|  |
| --- |
|  |
| Video Steganography: Hiding Video Sequences |
| CSE509: Digital Video Processing |
|  |
| **Aaron Gubrud**  **Jose Trigueros** |
| **25 April 2012** |

Table of Contents

[Introduction 1](#_Toc323060772)

[Related Work 1](#_Toc323060773)

[System Overview 1](#_Toc323060774)

[Results 1](#_Toc323060775)

[Discussion 1](#_Toc323060776)

[Conclusion 1](#_Toc323060777)

[References 1](#_Toc323060778)

[Appendix 1](#_Toc323060779)

# Introduction

The concept of steganography is one that has been around for centuries. Much like encryption its purpose is to take a message and assemble it into a form where - should it be intercepted - the interceptor should not be able to know what the message says. The approaches for encryption and steganography are completely different, however. Whereas encryption takes a given message and performs operations on it such that an interceptor will not be able to read the message, steganography banks on the interceptor not being able to detect the presence of a message at all. Early examples of steganography primarily rely heavily on the transportation medium of the message. One common example is of slave owners in ancient Greek times shaving the head of a slave, tattooing a message on their scalp, allowing the hair on the slave’s scalp to grow back, and then sending them to deliver the message. In the event that they were stopped, nothing would appear suspicious and they would be sent along to complete their task.

In the present, steganography has applications that are more modern. Taking advantage of least significant bits of pixel data in an image file can allow for storage of a message. Two common methods for this type of steganography are applied in the spatial and frequency domains. In the spatial domain, the last few bits of each pixel value within an image can store part of a message. In the frequency domain, a discrete cosine transform can be performed on regularly-sized blocks of a “carrier image”[[1]](#footnote-1) and the coefficient matrix created by the transform creates hiding spots in coefficients that are less important to image structure and quality. These are both simplified explanations but capture the basic principles behind their respective strategies.

When it is said that a message can be hidden within a carrier image, the message itself can be anything from encoded characters in a sequence to entire “seed images”[[2]](#footnote-2). Logically, there is a tradeoff between how much information can be hidden and the visible degradation in image quality of the carrier. This guides choices for both carrier and seed sizes.

# Problem Statement

Since steganographic principles can be applied within digital imaging, it should follow that similar techniques can be applied within digital video. Moreover, it should be possible to hide an entire seed video sequence within a carrier video sequence. Two approaches to this problem will be attempted: one working within the spatial domain and the other working within the frequency domain.

# Related Work

# System Overview

# Results

# Discussion

# Conclusion

# References

# Appendix

1. Carrier image: image in which a message will be stored. [↑](#footnote-ref-1)
2. Seed image: image which will be hidden within the carrier image. [↑](#footnote-ref-2)