International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2018.32894

Volume 4, Issue 10
October - 2018

# Model for Data Hiding Using Steganography

**Pratiwi Rachmadi**

Faculty of Information Technology

Asian Banking Finance and Informatics Institute Perbanas

Jakarta, Indonesia

e-mail: pratiwi@perbanas.ac.id ;wiek.pratiwi@gmail.com

## ABSTRACT

*Steganography is a technique to secure a data communication. Data form Message, secured by inserting message bits into carrier bit files. One of Method for inserting messages in carrier files is the Least Significant Bit method. Inserting the message bits in the carrier bit file bit. Generally, this report discussed designing of steganography applications that modified 2 bits of carrier file using LSB Method. There was some testing to be performed on this application, such as embedding and retrieving process testing to know functionality application, capacity testing to know cooperation carrier sizes before and after message embedded, and quality testing by using PSNR formula to know stegano file quality. Testing conducted includes testing the sending and receiving messages that have been inserted message. From the test, it can be concluded that the data PIN (Personal Identifier Number) inserted cannot be opened by unauthorized parties and accepted banking customers when receiving an ATM card or credit card.*

***Keywords:*** *Cryptography, LSB, Steganography, Personal Identifier Number.*

## 1. INTRODUCTION

Along with the rapid technological advancements, makes it easier for someone to convey a message to others. The techniques and methods of delivering messages are increasingly diverse. However, the technique and method of delivering the message does not guarantee the security of the message to the destination. Especially if the message you want to convey is important and confidential. Therefore, it is necessary to use various ways to secure the message in order to get to the destination as a whole. Like text messages, safeguarding image messages can be done with various techniques, one of which is by using steganography techniques [1-2]. Steganography is a way to hide a message into a digital media that human senses seem to contain nothing, except for people who understand how. In steganography messages are inserted in a relatively safe form so that the message delivered does not arouse suspicion. Steganography requires two properties, namely the container media and secret messages. Steganography can be used on a variety of digital media, namely images, sound and video.

The method commonly used in inserting messages is Least Significant Bit (LSB). The basic principle of this method is to hide the secret message into insignificant bits (the last bits) of the storage media [3]. Messages that are hidden using the Least Significant bit method can be easily intercepted, because the message bits are definitely in the LSB bit of the storage media. Therefore, a modification of the Least Significant Bit (LSB) method that has not yet been done is done on the Steganography technique. In this study the message hiding in the form of *. txt with steganography technique into the container image file (cover image) using the method of Green Significant Bit (LSB) by utilizing Linear Function as a key in the process of inserting secret message bits.

This method works by using a linear function with a single variable, f (x) = mx + b. This function will be the key (key) in the process of inserting a message into the BMP image that becomes the container. From the function above the variable m and b are elements of integers or integers (z). The values of m and b are the key of the message insertion and are only known by the sender and recipient. And this value will be used to open the Extracting Files, and the file will be calculated using the Fidelity measurement. Modification using this linear function is done by converting the bits of the image with values obtained from the ASCII (American Standard Code for Information Interchange) table. After the bits are converted into ASCII, then the data is inserted into the container image bits that are adjusted to the linear function of the single variable, f (x) = mx + b.

Steganography requires two properties, namely the message and the collecting medium. The container media that is commonly used now can be text, sound, image or video. While the hidden message can be in the form of text, images, or other messages. Various techniques are used in an effort to secure an important data. Previously there was a way to maintain data security known as cryptography [4-5]. With cryptographic data, the security is maintained, but the ciphertext form that is encrypted will be easily detected and alert third parties to the confidentiality of the file [6]. For this reason, steganography (covered writing) is applied in an effort to maintain data confidentiality.

In the world of authentication banking using one single factor authentication method, multi-factor authentication uses more than one, and thus is considered as a deterrent to abuse. When using ATMs, for example, you take advantage of multi-factor authentication; there are several factors such as atm numbers, atm passwords in the form of numbers. But in one of these methods, key elements such as passwords can be hacked and misused. So here is a technique to protect customer information and to defend possible counterfeiting. In traditional banking procedures there is a threat of counterfeiting during transactions. In online banking, security starts with an authentication process, used to confirm that it is you, and not someone who has stolen your identity. Authentication generally involves one or more basic factors:

- Something that the user knows (e.g., Password, PIN)
- Something the user has (e.g., ATM card, smart card)
- User something (eg, biometric characteristics)

In all kinds of banking applications, applicant has to sign in application form while opening an account in the bank. This signature is taken as input. Now from the application form, the signature of the applicant is scanned and taken as input. In order to thicken the lighter shades of the image and to increase the intensity of the image, image is pre-processed. In further stage pre-processed image is encrypted into some share depending upon the scheme followed by the bank.

## 2. STEGANOGRAFI

Steganography is considered as a complement to cryptography and is a science and is used to hide data on a media [7-8]. The data that will be hidden is the text in the form of a 6-digit pin into an image in the form of a logo from the bank issuing the ATM card or credit card. Steganography is created as one of the methods used to secure data by hiding it in other media so that it is "not visible". To hide messages in an image without changing the visible properties, the cover media can be changed in a "noisy" area with more color variations, so there is less attention to the modification area. The most common method used in image media is Least Significant Bits or LSB [9]. The goal of steganography is to hide messages in such a away that no one apart from the intended recipient even knows that a message has been sent. This can be achieving by concealing the existence of information within seemingly harmless carriers or cover. It can be understand by the following figure.

Important aspects of Steganalysis is detecting hidden information, disabling steganography.

