SECRET KEY ESTIMATION IN SEQUENTIAL STEGANOGRAPHY

By

Shalin Trivedi

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
MASTER OF ENGINEERING IN ELECTRICAL ENGINEERING
AT
STEVENS INSTITUTE OF TECHNOLOGY
HOBOKEN, NEW JERSEY
DECEMBER 2003

STEVENS INSTITUTE OF TECHNOLOGY
DEPARTMENT OF
ELECTRICAL AND COMPUTER ENGINEERING

The undersigned hereby certify that they have read and recommend to the Faculty of School of Engineering for acceptance a thesis entitled "**Secret Key Estimation in Sequential Steganography** " by **Shalin Trivedi** in partial fulfillment of the requirements for the degree of **Master of Engineering in Electrical Engineering**.

Dated: December 2003

Advisor: _____
Dr. R. Chandramouli

Reader: _____
Dr. Yu-Dong Yao

STEVENS INSTITUTE OF TECHNOLOGY

Date: **December 2003**

Author: **Shalin Trivedi**

Title: **Secret Key Estimation in Sequential Steganography**

Department: **Electrical and Computer Engineering**

Degree: **M.E.E.E** Convocation: **May** Year: **2003**

Permission is herewith granted to Stevens Institute of Technology to circulate and to have copied for non-commercial purposes, at its discretion, the above title upon the request of individuals or institutions.

Signature of Author

To My Late Parents.

Table of Contents

Abstract

We define sequential steganography as those class of embedding algorithms that hide messages in consecutive (time, spatial or frequency domain) features of a host signal. This paper presents a steganalysis method that estimates the secret key used in sequential steganography. A theory is developed for detecting abrupt jumps in the statistics of the stego signal during steganalysis. Stationary and non-stationary host signals with low, medium and high SNR embedding are considered. A locally most powerful steganalysis detector for the low SNR case is also derived. Several techniques to make the steganalysis algorithm work for non-stationary digital image steganalysis are also presented. Extensive experimental results are shown to illustrate the strengths and weaknesses of the proposed steganalysis algorithm.

Acknowledgements

I thank financial support from AFRL and NSF. This material is based on research sponsored by Air Force Research Laboratory under agreement number F306020-02-2-0193 and National Science Foundation under agreement number NSF DAS 0242417. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposed notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Air Force Research Laboratory or the U.S. Government.

I would like to thank my advisor Dr. R. Chandramouli for his constant support and guidance. He provided many hours of his valuable time to help me put my best. I am much obliged to his help throughout my graduate studies.

I thank Dr. Yu-Dong Yao for his inspiration and guidance. He provided me an encouragement when I needed the most. I deeply appreciate Dr. K. P. Subbalakshmi for giving me a chance to prove myself.

I dedicate my thesis to my parents. It was their blessings and invaluable contributions, which lead me to pursue and complete my studies. This is my tribute to their efforts, their sacrifices and their true love.

I am thankful to my grand parents for their interest in my career and their encouragement in my studies. I never forget support and enthusiasm I got from my sisters Amisha and Jigisha. I am indebted to Nischal and Sanjay for their kindness. Though they never helped me in anyway I would like to thank Shravani and Eeti. I wouldn't be able to complete my research without the help of other family members and well-wishers.

Last but not least I would like to thank Vishal and Vishwas for their true friendship, Naitik and Kiran for their support during my bad times, Siva for the nice food, Amol,

Rajesh and Mubashir for all the great parties we had together, Dharmesh and Sharmi for being my friends.

Hoboken, NJ Shalin Trivedi
November 22, 2003

Chapter 1

Introduction

Steganography deals with hiding messages in cover signals. To hide a message, some features of the cover signal chosen using a secret key are slightly modified by the embedding technique. We refer to the message embedding process as *sequential steganography* when the secret key consists of successive features (in some feature space such as spatial domain, frequency domain, etc.) of the cover signal. That is, successive features of the cover signal are chosen for message embedding. There are several popular message embedding algorithms that fall into this category such as the following:

- **Spread spectrum embedding**: Spread spectrum embedding [6],[14] attempt to embed a wideband message carrier signal in the cover signal. The low power carrier produces imperceptibility after embedding. Even though [6] is a watermarking technique, the idea proposed here has been the basis of several steganographic techniques. In [6], message is embedded in the discrete cosine transform (DCT) domain. The DCT coefficients of the cover signal are sorted in order of decreasing magnitude and the message is embedded in certain high magnitude coefficients that are consecutive (sequential) in the sorted DCT coefficient

domain.

- **EzStego**[13]: This technique embeds messages in the sorted palette domain sequentially. It first orders the palette to minimize color differences between consecutive colors. Then, the message bits are sequentially embedded as the LSBs of color indices to the sorted palette.

There are also some advantages in using sequential embedding. For example, some features of digital signals form a natural sequential ordering (such as the magnitude of frequency coefficients), ease of key management, etc. In this paper we primarily deal with digital images as cover medium though the proposed methodology can be easily applied to other types of cover media as well.

The goal of steganalysis is to *break* steganography. As described in [3], steganalysis can be classified into two categories: (a) *active* and (b) *passive*. In active steganalysis the goal is to estimate some parameter(s) of the embedding algorithm or the covert message while passive steganalysis deals with identifying the presence/absence of a covert message or the embedding algorithm used etc. Using this categorization we note that this paper deals with active steganalysis since the aim is to estimate the secret key used by the message embedding algorithm. Steganalysis algorithms test the security of steganographic techniques. Several steganalysis algorithms that operate on spatial or frequency domain have been already proposed.

LSB embedding replaces least significant bit (LSB) of an image by the message bit and seems to be the most popular spatial domain embedding algorithm. Several techniques are available to break the LSB embedding such as RS staganalysis [9] and Chi-square attack [22] on Pairs of Values (PoVs). RS steganalysis divides pixels groups in regular, singular and unchanged groups with negative and non-negative

masks and is based on the empirical observation that regular (and singular) groups with non-negative mask and regular (and singular) groups with negative masks are equal. It is seen that LSB steganography disturbs this balance. This technique is reliable in detecting the absence/presence of the message. In [22], a statistical attack is applied to an embedding technique in which a set of Pairs of Values (PoVs) are flipped into each other to embed message bits. The basic hypothesis is that before embedding, the two values from each pair are distributed unevenly in the cover image. But after embedding, the occurrences of the values in each pair will have a tendency to become equal depending on the message length. Statistical learning theory based steganalysis is also gaining interest [7],[1]. These methods use a large training set of images to learn the parameters or values of certain features before and after embedding. Once this training based classifier is designed it is then used to test images for the presence of stego messages. We refer to [10] for a good overview of the current steganalysis methods.

There are several important issues to be considered to develop good steganalysis algorithms. For example, from the above discussion we note that the steganalysis techniques in the literature are of two extremes: those that consider statistics of each individual image and those that average the statistics over a large training data set. These two approaches have their pros and cons. When using individual image statistics, the statistical estimates more accurately reflect that individual image's characteristics. But, images being non-stationary in nature, estimating these statistics reliably is a challenge. On the other hand, by averaging the statistics over a large training set, the non-stationarities are in a sense averaged out, but the estimated statistics may not accurately reflect the properties of an image that was

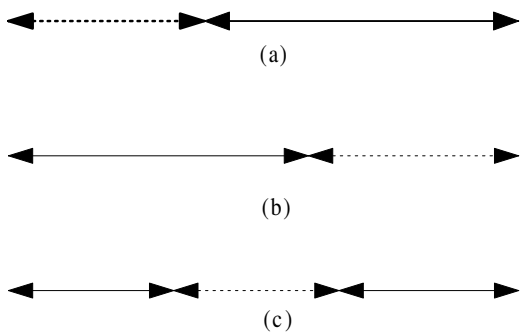

Figure 1.1: Example scenarios of sequential steganography. Dotted lines indicate locations where a message is embedded.

not originally part of the training data. Another important issue is estimating the steganographic capacity or safe embedding rate. This is the maximum message size that can be embedded such that a steganalysis algorithm will not detect it. Clearly, this embedding rate is a function of the steganalysis detector and its parameters. Not much theoretical analysis can be found in this area with the exception of [4] and [5].

