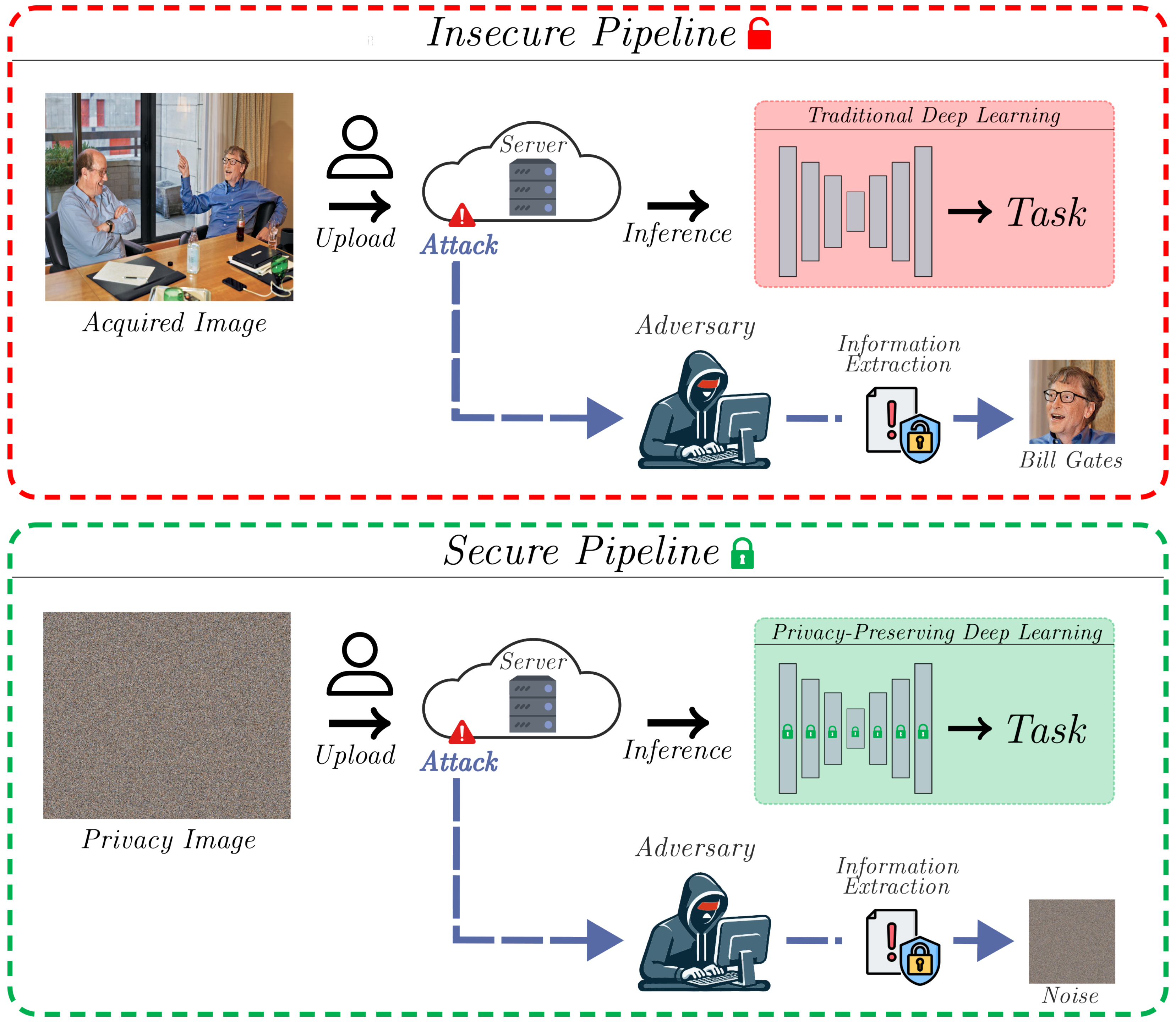
Privacy-Preserving Deep Learning Using Deformable Operators for Secure Task Learning

Fabian Perez, Jhon Lopez and Henry Arguello
Universidad Industrial de Santander, Department of Computer Science
Paper 3997

Introduction

Motivation: In the era of cloud computing, the paramount importance of preserving privacy in deep learning systems becomes evident as users increasingly upload sensitive data, exposing them to risks of unauthorized access. This underscores the urgent need for frameworks that can provide visually perturbed images in such a way that attackers cannot recover them yet still retain optimal task performance.



