Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 3, March -2016

STEGANOGRAPHY TECHNIQUE USED FOR MILITARY APPLICATION

Mrs.Deepali Yewale(Asst.proff)[1], Ms. Abhaya Badambe[2], Ms.Yogita Bagal[3], Ms.Poonam Khade[4]

[1-4]*Entc,aissm's ioit pune*

Abstract - *The aim of the "Steganography Information Hiding in Digital Images" is safe communication. The important of transmission is problem now days. There are different methods existing for hiding information in different cover media. To avoid illegal access of missile navigation data the technique of steganography is most excellent suitable. To launch or navigate missile a system contain so many important data and this data is saved from illegal access use steganography techniques. In this paper we designed this system for armed forces application. In this approach the Least Significant Bit (LSB) technique is used to secrete messages in an image. To apply steganography techniques any kind of wrap files can be used such as Image, sound or video files.*

Keywords-*Least Significant Bit, Missile, Navigation, Steganography, Zigbee*

I. INTRODUCTION

Transmission of data is from one place to another is biggest challenges in communication. Various methods are helpful for providing protection. One of the best methods is the steganography. Steganography is technique of hiding messages in other files for transmission in a approach that an viewer could not identify the occurrence of transmission, is in advance popularity in recent trade demands. It includes various techniques for covert communications. [6] Thus Steganography refers skill of unseen communication. The rising possibilities of modern communications need the special security on computer network system. The network security is becoming more significant because the number of data being exchanged on the Internet increases. Therefore, the essential data are requires to guard against illegal access and use. [5]The rapid growth of publishing and broadcasting technology also require an another solution in hiding information digitally. The copyright such as audio, video and other resource available in digital form may lead to illegal copying. In Steganography digital formats make possible to provide high image quality even under multi-copying file. The special part of unseen information is inserted in every image that could not be easily extracted without exact technique and saving image quality simultaneously. The word steanogarphy is a Greek word means "stegos " means"Cover" and "grafia" means "writing" defining it as "covered writing"[1].

II. METHODOLOGY

Following methods are present to hide information in digital images:

1] Least significant bit insertion
2] Masking and filtering
3] Algorithms and transformations

Here"least significant bit insertion" method is used
For example: 11111111 is an 8-bit binary number. In this the rightmost bit is called as LSB. To change LSB it has the smallest amount 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 every pixel in the image file. **[**2**]**

III.TYPES OF STEGANOGRAPHY

A. Text Steganography

Previously to hide information using text steganography the most important method of steganography. This method is helpful to hide a secret message in each nth letter of every word of a text message

.

B. *Audio/Video Steganography*

To hide information in audio files comparable techniques are used as for image files. One special technique is used in audio steganography called masking; it is helpful to exploits the properties of the human ear to hide information unnoticeably. In audio/video steganography is fewer accepted than image steganography. Audio/video files are large so it is complex to use.

C. Image Steganography

Images steganography is the majority accepted cover objects used for steganography. Many different image file formats contains in digital images; most of them are useful for definite applications. Different steganographic algorithms exist for these different image file formats

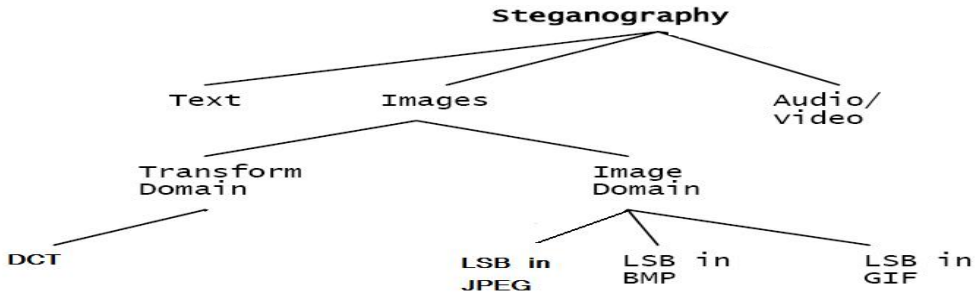


Fig1. Algorithm & Types

IV.PROBLEM STATEMENT

Steganography is a message hiding technique so that a user can send or communicate to the other user about their secret message securely. LSB is one of the most accepted method which is used for hiding the secret message. LSB hiding method works as it hides the secret message straight in the least two significant bits in the image pixels, which affects the image resolution, due to this it reduces the image quality and make the image easy to hit. Therefore there may be one possibility to remove this problem and make the secret message more secure and develop the quality of the image is proposed. The proposed method hides the secret message based on searching about the identical values between the secret messages and image pixels. By using this proposed method the image will remain same after encoding or hiding the secret message in the image. It will not affect the image resolution.

