A STYLOMETRY APPROACH FOR BLIND LINGUISTIC STEGANALYSIS MODEL AGAINST TRANSLATION-BASED STEGANOGRAPHY

SYIHAM BINTI MOHD LOKMAN

A thesis submitted in
fulfillment of the requirement for the award of the
Degree of Master of Information Technology

Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia

FEBRUARY, 2023

To my father, my mother and my husband.

ACKNOWLEDGEMENT

In the name of Allah, the Beneficent, the Merciful, all praise and thanks to Allah. First of all, I am thankful to Allah S.W.T for His blessings and for giving me the strength to complete my Master's degree in Information Technology. Secondly, I would like to express my gratitude to my supervisor Assoc. Prof. Dr Aida Mustapha for all her support and encouragement. She has always been willing to give her precious time when I asked for her advice to help me with her great ideas and knowledge. She is a very responsible and caring educator desirous of helping students succeed. This thesis would never have been possible without her great guidance. Credit also goes to Dr. Roshidi Din and his team from Universiti Utara Malaysia, all my lecturers and to all those who have shared with me their expertise, support and advice relevant to my project. A special mention goes to my family and friends for their moral support and motivation throughout the period of conduction this research and also during my studies at UTHM because they inspire me to succeed. Lastly, I would also like to thank the Ministry of Higher Education for partially sponsoring my study through the Fundamental Research Grant Scheme under FRGS/1/2015/ICT02/UTHM/02/1 with the title “A New Blind Linguistic Steganalysis Model based on Stylometric Approach for Higher Accuracy in Stego Text Detection”.

ABSTRACT

Steganography is the art of hiding information in ways that prevent the detection of a secret message. In Translation-based Steganography (TBS), the secret messages are encoded in the "noise" made via translation of natural language text programmed. The adversarial technique to extract the secret message is called steganalysis, which can be categorized into two types; targeted vs. blind. While targeted steganalysis is designed to attack a specific embedding algorithm, blind steganalysis use features extracted or selection from the medium to detect any anomalies that indicate a possibility that a secret data has been embedded within the medium. However, accuracy of blind steganalysis algorithms highly depend on the features selected from the input data especially when attacking embedding techniques in TBS. This thesis explore the potential of using stylometry or linguistic style to improve the representation of characteristics among the word distribution in distinguishing the stego text from the cover text for TBS. This is because all translated in TBS text have an intrinsic structural styles that can be used to improve the performance of a blind steganalysis model. The proposed stylometry-based blind steganalysis model consists of two stages, which are stylometric feature selection and classification. The proposed stylometric features selected from a set of cover text are categorized into two group features; lexical and syntactic features before implemented into the model Support Vector Machine (SVM) as the classifier. The performance of the stylometry-based blind steganalysis model is then evaluated based on all false rate, missing rate and accuracy rate and compared against three other standard classifiers in steganalysis; Naive Bayes (NB), *k*-Nearest Neighbor (*k*-NN), and Decision Tree (J48). The results showed that the stylometric features are impactful to a blind steganalysis model by giving higher detection performance. Meanwhile, SVM is the best classifier for stego text detection with significantly low processing time performance.

ABSTRAK

Steganografi adalah seni menyembunyikan maklumat dengan cara yang menghalang pengesanan mesej rahsia. Teknik *Translation Based Steganography (TBS)* adalah teknik yang menyembunyikan mesej rahsia dalam "*noise*" yang dibuat melalui terjemahan teks yang diprogramkan. Teknik untuk mendedahkan mesej rahsia dikenali sebagai steganalisis, yang dikategorikan kepada dua jenis; disasarkan vs buta. Steganalisis yang disasarkan, dirancang untuk menyerang algoritma penyembunyian tertentu manakala steganalisis buta menggunakan ciri yang diekstrak dari media untuk mengesan sebarang anomali yang menunjukkan kemungkinan data rahsia telah disembunyikan dalam media. Walau bagaimanapun, ketepatan algoritma steganalisis buta bergantung pada ciri-ciri yang diambil dari data yang dimasukkan terutamanya ketika menyerang teknik penyembunyian *TBS*. Tesis ini meneroka potensi menggunakan *stylometry* atau gaya linguistik untuk meningkatkan perwakilan ciri di antara perkataan dalam membezakan teks *stego* dari teks *cover* untuk *TBS*. Ini kerana semua yang diterjemahkan dalam teks *TBS* mempunyai gaya struktur intrinsik yang dapat digunakan untuk meningkatkan prestasi model steganalisis buta. Model steganalisis buta berasaskan *stylometry* yang dicadangkan terdiri daripada dua peringkat, iaitu pengekstrakan dan klasifikasi ciri *stylometry*. Ciri *stylometric* yang dicadangkan yang diekstrak dari sekumpulan teks *cover* dikategorikan kepada dua ciri; ciri *lexical* dan *syntactic* sebelum dilaksanakan ke dalam model *Support Vector Machine (SVM)* sebagai pengelasan. Prestasi model steganalisis buta berasaskan *stylometry* kemudian dinilai berdasarkan kadar salah, kadar hilang dan kadar ketepatan serta dibandingkan dengan tiga pengelasan standard lain dalam steganalisis; *Naive Bayes (NB), k-Nearest Neighbor (k-NN),* dan *Decision Tree (J48*). Hasil kajian menunjukkan bahawa ciri *stylometric* mempengaruhi model steganalisis buta dengan memberikan prestasi pengesanan yang lebih tinggi. Sementara itu, SVM adalah pengelasan terbaik untuk pengesanan teks *stego* dengan prestasi masa pemprosesan yang sangat rendah.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF PUBLICATIONS

Syiham Mohd Lokman, Aida Mustapha (2018) Chapter 4: Techniques for Targeted Linguistic Steganalysis: A Review. *Data Engineering and Information Security Series 2*, UTHM, 27, ISBN: 9789672216582.

Syiham Mohd Lokman, Aida Mustapha, Azizan Ismail, Roshidi Din. Analysis Review on Linguistic Steganalysis. *Indonesian Journal of Electrical Engineering and Computer Science.* 2019. 17(2): 950-956.

CHAPTER 1

INTRODUCTION

1.1 Research Background

Information privacy has continually been a struggle to everyone's concern. Through history, several techniques have been developed attempting to protect sensitive information against unauthorized people. The art of hiding information while not arousing suspicion is named steganography. The term came from Greek, steganos which means "covered" and graphos which means "writing". The first record regarding the term steganography was in Steganoraphia book written by Johannes Trithemius in 1499 (De Leeuw & Bergstra, 2007). According to Herodotus (1972), the first written evidence steganographic technique is used by the tyrant Histiaeus, who shaved a servant's head before tattooing a message on his poor scalp. The servant was dispatched to deliver his message after his hair had grown back. A message could be unkempt under the wax as the people were familiar to write in wax-covered tablets. Afterward, Aeneas Tacticus was in charge of giving a guide to ensure military communications safety. He prepared several forms to hide a physical message, such as in women's earrings or pigeons or in a letter as small holes over the paper hidden within the text (Aeneas, 1948).

