IMPROVED STEGANALYSIS TECHNIQUE BASED ON LEAST SIGNIFICANT BIT USING ARTIFICIAL NEURAL NETWORK FOR MP3 FILES

ALA ABDULSALAM SOLYIMAN ALAROOD

A thesis submitted in fulfilment of the
requirements for the award of degree of
Doctor of Philosophy (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

AUGUST 2017

ACKNOWLEDGEMENT

"*Whoever is not grateful to his fellow humans cannot be grateful to god*" - Prophet Mohammad (Peace be upon him)

I wish to acknowledge and express my sincerest appreciation to the individuals who contributed to the successful completion of this thesis. First and foremost, my supervisors, Prof Dr. Azizah Abd Manaf, I offer to you my sincerest gratitude for your invaluable advice, constant support and encouragement throughout my PhD journey. Without your understanding and guidance, this research could have never been successful. Your kind words of encouragement and your belief in me were both comforting and inspiring.

Thank you too to my dear wife, Mrs. Shefaa Khatatbeh who has always been there for the kids and me, especially whenever I need support and reassurance during those stressful periods.

Last but not least, my deepest gratitude goes to my parents for their endless love and du'a for my success in this life. Thus, with great pleasure, I am very pleased to dedicate this thesis to both of them and all of my brothers & sisters. Thank you all.

ABSTRACT

MP3 files are one of the most widely used digital audio formats that provide a high compression ratio with reliable quality. Their widespread use has resulted in MP3 audio files becoming excellent covers to carry hidden information in audio steganography on the Internet. Emerging interest in uncovering such hidden information has opened up a field of research called steganalysis that looked at the detection of hidden messages in a specific media. Unfortunately, the detection accuracy in steganalysis is affected by bit rates, sampling rate of the data type, compression rates, file track size and standard, as well as benchmark dataset of the MP3 files. This thesis thus proposed an effective technique to steganalysis of MP3 audio files by deriving a combination of features from MP3 file properties. Several trials were run in selecting relevant features of MP3 files like the total harmony distortion, power spectrum density, and peak signal-to-noise ratio (PSNR) for investigating the correlation between different channels of MP3 signals. The least significant bit (LSB) technique was used in the detection of embedded secret files in stego-objects. This involved reading the stego-objects for statistical evaluation for possible points of secret messages and classifying these points into either high or low tendencies for containing secret messages. Feed Forward Neural Network with 3 layers and traingdx function with an activation function for each layer were also used. The network vector contains information about all features, and is used to create a network for the given learning process. Finally, an evaluation process involving the ANN test that compared the results with previous techniques, was performed. A 97.92% accuracy rate was recorded when detecting MP3 files under 96 kbps compression. These experimental results showed that the proposed approach was effective in detecting embedded information in MP3 files. It demonstrated significant improvement in detection accuracy at low embedding rates compared with previous work.

ABSTRAK

Fail MP3 adalah salah satu format audio digital yang paling banyak digunakan yang memberikan nisbah mampatan yang tinggi dengan kualiti yang boleh dipercayai. Kegunaan meluas fail tersebut telah menyebabkan fail audio MP3 menjadi bahan yang sangat baik untuk membawa maklumat steganografi audio tersembunyi di Internet. Kepentingan dalam mengungkap maklumat tersembunyi sedemikian telah membuka suatu bidang penyelidikan yang dipanggil steganalisis yang melihat pengesanan mesej tersembunyi dalam media tertentu. Malangnya, ketepatan pengesanan dalam steganalisis terjejas disebabkan kadar bit, kadar pensampelan jenis data, kadar mampatan, saiz trek fail dan piawai, serta dataset penanda aras fail MP3. Oleh itu, tesis ini mencadangkan teknik yang berkesan untuk steganalisis fail audio MP3 dengan memperoleh kombinasi ciri-ciri dari sifat fail MP3. Beberapa ujian telah dijalankan untuk memilih ciri-ciri berkaitan dengan fail MP3 seperti penyimpangan jumlah harmoni, ketumpatan spektrum kuasa, dan nisbah isyarat kebisingan ke puncak (PSNR) untuk menyelidik korelasi antara saluran yang berbeza dari isyarat MP3. Teknik bit paling ketara (LSB) digunakan dalam pengesanan fail rahsia tersisip dalam objek stego. Ini melibatkan membaca objek stego untuk penilaian statistik untuk kemungkinan titik-titik mesej rahsia dan mengelaskan titi-titik tersebut ke dalam kecenderungan tinggi atau rendah untuk mengandungi mesej rahsia. Rangkaian Neural Forward Feed dengan 3 lapisan dan gdx dengan fungsi pengaktifan untuk setiap lapisan juga digunakan. Vektor rangkaian mengandungi maklumat mengenai semua ciri, dan digunakan untuk membuat rangkaian untuk proses pembelajaran yang diberikan. Akhirnya, proses penilaian yang melibatkan ujian ANN yang membandingkan hasil dengan teknik sebelumnya telah dilakukan. Kadar ketepatan 97.92% dicatatkan apabila mengesan fail MP3 di bawah mampatan 96 kbps. Hasil eksperimen ini menunjukkan bahawa pendekatan yang dicadangkan berkesan dalam mengesan maklumat tersembunyi dalam fail MP3. Ia menunjukkan peningkatan ketara dalam ketepatan pengesanan maklumat tersembunyi pada kadar penyisipan rendah berbanding dengan kajian-kajian lain sebelumnya.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	ACKNOWLEDGEMENT	iii
	ABSTRACT	iv
	ABSTRAK	v
	TABLE OF CONTENTS	vi
	LIST OF TABLES	xii
	LIST OF FIGURES	xiv
	LIST OF ABBREVIATIONS	xviii
	LIST OF APPENDICES	xx
1	**INTRODUCTION**	**1**
	1.1 Research Overview	1
	1.2 Problem Background	4
	1.3 Problem Statement	8
	1.4 Research Questions	9
	1.5 Research Objectives	10
	1.6 Research Scope	10
	1.7 Significance of the Research	11
	1.8 Thesis Structure	13
2	**LITERATURE REVIEW**	**15**
	2.1 Introduction	15
	2.2 Carrier Medium	15
	2.2.1 Overview of MP3 File	16
	2.2.2 MP3 Encoding	17
	2.2.3 MP3 File Format	17

2.2.4 MP3 Frame Headers 19
2.2.5 Transmission Environment MP3 20
2.3 Steganography 23
2.3.1 Steganography Categories 25
2.3.1.1 Pure Steganography 25
2.3.1.2 Secret Key Steganography 26
2.3.1.3 Public Key Steganography 27
2.3.2 Steganography under Various Media 28
2.3.3 Audio Steganography Methods 30
2.3.3.1 Least Significant Bit (LSB) 30
2.3.3.2 Phase Coding 32
2.3.3.3 Spread Spectrum (SS) 33
2.3.3.4 Echo Hiding 33
2.3.4 Main Approach of Steganography 34
2.3.4.1 Subjective Listening Tests 35
2.3.4.2 Objective Evaluation Tests 36
2.4 Steganalysis 37
2.4.1 A Definition of Security for Steganography 38
2.4.2 Measuring Security Empirically 40
2.4.3 Steganalysis Types 41
2.4.3.1 Targeted Steganalysis 41
2.4.3.2 Blind Steganalysis 41
2.4.3.3 Quantitative Steganalysis 42
2.4.3.4 Forensic Steganalysis 42
2.4.4 Main Approaches to Steganalysis 43
2.4.4.1 Statistical Steganalysis 43
2.4.4.2 Learning Steganalysis 44
2.4.5 Steganalysis of MP3 Files 45
2.4.5.1 Histogram of Block Length 45
2.4.5.2 Steganalysis of Under MP3 Cover 45
2.4.5.3 Statistics of Quantization Step 46
2.4.5.4 Calibrated Steganalysis 46
2.4.5.5 Statistics of MDCT coefficients 47
2.4.5.6 Numbers of Different Block Lengths 48

2.5 Feature Selection 49
2.5.1 Filter Approach 50
2.5.2 Wrapper Approach 51
2.5.3 Embedded Approach 52
2.6 Feature Normalization 54
2.7 Machine Learning 55
2.7.1 Classification 56
2.7.2 General Framework of Learning Classifier 58
2.7.3 Neural Network Classifier 60
2.7.3.1 Framework of Neural Networks 61
2.7.3.2 Processing Units 61
2.7.3.3 Connections between Units 62
2.7.3.4 Rules for Activation and Output 63
2.7.3.5 Network Topologies 65
2.7.3.6 Training of Artificial Neural Network 65
2.7.3.7 Paradigms of Learning 66
2.7.3.8 Modifying Patterns of Connectivity 66
2.8 Evolution of Steganalysis 67
2.8.1 False Negative Rate 68
2.8.2 False Positive Rate 68
2.8.3 Receiver Operating Characteristic 69
2.8.4 Equal Error Rate 69
2.8.5 Receiver Operating Characteristic 70
2.9 Empirical research on Steganalysis Technique 70
2.10 Summary 84

