جـــامـعـــة الـــشـرق الاوسـط
MIDDLE EAST UNIVERSITY
Amman - Jordan

The Detection of Data Hiding in RGB Images

Using

Statistical Steganalysis

كشف البيانات المخفية في صور RGB باستخدام تحليل غطاء الاخفاء الاحصائي

By

Zaid Ibrahim Rasool Rasool

Supervisor

Dr. Mudhafar Al-Jarrah

A Thesis Submitted in Partial Fulfillment of the Requirements for the

Master Degree in Computer science

Department of Computer Science

Faculty of Information Technology

Middle East University

May, 2017

Authorization

I, Zaid Ibrahim Rasool, authorize Middle East University (MEU) to provide copies of my thesis to the concerned libraries, establishments, and institutions upon request.

Name: Zaid Ibrahim Rasool

Date: 30-5-2017

Signature: 

Examination Committee Decision

This is to certify that the thesis entitled "The detection of data hiding in RGB images using statistical steganalysis" was successfully defended and approved on 30/5/2017

Examination Committee Members Signature

(Supervisor)

Dr. Mudhafar Munir Al-Jarrah

Middle East University

(Head of the Committee and Internal Committee Members)

Prof. Dr. Ahmad Kayed

Middle East University

(External Committee Members)

Dr. Mohamed Ahmed Alia

Al-Zaytoonah University

Acknowledgements

First, I would like to thank my God for his merciful and his continuous help over all the period of my life.

I would like to express my great appreciation to my supervisor Dr. Mudhafar Munir Al-Jarrah for his supervision, encouragement and his helpful advice. I also wish to express my deepest gratitude to the members of the committee for spending their precious time on reading my thesis and giving me encouragement and constructive comments. I would like to thank all Information Technology Faculty members at Middle East University.

Finally, and most importantly, I must thank my dearest family for giving me the support and encouragement that only a family can give.

Zaid

Dedication

(وقل رب زدني علماً) طه الاية(111)

This thesis is dedicate to my Father, Mother, Brothers and Sisters

Table of contents

List of Tables

List of figures

List of Abbreviations

RGB	Red Green Blue
LSB	Least Significant Bit
SVM	Support Vector Machine
GLCM	Gray Level Co-occurrence Matrix
CGCM	Colors Gradient Co-occurrence Matrix
LHB	Left Half Byte
RHB	Right Half Byte
ESS	Experimental Steganalysis System
TN	True Negative Rate
TP	True Positive Rate
FN	False Negative Rate
FP	False Positive Rate
2LSB	Two Least Significant Bit
4LSB	Four Least Significant Bit
CV	Coefficient of Variation
DA	Discriminant Analysis
CFS	Channel-Based Feature Set
BMP	bitmap
PNG	Portable Network Graphics
NB	Naïve Base
ANN	Artificial Neural Network Classification
KNN	Nearest Neighbor Classification
DT	Decision Tree Classification

POVs	Pairs of Values
QDA	Quadratic Discriminant Analysis

The Detection of Data Hiding in RGB Images Using Statistical Steganalysis

By: Zaid Ibrahim Rasool

Supervisor: Dr. Mudhafar Al-Jarrah

Abstract

Steganalysis, the science and technology of detecting the presence of hidden data inside digital media, is a counter measure against information hiding techniques that can be used for illegitimate purposes. The work in this thesis presents a steganalysis model that uses statistical texture features and the machine learning approach to detect the presence of hidden data in RGB color images. The work analyzes features of an RGB image as a composite unit, as well as analyzing individual color channels and dual combinations of the channels. The feature set used in this study consists of 26 features per channel, which includes the Gray Level Co-Occurrence Matrix (GLCM) features of correlation, contrast, homogeneity and energy, calculated for full bytes, half-bytes, 3-bit and 2-bit fragments of individual channels, Entropy of full bytes and half bytes, skewness of full bytes and half bytes, and additional statistical features. The features are applied to single channels, and the single channel features are merged into dual and three-channel image feature sets. The main machine learning binary classifier that is selected for this work is the Support Vector Machine (SVM) algorithm. The experimental work used two image datasets of 1500 BMP images each, for training and validation of the model, and an independent image dataset of 1000 uncompressed PNG images for testing purposes. Stego image datasets were created from the clean images datasets, which were embedded with secret data using 2LSB and 4LSB steganography techniques. The experimental results for the validation phase showed detection

accuracy of 100% for the 4LSB RGB stego images, and 99.73% for the 2LSB RGB stego images. Similar results were obtained, which shows the power of the SVM classifier in detecting pattern changes in stego images even when one channel is changed, individual channels (R, G, B) and dual channels (RG, RB, GB) were analyzed. Also, when only one channel was embedded with data, which was the blue channel, the same results were obtained. The testing phase analyzed 1000 PNG stego images, which confirmed results of the validation phase. The Discriminant Analysis (DA) classifier was used for comparison with the SVM classifier, and the results showed that the SVM classifier gave higher detection accuracy. MATLAB 2015a was used in the implementation of the image processing and classification parts of the proposed model.

Keywords: steganalysis; steganography; stego image; secret image; SVM classifier; feature set; embedding; extraction; detection accuracy; RGB.

كشف البيانات المخفية في صور RGB باستخدام تحليل غطاء الاخفاء الاحصائي

اعداد

زيد أبراهيم رسول

اشراف

الدكتور مظفر الجراح

الملخص

تحليل غطاء الاخفاء، هو علم و تكنولوجيا للكشف عن وجود البيانات المخفية داخل الوسائط الرقمية، هو إجراء مضاد لتقنيات إخفاء المعلومات التي يمكن استخدامها لأغراض غير مشروعة. البحث المقدم في هذه الأطروحة يعرض نموذج تحليل غطاء الإخفاء الذي يستخدم الملامح الإحصائية ونهج التعلم الآلي للكشف عن وجود البيانات المخفية في الصور الملونة RGB ، حيث يقوم بتحليل ملامح صورة RGB كوحدة مركبة، فضلا عن تحليل قنوات الألوان المنفردة والمزدوجة. تتألف مجموعة الخصائص المستخدمة في هذه الدراسة من 26 سمة لكل قناة، تشمل مصفوفة مستوى الرمادي (GLCM) والتي تشمل الارتباط، والتباين، والتجانس، والطاقة، المحسوبة للبايتات الكاملة وأنصف البايتات ومقاطع 3 بت و 2 بت من القنوات الفردية، بالاضافة الى الانتروبيا من البايت الكامل ونصف بايت، ومعامل الانحراف للبايت الكامل ونصف البايت، وميزات إحصائية إضافية. يتم حساب المميزات لقناة واحدة، ويتم دمج مميزات القناة المفردة في مجموعة مميزات لازواج القنوات والقنوات الثلاثة. الطريقة الرئيسية المستخدمة للمصنف الثنائي الذي تم اختياره هي خوارزمية ماكنة متجه الدعم (SVM). استخدم العمل التجريبي مجموعتين من البيانات، 1500 صورة نوع BMP لكل منهما، من أجل التدريب والتحقق من النموذج، ومجموعة بيانات مستقلة من 1000 صورة نوع PNG غير مضغوطة لأغراض الاختبار .تم إنشاء مجموعات بيانات للصور المتضمنة للاخفاء (ستيجو) من مجموعات البيانات للصور النظيفة، باستخدام تقنيات 2LSB و 4LSB لاخفاء المعلومات.

أظهرت النتائج التجريبية لمرحلة التحقق أن صحة دقة الكشف كانت 100٪ لصور الاخفاء نوع RGB 4LSB و 99.73٪ لصور الاخفاء نوع RGB 2LSB ، وتم الحصول على نتائج مماثلة عندما تم تحليل القنوات الفردية (R، G، B) والقنوات المزدوجة (RG، RB، GB) أيضا، عندما تم تضمين قناة واحدة فقط ، والتي كانت القناة الزرقاء، تم الحصول على نفس النتائج. في مرحلة الاختبار تم تحليل 1000 صورة إخفاء نوع PNG ، والتي أكدت نتائج مرحلة التحقق من صحة النموذج. تم كذلك استخدام مصنف تحليل التمييز (DA) للمقارنة مع المصنف SVM، وأظهرت النتائج أن المصنف SVM أعطى دقة كشف أعلى .وقد استخدم MATLAB 2015 في تنفيذ أجزاء معالجة الصور وتصنيفها في النموذج المقترح.

الكلمات المفتاحية: كشف الاخفاء، اخفاء المعلومات، صورة ستيغو، صورة سرية، المصنف SVM ، مجموعة ميزات ، تضمين، استخراج، دقة الكشف ، RGB.

Chapter 1
Introduction

1.1 Topic

The work in this thesis deals with the problem of detecting the existence of hidden messages within cover media. In particular, the work presents an enhanced solution for the detection of hidden secret images in RGB (Red, Green, and Blue) cover images, based on texture features, using statistical steganalysis techniques. Figure 1.1 shows the RGB color cube which was selected from (www.drmoron.org/images/color-cube)

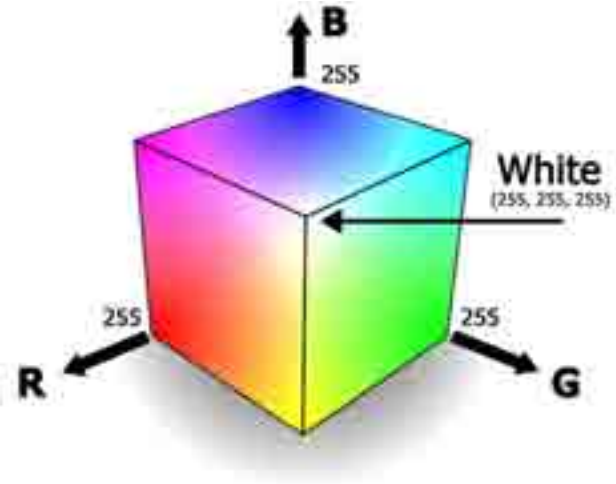

Figure 1.1: The RGB Color Cube.

1.2 Background of the Study

The growth of document exchange over different communication channels, in particular the Internet and social networks, has led to the awareness that the exchange of documents is being used for legitimate personal and business purposes as well as for illegal practices. Steganography, the hiding of messages inside multimedia files, has increased steadily, which has led researchers to focus on steganography and steganalysis techniques and the related fields of multimedia communication. The 9/11 attack in the United States has brought to attention the need for steganalysis techniques to uncover malicious communications by terrorists and criminals (Olguin-Garcia, Juarez-Sandoval, Nakano-Miyatake, & Perez-Meana, 2015).

In many cases, steganography is used to hide various types of information, such as medical, business and personal documents, for data privacy protection. However, steganography is also used for illegal purposes, to conceal documents that are exchanged in unlawful businesses; for example for money laundering, drugs trade, human trafficking, and terrorist activities. Insider's misuse of steganography to leak confidential company documents to competitors is a very serious problem to business.

Steganalysis refers to the group of techniques that can differentiate between clean images and stego images (images that have been used as a carrier media of an embedded message), (Olguin-Garcia et al, 2015).

1.3 Problem Statement

The problem addressed in this thesis is the development of steganalysis techniques to deal with the widespread misuse of steganography tools for hiding secret messages for illegal purposes. In particular, the study will consider steganalysis methods to detect a hidden message within RGB cover images.

1.4 Scope of Work

The scope of the research work covers the following areas:

1. Steganalysis of RGB images, focusing on the LSB part of an image regardless of the steganography scheme.

2. Using statistical image texture features

3. Using two-category classifiers

4. Evaluating the proposed model through experimental work by analyzing public datasets of color RGB images.

1.5 Limitations of the Proposed Work

The proposed work is limited to un-compressed color images, and compressed color images using lossless compression, such as PNG and BMP. Therefore, the proposed work does not apply to compressed images with lossey compression.

1.6 Goal and Objectives

The goal of this work is to develop a steganalysis method for detecting hidden messages in lossless or uncompressed RGB images by analyzing images' statistical texture features. The following objectives are considered:

1- Identify texture features to be measured.

2- Select an appropriate classifier for the application.

3- Design and implement a detection model.

4- Collect a dataset for evaluation.

5- Evaluate the detection accuracy of the proposed model.

1.7 Motivation

This work is motivated by the rapid increase in the use of information hiding for illegal purposes. The steganography tools for information hiding have become widely available on the internet, which made it easy for anyone to embed a secret document within a cover image. The security industry has focused on finding tools that can detect hidden messages within cover media. However, more work is needed to enhance the detection performance.

1.8 Significance of Work

This research is expected to enhance the detection capability of steganalysis tools to uncover the existence of secret messages hidden within cover images.

Detecting whether or not data is hidden in images will allow the monitor (steganalyst or warden) to further analyze the suspicious images, to prevent a secret message from being sent to a recipient over the network. It is envisaged that once a steganalyst detects the presence of a hidden message in a cover image, with a certain probability, the most important action is to stop it from being sent and may be to take other actions later to analyze the cover image and extract the secret message.

1.9 Questions to be Answered

1- What are the image features that will be used to enhance detection?