Another standard ancient technique known as acrostic, consists of hiding a message in a very specific spot of each word in a text, for example a literary composition. In spite of its simplicity, the utilization of acrostics has survived till modern wars. The invisible ink is another technique widely used, even during this time. Invisible ink has evolved from natural substances to a lot of complicated chemicals. In 1870, during Franco-Prussian War, Rene Dragon used photographic shrinking techniques in messages that allowed pigeons to hold more information. This concept

evolved into the modern microdot that consists images of the size of a printed period. The first detected microdot was introduced from a German spy in 1941. There are more in history, but with the introduction of digital communications, most of the previous techniques become outdated and new forms occur, taking advantage of media data (Johnson *et al.*, 2001).

In modern days, steganography is specifically used as a technique to protect confidential information in applications such as copyright protection, authentication, as well as author identification and edition management. For example, Xiang *et al.* (2017) proposed a novel linguistic steganography based on synonym run-length encoding. In 2018, Xiang *et al.* introduced a linguistic steganography based on word indexing compression and candidate selection. Meanwhile, in 2019, a steganography technique based on arithmetic coding with large-scale neural language model is utilized (Ziegler *et al.*, 2019). Zhang *et al.* (2020) used linguistic semantic steganography framework. They used a controlled text generation model for embedding and a semantic classifier for extraction.

In 2021, a framework for concealing information using Arabic calligraphy has been presented. String matching is used in the embedding step to generate stego text and accompanying letter shapes based on a secret message (Hamzah *et al.*, 2021). Yu *et al.* (2022) retained the decoding advantages of fixed-length coding in this paper, focus on finding solutions of existing steganography methods, and propose a multi-time-step-based steganography advisable to put multiple time steps to select words that can convey secret information and match the statistical distribution, then ensuring better text quality. However, there are some dangerous applications as terrorism or child pornography. Maney (2001) emphasized that according to USA, the government of Unites States has detected messages hidden in pictures published in popular websites and even in pornographic ones. A decade later, CNN also reported some documents regarding terrorist plans based on information revealed by German authorities. The terrorist plan was found in various digital storage devices containing pornographic contents, including more than a hundred covered documents (Robertson *et al.*, 2012).

Due to the wide application of steganography, it becomes necessary to plan or design a method that capable to detect potential hidden information. This method is known as steganalysis, which is a set of techniques responsible to discover, extract or destroy covered information. The main goal of steganalysis is to identify whether or

not a suspected medium is embedded with secret data. In detecting this, steganalysis techniques can be targeted or blind. In targeted steganalysis, the knowledge on specific steganographic technique or the embedding algorithm used to embed the secret message is necessary. This is because the detection or the steganalysis algorithm used will be specific to the embedding technique used to embed or hide the secret message in the first place. Blind steganalysis, on the other hand, is capable of detecting secret messages without any knowledge of the content or the embedding technique (Nissar & Mir, 2010), hence the term universal steganalysis.

The classification of blind steganalysis techniques is determined by the type of feature extraction or selection and data mining techniques used (Bera *et al.*, 2019). The features are refers to unique characteristics that exists which can be in the form of image, video, audio, or text. It is particularly helpful when the information under analysis came from an unknown source. Therefore, the media type has important influence to a blind steganalysis model because analyzing text, for example, needs totally different tools to those employed in images-based steganography. This is the main reason why blind steganalysis works well with statistical data, hence also known as statistical steganalysis (Sabnis & Awale, 2016).

1.2 Problem Statement

Blind steganalysis model works based on the assumption that there are some features being modified during the embedding process, which can be used as an input to train the steganalysis model. To achieve this, blind steganalysis algorithms employ supervised learning to distinguish between the plain cover against the stego image or text. In particular, blind steganalysis adopts a standard two-phase classification methodology; feature extraction or selection and classification. In feature selection phase, the linguistic features are selected from the cover text (with or without hidden information) and then used to predict cover text vs. stego text (Perez, 2013). It is imperative that these features to be very sensitive to the embedding changes, therefore, the accuracy of blind steganalysis models highly depend on the features selected from the input data.

From the literature in linguistic steganalysis, existing models employed various statistical and Natural Language Processing (NLP) techniques to statistically detect anomalies in cover text (suspected medium) such as word shift coding (Yang *et al.*,

2014) and word embedding (Xiang *et al.*, 2018; Zuo *et al.*, 2018). The techniques employed various features such as word distribution (Taskiran *et al.*, 2006; Sui *et al.*, 2006; Zhi-Li *et al.*, 2008; Meng *et al.*, 2010a; 2010b), space distribution (Xin-Guang & Hui, 2007), font types and sizes (Lingyun *et al.*, 2007), attribute value pairs (Xiang *et al.*, 2014), and semantic or contextual information (Gang *et al.*, 2008; Zuo *et al.*, 2018) to predict the presence of hidden or secret data.

However, steganalysis techniques specific to attack against the translation-based steganography is very limited. Remarkably, due to the difficulties in recognizing redundant bits in a text file, text steganalysis is commonly not takes priority (Majeed *et al.*, 2021). Text steganalysis is a difficult task in practice due to the wide variety of digital text characteristics, the comprehensive variation of embedding techniques, and, in most cases, the low encoding deformation (Taleby *et al.*, 2019). In practice, blind steganalysis is more appealing because it can operate independently of the technique and can even be generalized to unknown steganography approaches (Yang *et al.*, 2014; Gupta & Bandyopadhyay, 2020; Din *et al.*, 2012a; Din *et al.*, 2012b). Translation-based steganography hides secret data within the common errors or noise produced during the translation process of one language to another (Grothoff *et al.*, 2005; 2009). The idea is two-step; embed the secret data in a cover text of the original language and use machine translation to encode the secret message for all sentences in the cover text.

The basic premise in attacking TBS is that, when utilizing a machine translator to interpret texts from one language to different language, the translator will use words in some mechanical way. Therefore, the translated texts have a specific structural style set by the machine translator. Consequently, the stego texts must have a unique way of structure that are set by all the utilized translators. Similar to human writing texts, also known as natural texts, the translated text will have the intrinsic structural styles. Because TBS produces more natural-like text by conserving the correct syntax and coherent semantics, stego text of TBS are more difficult to analyze and detected.

Chen *et al.* (2008) proposed statistical linguistic steganography detection using Word Distribution Analysis (WDA) method. In the WDA technique, the spread degree (SD) of a word is characterized as the difference of its situation in the testing text. At that point, the normal and difference of the spread level of words in the preparation content are utilized to shape the order of vector. Then, a two-class SVM classifier is used to categorize the testing text into normal text and stego text. According to the

work, the structural information of testing text provided by WDA worked well in detection of linguistic steganography methods. However, there are many detailed information lost.

