



GANGRENE

Generative Adversarial Networks, Generating Robust Encodings for Network Exchange

Hiding in the Features

GANGRENE

Hiding in the Features

OVERVIEW

GANGRENE is a proof-of-concept steganographic capability based on an emerging way of training neural networks known as Generative Adversarial Networks (GANs). It is a medium-agnostic steganography framework for embedding messages in features rather than noise developed under internal research and development. For example, if the medium is a face, the GAN learns to embed messages by slightly altering the features of the face (e.g., opening the mouth, closing the eyes, changing the hair color).

Research Methodology

Assured Information Security (AIS) focused the proof-of-concept on images of faces as GANs are often targeted at images and image datasets are readily available. The team developed three deep neural networks that train in concert to embed within a medium (targeting 0.2 bits per pixel), detect altered instances of the medium, and decode messages.

Results

The GANGRENE framework is able to encode messages at a rate of 0.25 bits per pixel with 99% decoding accuracy with no visible image degradation. AIS is working to extend the framework to incorporate other mediums (e.g., network packets) and make the models robust to transforms that occur in the wild or are designed to break steganography techniques.

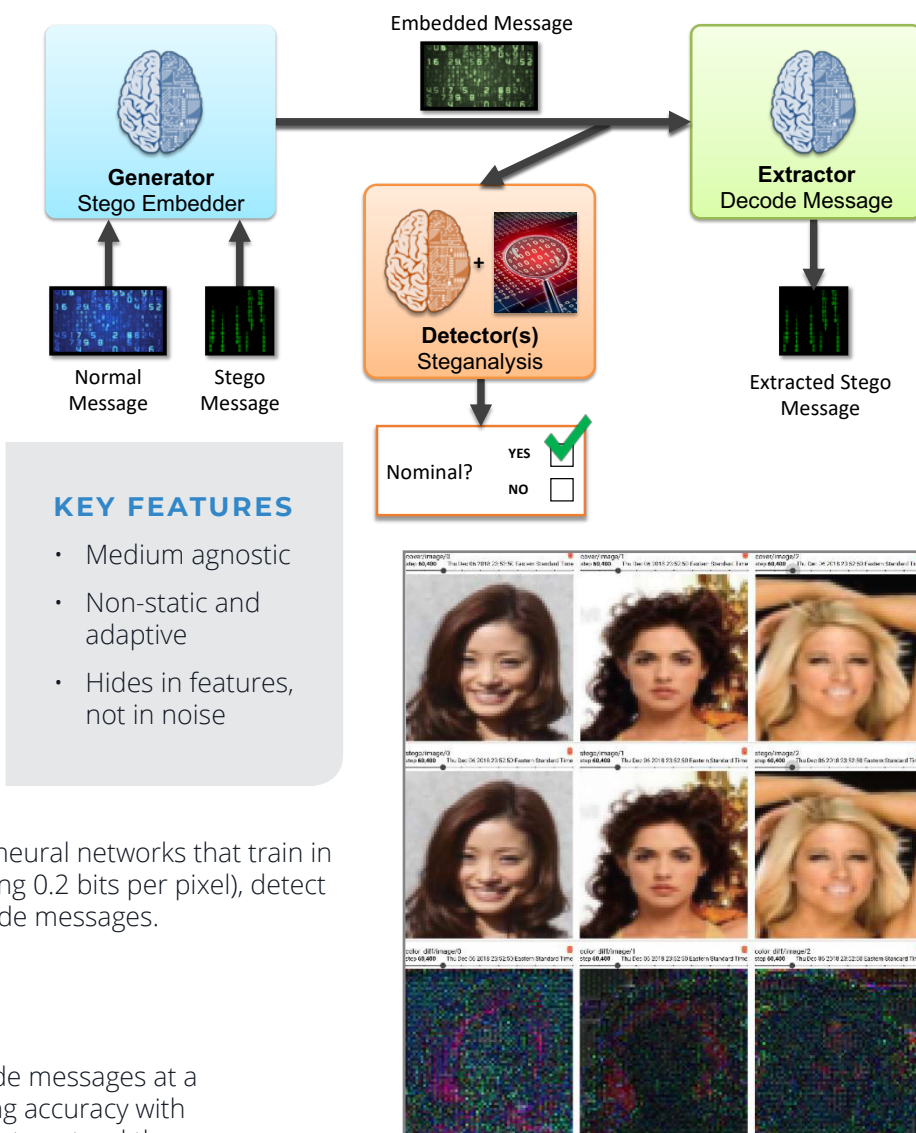
ABOUT AIS

AIS is a cyber and information technology company that plays a leading role in supporting critical cyber operations for the United States Department of Defense and Intelligence Community. AIS employs cyber engineers and scientists throughout the United States.

New York • Colorado • Georgia • Oregon • Massachusetts • Maryland • Virginia

Assured Information Security • 315.336.3306 • WWW.AINFOSEC.COM

Copyright © 2019 Assured Information Security, Inc. All rights reserved.



GAN-based steganographic results: Original cover instances of human faces (top). Processed instances with embedded steganographic messages (middle). RGB differences between original and steganographic images (bottom).

FOR MORE INFORMATION

bd@ainfosec.com