2- Which classification method will be used?

3- What is the detection accuracy of the validation phase?

4- What is the detection accuracy of the testing phase?

1.10 Thesis Organization

This thesis consist of five chapters, as below: Chapter one is the introduction, which introduced the topic of the research, background of the study, problem statement, scope of work, limitations of the proposed work, goal and objectives, motivation, significance of work and questions to be answered.

Chapter two presents literature review, concepts and definitions which introduced the introduction, steganography, steganalysis, classes of steganalysis, steganalysis approaches, classification techniques used in steganalysis, steganalysis methods, image formats, image feature models, features selection based on co-

occurrence matrix, gray level co-occurrence matrix, color gradient co-occurrence matrix, reasons for choosing steganalysis of images and the related work.

Chapter three presents methodology and the proposed model which introduced the methodology approach, outline of the proposed model, statistical features selection, the classifier, and proposed model, required functionalities of the proposed model, the proposed system and the evaluation metrics.

Chapter four pesents experimental results and discussion which introduced the introduction, clean image dataset creation, experimental work, training and field testing steps and results and discussion.

Chapter five presents conclusion and future work which introduced the conclusion and suggestions for future work.

Chapter 2

Literature Review, Concepts and Definitions

2.1 Introduction

This chapter starts by providing an overview of steganography and a formal definition. We also provide the description of its counterpart, namely steganalysis. We discuss different types of steganalysis methods and classification techniques that are used in the steganalysis method.

2.2 Steganography

Steganography is a technique that involves hiding a message in a suitable carrier, e.g., image, audio and video file. The steganography community derives largely from the signal- and image-processing community. The less frequent contributions from the cryptography and information theory communities do not always use the same terminology, and this can make it hard to see the connections between different works.

Figure 2.1: a diagram of steganography and steganalysis.

Steganography is the art of communicating a secret message while the idea of steganography dates back to ancient times (from the available records we have on it), it is only recently that the actual name has been devised, by Johannes Trithemius (1462–1516), as Steganography.

The intention of steganography is to provide the secret transmission of data. Hence, it is difficult for the third person to realize about the existence of the hidden message in the cover media.

In steganography, only the existence of the message is secret: the communication a channel is considered as open and the message itself is not usually modified so as to resist an attacker by itself (although it can be encrypted). The achievement is to hide the message as well as possible in an innocuous content so that any eavesdropper would have no suspicions.

Figure 2.2 a case of steganography for which the hiding of the message is invisible to the human eye. It is important to distinguish steganography from cryptography, first: cryptography aims at modifying the message so that it becomes impossible to read to an eaves dropper. It is of no concern to cryptography that the encrypted message might look suspicious. Steganography may not alter the message but only hides it in a medium, so that it will not raise suspicions.

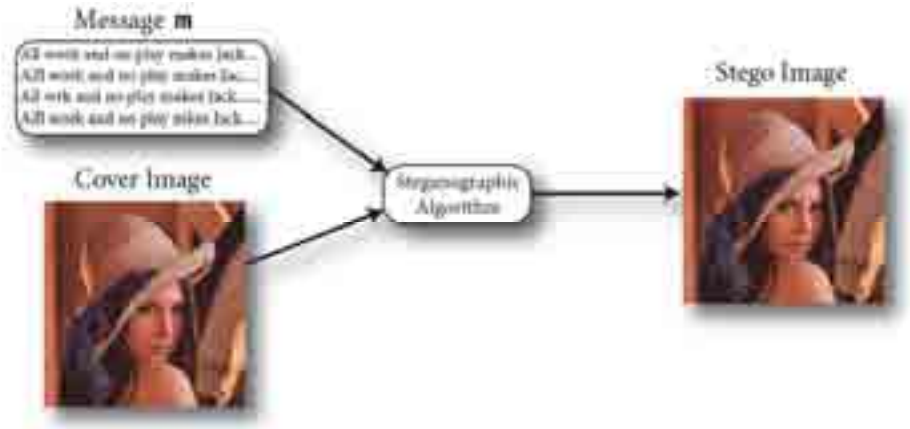

Figure 2.2: a simple illustration of steganography for an image (Miche, 2010).

A message *m* is embedded in the cover image by means of a steganographic algorithm. The resulting image, looking as similar as possible to the original cover image, is called stego image.

There are three main techniques that are used in data protection; steganography, watermarking and cryptography. Steganography protects the privacy of a document by embedding it inside a cover media, while watermarking protects the copy-right of a document by embedding data in the document so that an unauthorized user will not be able to access the document's contents without knowledge of the hidden data and how it is stored. Cryptography protects the privacy of a document by ciphering the document text. Table 2.1 and Figure 2.3 present a **c**omparison of steganography, watermarking and cryptography methods.

Table 2.1: comparison of steganography, watermarking and cryptography.

Steganography	Is the art and science of hiding information in ways that prevent the detection of hidden messages? Steganography literally means "covered writing" and is usually interpreted to mean hiding information in other information. Comparing it to cryptography, steganography has its advantage because the message itself will not attract the audiences, as the very nature of a steganography system is to hide the message in an imperceptible manner.
Watermarking	Is the process of embedding a message on a host signal? Watermarking, as opposed to steganography, has the additional requirement of robustness against possible attacks. A watermark can be either visible or invisible.
Cryptography	Is defined as the art and science of secret writing. The word itself comes from Greek where the words and graphen mean secret and writing, respectively. The focus in cryptography is to protect the content of the message and to keep it secure from unintended audiences. The purpose of cryptography is to create schemes or protocols which can still complete the intended tasks even in the presence of an adversary. Cryptography's main task is to ensure users able to communicate securely over an insecure channel. This communication however must ensure the transmission's privacy and authenticity.

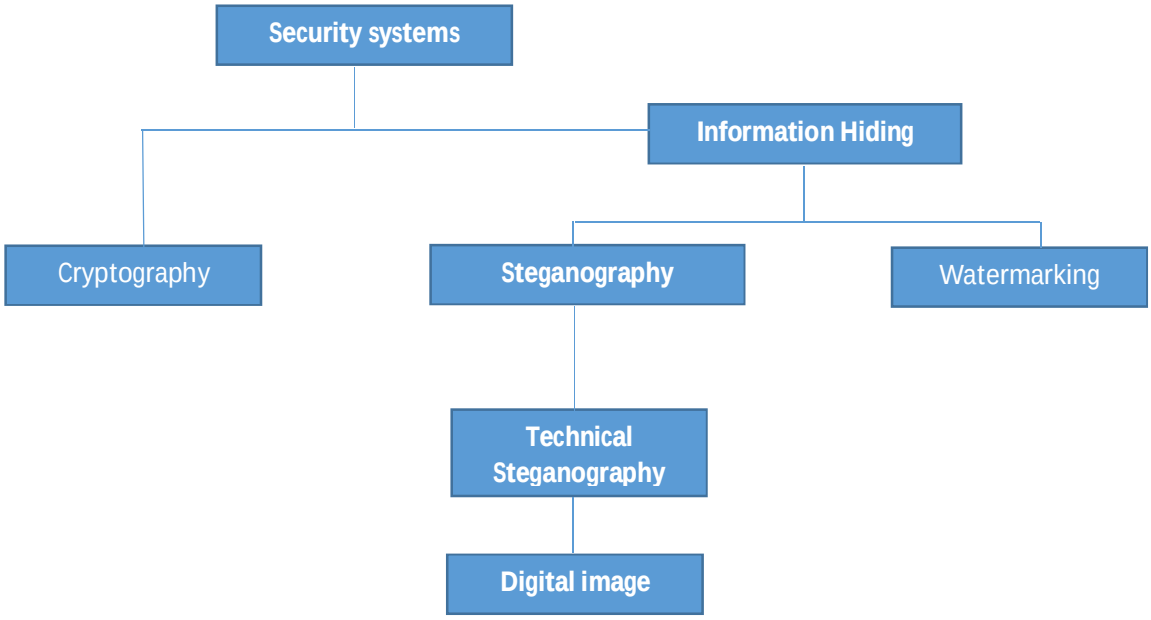

Figure 2.3: The different embodiment disciplines within the area of information hiding.

2.3 Steganalysis

Steganalysis is the art of seeing the unseen; to separate stego objects and not-stego-objects with practically no information about the steganography based algorithms. The objective of steganalysis is to gather any evidence about the presence of hidden data (Manveer, Gagandeep, 2014).

It is important to develop a steganalysis technique which detects the existence of hidden messages inside the digital medium. The documents without any hidden messages are called clean documents and the documents with hidden messages are named cover or stego documents.

The concept of steganalysis is again very different from that of cryptanalysis (as steganography differs from cryptography): in cryptanalysis, the aim is to “break the

code" and then get the encoded message. Steganalysis does not aim at obtaining the message hidden in the cover medium, but only at detecting the mere presence of it.

The original goal of steganalysis was hence to give two-category to the question "Is there a message hidden in this medium?" (Miche, 2010).

Steganalysis is usually performed in one of two ways: signature analysis and blind detection. In signature analysis, the steganographic hiding method is known, which makes detection easier. Embedding algorithms always leave a particular signature, which can be tracked for detection. (Johnson & Jajodia, 1998), (Luo, Wang, Wang, & Liu, 2008).

Figure 2.4 shown the classical steganalysis process, in contrast, the blind detection technique has no knowledge of the hiding method. Although this detection technique is obviously the most commonly used, it is by far the most difficult to implement (Johnson & Jajodia, 1998), (Luo, Wang, Wang, & Liu, 2008).

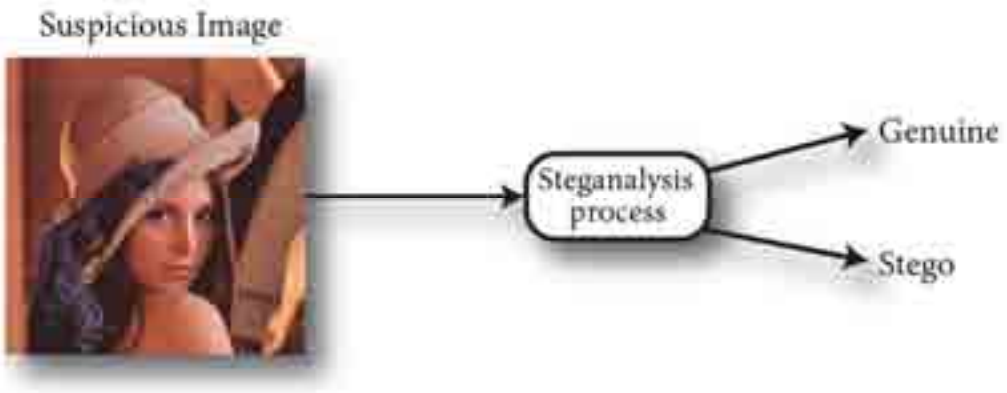

Figure 2.4: The classical steganalysis process (Miche, 2010).

A suspicious image processed using steganalysis is identified as genuine of stego (tampered). In other words, steganalysis is the counter measure to steganography methods, for the detection, extraction, destruction and manipulation of the hidden data in a stego object, Figure 2.5 Shows the Steganography and Steganalysis Processes

The challenges of steganalysis are: to get Stego-Image Database, to develop universal or specific steganalysis algorithms, to test the Steganalysis algorithm against different payload Stego Images, to check its robustness, detection of the presence of hidden message in a cover signal, identification of embedding algorithm, estimation of embedded message length, prediction of location of hidden message bits, estimation of the secret key used in the embedding algorithm, estimation of a parameter of embedding algorithm, and extraction of the hidden message. (Thiyagarajan, Aghila & Venkatesan, 2012).

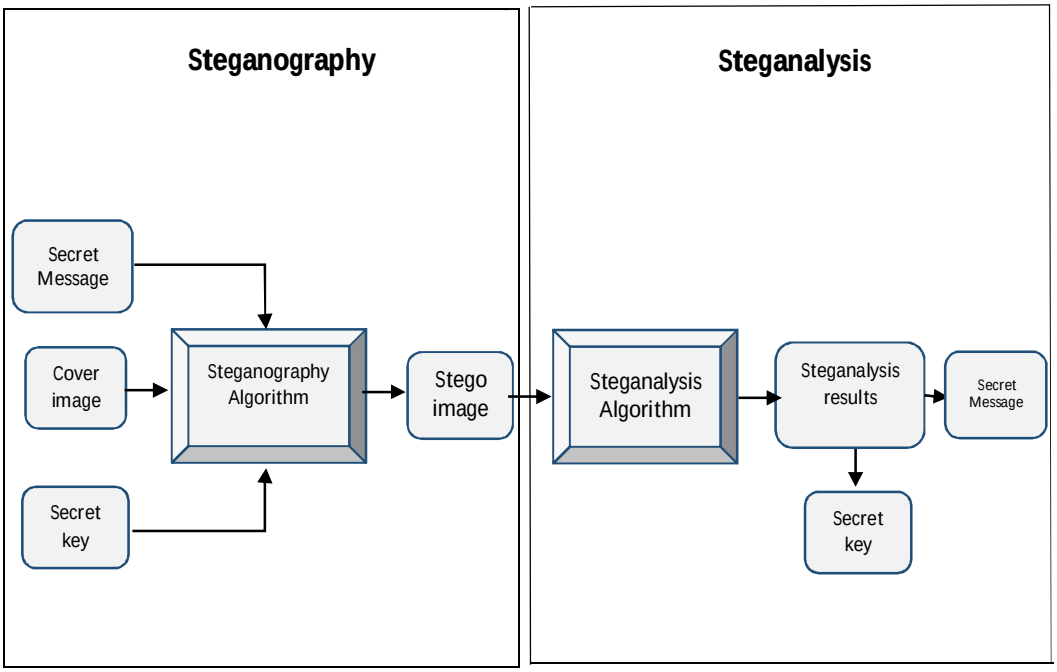

Figure 2.5: Steganography and Steganalysis Processes (Badr, Ismaial, Khalil, 2014)

2.3.1 Classes of Steganalysis

The primary steganalysis goal is to detect a message in a suspicious medium; the field has evolved towards some refinements, derived from the original idea. The two-category classification of images as clean or stego could be qualified as qualitative steganalysis, although this terminology is not often used (Miche, 2010).