Subsequent work by Meng *et al.* (2010a) used targeted steganography to attack TBS. However, in targeted steganography, the method needs to know type of machine translator (MT) used and language of cover text. Other than that, this method also has to find the translator set before do steganalysis as the translator set has the private key of TBS. This reduced the cohesion of the method. Besides, the cover text has to be translated twice via every translator, so, therefore is very expensive for large scale distribution.

In 2010, Meng *et al.* (2010b) approached the same problem with WDA but using blind steganography. The proposed method do not need to identify the machine translator used via TBS encoder. The method depends on the fact that in stego writings, there are less high recurrence words writings than normal texts. Similarly, they used two-class SVM classifier to differentiate stego texts and normal text by first extracting the feature vector related to the frequencies of the high frequency words. However, this method still have some weakness. It is not completely blind steganalysis as it need some prepared resources such as high frequency words and *n*-grams. In addition, the accuracy of detection needs to be enhanced, especially when the text size is small.

Chen *et al.* (2010) improved the WDA technique by using the Natural Frequency Zone (NFZ) in text. NFZ is a word group whose member words have similar occurrence frequencies called the NF values. The proposed NFZ-WDA technique was capable to blindly distinguish natural texts, machine translated texts and stego texts that are generated by TBS by examining distribution characteristics of words within the same natural frequency zone. However, the research concluded that the countermeasure of translation-based steganography is highly challenging because it is extremely difficult to change the word distributions in all NFZs (Chen *et al.*, 2010).

To address this gap, this thesis is set to investigate the potential for using stylometry, i.e., linguistic style, as opposed to only the structural style used on the WD-NFZ technique. The basic observation is that, linguistic style which consist of both structural and lexical style, both can be sources to detect embedded secret information. To date, stylometry has been widely used in several areas such as music lyrics (Kranenburg *et al.*, 2004), paintings (Elizabeth, 2007), literary works (Calix *et al.*, 2008), forensic linguistics (Abbasi & Chen, 2005), plagiarism (Zheng *et al.*, 2006),

social networking (Kucukyilmaz *et al.*, 2007; Mohtasseb & Amr, 2009), electronic mail (Calix *et al.*, 2008; Mohtasseb & Amr, 2009), and instant messaging (Abbasi & Chen, 2005; Kucukyilmaz *et al.*, 2007).

The effectiveness of the proposed stylometric features is then evaluated using the standard blind steganalysis methodology, which is a supervised learning experiment (Jung, 2019). Because the main body of research in blind steganalysis focuses on feature extraction or selection, many standard classifiers were used in the literature such as the Support Vector Machine (SVM) (Pevny *et al.*, 2010; Chiew & Pieprzyk, 2010; Chen *et al.*, 2011; Guan *et al.*, 2011; Menori & Munir, 2016; Shankar & Azhakath, 2020), Neural Networks (Lafferty & Ahmed, 2004; Shi *et al.*, 2005), Principal Component Analysis (Li *et al.*, 2011), ensembles of SVM (Shankar & Upadhyay, 2019; Gireeshan *et al.*, 2020) and hybrid Neural Networks (Niu *et al.*, 2019).

1.3 Objectives

The main goal of this thesis is to propose a new blind steganalysis model based on the stylometric approach in translation-based steganography. To achieve this goal, the following objectives are to be fulfilled:

1. To propose a new blind steganalysis model using stylometry approach.
2. To implement stylometric feature selection which include lexical feature and syntactics feature tailored to linguistic steganalysis for revealing the stego text.
3. To evaluate the performance of blind steganalysis model via supervised experiment using Support Vector Machine (SVM) classifiers using false rate, the missing rate, and the accuracy rate.

1.4 Scope of Study

This research is scoped to linguistic blind steganalysis using the text medium to attack translation-based steganography. The stylometry approach proposed is based on lexical features and syntactic features in the input text. Following the literature, the blind steganalysis model is evaluated via a classification experiment to detect stego text from input cover text.

1.5 Organization of Thesis

The rest of the thesis is organized as follows; Chapter 2 provides a review of the basic concepts about steganalysis. Compatibly, this paper introduces standard blind steganalysis concepts, its categorization and the main parts of the steganalysis process.

Chapter 3 describes proposed model including the feature extraction or selection and applied stylometric formula for detection of stego text.

Chapter 4 describe the experimental setup, which includes dataset and the embedding techniques used in the input cover text.

Chapter 5 reports and analyzes the experimental results when evaluating the performance of the proposed blind steganalysis model based on the stylometric features.

Finally, Chapter 6 concludes the research by discussing the contribution of this thesis with some indication for potential future works.

CHAPTER 2

LITERATURE REVIEW

This chapter introduces the domain of translation-based steganography and works in detecting or attacking them. This chapter also presents blind steganalysis, its classification and literature works. Next, this chapter introduces stylometry and how it can be applied to blind linguistic steganalysis. Finally, the chapter reviews and summarizes existing literature on previous approaches of linguistic steganalysis.

2.1 Translation-based Linguistic Steganography

Steganography is the art of hiding information in ways that prevent the detection of a secret message (Johnson & Jajodia, 1998). In modern definition, steganography is a well-known technique of hiding secret data in a non-secret medium such as image, audio, video, or text (Fridrich, 2009). There are two basic operations involved in steganography. The first operation is embedding the secret data in an input medium called the cover medium. Once the secret data already embedded, the medium is then known as the stego medium. The second operation is extracting the secret data from the stego medium to recover the original secret data (Chiew & Pieprzyk, 2010).

In 2005, Grothoff *et al.* (2005) introduced a different and comparatively secure methodology which was known as Translation-based Steganography (TBS). TBS conceals information inside the "noise" made via translation of natural language text programmed. The main idea of TBS is that, while translating a common text between two natural languages, usually, there are numerous of conceivable translations. Picking one in every of these translations can be utilized to encode information (Grothoff *et al.*, 2005). This is because there are common errors in valid programmed translated

texts. This is extreme for a computer to separate the additional errors inserted by an information hiding algorithm and the normal noise related to translation.

There are two versions of TBS, Lost in Translation (Lit) (Grothoff *et al.*, 2005) and Lost in Just the Translation (LiJtT) (Stutsman *et al.*, 2006). For Lit, the sender gets a cover text inside the source language, which does not should be kept secret and can be acquired from open sources. At that point, sender takes the source text to target language sentence by sentence utilizing different translators and encodes the hidden messages in this technique by picking one proper translator for each source sentence. The advantages of LiT system are it can operates within the constraints of machine translator, as machine translator models transform, so can the LiT system. Besides, the generation issue is avoided by simulating the outcomes of an imperfect transformation rather than correct, human-produced text. LiT system also has secret key for implementation, corpus training and configuration that is enables the use of multiple encoders. The cover text is public and can be gained from public sources (Grothoff *et al.*, 2005). However, LiT system has low bitrate and the requirement to send both the source text and the translation.