In this paper, we discuss a mathematical formulation of steganalysis to detect sequential steganography. The formulation is based on detection of abrupt changes in stochastic processes [16]. To our knowledge the first attempt in this direction for steganalysis was proposed in [19]. Several sequential message embedding scenarios are shown in Fig. 1.1. Fig. 1.2 shows the abrupt jump in the statistics for Fig. 1.1(b). Fig. 1.2 shows two examples: when the variance and mean of the host signal are changed by the embedding algorithm. We see that the statistics of the stego signal changes abruptly at the boundaries of dotted and solid lines. The magnitude of this change depends on the SNR. A high SNR would induce a higher jump in the

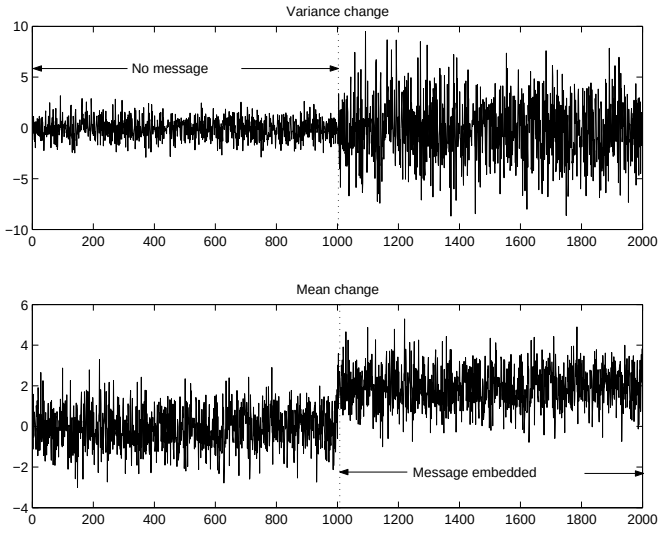

Figure 1.2: Examples of abrupt statistical change in stego signal due to sequential steganography, for the case of Fig. 1.1(b).

statistics thus facilitating more reliable steganalysis. The abrupt jump feature distinguishes sequential steganography embedding from other types of embedding. We show in this paper how this abrupt change in statistics can be successfully exploited by a steganalysis detector. We develop a cumulative sum (CUSUM) steganalysis detector that takes one image sample at a time and decides whether a change point has occurred and therefore estimates the secret embedding key. We handle the problem of low message signal to (host) noise ratio (SNR) (a requirement for imperceptible embedding) in steganalysis using a locally most powerful (LMP) sequential statistical test. We then employ a combination of CUSUM and LMP to exploit the sequential nature of stego embedding algorithm.

This paper is organized in the following manner. We develop the general mathematical theory for the proposed steganalysis scheme in Chapter 2. In Chapter 3,

a steganalysis algorithm for the stationary host signal case is presented. Chapter 4 deals with modifications to the steganalysis detection in Chapter 3 for non-stationary image data hiding. Experimental results and discussion are presented in Chapter 5. Chapter 6 contains some concluding remarks.

Chapter 2

Abrupt Change Detection Based Steganalysis

In this chapter we introduce sequential change detection technique called Cumulative Sum. We will show that steganalysis of sequential steganography is also a change detection problem. Hypothesis are developed to observe the changes in the parameter of interest. The decision thresholds are chosen according to the given values of probability of miss and false alarm.

2.1 Introduction

Consider the sequence of independent random variables $\{y_k\}$ (stego signal) with probability density $p_\theta(y)$ parameterized by θ. In general, θ can be a vector or a scalar. We assume that this parameter value could change due to message embedding after an unknown value of k. Therefore let's say, before the unknown change time, say k_0, the parameter θ is equal to θ_0, and after the change it is equal to $\theta_1 \neq \theta_0$. Thus the message is hidden in y_{k_0} to y_{k_1} and $\{k_0, k_0 + 1, \ldots, k_1\}$ for the secret embedding key which we try to estimate. k_0 can take value in between 2 to a maximum length and

k_1 can take value from k_0 to the maximum length. The problems are then to detect the abrupt change in the parameter θ and to estimate the change time k_0. Let's say H_0 is the hypothesis when there is no embedded message (no change) and H_1 is the hypothesis when message is embedded. That is,

$$\begin{aligned} &H_1 : \theta = \theta_1 \text{ when } k_0 < k < k_1 \text{ (message embedded from } k_0 \text{ to } k_1) \\ &H_0 : \theta = \theta_0 \text{ elsewhere} \end{aligned} \tag{2.1.1}$$

In this formulation, there are several cases to be considered:

- θ_0 **and** θ_1 **values are completely known:** This case arises as a result of Kerchoff's principle where the assumption is that, the stego embedding algorithm is made public and only the secret key is not.

- θ_0 **and** θ_1 **are partially known:** A (noisy) estimate of θ_0 and θ_1 may be obtained using a large training set obtained before and after embedding when the stego embedding algorithm itself may only be known as a black box (e.g., only the executable code of a steganography software may be available.).

- θ_0 **and** θ_1 **are completely unknown:** This is true for applications such as steganographic covert communications where only the stego signal may be available to the steganalysis detector with no further knowledge.

Note that k_0 and k_1 are unknowns in all the three cases.

2.2 Abrupt Change Detection Using SPRT

The sequential probability ratio test (SPRT) for hypothesis testing was first proposed by Wald [21]. Here, a probability ratio test is performed sequentially, i.e., by taking

sample observations one by one. Two detector decision thresholds are used. The test is terminated as soon as the test statistic reaches one of these decision thresholds. Clearly, the number of observations used by the SPRT is a random variable for fixed false alarm and miss error probabilities. It is known [21] that the SPRT consumes the least (average) number of samples to detect a hypothesis among all other hypothesis tests, for fixed false alarm and miss probabilities. For the hypothesis defined in Eq. (2.1.1), and probability density functions ($p_{\theta_i}(y)$), Wald's test statistic with two decision thresholds (A and B) can be shown to be given by,

$$S_1^k \begin{cases} \geq \ln A & \text{decide } H_1, \\ \leq \ln B & \text{decide } H_0, \\ k = k+1 & \text{otherwise.} \end{cases} \tag{2.2.1}$$

where,

$$S_1^k = \ln \frac{p_{\theta_1}(y_1)}{p_{\theta_0}(y_1)} + \ldots + \ln \frac{p_{\theta_1}(y_k)}{p_{\theta_0}(y_k)} \tag{2.2.2}$$

Therefore, the statistical test runs constantly until it reaches a decision. Under certain conditions [21] this test can be shown to terminate w.p. 1. The decision thresholds are defined in terms of probability of false alarm ($\alpha = P(\text{decide } H_1|H_0)$) and probability of miss ($\beta = P(\text{decide } H_0|H_1)$). To simplify notation, $P(H_j|H_i)$ stands for the probability of accepting H_j given that H_i is true, $i = 0, 1$ and $j = 0, 1$.

By neglecting the overshoot over the decision boundaries Wald showed that the optimal decision boundaries are given by:

$$A = \frac{1-\beta}{\alpha} \tag{2.2.3}$$

$$B = \frac{\beta}{1-\alpha} \tag{2.2.4}$$

for a desired error probability pair (α,β).

2.3 CUSUM With Repeated Use Of SPRT

Page [17] first proposed SPRT based repeated hypothesis testing with two thresholds h and $-\gamma$ to detect abrupt changes in a stochastic process. The SPRT is defined by a pair $(\phi, \tilde{N})$ where $\phi(.)$ is a decision function and $\tilde{N}$ is a stopping time. The SPRT is given by,

$$\phi = \begin{cases} H_0 & \text{if } S_1^{\tilde{N}} \leq -\gamma \\ H_1 & \text{if } S_1^{\tilde{N}} \geq h \end{cases} \tag{2.3.1}$$

where the stopping time $\tilde{N} = \tilde{N}_{-\gamma,h} = \inf\{k : S_1^k \geq h \bigcup S_1^k \leq -\gamma\}$, $\gamma \geq 0$ and $h > 0$ are constants. The SPRT test is repeated until $\phi = 1$ and the time at which this happens is called the *alarm time*. $\gamma = 0$ was shown to be the optimal threshold by [18]. Then the repeated cumulative sum based SPRT (CUSUM-SPRT) steganalysis detector using Eq. (2.1.1) is given by,

$$g_k = \begin{cases} g_{k-1} + s_k & \text{if } g_{k-1} + s_k > 0, \\ 0 & \text{if } g_{k-1} + s_k \leq 0, \\ 0 & \text{if } k = 0 \end{cases} \tag{2.3.2}$$

where,

$$s(y_k) = \ln \frac{p_{\theta_1}(y_k)}{p_{\theta_0}(y_k)} \tag{2.3.3}$$

is the log likelihood ratio (LLR). For simplicity we denote $s(y_k)$ by s_k in Eq. (2.3.2). Note from Eq. (2.3.3) that s_i will have a negative drift before change time k_0 (since $p_{\theta_0}(y_k) > p_{\theta_1}(y_k), 1 \leq k \leq k_0$) and a positive drift after the change. That is, the expected value of LLR when $\theta = \theta_0$, E_{θ_0}, will have negative drift and E_{θ_1} will have a positive drift. Compactly we can rewrite Eq. (2.3.2) as

$$g_k = (g_{k-1} + s_k)^+. \tag{2.3.4}$$

It is now not difficult to see that g_k and S_j^k are related as given by:

$$g_k = \left(S_{k-N_k+1}^k\right)^+ \tag{2.3.5}$$

where,

$$N_k = \begin{cases} N_{k-1} + 1 & \text{if } g(k-1) > 0, \\ 1 & \text{otherwise.} \end{cases} \tag{2.3.6}$$

From Eq. (2.3.5) it is clear that main idea of CUSUM is to restart SPRT as long as previously taken decision is in favor of hypothesis H_0 and the alarm time is given by,

$$T_a = \min\{k : g_k \geq h.\} \tag{2.3.7}$$

Also note that N_k starts incrementing as soon as the presence of a hidden message is detected. However, since we want to estimate both the start and end of the secret key, we reformulate the hypothesis test after the first alarm time to search for the end of the secret key.

