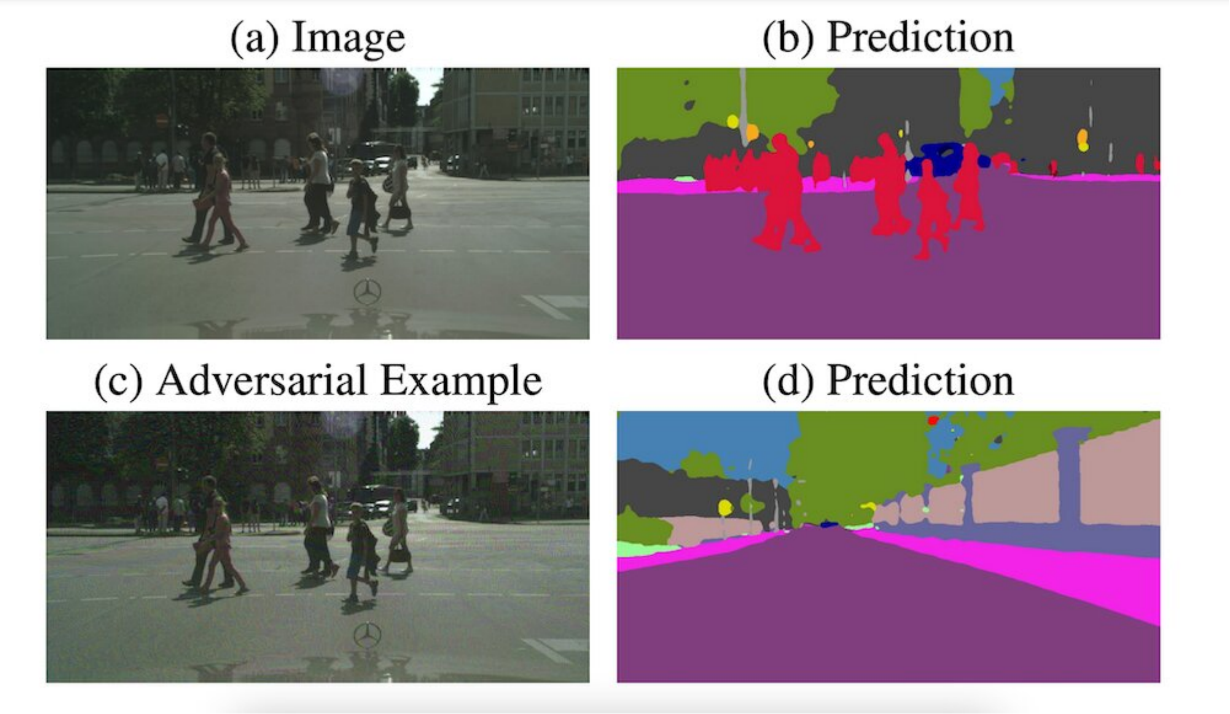
From self-driving cars to military surveillance: Quantum computing can help secure the future of AI systems

May 28 2023, by Muhammad Usman



In this example you can see an algorithm that correctly identifies humans based on an image input. However, when a few pixels are changed in an adversarial attack, the algorithm can no longer identify the humans. Credit: Jan Hendrik Metzen et. al., Author provided

Artificial intelligence algorithms are quickly becoming a part of everyday life. Many systems that require strong security are either already underpinned by machine learning or soon will be. These systems include facial recognition, banking, military targeting applications, and robots and autonomous vehicles, to name a few.

This raises an important question: how secure are these machine learning algorithms against malicious attacks?

In an article published today in *Nature Machine Intelligence*, my colleagues at the University of Melbourne and I discuss a potential solution to the vulnerability of machine learning models.

We propose that the integration of quantum computing in these models could yield new algorithms with strong resilience against adversarial attacks.

The dangers of data manipulation attacks

Machine learning algorithms can be remarkably accurate and efficient for many tasks. They are particularly useful for classifying and identifying image features. However, they're also highly vulnerable to data manipulation attacks, which can pose serious security risks.

Data manipulation attacks—which involve the very subtle manipulation of image data—can be launched in several ways. An attack may be launched by mixing corrupt data into a training dataset used to train an algorithm, leading it to learn things it shouldn't.

Manipulated data can also be injected during the testing phase (after training is complete), in cases where the AI system continues to train the underlying algorithms while in use.

People can even carry out such attacks from the physical world.

Someone could put a sticker on a stop sign to fool a self-driving car's AI into identifying it as a speed-limit sign. Or, on the front lines, troops might wear uniforms that can fool AI-based drones into identifying them as landscape features.

Either way, the consequences of data manipulation attacks can be severe. For example, if a self-driving car uses a machine learning algorithm that has been compromised, it may incorrectly predict there are no humans on the road—when there are.

How quantum computing can help

In our article, we describe how integrating quantum computing with machine learning could give rise to secure algorithms called quantum machine learning models.

These algorithms are carefully designed to exploit special quantum properties that would allow them to find specific patterns in image data that aren't easily manipulated. The result would be resilient algorithms that are safe against even powerful attacks. They also wouldn't require the expensive "adversarial training" currently used to teach algorithms how to resist such attacks.

Beyond this, quantum machine learning could allow for faster algorithmic training and more accuracy in learning features.

So how would it work?

Today's classical computers work by storing and processing information as "bits", or binary digits, the smallest unit of data a computer can process. In classical computers, which follow the laws of classical physics, bits are represented as binary numbers—specifically 0s and 1s.

Quantum computing, on the other hand, follows principles used in quantum physics. Information in quantum computers is stored and processed as qubits (quantum bits) which can exist as 0, 1, or a combination of both at once. A quantum system that exists in multiple states at once is said to be in a superposition state. Quantum computers can be used to design clever algorithms that exploit this property.

However, while there are significant potential benefits in using quantum computing to secure machine learning models, it could also be a double-edged sword.

On one hand, quantum machine learning models will provide critical security for many sensitive applications. On the other, quantum computers could be used to generate powerful adversarial attacks, capable of easily deceiving even state-of-the-art conventional machine learning models.

Moving forward, we'll need to seriously consider the best ways to protect our systems; an adversary with access to early quantum computers would pose a significant security threat.

Limitations to overcome

The current evidence suggests we're still some years away from quantum machine learning becoming a reality, due to limitations in the current generation of quantum processors.

Today's quantum computers are relatively small (with fewer than 500 qubits) and their error rates are high. Errors may arise for several reasons, including imperfect fabrication of qubits, errors in the control circuitry, or loss of information (called "quantum decoherence") through interaction with the environment.

Still, we've seen enormous progress in quantum hardware and software over the past few years. According to recent quantum hardware roadmaps, it's anticipated quantum devices made in coming years will have hundreds to thousands of qubits.

These devices should be able to run powerful quantum machine learning models to help protect a large range of industries that rely on machine learning and AI tools.

Worldwide, governments and private sectors alike are increasing their investment in quantum technologies.

This month the Australian government launched the National Quantum Strategy, aimed at growing the nation's quantum industry and commercializing quantum technologies. According to the CSIRO, Australia's quantum industry could be worth about A$2.2 billion by 2030.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: From self-driving cars to military surveillance: Quantum computing can help secure the future of AI systems (2023, May 28) retrieved 1 May 2024 from https://phys.org/news/2023-05-self-driving-cars-military-surveillance-quantum.html