LiJtT enhanced Lit to empower the receiver in recovering the hidden message utilizing only stego texts and a secret key. For LiJtT, firstly, multiple translations for a given cover text is generated by user. Then, sender and receiver uses secret key which is shared between the sender and the receiver to hash each translated sentence into a bit string. Furthermore, the lowest h bits of the hash string, alluded to as header bits, are interpreted as an integer b 0 and then the sentence who is lowest $[h + 1, h + b]$ bits coordinate with the bit-sequence to be encoded is chosen. Finally, the user gets a stego text, breaks the received text into sentences, applies a keyed hash to each sentence and interprets the lowest $[h + 1, h + b]$ bits of each hash string as the next b bits of the hidden message. The work flow of LiJtT is showed in Figure 2.1.

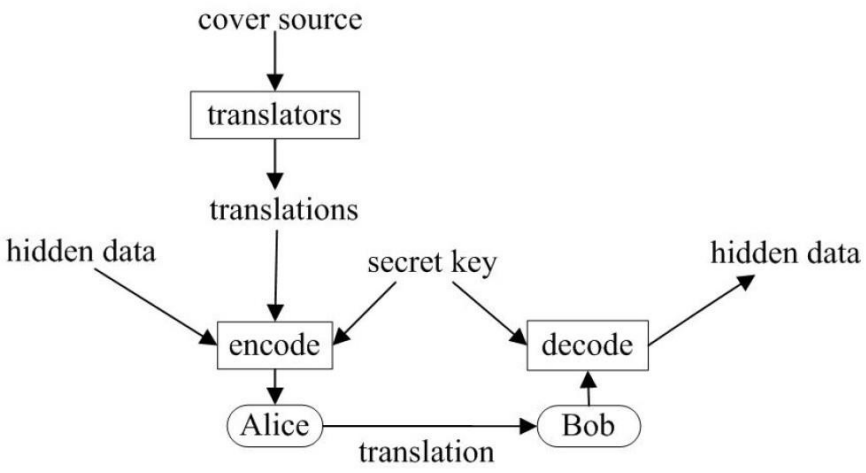

Figure 2.1: LiJtT Work Flow (Stutsman *et al.*, 2006)

The steganographic secret message is embedded in the translation by choosing from multiple translations produced by either modifying the translation process or post-processing the translated sentences. The new protocol can avoid transmitting the source text, making the protocol easier to use and decoding simpler. It also allows the sender to use a combination of human and machine translation during the encoding process. An adversary must illustrate that the probably results translation is unusual to be produced by any valid translation system in order to conquer the system.

2.2 Steganalysis

Research uncovers that a significant number of the new headings in steganography began from assault investigations are called steganalysis. The way toward breaking down steganographic protocol is completed with a specific end goal to identify and remove concealed messages known as stego message. Steganalysis begins with a few speculated data streams that has potential to contain stego messages. While the goal of steganography is to eliminate confusion about hidden messages in other information, the goal of steganalysis is to discover and extract secret messages, such as covert messages in a given message (Ranggo *et al.*, 2013).

2.2.1 Medium of Steganalysis

Based on recent cloud communication, steganalysis can be distributed into two domain areas, which are digital media and natural language as shown in Figure 2.2.

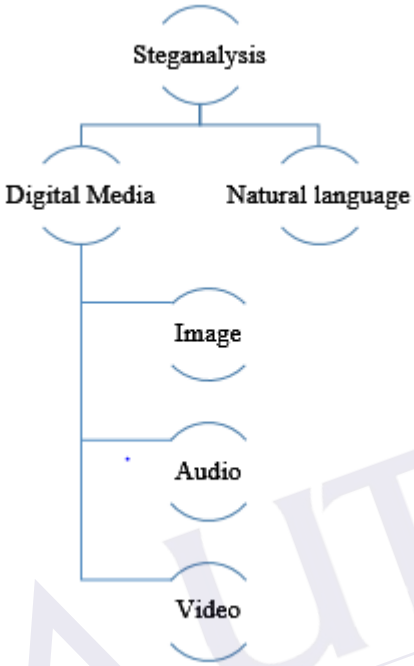

Figure 2.2: Steganalysis Domain

Digital steganalysis is classified into three categories which are image, audio and video. In image class, there are two main types of image algorithm: Specific and Generic. Image steganalysis techniques characterization class depends on the original steganographic algorithm used which is known as specific approach (Meghanathan *et al.*, 2010). It also consumes a high rate of achievement to recognize the existence of a secret message if the message is hidden by the proposed algorithm. In the meantime, Generic approach characterizes the class of image steganalysis techniques that are self-determining the basic steganography algorithm used to hide the message and produce great results for distinguishing the existence of a hidden message using new or unusual steganographic algorithms. Image steganalysis techniques in both specific and generic categories are often intended to recognize the existence of a secret message and the decoding of the same is considered to be complementary and not mandatory (Meghanathan *et al.*, 2010).

The process of recognizing the presence or absence of concealed messages inside audio files is identified as audio steganalysis. No substantial amount of writing is accessible on audio steganalysis. This can be credited to the presence of innovative audio steganography plans and the idea of audio signs to be high-capacity data streams requires the requirement for logically difficult statistical analysis (Kraetzer & Dittmann, 2008). In audio steganalysis, Ru *et al.* (2005) introduced the estimation of the features between the signal and the self-created reference signal through linear predictive coding called the detection method. Avcibas (2006) outlined the content-independent distortion steps as functions of the classification scheme. Ozer *et al.* (2006) made the detector dependent on the characteristics of the remains of the audio file. To identify secret messages in audios, Johnson *et al.* (2005) set up a statistical model by building a linear basis that captures certain statistical characteristics of audio signals. Kraetzer & Dittmann (2008) arranged a Mel-cepstrum-based investigation to discover hidden messages inserted. In the meantime, video steganalysis is a use of image steganalysis techniques for video orders at the edge-by-outline principle that has yielded poor execution performance.

Comparable to audio steganalysis, very limited video steganalysis techniques are available in writing. The underlying and comprehensive treatment for video steganalysis is from Budhia (2004). This method was used by the closer look to identify data introduced using additive white Gaussian noise in the space domain. Collusion uses data from contiguous frames to estimate the current frame. This research attempts a number of different collusion methods together with weighted averaging, blockage, and simple linear averaging based on the reconstruction of reference frames. Block-based recreation benefits for comparable blocks in adjacent frames and duplicate them in another reference frame. The difference between this reference frame and the first is that it is used to test the data added. Entropy, kurtosis and the 25th percentile over this approximation are used for their features.

2.2.2 Targeted vs. Blind Steganalysis

Secret message disclosure that is hidden in cover text most commonly demonstrates as a classification problem. In steganalysis, the input is an object and classified either cover text or stego text in steganalysis algorithm. At the other point, Bob and Alice are secretly communicating whereas Eve can being used. Eve must build up a steganalysis

REFERENCES

Abbasi, A. & Chen, H. (2005). Applying Authorship Analysis to Extremist Group Web Forum Messages. *IEEE Intelligent Systems, 20(5),* pp. 67-75.

Abramov, P. S. (2018). *Automatic Iq Estimation Using Stylometry Methods*. University of Louisville: Master's Thesis.

Aeneas T. (1948). *Loeb Classical Library Illinois* (Greek Club, Trans.).