Steganalysis techniques can be classified as:

- **Targeted Steganalysis**: A targeted steganalysis technique works on a specific type of steganography scheme and sometimes is limited to certain image formats.
- **Blind Steganalysis**: A blind steganalysis technique is designed to work on all types of embedding techniques and image formats.
- **Quantitative Steganalysis**: The quantitative steganalysis approach differs from the qualitative steganalysis in that it predicts the length of the message that has been hidden in the cover medium.
- **Forensic Steganalysis**: the forensic steganalysis goes beyond the detection step of the classical steganalysis, obtaining the actual hidden message (Miche, 2010).

2.3.2 Steganalysis Approaches

The different approaches of steganalysis are:

Visual attacks: by analyzing the images visually, when inspecting an image a compound with a known clean in the same image, to find out if there are differences (Prakash, 2006).

Structural attacks: the process of embedding secret data in a cover medium may result in structural or format changes which can be detected at steganalysis stage. For example a change in compression or resolution of the cover image is an indication that the image was manipulated.

Statistical attacks: in this types of attacks the statistical analyses of the images by some mathematical formulas is applied and the detection of hidden data is, based on these statistical results.

2.3.3 Classification Techniques Used in Steganalysis

Classification identifies images into classes such as a (cover or stego image) based on their feature values. The primary classification involved in steganalysis is supervised learning. In supervised learning, a set of training samples (consisting of input features and class labels) is fed in to train the classifier. Once the classifier is trained, it predicts the class label of an unclassified image based on the given features.

There are several classification techniques that are used in steganalysis (Schaathun, 2012), including: Discriminant analysis(DA), Support Vector Machine Classification (SVM), Naive Base(NB) and Decision Tree Classification (DT), K-Nearest Neighbor Classification (KNN), and Artificial Neural Network Classification (ANN). For steganalysis techniques that aim to detect the existence of a hidden message inside a carrier document, a binary classifier is used which results is negative or positive outcome. The Artificial Neural Network (ANN) and the new Deep learning Neural Network (DNN) are sometimes used in binary classifications but they tend to be generally slower when processes large sets of data.

2.3.4 Steganalysis Methods

Some of the steganalysis methods based on the color of the pixel, introduced a powerful statistical attack that can be applied to any steganography technique in which a set of Pairs of Values (POVs) are used to detect the presence of the secret message. The fact that any Steganographic techniques change the frequency of a pair of value during message embedding process. This method was effective in detecting Stego-images generated from the variety of Steganography algorithms. (Westfeld & Pfitzmann, 2000). Steganalysis methods are classified as follows:

1- Supervised learning based steganalysis.

2- Blind identification based steganalysis.

3- Parametric statistical steganalysis.

Most currant steganalysis research focus on the supervised learning method, to achieve blind steganalysis.

2.4 Image Formats

1- BMP image

The bitmap or BMP format is considered a simple image file format. BMP files are device-independent files most frequently used in Windows systems, and it is based on the RGB color model. Header region contains information and other details about size and color depth. Data region contains the values of each pixel.

Files in the BMP format can be single channel or three channels color or grayscale.

The bmp format allows for lossless compression but it is most often used with uncompressed images.

2- Tiff image

TIFF (Tag Image File Format) is a common format for exchanging raster graphics (bitmap) images between applications programs, A TIFF file can be identified as a file with a ".tiff" or ".tif" file name suffix. TIFF format supports RGB, indexed color, and grayscale images with alpha channels and bitmap mode images without alpha channels.

TIFF is a flexible bitmap image format supported by all paint, page layout, and image editing. TIFF documents have a maximum file size of 4 GB. TIFF image format allows for lossless compression.

3- JPEG image

Joint Photographic Experts Group (JPEG) format is commonly used to display photographs in HTML documents. JPEG format supports RGB, and grayscale color modes, and does not support transparency. The JPEG format retains all color information in an RGB image but compresses file size by selectively discarding data. A JPEG format is a commonly used method of lossy compression for digital images. A JPEG file is created by choosing a range of compression qualities. When a JPEG image is converted from another format to JPEG, image quality is required to be specified.

4- PNG image

Portable Network Graphics (PNG) format is a raster graphics file format that supports lossless data compression, it is expected to replace the Graphics Interchange Format (GIF) that is widely used on today on the Internet.

PNG format supports RGB, grayscale, indexed color and bitmap mode images.

PNG preserves transparency in grayscale and RGB images. The PNG format was developed by an Internet commission expressly to be patent-free. PNG supports 24-bit images and produces background transparency without jagged edges; however, some web browsers do not support it.

2.5 Image Feature Models

2.5.1 Features Selection Based on Co-occurrence Matrix

A co-occurrence matrix or co-occurrence distribution is a matrix that defines an image to be the distribution of co-occurring pixel values (grayscale values, or colors) at a given offset**.** (Wiki/Co-occurrence matrix, 2016)**,** Figure 2.6 shows the Illustration of the co-occurrence matrix as a 3D function which was selected from (www.researchgate.net).

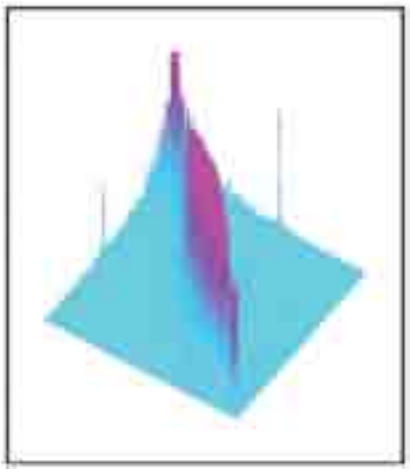

Figure 2.6: Illustration of the co-occurrence matrix as a 3D function.

2.5.2 GLCM (Gray Level Co-occurrence Matrix)

The gray level co-occurrence matrix (GLCM) is common technique in statistical image analysis that is used to estimate image properties related to second-order statistics. It was defined by Haralick et al (1973). It shows how often a pixel value

known as the sign pixel with the strength value (*i*) occurs in specific relationship to a pixel value known neighbor pixel with the strength value (*j*). So, each element (*i, j*) of the matrix is the number of case of the pair of the pixel with value (*i*) and a pixel with value j which are at a distance d about to each other. The GLCM is a measure of how often different combinations of pixel brightness values occur in an image. Because two samples are compared, GLCM is referred to as a second order texture classification method.

It is widely used for classification of satellite images (Eichkitz, Davies, Altmann, Schreilechner & de Groot, 2015).

(HAN, 1990) Defined 14 statistical features from the gray-level-co-occurrence matrix for texture classification. GLCM has shown to be effective in studying different images however no such claim can be made for image type. A statistical way of research work that considers the spatial relationship of pixels is the gray-level co-occurrence matrix (GLCM).

So, a GLCM is a histogram of co-occurring grey-scale values at a given offset over an image. The image statistic features are important clues to determine whether hiding information or not from the detection process.

Table 2.2 shows the properties of the image derived from GLCM.

Table 2.2: Properties of the image derived from GLCM.

Statistic	Description	Formula
Contrast	Measures the local variations in the gray-level co-occurrence matrix.	$\sum_{i,j} \lvert i-j \rvert^2 p(i,j)$
Correlation	Measures the joint probability occurrence of the specified pixel pairs.	$\sum_{i,j} \frac{(i-\mu i)(j-\mu j)p(i,j)}{\sigma_i \sigma_j}$
Energy	Provides the sum of squared elements in the GLCM. Also known as uniformity or the angular second moment.	$\sum_{i,j} p(i,j)^2$
Homogeneity	Measures the closeness of the distribution of elements in the GLCM to the GLCM diagonal.	$\sum_{i,j} \frac{p(i,j)}{1+\lvert i-j \rvert}$

2.5.3 CGCM (Color Gradient Co-occurrence Matrix)

The system was developed to detect RGB stego images with 24-bit depth (Haralick, Shanmugam, & Dinstein). An image database was formed to test and train the system. However, no single steganalysis method or tool can detect all types of steganography or support all available image formats. Therefore a need exists for enhancing steganalysis systems to deal with different image formats and to break different steganography methods .

Gong and Wang, in 2012 made the real achievement of the proposed system was performed within the decision-making model.

The detection system was prepared to work as a blind form of steganalysis. In this type of steganalysis, the system does not target particular steganography methods or specific image formats. The proposed system is based on read out statistical features from the color gradient co-occurrence matrix (CGCM), which is the most helpful detection technique regarding blind steganalysis (Aljarf, October 2013). Therefore, the proposed detection system was able to detect different types of stego images formed with various steganography methods. CGCM that are sensitive to the color interconnection between close pixels and breaks in image build.

2.6 Reasons for Choosing Steganalysis of Images

Image is the most available type of cover to hide a secret message over the internet. Also they can be used as carrier objects without raising much suspicion.
Image files have a lot of capacity redundancy, which provides space for embedding.
Therefore due to the wide use of images in information hiding, research work in steganalysis have addressed the problem of detecting hidden data inside various types of images.

2.7 Related Work

Steganalysis research has been investigating several aspects in the detection of hidden messages in stego images, including detecting the presence of a hidden message, estimating message length and extracting the message.

Also, features of cover media for steganalysis have been studied, in particular texture features of images, such as GLCM and Entropy.

Aveibas et al (2003) take the regress analysis to analyses image based an image metrics. Fridrich, Miroslav (2004) describe a new very accurate and reliable method that can detect LSB embedding in randomly scattered pixels in both 24-bit color images and 8-bit grayscale or color images. It is based on our previous work on lossless data embedding. By inspecting the differences in the number of regular and singular groups for the LSB and the “shifted LSB plane”, thy can reliably detect messages as short as 0.03bpp.

Arvis, et al (2004) have proposed a multispectral method considering the correlations between the colour bands. To study the efficiency of their method, they tested it in a classification problem on the image databases VisTex and Outex available on the internet. They also extended the co-occurrence method according to the two other approaches, which are: (fusion of texture and color descriptors and quantization of the color image) to have a comparison between the three approaches to the texture in color images.

Lyu, Farid (2004) described a universal steganalysis algorithm that exploits the inherent statistical regularities of natural images. The statistical model consists of rst and higher-order color wavelet statistics. A one-class support vector machine (OC-SVM) was employed for detecting hidden messages in digital images. The work

presented here builds on our earlier work where we used rst and higher-order grayscale wavelet statistics and a two-class support vector machine. The addition of color statistics provides a considerable improvement in overall detection accuracy. And, while a fully trained two-class SVM is likely to outperform an OC-SVM, the OC-SVM has the advantage that it is more likely to generalize to stego programs not previously seen by the classier. In addition, the training of the OC-SVM is simplied as it only requires training on the more easily obtained cover (non-stego) images.

Liu, Sung, Xu and Ribeiro (2006) proposed a scheme for steganalysis of LSB matching steganography based on feature extraction and pattern recognition techniques. Shape parameter of generalized Gaussian distribution (GGD) in the wavelet domain is introduced to measure image complexity. Several statistical pattern recognition algorithms are applied to train and classify the feature sets. Comparison of our method and others indicates our method is highly competitive. It is highly efficient for color image steganalysis. It is also efficient for grayscale steganalysis in the low image complexity domain. Zou et al (2006) proposed a supervised learning based on steganalysis method which uses two dimensinal Markov chain based framework to capture traces of message embedding. The proposed scheme in Zou et al (2006) uses local neighborhood of the current pixel to predict pixel values. The prediction-error image is then 4 generated by subtracting the predicted value from the actual pixel value and then comparing the different with a predened threes hold.

Liu, Sung, Xu and Ribeiro (2008) proposed a new metric of image complexity to enhance the evaluation of steganalysis performance. In addition, thy also present a scheme of steganalysis of least significant bit (LSB) matching steganography, based on feature mining and pattern recognition techniques. Compared to other well-known methods of steganalysis of LSB matching steganography.

