Images Stenography through Hiding Single and Multiple Data using Different Steganographic Tools

Preeti Chauhan[1], Prof. Yatin Agarwal[2]
[1]M.Tech. Scholar, [2]Professor
[12]Department of CSE, Greater Noida Institute Of Technology (GNIOT)
Greater Noida, Uttar Pradesh, India

I. INTRODUCTION

A. OVERVIEW

Recently, the concept of 'Image Steganography' is became an important issue in the computer security world. Image steganography simply means hide some secret data into an object. The object can be a text, an image or a sound, but the most popular cover object used for hidden secret message is images.

On the other hand, to detect these hidden messages, many methods and techniques can be used as well. However, the procedures of detecting any hidden data, is called 'Steganalysis'.

This paper focuses on creating stego-images through hiding secret messages into clean images. It also reviews some image steganography methods and tools. In order to create a number of stego-images, three steganographic tools are used. They are: OpenStego, S-Tools and F5 algorithm. With respect to the hidden data, one and more hidden data file is embedded. In addition, testing for differentiating between stego-images created and the clean one is presented.

Since the beginning of web, the security of data is the important parameter in IT and internet communication. Numerous systems like cryptographic techniques, watermarking and hiding strategies were created with a specific end goal to secure the data amid communication. Sadly it was insufficient to secure the substance of the hidden message from outside phishers and programmers.

There was a need of another method which can hold the presence of the hidden message mystery. The system used to actualize this is called as Steganography.Steganography can be characterized as a workmanship or art of invisible writing, which enabled hiding of secret data into another media. The term Steganography is gotten from the ancient Greek words "Stegos" meaning "cover" and "Grafia" meaning "written work" signifying it as "invisible writing". Consequently steganography is a novel procedure which is utilized to shroud the hidden message and keep it from identification. Going to the historical backdrop of Steganography, the Greek antiquarian Herodotus writes in his scholarly work "Histories" about an aristocrat, Histaeus, who needed to correspond with his child in law in Greece. To speak subtly with his child in law, he neatly shaves a trusted slave's hair and tattooed the hidden message on the scalp. Following couple of months when the hair grew on his scalp the slave was made to travel to Greece to carry the mystery message on his scalp as proof many such secret communication existed from ancient period but these were time consuming process. With advances in the technology and trends a new approach to enable secret data communication is developed called steganography. The proposed technique enable embedding of multiple secret image into single cover image using ANN in spatial domain along with AES encryption to enhance security level.

B. IMAGE STEGANOGRAPHY METHODS

In recent years, the number of steganography software that has been issued publicly around the Internet has reached more than 200 presently (Ming et al., 2006). The methods and carrier types tend to diversify. This section will give an overview of steganography tools: classifications and features. According to Ming et al.(2006), based on the analyses of steganography methods', they partition these methods into five categories as the following:

a) Spatial domain based steganography;
b) Transform domain based steganography.
c) Document based steganography.

II. RELATED WORKS

A. Literature Review

Steganography is an important research issues in computer security field **(Johnson and Jajodia, 1998; Provos and Honeyman, 2003).** Steganography is the science of communicating secret data in an appropriate cover object. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing", defining it as "covered writing" (Johnson and Jajodia, 1998).

Steganography and cryptography are having the same goal, which is securing messages. However, they are not the same. Cryptography scrambles a message so it cannot be readable. Steganography hides the message so it cannot be seen **(Hmood et al., 2010).**

There are four types of the cover objects, which are image, text, audio and video. According to these different covering objects; there are many types of steganography, such as image

steganography, steganography in txt files .etc. **(Johnson and Jajodia, 1998; Al-Ani et al, 2010).**

Different types of image steganography methods and tools are briefly presented in this paper. Also, some steganographic methods are used to create verities of stego-images. Then testing and analysing them.

The most popular cover object used for hidden secret message is images for many reasons. Images are widespread on the internet; also they can be used as carrier objects without raising much suspicion. In addition, image files have a lot of capacity for modification without noticeable damage to the content (**Duric 2004).**

In terms of digital images, different image file formats exist and most of them are used for specific application. However, JPEG and GIF are the most dominant. Different steganographic algorithms exist for these different image file formats (**Morke et al., 2005).**

On the other hand, compression plays a very important role in the choice of steganographic algorithm. Lossy compression techniques give smaller image file sizes, but due to the fact that excess image data will be removed the possibility that the embedded message might be partly lost is increased.

