INFORMATION HIDING USING STEGANOGRAPHY SYSTEM APPROACH

DRAKSHAVENI.G
Master of Computer Applications.
BMS Institute of Technology
Bangalore, India.
drakshaveni.mtech@gmail.com

SHARATH M.N
Master of Computer Applications
BMS Institute of Technology
Bangalore, India.
sharathmn1989@gmail.com

***Abstract*—Steganography is the science of invisible communication over an innocuous cover media. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to detect that there is a second secret message present. The concept in this paper is encrypting the original files into their respective binary files and modifying their least significant Bit insertion with the information to be hidden. Any plain text, Cipher text, Other images or anything that can be embedded in a Bit stream can be hidden in an image .The file after being affected by the LSB Algorithm looks and behaves the same as it would have behaved previous. The receiver knows how to decrypt and get the original information. Therefore, our proposed scheme is suitable for real time applications.**

Keywords-
InformationHiding,Steganography,JPEGImages,GIFImages,Cryptography,Least Significant Bit(LSB).

I. INTRODUCTION

Steganography is a technique of hiding information in digital media such as audio, video & text content.The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to detect that there is a second secret message present.

Steganography is derived from Greek literally means "covered writing ". It includes a vast array of secret communications methods that conceal the message's very existence .

The basic model of steganography consists of Carrier, Message& password. Carrier is also known as cover-object, which the messages is embedded & serve to hide the existence of the message.

These methods include invisible inks , microdots , character arrangement, digital signatures, covert channels , and spread spectrum communications.

The word Stegano means covered or Secret&graphy means writing or drawing therefore steganography means covered writing.

II. PURPOSE OF CRYPTOGRAPHY ALGORITHM

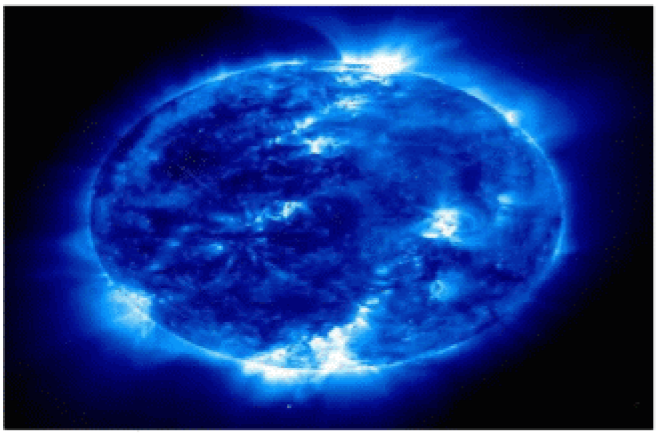
1. Data Encryption is a fundamental technique for protecting confidentiality of data.
2. It is also known as message passing & uses thecommon Technology.
3. Hence it forms basis of many protection andSecurity mechanism.
4. It uses the large expensive computing powerwhich Required for cracking.
5. "Encryption" is application of an algorithmic transformation to data".

III. PURPOSE OF LEAST SIGNIFICANT BIT INSERTION

1. Least significant bit (LSB) insertion is acommon , simple approach to embedding information in a cover file.
2. Unfortunately, it is vulnerable to even a slightimage manipulation.
3. Converting an image from a format like GIF or BMP, which reconstructs the original message exactly (loss less compression) to a JPEG , which does not (compression with loss), and then return back.
4. It could destroy the Information Hidden in the LSB.

JPEG IMAGE (COMPRESSION WITH LOSS)

GIF IMAGE (LOSS LESS COMPRESSION)



IV. IMPLEMENTING LSB

Steganography software processes LSB insertion to make the hidden information less detectable .

For example, the EzStego tool arranges the palette to reduce the occurrence of adjacent index colors that contrast too much - before it inserts the message. This approach works quite well in grayscaleimages and may work well in images with related colors.

S-Tools, another steganography, take a different approach by closely approximating the cover image, which may mean radical palette changes .

As with 24- bit images, changing the pixels LSB may create new colors . (New colors may not be added to an 8-bit image due to the palette limit) Instead, S-Tools reduce the number of colors while maintaining the imagequality ,so that the LSB changes do not drastically change color values .
To hide an image in the LSB s of each byte of a 24 -bit image, you can store 3 bits in each pixel.
If you compress the message to be hidden before you embed it, you can hide a large amount of information.