2.4 Decision Threshold Selection

Fig. 2.1 shows a pictorial representation of the proposed CUSUM-SPRT based steganalysis algorithm. In this figure, the decision thresholds h_0 and h_1 play important roles. These parameters play the role of h discussed in the previous section. h_0 is used to identify the beginning of the secret key and h_1 for the end of the key. Using the same argument as presented in [16], we observe that $h_0 = lnA$ is optimal. Therefore from Eq. (2.2.3) we get

$$h_0 = \ln \frac{1-\beta}{\alpha}. \tag{2.4.1}$$

Once the starting value of the secret key is identified the next step is to compute its ending value. So, we start looking for a negative drift in the statistics.

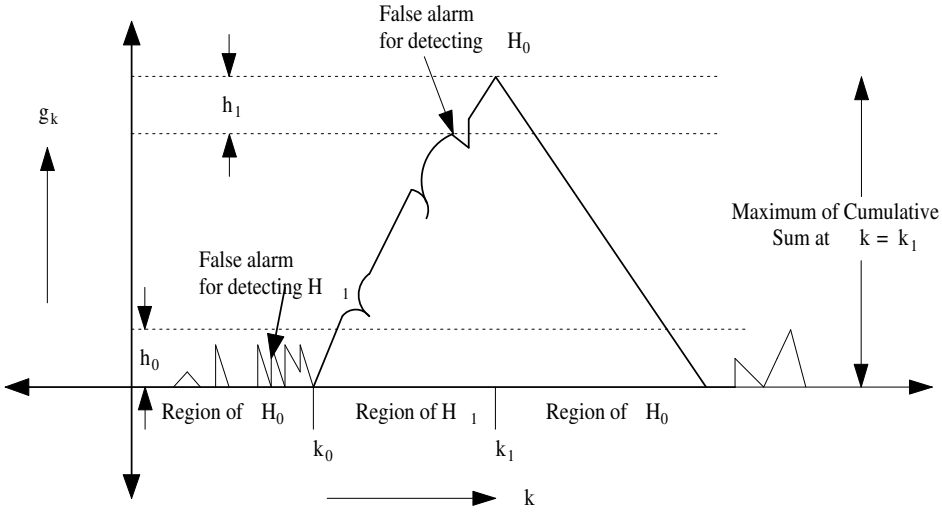

Figure 2.1: Pictorial representation of CUSUM-SPRT based secret key estimation algorithm.

Therefore after detecting the beginning of the message we swap the roles of H_0 and H_1 to detect its end. That is given $g_k \geq h_0$ then H_0**: message present** and H_1**: message absent**. We retain the same notations for false alarm and miss probabilities for simplicity. So we can write the new false alarm and miss probabilities as,

$$\alpha = P(H_1|H_0, g_k \geq h_0) \tag{2.4.2}$$

and,

$$\beta = P(H_0|H_1, g_k \geq h_0) \tag{2.4.3}$$

Then we can show that,

$$P(H_0|H_0, g_k \geq h_0) \geq e^{h_1} \cdot P(H_0|H_1, g_k \geq h_0) \tag{2.4.4}$$

and the approximate value of h_1 by approximating inequalities is given by,

$$h_1 = \ln \frac{1-\alpha}{\beta} \tag{2.4.5}$$

Therefore as shown in Fig. 2.1 once the test statistic g_k is less than $\max_k(g_k) - h_1$ it will detect hypothesis H_0: no message, at that index k. Note that h_1 will be in effect only if the test statistic first crosses the threshold h_0. If there is no such k then end of message will be detected at the last index k.

Chapter 3

Secret Key Estimation in Spread Spectrum Embedding: Stationary Case

After sufficient background developed in Chapter 2, we apply developed theory to the stationary signals in this chapter. Mathematical formulation of spread spectrum embedding is introduced. Different scenarios are developed according to the available information about parameter of interest. Solutions for all the cases including weak signal case are provided.

3.1 Introduction

In this section we derive a CUSUM-SPRT steganalysis detector for secret key estimation in spread spectrum embedding in order to illustrate the method. In this section we assume stationary signals just for illustration. We assume that the message bits modulate the sign of the Gaussian distributed carrier before embedding. Let,

$$y_k = x_k + \rho w_k,\ k = 1, 2, ..., N \tag{3.1.1}$$

where $y_k \in \Re$ is the k^{th} DCT coefficient of stego signal, $x_k \in \Re$ is the k^{th} DCT coefficient of cover signal, $w_k \in \Re$ is the Gaussian distributed message carrier, and $\rho > 0$ is the message strength. Note that if the message length is less than N, then $\rho = 0$ for the corresponding indices. Assume that $\{y_k\}$ and $\{x_k\}$ are independent and identically distributed (iid) random sequences. Also, if $x_k \sim \mathcal{N}(0, \sigma_0^2)$ and $w_k \sim \mathcal{N}(0, \sigma_w^2)$ then $y_k \sim \mathcal{N}(0, \sigma_1^2 = \sigma_0^2 + \rho^2\sigma_w^2)$ assuming x_k and w_k are independent $\forall\ k$. If the embedding key is the set $\{k : k_0 \leq k \leq k_1\}$ then,

$$y_k \sim \begin{cases} \mathcal{N}(0, \sigma_0^2) & k = 1 \text{ to } k_0 - 1, \\ \mathcal{N}(0, \sigma_0^2 + \rho^2\sigma_w^2) & k = k_0 \text{ to } k_1, \\ \mathcal{N}(0, \sigma_0^2) & k = k_1 + 1 \text{ to } N. \end{cases} \tag{3.1.2}$$

Note that this model assumes stationarity of the observations. If this assumption is violated (as it happens in digital images) then some sort of pre-processing may be necessary.

3.2 Known Parameters Case

Suppose that the exact values of σ_0 and σ_1 are known to the steganalyst then the parameter $\theta = \sigma$ is the parameter under test as given in Eq. (2.1.1). Then we can define the following hypothesis test,

$$\begin{aligned} H_1 &: \sigma = \sigma_1 \text{ when } k_0 \leq k \leq k_1 \\ H_0 &: \sigma = \sigma_0 \text{ elsewhere} \end{aligned} \tag{3.2.1}$$

The probability density functions under hypothesis H_0 and H_1 are given by,

$$p_{\theta_i}(y_k) = \frac{1}{\sqrt{2\pi\sigma_i^2}} \exp\left[\frac{-y_k^2}{2\sigma_i^2}\right], i = 0, 1 \tag{3.2.2}$$

and S_j^k can be shown to be,

$$S_j^k = N_k \cdot \ln \frac{\sigma_1}{\sigma_0} + \lambda_{j,k} \cdot \left(\frac{\sigma_0^2}{\sigma_1^2} - 1 \right) \tag{3.2.3}$$

where,

$$\lambda_{j,k} = \frac{1}{2} \sum_{i=j}^{k} \frac{y_i^2}{\sigma_0^2} \tag{3.2.4}$$

By using alarm time T_a in Eq. (2.3.7) and thresholds h_0 and h_1 we can get estimate of message beginning and ending indices k_0 and k_1 as,

$$\hat{k}_0 = \arg\min_k [g_k \geq h_0] \tag{3.2.5}$$

$$\hat{k}_1 = \arg\min_k [\max_k (g_k) - g_k > h_1] \tag{3.2.6}$$

3.3 Partially Known Parameters Case

Suppose σ_0 is known but not σ_1 (the case when σ_0 is unknown but σ_1 is known can be treated using a similar analysis presented in this section). This happens for example when the stego message goes through a noisy channel (attack) that does not affect the first few DCT coefficients. Then these first few DCT coefficients that are not used for embedding (as in [6]) and are not noisy can be used to obtain an estimate of σ_0. Suppose we have partial knowledge about the possible distribution of σ_1 (if the distribution of the noise attack is known) or assume a certain *a priori* distribution (Bayesian), say, $p(\sigma_1)$, then we can use Wald's weighting function [21] to obtain the likelihood ratio (LR),

$$LR = \int \frac{p_{\sigma_1}(y_j, \ldots, y_k|\sigma_1) \cdot p(\sigma_1)}{p_{\sigma_0}(y_j, \ldots, y_k)} d\sigma_1 \tag{3.3.1}$$

where,

$$p_{\sigma_i}(y) = \frac{1}{\sqrt{2\pi\sigma_i^2}} \exp\left[\frac{-y^2}{2\sigma_i^2}\right] \tag{3.3.2}$$

If $\sigma_1 \sim \text{Uniform}(a, b)$ then S_j^k is given by,

$$S_j^k = \ln \sigma_0 + \lambda_{j,k} + \ln \Gamma\left(\frac{N_k - 1}{2}\right) - \ln(2\lambda_{j,k}^{\frac{N_k-1}{2}}) - \ln(b-a) \tag{3.3.3}$$

where $\lambda_{j,k}$ and N_k are given by Eq. (3.2.4) and Eq. (2.3.6), and Γ denotes gamma function, namely, $\Gamma(n) = (n-1)!$. This result is derived in Appendix I. In simulations we use the approximation [15] $ln\Gamma(z) = \ln(z) + rz + \sum_{n=1}^{\infty}[ln(1 + z/n) - z/n]$ where $r = 0.5772156$ is the Euler-Mascheroni constant and $\ln(\Gamma(0)) = 0$.