3 RESEARCH METHODOLOGY 85
3.1 Introduction 85
3.2 Research Procedure 85
3.3 Research Framework 87
3.4 Operational Framework 88
3.5 Methodology Phases 89
3.5.1 Dataset Generation 91
3.5.1.1 Benchmark Dataset 91

3.5.1.2 Standard Dataset 92
3.5.1.3 Collect Secret Messages 93
3.5.2 Pre-processing and Embedding Technique 94
3.5.2.1 Acquisition File Properties 94
3.5.2.2 Conversion to Binary 95
3.5.2.3 Normalize MP3 File 96
3.5.2.4 Build Stego-Object 96
3.5.3 Detection Process 97
3.5.3.1 ANN Approach to MP3 file Steganalysis 97
3.5.3.2 Feature Extraction 99
3.5.3.3 Feature Normalization 102
3.5.3.4 Training Algorithm 102
3.5.3.5 Detect MP3 Files 103
3.5.4 Test and Evaluation 104
3.5.4.1 Classification 106
3.5.4.2 Matlab Tool 106
3.6 Software and Hardware Requirements 106
3.7 Summary 107

4 RESEARCH DESIGN & IMPLEMENTATION 108
4.1 Introduction 108
4.2 Research Design 108
4.3 Phase One: Generation of Dataset 109
4.4 Phase Two: Pre-Processing and Embedding Technique 110
4.4.1 Acquisition of File Properties 110
4.4.2 File Conversion 111
4.4.3 Normalization of Files 113
4.4.4 Build Stego Bit Stream 116
4.4.5 Converting a Bit Stream to an MP3 Stego-Object 119
4.5 Phase Three: Detection Process 123
4.5.1 ANN Approach to MP3 File Steganalysis 123
4.5.2 Evaluating of Feature Extraction 124
4.5.2.1 Peak Signal-to-Noise Ratio and Mean Square Error 125

4.5.2.2 Sum of Squared Error 126
4.5.2.3 Mean 127
4.5.2.4 Standard Deviation and Correlation Coefficient 128
4.5.2.5 Total Harmonic Distortion 129
4.5.2.6 Power Spectrum Density 129
4.5.2.7 Energy of Sound 130
4.5.2.8 Wavelet Domain PSNR and MSE 131
4.5.3 Feature Normalization 131
4.5.4 Training Process 132
4.5.4.1 Activation Function 135
4.5.4.2 Neural Network Layers 135
4.5.4.3 Training Algorithm 136
4.5.4.4 Performance Function 137
4.5.4.5 Detect MP3 File 139
4.6 Phase Four: Performance Evaluation 140
4.6.1 Cross-Validation 141
4.6.2 Confusion Matrix 141
4.6.3 Receiver Operating Curves 143
4.6.4 Equal Error Rate 145
4.7 Summary 145

5 RESULTS, ANALYSIS AND DISCUSSION 147
5.1 Introduction 147
5.2 Embedding Analysis Results 147
5.2.1 Standard Dataset 149
5.2.2 Benchmark Dataset 154
5.2.3 Discussion of Embedding Results 155
5.3 Analysis of Detection Results 157
5.3.1 Standard Dataset 158
5.3.2 Benchmark Dataset 165
5.3.3 Discussion of Detection Results 169
5.4 Performance Evaluation Analysis 171
5.4.1 Confusion Matrix Analysis 171

5.4.2 Average of Accuracy 173
5.4.3 Error Rate 175
5.4.4 ROC Curve Analysis 177
5.5 Comparison of Results 180
5.5.1 Background of Comparative Results 180
5.5.2 Analysis of the Comparative results 183
5.6 Summary 189

6 CONCLUSION 190
6.1 Introduction 190
6.2 Research Contribution 191
6.2.1 The Implementation of an Effective Detection Technique 191
6.2.2 The Performance of Detection Technique 192
6.3 Recommendations for Future Research 193
6.4 Research Conclusion 194

REFERENCES 196
Appendices A - B 209 - 223

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	Confusion matrix for two-class problem	67
2.2	Summary of comparison of different steganalysis method for MP3 detection. Notations of the table are as follows SI: side information, R: maximum capacity ratio, NR: not reported parameters, NA: non-applicable parameters	82
3.1	Operational research framework	89
3.2	Number of MP3 files per genre	92
3.3	Cover MP3 file dataset	93
3.4	Text dataset	94
3.5	Feature extraction	101
4.1	Key or signatures	116
4.2	Example showing the effect of normalization	132
4.3	Vector of an MP3 file	134
4.4	Confusion matrix	142
5.1	Classification of MP3 files for standard dataset	148
5.2	Classification of MP3 files for benchmark dataset	149
5.3	PSNR results for Data-1 at 320 kbps compression rate	150
5.4	PSNR results for Data-1 at 256 kbps compression rate	151
5.5	PSNR results for Data-1 at 192 kbps compression rate	152
5.6	PSNR results for Data-1 at 128 kbps compression rate	153
5.7	PSNR results for Data-1 at 96 kbps compression rate	154
5.8	PSNR results for Data-1 using the benchmark dataset	154
5.9	Accuracy of detection at 320 kbps compression rate	158
5.10	Accuracy of detection at 256 kbps compression rate	160
5.11	Accuracy of detection at 192 kbps compression rate	161
5.12	Accuracy of detection at 128 kbps compression rate	162

5.13	Accuracy of detection at 96 kbps compression rate	164
5.14	Accuracy of detection for 1-LSB	165
5.15	Accuracy of detection for 2-LSB	166
5.16	Accuracy of detection for 4-LSB	168
5.17	Summary of confusion matrix analysis for the standard dataset	172
5.18	Summary of confusion matrix analysis for the benchmark dataset	173
5.19	Comparison of the average accuracy of detection achieved by the proposed and previous models with 128 Kbps	184
5.20	Compression results for TPR using the proposed and previous models	185
5.21	Compression results for TNR using the proposed and previous models	185
5.22	Summary of Comparison result of different Steganalysis researcher. Notations of the table are as follows NR: not reported parameters, NA: non-applicable parameters	187

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
1.1	Hierarchy of the classification of steganalysis techniques	3
2.1	MP3 file structure	18
2.2	MP3 frame header	20
2.3	Various transmission types	22
2.4	Digital data security disciplines	24
2.5	Pure steganography	26
2.6	Secret key steganography	27
2.7	Public key steganography	28
2.8	Classical steganalysis process	38
2.9	Feature selection algorithm	49
2.10	Filter approach algorithm	50
2.11	Wrapper approach	51
2.12	Wrapper approach algorithm	52
2.13	Embedded algorithm	53
2.14	Categorization of steganalysis and classification approaches	57
2.15	Learning classifier model (Schaathun, 2012)	59
2.16	Basic components of neural networks	62
2.17	Different activation functions for a unit	64
2.18	Example ROC curve. The AUC for this curve is 80.13%. The EER (25.99%) is the point where the two lines cross	70
2.19	Proposed Steganalysis of MP3	71
2.20	Proposed steganalysis of MP3 based on Huffman coding	72
2.21	Proposed Steganalysis model	73
2.22	Proposed steganalysis model	74
2.23	Proposed steganalysis model	75

2.24	Proposed steganalysis model	76
2.25	Proposed steganalysis model	77
2.26	Block schematic of proposed merged feature extraction	78
2.27	Overview of the proposed approach	79
2.28	The proposed CNN Architecture for detection	80
3.1	Research procedure	86
3.2	Research framework	88
3.3	Research methodology flowchart	90
3.4	Convert text to bit stream	95
3.5	Converting an MP3 file to a bit stream	96
3.6	Neural network technique	98
3.7	Design of neural network structure	99
3.8	Learning process	103
3.9	Detect MP3 files	104
4.1	Research design	109
4.2	Obtaining the parameters of an MP3 file	110
4.3	Converting a text file to ASCII	113
4.4	Converting an MP3 file to a bit stream	115
4.5	Adding a signature to a text file	117
4.6	Insertion of one and two bits	117
4.7	Replacing bits in the carrier file	119
4.8	Embedding a text file in an MP3 file	122
4.9	Network structure	124
4.10	Feature components	125
4.11	Feature extraction	133
4.12	Target value after calculation	134
4.13	Layer of Neural Network	136
4.14	Adjustment of weights	136
4.15	Training function	137
4.16	Training performance	138
4.17	Training behaviour	138
4.18	Process of detection for MP3 files	140
4.19	Cross-validation of the dataset using 10 MP3 files	141

