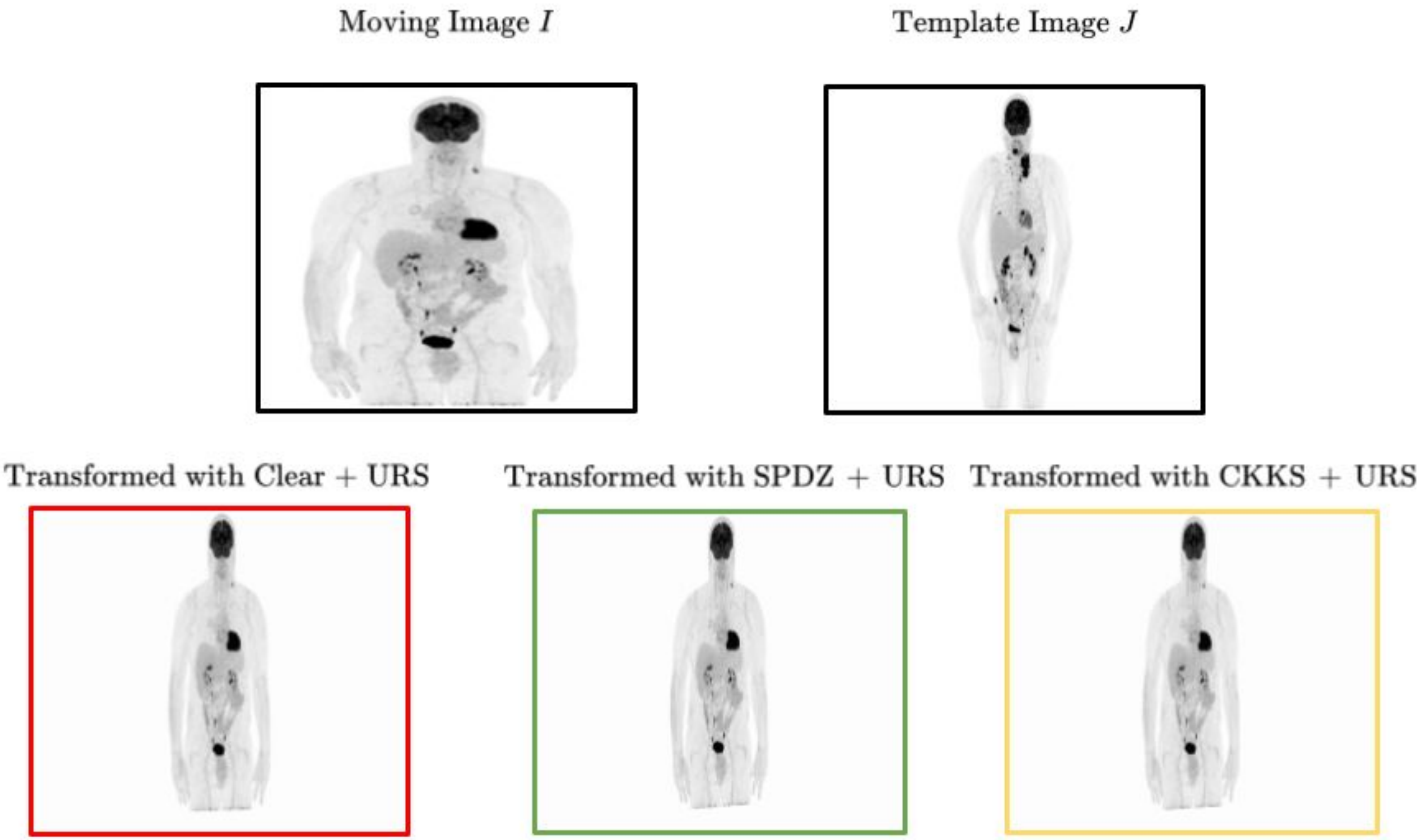
Moving Image I

Template Image J

Transformed with Clear + URS

Transformed with SPDZ + URS

Results



Moving Image I

Template Image J

Transformed with Clear + URS

Transformed with SPDZ + URS

Transformed with CKKS + URS

Conclusions

PPIR a novel framework to allow image registration when images are confidential and **cannot be disclosed in clear**.