3.4 Completely Unknown Parameters Case

One way to handle this case is to put two a priori probability distributions one for each of the unknown parameters under the two hypotheses and derive results similar to the partially known parameters case. We analyze this case for the case of digital images in a later section.

Performance of the steganalysis detector for the partially known parameter case is presented now. The length of the host sequence N was taken to be 10000 and a message carrier of length 2000 was sequentially embedded. $\alpha = \beta = 0.001$ was chosen as parameters for the steganalysis detector. Plots of the test statistic g_k by computing S_j^k from Eq. (3.3.3) are shown in Figs. 3.1, 3.2 and 3.3 for different secret keys. "Input" in these figures denotes the input to the embedding algorithm (secret key) and "Output" denotes the estimated secret key by the steganalysis detector. As seen in Fig. 3.1 the message is embedded at the very beginning of the host signal (from k=1 to 2000). We see that the proposed steganalysis algorithm detects the

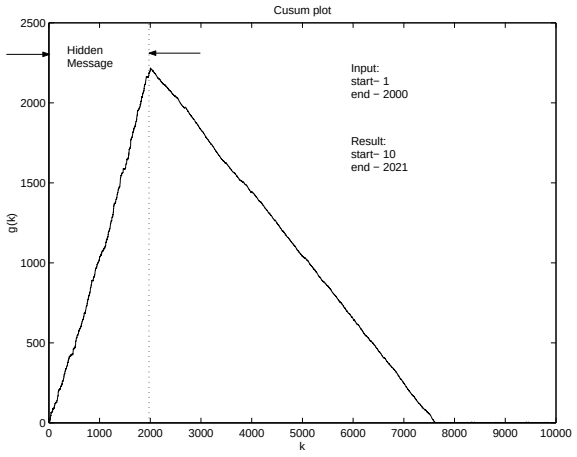

Figure 3.1: Steganalysis detection statistic when $\rho = 2$ and secret key consists of the beginning of the host signal.

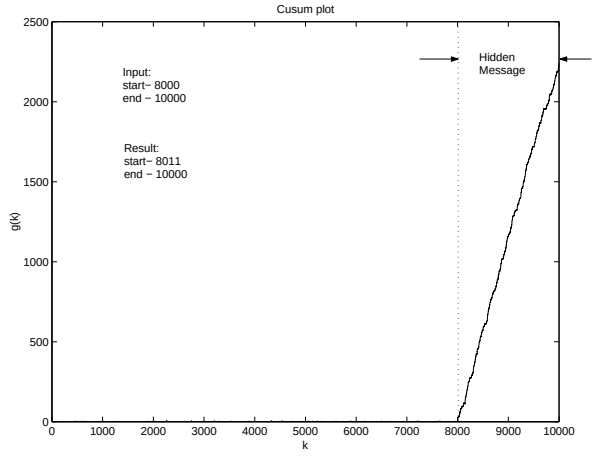

Figure 3.2: Steganalysis detection statistic when $\rho = 2$ and secret key consists of the ending of the host signal.

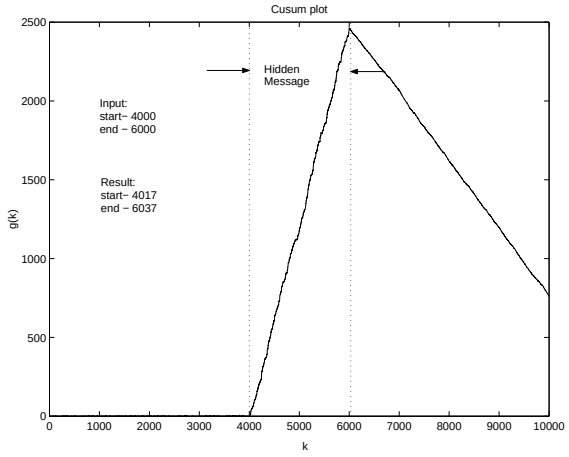

Figure 3.3: Steganalysis detection statistic when $\rho = 2$ and secret key consists of the middle portion of the host signal.

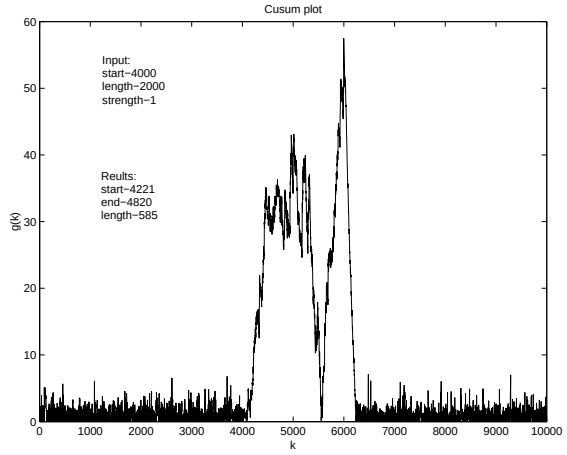

Figure 3.4: Steganalysis detection statistic for $\rho = 1$.

message start and end locations to be 10 and 2021. That is, the first 10 locations are missed and 21 locations are detected falsely as message carrying symbols. By changing the values of false alarm and miss probabilities a change in this performance can be observed. Similar performances are seen in Fig. 3.2 and Fig. 3.3. From these figures we conclude that under stationarity and reasonable SNR, the propose secret key estimation algorithm performs well.

Now, Fig. 3.4 show the performance of the steganalysis detector for $\rho = 1$. We see from this figure that the accuracy of the estimated secret key is low. This is because $\rho = 1$ corresponds to a lower SNR case and we know that the smaller the SNR the harder is the steganalysis detection process. But, most of the steganographic embedding algorithms use a small value for the message strength to achieve imperceptibility. In fact, in image spread spectrum embedding, [6] uses $\rho = 0.1$. For steganalysis algorithms to work reasonably well in such low SNRs we have to design it specifically for these smaller SNR values as discussed in the next section.

3.5 Locally Most Powerful Steganaysis Detector: Low SNR Case

This section deals with the design of a locally most powerful steganalysis detector specifically for the low SNR case. We first begin with a formal definition of the uniformly most power statistical test.

Definition 3.5.1. [8] A statistical test $\phi_1(x)$ of H_0 versus H_1 is uniformly most powerful (UMP) of size (prob. of false alarm) α if it has size α and its power (prob. of detection) is uniformly greater than the power of any other test $\phi_2(x)$ whose size

is less than or equal to α:

$$\sup_{\theta \in H_0} E_\theta \phi_1(x) = \alpha \quad ; \quad \sup_{\theta \in H_0} E_\theta \phi_2(x) \leq \alpha \tag{3.5.1}$$

$$E_\theta \phi_1(x) \geq E_\theta \phi_2(x), \qquad \forall \theta \in H_1 \tag{3.5.2}$$

In some cases, especially detecting a weak signal (low SNR) such a test may not exist. Therefore we resort to locally most power (LMP) tests. LMP test is an optimum test for the detection of weak signals [8]. For low SNR the hypothesis test formulation for secret key estimation becomes:

$$H_1 \;:\; \sigma_1 > \sigma_0 \;\; k_0 \leq k \leq k_1 \;\text{ and }\; \sigma_1 - \sigma_0 \simeq 0 \tag{3.5.3}$$

$$H_0 \;:\; \sigma_1 = \sigma_0, \forall k. \tag{3.5.4}$$

The key idea behind the LMP detector is that under H_1, if the slope of the power function of the detector at σ_0 is greater than or equal to the slope of the power function at the same point for any other detector then power of the LMP detector will be the maximum among all detectors subject to the constraint that size of the test is specified. Therefore a non-randomized detection rule for the above hypothesis test can be constructed as,

$$\frac{d}{d\sigma_1}\left[\ln \prod_{i=1}^{k} p_{\sigma_1}(y_i)\right]\Bigg|_{\sigma_1=\sigma_0} \begin{cases} \geq lnA & \text{select } H_1, \\ \leq lnB & \text{select } H_0 \\ k = k+1 & \text{otherwise} \end{cases} \tag{3.5.5}$$

where,

$$\frac{d}{d\sigma_1}\left[\ln \prod_{i=1}^{n} p_{\sigma_1}(y_i)\right]\Bigg|_{\sigma_1=\sigma_0} = \left.\frac{\frac{d}{d\sigma_1}\left[\prod_{i=1}^{n} p_{\sigma_1}(y_i)\right]}{\prod_{i=1}^{n} p_{\sigma_0}(y_i)}\right|_{\sigma_1=\sigma_0}. \tag{3.5.6}$$

3.6 LMP-CUSUM Steganalysis

In regular CUSUM test the test statistic depends on the log-likelihood ratio but on the other hand in LMP sequential detection the test statistic depends on slope of the power of the test computed at σ_0 given by Eq. (3.5.6) . While we modify CUSUM to accommodate LMP, we also notice that in most practical cases the steganalysis detector has access only to stego image/signal and not to the cover image/signal. In other words, σ_1 is available and σ_0 is unknown. Test statistic for the CUSUM steganalysis detector based on LMP test is given by Eq. (2.3.2) with s_k given by,

$$s_k = \frac{d}{d\sigma_0} \left[\ln p_{\sigma_0}(y_k)\right]\Big|_{\sigma_0=\sigma_1}. \tag{3.6.1}$$

From Eq. (3.6.1) we note that knowledge of σ_0 is not necessary here.