4.20	ROC curves: (a) regions of an ROC graph (b) an almost perfect classifier (c) a reasonable classifier (d) a poor classifier	144
5.1	PSNR for 1-LSB with different genres under different compression rates	155
5.2	PSNR for 2-LSB with different genres under different compression rates	156
5.3	PSNR for 4-LSB with different genres under different compression rates	156
5.4	PSNR result with different LSBs	157
5.5	Accuracy of detection at 320 kbps compression rate	159
5.6	Correct and incorrect classifications at 320 kbps compression rate	159
5.7	Accuracy of detection at 256 kbps compression rate	160
5.8	Correct and incorrect classifications at 256 kbps compression rate	160
5.9	Accuracy of detection at 192 kbps compression rate	161
5.10	Correct and incorrect classifications at 192 kbps compression rate	162
5.11	Accuracy of detection at 128 kbps compression rate	163
5.12	Correct and incorrect classifications at 128 kbps compression rate	163
5.13	Accuracy of detection at 96 kbps compression rate	164
5.14	Correct and incorrect classifications at 96 kbps compression rate	164
5.15	Accuracy of detection with 1-LSB	165
5.16	Correct and incorrect classifications with 1-LSB	166
5.17	Accuracy of detection with 2-LSB	167
5.18	Correct and incorrect classifications with 2-LSB	167
5.19	Accuracy of detection with 4-LSB	168
5.20	Correct and incorrect classifications with 4-LSB	168
5.21	Comparison of accuracy between different ERs and different compression rates	169

5.22	Comparison of accuracy for different payloads and different LSBs	170
5.23	Accuracy of detection (%) for the standard dataset	174
5.24	Accuracy of detection (%) for the benchmark dataset	175
5.25	Error rate (%) for the standard dataset	176
5.26	Error rate (%) for the benchmark dataset	176
5.27	ROC curves under different ERs at 96 kbps	177
5.28	ROC curves under different ERs at 128 kbps	178
5.29	ROC curves under different ERs at 192 kbps	178
5.30	ROC curves under different ERs at 256 kbps	179
5.31	ROC curves under different ERs at 320 kbps	179
5.32	Comparison of the average accuracy of detection achieved by the proposed and previous models (128 kbps)	184
5.33	Compression results for TPR using the proposed and previous models	185
5.34	Compression results for TPR using the proposed and previous models	186

LIST OF ABBREVIATIONS

AAC	-	Advanced Audio Coding
ABR	-	Average Bit Rate
AIFF	-	Audio Interchange File Forma
ALS	-	Amyotrophic Lateral Sclerosis.
ANN	-	Artificial Neural Network
ATRAC	-	Adaptive Transform Acoustic Coding
BAF	-	Before All Frames
BCI	-	Brain Computer Interface.
BF	-	Between Frames
CBR	-	Constant Bit Rate
DCT	-	Discrete Cosine Transform
DFT	-	Discrete Fourier Transform
DSSS	-	Direct-Sequence Spread Spectrum
DWT	-	Discrete wavelet transforms
ER	-	Embedding Rate
EER	-	Equal Error Rate
FHSS	-	Frequency-Hopping Spread Spectrum
FPR	-	False Positive Rate
FNR	-	False Negative Rate
GA	-	Genetic Algorithm
HAS	-	Human Auditory System
HVS	-	Human Visualized System
IQM	-	Image quality measurement
LSB	-	Least Significant Bit
MDCT	-	Modified discrete cosine transform
MSB	-	Most Significant Bit
MPEG	-	Moving Picture Experts Group

MSE	-	Means Squared Error
ODG	-	Objective Difference Grade
PSNR	-	Peak Signal-to-Noise Ratio
PSD	-	Power Spectrum Density
ROC	-	Receiver Operating Characteristic
SDG	-	Subject Difference Grade
SNR	-	Signal-to-Noise Ratio
SS	-	Spread Spectrum
SSE	-	Sum of Squared Errors
THD	-	Total Harmonic Distortion
TTA	-	The True Audio
VBR	-	Variable Bit Rate

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	PSNR Result from Data 2 to Data 5	209
B	Experimental Results for Detection Model Under Different Compression Rates	219

CHAPTER 1

INTRODUCTION

This chapter discusses the research background and overview, which leads to problem statement. From the problem statement, the research questions and objectives of this research specified. Furthermore, the research scope and significant to the study are stated throughout this chapter.

1.1 Research Overview

There are huge advancement of technology over the years. Most of the end product provide efficient services that uplift society. Owing to advancements in technology, digital media applications have become increasingly popular in our daily lives. Digital media manipulation such as hiding information in image and audio files for use over a covert channel has become common. Steganography is the study of hiding information in a carrier file; however, making covert communication based on steganography is a challenging technology. Steganalysis is the reserves process of steganography, but, without the awareness of the technique used for hiding the information, and using all efforts to detect the hiding message inside a carrier file. More studies are needed to develop new techniques to decode hidden information in carrier files (Mazurczyk *et al*., 2016).

There is a wide variety of information about steganography in the literature. The term ‘steganography’ originates from the Greek language and consists of ‘stegano’ = secret, hidden and ‘graphy’ = to write, to draw (Anguraj *et al*., 2011). According to Shelke (2014), Steganography is the art and science of communicating

in such a way that the existence of the message could not be detected" (Shelke *et al*., 2014). Steganography provides safe communication via hidden messages by preventing comprehensibility and retaining confidentiality. Steganography is widely used by the military and diplomats (Shahadi and Jidin, 2011). Nowadays, an added security layer is mostly used prior to performing steganography. Where the steganographic approach used for information is first encrypted and then hidden, finally transferred through a communication channel(Das and Tuithung, 2012).

There are three fundamental properties—imperceptibility, robustness, and capacity—which serve as restrictions for steganography designers and form a magic triangle for visualising the requirements of steganography (Westfeld *et al*., 2013). For a good steganographic technique, the capacity and robustness cannot be equally high. In order to achieve a highly robust steganography algorithm, the embedding of the capacity should be low and vice versa. Furthermore, a high capacity usually results in a fragile algorithm because highly embedded results have a low imperceptibility. Moreover, this increases the probability that an attacker will detect the secret message and retrieve it (Su, 2017).

Steganalysis is a technique for decoding information that is hidden in carrier file (Mirjavadi *et al*., 2013). In other words, it hinders the delivery of documents between government agents or other parties. Steganalysis can be used to evaluate the performance of the security of steganography (Subhedar and Mankar, 2014). Information is hiding in the shapes of small clues and may not be noticed visually. However, clues can lead to a statistically significant difference. Steganalysis techniques use detection and cracking to find indicators of the clues (Rana, 2016).

Steganalysis can be broadly categorised into two classes as shown in Figure 1.1, namely: signature steganalysis and statistical steganalysis (Muthuramalingam *et al*., 2016). The division is based on whether the signature of a steganography technique or the statistics of information are used to identify the presence of hidden information in a carrier file (Kessler and Hosmer, 2011). On the basis of its fields of application, it can be further divided into specific methods and universal methods. A specific steganalysis method utilises knowledge of a targeted steganographic

technique and may only be appropriate to this type of steganography (Li *et al*., 2011). A universal steganalysis method is used to detect several types of steganography. Usually, universal methods do not require knowledge of the embedding operations(Li et al., 2011).

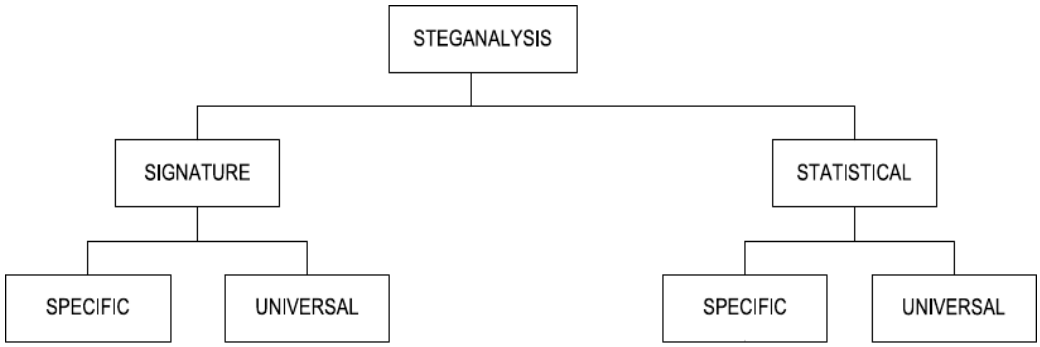

Figure 1.1 : Hierarchy of the classification of steganalysis techniques

The goal of steganalysis is to collect sufficient evidence about the presence of embedded messages and to break the security of its carrier (Chhikara and Singh, 2013a). The importance of steganalytic techniques that can reliably detect the presence of hidden information in audio files is increasing. Steganalysis is used in computer forensics, cyber warfare, tracking criminal activities over the internet, and gathering evidence for investigations, particularly in cases of anti-social elements (Chhikara and Singh, 2013b). In practice, a steganalytic is frequently interested in more than whether or not a secret message is present—the ultimate goal is to detect and extract the secret message.