Although lossless compression does not produce such a small file size, it keeps the original digital image intact without the chance of losing any of the hidden information **(Morke et al., 2005).**

This paper is focusing on creating stego-images using OpenStego, S-Tools and F5 algorithm. In addition, the differences between a clean image and its stego versions are tested through comparing the entropy values.

In **N. S. Raghava et.al's [1]** has effectively proposed a new algorithm using LSB based image stegnaography in which secret data is hidden in last four bits of cover image and encrypted using henon chaotic map this encryption generates a pseudo random numbers which enhances the security as same random numbers cannot be generated by any third party without the knowledge of random generator function hence its difficult for attackers to retrieve data. Results reveal that high security is provided with acceptable PSNR values

In **Arjun R. Nichal et.al [2]** demonstrated a performance analysis on LSB technique by embedding the secret image bits in various pixels of cover image and corresponding PSNR values are noted down. Results emphasize that PSNR value gradually decrease with increase in the embedding bits.

In **Marghny H. Mohamed et.al's [3]** proposed steganography approach which aims to increase the embedding capacity along with stego image quality by using an optimal LSBs method, on the basis of it optimal pixels are decided which are best suitable for embedding secret data. Methodology proposed is based on dividing the image into two parts, one for embedding the secret message and applies change to the value of some bits that have the secret bits obtained by the simple form of LSB substitution technique. The other part is used to indicate which change is applied to each pixel exist in the first part. The advantages of the presented method is increasing the amount of secret message in each pixel of the cover image and improving the quality of the stego image.

In **A. E.Mustafa et.al's [4]** demonstrated a spatial domain technique of hiding secret image bits in lsb-2 bits of the cover image in order to increase the robustness of technique. This technique helps to embed the secret data with minimum distortion to the cover file, By using this algorithm it is used for construction of blind steganalysis and accurate targeted method for various forms of images. Experiment analysis of new method shows PSNR is greater than other LSBs replacement.

In **Siddharth Singh et.al's [5]** proposed a robust steganography approach using DCT, chaotic sequence generator and Arnold transform, here the random sequence generator is used for hiding data in middle band DCT coefficient of cover image is generated using chaotic system. Security factor is improved by using Arnold transform to scramble hidden data before hiding. Experimental analysis demonstrate algorithm achieve more secure, robust to JPEG compression, LPF filtering and various crop attacks then various other approaches using DCT domain.

III. MATERIALS AND METHODS

A cascaded feed forward neural network along with it Levenberg Marquardt training algorithm is used for the proposed steganography approach. Cascade-forward networks are similar to feed-forward networks, consist of a series of layers. The first layer has a connection from the network input. Each subsequent layer has a connection from the previous layer. The final layer produces the network's output, but includes a connection from the input and every previous layer to following layers. While two-layer feed forward networks can potentially learn virtually any input output relationship, feed-forward networks with more layers might learn complex relationships more quickly. The function newcf creates cascade-forward networks. For example, a three layer network has connections from layer 1 to layer 2, layer 2 to layer 3, and layer 1 to layer 3. The three-layer network also has connections from the input to all three layers. The additional connections might improve the speed at which the network learns the desired relationship

Here the cover image pixels are given as input to cascaded feed forward network and trained using LMA algorithm and the shuffled positions of the cover image pixels are obtained in which the secret data bits are hidden in it.

A. PROPOSED METHODOLOGY

To get a well balance between invisibility and hiding capacity, the suggested system exploits adaptive LSB substitution and human visual system features to develop a lossless data hiding system for color images. This system works in spatial-domain with the help of some information extracted from transform domain to choose the image's locations that will be used for embedding.

The contribution of this paper is to develop a system for hiding information in true color images that tries to overcome the obstacles facing the previous techniques. The idea is that changing in the salient image pixels in specific image's color channels will not perceptually degrade the image.