V.PROPOSED METHOD

The fundamental model of steganography contains following block Carrier, Message and Password. Carrier is also known as cover-object which embeds the message and which is used to serves and to hide its presence.

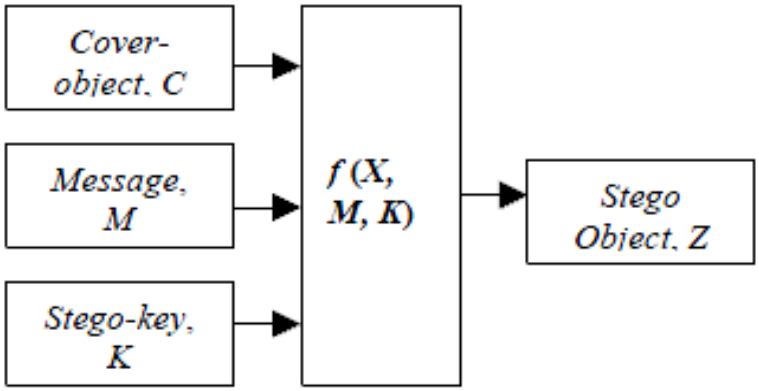


Fig. 2 fundamental Steganography Model

In general, the information hiding process extracts unneeded bits from cover-object. This process consists of two steps :

i. Identification of unneeded bits in a cover object. Unneeded bits are those bits that can be modified without mortifying the quality or destroying the integrity of the cover-object**.**
ii. Embedding process. It selects the subset of the unneeded bits to be replaced with data from a secret message. The stego-object is created by replacing the selected unneeded bits with message bit

A.Encoder side:

To offer superior security the secret information is encrypted first and encrypted ASCII value is transformed in binary form.

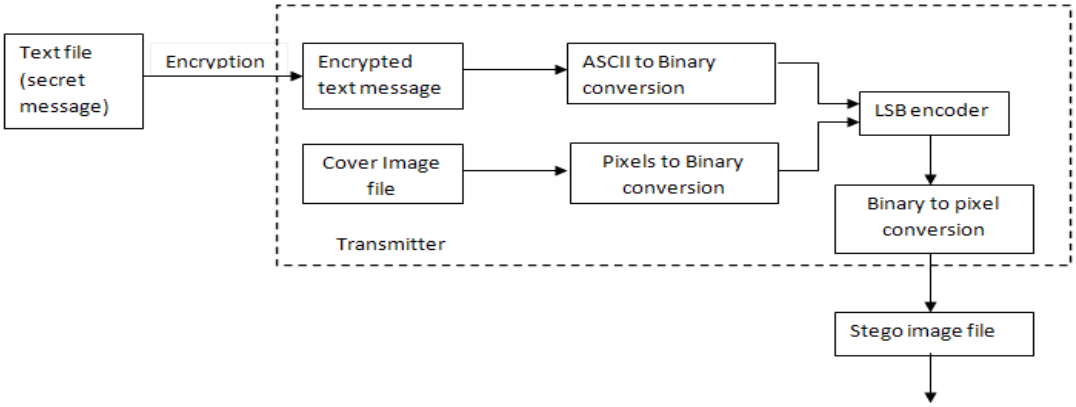


Fig 3. Proposed steganography system for encoder

The image pixels at the similar time are also converted into binary form. The image is now used as a wrap to embed the encrypted information. This method is done by LSB sender which replaces the least significant bit of pixel values with the encrypted information bits. The customized picture is now termed as Stego image.

B.Decoder Side:

Upon response of Stego image the receiver firstly converts the pixels into their corresponding binary values. LSB decoder then detaches the encrypted data from image pixel values. The encrypted data is decrypted with decryption algorithms. This is how, the pure text is improved from image.