Tomas pevny, Patrick bas and Jessica fridrich (2010), presents a method for detection of steganographic methods that embed in the spatial domain by adding a low-amplitude independent stego signal, an example of which is least significant bit (LSB) matching. First, arguments are provided for modeling the differences between adjacent pixels using first-order and second-order Markov chains. Subsets of sample transition probability matrices are then used as features for a steganalyzer implemented by support vector machines. The major part of experiments, performed on four diverse image databases, focuses on evaluation of detection of LSB matching. The comparison to prior art reveals that the presented feature set offers superior accuracy in detecting LSB matching. Even though the feature set was developed specifically for spatial domain steganalysis, by constructing steganalyzers for ten algorithms for JPEG images, it is demonstrated that the features detect steganography in the transform domain as well.

Jan Kodovský, Jessica Fridrich, Member, IEEE, and Vojtěch Holub (2010), propose an alternative and well-known machine learning tool ensemble classifiers implemented as random forests and argue that they are ideally suited for steganalysis. Ensemble classifiers scale much more favorably w.r.t. the number of training examples and the feature dimensionality with performance comparable to the much more complex SVMs. The significantly lower training complexity opens up the possibility for the steganalyst to work with rich (high-dimensional) cover models and train on larger training sets two key elements that appear necessary to reliably detect modern steganographic algorithms. Ensemble classification is portrayed as a powerful developer tool that allows fast construction of steganography detectors with markedly improved detection accuracy across a wide range of embedding methods. The power of

the proposed framework is demonstrated on three steganographic methods that hide messages in JPEG images.

Natarajan Meghanathan1 and Lopamudra Nayak (2010), analyzed the steganalysis algorithms available for three commonly used domains of steganography (Image, Audio and Video). Image steganalysis algorithms can be classified into two broad categories: Specific and Generic. The Specific steganalysis algorithms are based on the format of the digital image (e.g. GIF, BMP and JPEG formats) and depend on the underlying steganography algorithm used. The Generic image steganalysis algorithms work for any underlying steganography algorithm, but require more complex computational and higher-order statistical analysis.

Kang Leng Chiew (2011), investigated steganalysis that extract information related to a secret message hidden in multimedia document. He focused analysis on steganographic methods that use binary images as the medium for a secret message. The work organised according to the amount of information extracted about the hidden message.

Wang and Gong, (2012) proposed a steganalysis algorithm based on colors-gradient co-occurrence matrix (CGCM) for GIF images. CGC Misco structed with colors matrix and gradient matrix of the GIF image, and 27-dimensional statistical features of CGCM, which are sensitive to the color-correlation between adjacent pixels and the break in go fima get exture, are extracted. This proposed steganalysis algorithm does not require lot of computing time.

Ahd Aljarf (2013) has proposed a steganalysis system for both gray and color images based on four features which are contrast, energy, homogeneity and correlation, using grey images for steganography has many limitations. First, the capacity of hiding data is low, due to the fact that the image bit depth is always 8. Moreover, most of the

grey images are BMP file format. In addition, in case of converting them to another format, they will convert to color images. Otherwise, the resolution of these images will noticeably affect. However, in regards to the initial test, the co-occurrence function used in MATLAB supports the grey images only. This means this function has to be used with each single color channel in the color image. For example, extract the co-occurrence matrix for the red, green and blue channel; therefore, there will be three matrixes for each color image.

Veenu Bhasin, Punam Bedi (2013) proposes a novel blind Steganalysis process, for colored JPEG images. Extreme Learning Machine (ELM) has been used to classify the images into stego images and non-stego images. The feature set used for classification of images consists of 810 features. First 405 features are based on Markov random process applied on correlations among JPEG coefficients of image. Calibration is applied on these Markov features to get the remaining 405 features. These calibrated features are the difference between the Markov features of the image and Markov features of a reference image, obtained by decompressing, cropping and recompressing the image. Experimental results show that our proposed ELM based steganalysis method clearly outperforms other SVM based steganalysis methods in terms of percentage of correctly classified images and in terms of time taken for both training and testing. The fast speed of the proposed method due to fast learning time of ELM makes it useful for real-time steganalysis.

Manveer, Gagandeep (2014) proposed to extract the content of the image by some techniques in which we make an image blurred and up to some extent distortion. This so-called Kerckhoff's principle is always assumed in cryptography Critical review of the current Steganalysis algorithms that is used in the steganalysis technique.

Christoph Georg Eichkitz1, John Davies, Johannes Amtmann1, Marcellus Gregor Schreilechner1 and Paul de Groot (2015) demonstrate how gray level co-occurrence matrix can be adapted to work on 3D imaging of seismic data. GLCM can provide important insight into the subsurface through attribute analysis. Different authors have shown that the GLCM is a useful tool for the description of seismic facies. Because GLCM-based attributes can be calculated in different directions, they can be used to determine directional variations in seismic data. This opens the door to differentiate between sedimentary facies and patterns of fracturing, including the delineation of fractured zones and their strike and dip.

Cecilia Di Ruberto, Giuseppe Fodde and Lorenzo Putzu, (2015) proposed Different Color Spaces for Medical Color Image Classification. In order to extend the classical grey level texture features to color texture features they started by decomposing the color image into the three channels Ch1, Ch2 and Ch3, obtaining three different images. The most intuitive way to take into account color information for the computation of texture feature is to use the classical implementation and pass to them every time a different color channel. The results of the combination is a feature vector nine time larger than the classical feature vector, composed of three intra-channel feature vector (Ch1, Ch1), (Ch2, Ch2) and (Ch3,Ch3) and six inter-channels feature vector (Ch1, Ch2), (Ch2, Ch1), (Ch1, Ch3), (Ch3, Ch1), (Ch2, Ch3) and (Ch3, Ch2). The combination did not include the three channels as one vector.

Al-Taie (2017) presented a steganalysis model that is based on an enhanced GLCM feature set, in the analysis of gray-scale one channel images. The research included experimental results of analyzing a large number of gray-scale images from public datasets. The Discriminant Analysis two-category classifier was used in the proposed model. Table 2.3 summarizes the main features of the related work.

Table 2.3 the main features of the related work

Papers	Year	Features and Benefits
Aveibas	2003	take the regress analysis to analyses image based an image metrics
Fridrich, Miroslav	2004	Describe a new very accurate and reliable method that can detect LSB embedding in randomly scattered pixels in both 24-bit color images and 8-bit grayscale or color images. It is based on lossless data embedding.
Arvis	2004	Proposed a multispectral method considering the correlations between the color bands. To study the efficiency of their method, they tested it in a classification problem on the image databases VisTex and Outex available on the internet.
Lyu, Farid	2004	Described a universal steganalysis algorithm that exploits the inherent statistical regularities of natural images. The statistical model consists of rst and higher-order color wavelet statistics.
Liu, Sung, Xu and Ribeiro	2006	Proposed a scheme for steganalysis of LSB matching steganography based on feature extraction and pattern recognition techniques. Shape parameter of generalized Gaussian distribution (GGD) in the wavelet domain is introduced to measure image complexity
Zou	2006	Proposed a supervised learning based on steganalysis method which uses two dimensional Markov chain based framework to capture traces of message embedding.
Liu, Sung, Xu and Ribeiro	2008	Proposed a new metric of image complexity to enhance the evaluation of steganalysis performance. In addition, thy also present a scheme of steganalysis of least significant bit (LSB) matching steganography, based on feature mining and pattern recognition techniques
Tomas pevny, Patrick bas and Jessica fridrich	2010	Presents a method for detection of steganographic methods that embed in the spatial domain by adding a low-amplitude independent stego signal, an example of which is least significant bit (LSB) matching.
Jan Kodovský, Jessica Fridrich, Member, IEEE, and Vojtěch Holub	2010	Propose an alternative and well-known machine learning tool ensemble classifiers implemented as random forests and argue that they are ideally suited for steganalysis. Ensemble classifiers scale much more favorably w.r.t. the number of training examples and the feature dimensionality with performance comparable to the much more complex SVMs.
Natarajan Meghanathan1 and Lopamudra Nayak	2010	Analyzed the steganalysis algorithms available for three commonly used domains of steganography (Image, Audio and Video).
Kang Leng Chiew	2011	investigated steganalysis that extract information related to a secret message hidden in multimedia document
Wang and Gong	2012	Proposed a steganalysis algorithm based on colors-gradient co-occurrence matrix (CGCM) for GIF images. CGC Misco structed with colors matrix and gradient matrix of the GIF image, and 27-dimensional statistical features of CGCM

Ahd Aljarf	2013	proposed a steganalysis system for both gray and color images based on four features which are contrast, energy, homogeneity and correlation, Using grey images for steganography has many limitations
Veenu Bhasin, Punam Bedi	2013	Proposes a novel blind Steganalysis process, for colored JPEG images. Extreme Learning Machine (ELM) has been used to classify the images into stego images and non-stego images. The feature set used for classification of images consists of 810 features. First 405 features are based on Markov random process applied on correlations among JPEG coefficients of image
Manveer, Gagandeep	2014	Proposed to extract the content of the image by some techniques in which we make an image blurred and up to some extent distortion.
Christoph Georg Eichkitz1, John Davies, Johannes Amtmann1, Marcellus Gregor Schreilechner1 and Paul de Groot	2015	Demonstrate how gray level co-occurrence matrix can be adapted to work on 3D imaging of seismic data. GLCM can provide important insight into the subsurface through attribute analysis
Cecilia Di Ruberto, Giuseppe Fodde and Lorenzo Putzu	2015	Proposed Different Color Spaces for Medical Color Image Classification. In order to extend the classical grey level texture features to color texture features they started by decomposing the color image into the three channels Ch1, Ch2 and Ch3, obtaining three different images
Al-Taie, zaid	2017	Presented a steganalysis model that is based on an enhanced GLCM feature set, in the analysis of gray-scale one channel images.

Chapter 3

Methodology and the Proposed Model

3.1 Methodology Approach

This work follows an experimental approach for achieving the research objectives. Relevant data about secret and cover images will be analyzed as necessary to enhance the detection performance of the proposed model.

3.2 Outline of the Proposed Model

The proposed model aims to detect the existence of a hidden message that has been embedded inside an RGB cover image. The detection task is based on prior training of a classifier on the features of a dataset of clean and stego images, using supervised learning techniques. The statistical texture features of the proposed model consists of two parts: a single channel feature set and multi-channel feature sets. The single channel features set includes standard texture features as well as additional statistical features. The feature sets are used in the training and the detection phases.

3.3 Statistical Features Selection

The proposed model is founded on a channel-based feature set evaluation that will be combined into two or three channels feature sets for image-based steganalysis. The channel based feature set (CFS) consists of GLCM features, (Contrast, Correlation, Energy and Homogeneity), as well as other texture features such as Entropy, that was suggested by haralick (1973) in the study of texture features of images, and have been used in many steganalysis research work , Kang Leng Chiew (2011), Ahd Aljarf (2013) and Zaid Al-Taie (2017).

The single channel feature set consists of the features shown in table 3.1

Table 3.1 list of the selected single channel features

Feature Name	Feature Description
CC-LR	Correlation coefficient between LHB and RHB
CV-B	Coefficient of variation of full bytes
CV-R	Coefficient of variation of RHB
GLCM-B	Contrast, Correlation, Homogeneity Energy, of full bytes
GLCM-R	Contrast, Correlation, Homogeneity, Energy, of RHB
GLCM-3LSB	Contrast, Correlation, Homogeneity, Energy, of 3LSB
GLCM-4LSB	Contrast, Correlation, Homogeneity, Energy, of 4LSB
Entropy-B	Entropy of full bytes
Entropy-R	Entropy of RHB
Diff-R	Average of absolute difference between successive right half bytes
Skew-B	Skewness of full bytes
Skew-R	Skewness of RHB

3.3.1 Gray-Level Co-occurrence Matrix

The GLCM (Gray-level co-occurrence matrix) is a common technique in statistical image analysis, The GLCM, which is a square matrix can reveal certain properties of the spatial distribution of the Gray levels in the texture image.

The GLCM is created from a gray-scale image. The GLCM calculates how often a pixel with gray-level (grayscale intensity or Tone) value *i* occur either horizontally, vertically, or diagonally to adjacent pixels with the value *j*. Where *i* & *j* are the gray level values in the image.

GLCM is the two-dimensional matrix of joint probabilities Pd,θ (*i, j*) between pairs of pixels, separated by a distance d in a given direction θ. The GLCM is a measure

of how often different combinations of pixel brightness values occur in an image. Because two samples are compared, GLCM is referred to as a second order texture classification method. GLCM function result can be either logical or numeric, and it must contain real, non-negative, finite integers.

3.3.2 Entropy

A scalar value representing the entropy of grayscale image. Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image. Entropy is defined as a function that is represented mathematically as in the equation below:

$$Entropy = \sum_{i} pi \ \log_2 pi$$

Where p contains the histogram counts. In the proposed model, the entropy function will be calculated for full bytes and right half bytes.

