CryPic: A Web App for Securely Disguising Messages as Pictures

Brendan Van Allen

Marist College, Poughkeepsie, NY

brendan.vanallen1@marist.edu

Abstract. TODO

Introduction

Cryptography and steganography are separate disciplines that have the same goal: to conceal information from third parties. Cryptography achieves this goal by encrypting the information, rendering it incomprehensible even if the information is transported in plain sight. Much of cryptography is grounded in mathematics and takes advantage of modern technology's inability to efficiently solve mathematically complex algorithms. On the contrary, steganography achieves the goal by concealing information as some other form of data, and relies on humans being relatively naive.

Each of these disciplines have vulnerabilities that are not present in the other. In cryptography, encrypted messages are unreadable to the human eye, but this may make an important message stand out amongst plaintext messages. If a malicious third party comes into possession of a message that is encrypted with a relatively weak algorithm, or also obtains even part of the key for a strong algorithm, it could take as little as a few minutes to crack it due to the abundance of resources available for nearly all major encryption techniques. Steganography does have its fair share of resources pertaining to it, but is not nearly as widely studied as cryptography. Furthermore, messages hidden using steganography are generally

indistinguishable from other information. However, since these messages are hidden in plain sight, it only takes one cunning individual to uncover the information.

The goal of creating CryPic was to combine cryptography with steganography in a way that is easily accessible, highlights the advantages of both disciplines, and uses each one to overcome some shortcomings of the other. Concealing the message as an image prevents it from drawing attention to itself, while the encryption protects the message even if it is able to be extracted from the image.

Related Work

The idea of combining cryptography and steganography is not novel, and is the subject of a number of publications (see references). The majority of the previous body of work in this area is aimed at large-scale implementations that protect highly sensitive information. CryPic takes a simpler approach that targets normal communications amongst regular people. While this application is not intended to protect critical information such as nuclear launch codes, it does provide an easily accessible way for anyone who wishes to add an additional layer of security other than cryptography or steganography alone.

Methodology

The process CryPic uses to combine cryptography with steganography is not actually a combination, but rather uses each approach in sequence. The message received from the user is first encrypted using AES to produce ciphertext. This ciphertext, along with the encrypted key, is then put into an algorithm that converts each character to a value in the range 0-255 that represents a grayscale pixel. These values are then used to create a grayscale image which is able to be downloaded by the user and transported to the recipient. In order for a recipient to view the message, CryPic simply reverses the process by extracting the pixel values from the image, converting these values back to ASCII characters, and then decrypting the ciphertext.

Present State

My early work on the application was aimed at getting the frontend to be presentable, while building the foundation of research and knowledge to develop the backend. As of this writing, the web interface of the application is nearly completed aside from some minor

changes. The user is able to input their message and key, but the backend is not connected just yet. On the backend, the application is able to encrypt and decrypt messages using AES, but the conversion of the ciphertext to values to be used for pixels is still under development. The code for creating an image from these pixel values is complete, but is yet to be properly tested due to the previous step still being developed.

Remaining Work

The following are features/tasks that remain to be completed:

- Conversion of ciphertext to pixel values (and the reverse conversion)
- Testing of image creation
- Connecting the backend to take input from the UI and display the created image
- Creation of webpage for recipient to decode message
- Thorough and rigorous testing of all components
- Code cleanup and comments

References (to be cleaned up)

https://www.researchgate.net/publication/322477779_Combining_Cryptography_and_Steganography_for_Data_Hiding_in_Images
https://www.researchgate.net/publication/322077813_Cryptography_and_Steganography_New_Approach