CHAPTER 1

INTRODUCTION

This chapter discusses the underlying background of the research and the method to solve the problem.

1.1 Rationale

Steganography is the art of hiding information and attempts to hide the existence of embedded information [7]. Steganography has the goal of sending confidential message information openly without being detected by anyone other than the recipient. However, there is a method that can be used to attack steganography, namely steganalysis. Steganalysis aims to find the existence of information hidden by steganography and even extract hidden information [21].

Steganalysis can threaten the privacy of information, in the process of maintaining the privacy of the information. Privacy information such as passwords, credit cards, account cards, identity cards, etc. can be captured by Trojans [19]. If that happens it will result in economic loss and also put the object in a dangerous situation. Steganography can be used to transmit private information in an invisible or open manner, thereby reducing the potential for misuse of private information.

One type of steganography that can be used to hide private information is steganography with text media based on synonym substitution [18]. However, based on research from Linyun Xiang, et al [19] steganography can be attacked by using the Word Embedding Steganalysis (WES) technique. Statistically, the results of steganalysis of synonym-based steganography have a high value with a Precision of 95.24%, Recall 93.30%, and F-Value 94.26% [19].

Word Embedding Steganalysis (WES) can clearly be a weakness for steganography with synonym-based text media. WES works by classifying text into two categories, namely is cover text and stego text using the Support Vector Machine (SVM) [23]. The detection feature is used as input to the SVM classifier. The detection feature is the fitness context value in the text that is calculated and grouped into three types of features, namely Context Fitness Maximum Rate (CFMR), Context Fitness Mean Deviation (CFMD), and Context Fitness Mean (CFM). The feature has defined characteristics such as the CFM and CFMR fitness values are greater in cover text than steganography text. Meanwhile, the CFMD value is smaller in cover text than in steganographic text [19].

Classification results with high accuracy become a dangerous condition because one step further makes it easier for attackers to extract confidential information. Therefore, this research focuses on making steganography that can overcome word embedding steganalysis.

1.2 Theoretical Framework

Text steganography method based on synonym substitution, included in linguistic steganography, is widely used because it is strong and simple [13]. This type of steganography will not change the meaning of the cover text during the embedding process. However, some of the statistical features of the text change because they have different values for each word.

Steganography text based on synonym substitution, there are two types of text [5], namely are cover text that looks more natural which will keep hidden information, and stego text which has a decreased natural level which is a cover text that has been inserted with a secret message. The stego text generated by the synonym substitution method has rare and suspicious synonyms. We can identify the differences in characteristics between cover text and stego text from their natural level and the value of stego text is lower than cover text [19].

This research tries to eliminate the differences in characteristics between cover text and stego text. The process is done by modifying the cover text into sentences with a natural level of value that is not maximum. Stego text generated from a cover text whose value is not maximum will have approximately the same natural level so that the characteristics of the two texts cannot be identified.

1.3 Conceptual Framework/Paradigm

In this research, we make sentences from a collection of words that are generated from the corpus. These words will be grouped according to their respective POS tagging [8]. Each word will be assigned a value using the Word2Vec Skip Gram Model [10], then the context fitness value [19] is calculated using the TF-IDF value formula [14] multiplied by the Cosine Similarity value [19]. Sentences are made using the concept of Context-Free Grammar (CFG) [20], [12] by choosing grammar tenses so that the resulting sentences comply with grammatical rules. The purpose of generating this sentence is to have sentences with a maximum natural level based on the context's fitness value, such as cover text sentences in general [19]. We call the result of generating this sentence the original cover text.

The original cover text will be modified by using binary bits (0 and 1). Binary bits are generated from the Quantum Random Number Generator (QRNG) [4]. If 1 then the word will be replaced with a lower synonym word. Meanwhile, if 0 then the word does not change. The modification of the original cover text on Thursday is referred to as cover text. Binary bits will be hidden in sentences in the form of Zero Width Character (ZWC) [16].