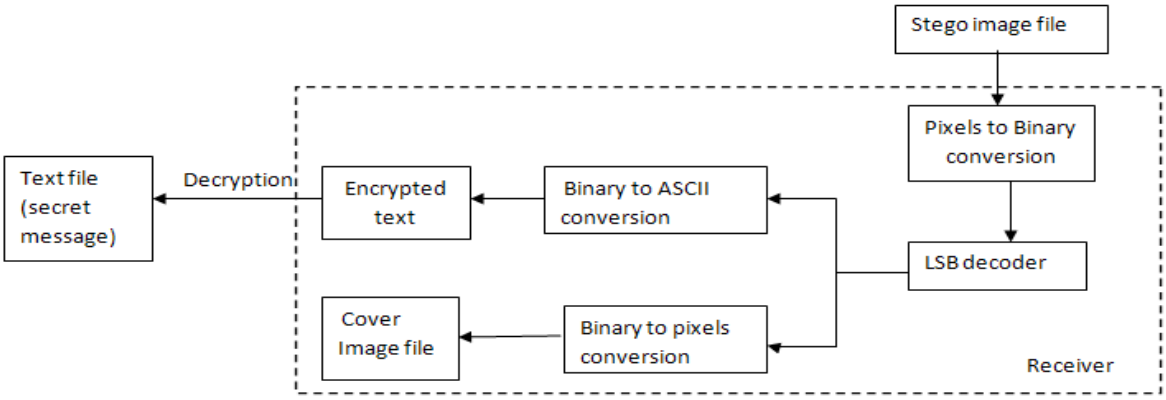
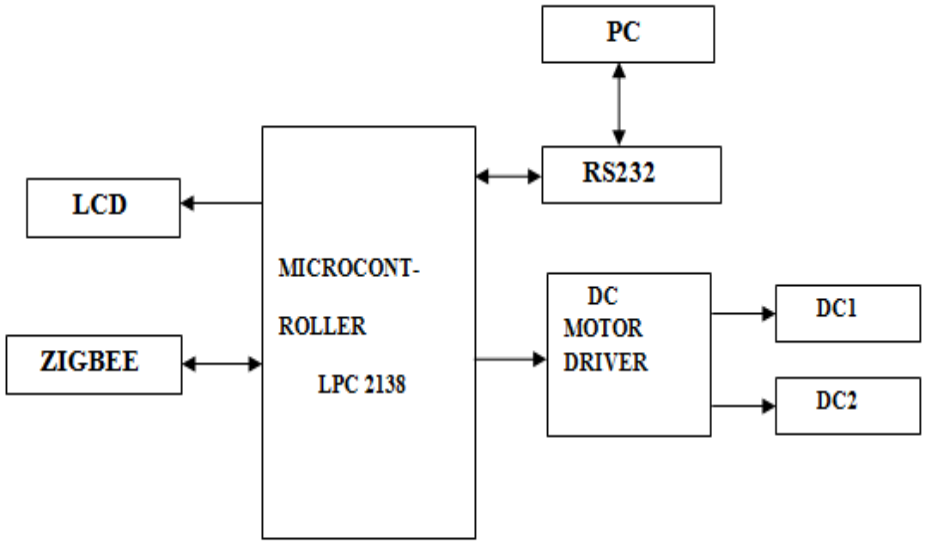


Fig 4. Proposed steganography system for decoder

VI. BLOCK DIGRAM AND PRINCIPLE



A. MICROCONTROLLER LPC 2138

The LPC2131/32/34/36/38 microcontrollers are based on a 16/32-bit ARM7TDMI-S CPU with real-time emulation and embedded trace support, that combine the micro controller with 32 kB, 64 kB, 128 kB, 256 kB and 512 kB of embedded high-speed flash memory. A128-bit broad memory interface and a matchless accelerator architecture allow 32-bit code execution at maximum clock rate. For significant code size applications, thealternative16-bitThumb mode reduces code by greater than 30 % with minimal performance penalty. With a broad range of serial communications interfaces and on-chip SRAM options of 8 kB, 16 kB, and 32 kB, they are very well suited for communication gateways.