Chapter 4

Secret Key Estimation in Sequential Image Steganography: Non-stationary Case

This chapter deals with practical situations. Algorithm developed in Chapter 3 for the weak signal and unknown parameter is now applied to the real images. Unknown variance is estimated by maximum likelihood approach from available data. Later algorithm is modified to accommodate non-stationary behavior.

4.1 Introduction

Digital images are known to exhibit non-stationary characteristics. This property has been widely acknowledged in digital image processing and compression communities. Therefore, some modifications are needed to extend the proposed steganalysis detector for digital image steganography. We again assume spread spectrum embedding in digital images as proposed in [6] for the sake of consistency. It is assumed that message is sequentially hidden in the DCT domain. Now, $\{y_k\}$ and $\{x_k\}$ denote the stego and cover image's DCT coefficients, respectively. Clearly, this type of message

embedding will result in a change of variance. In addition to the statistically non-stationary behaviour, estimating the unknown variance of the original image and pdf models for DCT coefficients are important issues. Some authors ([11] and [2]) have suggested using the generalized Gaussian pdf to approximate AC coefficients. Although generalized Gaussian pdf may be a good choice, our experience suggests that the Gaussian pdf model (a particular case of generalized Gaussian model) works reasonably well while also facilitating closed form solution to the steganalysis detector design.

Non-stationarity in natural images implies that using one single variance estimate for the entire image is not a good approximation. Therefore we assume piece-wise stationarity and using a sliding window to compute several local variance estimates. The sliding window variance estimate for the kth DCT coefficient of the stego image is given by,

$$\hat{\sigma}^2_{1,k} = \left\lfloor \frac{\sum_{i=k-\frac{M}{2}}^{k+\frac{M}{2}} |y_i - \mu_k|^2}{M-1} \right\rfloor \tag{4.1.1}$$

where, μ_k is the mean of the given window and M is the window length. It turns out that Eq. (4.1.1) is a maximum likelihood estimate [12] and is also an efficient estimate.

One consequence of introduction the sliding window is that the condition for the one-sided steganalysis hypothesis test may no longer be valid by using the plug-in estimate given in Eq. (4.1.1) for detection. That is, $\hat{\sigma}_{1,k} < \hat{\sigma}_{0,k}$ may occur for some coefficients as illustrated in Fig. 4.1 for the Cameraman image. Here, the message is hidden from DCT coefficients 5000 to 7000 with the strength $\rho = 0.1$. Clearly, $\sigma_{0,k} \neq \sigma_{1,k}$ for $k = 5000, 5001, \ldots, 7000$ but equal elsewhere. Since the one sided hypothesis test condition is violated as explained above the CUSUM-SPRT steganalysis detector

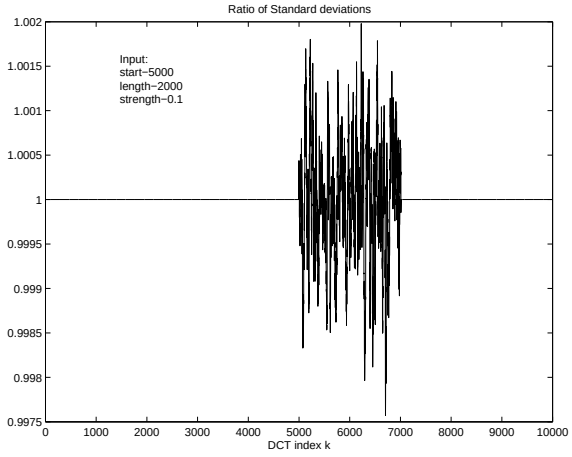

Figure 4.1: Ratio of $\hat{\sigma}_{1,k}$ to $\hat{\sigma}_{0,k}$ oscillates around the value of 1.

fails as shown in Fig. 4.2. Overcoming this problem in a mathematical sense is somewhat difficult because the value of the empirical estimate of the variances depend on a variety of factors including: (a) the estimation algorithm, (b) the host image statistics, and the (c) value of ρ. Note that the host image statistics is not under the control of the steganalysis detector. Therefore, we have taken an experimental approach to somewhat alleviate this problem. Through extensive experimentation with different types of images we found that, for low SNR cases when the message location consists of mid to high frequency DCT coefficients, using $|y_k|$ instead of y_k as input to the steganalysis detector mostly results in a one-sided hypothesis test. Now, let $\xi_{1,k}$ be the standard deviation of $|y_k|$ and $\xi_{0,k}$ be the standard deviation of $|x_k|$. Since we assume that y_k and x_k are zero mean and normally distributed, the pdf of these new random variables are given by,

$$p_z(z) = \frac{2}{\sqrt{2\pi\sigma_i^2}} \exp\left[\frac{-z^2}{2\sigma_i^2}\right] \ , \ z \geq 0 \tag{4.1.2}$$

$i = 0$ stands for $z = x_k$ and $i = 1$ for $z = y_k$. It is then shown in Appendix II that

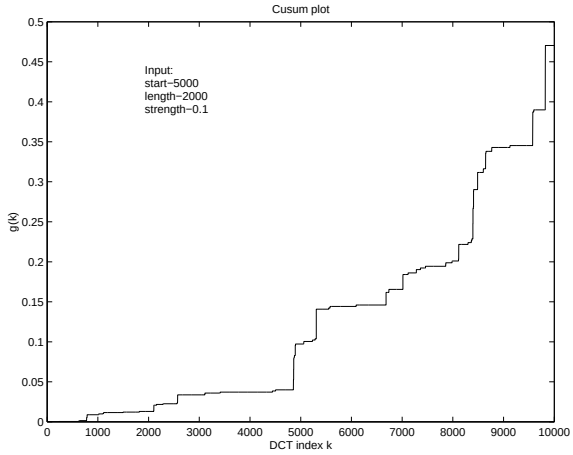

Figure 4.2: CUSUM steganalysis detector fails to detect the message.

$\xi_i^2 = 0.3634\sigma_i^2$.

The plot of the ratio of empirically computed $\xi_{1,k}$ and $\xi_{0,k}$ is shown in Fig. 4.3 which indicates that hypotheses are no longer two sided.

4.2 Modified CUSUM-LMP Steganalysis Detector

Considering the new observation random variable we modify the CUSUM with LMP test statistic and obtain the following:

$$H_1 \quad : \quad \xi_{0,k} \leq \xi_{1,k} \text{ when } k_0 \leq k \leq k_1 \text{ and } \xi_{1,k} - \xi_{0,k} \simeq 0 \tag{4.2.1}$$

$$H_0 \quad : \quad \xi_{0,k} = \xi_{1,k}, \text{ otherwise} \tag{4.2.2}$$

and s_k that maximizes the slope of the power of the test at $\xi_{0,k}$ is give by

$$s_k = \frac{\partial}{\partial \xi_{0,k}} \left[\ln p_z(z|\xi_{0,k})\right]\Big|_{\xi_{0,k}=\xi_{1,k}} \tag{4.2.3}$$

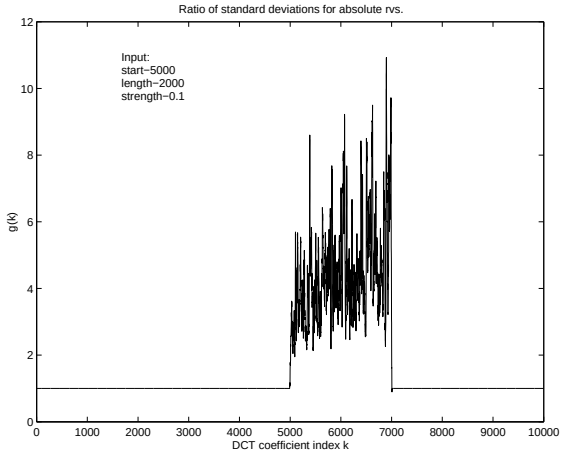

Figure 4.3: Ratio of empirical estimates of standard deviations $\xi_{1,k}$ and $\xi_{0,k}$.

where all the M observations of the k^{th} window are considered. Then, s_k in Eq. (4.2.3) is given by

$$s_k = \frac{0.3634 \cdot (|y_k| - \mu_k)^2}{\xi_{1,k}^3} - \frac{1}{\xi_{1,k}}. \tag{4.2.4}$$

as shown in Appendix III.

