SECRET

A parallel approach to image stenography

INTRODUCTION

The project aims to implement parallel processing for stenographic embedding using CUDA technology. The primary objective is to leverage the power of GPUs for high-performance computing tasks and accelerate the execution time of computationally intensive algorithms.

HOW IT WORKS

- This program allows users to input a message and a 4-digit passcode. The algorithm takes the thread ID and passcode to generate a unique hash value, which determines which pixels will be modified.

- Each thread is responsible for each character. Specifically, it modifies 8 consecutive pixels in a row to encode a single character of the message.

- Additionally, the code generates a second passcode, which is used to extract the encoded message from the modified pixels.

AND EXACTLY THE OPPOSITE TO DE-EMBED

Even if one of the passwords are wrong, the output will be complete garbage. Only both keys together can unlock the SECRET.

THE GOALS

01

The new image must be absolutely identical to the original image. Image analysis tools must not flag this image as tampered.

To accomplish this we use a hash to generate a random 256bit code of which one byte is interpreted as a starting pixel. To further bypass detection we modify 8 bits for a single character thereby reducing the change per pixel. And further more, we modify different layers (ie. R G B A) to evade detection.

02

Any wrong password, even a small change must not reveal the original message.

To accomplish this we use SHA256 on top of our previous hash to generate a completely random but consistent 256bit code of which one byte is interpreted as a starting pixel.
SHA is designed in a way to cause huge changes in the hash for even the slightest change in the seed.

Does it work?

Let's look at the demo.

FUTURE WORKS

- Implement a stronger algorithm that utilises many more pixels in a more complex way to ensure:
    1. Minimal modification traces
    2. Impossibility during brute force attacks

- More user-friendly in the way that they need only remember a single password which includes all necessary information for decoding.