ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 4, Issue 6, June 2015

STEGANOGRAPHY BASED NAVIGATION OF MISSILE

Ashitosh S. Thorat, Prof. Dr. G. U. Kharat

Electronics & Telecommunication Engineering Department

Sharadchandra Pawar College Of Engineering,
Dumberwadi, Otur, Pune.

Abstract: **The aim of the "Steganography Information Hiding in Digital Images" is secure communication. The important of transmission is an issue now days. There are different methods available for hiding information in different cover media. To prevent unauthorized access of missile navigation data the technique of steganography is best suitable. To launch or navigate missile a system contain so many important data and this data is saved from unauthorized access use steganographic techniques. In this paper we designed this system for military application. In this approach the Least Significant Bit (LSB) technique is used to hide messages in an image. To apply steganographic techniques any kind of cover files can be used such as Image, sound or video files. Here the language used is embedded 'c' and MATLAB 7.4 version and the lcd is used for monitoring the status of the project.**

Keywords: Steganography, Least Significant Bit (LSB), MATLAB 7.4

I. INTRODUCTION

Transmission of data is from one place to another is biggest challenges in communication. Various methods is useful for providing security. One of the best methods is the steganography [2]. Steganography is the technique of hiding messages in other files for transmission in a manner that an observer could not identify the occurrence of transmission, is gaining popularity in current industry demands. It includes various techniques for secret communications [3].

Thus Steganography refers science of invisible communication. The growing possibilities of modern communications need the special security on computer network system. The network security is becoming more important because the number of data being exchanged on the Internet increases. Therefore, the important data are requires to protect against unauthorized access and use [6].

The rapid growth of publishing and broadcasting technology also require an alternative solution in hiding information digitally. The copyright such as audio, video and other source available in digital form may lead to unauthorized copying. In Steganography digital formats make possible to provide high image quality even under multi-copying file. The special part of invisible information is inserted in every image that could not be easily extracted without specific technique and saving image quality simultaneously [2]. All this is concern with the music, film, book and software publishing industries. The word steganography is a Greek words "*stegos*" meaning means "Cover" and "*grafia*" meaning means "writing" defining it as "covered writing [4].

II. METHODOLOGY

There are many methods are present to hide information in digital images. Following methods is present:

1] Least significant bit insertion

2] Masking and filtering

3] Algorithms and transformations

Here the "least significant bit insertion" (LSB) technique is used

Many stego tools make use of least significant bit (LSB).

For example, 1111111<u>1</u> is an 8-bit binary number. The rightmost bit is called the LSB. To change LSB it has the least effect on the value of the number.

The idea is that the LSB of every byte can be replaced with little change to the overall file.

First the binary data of the secret message is broken up and then inserted into the LSB of each pixel in the image file.

III. TYPES OF STEGANOGRAPHY

1 Text Steganography

To hide information using text steganography is historically the most important method of steganography. This method is useful to hide a secret message in every *nth* letter of every word of a text message [3].

2 Audio/Video Steganography

To hide information in audio files similar techniques are used as for image files. One different technique is used in audio steganography called masking; it is useful to exploits the properties of the human ear to hide information unnoticeably. In audio/video steganography is less popular than image steganography. Audio/video files are large so it is difficult to use [3].

3 Image Steganography

Images steganography is most popular cover objects used for steganography. Digital images contain many different image file formats; most of them are useful for specific applications. Different steganographic algorithms exist for these different image file formats [3].

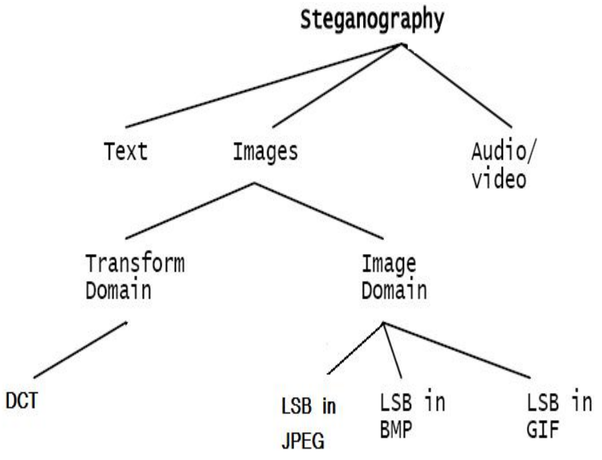


Figure 1 Algorithm & Types

IV PROPOSED WORK

A . Embedding and detecting secret information

The basic model of steganography contains following block Carrier, Message and Password. Carrier is also known as cover-object. In cover-object message is embedded and serves to hide the presence of the message.