3.3.3 Coefficient of Variation

A coefficient of variation (CV) is a statistical measure of the dispersion of data points in a data series around the mean. The coefficient of variation represents the ratio of the standard deviation to the mean. The CV metric is considered a useful statistic for comparing the degree of variation from one data series to another, even if the means are drastically different from one another. In this work the CV will be calculated for full bytes and half bytes.

3.3.4 Difference between Adjacent Bytes

This feature is used as a measure of the degree of change in intensity between adjacent bytes. The difference feature is calculated as the average of the absolute difference in value between every two adjacent bytes of an image.

It is assumed that a tampered image will have higher differences in the values of adjacent bytes than in clean images, due to the change introduced by bit replacement in bytes of the stego image. This feature can be calculated for the full byte or the right half byte. (Al-Taie, 2017).

3.3.5 Skewness

Skewness is a measure of the asymmetry of the probability distribution of a real-valued random variable about its mean. The skewness value can be positive or negative, or even undefined. (Kumar, Gupta, 2012).

3.3.6 Multi-Channel Feature Merge

In this work, an image is evaluated according to each individual channel, and using a multi-channel merge. When the three channels are evaluated separately, the steganalysis outcome will result in 'stego' decision if any of the three channels is classified as stego. The three channels feature sets will be combined to provide a full image feature set, as below:

- Channel-based feature set (CFS) for each of the (R, G, and B) channels.
- Dual channel feature set (RG, RB, GB) which are formed by merging two channel feature sets.
- Triple channel feature set, which is formed by merging feature sets of individual RGB channels.

3.4 The Classifier

The support vector machine (SVM) binary classifier will be used in the classification process. A comparison will be made with the QDA classifier, which is also used in steganalysis experimental work.

Implementation of the proposed model will use the SVM and QDA classifiers that are available in MATLAB.

3.4.1 Support Vector Machine

Support Vector Machine (SVM) is a supervised learning technique for classification. SVM is widely used and most popular in Machine learning community. The way to the success of SVM is the kernel function which maps the data from the original space into a high dimensional feature space. The SVM produces non-linear boundaries in the original space.

One of the most important advantage for the SVM is that it secure generalization to some extent. Because of the many properties of SVM, it has been widely applied to virtually every research field (Prakash, 2006).

In the implementation of this work is the SVM classifier in MATLAB is called as an out-of-the-box classifier (James, Witten, Hastie, & Tibshirani, 2013), and is given a training set and an unseen vector of features of an image. The output from the classifier is a single two category value (0, 1) about the outcome of classifying the unseen images.

3.5 The Proposed Model

The proposed steganalysis model is based on analyzing texture features of an RGB image, with the aim of detecting the existence of hidden data.

The model evaluates features of single channels, and combined features of dual and triple channels.

To realize the objectives of the proposed model, three processes are required:

- Steganography, which involves embedding of secret data inside cover images
- Feature extraction from clean and stego images
- Training and testing of a classifier based on the selected features and the classifier

3.6 Required Functionalities of the Proposed Model

- Steganography modules to embed a secret file inside an RGB image
- Feature extraction from a batch of clean and stego images
- Batch classification of a group of test images against a training set
- Single image classification, against a training set

3.7 The Proposed System

The steganalysis system for this study is developed to implement the required functionalities of the proposed model, the implementation of the proposed system which includes the required functionalities as below:

1- Phase 1: Embedding

The steganography methods that will be used for the stego images are the spatial domain 2LSB and 4LSB, with sequential embedding in single channels or three channels. Figure 3.1 shows a flow chart of embedding

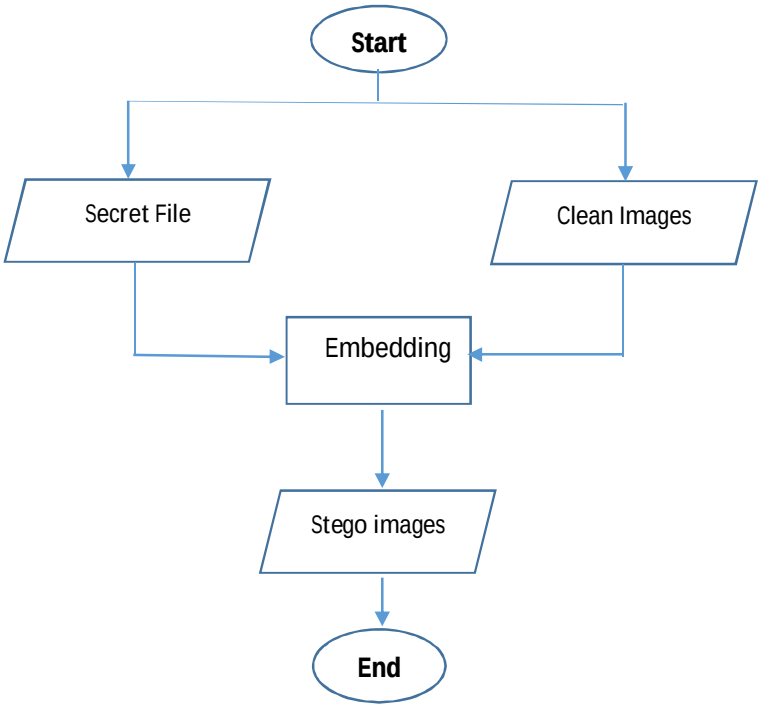

Figure 3.1 Flow chart of embedding

2- Phase 2: Feature Extraction

The selected channel based features are extracted from each color channel of clean and stego images. The features are extracted using built-in functions in MATLAB, including GLCM, Entropy, Correlation Coefficient, Standard deviation, mean, skewness. The coefficient of variation (CV) is calculated as below:

$$CV = \frac{\text{Standard Deviation (n)}}{\text{Mean (n)}}$$

Where n is vector of single bytes or parts of bytes.

Output from the feature extraction is a feature set file in Excel that contains features of single channels in separate worksheets. The feature set file is used in the creation of single channel and multi-channel training and testing files in CSV format (comma-separated-values), for processing by the classifier.

The training files, (single channel or multi-channel) are formed by margining equal number of clean and stego images features set data.

The testing (unseen) files contains feature set data of one or more images that are not part of the tanning data.

Figure 3.2 shows a flowchart of the Feature Extraction process.

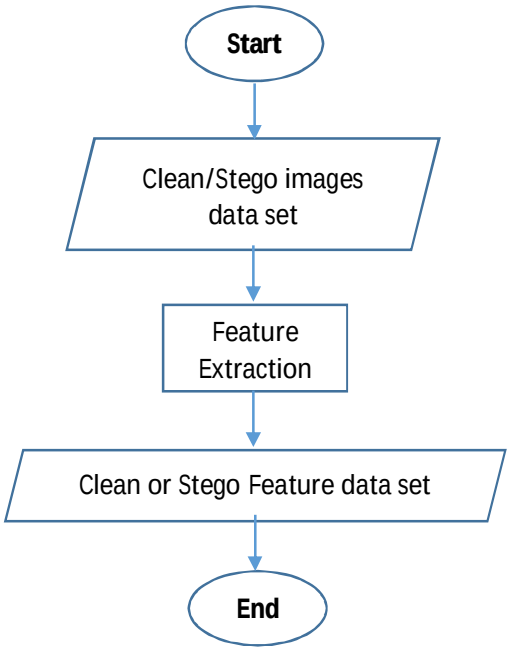

Figure 3.2 Flowchart of the Feature Extraction process

3- Phase 3: Single Image Classification

In this phase, the feature set vector of a single image is processed by the classifier, which represent the test data to be classified as clean or stego. The classifier is called twice, where in each run a different training file is used that represents a different stego scheme.

A testing (unseen) image is classified as stego if one of the classifiers classifies it as such. This represents a blind steganography approach where training data from multiple stego schemes are used. It is possible to include other training files from spatial or transform domain embedding stego schemes. Figure 3.3 shows a flowchart of the Single image Classification.

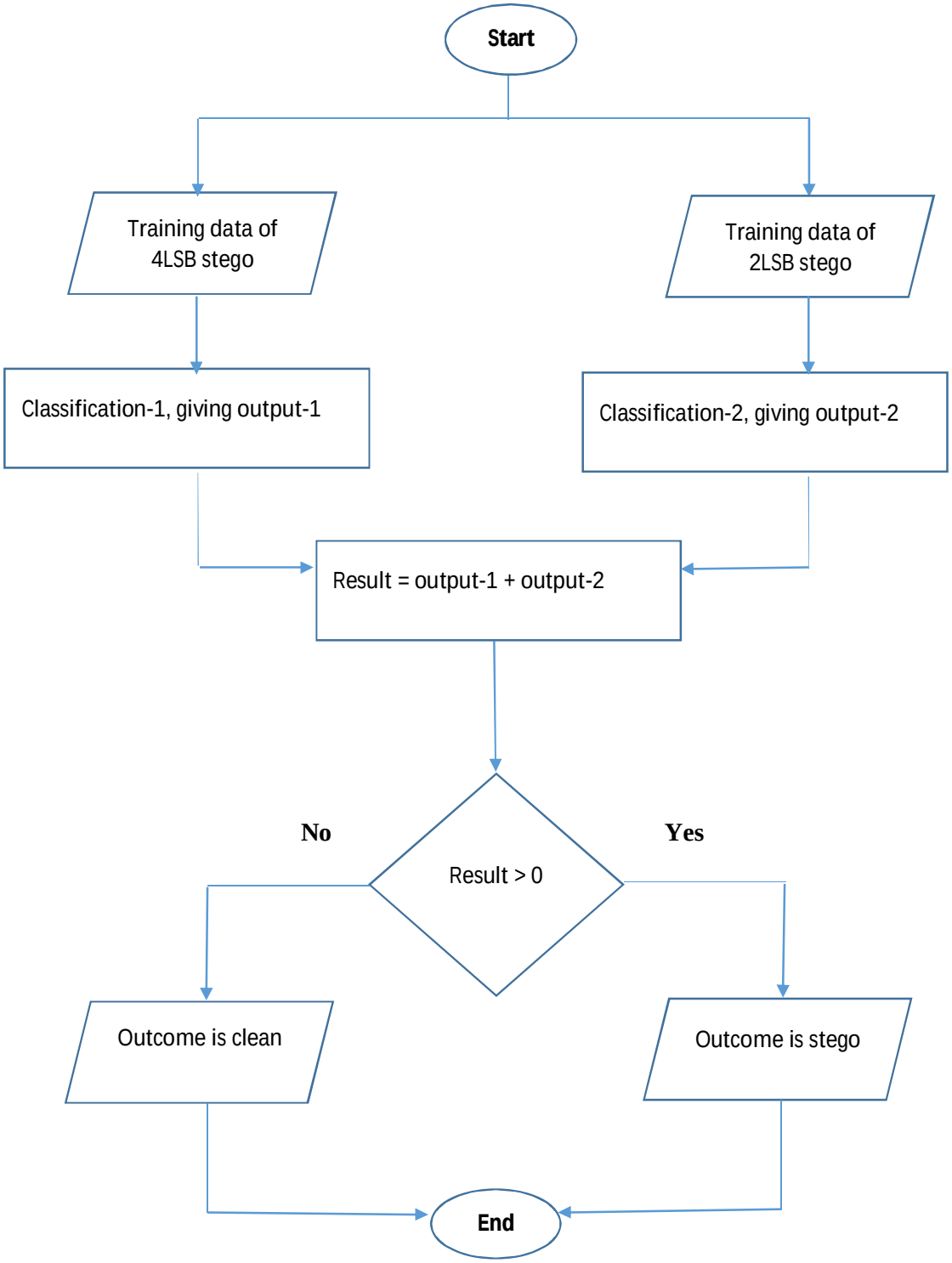

Figure 3.3 Flowchart of the single image classification process

4- Phase 4: Batch of Image Classification

In this phase, a batch of testing images are classified as in the single image classification phase. The feature set data of individual testing images are processed independently, giving the outcome for each image. The purpose of this phase is to simplify the process of classifying a large number of images.

3.8 Evaluation Metrics

The following metrics will be used in evaluating the detection performance of the proposed model:

- True Negative Rate (TN): The ratio of true negative detections to the number of clean images.
- True Positive Rate (TP): The ratio of true positive detections to the number of stego images.
- False Negative Rate (FN): The ratio of false negative detection to the number of stego images.
- False Positive Rate (FP): The ratio of false positive detection to the number of clean images.

- Detection Accuracy: The ratio of correctly detected clean and stego images to the total number of clean and stego images represent the detection accuracy (James, Witten, Hastie, & Tibshirani, 2013), as bellows:

$$\text{Accuracy} = (TN + TP) / (TN + TP + FP + FN).$$

Chapter 4

Experimental Results and Discussion

4.1 Introduction

The proposed model was implemented in MATLAB as a working system. A titled “Experimental Steganalysis System (ESS)”. The stego images that were analyzed in this work were created using two steganography models, the 2LSB model which embeds 2 bits per pixel (2 bpp) and 4LSB model, which embed 4 bits per pixel (4 bpp). The experimental work included embedding of secret images in two training datasets and one testing dataset (in three channels or one channel), features extractions, training and validation, and testing.