Sharma and Bera (2012) proposed a steganalysis method based on the statistical moments of a wavelet characteristic function (SMWCF) and an artificial neural network (ANN) as a classifier(Sharma and Bera, 2012). In recent years, neural networks have proved their effectiveness in many applications, and ANN are recognized as powerful data analysis and modelling tools (Usha *et al*., 2013). ANN consist of an interconnected collection of artificial neurons that change their structure based on the information that flows through the artificial network.

In steganography techniques, media such as images, audio, videos, and text can be used to embed a secret message into cover (Gomez-Coronel *et al*., 2014).

MPEG-1 Audio Layer 3, known as MP3, has become one of the most popular formats for compressed audio, and is commonly used for steganography. Steganographic tools such as MP3stego, UnderMP3Cover, and MP3stegz can be used to embed compressed and encrypted data in the MP3 bit stream. Primary information regarding the carrier or host is typically hidden within the secondary information, and could be in the form of a file or message. The media containing the embedded information is called the stego-object file (Farouk, 2014). Proposed a steganalytic method to detect up to 1% steganographic capacity in MP3 files. Later, Wan *et al*., (2012) presented a steganalysis approach for detecting messages embedded using MP3Stego (28 hidden bytes of data)(WAN *et al*., 2012).

1.2 Problem Background

In today's digital age, there are more opportunities to change the information represented in digital format. Forensic investigations, surveillance systems, criminal investigations, and intelligence services need reliability while transferring information in the form of digital files. With the rapid increase in the use of digital multimedia (image or audio files) on the Internet, the security problem has become increasingly important. Moreover, the communication of secret messages using digital multimedia has become an increasingly popular demanding.

The advances of the computer era have given a new dimension to the art of securing or hiding secret messages in digital medium. Computer-based techniques hide data in digital carriers by changing the carriers in such a manner that, even after altering them, they appear to be innocuous. These carriers are called Cover Media (Meghanathan and Nayak, 2010). Cover media can be audio files, images, video, and text. The process of hiding information in the cover media is called embedding (Jayaram *et al*., 2011). Different steganographic schemes have their own ways of embedding the message. These are collectively called 'steganographic algorithms.

Audio steganography methods are divided into different classes: embedding during compression (least-significant-bit encoding, phase coding, echo hiding, and

spread spectrum) and embedding after compression (unused header bit stuffing, padding byte stuffing, before all frames, between frames, M4M, and M16M)(Atoum, 2015a). One simple and effective method of steganography uses the Least Significant Bit (LSB). LSB embedding is the most widely used steganographic technique. Thus, modified versions of LSB embedding have been of great interest in the field of steganography in recent decades. Generally, the major issues of steganographic technique, lies with bit rates and sampling rate influence. Although steganography techniques heavily relies on three fundamental tradeoff; robustness, capacity, and imperceptibility as the key requirement. Nevertheless, a good steganographic technique, in most cases do not achieved these requirements. Because the most important challenge of the field of steganography are in Technical, Linguistic, and Semagrams.

Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size-reduction methods. How effective it is? Could the detection of the hidden messages be easier or difficult in this area? Using these techniques does not mean that the technicality solves detection. But it could be tested, where a method for detection is proposed with the grounds that it's capable of detecting at a high degree.

Linguistic steganography hides the message in the carrier in some nonobvious ways and is further categorized as semagrams or open codes. Semagrams hide information by the use of symbols or signs. A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of items on a desk or Website. A text semagram hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or type, adding extra spaces, or different flourishes in letters or handwritten text. These are successful steganographic scheme, however, their implementations remains critical. Although they are simple to use, but they might be difficult to detect.

Open codes hide a message in a legitimate carrier message in ways that are not obvious to an unsuspecting observer. The carrier message is sometimes called the overt communication, whereas the hidden message is the covert communication.

This category is subdivided into jargon codes and covered ciphers. Jargon code, as the name suggests, uses language that is understood by a group of people but is meaningless to others. Jargon codes include warchalking (symbols used to indicate the presence and type of wireless network signal), underground terminology, or an innocent conversation that conveys special meaning because of facts known only to the speakers. A subset of jargon codes is cue codes, where certain prearranged phrases convey meaning. Covered or concealment ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed. A grille cipher employs a template that is used to cover the carrier message. The words that appear in the openings of the template are the hidden message. A null cipher hides the message according to some prearranged set of rules, such as "read every fifth word" or "look at the third character in every word." The crucial challenges faced in the detection is the use of “keys”. Over here while the technique for hiding are available with good accuracy, but many are yet to be uncover. In terms of detection, how could a detection technique with a high degree of detecting secret massage be involved in this? How feasible is the current techniques used in the detection? There could be lots of ideas out there for enhancing the method of hiding message used in this area. Similarly there could be for detection as well. However research on both areas can never end. As a new method for hiding secret message evolves, so also a new method for detection will be required.

Even though steganalysis procedure is also affected by bit rate, compression method, file size and secret message. Furthermore, datasets is also crucial in experimenting both steganography and steganalysis. Finally, compression rates of a media, specifically MP3 carrier file also affect the results of steganalysis. (Kekre *et al*., 2011).

Many other steganalysis techniques have been proposed in recent years. For instance, targeted steganalysis is based on analysing changes in the statistical properties of a file after embedding. The advantage of using specific steganalysis is that the results are very accurate (Bhattacharyya, 2011). Blind steganalysis is the process of creating a set of distinct statistical attributes of a file by categorizing the file into classes depending on their feature values (Poisel and Tjoa, 2011), whereas

quantitative steganalysis estimates the length of the message (Katzenbeisser and Petitcolas, 2016). Forensic steganalysis is most popular form of steganalysis, and aims to find out everything about the message (presence, length, content, and so on) (Ker and Pevný, 2014). Steganalysis also ranges from manual scrutiny by experts to automated data analysis. Unfortunately most of the automated techniques suffers from accuracy.

The motivation of this work dwells on steganalysis. There are various techniques involve. Almost all of them relies on qualitative analysis. However, they are categorized into Targeted Steganalysis, Blind steganalysis, Quantitative steganalysis and Forensic steganalysis. These classification is with respect to objectives set. All of them faced crucial challenges that required a research attentions. The general research motivation in this area "Is there a message hidden in this medium". (Miche *et al*., 2009).

Learning steganalysis overcomes the analytic challenge by obtaining an empirical model through brute-force data analysis (Ge and Tian, 2015). The solutions come from areas known as pattern recognition, machine learning, or artificial intelligence. Most of the recent research on steganalysis has been based on machine learning. The most common steganalysis techniques based on machine learning are decision trees, Support Vector Machine (SVM) methods, Naive Bayes (NB), K-Nearest Neighbour methods, and ANN (Kesavaraj and Sukumaran, 2013).The ANN approach to steganalysis detects the presence of an eventual hidden message in a file (Ker *et al*., 2013), with the ANN itself chosen as a classifier to train and test the given audio. ANN reflects a system based on biological nervous networks, and can be defined as an emulation of biological nervous systems. Over the past two decades, ANN has been shown to provide solutions to data mining-type problems that are not easily manipulated by classical methods. Applying ANN to steganalysis, dwells on the facts that handling different bit rates and sampling rate for embedding could yield some pattern. This can aid detection during steganalysis process. Although there are still some crucial issues yet to be addressed in terms of detection scheme of steganalysis. Most notably is the detection accuracy in steganalysis using standard

dataset and benchmark dataset. The dynamics of compression rates and file track size. The relationships between accuracy and embedding rate.

In this study, an attempt to overcome the drawbacks listed above has been considered. Hence a new steganalysis techniques employ statistical analysis by extracting the features (total harmonic distortion, power spectrum density, energy of sound, correlation coefficient, mean, standard deviation, sum of squared error, peak signal-to-noise ratio, and mean squared error) of MP3 files used as the input to ANN. Therefore, the proposed technique has a solution that depends on a probability. If the probability is close to zero, then the MP3 files are considered to be Stego-objects; if the probability is not close to zero, then the MP3 is considered to be original (free of ambiguity intervention).

