CHAPTER 1
INTRODUCTION

This chapter discusses the underlying background of the research, followed with the overview of previous method in Headstega paradigm.

1.1 Rationale

For more reasons and needs, people need to share information to their intended recipients. On the other hand, information is an asset to all individuals that need to be protected from malicious parties. Therefore, efforts to secure information against malicious parties become necessary.

Protecting information can be done by using steganography. Steganography is a method for concealing secret messages, images, or videos within another content which is called as the cover. In this case, the embedded cover is seen as the original one. The secret messages can not be detected except by its intended recipients.

In 2010, Desoky introduced Noiseless Steganography or Nostega paradigm. Nostega describes a paradigm for designing steganography system, which does not introduce noise to its cover, nor exploit noise as stego-carrier. There are several Nostega-based methodologies, such as Listega or List-based steganography, Headstega or Header based Steganography, Graphstega or Graph steganography, Chestega or Chess steganography, Edustega or Education-centric steganography, etc.

One of the Nostega methods is Headstega. Headstega camouflages data only in email header as the cover (e.g., recipient's email addresses, names, or subject fields) in order to achieve the steganographic goal [1]. Since email is frequently used for communication between parties, secure communication without suspicion is necessary. To satisfy this requirement Headstega has been proposed.

Headstega in the previous method had several problems. First, Headstega has low embedding capacity because Headstega uses 4-bit slices to encode message into the first characters of email address. Thus for each character of 8-bit ASCII representation, Headstega requires 2 (two) email addresses to encode a character of message. Second,

Headstega has high level of suspicion because the cover is generated based on secret message by using invalid email domains. This will raise suspicion.

1.2 Theoretical Framework

Headstega conceals data in email header such as in email address, subject, name etc while the body of the email is not used to conceal data.

To have a better understanding of the Modified Headstega based on bitwise operation and randomization process, consider the scenario below : Bob and Alice work in the same company. Bob often sends email to Alice to tell his work. They agree on concealing messages in email headers by embedding it in email addresses, and the subject in such a way that looks unsuspicious, whereas the context of emails (the body of emails) is fully legitimate and nothing is concealed in it. To make this work, Bob and Alice use the reply and forward email. Since, Alice is not the only recipient of Bob's emails, then this will not raise suspicion.

To enhance the capability of Headstega, this research proposes two improvements, the improvement of embedding capacity and the decreasing suspicion level.

For improving the embedding capacity and decreasing the suspicion level, the email address and subject will used as steganographic covers.

1.3 Conceptual Framework

The basic concept of the proposed method was to modify the encoding scheme of Headstega to enhance the capacity and the security level. To perform the enhancements, the message was embedded based on bitwise operation and randomization process. The message was embedded into the cover using a key. The key is agreed upon by the sender and recipient. After embedding the message into the cover, then the sender send the embedded cover and the symbols to the recipient using public channel. Meanwhile the sender send the key to the recipient using secret channel. Secret channel is a way of transferring data that is resistant to overhearing and tampering. For satisfying the secret channel, the Diffie-Hellman key exchange are used.

In this research, the embedding capacity depends on the length of the cover, while the suspicion level depends on naturalness of the cover.

1.4 Problem Statements

Based on the theoretical and conceptual frameworks, there are several problems that have to be overcome from Headstega. First, Headstega has low embedding capacity because Headstega uses 4-bit slices to encode message into first characters of email address. Since each character requires 8-bit ASCII representation, Headstega requires 2 (two) email addresses to encode a character of the message. Second, Headstega has high level in suspicion because the cover is generated based on secret message by using an invalid email domain. This will raise suspicion.

1.5 Hypothesis

In order to improve the embedding capacity and security level of Headstega, the bitwise operation and randomization process for embedding message in existing email address and subject are used.

Using the bitwise operation and randomization process, one email address can conceal more than one character. Furthermore, by adding the subject as the cover, the capacity will be increased as well. Thus, the capacity using the proposed method will be greater than the original Headstega.

1.6 Assumption

In this research, an email address and subject used as a cover by using the email forwarder or email replies.

According to the RFC [2], the only required header fields are the origination date field and the originator address fields. While other header fields are syntactically optional. Beside that, based on email database, most (99,19%) of the email only have origination date field, originator address fields and subject fields.

In this case, the origination date field is not used as a cover because the pattern of the origination date field is fixed and its length is relatively unchanged. Thus the length of secret message that can be embedded into the origination date field are very limited. Meanwhile, the addition of subject as a cover was proposed to increase the capacity of message concealment. Subject is chosen because it has various pattern and length. Therefore, the length of the secret message that can be embedded in subject can be variant as well such that it will reduce the suspicion.

The email address consisted of two parts, that is the local part comes before @ sign and the domain part that comes after @. The secret message is embedded both in local part and the domain part. The local part must not exceed 64 characters and the domain part cannot be longer than 255 characters. The total length of all characters (including '@' and punctuation) should not exceed 320 characters.

The characters used in the secret message are the alphabets and also special characters, such as period, comma and space.

In its implementation, the sender and recipient both should agree to determine the location of the message concealment, since it can be embedded in email address, in the subject or both.

1.7 Scope and Delimitation

The modified Headstega based on bitwise operation and randomization process exploits bitwise operation and randomization process to conceal data in the existing email address and subject, while email body is not modified.

1.8 Importance of The Study

This research can improve message embedding capacity and lower level of suspicion of the original Headstega. It can be done by proposing an existing email address and subject as the cover without arousing any suspicion.

Headstega is possible to be implemented in organizations such as legal, government, education, such that the enhancement would not raise any suspicion. For example, an employer will send a secret message to his subordinates. For reducing the suspicion level, they use the official email address and subject to camouflage the secret message.