The robustness of the created system is realized by employing LSB substitution technique in various color channels and different least significant bits to increase hidden data capacity, whereas security is achieved by adapting a wavelet filter parameterization technique. Furthermore, this system requires no knowledge of the original image for the recovery of the secret image, yet yields high signal-to-noise ratios for the recovered output.

This comes from our observation that different subbands of frequency domain coefficients give significant information about where salient and non-salient pixels of image reside.

The most important differences that distinguish the proposed system from existing state-of-the-art approaches are: (1) it works at a true color image and embedding process can be carried out in

multi-color channel, thus increasing the hiding capacity; (2) more secure- it can battle a range of attacks (tamper resistance) by exploiting the concept of parametric wavelet filter; (3) the computational complexity is reduced because of working at spatial domain instead of transform domain, which is very complex, takes more time and makes more changes in the cover image; (4) the ability to support low invisible degradation because of utilizing color space mapping technique; (5) adaptive- the system takes statistical global features of the image before attempting to interact with its LSB pixels. The system is driven by separate functions: adaptive excerption of the place to conceal; adaptive excerption of number of bits per pixel to conceal.

At first color conversion is applied on the input image through HSV color space. Secondly cover

image is converted to transform domain. This is attained by applying parameterized DWT on cover image leading to four subbands. Then payload locations are determined depending on wavelet based salient points coefficients. Finally secret data embedding is performed in image pixels directly by locating those pixels corresponding to salient subbands' coefficients. The systematic block diagram of the proposed scheme is shown in Fig.1 and the following subsections briefly outline each step.

B. Embedding Steps

a. Convert into HSV color space:

Change RGB color image into HSV color space. The HSV model separates out the luminance component (Intensity) of a pixel color from its chrominance components (Hue and Saturation). This representation is more similar to the human perception of color through eye cells [13]. In computer vision anyone often wants to separate color components from intensity for many reasons, such as robustness to lighting changes, or removing shadows. HSV is often used simply because code for conversion between RGB and HSV is commonly available and can be executed easily. In this research and through experiments, the proposed system can determine the best color channels that can be used in the process of concealment, and that do not result in any deformation regarding cover image visibility and quality of secret image after extraction.

b. Apply wavelet filter parameterization:

Robustness of data hiding technique can be enhanced if properties of the cover image could be exploited. Taking this facet into consideration, working in transform domain becomes more attractive. The use of wavelet in image steganographic model lies in the fact that the wavelet transform clearly splits the high frequency information (LH, HL, HH subbands) that hold the edges and textures of the image in different directions and low frequency information (LL subbands) that comprises the supreme energy of the image on a pixel by pixel basis[11].

c. Extraction Steps

By doing the same sequences of steps required to determine the embedding locations, the secret image will be extracted. As shown in Fig.1 the received stego image, which may be attacked is firstly converted to HSV color space and then the predefined color channel is transformed into wavelet coefficients by one-level parametric integer lifting wavelet transform with a suggested secret-key $\propto$, in embedding process, to deal with the correct location of the secret message. Then, the three high frequency vertical, horizontal, and diagonal subbands are set to zero. Perform the inverse wavelet transform and obtain the reference image. As in embedding process, the computed difference between the color channel's image and its reference image is utilized to achieve blindness of the proposed system. According to the sequence of embedding locations, the hidden data is gained by the LSB extraction process.

C. PROPOSED ALGORITHM

a. Data embedding

The procedure for embedding of secret data is shown in figure 3.1

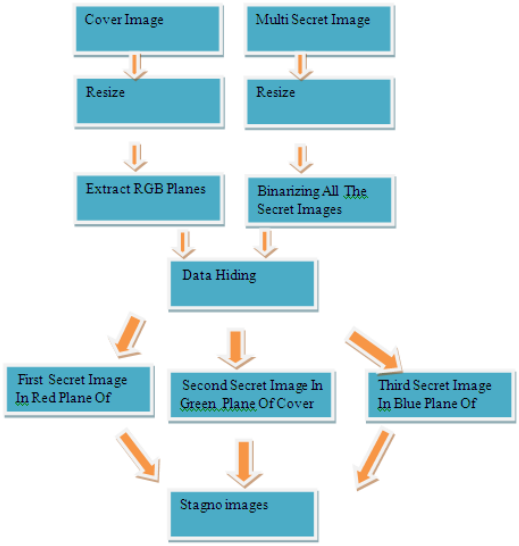

Fig.1: Data embedding

Step1: The input cover image and secret images are resized
Step2:- The secret images are binarize image.
Step3:- The encrypted secret images are binarized such that each pixel contains 8 bit binary value
Step4:-The binarized first secret image bits are hidden in the Last bit positions of red plane of cover image
Step5: Further the second and third secret images are hidden in of blue and green of the cover image
Step6:- The obtained image after embedding the secret images is called as stego image