Ahvanooey M. T., Li, Q., Hou, J., Rajput, A. R. & Chen, Y. (2019) Modern Text Hiding, Text Steganalysis, and Applications: A Comparative Analysis. *Entropy, 21(4),* pp. 2-29.

Amancio, D. G., Comin, C. H., Casanova, D., Travieso, G., Bruno, O. M., Rodrigues, F.A. & Costa, L. F. (2014). A Systematic Comparison of Supervised Classifiers. *Plos One, 9(4),* pp. 1-14.

Argamon, S., Saric, M. & Stein, S. S. (2003) Style Mining of Electronic Messages for Multiple Authorship Discrimination: First Results. *Proc. of 9th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining.* Association for Computing Machinery. pp. 475-480.

Argamon, S., Whitelaw, C., Chase, P., Hota, S. R., Garg, N. & Levitan, S. (2007) Stylistic Text Classification using Functional Lexical Features. *Journal of the American Society for Information Science and Technology, 58(6),* pp. 802-822.

Avcibas, I. (2006) Audio Steganalysis with Content-Independent Distortion Measures. *IEEE Signal Processing Letters, 13(2),* pp. 92-95.

Baayen, R., van Halteren, H., & Tweedie, F. (1996) Outside The Cave of Shadows: Using Syntactic Annotation to Enhance Authorship Attribution. *Literary and Linguistic Computing, 11(3),* pp. 121-131.

Biber, D. (1992). *Variation across Speech and Writing* (Reprint ed.). Cambridge University Press.

Bihani, G., & Rayz, J. T. (2022). *On Information Hiding in Natural Language Systems*. ResearchGate. Retrieved on 2021, from https://www.researchgate.net/publication/359228019_On_Information_Hiding_in_Natural_Language_Systems

Bera, S., Sharma, M., & Singh, B. (2019). An Experimental Analysis of Feature Based Blind Steganalysis Techniques. *International Journal of Innovative Technology and Exploring Engineering*, *8(8S3)*, pp. 340–360.

Bhattacharyya, S., Banerjee, I. & Sanyal, G. (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(4)*, pp. 1-16.

Calix, K., Connors, M., Levy, D., Manzar, H., McCabe, G. & Westcott S. (2008). Stylometry for E-mail Author Identification and Authentication. *Proc. of CSIS Research Day*. Pace University. Semantic Scholar. pp. 1-7.

Cervantes, A., Sloan, T., Hernandez-Castro, J. & Isasi P. (2018) System Steganalysis with Automatic Fingerprint Extraction. *Plos One*, *13(7)*, pp. 1-26.

Chang, C. Lin, C. (2011). LIBSVM: A Library for Support Vector Machines. *ACM Transactions on Intelligent Systems and Technology*, *2(3)*.

Chatterjee, S. & Hadi, A. S. (2013). *Regression Analysis by Example*. 5th ed. United States: Wiley.

Chen, Z., Huang, L., Zhenshan, Y., Lingjun, L. & Yang, W. (2008). A Statistical Algorithm for Linguistic Steganography Detection Based on Distribution of Words. *Proc. of the 3rd Int. Conf. on Availability, Reliability and Security.* Barcelona Spain. IEEE. pp. 558-563.

Chen, Z., Huang, L., Meng, P., Yang, W. & Miao, H. (2010). Blind Linguistic Steganalysis against Translation-Based Steganography. *Proc. of the 9th Int. Conf. on Digital Watermarking*. Seoul. Springer. pp. 251-265.

Chiew, K. L., & Pieprzyk, J. (2010) Blind steganalysis: A Countermeasure for Binary Image Steganography. *International Conf. on Availability, Reliability and Security.* IEEE. pp. 653-658.

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

Christian, G., Krista, G., Ludmila, A., Ryan, S. & Mikhail, A. (2005). Translation-Based Steganography. *Proc. of Information Hiding*. Purdue University. Springer. pp. 221-233.

Cox, I. J., Miller M. L., Bloom, J.A., Fridich, J. & Kalker, T. (2008) *Digital Watermarking and Steganography*. 2nd ed. Amsterdam: Morgan Kaufmann.

Coyotl-Morales, R.M., Villaseñor-Pineda, L., Montes-y-Gómez, M., & Rosso, P. (2006). Authorship Attribution Using Word Sequences. *In Proc. of the 11th Iberoamerican Congress on Pattern Recognition*. Berlin. Springer. 2006. pp. 844-853.

Davis, M. & Putnam, H. (1960). A Computing Procedure for Quantification Theory. *Journal of ACM*. *7(3),* pp. 201-215.

Deng, X., Li, Y., Weng, J., & Zhang, J. (2019) Feature selection for text classification: A review. *Multimedia Tools and Applications*. *78(3),* pp. 3797-3816.

Din, R., Samsudin, A., & Lertkrai, P. (2012). A framework components for natural language steganalysis. *International Journal of Computer Theory and Engineering*, *4(4),* pp. 641.

Din, R., Samsudin, A., Muda, T. Z. T., Lertkrai, P., Amphawan, A., & Omar, M. N. (2013). Fitness value based evolution algorithm approach for text steganalysis model. *International Journal of Mathematical Models and Methods in Applied Sciences*. *7(5),* pp. 551-558.

Din, R., Ahmad, F., Hussain, H. S., Sabri, S., Khidzir, N. Z., & Musa, M. (2016) A Performance of Text Steganalytic System using Genetic-based Method. *ARPN Journal of Engineering and Applied Sciences. 11(10),* pp. 6216-6221.

Din, R. (2014) Designing the key detection of text steganalysis based. *Advanced Science Letters*. *20(1),* pp. 158-163.

Ding, S. H., Fung, B. C., Iqbal, F., & Cheung, W. K. (2017) Learning Stylometric Representations for Authorship Analysis. *IEEE Transactions on Cybernetics. 49(1),* pp. 107-121.

Dwidevi, Y. P., Beta, S., & Sharma, M. (2017). Review on Universal Steganalysis Techniques Based on the Feature Extraction in Transform Domain. *International Journal of Engineering Research and Development. 13(9),* pp. 07-11.

El-Fiqi, H., Petraki, E. & Abbass, H. A. (2019). Network Motifs for Translator Stylometry. *Plos One*. *14(2),* pp. 1-33.

Elizabeth, S. (2007). *Is that painting real? Ask a mathematician.* Retrieved on May 10, 2007, from https://www.csmonitor.com/2007/0510/p15s02-stss.html.

El-Kwae, E. A. & Cheng L. (2002). HIT: A New Approach for Hiding Multimedia Information in Text. *Proc of Society of Photo-Optical Instrumentation Engineers (SPIE).* San Jose. SPIE. pp. 132-140.

Fridrich, J. & Goljan, M. (2002). Practical Steganalysis: State of the Art. *Proceedings of the SPIE – The Int. Society for Optical Engineering 4675*. San Jose. SPIE. pp. 1-13.