1.3 Problem Statement

With the rapid growth of information technology, many studies have described how audio file formats can be applied to steganography systems either before compression or after compression. However, such file formats suffer from low security and limited capabilities. There should be some benchmark statistical tool for assessing the data and identifying the hidden message in an audio object. Steganography techniques are used to hide secret information in MP3 files, with the information embedded during or after the compression process. Despite the suitability of MP3 files for steganography, the amount of steganalysis for this format is still quite limited because of the low embedding rate. This shows that the steganalysis of MP3 is still a very challenging issues with low embedding rates. The most critical issues with detection of secret message in MP3 files are; bit rate, sampling rate, compression method and the carrier file is either standard or benchmark.

It not clear if different bit rates or a constant sampling rate for embedding ease detection during steganalysis. Using standard dataset and benchmark dataset in an experiment to determine the detection accuracy in steganalysis is crucial. The

results might not be the same. Hence, detection could be doubted if only a single data set is used. Although some previous studies acknowledged that standard dataset is more reliable in testing for detection (Atoum, 2015c), however it's also argued that benchmark dataset can be more suitable for testing of steganalysis (Homburg *et al*., 2005). Even though detection could be difficult if embedding is done in 1 and 2, but not in 4 LSBs at compression rates of 320, 256, 192, 128, and 96 kbps, nevertheless, there isn't' a consensus on a technique to addressed that. In most cases compression rates affects steganalysis process when using standard dataset, but in benchmark dataset only a single compression rate is used (128kbPS). Compression rates could either affect the results of steganalysis positively or otherwise. It could be that the results of the accuracy of detecting hidden information drop or not. This drop might be caused by either the increase in file track size or any other issues. Hence, it's still not clear how accuracy and embedding rate are related or is there any significant positive relationship between accuracy and embedding rate which could affect Steganalysis process?

1.4 Research Questions

This study investigates the detection of MP3 Stego-files based on extracted feature (total harmonic distortion, power spectrum density, energy of sound, correlation coefficient, mean, standard deviation, peak signal-to-noise ratio, mean squared error, and sum of squared error) from MP3 files and examines how these features can be used in machine learning to build a training technique. Hence, the following research questions are proposed:

i. What are the techniques used for detecting hidden messages in MP3 files?
ii. How can a hidden file be detected in an MP3 carrier file.
iii. How the detection accuracy be enhanced for some embedded secret message?

1.5 Research Objectives

The main objective of this research is to build a suitable technique to identify MP3 audio files that contain an embedded secret message. Statistical analysis can be performed to find inconsistencies in the audio file when external heterogeneous data exist. In fact, large-scale statistical analysis is necessary to detect such files. However, an intelligent computational technique could be used instead of pure mathematical analysis, such as a neural network. Neural networks offer many benefits as intelligent detectors or recognizers. Thus, they may be able to predict the existence of a Stego-object or not normal files and assist with the extraction of the secret message. Thus, the study set to achieve the following objectives:

i. To examine the techniques used for detecting hidden messages in MP3 files.
ii. To design and implement an effective detection technique capable of detecting hidden files in an MP3 carrier file using an ANN.
iii. To enhance the accuracy of ANN-based steganalysis

1.6 Research Scope

The rapid development of digital media and information technology has made them ubiquitous. Nowadays, an abundance of information is stored digitally. Specifically, there are multitude of daily tasks that involve dealing with documents. The origins of these documents might be digital, or they may be converted from hard copies into appropriate digital formats.

i. This study was delimited to the data acquisition, feature extraction, and classification of MP3 files by an ANN process.
ii. The proposed detection technique is only compatible for MP3 file with different compression rate and format (channel mode).
iii. This study's experiments dwells on the extraction of features from MP3 files. The extracted features are normalized by scaling their

values using Min-Max normalization, so that they are within a certain specified range.

iv. The datasets used in this study fall into two categories: benchmark datasets were obtained from Homburg *et al*. (2005) and standard datasets were obtained from Atoum (2015). All of these files are pre-integrated and have been validated.

v. This study relies on MATLAB as its experimental tool.

1.7 Significance of the Research

There are remarkable increases in using digital steganalysis for solving the concerns about preserving the integrity of digital content. Detection of unauthorized modification is also another issue. In fact the widespread of excellent distribution system of digital media in internet, bought a chance to the third parties to exploit the media for their own benefits. Various research output shows the strength of detecting techniques on different cover media. Most importantly to this research is those found for audio medium. Although those techniques considered steganalysis of mono signals. Investigating the correlation between different channels of stereo signals will improve performance of steganalysis. That is why this research is highly significant. Moreover, there are many impacts that this research brought. Among these are:

i. Computer Forensics: the new detection technique proposed in this thesis, can help in forensics. For the fact that identification, extraction, documentation, and interpretation of any traces of data (in bits/bytes) is the key central part of computer forensic, then this study helps in those elements. Hence leads to an easier way of determining the evidentiary and/or root cause analysis of a crime.

ii. Cyber warfare: Detection techniques that is able and capable of detecting the present of enemy’s secret message in a cover medium, will surely safes life in a war front. This dwells to acyber-warfare, where a nation-state intended to penetrate another nation's through embedding secret massage on a cover medium over computers and

networks for the purposes of causing damage or disruption. If Nations states are capable of detecting any hidden message. Then those nations are safe in a cyber-warfare. In another perspective, digital steganalysis for MP3 authentication allows the military organizations to verify whether the digital MP3 they received, arrived from the genuine source and to authenticate whether the content within the digital media is original. In case the content is marked as manipulated, an effective authentication technique is expected to illustrate as much information about the embedding information. Therefore, this study, is significant in the area of cyber warfare.

iii. Industrial: The research findings are significant to Industries in using the technique proposed in this research as a software implementable tool for detection of any secret data in an MP3 file.

iv. Security firms: The research output can be significant to security firms which are mostly concern with the tools for detecting a hidden information inside an MP3 file.

v. Computing community: Generally, to the computing research community, this thesis is significant in terms of providing a methodological contribution, where a new technique has been devised to aid the exploration of information hidden technique.

vi. Theoretically: A theory has been produce in this work, where embedding at a random location and using ANN for detection accuracy has been found.

Therefore, Security firms are seeking technologies that promise to protect and preserve their digital MP3 and rights. As a result of that, the contents originality and the integrity of information need some strong degree of protection. Steganalysis has been considered as solution for copy prevention and MP3 authentication as well as detecting unauthorized modification.

1.8 Thesis Structure

This thesis consists of five major parts, excluding the introductory chapter which presented a background of the problem as well as outlined the purpose and objectives of the research. The importance and expected contributions of the research are also highlighted and emphasized. While the second part describes the research setting as well as previously published work in the field of audio steganography and steganalysis, the third part describes the scope of research. Finally, the last part presents the phases for research frameworks.

Chapter 2, is the *Literature Review*, which discusses the related work of this study and examined the issues raised by many researchers. There are two main sections: first, is the descriptions of the concept of Information hiding and detection as well as MP3 file structure as a carrier file. Which discuss steganography and steganalysis techniques. The other section deals with machine learning processes and the presentation of past empirical research technique.

Chapter 3, present the *Research Methodology*, The proposed methods are explained, starting with data acquisition before moving on to feature extraction, pre-processing, feature selection, and classification. Finally, the testing and evaluation of the proposed method are presented. This has been vividly discussed on the basis of the design, and procedure of detection techniques as well as the operational framework for the research.

Chapter 4, is the *Analysis and Implementation of the Proposed Technique*: This chapter discusses the philosophy for the design of the proposed technique of MP3steganalysis, and demonstrates the implementation of the proposed framework for detection of secret message in MP3 file. Finally, the technical and practical evaluation of the proposed framework was illustrated.

Chapter 5,is *Results and discussion* of the study. It present the results based on the experimental work. The analytical and test based on machine learning approach are presented. Various useful features that provide discriminative

information for detecting steganographic MP3 (hidden) files within a carrier file are identified and presented. The proposed approach is compared with other methods that use ANN. Furthermore, a comparative study between the technique proposed for this research and other steganalysis techniques that use artificial intelligence algorithms is presented and discussed. This chapter also presents a feasibility study based upon using the technique to detect MP3 files.

The last **chapter 6** presents the *Conclusion and Future Work.* This chapter reviews the main conclusions from this research. The contributions of this research are highlighted and recommendations for future work are stated.

REFERENCES

ABOUDIB, A., GRIPON, V. & JIANG, X. 2013. A study of retrieval algorithms of sparse messages in networks of neural cliques. *arXiv preprint arXiv:1308.4506*.

ACEVEDO, A. G. 2006. Audio watermarking quality evaluation. *e-Business and Telecommunication Networks.* Springer.

AGAIAN, S. S. & RODRIGUEZ, B. M. 2006. Basic Steganalysis Techniques for the Digital Media Forensics. *Digital Crime and Forensic Science in Cyberspace***,** 175.

ALAVALA, C. R. 2008. *Fuzzy logic and neural networks*, New Age International.

