Matt Sokoloff
MSCS 630
Spring 2017

Project Proposal

For the semester project, I would like to use artificial neural networks for creating new encryptions methods. This project would recreate the experiments explained by the paper *Learning to protect communications with adversarial neural cryptography* (Abadi et al)[1]. As the paper explains, generative adversarial networks can be used to effectively produce custom encryption algorithms. The overall idea is that there are three parameterized functions that we refer to as networks. Two of the networks, named Bob and Alice, attempt to privately communicate. The third network, Eve, then attempts to eavesdrop on Bob and Alice's private conversation. This situation where there is a conflicting objective between the different networks creates a minimax scenario. This minimax objective is a differentiable function which can then be used for optimizing the network parameters. Eve becomes a better snooper, and in response, Bob and Alice become better at secretly communicating.

Upon achieving similar results to what the paper has outlined, the next step for the project would be to find ways to improve the algorithm. Simple improvements could be made by altering the network architectures. Recent advances in generative adversarial networks lead to faster convergence and more optimal solutions[2]. Additionally, altering network architectures may lead to more effective learning. Such architectures include residual, inception style, or recurrent connections. As these architectures become more complex, the run time will increase. To reduce the associated overhead, it might be possible to use shallow convolutional networks to approximate the learned representations of these deeper, more complex networks[3]. Furthermore, as these networks become deeper, learning becomes less stable. We could investigate instance normalization as an effective method for improving learning stability[4]. Finally, adversarial methods for steganography could be incorporated for an additional layer of security.[5]

While there are many avenues for exploring methods to improve the model, there will be certain challenges in implementing function approximators as an encryption method. Primarily, generative adversarial networks are notorious for being difficult to converge. Computing power must be an additional concern. For practical purposes, Alice and Bob must be able to quickly encode and decode a message. While training speed is less of a factor for usability, it will be impossible to test the efficacy of each proposed change without a short enough run time.

Overall encryption is an exciting application for artificial neural networks. The use case for powerful encryption methods are endless.

---

[1] https://arxiv.org/pdf/1610.06918.pdf
[2] https://arxiv.org/pdf/1511.06434v2.pdf
[3] https://arxiv.org/pdf/1511.06433.pdf
[4] https://arxiv.org/pdf/1607.08022v2.pdf
[5] https://openreview.net/pdf?id=H1hoFU9xe