Future extensions:

- 3D medical image data;
- multimodal image registration problem.

References

Taiello, R., Önen, M., Humbert, O., Lorenzi, M.: Privacy Preserving Image Registration [**ACCEPTED MICCAI 2022**] https://arxiv.org/abs/2205.10120

Thanks!

3iA Côte d'Azur

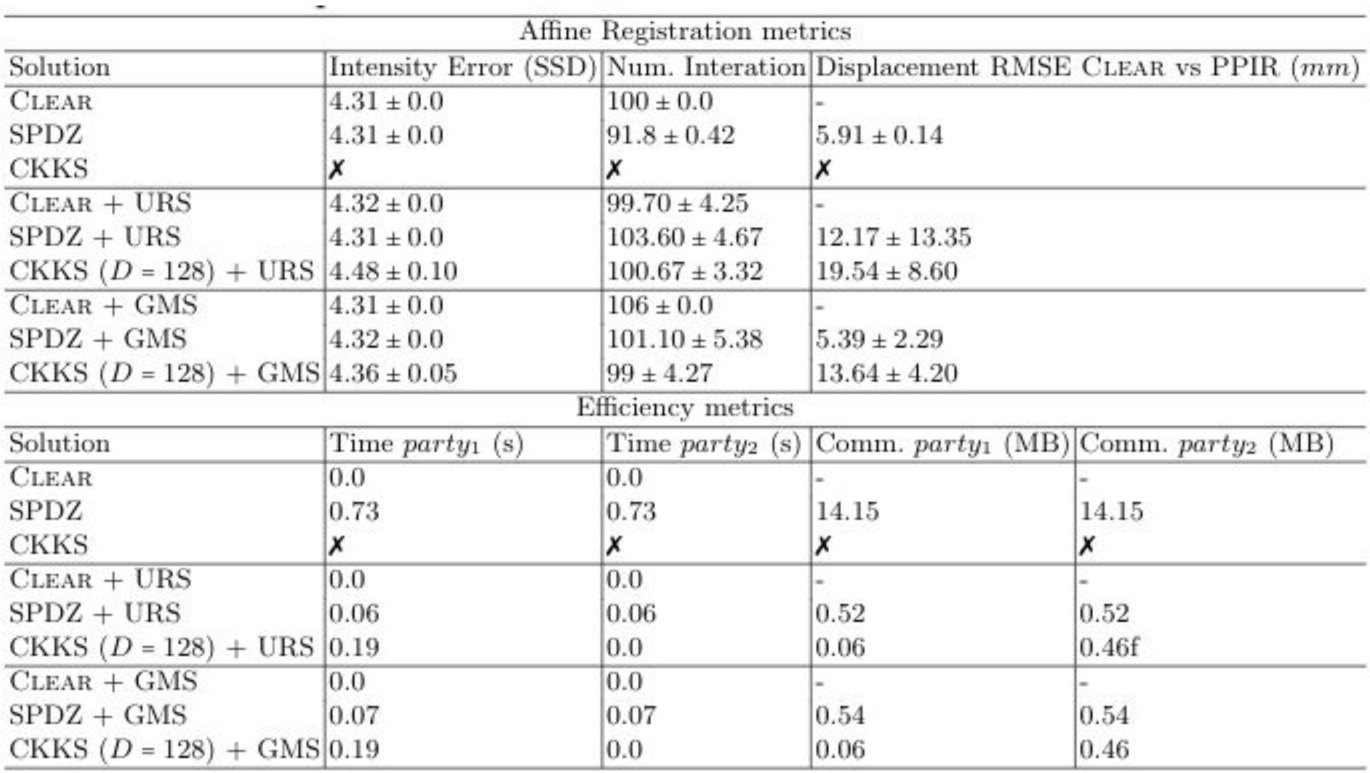
Institut interdisciplinaire d'intelligence artificielle

