Image steganography for criminal cases

Divya Suryawanshi [1], Meetali Salvi[2], Soumya Pandey[3z]
Terna Engineering College, Nerul, Navi Mumbai
IT Department, Mumbai University

***Abstract* - Crime scene investigators document everything they collect at a crime scene, keeping detailed records of what they found and in what position they found it. Maintaining documents secrecy is very important aspect otherwise forgery could happen. To help maintain data privacy and security, we can make use of image steganography. The algorithm implemented in this system is used to embed data inside an image using the steganography technique. The original data can also be retrieved from the image using the same approach. Hiding data inside an image is a practical way of hiding secret information from intruders. Image processing can then be used to get the data back from the image. The scope of the project is implementation of steganography tools for hiding sensitive information.**

***Key Words* - Steganography technique, PSNR value, image processing, information retrieval, stegoimage, encryption/decryption.**

I. INTRODUCTION

"Image Steganography for Criminal Cases" system can be used to hide data inside an image, and send it securely. The term information hiding can refer to either making the information undetectable or keeping the existence of the information secret. Steganography is an area of information hiding which mean "secret or covered writing". Steganography is used to communicate secret data using image as a carrier. The main objective is to conceal the existence of data or information to protect it from getting attacked

In this system, we have two layers of security which provide data security as well as data privacy. Data security means protecting sensitive data from breaches, theft or any other malicious activity by unauthorised users. Sensitive data is always at risk of getting in the wrong hands. This system is capable of hiding data inside the image such that attackers will not be aware of the existence of sensitive data.

The major intent is to prevent the detection of the hidden information. Image steganography system is a stand-alone application that combines steganography and encryption to enhance the confidentiality of intended message. Unlike encryption, which secures the content of a message, steganography hides the message's existence. The main advantage of using steganography algorithm is its simple security mechanism. Because the steganography message is integrated invisibly and covered inside other harmless sources, it is very difficult to detect the message without knowing its existence and the appropriate encoding scheme.

This system will secure the files by applying the algorithm. The algorithm will hide the data inside the image and along with a secret key which will be used for encryption and decryption. Only authorized people will have the access to particular file.

II. LITERATURE WORK

Steganography was in practice since ancient times. The earlier steganography techniques included shaving the head of a person to write the message and waiting for the hair to grow back so that the person can be used as a carrier without raising any suspicion.

Another technique used was making use of 'invisible ink' to write under or in between the blank parts of messages.

During World War II, agents used photographically produced microdots to send information back and forth. Microdots were typically minute (less than the size of the period produced by a typewriter). World War II microdots were embedded in the paper and covered with an adhesive, such as collodion. This was reflective, and thus detectable by viewing against glancing light.

Modern steganography entered the world with the advent of personal computers. Steganography in today's time can be used for almost all digital file formats like text, image, audio, video.

Image steganography the information is hidden exclusively in images. It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. [4]

Steganography in images are classified into two categories: Spatial-domain based Steganography and the Transform domain based Steganography.

There are several steganography techniques used for hiding data such as batch steganography, permutation steganography, least significant bits (LSB), bit-plane complexity segmentation (BPCS) and chaos based spread spectrum image steganography (CSSIS). [4]

We are going to implement concept introduced by El-Emam . A bitmap (bmp) image will be used to hide the data. Data will be embedded inside the image using the pixels. Then the pixels of stego image can then be accessed back in order to retrieve back the hidden data inside the image. Two stages are involved. The first stage is to come up with a new steganography algorithm in order to hide the data inside the image and the second stage is to come up with a decryption algorithm using data retrieving method in order to retrieve the hidden data that is hided within the stego-image.[1]

III. METHODOLOGY

Our proposed algorithm uses two layers of security to maintain the privacy, confidentiality and accuracy of the data. Following Figure shows the framework for the overall process of the system. The system is able to hide the data inside the image as well as retrieve the data from the image.

From Figure 1, for hiding the data, a username and password is required prior to using the system. Once the user has logged into the system, the user can use the information (data) together with the secret key to hide the data inside a chosen image. Using a new steganography algorithm, the data will be embedded and hidden inside the image with almost zero distortion of the original image.

