CHAPTER 1
INTRODUCTION

This chapter discusses the underlying background of this research. It also discusses the overview of previous method in Graphstega paradigm and Graphstega itself.

1.1 Rationale

Nowadays, distribution of information became popular along with the development of information technology. For protecting secret information, people usually use steganography or cryptography.

Steganography means 'covertly writing' while cryptography means 'secretly writing'. The goal of steganography is different from the goal of cryptography. Cryptography makes the information unreadable by scrambling the message, while the goal of steganography is to hinder the presence of message in a cover. However, many policies of governments or companies limit the strength of cryptosystem [2]. Steganography gives advantage in this condition by hiding message within a digital file such as image, audio, video or text called cover media.

Contemporary Steganography method such as LSB (Least Significant Bit) will hide the message by altering the last bit of cover media file. The alteration process will produce noise in cover media that is assumed too look innocent. Human's eye can be easily fool to see changes or different of colors in image cover, while machine (computer) cannot easy to fool. This noise will raise suspicion such that the message can be detected [3].

In 2008, Desoky and Younis proposed a method namely *Noiseless Steganography* or Nostega that will not produce noise while camouflaging process [1]. One of the Nostega paradigms is Graphstega that avoids the arousal of suspicion in covert communications by concealing message as data points in a chart. The popular usage of chart in almost all areas such as climate, economics, or business makes the author chose Graphstega as the previous method to be enhanced in this research.

1.2 Theoretical Framework

Graphstega conceals the message by camouflaging it as data points in a chart to avoid the arousal of suspicion. The implementation of Graphstega is illustrated as follows:

Suppose there are two parties Alice and Bob. They agree to set of rules for communicating covertly by concealing message as data points in a chart. The subject of the chart is chosen based on their profession. For the example, Alice is a teacher of an elementary school and Bob is a salesman of a company. To communicate with Bob, Alice will camouflages the message as a chart and try to find a chart related to Alice's job as a teacher such as the exam scores of her students. While Bob camouflages his message as a chart about the salary of his company employees.

To enhance the security level of Graphstega, this research focused on encoding scheme such that will not raise suspicion when further investigation of camouflaged chart was conducted by adversaries. Furthermore, this research used existing chart (a chart built based on existing real data instead of the message), Sudoku puzzle and several methods of number theory were applied to enhance the security level.

1.3 Conceptual Framework

The basic concept of the proposed method was modifying the encoding scheme of Graphstega to enhance the security level. The solution of Sudoku puzzle was used for determining the points where the message was camouflaged. This research observes the suspicion level, security level of the chart-cover against guessing attack by the adversaries to get the message and robustness measurement.

1.4 Problem Statements

Based on theoretical and conceptual framework, Graphstega has high level in suspicion. Since the chart as cover in Graphstega is built by the message, it is possible that the value that represented by the chart was an impossible condition and this will raise suspicion.

1.5 Hypothesis

To overcome the problem, the proposed method would camouflage the hidden message into the existing chart. This research would use Sudoku puzzle for generating shared

secret. The solution of Sudoku puzzle is used for determining the points where the message was camouflaged.

Sudoku as secret sharing scheme is chosen because it has large number of solutions. The large number of solution in Sudoku will increase the transmission security [4].

1.6 Assumption

The existing chart was plotted based on Microsoft Excel file. The chart will be converted into image and sent to the receiver. The receiver converted the chart-cover image into Microsoft Excel file by using chart digitizer tool [5]. The chart-cover was only suitable for line and bar chart. The sender and recipient were assumed to have the same rules that had been agreed before the system was used.

1.7 Scope and Delimitation

The input of the proposed method is a message (characters) which is going to be camouflaged and an existing chart as the cover. In this case, the chart is plotted based on Excel data. In this research, a chart with a single curve is used to conceal n bits message and at least consists of 10 x-axis scales, and less than the 81 (number of cells in a Sudoku) such that each scale represented at least $n/10$ bits. If there are fraction data, then the fraction data are converted into integer. The output is a chart with camouflaged message.

1.8 Importance of The Study

This research can improve the suspicion level of Desoky's method in Graphstega by proposing an existing and realistic chart as the cover without arousing any suspicion. Furthermore, this research can also camouflage the message related to its cover. As an example, a health surveillance chart predicts an increasing number of diseases suspected for next month. It is impossible to give this warning message directly as it may cause mass panic. The sender can conceal the warning message into a chart as the cover as well as the evidence of that warning message.