b. Data retrieval

The stego image is obtained after embedding the secret images into cover image RGB planes, the
obtained stego image is conveyed to the receiver side, At reception side the reverse operations are performed to extract the secret .

CHAPTER 4

IV. SIMULATION RESULTS AND DISCUSSION

The MATLAB tool 7.10.0.499 (R2013a) is utilized to implement and analyse the proposed algorithm due to its advances in image processing tool boxes and inbuilt function. The parameters used are RGB cover images of size 512X512 jpg and png formats the three RGB secret images of size 64x64.bmp format. For the illustration only four cover images and secret images are given Figure 4.1

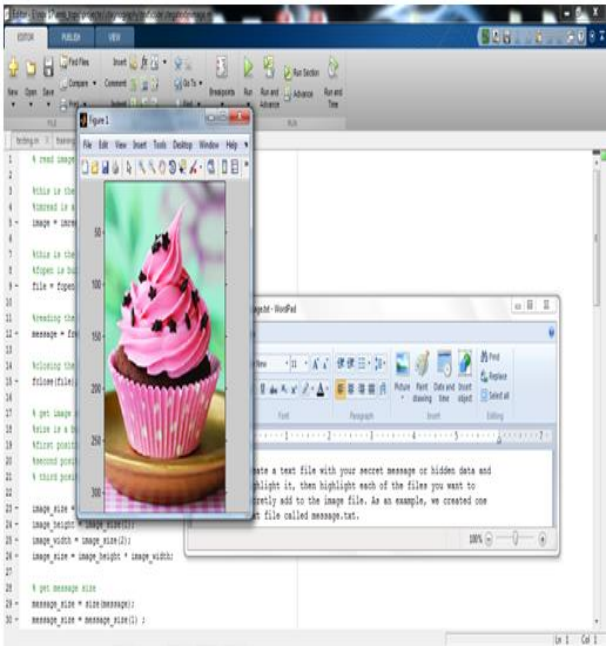

Fig.2: Data Hide in Image

In this image we select a image file and we are using a test file for hide . arfter runing code text file will hide in image.

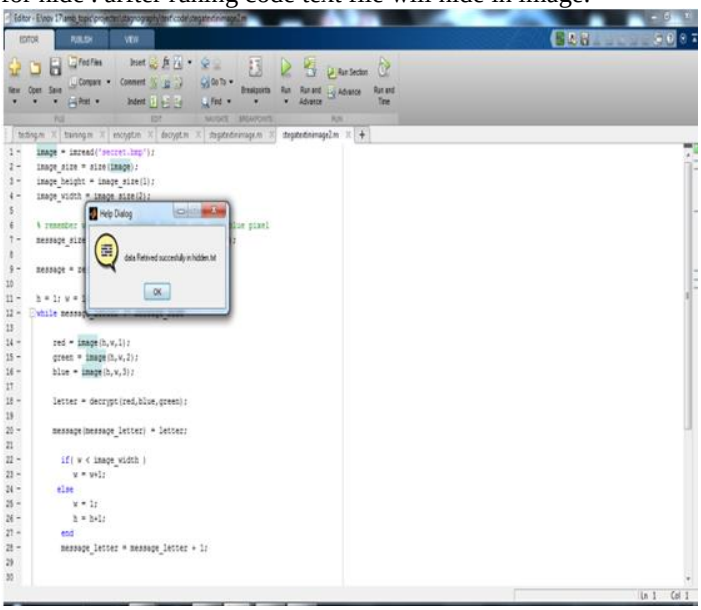

Fig.3: Text File

In this image we select image name and after extraction we will get text file .

Multi Image Hide In Single Image.

