Concealment Charm: Generating Steganographic Sequential Data using Generative Adversarial Nets (LeakGAN)

Nurpeiis Baimukan[1], Quanyan Zhu[2]

1. Undergraduate Researcher, NYU Abu Dhabi 2. Project Advisor, New York University

PROBLEM:

- How to conceal a message in sequential data (texts and scripts) is important for covert online communication and protection of intellectual properties.

AIM:

- Develop steganographic solutions for sequential data to (1) circumvent totalitarian censorship and (2) protect intellectual property (textual data as case study)

SOLUTION:

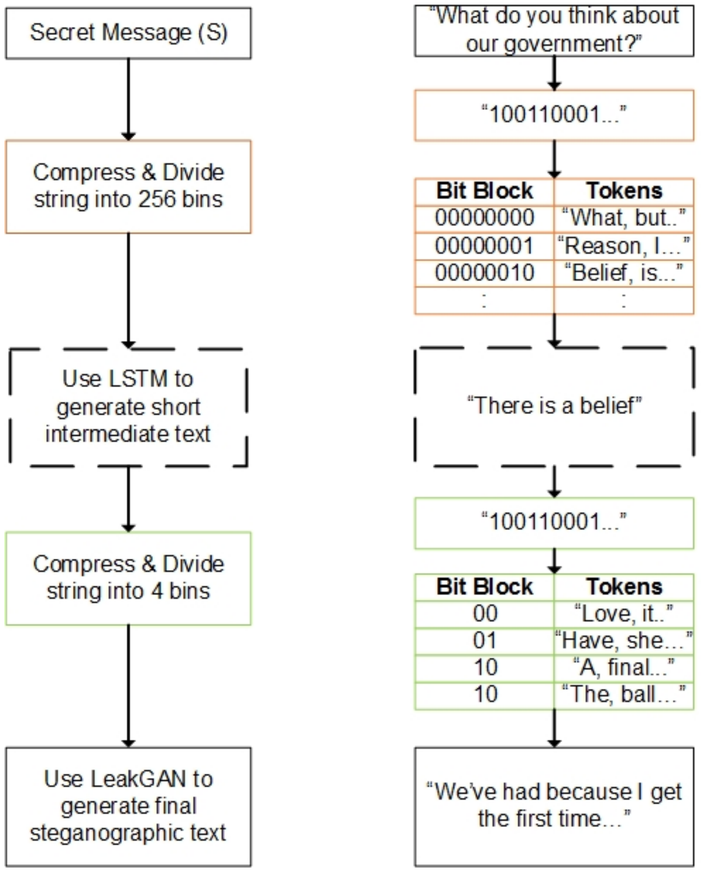

Figure 1: Double Layer Steganographic LeakGAN system

Double Layer of Encoding addresses **DIFFICULTY OF EXTRACTION** of secret message, whilst LeakGAN model copes with **DETECTABILITY** when generating longer sequences

Take a picture to learn more about the project

RESULTS & DISCUSSION:

- LeakGAN Model addresses (1) exposure bias associated with LSTM, (2) non-informativeness, (3) sparsity issues associated with sequential GAN models [1].
- The next word is selected based on the highest probability and the restrictions set by bit block: $P[x = W_j] = 0$ for $j \notin B$ [2].

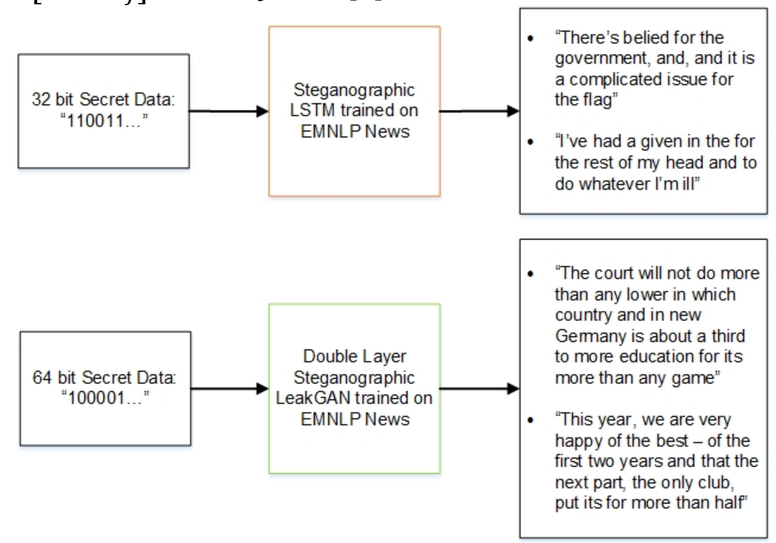

Figure 2: Comparison of Double Layer Steganographic LeakGAN and Steganographic LSTM systems

FUTURE WORK:

- Integrate encoder-decoder architecture to generate context specific steganographic data
- Evaluate the text against human judges & classifiers used in real messenger systems, such as WeChat
- Apply system for generating software scripts

WORKS CITED:

[1] Jiaxian Guo, Sidi Lu, Han Cai, Weinan Zhang, Jun Wang, and Yong Yu. 2017. Long Text Generation via Adversarial Training with Leaked Information. arXiv preprint arXiv:1709.08624.

[2] Fang, T., Jaggi, M., Argyraki, K. 2017. Generating steganographic text with LSTMs. In: ACL Student Research Workshop 2017. Number EPFL-CONF-229881

ACKNOWLEDGMENTS:

The authors thank NYU Tandon School of Engineering's Office of Undergraduate Academics for generous funding of the project

NYU TANDON SCHOOL OF ENGINEERING