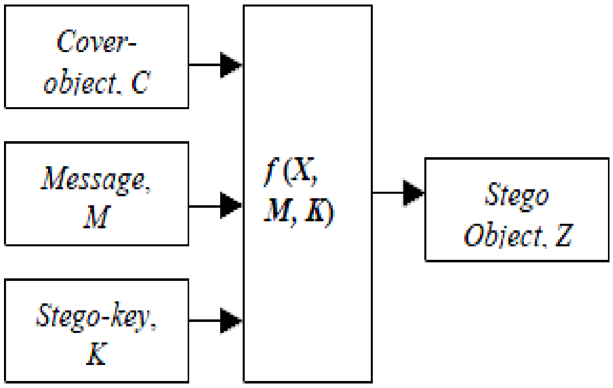
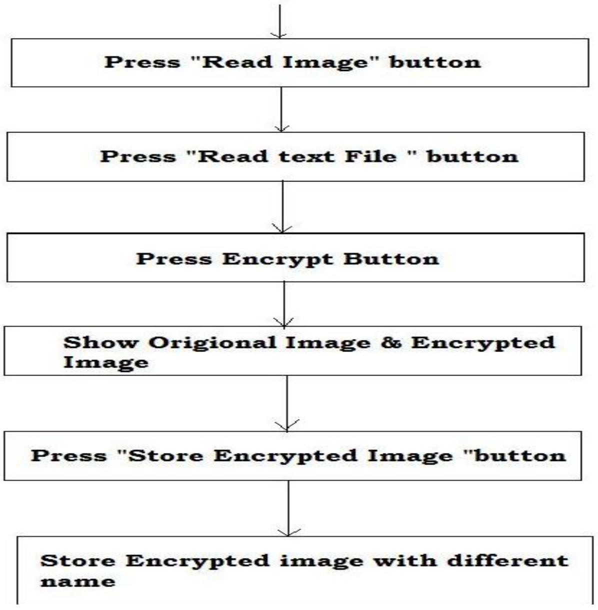


Figure 2 Basic Steganography Model

B. Encryption

For hiding missile navigation data in digital image following encryption algorithm is used.

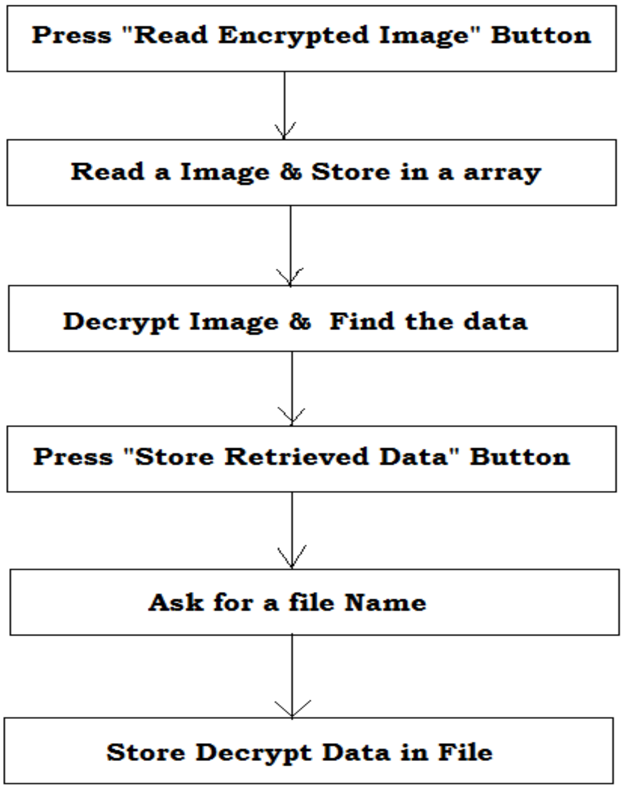
Encryption Phase


Press "Read Image" button
Press "Read text File " button
Press Encrypt Button
Show Origional Image & Encrypted Image
Press "Store Encrypted Image "button
Store Encrypted image with different name

C . Decryption

To read information from stego-image the decryption algorithm is used.

