Data Hiding Using Image Steganography

V.Pragadeesh Dharsha[1], Nalawade Vineet Sanjay[2]

Computer Science, Vellore Institute of Technology,

Vellore, Tamil Nadu, India

pragadeeshdharsha@gmail.com

vineetn23@gmail.com

Abstract *-- The purpose of this project is to make software through which we can perform basic image operations on the desired images and also can encrypt messages or for the purpose of keeping messages secret, numerous distinct methods of encrypting and decryping have been created. Such methods include, but do not limit to, steganography and cryptography. Steganography allows the message to be encrypted, whereas cryptography allows the message to be secured. These methods are mainly used by Government officials to transfer the information to others. In this the information is stored inside the image. The user can find the original message after decrypting it with the decrypting code. This program was completely written with the help of python. Both encryption and decryption are included.*

Keywords: *Steganography, LSB bit, Stego image*

I. Introduction

Since the rise of internet, regarding communication and information technology. Securing the information and privacy of the data is critically important. Cryptography was the most widely used technique to secretly send confidential information [3]. It is not important to keep the content of the message confidential, but it is also important to keep your actual messages existence unknown to others. In response to this importance, steganography was developed.

Steganography is the art of invisible communication. Germans developed the Microdot technique during the World War II [4]. Therefore, normal cover messages were able to be sent through and insecure Channel containing such periods [5]. In today's age, steganography is frequently utilized by computers where the networks are the high-speed delivery channel and he digital data are the carriers. Steganography and Cryptography have many differences. The main difference between them is cryptography is used to keep the information secured and secret. Whereas Steganography's purpose is to keep the message's existence a secret. Steganography and cryptography, on the other hand, also share some similarities as they are both methods used to protect data. Strength of Steganography is defeated when the intruder finds out that the image is an Stego object. When combined with cryptography, the strength increases substantially.

a) ***Types of Steganography***

Almost all digital files can be used for steganography, but the format with high redundancy bits are more suitable for steganography.

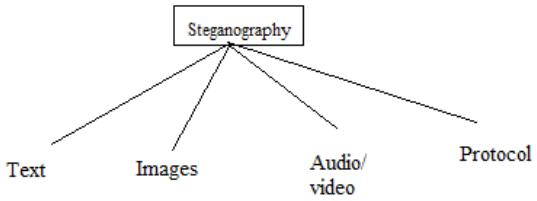


Fig1: Categories of steganography

In all the above mentioned types the data can be hidden without any change in the actual stego object. When the data is embedded inside an image or a video or an audio, the listener will not be able to find any difference between the actual object and the stego object. In image steganography, complete data is hidden inside the image within the pixels. There are different methods for embedding data into the image.

Table 1: Types of Image steganography

Steganography Techniques	Cover Media	Embedding Techniques	Advantages
Image Hiding	Image		
1.LSB(Least Significant Bit)		This method is used the least significant bit of every pixel in one image to hide the most significant bit of another	Simplest & easiest way of hiding information
2.DCT (Discrete Cosine Transform)		Embeds the information by altering the transformed DCT co-efficient	Hide data can be distributed more evenly over the whole image in such a way to make it robust
3.DWT (Discrete Wavelet transform)		This technique work by talking many wavelet to encode a whole image	Coefficient of wavelet are altered with the noise within tolerable level

Image Steganography Features:

1) Transparency: The quality of the original image should not be affected after using steganoraphy.

2) Robustness: Simple image processing systems which includes contrast or enhancement brightness gamma correction, allows steganography to be removed both intentionally and unintentionally. Therefore, steganography should be robust against numerous attacks of a similar nature. [5] [11].

3) Data payload or capacity: For a Steganography to accurately detect during extraction, a specific amount of data should be embedded [8] [7].

II. Literature Survey

Authors compare of stego image regarding the cover image using several image quality parameters; such as Peak Signal to Noise Ratio (PSNR), Structure Similarity (SSIM), Feature Similarity Index Measure (FSIM) and Mean Square Error (MSE) [13]. The secret allows the information to be hidden on different LSB bits of image. This technique uses RGB true color images for embedding process [14]. Data is first encrypted, then embedded within the image through use of steganography techniques [13]. An improved version of Image Steganography, through use of status bits, results in efficient filtering techniques [10]. For higher stego image quality, pixel adjustment technique is used which results in high hidden capacity [12]. The Huffman tree can also be used for image steganography. It is hard for the attacker to extract the data as the Huffman table reduces the cover image size [9]. The secret information is embedded inside the cover image after the least significant bit is randomly selected [10].

III. Proposed Work

The encrypted data can be any normal data you wish to encrypt into suitable code. Before sending it to the person, hide it using the code. The user is allowed to use only alphabets without numbers and special characters so that if any intrudere decrypts it without the keyword the output will be different.

a) Requirement of Hiding data

Our goal is to send and receive encrypted messages embedded within images through a simple application. The user can select the image he/she prefers, then the program will understand if this image will suit the text. Pixel deformation or size distortion will not be allowed.