To address this need, we propose a framework that adheres to a secure pipeline while maintaining the same performance on a selected task

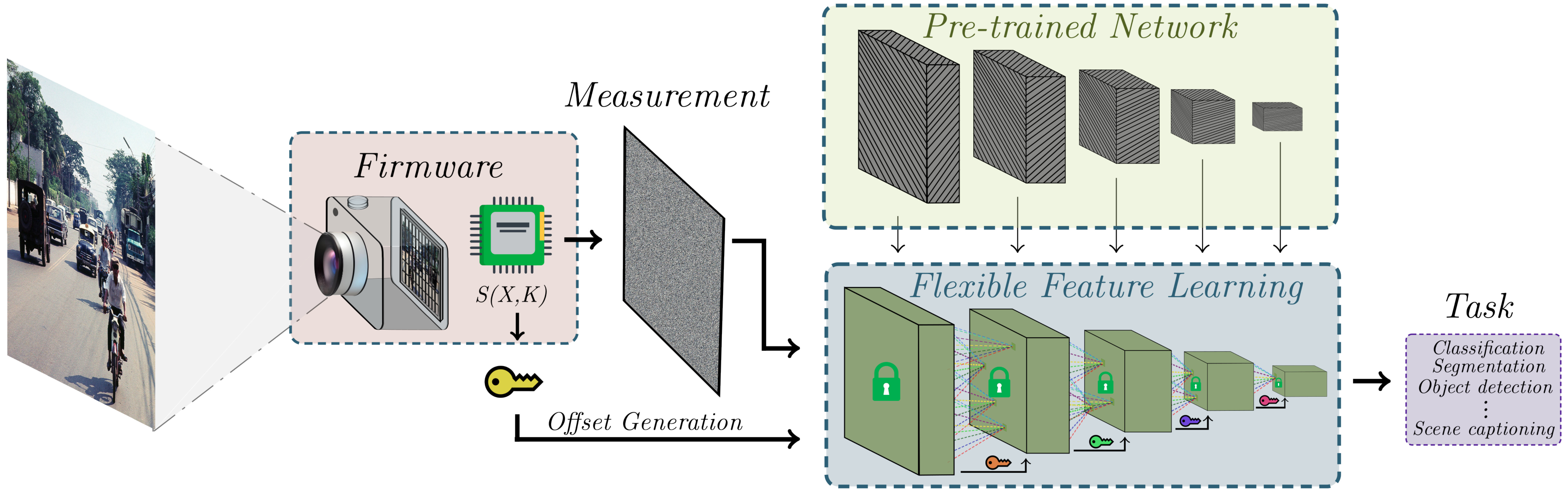
Conclusions

- A comprehensive framework was proposed to ensure complete privacy for any task using CNNs.
- Demonstrated that increased privacy does not necessarily mean a trade-off in performance or more complex models
- Pretrained neural networks on non-private images can also be used effectively on private images.

Contact

Contact PhD. Henry Arguello
Email henarfu@uis.edu.co
Code github.com/factral/privDL
Linkedin www.linkedin.com/in/henry-arguello-2905929