Decryption Phase


Press "Read Encrypted Image" Button
Read a Image & Store in a array
Decrypt Image & Find the data
Press "Store Retrieved Data" Button
Ask for a file Name
Store Decrypt Data in File

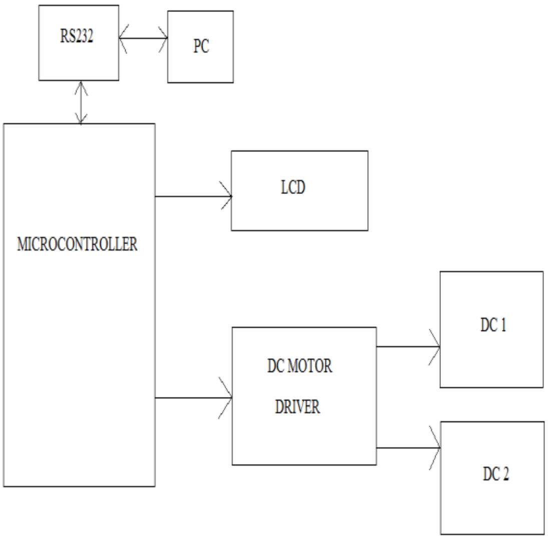


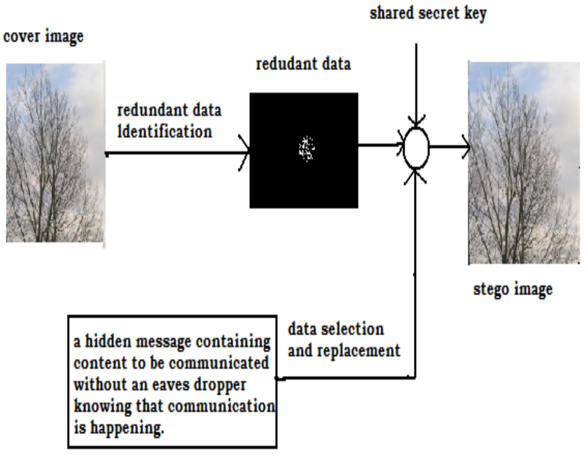
Figure 3 Actual Block diagram of the proposed system

D . Key Based Steganography:

The key plays a very important role in embedding the message. Larger the key size, is more difficult to access [1].

Following keys type is used in Steganography are as follows:

1. Pure Steganography
2. Public key Steganography
3. Private key Steganography



a hidden message containing content to be communicated without an eaves dropper knowing that communication is happening.

Figure 4 block diagram of private key steganography

V. RESULTS

In order to demonstrate the online transmission of the hidden data, 4 result is obtained