To test the proposed modification we used the Lenna image. Message was embedding in DCT coefficient 5000 to 7000. $\xi_{1,k}$ was computed using the moving window based empirical estimate for each coefficient k. For each k, s_k was calculated using Eq. (4.2.4). The plot in Fig. 4.4 indicates that the changes in statistics are reflected by using the modified random variables. The values of s_k in the H_1 region (i.e., between 5000 to 7000) are nearer to the zero line (shown dotted) than the values in the H_0 region. Careful observation of the plot however values reveals that $\{s_k\}$ contains some negative values in the H_1 region, again due to image non-stationarity. This suggests that the required positive drift of g_k may not be strong enough. We therefore make one more modification by thresholding s_k to remove outlier values. The

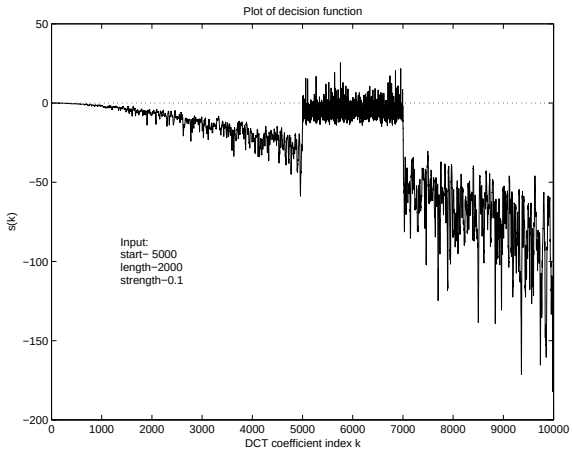

Figure 4.4: Plot of s_k shows negative values in the message region.

threshold value trades-off miss versus false alarm probability. We empirically choose the threshold value based on the negative value of s_k with the highest magnitude in the message region. We also note that this value occurring in the message region depends on the message carrier signal strength that is not a priori available to the steganalysis detector. Therefore we again resort to extensive experimentation to study the effect of this thresholding on the steganalysis reliability. We modify Eq. (2.3.2) to the following to remove the outlier values and produce required positive drift for low SNR, non-stationary image steganalysis:

$$g_k = \begin{cases} g_{k-1} + s_k & \text{if } s_k > 0, \\ g_{k-1} & \text{if } 0 \geq s_k \geq v, \\ 0 & \text{if } s_k \leq v \\ 0 & \text{if } k = 0 \end{cases} \tag{4.2.5}$$

where v depends on the message strength.

Chapter 5

Experimental Results

A number of experiments were carried out for spread spectrum image data embedding. We present results only for Lenna (256×256) and the Cameraman (256×256) images. Different message strengths were tested and results for $\rho = 0.1, 1, 10$ are presented here. The corresponding values for $v = -20, -2, -0.5$ were chosen, respectively. The poem for Lenna [20], *'O dear Lenna, your beauty is so vast; It is hard sometimes to describe it fast. I thought the entire world I would impress; If only your portrait I could compress. Alas! First when I tried to use VQ; I found that your cheeks belong to only you. Your silky hair contains a thousand lines; Hard to match with sums of discrete cosines.'* was used as the secret message. Each character is mapped to the six bit binary word to represent the binary message. The message bits modulate (BPSK modulation) the sign of the Gaussian message carrier. The length of the binary message was found to be 1992. We evaluate the performance of the secret estimation algorithm for the following embedding conditions: for Cameraman image—embedding in low, mid and high frequency components and for Lenna image—embedding in low and mid frequency components.

Fig. 5.1, Fig. 5.2 and Fig. 5.3 show the steganalysis detector statistic (CUSUM) for

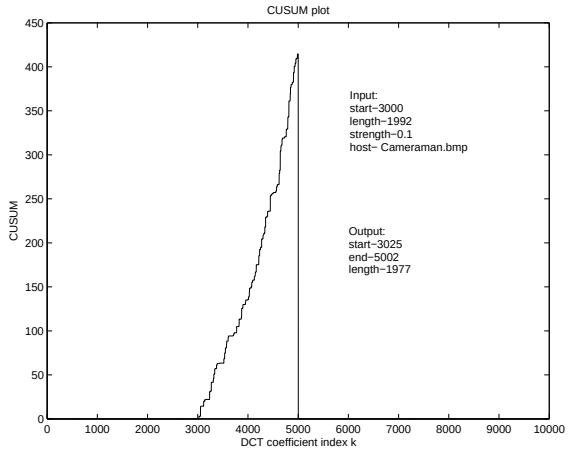

Figure 5.1: Steganalysis detector output for Cameraman image when strength $\rho = 0.1$ and mid-frequency embedding.

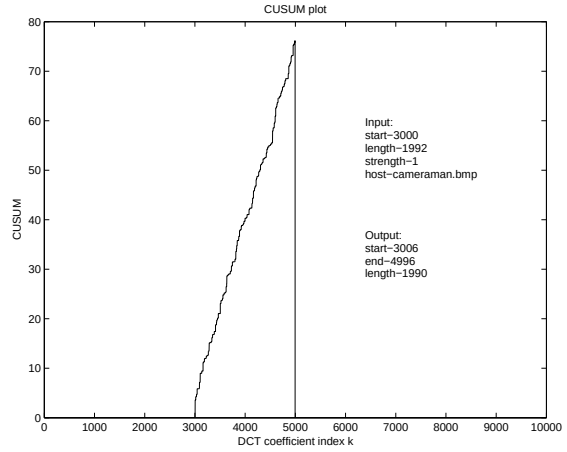

Figure 5.2: Steganalysis detector output for Cameraman image when strength $\rho = 1$ and mid-frequency embedding.

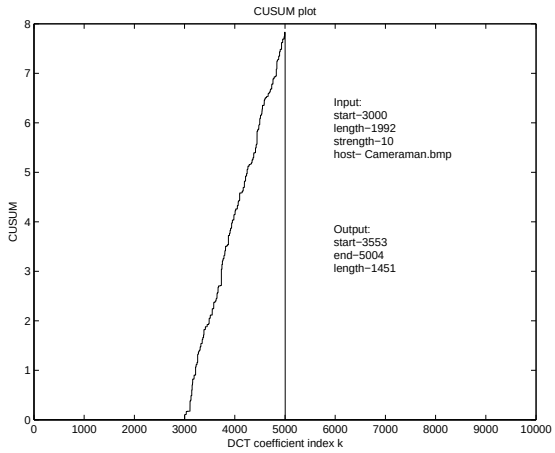

Figure 5.3: Steganalysis detector output for Cameraman image when strength $\rho = 10$ and mid-frequency embedding.

mid frequency range ($k_0 = 3000$) for the Cameraman host image. "Input" in these figures denotes the input to the embedding algorithm (secret key) and "Output" denotes the estimated secret key by the proposed steganalysis algorithm. Only the first 10000 indices are shown in these figures. $\alpha = \beta = 0.1$ was chosen for steganalysis. We observe that the secret key estimation algorithm works well. We also notice from these figures that the slope of $\{g_k\}$ is highest when $\rho = 0.1$ compared to the slope at $\rho = 10$. One of the possible reasons is that although LMP test is good at detecting small departures from the hypothesis H_0 (due to the very nature of the small SNR assumption) it is weak in detecting sufficiently large ones, as also observed in [8]. We know that in mid and high frequency ranges, DCT magnitudes are more or less uniform. Therefore the corresponding window based variance estimates are also small. Because of the low slope of $\{g_k\}$ for $\rho = 10$, $\hat{k_0}$ is estimated to be 3553 which is not very accurate compared to $\hat{k_0}$ in the cases with $\rho = 0.1$ and $\rho = 1$. If we choose lower value of threshold h_0 by changing α and β, a more accurate estimate $\hat{k_0}$ is obtained.

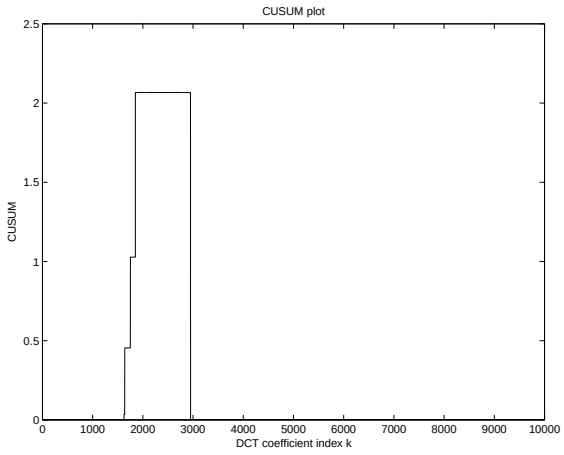

Figure 5.4: Steganalysis detector response for Cameraman image for strength $\rho = 0.1$ and low frequency embedding.

With $\alpha = \beta = 0.4$ for $\rho = 10$, $\hat{k_0}$ is estimated to be 3170 and total length is estimated to be 1830 which shows improved performance compared to the previous experiment.