Inria

Antoine Lacassagne
CENTRE DE LUTTE CONTRE LE CANCER
unicancer NICE

EURECOM
Sophia Antipolis

Result - Linear Transformation



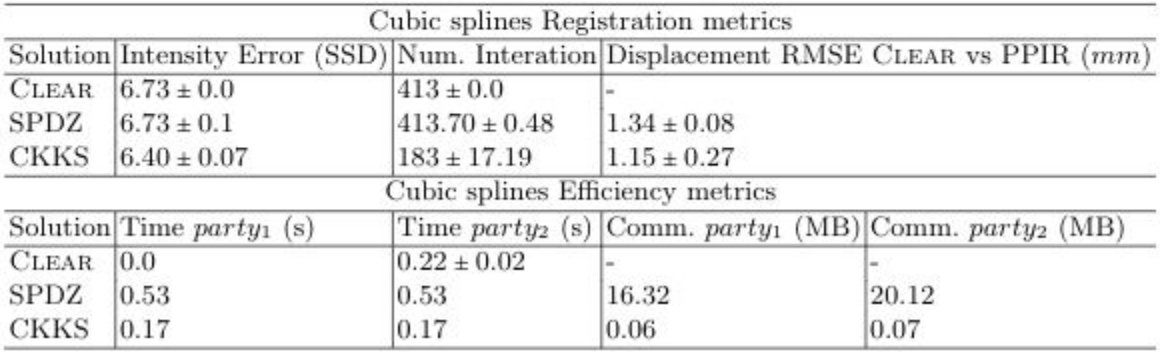
Affine Registration metrics

Solution	Intensity Error (SSD)	Num. Interation	Displacement RMSE Clear vs PPIR (mm)
Clear	4.31 ± 0.0	100 ± 0.0	-
SPDZ	4.31 ± 0.0	91.8 ± 0.42	5.91 ± 0.14
CKKS	✗	✗	✗
Clear + URS	4.32 ± 0.0	99.70 ± 4.25	-
SPDZ + URS	4.31 ± 0.0	103.60 ± 4.67	12.17 ± 13.35
CKKS (D = 128) + URS	4.48 ± 0.10	100.67 ± 3.32	19.54 ± 8.60
Clear + GMS	4.31 ± 0.0	106 ± 0.0	-
SPDZ + GMS	4.32 ± 0.0	101.10 ± 5.38	5.39 ± 2.29
CKKS (D = 128) + GMS	4.36 ± 0.05	99 ± 4.27	13.64 ± 4.20

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	0.73	0.73	14.15	14.15
CKKS	✗	✗	✗	✗
Clear + URS	0.0	0.0	-	-
SPDZ + URS	0.06	0.06	0.52	0.52
CKKS (D = 128) + URS	0.19	0.0	0.06	0.46f
Clear + GMS	0.0	0.0	-	-
SPDZ + GMS	0.07	0.07	0.54	0.54
CKKS (D = 128) + GMS	0.19	0.0	0.06	0.46

Result - Non Linear Transformation



Cubic splines Registration metrics

Solution	Intensity Error (SSD)	Num. Interation	Displacement RMSE CLEAR vs PPIR (mm)
CLEAR	6.73 ± 0.0	413 ± 0.0	-
SPDZ	6.73 ± 0.1	413.70 ± 0.48	1.34 ± 0.08
CKKS	6.40 ± 0.07	183 ± 17.19	1.15 ± 0.27

Cubic splines Efficiency metrics

Solution	Time $party_1$ (s)	Time $party_2$ (s)	Comm. $party_1$ (MB)	Comm. $party_2$ (MB)
CLEAR	0.0	0.22 ± 0.02	-	-
SPDZ	0.53	0.53	16.32	20.12
CKKS	0.17	0.17	0.06	0.07