Result 1

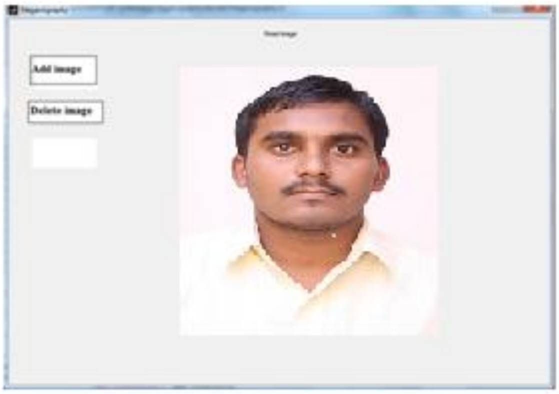


Figure 5. Module to create, delete & modify the Image

Result 2

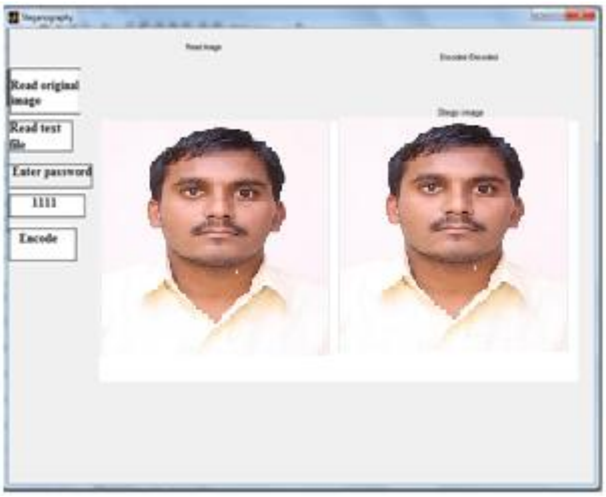


Figure 6. Module to embed the secret message in image

Result 3

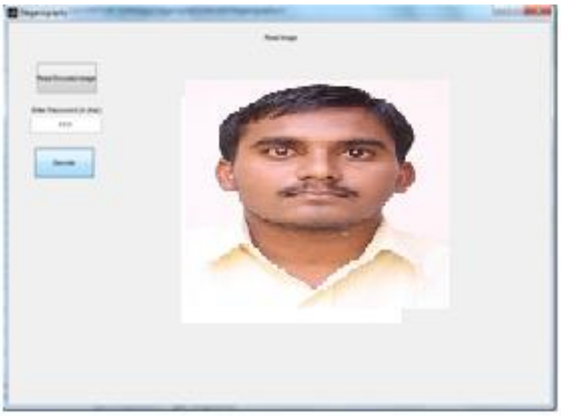
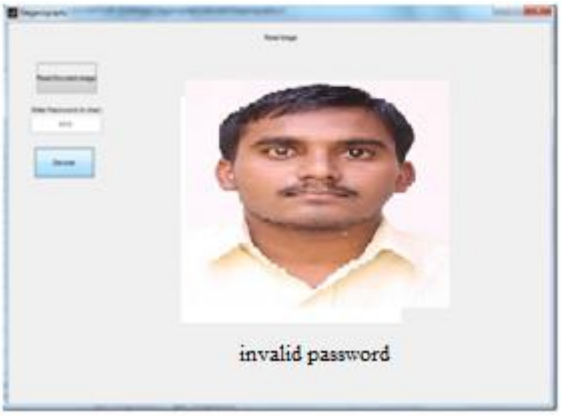


Figure 7 . Module to decode the secret information from

digital image

Result 4



invalid password

Figure 8 Model for detecting or inserting wrong Password

VI. CONCLUSION

Steganography can be used for hidden communication. Pointed out the enhancement of the image steganographic system using LSB approach to provide a means of secure communication. A stego-key is applied to the system during embedment of the message into the cover-image. In proposed approach, the message bits are embedded randomly into the cover-image pixels instead of sequentially. Finally, steganography that uses a key has a better security than non-key steganography. The way this technology is growing exponentially the bounds for steganography seems limitless.

REFERENCES

[1] C. Cachin, “An Information-Theoretic Model for Steganography”, in *proceeding 2nd Information Hiding Workshop*, vol. 1525, pp. 306-318, 1998.

[2] D. Artz, “Digital Steganography: Hiding Data within Data”, *IEEE Internet Computing*, pp. 75-80, May-Jun 2001.

[3] E.T. Lin and E.J. Delp, "A Review of Data Hiding in Digital Images," *in Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference*, PICS '99, Ed., Apr. 1999, pp. 274--278.

[4] Shashikala Channalli et al /International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141

[5] Mohammad Shirali-Shahreza , “A new method for real time steganography”, *ICSP 2006 Proceedings of IEEE* .

[6] Yuk Ying Chung, fang Fei Xu , “Development of video watermarking for MPEG2 video” *City university of Hong Kong ,IEEE 2006.*

[7] C. Lu, J. Chen and K. Fan, "Real-time Frame-Dependent Video Watermarking in VLC Domain", *Signal Processing : Image Communication 20,2005, pp. 624–642.*