Fridrich, J. (2009). *Steganography in digital media: principles, algorithms, and applications*. Cambridge University Press.

Gamon, M. (2004). Linguistic correlates of style: Authorship Classification with Deep Linguistic Analysis Features. *Proc. of the 20th Int. Conf. on Computational Linguistics*. Geneva. COLING. pp. 611-617.

Gang, L., Xingming, S., Lingyun, X., Yuling, L., & Can, G. (2008). Steganalysis on synonym substitution steganography. *Journal of Computer Research and Development*. pp. 10.

Ge, H., Huang, M., & Wang, Q. (2011). Steganography and steganalysis based on digital image. *In 4th International Congress on Image and Signal Processing*. IEEE. pp. 252-255.

Gireeshan, M. G., Shankar, D. D., & Azhakath, A. S. (2020). Feature Reduced Blind Steganalysis Using DCT and Spatial Transform on JPEG Images with and without Cross Validation Using Ensemble Classifiers. *Journal of Ambient Intelligence and Humanized Computing*,

Grieve, J. (2007). Quantitative Authorship Attribution: An Evaluation of Techniques. *Literary and Linguistic Computing. 22(3), pp.* 251-270.

Grothoff, C., Grothoff, K., Alkhutova, L., Stutsman, R., & Atallah, M. (2005). Translation-based steganography. *In International Workshop on Information Hiding*. Berlin. Springer. pp. 219-233.

Grothoff, C., Grothoff, K., Stutsman, R., Alkhutova, L., & Atallah, M. (2009). Translation-based steganography. *Journal of Computer Security*. *17(3),* pp. 269-303.

Guan, Q., Dong, J., & Tan, T. (2011). An effective image steganalysis method based on neighborhood information of pixels. *18th IEEE International Conf. on Image Processing*. IEEE. pp. 2721-2724.

Gupta Banik, B., & Bandyopadhyay, S. K. (2020). Novel text steganography using natural language processing and part-of-speech tagging. *IETE Journal of Research, 66(3).* pp. 384-395.

Hamzah, A. A., Khattab, S., & Bayomi, H. (2021). A linguistic steganography framework using Arabic calligraphy. *Journal of King Saud University-Computer and Information Sciences, 33(7),* pp. 865-877.

Herodotus (1972). *The Histories* (Selincourt, A., Trans.). England: Penguin. (Original work published 430 BC)

Holmes, D. I. & Kardos, J. (2003). Who was the Author? Stylometry. *Chance*, 16(2), pp. 5-8.

Holmes, D.I., & Forsyth, R. (1995). The Federelist Revisited: New Directions in Authorship Attribution. *Literary and Linguistic Computing*. *10(2),* pp. 111-127.

Houvardas, J., & Stamatatos E. (2006). N-gram Feature Selection for Authorship Identification. *Proc. of the 12th International Conf.on Artificial Intelligence: Methodology, Systems, Applications*. Berlin. Springer. pp. 77-86.

Ingale, A. K., Dharwadkar, N. V., & Kodulkar, P. (2016). Universal Steganalysis using DWT and Entropy Features. *International Conference on Signal and Information Processing (IConSIP).* Vishnupuri. IEEE.

Johnson, N. F., Jajodia, S. (1998). Exploring Steganography: Seeing the Unseen. *IEEE Computer Society*. *31(2),* pp.26–34.

Johnson, N. F., Dunic, Z. & Jajodia, S. (2001). *Information Hiding: Steganography and Watermarking-Attacks and Countermeasures.* New York. Springer.

Johnson, M.K., Lyu, S., & Farid, H. (2005). Steganalysis of Recorded Speech. *Proc. of SPIE- The Int. Society for Optical Engineering.* San Jose. SPIE. pp. 664-672.

Jung, K. (2019). A Study on Machine Learning for Steganalysis. *Proceedings of the 3rd Int. Conference on Machine Learning and Soft Computing.* Da Lat Vietnam, ACM.

Kim, H. J., Shi, Y. Q., & Barni, M. (2011). *Digital Watermarking*. Berlin: Springer.

Kraetzer, C., Oermann, A., Dittmann, J. & Lang, A. (2007) Digital Audio Forensics: A First Practical Evaluation on Microphone and Environment Classification.

Proc. of the 9th workshop on Multimedia and Security. Dallas. Association for Computing Machinery. pp. 63-74.

Kranenburg, V. P. & Backer, E. (2005). Musical Style Recognition – a Quantitative Approach. Chen, C. H. & Wang, P. S. P. *Handbook of Pattern Recognition and Computer Vision*. United States. World Scientific Publishing. pp. 583-600.

Koppel, M., Schler, J., Argamon, S., & Messeri, E. (2006). Authorship Attribution with Thousands of Candidate Authors. *Proc. of the 29th ACM SIGIR.* Association for Computing Machinery. pp. 659-660.

Kucukyilmaz, T., Cambazoglu, B, Aykanat, C. & Can, F. (2008) Chat Mining: Predicting User and Message Attributes in Computer-Mediated Communication. *Information Processing & Management*. *44(4),* pp. 1448-1466.

Lafferty, P., & Ahmed, F. (2004). Texture-based steganalysis: results for color images. In Mathematics of Data/Image Coding, Compression, and Encryption VII, with Applications. *55(61),* pp. 145-151.

Li, H., Sun, Z., & Zhou, Z. (2011). An Image Steganalysis Method Based on Characteristic Function Moments and PCA. *Proc. of the 30th Chinese Control Conf.* IEEE. pp. 3005-3008.

Lingyun, X., Xingming, S., Gang, L. & Can, G. (2007). Research on Steganalysis for Text Steganography Based on Font Format. *Third International Symposium on Information Assurance and Security*. Manchester. IEEE. pp. 490-495.

Luo, X. Y., Wang, D. S., Wang, P., & Liu, F. L. (2008). A review on blind detection for image steganography. *Signal Processing, 88(9),* pp. 2138-2157.

Majeed, M. A., Sulaiman, R., Shukur, Z., & Hasan, M. K. (2021). A Review on Text Steganography Techniques. *Mathematics*, *9(21),* pp. 2829.

Mark, C. & Davida, G. (1997). *Hiding the Hidden: A Software System for Concealing Ciphertext as Innocuous Text.* Retrieved on June 17, 2005, from https://link.springer.com/.

Matsuura, T., & Kanada, Y. (2001). Extraction of Authors' Characteristics from Japanese Modern Sentences via N-Gram Distribution. *Proc. of the International Conference on Discovery Science.* Berlin. Springer. pp. 315-319.

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(1),* pp. 43-55.

Meng, P., Huang, L., Yang, W., & Chen, Z. (2009). Attacks on Translation-based Steganography. *Proc. of IEEE Youth Conference on Information, Computing and Telecommunication*. Beijing. IEEE. pp. 227-230.

Meng, P., Hang, L., Chen, Z., Hu, Y., & Yang, W. (2010a). STBS: A Statistical Algorithm for Steganalysis of Translation-Based Steganography. In *International Workshop on Information Hiding*. Berlin. Springer. pp. 208-220.

