Steganography

P2-project
Group A325a
Software
Aalborg University
May 24, 2016

AALBORG UNIVERSITY
STUDENT REPORT

Første Studieår v/ Det Teknisk-Naturvidenskabelige Fakultet
Byggeri og Anlæg
Strandvejen 12-14
9000 Aalborg
http://www.tnb.aau.dk

Title:

Steganography

Project:

P2-project

Project period:

February 2016 - May 2016

Project group:

A325a

Authors:

Anders L. Jakobsen
Andreas N. Jensen
Matias R. Jensen
Rasmus Jespersen
Simon N. Linnebjerg
Theis E. Jendal
Thomas B. Andersen

Supervisor:

Søren Enevoldsen

Pagecount: TODO
Appendix: TODO
Finished 24-05-2016

Abstract:

Synopsis

Preface

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam neque augue, tincidunt id augue at, mollis bibendum felis. Vestibulum ultrices nisi at tortor venenatis, nec ultrices justo pulvinar. Nam non iaculis metus, et consequat lectus. Sed vestibulum dui dolor, quis auctor orci posuere non. Aenean commodo pulvinar augue, eu aliquam sapien iaculis at. Sed eget vestibulum risus, vel viverra justo. Pellentesque ut lacinia dui, vel vestibulum nisi. Sed imperdiet consectetur turpis, id lobortis mi viverra sit amet. Ut quis aliquet nisi. Quisque dolor quam, efficitur quis aliquet eget, commodo consequat tellus. Morbi tincidunt ipsum sit amet velit pretium blandit varius non diam. Nam vitae purus tempus, auctor justo in, malesuada tortor. Donec nulla mauris, faucibus id diam et, finibus maximus orci. Aenean euismod maximus odio, a molestie urna cursus id. Maecenas congue ut sapien blandit tristique.

Duis est purus, lobortis eu ex scelerisque, viverra rhoncus risus. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec dictum augue et arcu volutpat ullamcorper. Nulla suscipit eget sem sit amet porta. Praesent consectetur tellus in eros sagittis, id rutrum augue molestie. Nam lobortis massa eu dapibus malesuada. Etiam id velit commodo neque maximus sollicitudin. Maecenas finibus cursus orci, eu fermentum lectus pharetra at. Pellentesque ornare, orci sed ultrices maximus, risus nisi posuere orci, in finibus urna nisl sit amet mi. Ut id accumsan quam. Vivamus porta sem sit amet aliquam hendrerit. Vivamus sagittis magna porttitor hendrerit volutpat. Integer dolor massa, ullamcorper vel arcu euismod, viverra dapibus lectus. Sed sodales porta magna, non pretium risus aliquet vitae.

Contents

1 Project description

Part I

Theory

Introduction 2

Analysis of stakeholders 3

To enable a proper definition of a problem to be solved, it is necessary to examine the stakeholders in question, in regards to steganography. As such the following analysis will cover two major areas of interest. The interest in using steganography, and the interest in discovering steganography using steganalysis. These can be seen as opposing, but not mutually exclusive interests.

Steganography users have an interest in hiding information, this information can be applied in many areas, and has a usefulness for not only personal or criminal use, but also for government or corporate offices, where secret information can be sent with reduced risk of unauthorized interception. This information could range from classified information such as state secrets to simply private information such as citizens taxes.

Steganalysis users have an interest in discovering hidden data, this is mostly done with statistical analysis of the data structure in question, and is mainly used by governments or corporate offices. This may heighten a nation's or corporate office's security, and make them able to preemptively make decisions to help their own interests such as increasing security based on intercepted messages and thus prevent an attack.

The stakeholder analysis will be a basis for further research, as different parties have different requirements to a potential steganography program.

3.1 Privacy advocates

Some steganography stakeholders are difficult to place in a specific group. Privacy advocates, for lack of a better name, are those who want to protect themselves from prying eyes, whether those are government bodies, criminals with ill intentions or simply other common people. As such, a subset of these advocates may be referred to as IT-activists, as their sole intention with steganography and cryptography is to counter mass surveillance. With that said, their interest in steganography is obviously broad. Some of these people may have an interest in hiding certain files on their file system, while others may simply use it to send messages to their friends. The motivation for these groups may seem vague or difficult to understand for somebody who does not care about privacy, but the matter is obviously quite important for the privacy advocates.

An argument often used against this group is the 'nothing to hide' argument. People who support this argument will argue that mass surveillance does not threaten the privacy of individuals, unless government agencies uncover illegal activities by this individual, in which case they don't have the right for privacy. On the other hand, privacy advocates will argue that the argument implies full trust in the state, which they argue can be hard

to assume, even in fully developed nations. Nonetheless, some people want to hide from criminals trying to misuse their personal information, and tools like steganography and cryptography can be useful in this scenario.

Analysis of technologies 4

4.1 Least Significant Bit method

A commonly used method in digital steganography is the Least Significant Bit (LSB) method. The basic principle of this method is to make small changes to a large amount of data. LSB is useful in data formats where small change don't cause big differences. Embedding hidden messages in text would for example be a bad idea, as changes would be apparent, but on an image such changes may not be apparent. In a lossless image format like PNG (see **??**), the decompressed data is represented as a 2D matrix of pixels. Depending on the pixel format (sRGB, aRGB or perhaps even grayscale) each pixel has a set amount of color channels, where each value is a byte (8 bits), which determines the intensity of the color channel on that specific pixel. Of course the bit depth is not necessarily always 8 bits, but this is the case in most images shared over the internet. The purpose of the LSB method is to change the least significant bit in each of these bytes, and perhaps even the second least significant bit as well. This means that the decimal value may only change by 1 if modifying one bit and by 3 if modifying two least significant bits.

For example, say we want to embed the character '*****' in a message. This ASCII character has a decimal value of 42, which can be represented as an 8-bit binary number:

$$00101010 \tag{4.1}$$

Since this message is 8 bits long, we would need 8 bytes when modifying one bit and 4 bytes when modifying two bits. In the former case, this means that we would need two aRGB pixels, as this gives us 2 * 4 bytes to hide our message in. For example, let's say we want to hide our image in the two pixels:

$$\begin{array}{cccc} 11111111 & 01001111 & 10110000 & 10000111 \\ 11111111 & 10010110 & 10001110 & 10000001 \end{array} \tag{4.2}$$

With the LSB method, we now need to look at the least significant bit in each of these bytes, and negate the bit if it does not correspond to the bit we want to insert. When the message is embedded in the original pixels, the produced result is:

$$\begin{array}{cccc} 1111111\mathbf{0} & 0100111\mathbf{0} & 1011000\mathbf{1} & 1000011\mathbf{0} \\ 1111111\mathbf{1} & 1001011\mathbf{0} & 1000111\mathbf{1} & 1000000\mathbf{0} \end{array} \tag{4.3}$$

The embedded message can then be extracted by simply combining each least significant bit of the 8 bytes. After doing this, we end up with the message seen in Equation 4.1.

When comparing the pixel values of a modified image (now referred to as a stego-image) and the original image, the change is clear on the bit/byte level, but not be apparent to a

human comparing the two images. This means that LSB is prone to steganalysis (see **??**). With the stego-image and original image in possession, it is trivial for a piece of software to detect that one of the images have been edited. In addition, the LSB method will typically increase the size of the image, since adding noise to the least significant bits increases the amount of colors and can affect lossless compression used in formats such as PNG.

Bibliography