DOI: 10.31695/IJASRE.2018.32842

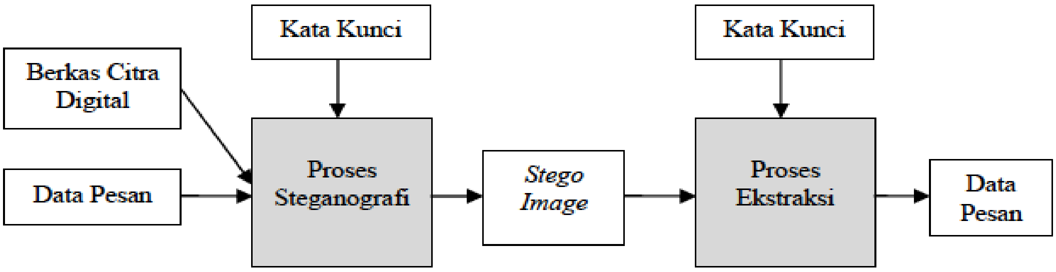

**Figure 1. Model Sistem Steganography for data hiding**

## 3. DESIGN RESERACH

The research was done by making software for steganography on the card in hiding the teks as personal identifier number (PIN), then this research including constructive research. Methodology is a procedure that is arranged in a certain, systematic and logical as the foundation for a particular activity. The required methodology consists of several stages as shown in Figure 2.

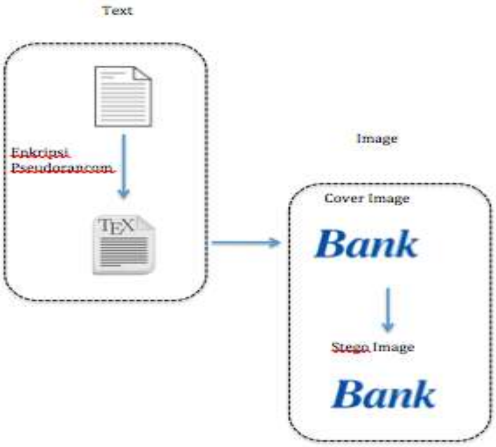

**Figure 2. Stegano Personal Identifier Number**

## 3. RESEARCH METHODOLOGY

### a Inserted message

The message inserted in this study is a message in the form of a pin number of the ATM that will be used by the customer.

### b Message encryption

Steganography and cryptography are closely related but both are different things. Cryptography messes up the message so that the message is incomprehensible while steganography hides the message in such a way that no one knows the existence of the message. In some situations, sending a message that has been encrypted will cause suspicion while a secret message that does not appear will certainly not be suspected. Both of these techniques can be combined to produce better protection against a message, ie when steganography fails and the message can be seen, the message still cannot be interpreted because it has been encrypted using cryptographic techniques.

### c Messages that have been encrypted

### d Steganography

### e Stegography (image containing text)

DOI: 10.31695/IJASRE.2018.32842

## 4. CONCLUSION

The object in this study is image data and text data. Image data in the form of images from bank logos on ATMs or credit cards, while text is a number or alphabetical text that may be used as a password on the card.

a. Message to be inserted. The text that will be entered as mentioned above is a number and alphabet that is used as a password

b. Image in the form of a logo as a message insertion media. Image data in the form of banking logo’s used.

c. The process of inserting text into the image that text inserted into the image

d. In the text encryption is done with pseudorandom. This process is carried out by referring to previous research using the Pseudorandom Encryption Cropping Selection method

e. Steganography process. This process is done by inserting text that has been encrypted into the image.

Researcher found that steganography techniques can be used for hiding data or secret messages especially data PIN (Personal , *Personal Identifier Number)*.

## OTHER RECOMMENDATIONS

It is possible to insert data in the form of text on images can use many other methods that can be used in the field of computers and cryptography which can still be explored further.

## ACKNOWLEDGMENT

The author would like to thank Perbanas Institute for funding this research, so that this research can be completed properly.

## REFERENCES

[1.] Acharya B, *Image Encryption Using Advanced Hill Cipher Algorithm*, Research Paper International Journal Of Recent Trends In Engineering, Vol. 1, No. 1, May 2009

[2.] Abdul Halim Hasugian, *Implementasi Algoritma Hill Cipher Dalam Penyandian Data* , Pelita Informatika Budi Darma, Volume IV no 2, 2013

[3.] Alatas Putri, M. Subali, *Implementation Technique With Steganography LSB Method in Digital Images*, Undergraduate Program, Faculty of Computer Science, Gunadarma University, 2009

[4.] Budi Raharjo, *Keamanan Sistem Informasi Berbasis Internet*, PT Insan Infonesia Bandung & PT INDOCISC – Jakarta 2002

[5.] Hondro ,Rivalri Kristianto, *Aplikasi Enkripsi Dan Dekripsi Sms Dengan Algoritma Zig Zag Cipher Pada Mobile Phone Berbasis Android*, 2006

[6.] JJ Siang dan Ronald S Laser, *Implementasi Sandi Hill Untuk Penyandian Citra*, Journal informatics Petra vol 3, no 1 Mei 1002

[7.] Rohayah S, Sasmito G.W, Somantri O, *Aplikasi Steganografi Untuk Penyisipan Pesan* , Jurnal Informatika Vol. 9, No. 1, Jan 2015

[8.] Schneier , *An Introduction Cryptography*, e book Copyright © 1990–2000 Network Associates, Inc. and its Affiliated Companies , 2000

[9] K.B Radja, CR Chowdary2, Venegopal Kr3,LM Patnaik, *A Secure Image Steganofrapgy using LSB, DCT and Compression Techniques on Raw Images* , , IEEE 2005

DOI: 10.31695/IJASRE.2018.32842