4.2 Clean Image Dataset Creation

The selected clean cover image type is the uncompressed BMP-RGB in three channels. Two dataset were used, for dual validation. The first validation dataset consists of 1500 clean images that were downloaded from the Natural Resources Conservation (NRC) image dataset (www.photogallery.sc.egov.usda.gov). The original NRC images were converted from TIFF to BMP format, and resized to (512×512 dimensions). The second validation dataset is based on the Caltech bird's images dataset (www.vision.caltech.edu), which is in color JPG formats. A set of 1500 Caltech images were converted to BMP format, (512×512 dimensions). Figure 4.1 and 4.2 shows a sample of the NRC and Caltech images one of the converted images. The testing dataset consists of a set of 1000 NRC images that were not part of the training dataset, and were converted to uncompressed PNG format, (512×512 dimensions), to test the model on an alternative RGB format.

The clean images from the training and testing datasets were embedded with different secret images to generate the stego datasets.

Figure 4.1 Sample of NRC cover image.

Figure 4.2 Sample of Caltech cover image.

For the secret image, we have used two images; one for high capacity embedding using the 4LSB scheme and the other for low capacity embedding using 2LSB scheme.

The secret image for high capacity embedding is the, the house.bmp image from SIPI dataset was chosen (www.sipi.usc.edu). Figure 4.3 shows the house.bmp. It was resized to fit the maximum hiding capacity of the selected cover images using 4LSB, i.e. its size is equal to 50% of the cover size.

Figure 4.3 The secret image house.bmp (360×360, 379 KB)

(www.sipi.usc.edu)

The secret image for low hiding capacity experiments were conducted. The image Peppers.jpg, shown in figure 4.4, was selected from the Gonzales dataset (www.imageprocessingplace.com). It was resized to fit the maximum hiding capacity of the selected cover images using 2LSB, i.e. its size is equal to 25% of the cover size.

Figure 4.4 The secret image peppers.bmp (254×254, 189 KB)

(www.imageprocessingplace.com)

For single channel embedding using the 2LSB technique, the secret image Harvard.jpg was used, as shown in Figure 4.5, which was selected form wikimedia.org images.

Figure 4.5 The secret image Harvard.jpg (354×520, 63 KB), (wikimedia.org images)

4.3 Experimental Work

This research work is based on an experimental evaluation of the proposed model using an RGB cover image dataset. The cover images are uncompressed, RGB images.

The experimental work is carried out in the stages shown in activity diagram

Figure 4.6

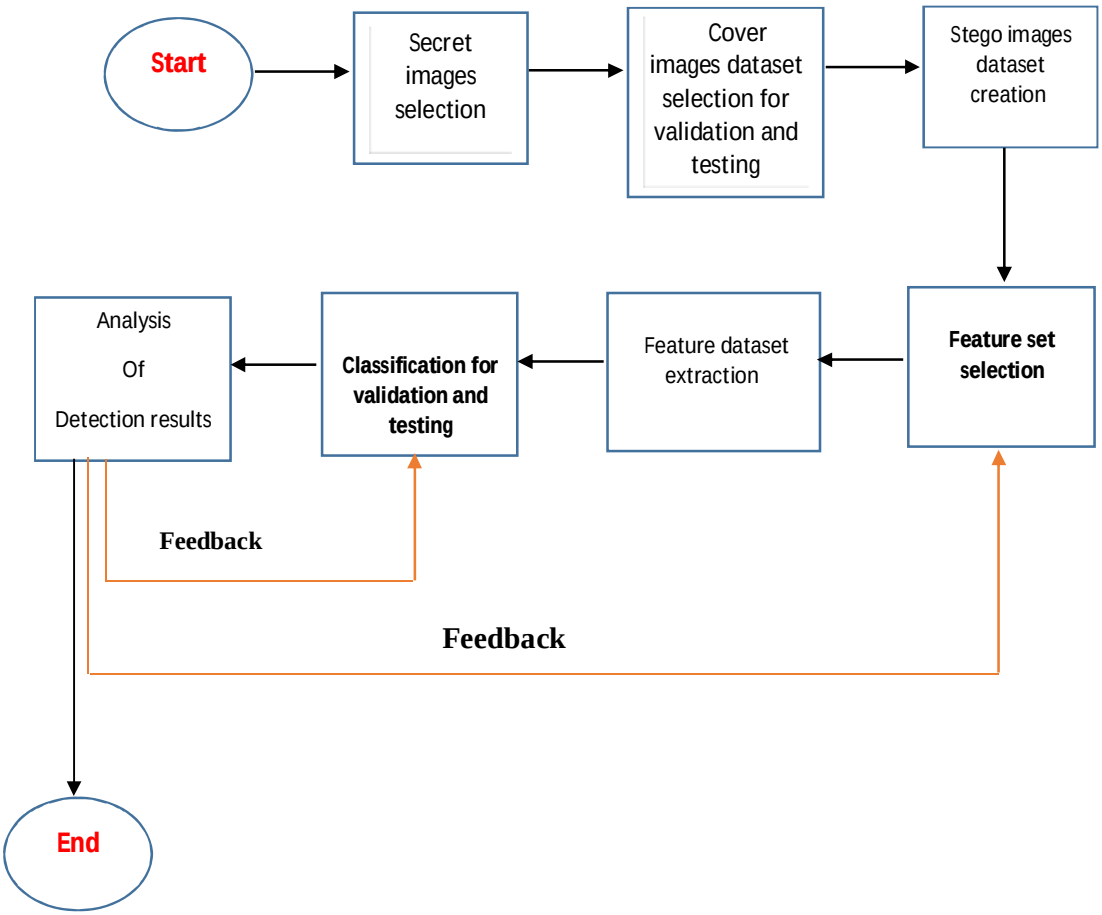

Figure 4.6: Stages of the experimental work

4.4 Training and Field Testing Steps

To proceed with training and testing, the clean and stego image datasets were created as in the following steps.

1- Dataset creation: two datasets of 1500 clean images each, for training and validation, and 1000 images for testing using additional images that were not part of the training dataset.

2- Steganography set creation: the selected secret images were embedded in the selected cover image datasets to create two stego images dataset, as below:

   a. **4-bit stego datasets for validation:** two stego dataset were created using the LSB replacement technique, where 4LSB bits were replaced in every channel, which provides for maximum hiding capacity that does not cause visible distortion in an image.

   b. **2-bit stego dataset for validation:** this dataset was created using the LSB replacement technique, in which 2LSB bits were replaced in every channel, which provides for maximum hiding capacity that does not cause visible distortion in an image. The dataset consists of two parts, for validation and for testing. The dataset was created from the clean image datasets.

   c. **2-bit stego dataset for blue channel embedding validation:** this dataset was created using the 2LSB method, which was applied to the blue channel only.

   d. **2-bit stego dataset for testing:** this stego dataset was created using the 2LSB technique for embedding in 1000 PNG images from the NRC dataset.

3- Feature extraction: The selected features were extracted from the training and testing dataset, using the feature extraction module. Table 4.1 shows a sample of the extracted features from one color channels. The full feature set from the entire dataset collection have been uploaded to (www. data.mendeley.com). The feature sets are groped in to validation datasets and training datasets as below:

a. Feature extraction of validation datasets: using the proposed feature set, the clean and stego images, have been processed and the features extracted, which resulted in clean image feature dataset and three stego image feature datasets.
b. Feature extraction of the testing dataset: the clean and stego testing data sets were processed and their features were extracted for analysis.

4- Classification for cross-validation: the chosen classifiers are the SVM and DA algorithms that are available in the MATLAB environment. The classification process utilized the clean and stego images for validation and testing.

Two thirds of each validation dataset is used for training and the remaining third part is used for testing. The training subset were labelled as stego or clean, while the testing subset were unlabeled. A 3-fold cross validation were used to calculate the detection accuracy of the proposed model.

5- Field testing: in this step, a testing dataset of 1000 clean images and 1000 stego images were classified, based on training of the classifier using the full validation image set of 1500 clean and 1500 stego images. The detection accuracy for the field testing were calculated based on the results of classification of the 2000 images, for the Natural Resources Conservation (NRC) PNG dataset.

Table 4.1: feature set sample (part-1:12 columns) cont.

			GLCM-Byte				GLCM-4LSB			
CC-LR	CVH	CVR	Contrast	CC	Energy	Homogn	Contrast	CC	Energy	Homogn
-0.0869	0.7660	0.6231	1.3430	0.7721	0.0894	0.7569	5.8633	0.0294	0.7714	0.8953
-0.0767	0.6886	0.6136	0.5696	0.8896	0.1384	0.8470	5.4753	0.0557	0.7849	0.9022
-0.1565	0.6814	0.6232	0.2386	0.9435	0.1430	0.9047	5.6809	0.0655	0.7734	0.8986
-0.1944	0.7970	0.6219	0.4026	0.9425	0.1229	0.8955	6.0310	0.1489	0.7474	0.8923
-0.2842	0.8714	0.5276	0.2011	0.9553	0.1748	0.9255	4.2405	0.1077	0.8340	0.9243
-0.0582	0.5326	0.6128	0.3458	0.9118	0.1377	0.8873	5.3426	0.0547	0.7875	0.9046
-0.1166	0.5222	0.6171	0.4277	0.8558	0.1367	0.8578	5.5654	0.0563	0.7790	0.9006
-0.1029	0.5148	0.6017	0.3112	0.8936	0.1307	0.8714	5.4416	0.0558	0.7861	0.9028
-0.1654	0.7812	0.6058	0.5360	0.8914	0.1138	0.8644	5.6830	0.0579	0.7743	0.8985
-0.1742	0.9611	0.5966	0.4963	0.8966	0.1544	0.8597	5.7557	0.0417	0.7738	0.8972
-0.1380	0.7553	0.6062	0.5379	0.9030	0.1008	0.8393	5.5661	0.0492	0.7798	0.9006
-0.1368	0.7842	0.6095	0.5729	0.8693	0.1555	0.8580	5.6016	0.0674	0.7762	0.9000
-0.1166	0.7426	0.5977	0.5124	0.9199	0.0983	0.8528	5.3815	0.0721	0.7839	0.9039
-0.0298	0.7417	0.6560	0.5590	0.8953	0.1200	0.8205	6.0476	0.1034	0.7542	0.8920
-0.0717	0.6736	0.6215	0.6042	0.9253	0.1046	0.8287	5.6813	0.0423	0.7764	0.8985
-0.0791	0.8484	0.6146	0.9420	0.8242	0.1270	0.7761	5.5175	0.0429	0.7824	0.9015
0.0386	0.8542	0.5991	0.4721	0.9333	0.1972	0.8483	5.4409	0.0349	0.7882	0.9028
-0.0894	0.7058	0.6138	0.3779	0.8673	0.2414	0.8569	5.6790	0.0153	0.7798	0.8986
-0.0307	0.7345	0.6196	0.6671	0.9107	0.1326	0.8349	5.6372	0.0581	0.7761	0.8993
-0.0223	0.7674	0.6171	0.5571	0.9220	0.1786	0.8569	5.3710	0.0336	0.7890	0.9041
-0.0248	0.7886	0.6065	0.3886	0.9280	0.2238	0.8681	5.4960	0.0293	0.7849	0.9019
-0.0516	0.6370	0.6226	0.3481	0.9611	0.0912	0.8735	5.3497	0.0649	0.7880	0.9045
-0.0495	0.5838	0.6187	0.3759	0.9362	0.1025	0.8542	5.4902	0.0399	0.7838	0.9020
-0.0730	0.6242	0.6349	0.2427	0.9657	0.1181	0.9018	5.6337	0.0579	0.7761	0.8994
-0.0599	0.7477	0.6241	0.4983	0.9277	0.1467	0.8499	5.5482	0.0551	0.7798	0.9009
-0.0175	0.6442	0.6237	0.3568	0.9227	0.1579	0.8832	5.8671	0.0786	0.7646	0.8952
0.0017	0.8811	0.6598	0.3690	0.9549	0.1896	0.8855	5.5837	0.1042	0.7718	0.9003
-0.1305	0.9694	0.5994	0.9006	0.8886	0.1050	0.7871	5.4730	0.0378	0.7847	0.9023
-0.1644	0.7757	0.5933	0.6315	0.8842	0.1123	0.8130	5.4787	0.0267	0.7858	0.9022
-0.0911	0.7031	0.6348	0.3930	0.9055	0.1343	0.8514	5.9803	0.0347	0.7664	0.8932
-0.0347	0.6351	0.6347	0.3598	0.9055	0.1471	0.8655	5.8491	0.0469	0.7696	0.8956
-0.0782	0.6046	0.6036	0.4477	0.9093	0.1235	0.8439	5.4955	0.0304	0.7848	0.9019
-0.0381	0.7161	0.6264	0.8858	0.8587	0.0991	0.8001	5.7317	0.0420	0.7746	0.8976
-0.0658	0.7133	0.6198	0.6893	0.9039	0.0875	0.8283	5.5972	0.0544	0.7780	0.9001
-0.1038	0.5911	0.6141	0.3389	0.8499	0.2541	0.8735	5.6144	0.0109	0.7827	0.8997
-0.0741	0.6999	0.6183	0.4044	0.8674	0.2239	0.8656	5.7190	0.0189	0.7779	0.8979
-0.0896	0.6984	0.6134	0.4374	0.8419	0.2145	0.8605	5.6643	0.0163	0.7803	0.8989
-0.1059	0.4678	0.6349	0.1599	0.9162	0.2106	0.9248	5.9415	0.0657	0.7637	0.8939
-0.1495	0.4616	0.6182	0.1920	0.8622	0.3016	0.9205	5.6843	0.0408	0.7765	0.8985
-0.0843	0.5676	0.6206	0.3376	0.9142	0.1373	0.8663	5.6973	0.0227	0.7783	0.8983
-0.1143	0.5710	0.6110	0.4343	0.8099	0.2011	0.8464	5.6084	0.0054	0.7836	0.8999
-0.1836	0.6882	0.5928	0.3976	0.8749	0.1828	0.8649	5.4338	0.0212	0.7881	0.9030
-0.1798	0.7477	0.5885	0.4561	0.8732	0.1505	0.8563	5.3396	0.0260	0.7910	0.9047
-0.1747	1.1496	0.5380	0.4777	0.9229	0.2273	0.8812	4.2087	0.2766	0.8028	0.9248
-0.0365	0.8164	0.6621	0.3396	0.9557	0.1296	0.8952	5.8925	0.1498	0.7528	0.8948