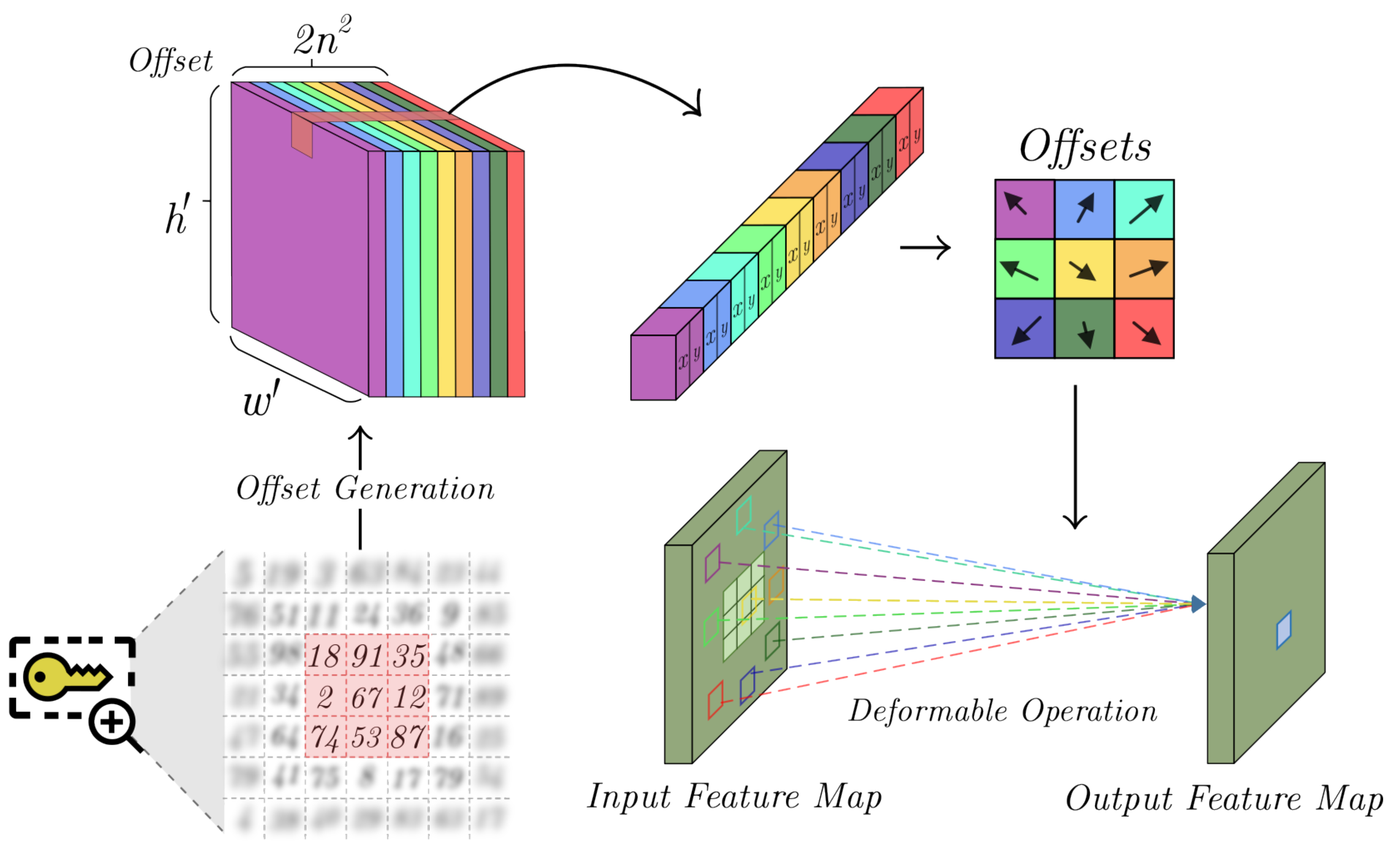
Proposed Framework



Proposed framework for private images. The camera captures an image, which is then passed through a custom analog-to-digital converter to apply a transformation. The resulting measurement is a private image that is an input to the flexible feature learning module which is initialized with pre-trained weights. This module generates underlying features that can be used in any task.