ALI, A. H., MOKHTAR, M. R. & GEORGE, L. E. 2017. ENHANCING THE HIDING CAPACITY OF AUDIO STEGANOGRAPHY BASED ON BLOCK MAPPING. *Journal of Theoretical & Applied Information Technology,* 95.

ANDRES, G. 2002. Measuring and evaluating digital watermarks in audio files. *Washington Dc*.

ANGURAJ, S., SHANTHARAJAH, S., MURUGAN, R. A., BALAJI, E., MANEESH, R. & PRASATH, S. A fusion of AB MAP Cipher and ASET algorithms for the enhanced security and robustness in audio steganography. Recent Trends in Information Technology (ICRTIT), 2011 International Conference on, 2011. IEEE, 205-210.

ARNOLD, M. Subjective and objective quality evaluation of watermarked audio tracks. Web Delivering of Music, 2002. WEDELMUSIC 2002. Proceedings. Second International Conference on, 2002. IEEE, 161-167.

ARORA, C. & ANAND, N. Survey on Techniques for Steganography of Audio Files.

ATOUM, M. S. 2015a. A Comparative Study of Combination with Different LSB Techniques in MP3 Steganography. *Information Science and Applications*, 551-560.

ATOUM, M. S. 2015b. *Embedding Encrypted Text in MP3 Steganography*, LAP LAMBERT Academic Publishing.

ATOUM, M. S. New MP3 Steganography Data Set. IT Convergence and Security (ICITCS), 2015 5th International Conference on, 2015c. IEEE, 1-7.

BASU, D. N., BHATTACHARYYA, S. & DAS, P. 2013. Influence of geometry and operating parameters on the stability response of single-phase natural circulation loop. *International Journal of Heat and Mass Transfer,* 58**,** 322-334.

BEN-YAACOV, Y. & BEN-YAACOV, B. 2014. Portable music player and transmitter. Google Patents.

BENDER, W., GRUHL, D., MORIMOTO, N. & LU, A. 1996. Techniques for data hiding. *IBM systems journal,* 35**,** 313-336.

BHATTACHARYYA, S. 2011. A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier. *Journal of global research in computer science,* 2.

BHATTACHARYYA, S. & SANYAL, G. 2012. Feature based audio steganalysis (FAS). *International Journal of Computer Network and Information Security,* 4**,** 62.

BHOWAL, K., PAL, A. J., TOMAR, G. S. & SARKAR, P. Audio steganography using GA. Computational Intelligence and Communication Networks (CICN), 2010 International Conference on, 2010. IEEE, 449-453.

BHOWAL, K., SARKAR, D., BISWAS, S. & SARKAR, P. P. 2016. Secured Genetic Algorithm Based Image Hiding Technique with Boolean Functions. *IJ Network Security,* 18**,** 758-768.

BÖHME, R. Assessment of steganalytic methods using multiple regression models. International Workshop on Information Hiding, 2005. Springer, 278-295.

BRANDENBURG, K. & POPP, H. 2000. MPEG layer-3. *EBU Technical review***,** 1-15.

CACHIN, C. An information-theoretic model for steganography. International Workshop on Information Hiding, 1998. Springer, 306-318.

CASTELAN, Y. & KHODJA, B. MP3 Steganography Techniques. Proceedings of the 4th Annual ACM Conference on Research in Information Technology, 2015. ACM, 51-54.

CHANDRAMOULI, R. & MEMON, N. D. A distributed detection framework for steganalysis. Proceedings of the 2000 ACM workshops on Multimedia, 2000. ACM, 123-126.

CHEN, B., LUO, W. & LI, H. Audio Steganalysis with Convolutional Neural Network. Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security, 2017a. ACM, 85-90.

CHEN, M., SEDIGHI, V., BOROUMAND, M. & FRIDRICH, J. 2017b. JPEG-Phase-Aware Convolutional Neural Network for Steganalysis of JPEG Images.

CHHIKARA, R. & SINGH, L. 2013a. A Review on Digital Image Steganalysis Techniques Categorised by Features Extracted. *image,* 3.

CHHIKARA, S. & SINGH, P. 2013b. SBHCS: Spike based Histogram Comparison Steganalysis Technique. *International Journal of Computer Applications,* 75.

COX, I., MILLER, M., BLOOM, J., FRIDRICH, J. & KALKER, T. 2007. *Digital watermarking and steganography*, Morgan Kaufmann.

CRAWFORD, H. A. 2012. *A framework for continuous, transparent authentication on mobile devices.* University of Glasgow.

DAS, R. & TUITHUNG, T. A novel steganography method for image based on Huffman Encoding. Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on, 2012. IEEE, 14-18.

DENG, K., ZHANG, R., TIAN, Y., YU, X., NIU, X. & YANG, Y. Steganalysis of the MP3 steganographic algorithm based on Huffman coding. Intelligent Computing and Integrated Systems (ICISS), 2010 International Conference on, 2010. IEEE, 79-82.

DESAI, M. B., PATEL, S. & PRAJAPATI, B. 2016. ANOVA and Fisher Criterion based Feature Selection for Lower Dimensional Universal Image Steganalysis. *International Journal of Image Processing (IJIP),* 10**,** 145-160.

DITTMANN, J. & HESSE, D. Network based intrusion detection to detect steganographic communication channels: on the example of audio data. Multimedia Signal Processing, 2004 IEEE 6th Workshop on, 2004. IEEE, 343-346.

FAROKHZAD, S., AHMADI, H., JAEFARI, A., ASADI ASAD ABAD, M. & RANJBAR KOHAN, M. 2012. Artificial neural network based classification of faults in centrifugal water pump. *Vibroengineering,* 14**,** 1734-1744.

FAROUK, M. H. 2014. Steganography and Security of Speech Signal. *Application of Wavelets in Speech Processing.* Springer.

FAZEL, K. & KAISER, S. 2013. *Multi-Carrier Spread-Spectrum & Related Topics: Third International Workshop, September 26–28, 2001, Oberpfafenhofen, Germany*, Springer Science & Business Media.

FERREIRA, J. S., RODRIGUES, H. D., GONZALEZ, A. A., NIMR, A., MATTHÉ, M., ZHANG, D., MENDES, L. L. & FETTWEIS, G. 2017. GFDM Frame Design for 5G Application Scenarios. *Journal of Communication and Information Systems,* 32.

FRIDRICH, J. Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes. International Workshop on Information Hiding, 2004. Springer, 67-81.

FRIDRICH, J. & GOLJAN, M. 2004. Reliable detection of LSB steganography in color and grayscale images. Google Patents.

FRIDRICH, J. & KODOVSKY, J. 2012. Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security,* 7**,** 868-882.

GE, X. & TIAN, H. 2015. On the influence of feature selection and extraction for the classification of steganalysis based on the JPEG image. *Journal of Computational Methods in Sciences and Engineering,* 15**,** 695-705.

GHASEMZADEH, H. & KAYVANRAD, M. H. 2017. A Comprehensive Review of Audio Steganalysis Methods. *arXiv preprint arXiv:1701.05611*.

GOMEZ-CORONEL, S. L., ESCALANTE-RAMıREZ, B., ACEVEDO-MOSQUEDA, M. A. & ACEVEDO, M. E. 2014. Steganography in audio files by hermite transform. *Appl. Math,* 8**,** 959-966.

GOPALAN, K. & SHI, Q. Audio Steganography Using Bit Modification-A Tradeoff on Perceptibility and Data Robustness for Large Payload Audio Embedding. ICCCN, 2010. 1-6.

HASHEMI, S. A., MONADJEMI, S. A. H. & RAMIN, M. 2014. Price Index Forecasting Using BP Neural Network and Wavelet Neural Networks. *Asian Journal of Research in Banking and Finance,* 4**,** 105-116.

HOGAN, M. T., SILVESTRE, G. C. & HURLEY, N. J. Performance evaluation of blind steganalysis classifiers. Electronic Imaging 2004, 2004. International Society for Optics and Photonics, 58-69.

HOLUB, V. & FRIDRICH, J. Designing steganographic distortion using directional filters. Information Forensics and Security (WIFS), 2012 IEEE International Workshop on, 2012. IEEE, 234-239.

HOMBURG, H., MIERSWA, I., MÖLLER, B., MORIK, K. & WURST, M. A Benchmark Dataset for Audio Classification and Clustering. ISMIR, 2005. 528-31.

HOU, Y., NI, R. & ZHAO, Y. Steganalysis to adaptive pixel pair matching using two-group subtraction pixel adjacency model of covers. Signal Processing (ICSP), 2014 12th International Conference on, 2014. IEEE, 1864-1867.

JAN-TI, Y. & YU, J.-M. A novel hardware implementation of MP3 decoder for low power and minimum chip size. ASIC, 2005. ASICON 2005. 6th International Conference On, 2005. IEEE, 1085-1088.