B. RS 232

RS 232 IC is a driver IC to translate the µC TTL logic(0-5) to the RS 232 logic (+-9v).Many device today work on RS 232 logic such as PC, GSM modem , GPS etc.so in arrange to communicate with such devices we have to bring the logic levels to the 232 logic (+/-9v). Here as we can see the RS 232 chips have 2 pairs of TTL and 232 logic viz, Pair 1: Pin 7, 8,9,10 of RS 232 Pair 2: pin 11,12,13,14 of RS 232 We can use any one pair in our project. If we require 2 serial ports then Depending on the necessity of the project we may have to use both the pair in the same project. The µC works on TTL logic (0-5 v).So to convert the TTL logic to 232 logic we use the 4 capacitors connected to the RS232 IC. These capacitors are called charge pumps used to convert the TTL voltage to the +/- 9 v swing required by the 232 IC.

C. DC MOTOR

DC motors are used to physically drive the application as per the requirement provided in software. The dc motor works on 12v. To drive a dc motor, we need a dc motor driver called L293D. This dc motor driver is capable of driving 2 dc motors at a time. In order to protect the dc motor from a back EMF generated by the dc motor while changing the direction of rotation, the dc motor driver have an internal protection suit. We can also provide the back EMF protection suit by connecting 4 diode configurations across each dc motor. Here in our project we are using a 12v DC motor which is Bipolar, which means that the DC motor can rotate both the sides .For this we are using a DC motor driver IC L293D. This driver IC can drive 2 DC motor. In our project we are connecting only 1 DC motor so we are connecting only the 1st pair of the DC motor (in1 and in2 of L293D).The DC motor will be connected at OUT1 and OUT2 of L293D respectively.

D. LCD

Lampex,16*2, Backlit facility,100mamp consumption.

E.RC4 ALGORITHM

The RC4 encryption algorithm was developed by Ronald Rivets of RSA. The RC4 algorithm is used identically for encryption and decryption as the data stream is simply XORed with the generated key sequence. The algorithm is serial as it requires successive exchanges of state entries based on the key sequence. Hence implementations can be very computationally intensive. This algorithm has been released to the public and is implemented by many programmers. This encryption algorithm is used by standards such as IEEE 802.11 within WEP (Wireless Encryption Protocol) using a 40 and 128-bit keys. Published procedures exist for cracking the security measures as implemented in WEP.