V. V. IMPLEMENTING CRYPTOGRAPHY

Generally we refer to the original form of the data as the plain text form and the transformed as the encrypted or the cipher text form.
Applying a standard encryption algorithm. E with a specific encryption key K chosen by the user or application program performs encryption.
The cipher text has to be decrypted using a decrypted algorithm D with the same key to obtain its plaintext form .

VI. FEATURES

- It allows us to embed the messages or files in encrypted form using **32 bit DES**.
- The message or file could be retrieved (or decrypted) from a Master file only after specifying the correct password which was used at the time of encryption.
- It allows embedding messages and files in compressed form using ZIP compression format. Gives you a choice of compression level to be used.
- It uses the technology still being developed for certain formats.

VII. WORKING OF PROJECT

1. A Cover-Object which may contain the images should be encoded with the existing System.
2. Once the Images is encoded then the messages should be encoded or encrypted with the existing System.
3. AStegoKeywhich may contains the password to encrypt the messages in the cover-object.
4. AStegoObject must be generated which is created by replacing the selected redundant bits with the message bits.

VIII. EXAMPLE FOR PRODUCING STEGO-IMAGE PROCESS

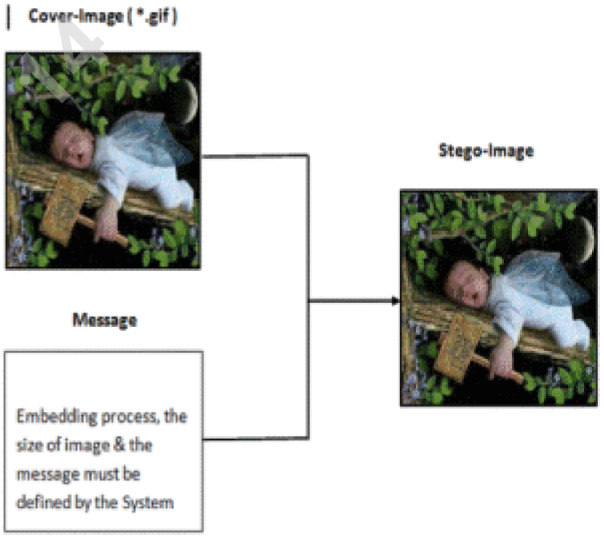


Fig 1 - Basic Architecture of Steganography

1. The Cover-image which is usually in the GIF Format (Graphical Interchange Format).
2. The Cover-Image usually combines with the particularmessage.
3. This will both the Cover-Images & the message combines to produce the output called as StegoImage.
4. TheStegoImage which is almost identical to the particular Cover-image.

5. However there are Hidden messages in the StegoImage that are imperceptible (difficult to perceive by the mind or impossible).

IX. ALGORITHM DEVELOPMENT

Algorithm:Embedding& Retrieving Data.

Input: Select the file which is to be embedded.

Output: Retrieve the File which is embedded.

Method:

1) The User must select the file.
2) The file can be Text, Image, Videofile or Audio file.
3) The Selected File should be embedded.
4) The embedded File should be revealed or decrypted as a output File by the user.

X. ALGORITHM DESCRIPTION

In this algorithm following criteria should be satisfied.

- The user must choose appropriate File which is need to be embedded.
- The embedded File should show the compression level of that particular file,& the file should be revealed or decrypted by the particular user.

XI. CONCLUSION

In this paper we have created algorithm that hides any information, be it text or privacy.
The encryption included as an enhancement to text hiding enhances the reliability of this tool.

ACKNOLEDGEMENT

We wish to thank for all friends for helping in providing the information.

REFERENCE

[1] A.Kerckhoffs, —La CryptographieMilitaire, Journal des Sciences Militaires, 9th series, IX pp 5–38; Feb. pp 161–191, Jan. 1883.

[2] R. J. Anderson, and F.A. Petitcolas, — On the limits of Steganography,l J. Selected Areas in Comm., vol.16, no. 4, pp. 474–481, 1998.

[3] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon " Image Steganography: Concepts and Practice," WSPC/Lecture Notes Seriesm, April 22, 2004.

[4] Wikipedia, the free Encyclopedia.

[5] "Cryptography & Network Security"

[6] Principles & Practices by "William Stallings".