Fig. 5.4, Fig. 5.5 and Fig. 5.6 shows CUSUM statistic for low frequency range ($k_0 = 2$) for the Cameraman image. Again, only the first 10000 indices are shown. $\alpha = \beta = 0.1$ was chosen for the steganalysis detector. It is clear from Fig. 5.4 that the algorithm fails to detect reliably the presence of message when $\rho = 0.1$. As explained earlier, the reason for this is that using absolute values of the DCT coefficients for detection remains two sided for low frequency ranges (up to $k = 2000$) as seen in Fig. 5.7 which violates the assumption of one sided hypothesis test. Fig. 5.8 shows that as ρ increases to 10, choosing absolute values of the observations for steganalysis detection seems to result in a one-sided hypothesis test. In our experiments we found that values of ρ higher than 1 mostly results in a one-sided test. Also, since the DCT coefficient magnitudes in the low frequency range is much higher than the mid and high frequency ranges, addition/subtraction of small values from higher magnitudes

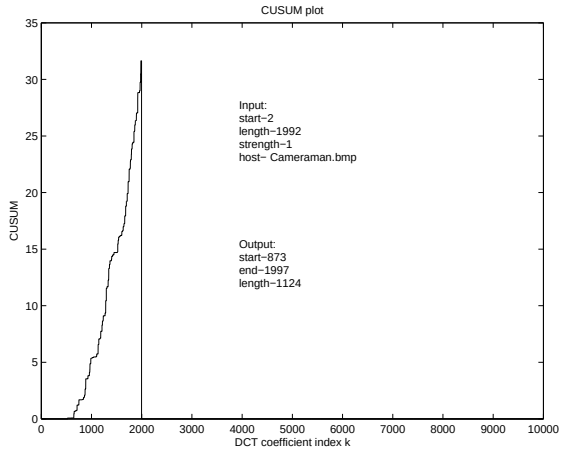

Figure 5.5: Steganalysis detector response for Cameraman image for strength $\rho = 1$ and low frequency embedding.

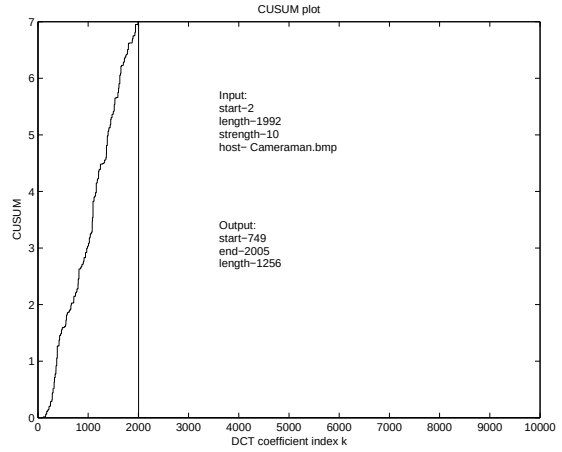

Figure 5.6: Steganalysis detector response for Cameraman image for strength $\rho = 10$ and low frequency embedding.

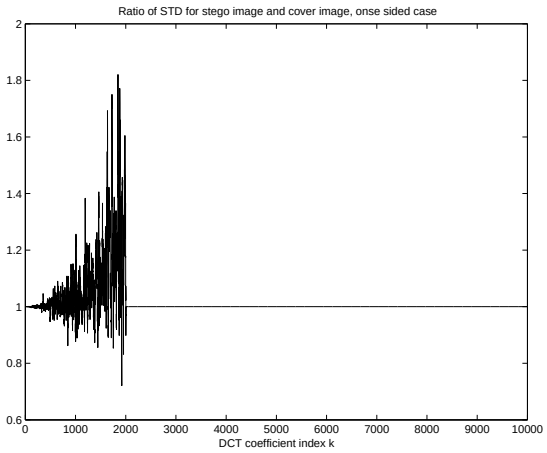

Figure 5.7: Ratio of standard deviations $\xi_{1,k}$ and $\xi_{0,k}$ when $\rho = 0.1$.

is not detectable by the LMP steganalysis detector.

Fig. 5.9 shows the result for embedding in the high frequency coefficients. Again we see observe that the steganalysis detector performs very well in estimating the secret key.

The next set of experiments were conducted using the Lenna image. Once again $\alpha = \beta = 0.1$ is selected and first 10000 indices are plotted in the figures. Fig. 5.10 shows response of the steganalysis detector for the case when $\rho = 0.1$ and message embedding is in the mid frequency range. Plot for the case when $\rho = 1$ and location of message is in low frequency range is shown in Fig. 5.11. The results are very similar to that obtained with Cameraman. Stego images with embedding strengths 0.1 and 10 are shown in Figs. 5.12 and 5.13. These figures indicate that the perceptual quality degradation due to message embedding is not significant.

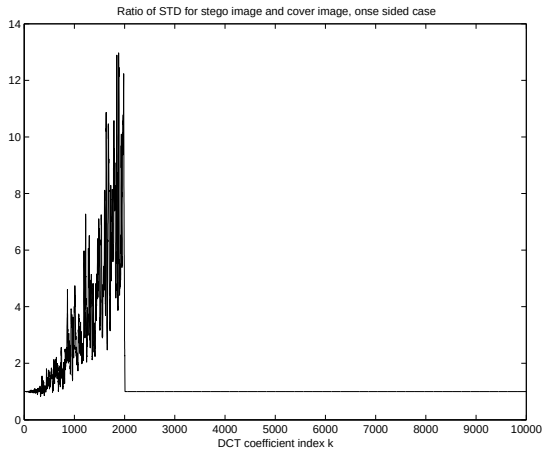

Figure 5.8: Ratio of standard deviations $\xi_{1,k}$ and $\xi_{0,k}$ when $\rho = 1$.

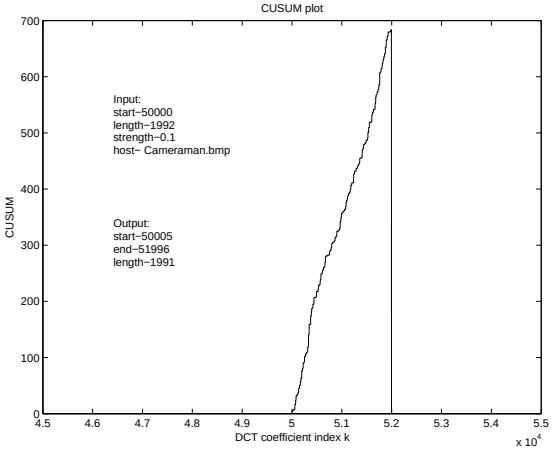

Figure 5.9: Steganalysis detector response for Cameraman for strength $\rho = 0.1$ and high frequency embedding.

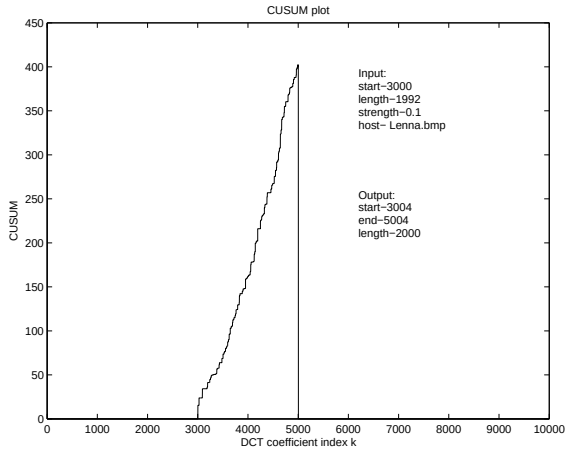

Figure 5.10: Steganalysis detector response for Lenna image for strength $\rho = 0.1$ and mid-frequency embedding.

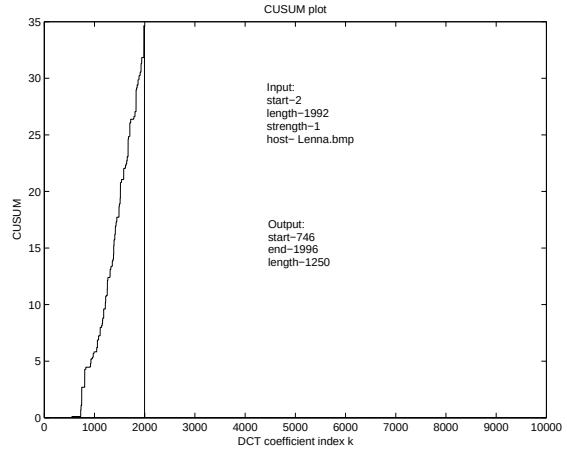

Figure 5.11: Steganalysis detector response for Lenna image for strength $\rho = 1$ and low frequency embedding.

Figure 5.12: Cameraman (256×256) stego image with $\rho = 0.1$.

Figure 5.13: Camerama (256×256) stego image with $\rho = 10$.