Table 4.1: feature set sample (part-2:12 columns)

GLCM-3LSB				GLCM-2LSB								
Contrast	CC	Energy	Homog	Contrast	CC	Energy	Homog	EntroB	EntrR	M-Diff	Skew-B	Skew-R
10.351	0.015	0.619	0.815	18.256	0.005	0.392	0.674	7.415	0.351	4.802	0.754	-0.020
10.430	0.019	0.616	0.814	18.193	0.004	0.394	0.675	7.370	0.334	4.610	0.504	-0.002
10.077	0.037	0.623	0.820	18.261	0.015	0.388	0.674	7.233	0.353	4.217	0.691	-0.037
9.854	0.091	0.618	0.824	17.371	0.051	0.398	0.690	7.295	0.397	3.892	0.630	-0.165
7.809	0.088	0.691	0.861	16.783	0.102	0.393	0.700	6.775	0.291	3.104	0.946	-0.435
10.210	0.034	0.619	0.818	18.305	0.006	0.390	0.673	7.464	0.333	4.343	0.510	-0.002
10.461	0.035	0.611	0.813	18.256	0.007	0.391	0.674	7.318	0.344	4.353	0.701	-0.005
10.459	0.016	0.615	0.813	18.313	0.003	0.391	0.673	7.264	0.333	4.629	0.809	-0.065
9.803	0.033	0.633	0.825	18.318	0.015	0.387	0.673	7.225	0.351	4.343	0.763	-0.142
9.612	0.034	0.639	0.828	18.009	0.021	0.392	0.678	6.780	0.349	4.371	1.268	-0.192
10.073	0.029	0.625	0.820	18.114	0.015	0.392	0.677	7.480	0.342	4.513	0.780	-0.091
10.057	0.040	0.623	0.820	17.973	0.024	0.392	0.679	7.227	0.349	4.291	1.514	-0.087
9.890	0.042	0.628	0.823	18.041	0.038	0.385	0.678	7.593	0.340	4.339	0.819	-0.123
10.541	0.053	0.604	0.812	17.800	0.024	0.396	0.682	7.363	0.382	4.660	0.833	0.094
10.152	0.026	0.623	0.819	18.345	0.010	0.388	0.672	7.530	0.346	4.619	0.217	-0.022
10.212	0.028	0.621	0.818	18.101	0.013	0.393	0.677	7.298	0.338	4.737	1.381	-0.010
10.238	0.027	0.620	0.817	17.948	0.016	0.396	0.680	7.023	0.333	4.725	1.486	-0.076
10.516	0.008	0.615	0.812	18.294	0.005	0.391	0.673	6.856	0.338	5.092	2.321	-0.013
10.596	0.030	0.608	0.811	18.174	0.011	0.392	0.675	7.645	0.348	4.766	0.814	0.001
10.428	0.021	0.615	0.814	18.165	0.010	0.392	0.676	7.492	0.329	4.640	0.899	0.036
10.792	0.034	0.600	0.807	18.306	0.008	0.389	0.673	6.921	0.334	4.878	2.043	-0.013
10.388	0.040	0.612	0.814	18.011	0.013	0.395	0.678	7.818	0.336	4.281	0.259	0.061
10.247	0.029	0.619	0.817	18.079	0.013	0.394	0.677	7.686	0.336	4.695	0.759	0.015
10.468	0.031	0.611	0.813	18.201	0.013	0.390	0.675	7.733	0.348	4.360	0.447	0.088
10.454	0.030	0.612	0.813	18.063	0.016	0.393	0.677	7.521	0.343	4.639	0.736	0.023
10.570	0.042	0.606	0.811	18.139	0.011	0.392	0.676	7.289	0.365	4.395	0.511	-0.036
10.538	0.052	0.604	0.812	18.276	0.014	0.388	0.674	7.091	0.359	4.063	0.862	0.195
9.897	0.030	0.631	0.823	17.745	0.017	0.401	0.683	7.193	0.335	4.648	1.252	-0.093
9.774	0.021	0.637	0.825	17.502	0.022	0.405	0.687	7.252	0.332	4.730	1.353	-0.129
10.483	0.016	0.614	0.813	18.119	0.015	0.391	0.676	7.259	0.358	4.949	1.331	0.014
10.810	0.017	0.604	0.807	18.415	0.003	0.389	0.671	7.311	0.355	4.844	1.111	0.070
10.416	0.017	0.616	0.814	18.457	0.004	0.387	0.670	7.352	0.334	4.713	0.518	-0.062
10.529	0.020	0.612	0.812	18.235	0.006	0.392	0.674	7.565	0.348	4.708	0.697	0.017
10.184	0.030	0.621	0.818	18.213	0.013	0.390	0.675	7.623	0.345	4.418	0.479	-0.025
10.720	0.000	0.610	0.809	18.352	0.000	0.391	0.672	6.897	0.334	5.082	1.504	0.004
10.577	0.009	0.613	0.811	18.286	0.005	0.391	0.673	6.988	0.341	4.970	2.026	-0.001
10.403	0.007	0.619	0.814	18.292	0.005	0.391	0.673	6.957	0.338	5.014	2.020	-0.028
10.734	0.027	0.604	0.808	18.294	0.007	0.390	0.673	6.949	0.365	4.687	0.179	0.032
10.516	0.015	0.613	0.812	18.368	0.001	0.390	0.672	6.654	0.346	4.616	1.564	-0.015
10.650	0.007	0.611	0.810	18.278	0.000	0.393	0.674	7.472	0.341	4.945	0.721	0.018
10.613	0.002	0.613	0.810	18.306	0.002	0.392	0.673	7.011	0.333	5.112	1.479	-0.006
9.837	0.018	0.635	0.824	17.946	0.024	0.393	0.680	6.915	0.329	4.802	1.807	-0.141
9.835	0.021	0.635	0.824	17.837	0.015	0.399	0.681	7.035	0.325	4.671	1.491	-0.121
7.647	0.188	0.676	0.863	15.354	0.147	0.418	0.726	6.605	0.341	3.317	1.589	-0.442
10.206	0.096	0.605	0.818	17.218	0.047	0.403	0.693	7.313	0.390	3.718	0.648	0.082

4.5 Results and Discussion

4.5.1 Cross Validation Results Using the NRC Dataset

1- Cross Validation results for three channels using 1500 NRC images dataset with 4LSB model for embedding and SVM for classifier, are presented in Table 4.1, which shows the detection accuracy and confusion matrix results for RGB channels. The rest of results for single and dual channels are shown in appendix A

Table 4.2: 3-fold cross validation results of the RGB channels 4LSB stego images using the NRC dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.00%**
TN	**100.00%**
TP	**100.00%**
Accuracy	**100.00%**

2- Validation results for three channels using 1500 NRC images dataset with 4LSB model for embedding and DA for classifier, are presented in Table 4.2 witch shows the detection accuracy and confusion matrix results for the RGB channels. The rest of results for single and dual channels are shown in appendix A

Table 4.3: 3-fold cross validation results of the RGB channels 4LSB stego images using the NRC dataset with DA classifier

Metric	Average of 3 folds (%)
FN	**0.67%**
FP	**0.00%**
TN	**100.00%**
TP	**99.33%**
Accuracy	**99.67%**

3– Cross Validation results for single channel using NRC images dataset with 2LSB model for embedding and SVM for classifier. The blue channel was embedded with secret, to verify the detection performance when only one channel is used for embedding. Table 4.3 shows the detection accuracy results for the RGB channels, which is similar to the strong results when all the channels were embedded with secret data. This demonstrates the detection power of the proposed model and the classifier even when less distortion is added to the stego images.

Table 4.4 : 3-fold cross validation results of the RGB channels 2LSB stego images using the NRC dataset with SVM classifier (Blue channel embedding only)

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.00%**
TN	**100.00%**
TP	**100.00%**
Accuracy	**100.00%**

4- Cross validation results for three channels using NRC images dataset with 2LSB model for embedding and SVM for classifier. Table 4.4 shows the detection accuracy and confusion matrix results for RGB channels. The rest of results for single and dual channels are shown in appendix A.

Table 4.5: 3-fold cross validation results of the RGB channels 2LSB stego images using the NRC dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.07%**
FP	**0.07%**
TN	**99.93%**
TP	**99.93%**
Accuracy	**99.93%**

4.5.2 Validation Results Using the Caltech Dataset

1-Validation results for three channel using Caltech images dataset using 2LSB for embedding and SVM for classifier, Table 4.5 shows the detection accuracy and confusion matrix results for RGB channels. The rest of results for single and dual channels are shown in appendix B.

Table 4.6: 3- fold cross validation results of the RGB channels 2LSB stego images using the Caltech dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.07%**
TN	**99.93%**
TP	**100.00%**
Accuracy	**99.97%**

5-Validation results for three channel using Caltech images dataset using 4LSB for embedding and SVM for classifier, Table 4.6 shows the detection accuracy and confusion matrix results for RGB channels. The rest of results for single and dual channels are shown in appendix B.

Table 4.7: 3-fold cross validation results of the RGB channels 4LSB stego images using the Caltech dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.47%**
FP	**1.33%**
TN	**98.67%**
TP	**99.53%**
Accuracy	**99.10%**

4.5.3 Testing Results

The field test used 1000 PNG images from the NRC dataset that were not part of the training dataset. The training dataset consisted of 3000 clean and 2LSB stego images of the NRC dataset BMP format. Table 4.7 shows the detection accuracy and confusion matrix results using 2LSB for embedding and SVM for classifier, which confirm the results obtained in the validation step.

Table 4.8 Testing results of the RGB channels 2LSB PNG stego images using the NRC dataset with SVM classifier.

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.00%**
TN	**100.00%**
TP	**100.00%**
Accuracy	**100.00%**

Chapter 5

Conclusion and Future Work

5.1 Conclusion

This thesis presented a steganalysis model to detect the existence of hidden data inside RGB color images, using statistical texture features of the stego images. The selected feature sets were extracted from datasets of clean and stego images, and classified using the Support Vector Machine algorithm. The focus of this work was on analyzing the individual color channels separately, using channel feature set, then to combine features of dual channels, as well as features of the three channels. A dataset of 1500 images were used for training, while testing was performed on two datasets of 1000 images each. Three secret images of different sizes (small, medium, large) were used to generate the stego images, which were embedded using the 2LSB and 4LSB methods.

Taking into consideration the experimental results of cross validation and testing, the following conclusions are made:

1. The proposed model has given very high accuracy of over 99% for the combined RGB channels features as well as for dual channel combinations and single channels, despite the difference in the number of features.

2. When embedding in one channel only (the blue channel) there was no reduction in the detection accuracy, which confirms robustness of the proposed model even when two channels remain clean. Therefore, if only one channel is embedded with data, we can use the detection outcome of this channel as an indicator for the entire image.

3. Reducing embedded data size did not affect the detection accuracy.

4. The results confirm that the SVM classifier is a better choice than the DA classifier for this type of analysis and data sizes.

4. Using 2LSB embedding gave similar results to 4LSB, despite the higher distortion caused by the 4LSB method.

5.2 Suggestions for Future Work

No research is complete, and one research work can provide ideas for further work. Based on the outcome of the present research, the following ideas are suggested for future research:

1. Extending the proposed model to deal with other types of cover media such as lossy compressed color images, color images with the alpha channel, and audio and video media.

2. Investigating the steganalysis of images produced by other steganography models such as the transform domain models.

3. Creating a public stego images datasets that are based on various steganography models, for comparison of steganalysis methods.

