Henry Post

ITMS 428

Data in Transit:

Ensuring integrity and confidentiality

Contents

[Steganography 2](#_Toc526085809)

[Upsides 2](#_Toc526085810)

[Downsides 2](#_Toc526085811)

# Steganography

Steganography is the process of encoding information into images, and sometimes text.

The information encoded doesn’t necessarily have to be encrypted in any way, and the definition of “encoding” here is intentionally vague. You can implement steganography in any way you like!

## Upsides

The upside of using steganography is that it can be hard to determine whether or not any data is actually inserted into an image or not, depending on how you encode the information.

It can also be used to transport encrypted or secret information that isn’t immediately recognizable as actually being encrypted information.

If you live in a place where encryption is illegal or a bad idea to use, steganography can be a good choice if you don’t want the fact that you’re using encryption to be detected.

## Downsides

If you have a copy of the original image, or know how to spot extra data in-between RGB values in PNGs, JPGs, or GIFs, then you can tell if an image has been tampered with.

In addition to this, relying on, perhaps, a custom encoding algorithm or some other obscure method to encode your information will only work as long as anyone else doesn’t either:

* Figure out how to extract the data, or
* Reverse-engineers your algorithm.

Relying on the obscurity of your algorithm is called **security through obscurity**, and is discouraged as a single security method.

Rather, one should encrypt the data as well as encode it into an image with a sufficiently strong encryption algorithm.