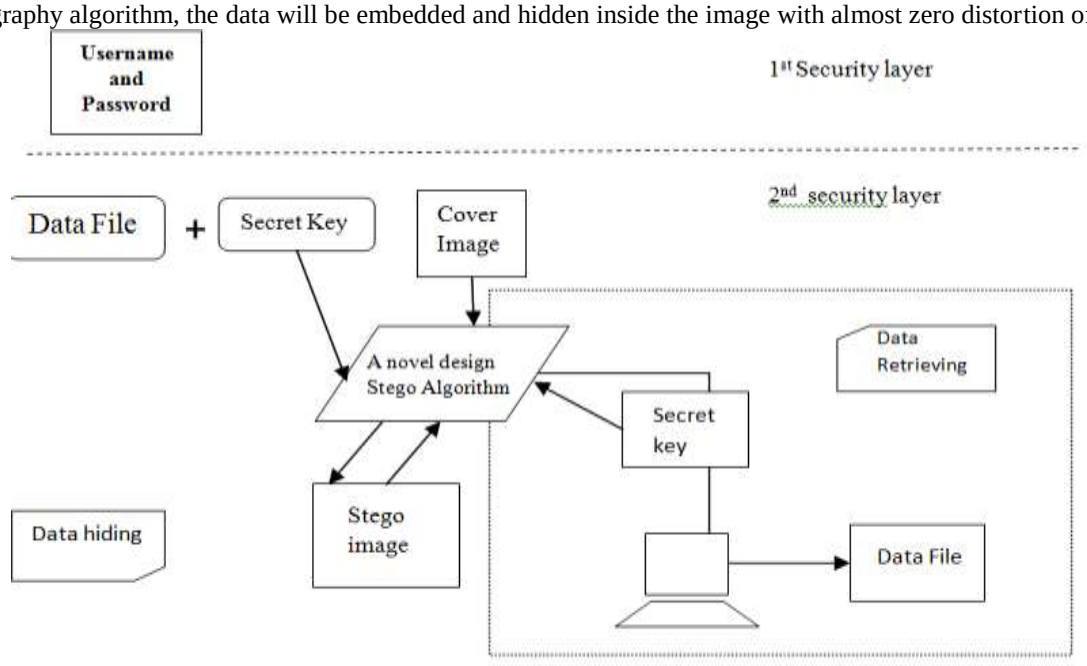

Fig. Architecture of application

Fig.1

For retrieving the data, a secret key is required to retrieving back the data that have been embedded inside the image. Without the secret key, the data cannot be retrieved from the image. This is to ensure the integrity and confidentiality of the data. For the steganography algorithm, Fig. 2 shows the algorithm for embedding the secret message/file inside the image. During the process of embedding the message inside the image, a secret key is needed for the purpose of retrieving the message back from the image.

The proposed steganography algorithm consists of two image embedding techniques which are data hiding method and data retrieving method. The original secret message will not be directly embedded inside image, message will be encrypted using algorithm. It will provide more secrecy. Data hiding method is used to hide the encrypted message in cover image by using an auto generated key while data retrieving method is used to retrieve and the hidden encrypted message from stego-image, secret message decrypted using same key which was used while encrypting message. Hence, data or in particular a secret message, is protected in image without revealing to unauthorized party.

The secret key in this proposed steganography algorithm is playing an essential role where the key is acts as a locker that used to lock or unlock the secret message. The key will be automatically generated by system. To Generate key the Rijndael Algorithm is used .Rijndael is the block cipher algorithm recently chosen by the National Institute of Science and Technology (NIST) as the Advanced Encryption Standard (AES). It supersedes the Data Encryption Standard (DES). Inside the image encrypted message will be hidden so that message cannot be retrieved without key. Once the encrypted message is hidden inside the image, this message can be extracted back from the stego-image. Fig. 3 shows the algorithm for extracting the secret message from the stego-image. In order to retrieve a correct message from the image, a secret key is needed for the purpose of verification.

```
Begin
Input:Cover_Image, Secret_Message;
Genrate Secret_Key;
Encrypt message;
Embed encrypted message inside image;
Output: Stego-Image;
End
```

fig 2 Algorithm for embedding data inside image

Begin
Input: Stego-Image, Secret_Key;
Compare Secret-Key;
Retrieve Message from image;
Decrypt Message;
Output: Secret Message;
End

fig 3 Algorithm for extracting data from stego-image

The new stego-image can then be used by user to send it via internet or email to other parties without revealing the secret data inside the image. If the other parties want to reveal the secret data hidden inside the image, the new stego-image file can then be upload again using the system to retrieve the data that have been embedded inside the image using the secret key.
To check the quality of the image PSNR (Peak signal-to noise ratio) algorithm used.

IV. IMPLEMENTATION

Following are the snaps of implemented system:

Fig 4 Main Interface

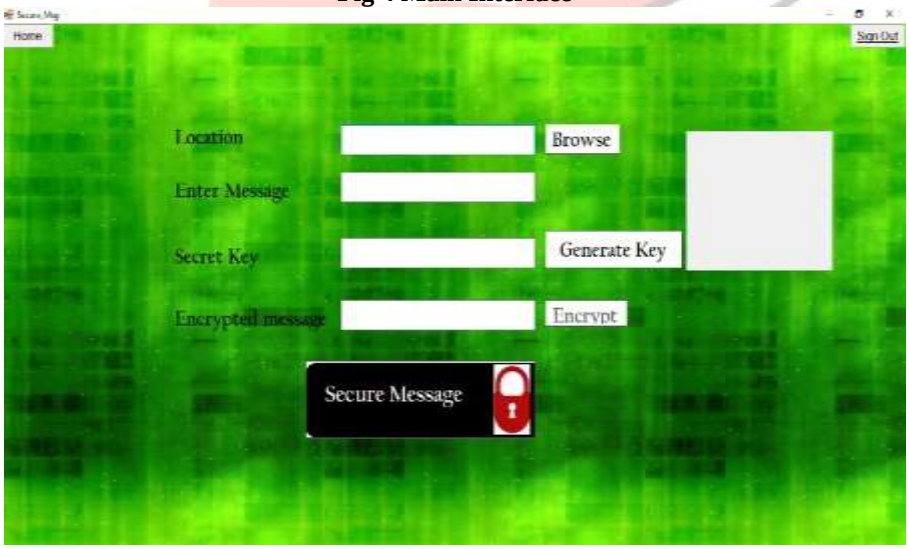

Fig 5 Secure Message Module

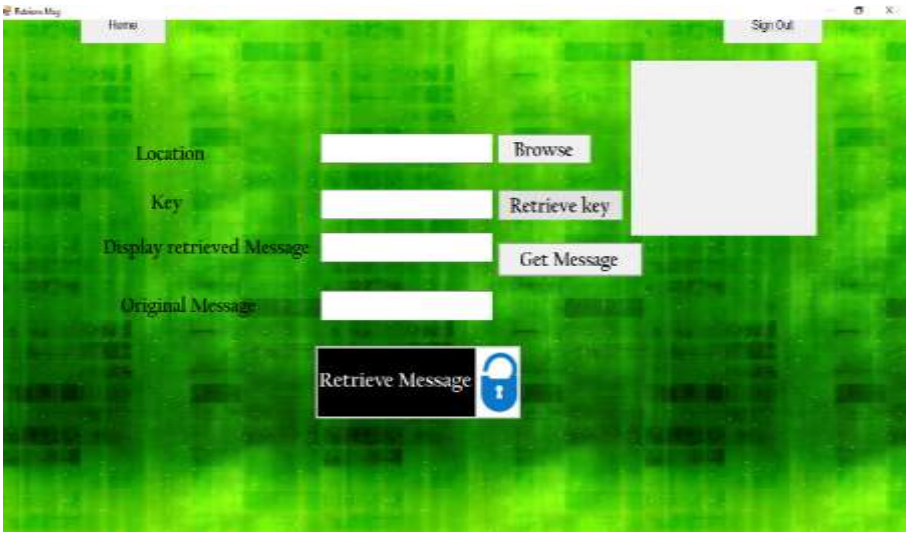

Fig 6 Retrieve Message Module

V. PSNR

To ensure the quality of image we will test the algorithm using the PSNR (Peak signal-to noise ratio). PSNR is a standard measurement used in steganography technique in order to test the quality of the stego-images. The higher the value of PSNR, the better the quality of the stego-image. For standard quality images, the PSNR value must be higher than 50.

PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs. The signal in this case is the original data, and the noise is the error introduced by compression.

If the cover image is C of size M x M and the stego-image is S of size N x N, then each cover image C and stego-image S will have pixel value (x, y) from 0 to M-1 and 0 to N-1 respectively

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right)$$

Here R is the possible pixel value. PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image, but between-image comparisons of PSNR are meaningless.

VI. Conclusion

This paper discusses a system named ISCC (Image Steganography for Criminal Cases). ISCC has been developed using the steganography algorithm discussed in [III]. It can be used by police staffs who want to hide the data inside an image without revealing the data to other parties. PRIS maintains privacy, confidentiality and accuracy of the data. "ISCC" also helps to maintain data privacy, security and confidentiality.

With the proposed algorithm, we found that the stego-image does not have a noticeable distortion in it (as seen by the naked eyes). We also tested the images using PSNR value and found that the PSNR value is higher than 50. Hence this proposed steganography algorithm is very efficient to hide the data inside the image.

VII. REFERENCES

[1] Rosziati Ibrahim and Teoh Suk Kuan (2011).PRIS:Image Processing Tool for Dealing with Criminal Cases using Steganography Technique, IEEE/978-1-4577-1539/11 ,pp193-198

[2] ParmarAjit Kumar Maganbhai, Prof. Krishna Chouhan (2015), A Study and literature Review on Image Steganography, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1), 2015, 685-688

[3] N. N. El-Emam, hiding a large amount of data with high security using steganography algorithm, Journal of Computer Science 3 (2007) 223-232.

[4] Rosziati Ibrahim and Teoh Suk Kuan, (2011). Steganography Algorithm to Hide Secret Message inside an Image, Journal of Computer Technology and Application, USA, Volume 2, No. 2, February 2011, pp102-108, (ISSN1934-7340).