Chapter 6

Conclusion

A secret key estimation algorithm for sequential message hiding is proposed. While the general mathematical theory presented is applicable to any type of sequential message embedding, the paper primarily focuses on spread spectrum embedding. The proposed steganalysis algorithm looks for abrupt jumps in the statistics of the stego signal to estimate the secret key. Several theoretical results are derived for stationary and non-stationary host signals for different message strengths. A locally most powerful steganalysis detector is also derived for the low SNR case. Extensive experiments show that the proposed algorithm is shown to perform well for stationary host signals. For non-stationary digital image data hiding in the DCT domain, the secret key estimation accuracy is good when the embedding is done in mid and high frequency DCT coefficients. Its performance suffers for low frequency embedding in the DCT domain. One reason for this is the violation of the one-sided hypothesis test condition assumed by the steganalysis algorithm. Further modifications to the algorithm are underway to improve its performance for low frequency embedding also.

Appendix

Appendix I

Derivation of Eq. (3.3.3). If the probability distribution of σ_1 is assumed to be uniform, then the likelihood ratio is given by,

$$LR = \frac{\sigma_0}{\sigma_1} \times \frac{e^{-\frac{(y_i-\mu)^2}{2\sigma_1^2}}}{e^{-\frac{(y_i-\mu)^2}{2\sigma_0^2}}}$$

$$\prod_j^k LR = \frac{\sigma_0^{N_k}}{\sigma_1^{N_k}} \cdot e^{\lambda_{j,k} \cdot \left(1-\frac{\sigma_0^2}{\sigma_1^2}\right)}$$

$$\int_0^\infty \prod_j^k LR = \int_0^\infty \frac{\sigma_0^{N_k}}{\sigma_1^{N_k}} \cdot e^{\lambda_{j,k} \cdot \left(1-\frac{\sigma_0^2}{\sigma_1^2}\right)} d\sigma_1$$

$$\int_0^\infty \prod_j^k LR = e^{\lambda_{j,k}} \cdot \frac{\Gamma(\frac{N_k-1}{2})}{2 \cdot \lambda_{j,k}^{\frac{N_k-1}{2}}}$$

$$S_j^k = \ln \int \prod_j^k LR = \lambda_{j,k} + \ln \Gamma\left(\frac{N_k-1}{2}\right) - \ln 2\lambda_{j,k}^{\frac{N_k-1}{2}} - \ln(b-a)$$

Similar derivation applies when σ_1 is normally distributed.

Appendix II

Derivation of Eq. (4.1.2). Probability density function of z is given by,

$$\begin{aligned} p_z(z) &= p_{\sigma_i}(z) + p_{\sigma_i}(-z) \\ &= \frac{2}{\sqrt{2\pi\sigma_i^2}} \exp\left[\frac{-z^2}{2\sigma_i^2}\right] \ , \ z \geq 0 \end{aligned}$$

Expected value of the random variable z can be computed as,

$$\begin{aligned} E(z) &= \int_0^\infty z \cdot p_z(z) dz \\ &= \frac{2}{\sqrt{2\pi\sigma_i^2}} \int_0^\infty z \cdot \exp\left[\frac{-z^2}{2\sigma_i^2}\right] dz \\ &= \frac{2}{\sqrt{2\pi\sigma_i^2}} \int_0^\infty -\sigma_i^2 \cdot d\left(\exp\left[\frac{-z^2}{2\sigma_i^2}\right]\right) \\ &= \frac{2\sigma_i}{\sqrt{2\pi}}. \end{aligned}$$

Variance of the random variable z is given by,

$$\begin{aligned} E(z^2) &= \int_0^\infty z^2 \cdot p_z(z) dz \\ &= \frac{2}{\sqrt{2\pi\sigma_i^2}} \int_0^\infty z^2 \cdot \exp\left[\frac{-z^2}{2\sigma_i^2}\right] dz \\ &= \frac{2}{\sqrt{2\pi\sigma_i^2}} \int_0^\infty -z\sigma_i^2 \cdot d\left(\exp\left[\frac{-z^2}{2\sigma_i^2}\right]\right) \\ &= \frac{2\sigma_i}{\sqrt{2\pi}} \int_0^\infty \exp\left[\frac{-z^2}{2\sigma_i^2}\right] dz \\ &= \sigma_i^2 \end{aligned}$$

$$\begin{aligned} \xi_i^2 &= E(z^2) - (E(z))^2 \\ &= \sigma_i^2 - \left(\frac{2\sigma_i}{\sqrt{2\pi}}\right)^2 \\ \xi_i^2 &= 0.3634\sigma_i^2. \end{aligned}$$

Appendix III

Derivation of Eq. (4.2.4).

$$\begin{aligned} p_z(z|\xi_{0,k}) &= p_z(|y_k|) \\ \ln p_z(z|\xi_{0,k}) &= \ln \frac{2}{\sqrt{2\pi\sigma_{1,k}^2}} - \frac{(|y_k| - \mu_k)^2}{2\sigma_{1,k}^2} \end{aligned}$$

By using the relation between variances in Eq. (4.1.1),

$$\ln p_z(z|\xi_{0,k}) = \ln \frac{2\sqrt{0.3634}}{\sqrt{2\pi\xi_{0,k}^2}} - \frac{0.3634 \cdot (|y_k| - \mu_k)^2}{2\xi_{0,k}^2}$$

$$\frac{\partial}{\partial \xi_{0,k}} \left[\ln p_z(z|\xi_{0,k})\right] = \frac{-1}{\xi_{0,k}} + \frac{0.3634 \cdot (|y_k| - \mu_k)^2}{\xi_{0,k}^3}$$

$$\left.\frac{\partial}{\partial \xi_{0,k}} \left[\ln p_z(z|\xi_{0,k})\right]\right|_{\xi_{0,k}=\xi_{1,k}} = \frac{0.3634 \cdot (|y_k| - \mu_k)^2}{\xi_{1,k}^3} - \frac{1}{\xi_{1,k}}$$

Bibliography

[1] I. Avcibas, N. Memon, and B. Sankur, *Steganalysis using image quality metrics*, IEEE Trans. on Image Processing **12** (2003), no. 2, 221–229.

[2] M. Barni, F. Bartolini, A. De Rosa, and A. Piva, *A new decoder for the optimum recovery of nonadditive watermarks*, IEEE Trans. on Image Processing **10** (2001), no. 5.

[3] R. Chandramouli, *A mathematical framework for active steganalysis*, Special issue on multimedia watermarking Springer/ACM Multimedia Systems **9** (2003), no. 3, 303–311.

[4] R. Chandramouli and N. Memon, *Analysis of lsb based image steganography techniques*, Proc. of IEEE ICIP **3** (2001), no. 5, 1019–1022.

[5] ———, *Steganography capacity: A steganalysis perspective*, Proc. SPIE Security and Watermarking of Multimedia Contents (2003).

[6] J. Cox, J. Kilian, T. Leighton, and T. Shamoon, *Secure spread spectrum watermarking for multimedia*, IEEE Trans. on Image Processing **6** (1997), no. 12, 1673–1687.

[7] H. Farid, *Detecting steganographic message in digital images*, Tech. Report TR2001-412, Dartmouth College, 2001.

[8] T. S. Ferguson, *Mathematical statistics*, Academic Press, 1967.

[9] J. Fridrich, M. Golijan, and R. Du, *Reliable detection of lsb steganography in greyscale and color images*, Proc. ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada (2001), 27–30.

[10] J. Fridrich and M. Goljan, *Practical steganalysis of digital images state of the art*, Proc. SPIE Photonics West **4675** (2002), 1–13.

[11] J. R. Hernandez, M. Amado, and F. Perez-Gonzalez, *Dct-domain watermarking techniques for still images: Detector performance analysis and a new structure*, IEEE Trans. on Image Processing **9** (2000), no. 1.

[12] R. L. Joshi and T. R. Fischer, *Comparision of generalized gaussian and laplacian modelling in dct image coding*, IEEE Signal Processing Letters **2** (1995), no. 5, 81–82.

[13] R. Machado, *Ezstego*.

[14] L.M. Marvel, C.G. Boncelet Jr., and C.T. Retter, *Spread spectrum image steganography*, IEEE Transactions on Image Processing **8** (1999), no. 8, 1075–1083.

[15] Mathworld, *http://www.mathworld.worlfram.com*.

[16] I. Nikiforov and M. Basseville, *Detection of abrupt changes*, Printice-Hall, 1998.

[17] E. Page, *Continuous inspection schemes*, Biometrika (1954).

[18] A. N. Shiryaev, *On optimum methods in quickest detection problems*, Theory Probability and Applications **8**, no. 1, 22–46.

[19] S. Trivedi and R. Chandramouli, *Active steganalysis of sequential steganography*, SPIE conference California **5020** (2003), no. 13, 123–130.

[20] Unknown, *http://www.public.asu.edu/∼akandan/tech/lena/*.

[21] A. Wald, *Sequential detection*, Willey, 1947.

[22] A. Westfield and A. Pfitzmann, *Attacks on steganographic systems*, Lecture notes in computer science **1768** (2000), 51–75.