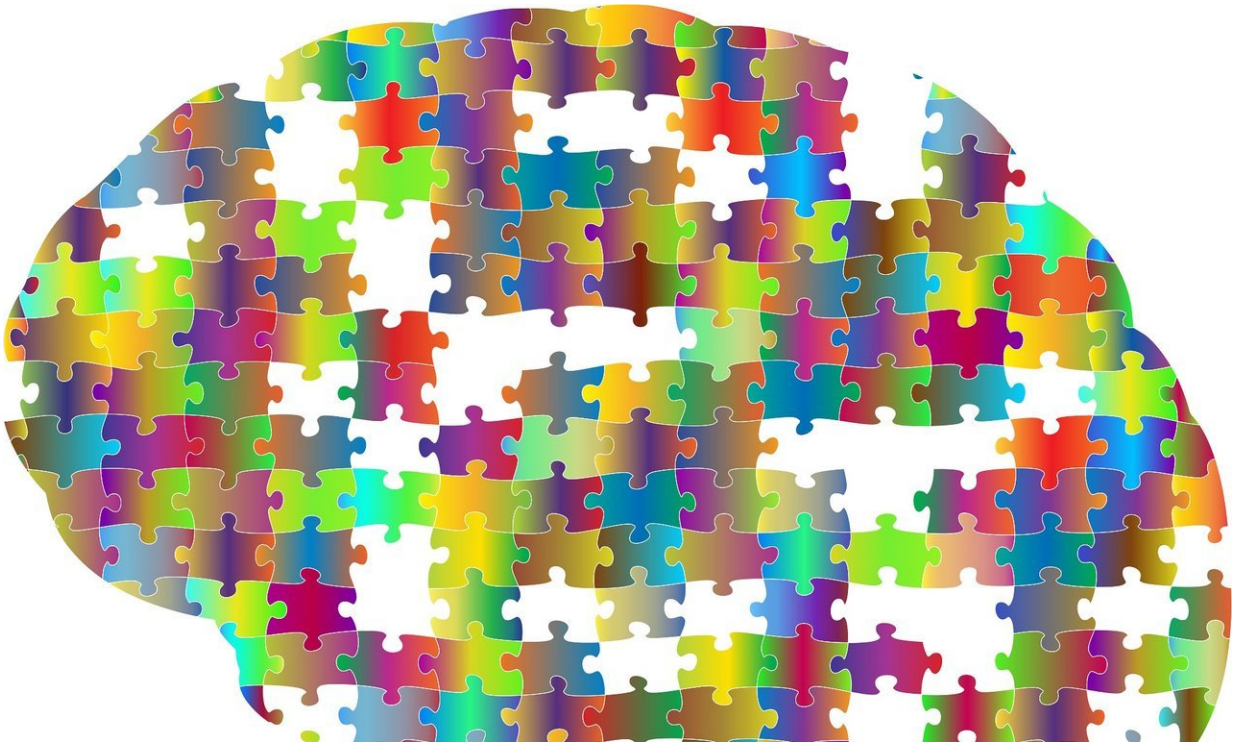
Researchers use WWII code-breaking techniques to interpret brain data

December 13 2017



Credit: CC0 Public Domain

Cracking the German Enigma code is considered to be one of the decisive factors that hastened Allied victory in World War II. Starting with clues derived from espionage, computer scientists were able to work out the rules that turned a string of gibberish characters into plain German, providing life-saving and war-shortening intelligence.

A team of researchers from the University of Pennsylvania, the Georgia Institute of Technology, and Northwestern University have now accomplished a similar feat, using cryptographic techniques to decode the activity of motor neurons. Their approach has allowed them to predict, from brain data, and with only generic knowledge of typical movements, which direction monkeys will move their arms.

The same cryptography-inspired technique could eventually be used to decode more complex patterns of muscle activation, for use in prosthetic devices, or even speech, to aid those with total paralysis.

The research team was led by Konrad Kording, a Penn Integrates Knowledge Professor with appointments in the Department of Neuroscience in Penn's Perelman School of Medicine and in the Department of Bioengineering in the School of Engineering and Applied Science, and Eva Dyer, then a postdoctoral researcher in Kording's lab and now an assistant professor in the Department of Biomedical Engineering at the Georgia Institute of Technology and Emory University. They collaborated with the group of Lee Miller, a professor of physiology at Northwestern University.

The researchers published their study in the journal *Nature Biomedical Engineering*.

In an experiment with three rhesus macaques, the researchers took data from several hundred neurons associated with arm movement. As the monkeys completed tasks where they had to reach to a target that appeared at different points around a central starting point, in-dwelling electrodes recorded spikes of electrical activity that corresponded with the movement of the monkey's arm.

Existing brain-computer interfaces can use such data to move a robotic prosthesis, but do so using a process known as "supervised learning." The

interface is trained to recognize how the patterns of neural firings correspond to each movement, and can thus "reconstruct" movements based on the on-going neuronal signals recorded from the monkey's brain.

In the cryptography approach, however, there was no such supervised training.

"In cryptography, 'supervised learning' would be called a 'known plaintext attack'," Kording said. "That is, we have both the encrypted and unencrypted message and just need to figure out the rules that turn one into the other. What we wanted to do in this study was to be able to decode the brain, using a movement model, from the encrypted message alone."

Starting with each neuron's firing pattern, the team's goal was to discover a consistent way of mathematically mapping those patterns to the monkeys' actual arm movements. Their approach was made possible by finding statistical structures of movements. Similar insights about language structure, such as the frequency and distribution of vowels, were involved in breaking the Enigma code.

"Essentially, the algorithm tries a range of possible decoders until we get something where the output looks like typical movements," Kording said. "There are issues scaling this up — it's a hard computer science problem — but this is a proof-of-concept that cryptanalysis can work in the context of neural activity."

A cryptanalysis approach to decoding neural activity is particularly attractive when it comes to brain-computer interfaces that control prosthetics. Having robotic limbs that can directly interpret their user's thoughts without having to be calibrated would represent a significant quality-of-life improvement.

"These training periods can be long and annoying, and in some circumstances, they're truly problematic—say, if your arm is missing, rather than paralyzed," said Kording. "Willing movement is different from imagining moving a nonexistent arm."

This cryptanalysis approach could provide a way for brain-computer interfaces to achieve literal mindreading.

"You could ask a 'locked-in' patient to generate neural patterns associated with specific words, but the corpus of language is very large," Kording said. "Rather than having them generate a pattern that is associated with every word they want to say, we could build a decoder that transforms those patterns until it looks like language."

"I think we should be able to do this within the next decade," he said.

Working in favor of this goal is a consistent improvement in brain-recording technology, with scientists currently working toward electrode arrays capable of simultaneously sampling data from a million neurons.

"As this capability grows, our technique becomes more useful," Kording said, "At the same time, I think we need to be very careful about the possibility of it being applied to people without their consent. What spy agencies could do with this technology is scary."

Though at a very preliminary stage, the researchers believe their cryptanalysis approach to decoding neural activity is a fundamentally good match for the problem.

"The Germans were actively working against decryption and modern ciphertexts are basically impossible to break," Kording said. "We have it easier. The brain ended up with this encryption system through natural selection, so it's essentially making the same kind of 'mistakes' that

allowed us to crack Enigma in the first place."

More information: Eva L. Dyer et al, A cryptography-based approach for movement decoding, *Nature Biomedical Engineering* (2017). DOI: 10.1038/s41551-017-0169-7

Provided by University of Pennsylvania