Cover text will be inserted secret message in binary form. The concept of embedding uses the T-Lex system [17]. Synonym words will be selected based on the secret message that will be matched with the code provided in the Huffman code table. The result of Cover Text which has been inserted a secret message is stego text.

1.4 Statement of the Problem

In previous research from Linyun Xiang, Word Embedding Steganalysis[19] utilized the context fitness value in the sentence text as a detection feature which grouped into three types of features, namely Context Fitness Maximum Rate (CFMR), Context Fitness Maximum Deviation (CFMD), and Context Fitness Mean (CFM) with the condition that the CFM and CFMR fitness values are greater in cover text than in stego text. Meanwhile, the CFMD value is smaller in cover text than in stego text. This feature is input to the SVM classifier to distinguish between cover text and stego text.

The results of previous studies make synonym-based steganography text a step forward easier to identify or attack by criminals to extract confidential information. Steganography using synonym substitute with detection feature values that can be recognized easily by steganalysis SVM to classified between cover text and stego text. The proposed research will create a steganography text that can overcome word embedding steganalysis with the sama dataset. [19].

1.5 Objective and Hypotheses

Building a cover text with conditions where the words in the sentence do not have the highest fitness value. The steganography system created in this research produces stego text with a fitness value that is also not too high. That way, the value of the CFM, CFMD, and CFMR features in each sentence will be different from the conditions in the previous method[19] and SVM will no longer be able to find cover or stego correctly.

1.6 Assumption

Sentences in the cover text and stego text are made in English with tenses grammar according to the rules that are justified. Sentences are generated using the concept of Context-Free Grammar (CFG) from words that have been filtered and obtained from the Gutenberg corpus with a total of 18 books and a total of 2,621,613 words.

The resulting sentence is a sentence with a maximum fitness value. The fitness value is obtained from the Word2Vec Skip-Gram model and then calculates the TF-IDF and Word Correlation values.

In making cover text, the generated sentence needs to be modified so that the fitness value is not maximized by using binary bits.

Binary bits are generated from the Quantum Random Number Generator (QRNG). In terms of security, these binary bits need to be hidden in stego text by using the Zero-Width Character (ZWC).

The secret message is embedded in the cover text using the theory of the T-Lex System and the Huffman Code, resulting in a stego text that will be given to the recipient.

Receiver only receive stego text. Receiver need to create own huffman code table based on the same corpus, then receiver find out zwc code hidden in stego text and convert it as binary code to extract binary code. Cover text is not given to the receiver so it is not possible for attackers to attack the cover text.

Stego text with Zero Width Character in it is intended for public users so that even though in the stego text there are unusual characters, they are not printed on the monitor display, because ZWC can only be seen using special tools.

The main purpose of this research is to beat the word embedding synonym substitution steganalysis. We consider the naturalness of the sentence by limiting only synonymous words within the threshold limit that we use. However, there may be rare words within the threshold depending on the availability of synonyms for each word.

1.7 Scope and Delimitation

The cover text is a sentence with a modified fitness value so that it has a not maximum value. Cover text has a minimum of three words and a maximum of six.

One cover text can produce more than one stego text based on the number of synonyms for each available word. Stego text is a sentence that has been inserted a secret message and Zero-Width Character (ZWC). The secret message is information in binary form with a minimum length of 2 bits and a maximum of 8 bits inserted in the cover text to become stego text. The minimum bit in the secret message is the minimum number of binary bits that can be formed from the concept of T-Lex and Huffman Code.

The requirements of word can be embedded are the tagging is verb and noun, have a synonym who the number will form a pattern match with secret message.

1.8 Significance of the Study

This research on word embedding-based steganography by utilizing synonym substitution aims to send a secret message by hiding it in a sentence. This study pays attention to the characteristics of the fitness value in the sentence so that it cannot be attacked by steganalysis. This research can be used by institutions or institutions especially those that pay attention and focus on data security aspects. These institutions include the police, military, defense and security agencies, forensic agencies, intelligence agencies, and others [3].