JAYARAM, P., RANGANATHA, H. & ANUPAMA, H. 2011. Information hiding using audio steganography–a survey. *The International Journal of Multimedia & Its Applications (IJMA) Vol,* 3**,** 86-96.

JIN, C., WANG, R. & YAN, D. 2016. Steganalysis of MP3Stego with low embedding-rate using Markov feature. *Multimedia Tools and Applications***,** 1-16.

JIN, C., WANG, R., YAN, D., MA, P. & YANG, K. A novel detection scheme for mp3stego with low payload. Signal and Information Processing (ChinaSIP), 2014 IEEE China Summit & International Conference on, 2014. IEEE, 602-606.

JIN, C., WANG, R., YAN, D. & YU, X. 2012. Steganalysis of UnderMP3Cover. *J. Comput. Inf. Syst.,* 8**,** 10459-10468.

KABAL, P. 2002. An examination and interpretation of ITU-R BS. 1387: Perceptual evaluation of audio quality. *TSP Lab Technical Report, Dept. Electrical & Computer Engineering, McGill University***,** 1-89.

KARTALOPOULOS, S. V. & KARTAKAPOULOS, S. V. 1997. *Understanding neural networks and fuzzy logic: basic concepts and applications*, Wiley-IEEE Press.

KATZENBEISSER, S. & PETITCOLAS, F. A. 2016. *Information hiding*, Springer.

KEKRE, H., ATHAWALE, A. A. & PATKI, S. A. Improved steganalysis of LSB matching steganography based on counting alteration rate of the number of neighbourhood gray levels. Proceedings of the International Conference & Workshop on Emerging Trends in Technology, 2011. ACM, 432-435.

KEKRE, H. B., ATHAWALE, A., RAO, B. S. & ATHAWALE, U. Increasing the capacity of the cover audio signal by using multiple LSBs for information hiding. Emerging Trends in Engineering and Technology (ICETET), 2010 3rd International Conference on, 2010. IEEE, 196-201.

KER, A. D., BAS, P., BÖHME, R., COGRANNE, R., CRAVER, S., FILLER, T., FRIDRICH, J. & PEVNÝ, T. Moving steganography and steganalysis from the laboratory into the real world. Proceedings of the first ACM workshop on Information hiding and multimedia security, 2013. ACM, 45-58.

KER, A. D. & PEVNÝ, T. 2014. The steganographer is the outlier: realistic large-scale steganalysis. *IEEE Transactions on information forensics and security,* 9**,** 1424-1435.

KESAVARAJ, G. & SUKUMARAN, S. A study on classification techniques in data mining. Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on, 2013. IEEE, 1-7.

KESSLER, G. C. & HOSMER, C. 2011. An overview of steganography. *Advances in Computers,* 83**,** 51-107.

KHAN, A., TAHIR, S. F., MAJID, A. & CHOI, T.-S. 2008. Machine learning based adaptive watermark decoding in view of anticipated attack. *Pattern Recognition,* 41**,** 2594-2610.

KIM, D.-S., LEE, G.-J. & YOO, K.-Y. A reversible data hiding scheme based on histogram shifting using edge direction predictor. Proceedings of the 2014 Conference on Research in Adaptive and Convergent Systems, 2014. ACM, 126-131.

KIPPER, G. 2003. *Investigator's guide to steganography*, crc press.

KODOVSKY, J., FRIDRICH, J. & HOLUB, V. 2012. Ensemble classifiers for steganalysis of digital media. *IEEE Transactions on Information Forensics and Security,* 7**,** 432-444.

KODOVSKÝ, J., PEVNÝ, T. & FRIDRICH, J. Modern steganalysis can detect YASS. IS&T/SPIE Electronic Imaging, 2010. International Society for Optics and Photonics, 754102-754102-11.

KOTSIANTIS, S. B., ZAHARAKIS, I. & PINTELAS, P. 2007. Supervised machine learning: A review of classification techniques.

KRAETZER, C. & DITTMANN, J. Pros and cons of mel-cepstrum based audio steganalysis using SVM classification. Information Hiding, 2007. Springer, 359-377.

KRENN, R. 2004. Steganography and steganalysis. *Retrieved September,* 8**,** 2.

KUMAR, V. & MINZ, S. 2014. Feature Selection. *SmartCR,* 4**,** 211-229.

LI, B., HE, J., HUANG, J. & SHI, Y. Q. 2011. A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing,* 2**,** 142-172.

LIN, Y. & ABDULLA, W. H. Perceptual evaluation of audio watermarking using objective quality measures. Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on, 2008. IEEE, 1745-1748.

LIU, Q., SUNG, A. H., CHEN, Z. & XU, J. 2008. Feature mining and pattern classification for steganalysis of LSB matching steganography in grayscale images. *Pattern Recognition,* 41**,** 56-66.

LIU, Q., SUNG, A. H. & QIAO, M. 2010. Detection of double MP3 compression. *Cognitive Computation,* 2**,** 291-296.

LIU, Q., SUNG, A. H. & QIAO, M. 2011. Derivative-based audio steganalysis. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM),* 7**,** 18.

LIU, W. M., JELLYMAN, K. A., MASON, J. S. & EVANS, N. W. Assessment of objective quality measures for speech intelligibility estimation. Acoustics, Speech and Signal Processing, 2006. ICASSP 2006 Proceedings. 2006 IEEE International Conference on, 2006. IEEE, I-I.

LUO, D., SUN, M. & HUANG, J. 2016. Audio postprocessing detection based on amplitude cooccurrence vector feature. *IEEE Signal Processing Letters,* 23**,** 688-692.

MAZURCZYK, W., WENDZEL, S., ZANDER, S., HOUMANSADR, A. & SZCZYPIORSKI, K. 2016. *Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures*, John Wiley & Sons.

MEGHANATHAN, N. & NAYAK, L. 2010. Steganalysis algorithms for detecting the hidden information in image, audio and video cover media. *international journal of Network Security & Its application (IJNSA),* 2**,** 43-55.

MICHE, Y., BAS, P., LENDASSE, A., JUTTEN, C. & SIMULA, O. 2009. Reliable steganalysis using a minimum set of samples and features. *EURASIP Journal on Information Security,* 2009**,** 901381.

MIRJAVADI, S., HAMOUDA, A., PANAHI, M. S., JEBELI, S. M. & MOUSAVI, M. 2013. A Combined Approach for Steganalysis embedded data stored in gray-scale images through LSB.

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

MOUAZEN, A., KUANG, B., DE BAERDEMAEKER, J. & RAMON, H. 2010. Comparison among principal component, partial least squares and back propagation neural network analyses for accuracy of measurement of selected soil properties with visible and near infrared spectroscopy. *Geoderma,* 158**,** 23-31.

MUTHURAMALINGAM, S., KARTHIKEYAN, N., GEETHA, S. & SINDHU, S. S. S. 2016. Stego anomaly detection in images exploiting the curvelet higher order statistics using evolutionary support vector machine. *Multimedia Tools and Applications,* 75**,** 13627-13661.

NEMATOLLAHI, M. A., VORAKULPIPAT, C. & ROSALES, H. G. 2016a. *Digital Watermarking*, Springer.

NEMATOLLAHI, M. A., VORAKULPIPAT, C. & ROSALES, H. G. 2017. Audio Watermarking. *Digital Watermarking.* Springer.

NEMATOLLAHI, O., HOGHOOGHI, H., RASTI, M. & SEDAGHAT, A. 2016b. Energy demands and renewable energy resources in the Middle East. *Renewable and Sustainable Energy Reviews,* 54**,** 1172-1181.

NILSSON, M. 2000. ID3 tag version 2.4. 0-Main Structure. *http//www. id3. org/id3v2*.

PANG, W., LUO, X., REN, J., YANG, C. & LIU, F. Rapid detection of stego images based on identifiable features. Advanced Communication Technology (ICACT), 2016 18th International Conference on, 2016. IEEE, 708-716.

PAULIN, C., SELOUANI, S.-A. & HERVET, É. A comparative study of audio/speech steganalysis techniques. Electrical and Computer Engineering (CCECE), 2017 IEEE 30th Canadian Conference on, 2017. IEEE, 1-4.

PEVNÝ, T. & FRIDRICH, J. Novelty detection in blind steganalysis. Proceedings of the 10th ACM workshop on Multimedia and security, 2008. ACM, 167-176.

PHAM, D. & AFIFY, A. 2005. Online discretization of continuous-valued attributes in rule induction. *Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science,* 219**,** 829-842.

POISEL, R. & TJOA, S. Forensics investigations of multimedia data: A review of the state-of-the-art. IT Security Incident Management and IT Forensics (IMF), 2011 Sixth International Conference on, 2011. IEEE, 48-61.

