CALIFORNIA STATE SCIENCE FAIR
2017 PROJECT SUMMARY

Name(s)

Alexander T. McDowell

Project Number

J0805

Project Title

Neural Espionage: Can Adversarial Neural Networks Learn to Apply Encryption to Images?

Abstract

Objectives/Goals

To determine if two neural networks, a Provider and a Receiver, can successfully encrypt and decrypt an image while preventing an intercepting neural network from deciphering the original image.

Methods/Materials

I started with three Adversarial Convolutional Neural Networks as a framework and developed them so that they could perform encryption to images instead of matrixes. I then trained the neural networks on 13 different tests. The variables I changed in my experiments were the number of training iterations, image and key sizes, types of images and keys, the rate at which the network learned, and the message and key lengths.

Results

The neural network achieved its training goals of minimizing guess error between the Provider and the Receiver. However, the intercepting neural network always managed to decrypt the image into a faint outline, which was decipherable to a human observer. As well, the image encrypted by the Provider wasn't cryptographically secure and was easy for a human to determine. In 12 out of the 13 tests, the Receiver successfully decrypted the message while in 8 out of the 13 tests the interceptor had an accurate outline of the encrypted image.

Conclusions/Discussion

Neural Networks can learn to apply encryption to images. However, the encryption being applied by the networks was not cryptographically strong. The data suggested that changing the loss function I was using would significantly improve the neural networks' ability to encrypt and decrypt images. Changing the architecture of the networks could also improve that same ability.

Summary Statement

I tested if Adversarial Neural Networks could learn to apply encryption to images.

Help Received

I designed my experiments myself. I received help understanding the scientific paper I used as a basis for my project from Cybersecurity Expert Chris K. Williams.