Meng, P., Huang, L. S., Chen, Z. L., Yang, W., & Yang, M. (2010b). Analysis and Detection of Translation-Based Steganography. Dianzi Xuebao (Acta Electronica Sinica). 38(8):1748-1752.

Meng, P., Shi, Y. Q., Huang, L., Chen, Z., Yang, W., & Desoky, A. (2011). *LinL:Lost in n-best List.* Retrieved from doi: 10.1007/978-3-642-24178-9_23.

Menori, M. H., & Munir, R. (2016). Blind Steganalysis for Digital Images using Support Vector Machine Method. *International Symposium on Electronics and Smart Devices (ISESD)*. IEEE. pp. 132-136.

Mohtasseb, H. and Ahmed, A. (2009). Mining Online Diaries for Blogger Identification. *Proc. of the World congress on Engineering*. London. Live Journal. pp. 1-8.

Neal, T., Sundrarajan, K., Fatima, A., Yan, Y., Xiang, Y. & Woodard, D. (2017). Surveying Stylometry Techniques and Applications. *ACM Computing Surveys*. *50(6)*, pp. 86:1-86:33.

Nechta, I. & Fionov, A. (2011). *Applying Statistical Methods to Text Steganography*. Retrieved on October 12, 2011, from https://arxiv.org/

Nissar, S. & Mir, A. H. (2010). Classification of Steganalysis Techniques: A Study. *Digital Signal Processing, 20(6),* pp. 1758-1770.

Niu, Y., Wen, J., Zhong, P., & Xue, Y. (2019). A Hybrid R-BILSTM-C Neural Network Based Text Steganalysis. *IEEE Signal Processing Letters, 26(12),* pp. 1907-1911.

Osman, B., Yasin, A., Omar, M. N. (2016). An Analysis of Alphabet-based Techniques in Text Steganography. *Journal of Telecommunication, Electronic and Computer Engineering, 8(10),* pp. 109-115.

Ozer, H., Sankur, B., Memon, N. D. & Avcibas I. (2006). Detection of Audio Covert Channels Using Statistical Footprints of Hidden Messages. *Digital Signal Processing, 16(4),* pp. 389-401.

Peng, F., Shuurmans, D., & Wang, S. (2004). Augmenting Naive Bayes Classifiers with Statistical Language Models. *Information Retrieval Journal*.. 7(1): 317-345.

Perez, M. R. (2013). *Blind Steganalysis Method for Detection of Hidden Information in Images*. National Institute for Astrophysics, Optics and Electronics: Master Thesis.

Pevny, T., Bas, P., & Fridrich, J. (2010). Steganalysis by subtractive pixel adjacency matrix. *IEEE Transactions on information Forensics and Security*, 5(2), pp. 215-224.

Philipp, K. (2004). *Europarl: A Parallel Corpus for Statistical Machine Translation*. Retrieved on November, 2004, from https://www.researchgate.net/

Rauf, R. H. A., & Jamal, N. (2014). Feasibility of Text Visualization in Text Steganalysis. *The 13th International conference on Intelligent Software Methodologies, Tools and Techniques*. Langkawi. SOMET. pp. 103-115.

Raggo, M. T., Hosmer, C., & McGrew, W. (2012). *Data Hiding: Exposing Concealed Data In Multimedia, Operating Systems, Mobile Devices and Network Protocols*. Amsterdam: Elsevier.

Raggo, M. T. (2013). *Steganography, Steganalysis, & Cryptanalysis* [Slides]. Blackhat. Retrieved from https://www.blackhat.com/presentations/bh-usa-04/bh-us-04-raggo/bh-us-04-raggo-up.pdf.

Reddy, S. K. P. (2007). *Steganalysis Technique: A Comparative Study*. University of New Orleans: Master Thesis.

Ru, X.M., Zhang, H.J., & Huang, X. (2005). Steganalysis of audio: Attacking the Steghide. *Proc. 4th Int.Conference on Machine Learning and Cybernetics*. Guangzhou. IEEE. pp. 3937-3942.

Rishidas, S., Krishnan, G. L. & Kumar, S. (2015). A Comparative Study of Steganalysis using Support Vector Machines on Different Image Formats. *International Journal of Engineering Research and Technology, 4(3),* pp. 762-764.

Ryan, S., Christian, G., Mikhail, A. & Krista, G. (2005). Lost in Just the translation. *Proc. of ACM Symposium on Applied Computing*. Association for Computing Machinery. pp. 338-345.

Sabnis, S. K., & Awale, R. N. (2016). Statistical Steganalysis of High Capacity Image Steganography with Cryptography. *Procedia Computer Science, 79(3),* pp. 321-327.

Sanderson, C., & Guenter, S. (2006). Short Text Authorship Attribution via Sequence Kernels, Markov Chains and Author Unmasking: An Investigation. *In Proc. of the Int. Conf. on Empirical Methods in Natural Language Engineering*. Sydney. Association for Computing Machinery. pp. 482-491.

Samanta, S., Dutta, S., & Sanyal, G. (2016). A Real Time Text Steganalysis by using Statistical Method. *IEEE Int. Conf. on Engineering and Technology (ICETECH)*. Coimbatore. IEEE. pp. 264-268.

Shankar, D. D., & Upadhyay, P. K. (2019). Blind Steganalysis for JPEG Images using SVM and SVM-PSO Classifiers. *International Journal of Innovative Technology and Exploring Engineering, 8(11).* pp 1239-1246.

Shankar, D. D., & Azhakath, A. S. (2020). Blind Feature-Based Steganalysis with and Without Cross Validation on Calibrated JPEG Images Using Support Vector Machine. *In Innovation in Electrical Power Engineering, Communication, and Computing Technology*. Singapore. Springer. pp. 17-27.

Shi, Y.Q., Xuan, G., Zou, D., Gao, J., Yang, C., Zhang, Z., Chai, P., Chen, W. and Chen, C. (2005). Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network. *IEEE International Conference on Multimedia and Expo*. IEEE. pp. 4.

Shufeng, W. (2003). *Research on Information Hiding*. University of Science and Technology of China: Master Thesis.

Solanki, K., Sarkar, A., & Manjunath, B. S. (2007). YASS: Yet another steganographic scheme that resists blind steganalysis. *In International Workshop on Information Hiding*. Berlin. Springer. pp. 16-31.

Stamatatos, E. (2009). A Survey of Modern Authorship Attribution Methods. *Journal of American Society for Information Science and Technology, 60(3),* pp. 538-556.

Stamatatos, E., Fakotakis, N., & Kokkinakis, G. (2000). Automatic Text Categorization In Terms Of Genre and Author. *Computational Linguistics, 26(4),* pp. 471–495.

Stamatatos, E., Fakotakis, N., & Kokkinakis, G. (2001). Computer-based Authorship Attribution without Lexical Measures. *Computers and the Humanities, 35(2),* pp. 193-214.