References

Abdulrahman, H., Chaumont, M., Montesinos, P., & Magnier, B. (2015). *Color image steganalysis using correlations between RGB channels*. In Availability, Reliability and Security (ARES), 10th International Conference on (pp. 448-454). IEEE.

Aljarf, A., Amin, S., Filippas, J., & Shuttelworth, J. (2013). *Develop a detection system for grey and colour stego images*. International Journal of Modeling and Optimization, 3(5), 458.

Al-Taie, Z. H. (2017). *Statistical Steganalysis Detector Model for 8-bit Depth Images* (Doctoral dissertation, Middle East University).

Badr, S. M., Ismaial, G., & Khalil, A. H. (2014). *A Review on Steganalysis Techniques: From Image Format Point of View*.

Battle, B. P., Prasad, R. S., REDDY, I. P., RAM, B. S., SONPIMPLE, M., BAPAT, P., & ALMAHAMID, S. (2005). *Essentials of image steganalysis measures.* Journal of Theoretical and Applied Information Technology.

Bhasin, V., & Bedi, P. (2013). *Steganalysis for JPEG images using extreme learning machine*. IEEE International Conference on Systems, Man, and Cybernetics (pp. 1361-1366). IEEE.

Caltech-UCSD Birds-200-2011 Dataset (2016), http://www.vision.caltech.edu/visipedia/CUB-200-2011.html, viewed on 1/10/2016.

Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). *Digital image steganography: Survey and analysis of current methods*. Signal Processing.

Chiew, K. L. (2011). *Steganalysis of binary images*. Macquarie University.

Coron, J.S. (2006). *What is cryptography?* IEEE Security and Privacy.

Eichkitz, C. G., Davies, J., Altmann, J., Schreilechner, M. G., & de Groot, P. (2015). *Grey level co-occurrence matrix and its application to seismic data*. First break, 33(3), 71-77.

Goljan, M., Fridrich, J., & Cogranne, R. (2014). *Rich model for steganalysis of color images.* IEEE International Workshop on Information Forensics and Security (WIFS) (pp. 185-190). IEEE.

Gong, R & Wang, H. (2012) *Steganalysis for GIF images based on colors-gradient co-occurrence matrix.* Optics Communications, (vol. 285), no. 24, pp. 4961-4965.

Haralick, R.M., Shanmugam, K. & Dinstein, I. (1973). *Textural features for image classification*, IEEE Trans. on Systems, Man and Cybernetics.

Harmsen, J.J. & Pearlman, W. A. (2003). *Steganalysis of additive-noise modelable information hiding*, In Electronic Imaging International Society for Optics and Photonic.

http://www.imageprocessingplace.com/root_files_V3/image_databases.htm, Gonzales dataset

Jain, R. (2014). *An extensive survey on image steganography*. International Journal of Emerging Technology and Advanced Engineering.

James, G., Witten, D., Hastie, T., & Tibshirani, R. (2013). *An introduction to statistical learning* (Vol. 6). New York: springer.

Kumar, V., & Gupta, P. (2012). Importance of statistical measures in digital image processing. *International Journal of Emerging Technology and Advanced Engineering*, *2*(8), 56-62.

Liu, Q., Sung, A. H., Xu, J., & Ribeiro, B. M. (2006). *Image complexity and feature extraction for steganalysis of LSB matching steganography*. In Pattern Recognition, 2006. ICPR 2006.

Lubenko, I., & Ker, A. D. (2012). *Going from small to large data in steganalysis*. Media Watermarking, Security, and Forensics.

Luo, X., Wang, D., Wang, P & Liu, F. (2008). *A review on blind detection for image steganography*. Signal Processing, (vol. 88).

Manveer Kaur1 & Gagandeep Kaur2. (2014). *Review of various steganalysis techniques*.

Miche, Y. (2010). *Developing fast machine learning techniques with applications to steganalysis problems* (Doctoral dissertation, Institut National Polytechnique de Grenoble-INPG).

Mishra, R., & Bhanodiya, P. (2015). *A review on steganography and cryptography*. In Computer Engineering and Applications (ICACEA), International Conference on Advances in (pp. 119-122). IEEE.

Mohammadi, F. G., & Abadeh, M. S. (2012). *A survey of data mining techniques for steganalysis*. Recent Advances in Steganography, 1-25.

NRCS Photo Gallery natural resource and conservation related photos, https://photogallery.sc.egov.usda.gov/res/sites/photogallery.

Olguin-Garcia, H. J., Juarez-Sandoval, O. U., Nakano-Miyatake, M., & Perez-Meana. H. (2015). *Color image steganalysis method for LSB matching*. Computer Engineering and Applied Computing (World Comp) (pp. 27-30).

Patel, C. B., Wandra, K. H., & Shah, S. (2016). *Pixel swapping and parity based image steganography algorithm*. In Electrical, Electronics and Computer Science (SCEECS).

Paul, R. T. (2011). *Review of robust video watermarking techniques.* IJCA Special Issue on Computational Science.

Prakash, G. S. (2006). *Measures for Classification and Detection in Steganalysis* (Doctoral dissertation, Indian Institute of Science, Bangalore).

Schaathun, H. G. (2012). *Machine learning in image steganalysis*, Wiley and Sons,

Sujatha, P. Purushothaman, S. & Rajeswari, R. (2012). *Detecting the presence of hidden information using back propagation neural network classifier.* International Journal of Computer Science and Information Security.

Swanson, M.D., Kobayashi, M., Tewfik, A.H. (1998). *Multimedia data-embedding and watermarking technologies*, Proc of the IEEE, (vol. 86), no. 6, pp. 1064-1087.

Thiyagarajan, P. Aghila, G. & Venkatesan, V. P. (2012). *Steganalysis using color model conversion.*

Westfeld, A. & Pfitzmann, A. (2000). *Attacks on Steganographic Systems.*

Wiles, J. & Rogers, R. (2007). *Techno security's guide to managing risks for it managers, auditors, and investigators*. Security & Networking.

Appendix A

Cross validation results of the NRC dataset for single and dual channels (4LSB and 2LSB)

A1: NRC dataset results using 4LSB embedding

1-SVM classifier results.

Table A1.1: 3-fold Cross validation results of the RG channels 4LSB stego images using the NRC dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.00%**
TN	**100.00%**
TP	**100.00%**
Accuracy	**100.00%**

Table A1.2: 3-fold Cross validation results of the RB channels 4LSB stego images using the NRC dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.00%**
TN	**100.00%**
TP	**100.00%**
Accuracy	**100.00%**

Table A1.3: 3-fold Cross validation results of the R channel 4LSB stego images using the NRC dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.07%**
TN	**99.93%**
TP	**100.00%**
Accuracy	**99.97%**

Table A1.4: 3-fold Cross validation results of the GB channels 4LSB stego images using the NRC dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.00%**
TN	**100.00%**
TP	**100.00%**
Accuracy	**100.00%**

Table A1.5: 3-fold Cross validation results of the G channel 4LSB stego images using the NRC dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.00%**
TN	**100.00%**
TP	**100.00%**
Accuracy	**100.00%**

Table A1.6: 3-fold Cross validation results of the B channel 4LSB stego images using the NRC dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.00%**
TN	**100.00%**
TP	**100.00%**
Accuracy	**100.00%**

2-DA classifier results.

Table A1.7: 3-fold Cross validation results of the RG channels 4LSB stego images using the NRC dataset with DA classifier

Metric	Average of 3 folds (%)
FN	**0.67%**
FP	**0.00%**
TN	**100.00%**
TP	**99.33%**
Accuracy	**99.67%**

Table A1.8: 3-fold Cross validation results of the RB channels 4LSB stego images using the NRC dataset with DA classifier

Metric	Average of 3 folds (%)
FN	**0.67%**
FP	**0.00%**
TN	**100.00%**
TP	**99.33%**
Accuracy	**99.67%**

Table A1.9: 3-fold Cross validation results of the R channel 4LSB stego images using the NRC dataset with DA classifier

Metric	Average of 3 folds (%)
FN	**0.67%**
FP	**0.00%**
TN	**100.00%**
TP	**99.33%**
Accuracy	**99.67%**

Table A1.10: 3-fold Cross validation results of the GB channels 4LSB stego images using the NRC dataset with DA classifier

Metric	Average of 3 folds (%)
FN	**2.20%**
FP	**0.00%**
TN	**100.00%**
TP	**97.80%**
Accuracy	**98.90%**

Table A1.11: 3-fold Cross validation results of the G channel 4LSB stego images using the NRC dataset with DA classifier

Metric	Average of 3 folds (%)
FN	**2.20%**
FP	**0.00%**
TN	**100.00%**
TP	**97.80%**
Accuracy	**98.90%**

Table A1.12: 3-fold Cross validation results of the B channel 4LSB stego images using the NRC dataset with DA classifier

Metric	Average of 3 folds (%)
FN	**0.40%**
FP	**0.00%**
TN	**100.00%**
TP	**99.60%**
Accuracy	**99.80%**

A2: NRC dataset results using 2LSB embedding

Table A2.1: 3-fold Cross validation results of the RG channels 2LSB stego images using the NRC dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.07%**
FP	**0.07%**
TN	**99.93%**
TP	**99.93%**
Accuracy	**99.93%**

Table A2.2: 3-fold Cross validation results of the RB channels 2LSB stego images using the NRC dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.00%**
TN	**100.00%**
TP	**100.00%**
Accuracy	**100.00%**

Table A2.3: 3-fold Cross validation results of the R channel 2LSB stego images using the NRC dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.07%**
TN	**99.93%**
TP	**100.00%**
Accuracy	**99.97%**

Table A2.4: 3-fold Cross validation results of the GB channels 2LSB stego images using the NRC dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.20%**
TN	**99.80%**
TP	**100.00%**
Accuracy	**99.90%**

Table A2.5: 3-fold Cross validation results of the G channel 2LSB stego images using the NRC dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.13%**
TN	**99.87%**
TP	**100.00%**
Accuracy	**99.93%**

Table A2.6: 3-fold Cross validation results of the B channel 2LSB stego images using the NRC dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.07%**
FP	**0.53%**
TN	**99.47%**
TP	**99.93%**
Accuracy	**99.70%**

Appendix B

Cross validation results of the Caltech dataset for single and dual channels (2LSB and 4LSB)

B1: Caltech dataset results using 2LSB embedding

Table B1.1: 3-fold Cross validation results of the RG channels 2LSB stego images using the Caltech dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.07%**
TN	**99.93%**
TP	**100.00%**
Accuracy	**99.97%**

Table B1.2: 3-fold Cross validation results of the RB channels 2LSB stego images using the Caltech dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.27%**
TN	**99.73%**
TP	**100.00%**
Accuracy	**99.87%**

Table B1.3: 3-fold Cross validation results of the R channel 2LSB stego images using the Caltech dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.20%**
TN	**99.80%**
TP	**100.00%**
Accuracy	**99.90%**

Table B1.4: 3-fold Cross validation results of the GB channels 2LSB stego images using the Caltech dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.00%**
FP	**0.13%**
TN	**99.87%**
TP	**100.00%**
Accuracy	**99.93%**

Table B1.5: 3-fold Cross validation results of the G channel 2LSB stego images using the Caltech dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.07%**
FP	**0.07%**
TN	**99.93%**
TP	**99.93%**
Accuracy	**99.93%**

Table B1.6: 3-fold Cross-validation results of the B channel 2LSB stego images using the Caltech dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**0.07%**
FP	**0.47%**
TN	**99.53%**
TP	**99.93%**
Accuracy	**99.73%**

B2: Caltech dataset results using 4LSB embedding

Table B2.1: 3-fold Cross validation results of the RG channels 4LSB stego images using the Caltech dataset with SVM classifier)

Metric	Average of 3 folds (%)
FN	**0.47%**
FP	**1.33%**
TN	**98.67%**
TP	**99.53%**
Accuracy	**99.10%**

Table B2.2: 3-fold Cross validation results of the RB channels 4LSB stego images using the Caltech dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**1.73%**
FP	**2.80%**
TN	**97.20%**
TP	**98.27%**
Accuracy	**97.73%**

Table B2.3: 3-fold Cross validation results of the R channel 4LSB stego images using the Caltech dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**1.47%**
FP	**3.87%**
TN	**96.13%**
TP	**98.53%**
Accuracy	**97.33%**

Table B2.4: 3-fold Cross validation results of the GB channels 4LSB stego images using the Caltech dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**1.00%**
FP	**3.73%**
TN	**96.27%**
TP	**99.00%**
Accuracy	**97.63%**

Table B2.5: 3-fold Cross validation results of the G channel 4LSB stego images using the Caltech dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**9.53%**
FP	**24.13%**
TN	**75.87%**
TP	**90.47%**
Accuracy	**83.93%**

Table B2.6: 3-fold Cross validation results of the B channel 4LSB stego images using the Caltech dataset with SVM classifier

Metric	Average of 3 folds (%)
FN	**1.53%**
FP	**6.40%**
TN	**93.60%**
TP	**98.47%**
Accuracy	**96.03%**

Appendix C

(NRC and Caltech datasets)

1- NRC image dataset

2- Caltech dataset