The purpose of this project is to make software through which we can perform basic image operations on the desired images and also can encrypt messages or hide the messages for the purpose of security [1][3]. Through steganography we are encrypting the messages. Cryptography, on the other hand, is used for acquiring communication secrecy. Many different methods have been developed to encrypt and decrypt data to secure the secrecy of messages.

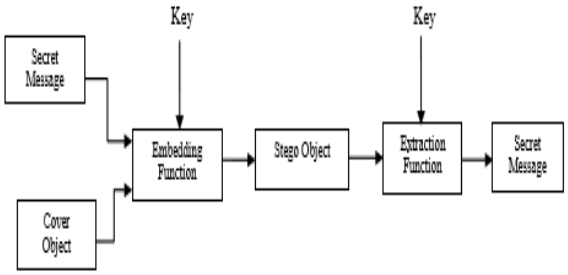


Fig 2: A model of steganographic process

b) Algorithm

Encryption:

i. Check whether the picture is in the proper format(PNG) according to the program.

ii. Get the data from the user and convert it into binary stream of data.
iii. Use for loops to extract each pixel value and convert it into binary.
iv. Now compare each bit of data and the last bit of 'B' value in binary must be taken.
v. Replace the last bit of each pixel with each bit of data.
vi. Run the for loop until the complete stream of data is stored inside the image
vii. Save the image in a separate name. and send the number of words as the key.

Decryption:

i. Run for loops with a range of the sent keyword.
ii. Start extracting each pixel and extract the last bit of the tuple.
iii. Separate the stored stream of bits with the delimiter as space.
iv. Use the functions of python to convert the binary data into original data.

The key plays a vital role in decrypting the data. The larger the key the harder it becomes for the intruder to decrypt the data.

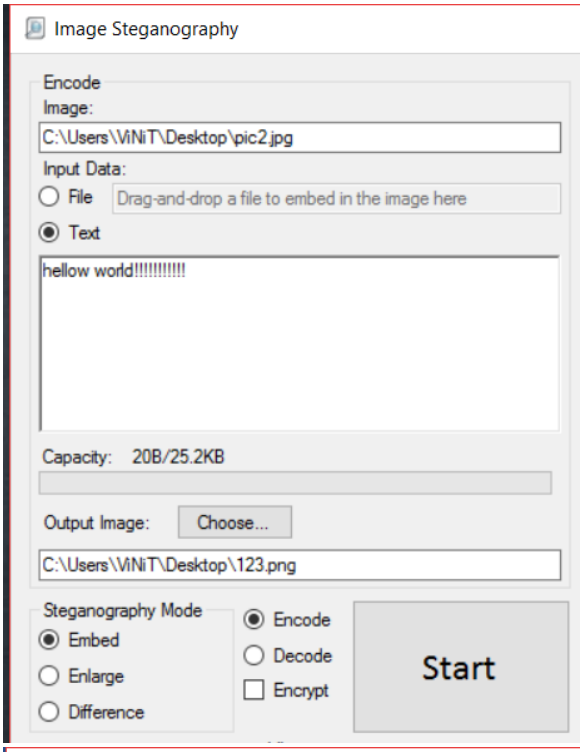
c) Performance Measures

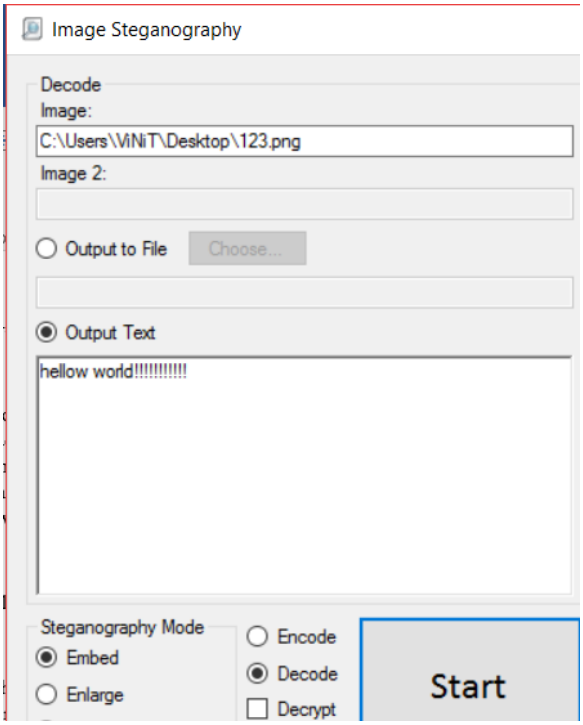
i. The information hidden inside the image should not change after the encryption.
ii. The changes in the image should not be visible to the naked eye.
iii. Exact data must be extracted.