Sui, X. G., Luo, H., & Zhu, Z. L. (2006). A steganalysis method based on the distribution of first letters of words. *Int. Conf. on Intelligent Information Hiding and Multimedia*. IEEE. pp. 369-372.

Svenonius, P. (2019). *Syntactic Features*. Retrieved on April 26, 2019, from https://oxfordre.com/linguistics/view/10.1093/acrefore/9780199384655.001.0001/acrefore-9780199384655-e-179.

Taleby Ahvanooey, M., Li, Q., Hou, J., Rajput, A. R., & Chen, Y. (2019). Modern text hiding, text steganalysis, and applications: a comparative analysis. *Entropy, 21(4),* pp. 355.

Taskiran, C. M., Topkara, U., Topkara, M., & Delp, E. J. (2006). Attacks on Lexical Natural Language Steganography Systems. *Proc. of SPIE - The International Society for Optical Engineering.* San Jose. SPIE.

Topkara, M., Riccardi, G., Hakkani-Tuer, D. & Atallah, M. (2006). Natural Language Watermarking: Challenges in Building a Practical System. *Proc. of SPIE – The Int.Society for Optical Engineering.* San Jose. SPIE. pp. 106-117.

Vyas, A. O. & Dudul, S. V. (2015). Study of Image Steganalysis Techniques. *International Journal of Advanced Research in Computer Science, 6(8),* pp. 7-11.

Wayner, P. (1995). Strong Theoretical Steganography. *Cryptologia*. *19(3),* pp. 285-299.

Williams, L. (2021). *WordNet: A Lexical Taxonomy of English Words - Towards Data Science.* Retrieved on January 27, 2021, from https://towardsdatascience.com/%EF%B8%8Fwordnet-a-lexical-taxonomy-of-english-words-4373b541cfff

Xiang, L., Guo, G., Yu, J., Sheng, V. S., & Yang, P. (2020). A convolutional neural network-based linguistic steganalysis for synonym substitution steganography. *Mathematical Biosciences and Engineering, 17(2),* pp. 1041-1058.

Xiang, L., Sun, X., Luo, G., & Xia, B. (2014). Linguistic steganalysis using the features derived from synonym frequency. *Multimedia tools and applications, 71(3),* pp. 1893-1911.

Xiang, L., Wang, X., Yang, C., & Liu, P. (2017). A novel linguistic steganography based on synonym run-length encoding. *IEICE transactions on Information and Systems*, *100*(2), pp. 313-322.

Xiang, L., Wu, W., Li, X., & Yang, C. (2018). A linguistic steganography based on word indexing compression and candidate selection. *Multimedia Tools and Applications*, *77(21)*, pp. 28969-28989.

Xiang, L., Yu, J., Yang, C., Zeng, D., & Shen, X. (2018). A word-embedding-based steganalysis method for linguistic steganography via synonym substitution. *IEEE Access*, *6*, pp. 64131-64141.

Xin-Guang, S., & Hui, L. (2007). A Steganalysis Method Based on the Distribution of Space Characters. *International Conference on Communications, Circuits and Systems*. Guilin. IEEE. pp. 54-56.

Yang, Y., Lei, M., Wang, J., & Liu, B. (2014). A SVM based text steganalysis algorithm for spacing coding. *China Communications*, *11(13)*, pp.108-113.

Yang, Z., Wei, N., Sheng, J., Huang, Y., & Zhang, Y. J. *TS-CNN: Text steganalysis from semantic space based on convolutional neural network*. Retrieved on October 18, 2018, from https://arxiv.org/abs/1810.08136.

Yang, Z., Wang, K., Li, J., Huang, Y., & Zhang, Y. J. (2019) TS-RNN: Text Steganalysis Based on Recurrent Neural Networks. *IEEE Signal Processing Letters*, *26(12)*, pp. 1743-1747.

Yu, L., Lu, Y., Yan, X., & Yu, Y. (2022). MTS-Stega: Linguistic Steganography Based on Multi-Time-Step. *Entropy*, *24(5)*, pp. 585.

Yu, Z., Huang, L., Chen, Z., Li, L., Zhao, X., & Zhu, Y. (2008). Detection of Synonym-Substitution Modified Articles using Context Information. *Second Int. Conf. on Future Generation Communication and Networking*. Hainan. IEEE. pp. 134-139.

Yu, Z., Huang, L., Chen, Z., Li, L., Zhao, X., & Zhu, Y. (2009). Steganalysis of Synonym-Substitution Based Natural Language Watermarking. *International Journal of Multimedia and Ubiquitous Engineering*, *4(2)*, pp. 22-34.

Zhang, G. (2000). Neural Networks for Classification: A Survey. *IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews*, *30(4)*, pp. 451-462.

Zhang, S., Yang, Z., Yang, J., & Huang, Y. (2021). Linguistic steganography: From symbolic space to semantic space. *IEEE Signal Processing Letters, 28,* pp. 11-15.

Zhao, X., Huang, L., Li, L., Yang, W., Chen, Z., & Yu, Z. (2009). Steganalysis on character substitution using support vector machine. *Second Int. Workshop on Knowledge Discovery and Data Mining.* Moscow. IEEE. pp. 84-88.

Zheng, R., Li, J., Chen, H. & Huang, Z. (2006). A Framework for Authorship Identification of Online Messages: Writing-Style Features and Classification Techniques. *Journal of the American Society for Information Science and Technology, 57(3),* pp. 378-393.

Zhi-li, C., Liu-sheng, H., Zhen-shan, Y., Ling-jun, L., & Wei, Y. (2018). A Statistical Algorithm for Linguistic Steganography Detection Based on Distribution of Words. *Third International Conference on Availability, Reliability and Security*. Barcelona. IEEE. pp. 558-563.

Zhu, L. (2017). A Linguistic Steganalysis Approach Base on Source Features of Text and Immune Mechanism. *Computer and Information Science, 10(4),* pp. 60-66.

Ziegler, Z. M., Deng, Y., & Rush, A. M. (2019). Neural Linguistic Steganography. *Proc. of the 2019 Conf. on Empirical Methods in Natural Language Processing and the 9th Int. Joint Conference on Natural Language Processing (EMNLP-IJCNLP).* Hong Kong. Association for Computational Linguistics. pp. 1210-1215.

Zuo, X., Hu, H., Zhang, W. & Yu, W. (2018). Text Semantic Steganalysis Based on Word Embedding. *International Conference on Cloud Computing and Security*. Haikou. Springer Nature Switzerland AG. pp. 485-495.

VITA

Syiham binti Mohd Lokman was born in November 13, 1993 at Tumpat Hospital, Kelantan. She went to Sekolah Kebangsaan Pasir Pekan for primary school and continued her studied at Sekolah Menengah Kebangsaan Agama Lati for her secondary school. She furthered her studies at Kolej Matrikulasi Pulau Pinang before she did her Bachelor Degree in Computer Science majoring in Information Security at University Tun Hussein Onn Malaysia (UTHM) on 2012. In March 2018, she joined University Tun Hussein Onn Malaysia (UTHM) to continue her Master Degree in Information Technology.