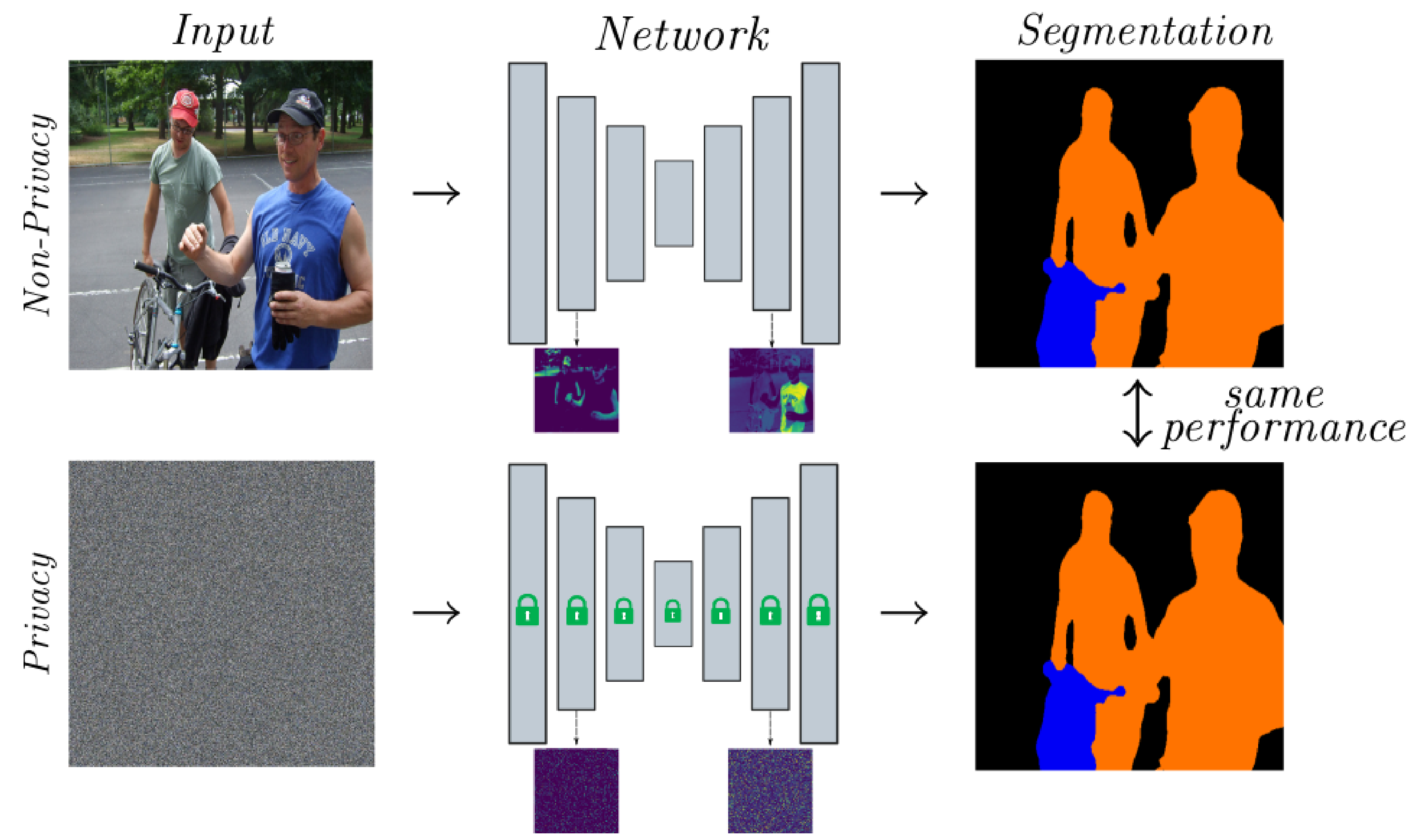
Offset Generation

Offset generation from a key $\mathbf{K} \in \mathbb{Z}_+^{h\times w}$. The key stores the true pixel positions, while the offset $\Delta\mathbf{p} \in \mathbb{R}^{h'\times w'\times(2*n*n)}$ holds the distance to the true position from the kernel sampling



Results

Method	Model	# Parameters (10^6)	Acc
ELE [7]	Shakedrop	29.31	83.06
EtC [19]	Shakedrop	5.35	89.09
PrivConv [8]	ConvMixer-512/16	5.35	92.65
Ours	PreResNet-110	**1.70**	**95.06**



Bibliography

[1] Jeffrey Byrne, Brian DeCann, and Scott Bloom, “Key-nets: Optical transformation convolutional networks for privacy preserving vision sensors” arXiv preprint
[2] Hinojosa, C., et al, "Privhar: Recognizing human actions from privacy-preserving lens," in European Conference on Computer Vision, 2022, pp. 314–332.
[3] Paula Arguello, Jhon Lopez, Carlos Hinojosa, Henry Arguello. "Optics lens design for privacy-preserving scene captioning." ICIP. 2022.
[4] Hinojosa, Carlos, Juan Carlos, Niebles, Henry, Arguello. "Learning privacy-preserving optics for human pose estimation." CVPR. 2021.