Alex Johnson

Computer Security: Final Project Proposal

Title: “An Implementation and Comparison of Basic Image Steganography Techniques”

Why I chose Steganography?

I chose to research and implement image basic image steganography because the idea of being able to hide something very important and top secret in plain sight was very interesting to me. Upon further research I discovered that not only are short messages hidden in images, but one can hide an entire file of data in an image without the image looking any different to the human eye. This is where I got really pulled into the subject of steganography, and eventually found out that there are numerous applications, and methods for implementing image based steganography. After discovering the capability of image-based steganography, I decided that implementing it on my own seemed like an excellent choice for a final project.

Overview of Steganography

Steganography is a Greek word that means covered writing. It refers to writing a secret message out, and using some sort of method, cover the secret message in a way that only the intended recipient knows how to uncover and read the original message. Use of various steganographic methods dates back to ancient Greece, where noblemen would shave the scalps of their slaves, and tattoo a secret message onto the back of their head. Once the hair grew back, the message was hidden, and the slave was sent off to the intended recipient of the message. There is also evidence that suggests steganography was used by the German military during World War II. Steganography has had many applications and methods of use throughout history, although it has mostly been used to hide secret messages.

With the advancement of computer processors and computer technology, steganography has become a growing field of research when it comes to computer security. Perhaps the more obvious use of steganography is simply hiding a message in a digital image (although it is not actually very simple). However steganography can be seen all over the place when it is used to show ownership over a picture or video. Major television channels and professional photographers used steganography to add watermarks to their material, essentially putting a fingerprint on their pictures or videos, which is very difficult to remove. The point of doing this is so that no one can take the content, put it elsewhere and falsely claim it as his or her own.

It is easy to see how useful steganography can be in the real world both for sending secret messages undetected, and for proving ownership over some form of visual media. As research in the field of steganography grows, so does the research in breaking

steganographic methods. For this reason, the methods that work securely, efficiently, and effectively are very complex. There are three main categories that a steganographic method can fall into, first being Spatial Domain Steganography. Spatial Domain methods deal with handling the individual pixels of the cover image (image designated to hide the message). Typically the Least Significant Bit or LSB is determined for each pixel, and then this is swapped out for some bit of the secret message. By substituting for the LSB the overall value of the pixel is not changed by very much, and it turns out that the human eye cannot detect such an insignificant change to the picture even though it may be happening to every pixel in the picture.

The second category of steganographic methods is Frequency Domain Steganography, which hides the secret message or data in significant areas of the image, which helps prevent against compression, cropping, or image processing attacks. Frequency Domain methods are known to be generally more secure than Spatial Domain methods, but they are usually also more complex and thus can be less efficient. The final category is Adaptive Steganography, which is seen as a combination of both Spatial Domain and Frequency Domain. In Adaptive methods, certain statistical features are determined about the picture, and these features are then used to determine where in the picture the changes will be made in order to hide the secret message or data.

It is clear that the applications of steganography are fairly far reaching when it comes to computer security, and the amount of methods to implement steganography is also large. While there is not determined best way to implement steganography, the goal of this implementation/experiment project is to determine what methods work best under what conditions, given the desired levels of security and efficiency.

Steganography Project Skeleton

For this project I plan on implementing two different methods of steganographic message embedding. One of these methods will fall under the Spatial Domain category, and the other will fall under the Frequency Domain category. With each of these steganographic methods I hope to capture the general characteristics that apply to their respective categories. For example with the Spatial Domain method, I will be using some form of LSB substitution, and for the Frequency Domain method, I will likely be breaking the cover image into blocks to prevent against a cropping attack. After completing the implementation of these two methods I will compare the efficiency of each, and then try to determine how secure each method is.

Determining which method is more efficient is simply running the embedding processes for each and figuring out which method completes first. Determining which method is more secure however, will likely take some research to understand the different kinds of attacks that work or do not work effectively on each method. Once I have completed my review of each method based on efficiency and security, I will be able to suggest what method, or category of methods to use depending on whether security or efficiency is the overriding concern.

If time permits, I would like to do some experimentation with implementing a program that adds a digital watermark or fingerprint to an image. I hope to not only be able to write a program that adds a customized watermark to any image, but also test and see how difficult it may be to get the original image without having the watermark. In the end of this project, I hope to have a deep understanding of how steganography works, and know how to implement various methods of steganographic data embedding.

Resources

1. https://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS5/Steganography.pdf

2. http://www.rroij.com/open-access/a-review-on-steganographymethods.php?aid=42238

3. http://www.sciencedirect.com/science/article/pii/S0165168409003648

4. http://repository.root-me.org/St%C3%A9ganographie/EN%20-%20Image%20Steganography%20Overview.pdf

5. http://opencv.org/about.html

6. https://www.zurich.ibm.com/~cca/papers/stego.pdf

7. http://easybmp.sourceforge.net/steganography.html

8. http://www.ijcttjournal.org/Volume11/number-4/IJCTT-V11P131.pdf

9. https://arxiv.org/pdf/1506.02100.pdf

10. https://users.ece.cmu.edu/~adrian/487-s06/westfeld-pfitzmann-ihw99.pdf