QIAO, M., SUNG, A. H. & LIU, Q. Steganalysis of mp3stego. Neural Networks, 2009. IJCNN 2009. International Joint Conference on, 2009. IEEE, 2566-2571.

QIAO, M., SUNG, A. H. & LIU, Q. 2013. MP3 audio steganalysis. *Information sciences,* 231**,** 123-134.

QUACKENBUSH, S. 2012. MPEG Audio Compression Advances. *The MPEG Representation of Digital Media.* Springer.

RAMAN, B. & IOERGER, T. R. 2003. Enhancing learning using feature and example selection. *Texas A&M University, College Station, TX, USA*.

RAMESHKUMAR, P., MONISHA, M. & SANTHI, B. 2014. Enhancement of information hiding in audio signals with efficient LSB based methods. *Indian Journal of Science and Technology,* 7**,** 80-85.

RANA, M. 2016. Parameter Evaluation and Comparison of algorithms used in Steganography. *International Journal of Engineering Science,* 8134.

REDDY, K. S. M., BABU, G. R. & RAO, S. K. M. 2015. Global Optimization for the Forward Neural Networks and Their Applications. *i-Manager's Journal on Computer Science,* 3**,** 9.

SAEVANEE, H., CLARKE, N., FURNELL, S. & BISCIONE, V. 2015. Continuous user authentication using multi-modal biometrics. *Computers & Security,* 53**,** 234-246.

SAEYS, Y., INZA, I. & LARRAÑAGA, P. 2007. A review of feature selection techniques in bioinformatics. *bioinformatics,* 23**,** 2507-2517.

SALIH, M. M. 2015. *A New Audio Steganography Method Using Bi-LSB Embedding and Secret Message Integrity Validation.* Middle East University.

SAYOOD, K. 2012. *Introduction to data compression*, Newnes.

SCHAATHUN, H. G. 2012. BOOK TOOLS.

SHAHADI, H. I. & JIDIN, R. High capacity and inaudibility audio steganography scheme. Information Assurance and Security (IAS), 2011 7th International Conference on, 2011. IEEE, 104-109.

SHAHZAD, M., LIU, A. X. & SAMUEL, A. Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it. Proceedings of the 19th annual international conference on Mobile computing & networking, 2013. ACM, 39-50.

SHANMUGAPRIYA, V. & PADMAVATHI, G. Keystroke dynamics authentication using neural network approaches. International Conference on Advances in Information and Communication Technologies, 2010. Springer, 686-690.

SHARMA, M. & BERA, S. 2012. A review on blind still image steganalysis techniques using features extraction and Pattern classification method. *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT),* 2**,** 117-135.

SHARMA, N. & DEEP, E. G. 2015. To Study Scope of Data Hiding in MP3 Files. *International Journal of Science, Engineering and Computer Technology,* 5**,** 138.

SHELKE, F. M., DONGRE, A. A. & SONI, P. D. 2014. Comparison of different techniques for Steganography in images. *International Journal of Application or Innovation in Engineering & Management,* 3**,** 171-176.

SINDER, D. J., VARGA, I., KRISHNAN, V., RAJENDRAN, V. & VILLETTE, S. 2015. Recent speech coding technologies and standards. *Speech and Audio Processing for Coding, Enhancement and Recognition.* Springer.

SINGH, A. K., TYAGI, B. & KUMAR, V. 2013. Application of feed forward and recurrent neural network topologies for the modeling and identification of binary distillation column. *IETE Journal of Research,* 59**,** 167-175.

SINGH, P. K., SINGH, H. & SAROHA, K. A survey on steganography in audio. Proceedings of the 3rd National Conference, 2009. 26-27.

SOKOLOVA, M. & LAPALME, G. 2009. A systematic analysis of performance measures for classification tasks. *Information Processing & Management,* 45**,** 427-437.

SRIDEVI, G. & SRINIVASAMURTHY, C. 2011. Source separated anthropogenic liquid waste (Human Urine)-A potential plant nutrients for banana cultivation. *Biores Bulletin,* 1**,** 052-057.

STERNE, J. 2012. *MP3: The meaning of a format*, Duke University Press.

STERNE, J. 2014. How tHe MP3 BecaMe UBiqUitoUs. *The Oxford Handbook of Mobile Music Studies,* 1**,** 37.

STOLL, G. & KOZAMERNIK, F. 2000. EBU listening tests on Internet audio codecs. *EBU technical review,* 28**,** 1-24.

SU, Q. 2017. *Color Image Watermarking: Algorithms and Technologies*, Walter de Gruyter GmbH & Co KG.

SUBHEDAR, M. S. & MANKAR, V. H. 2014. Current status and key issues in image steganography: A survey. *Computer science review,* 13**,** 95-113.

SUPUROVIC, P. 1998. MPEG audio frame header. *Available In Internet*.

THIAGARAJAN, J. J. & SPANIAS, A. 2011. Analysis of the MPEG-1 Layer III (MP3) algorithm using MATLAB. *Synthesis Lectures on Algorithms and Software in Engineering,* 3**,** 1-129.

TINT, Y. & MYA, K. T. 2012. Audio Steganalysis Using Features Extraction and Classification. *Science,* 3.

TRAORÉ, J. 2016. *Mohamed SABT.* Orange Labs.

TRIVEDI, M. C., SHARMA, S. & YADAV, V. K. Analysis of Several Image Steganography Techniques in Spatial Domain: A Survey. Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, 2016. ACM, 84.

UHL, T., PAULSEN, S. & NOWICKI, K. 2017. New approach for determining the QoS of MP3-coded voice signals in IP networks. *EURASIP Journal on Audio, Speech, and Music Processing,* 2017**,** 1.

USHA, B., SRINATH, D. N. & CAUVERY, D. N. 2013. Data embedding technique in image steganography using neural network. *International journal of advanced research in computer and communication engineering,* 2**,** 2319-5940.

WAN, W., ZHAO, X.-F., HUANG, W. & SHENG, R.-N. 2012. Steganalysis of MP3Stego based on Huffman table distribution and recording. *Journal of Graduate University of Chinese Academy of Science,* 29**,** 118-124.

WANG, Y. & MOULIN, P. 2007. Optimized feature extraction for learning-based image steganalysis. *IEEE Transactions on Information Forensics and Security,* 2**,** 31-45.

WESTFELD, A. Detecting low embedding rates. International Workshop on Information Hiding, 2002. Springer, 324-339.

WESTFELD, A., WURZER, J., FABIAN, C. & PILLER, E. Pit stop for an audio steganography algorithm. IFIP International Conference on Communications and Multimedia Security, 2013. Springer, 123-134.

WITTEN, I. H., FRANK, E., HALL, M. A. & PAL, C. J. 2016. *Data Mining: Practical machine learning tools and techniques*, Morgan Kaufmann.

WU, M. & LIU, B. 2013. *Multimedia data hiding*, Springer Science & Business Media.

XIA, Z., WANG, X., SUN, X. & WANG, B. 2014. Steganalysis of least significant bit matching using multi-order differences. *Security and Communication Networks,* 7**,** 1283-1291.

YAN, D. & WANG, R. 2014. Detection of MP3Stego exploiting recompression calibration-based feature. *Multimedia tools and applications,* 72**,** 865-878.

YAN, D., WANG, R., YU, X. & ZHU, J. 2013. Steganalysis for MP3Stego using differential statistics of quantization step. *Digital Signal Processing,* 23**,** 1181-1185.

YANG, Y., PINTUS, R., RUSHMEIER, H. & IVRISSIMTZIS, I. 2017. A 3D steganalytic algorithm and steganalysis-resistant watermarking. *IEEE transactions on visualization and computer graphics,* 23**,** 1002-1013.

YAVANOGLU, U., OZCAKMAK, B. & MILLETSEVER, O. A new intelligent steganalysis method for waveform audio files. Machine Learning and Applications (ICMLA), 2012 11th International Conference on, 2012. IEEE, 233-239.

YU, X., WANG, R. & YAN, D. 2013. Detecting MP3Stego using calibrated side information features. *Journal of Software,* 8**,** 2628-2636.

ZAMANI, M., ABDUL MANAF, A., AHMAD, R., ZEKI, A. M. & ABDULLAH, S. 2009. A genetic-algorithm-based approach for audio steganography. *World Academy of Science, Engineering and Technology,* 54**,** 360-363.

ZAMANI, M. & MANAF, A. B. A. 2015. Genetic algorithm for fragile audio watermarking. *Telecommunication Systems,* 59**,** 291-304.

ZHU, Q., SHACHAM, O., MEIXNER, A., REDGRAVE, J. R., FINCHELSTEIN, D. F., PATTERSON, D., DESAI, N., STARK, D., CHANG, E. T. & MARK, W. R. 2015. Architecture for high performance, power efficient, programmable image processing. Google Patents.