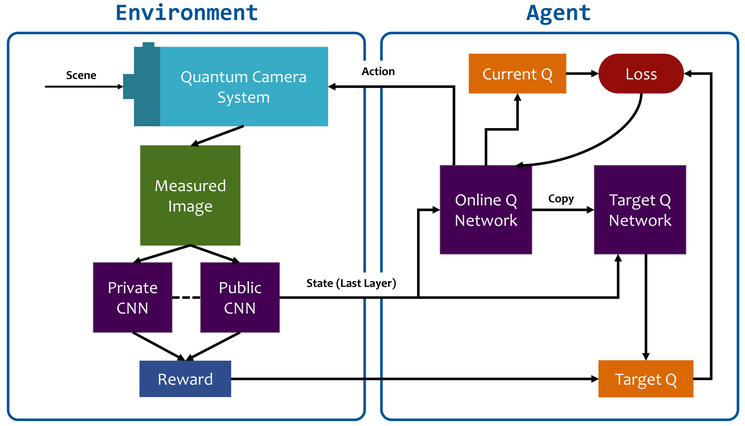
Schrödinger's Camera: First Steps Towards a Quantum-Based Privacy Preserving Camera

Hannah Kirkland and Sanjeev J. Koppal
University of Florida

JUNE 18-22, 2023 CVPR VANCOUVER, CANADA

Quantum-Based Privacy for Vision

- Machine learning algorithms can infer sensitive, private information *without permission.*
- **Clear images:** useful, but no privacy
- **Blank images:** completely private, but not useful
- **Privacy Preserving Vision:** allows machine learning algorithms to access visual information useful for a desired task, but not additional sensitive information

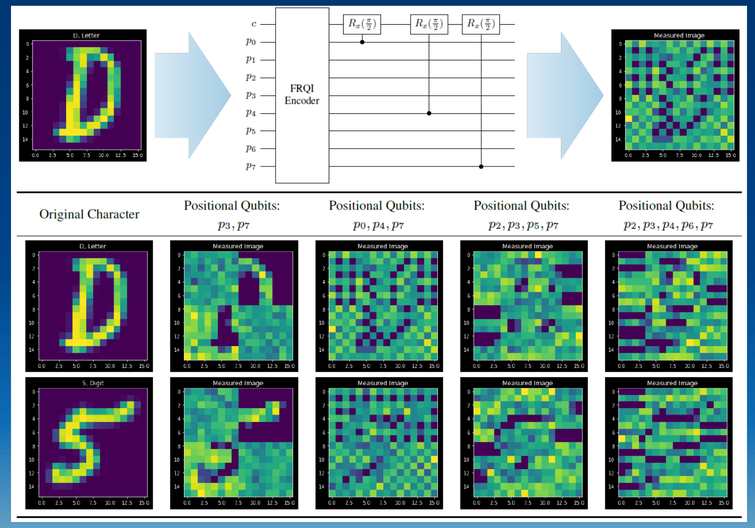


Workflow of our system showing how the quantum camera environment interacts with the DDQN agent. The image data is stored in quantum states, and the agent manipulates these with a set of actions — quantum circuits that are part of our contribution. Adversarial CNNs create the reward and, during testing, new CNNs are trained from scratch against fixed DDQN weights.

Privacy through Quantum Gates

Different methods of redacting FRQI (Flexible Representation of Quantum Images) image information were explored. The privacy for these methods is found after measurement, as quantum gates are reversible.

We propose a quantum framework where data, in a quantum sense, is both private and non-private until the point of measurement[1]. Our design is a hybrid quantum-silicon system. The algorithm learns what actions to take within the quantum computer framework *before* measurement, such that the measured image has the desired privacy-utility characteristics.



- **Controlling the Number of Shots:** FRQI stochastically encodes images onto quantum states, meaning the accuracy of the pixel grey scale value is directly related to how many times the circuit is run[2]. This is referred to as the number of "shots" and can be exploited to determine the level of noise in a measured image.
- **Adding Quantum Gates:** Additional gates can be added after encoding the image via FRQI to redact parts of the image. *Selection of these gates was not trivial.* Only controlled quantum rotations were found to be promising. Other gates simply translated or inverted the image.

Results and References

- **Public task (random – 50%):** categorize EMNIST data into letter or number
- **Private task (random – 2.8%):** categorize EMNIST data into which specific letter or number

Privacy and Utility Preservation Performance		
Baseline / Policy	**Public Accuracy**	**Private Accuracy**
Quantum Augmentation Baseline	88.5%	85.0%
Gaussian Noise Augmented EMNIST Baseline	56.5%	11.4%
Public-Based Reward Policy	**56.5%**	**2.5%**
Length-Based Reward Policy	51.5%	4.3%
Accuracy-Based Reward Policy	48.7%	2.8%

[1] Christopher Monroe, DM Meekhof, BE King, and David J Wineland. A "schrödinger cat" superposition state of an atom. Science, 272(5265):1131–1136, 1996.

[2] Phuc Q. Le, Fangyan Dong, and Kaoru Hirota. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. 10(1):63–84.