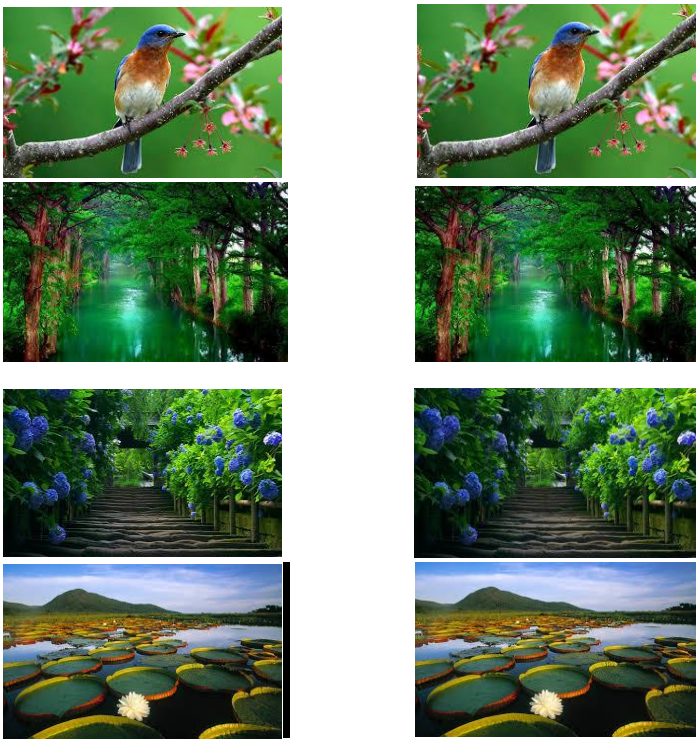
IV. Result and discussion

We have seen the proper algorithm for the encryption and decryption of the image. In this o special characters can be used which is an advantage for the user, because even though if intruder manages to get the image the decryption of the image will result in a combination of alphanumeric characters with special characters, which is meaningless.

The image will also ask for the key for decryption, which can be sent separately. If proper key is not provided the data inside the image will automatically be damaged. The hiding of data was properly executed. It is user wish to generate a key for the protection.







Original image Stego image

V. Conclusion:

As Steganography are used widely to hide the secret information, the attacks to retrieve the information is also increasing rapidly. The method of evaluating the technique is mostly based on the following conditions:

The quality of the image or the steganography object should not be change upon adding excess data.

The data will be damaged if the key is improper.

The secrete data should survive attacks by the intruders.

In this only alphabets can be used. This helps us to keep the data secured more because when the image is stolen, the code for decryption will yield a result with special characters and numbers. This will not be the actual information. The actual information can be extracted only with proper conditions on the decrypting code

VI. References

[1]. Kesslet, Gary C. *An Overview of Steganography for the Computer Forensics Examiner*, Burlington, 2004.

[2]. Lin, Eugene and Edward Delp*: A Review of Data Hiding In Digital Images*, West Lafayette, 1999.

[3]. Hosmer, Chet. *Discovering Hidden Evidence*, Cortland, 2006.

[4]. Fridrich, J., R. Du, M. Long: Steganalysis Of LSB Encoding In Color Images, Binghamton, 2007.

[5]. Vehse, Heymo. YAVI: *Yet Another Vigenere Algorithm* www.leafraker.com/yavi

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

[7]. Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert *Parlett, "Steganography and digital watermarking"* School of Computer Science, The University of Birmingham. 2003. www.cs.unibo.it/people/phdstudents/scacciag/home_files/teach/datahide.pdf.

[8] Ravi shah , Abhinav Agraval & subramaniam Ganesham*, "Frequency domain real time digital image watermarking "* Oakland university.

[9] A. Nag, J.P. Singh, S. Biswas, D. Sarkar, and P.P. Sarkar*, "A Huffman Code Based Image Steganography Technique",* 1st International Conference on Applied Algorithm (ICAA) Jan. *2014, pp. 257-265.*

[10] *"Image Steganography Least Significant Bit with Multiple Progressions"*Savita Goel.

[11] *"A New Approach for LSB Based Image Steganography using Secret Key*". S. M. M. Karim,

[12] D. Debnath, S. Deb, N. Kar, *"An Advanced Image Encryption Standard Providing Dual Security: Encryption Using Hill Cipher and RGB Image Steganography"*, IEEE International Conference on Computational Intelligence and Networks (CINE), Jan. 2015, pp. 178-183.

[13] D. Debnath, S. Deb, N. Kar, *"An Advanced Image Encryption Standard Providing Dual Security: Encryption Using Hill Cipher and RGB Image Steganography"*, IEEE International Conference on Computational Intelligence and Networks (CINE), Jan. 2015, pp. 178-183.

[14] H. Yang, X. Sun and G. Sun*, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution",* Journal of Radio Engineering, Vol. 18, No. 4, pp. 509-516, 2009.