VIII.RESULT

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

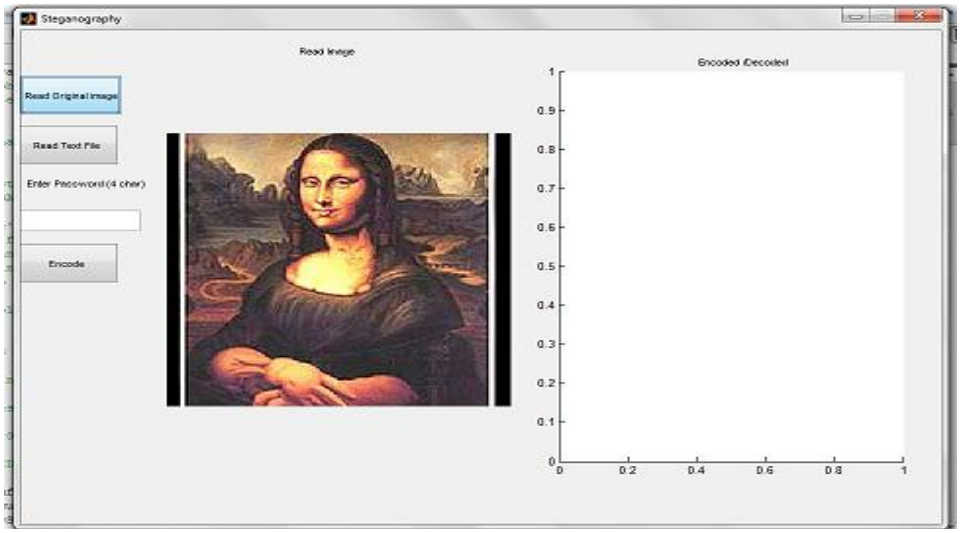


Fig.5 Module to create, delete & modify the Image

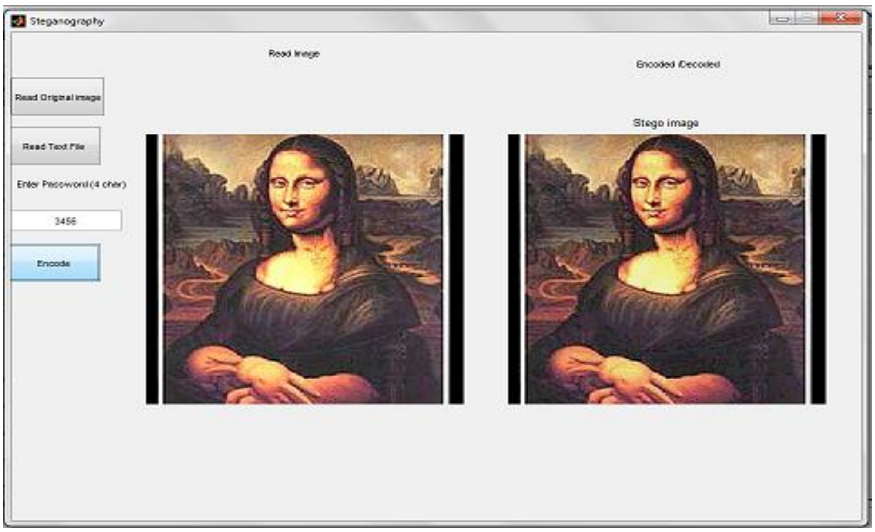


Fig.6 Module to embed the secret message in image

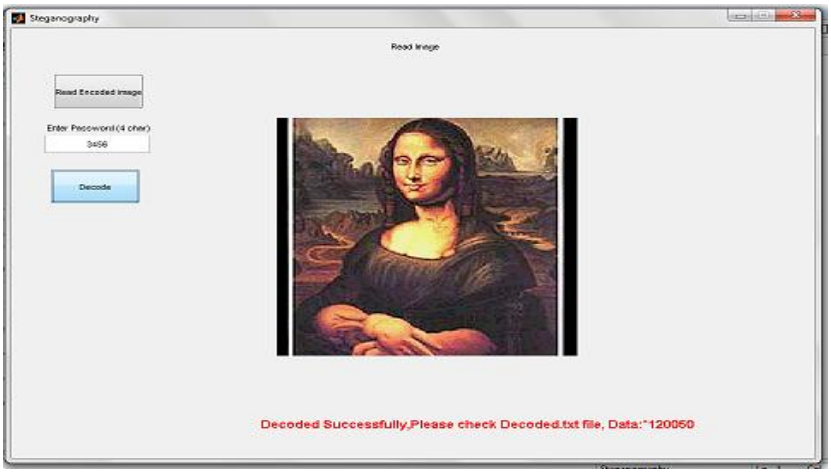


Fig.7 Model for detecting or inserting wrong Password

REFERENCES

[1]. M. M Amin, M. Salleh, *S* . Ibrahim, M.R.K atmin and M.Z.I. Shamsuddin -"Information Hiding using Steganography" 2003.

[2]. Shailender Gupta ,Ankur Goyal ,Bharat Bhushan - "Information Hiding Using Least Significant Bit Steganography and Cryptography" I.J.Modern Education and Computer Science, 2012.

[3]. Gaurav Gupta, Harsh Kapil, V. H. Patil – **"**Radar based Missile Navigation" International Journal of Innovative Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-2 Issue-11, October 2014.

[4]. Pawar Ashwini , Pawar Bhagyashree, Rajguru Ashwini, Prof.Y.R.Nagargoje, Prof.M.A.Khan – "Image And Audio Based Secure Encryption And Decryption" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 3, March 2014.

[5]. Maura Conway "Code Wars:Steganography, Signals Intelligence, and Terrorism" Knowledge, Technology and Policy (Special issue entitled 'Technology and Terrorism') Vol. 16, No. 2 (Summer 2003).

[6]. Arvind Kumar Km. Pooja "Steganography- A Data Hiding Technique" International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010