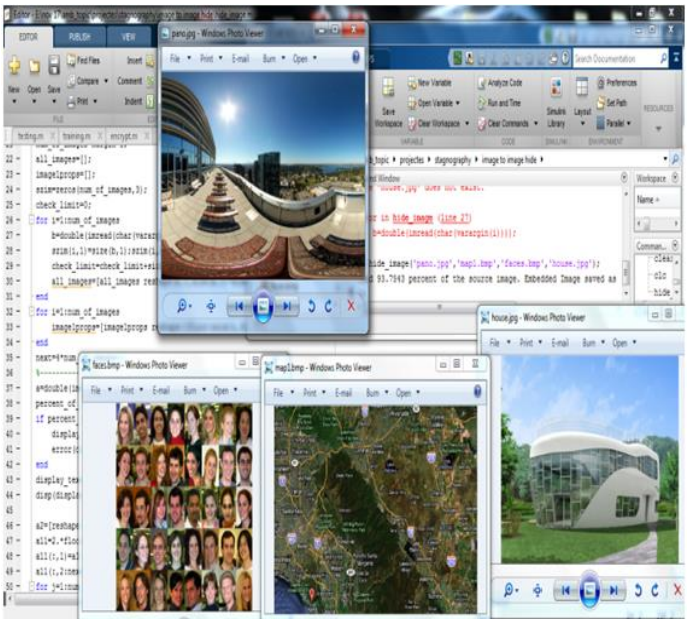

Fig.4: Multi Image Hide In Single Image

In this Fig 4.3 we chose a image and we are selecting three images for hind in single images. arter runing code all images will hide in a single imges.

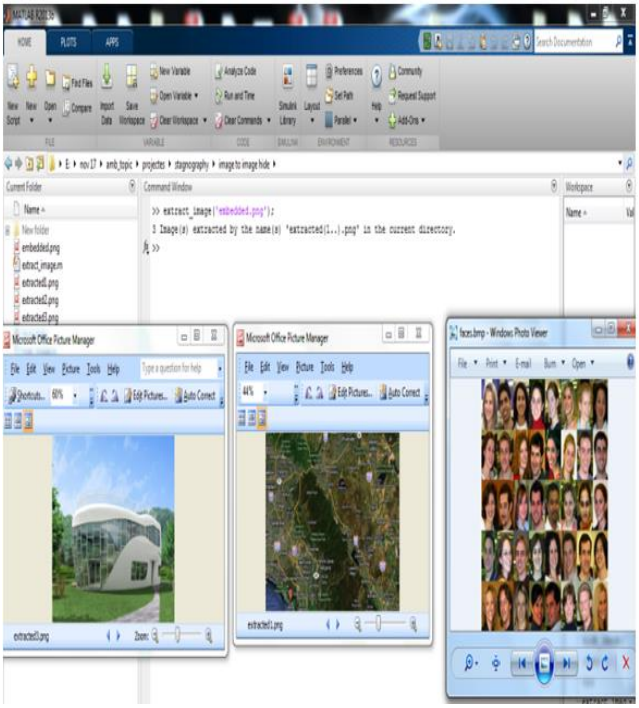

Fig.5: Final Output

After select embedded image extract code we will get all three images

V. CONCLUSION

In this thesis a secure steganographic algorithm is proposed to embedd multiple secret image into a single cover image and obtained a high quality stego image with enhanced security level by including cryptography along with stegoangraphy. The quality of the stego image obtained is ensured in terms of, high PSNR Security of the approach is ensured by using AES method for secret image encryption before embedding into cover image. This approach can be develpoed further for improving the embedding capacity level while maintaning the high quality of stego image.

In this thesis, an efficient steganographic system for embedding secret messages into true color image without producing any major change has been proposed. To increase the system performance in terms of both capacity and security; the method of optimal LSB substitution is presented in combination with parameterization based lifting wavelet transform. The proposed system allows complete recovery of the original host image with small visual distortion in stegoimages because of consideration of human perceptual factor that is inherited from HSV color space of image. In addition, the system is able to extract the secret message without the cover image.

Extensive experiments show advantages of our lossless color image data hiding system for providing good image quality and large message capacity as well as increasing in the system immunity to specific range of attacks. The proposed system is very practical for most image files that are stored and transmitted in the PNG and BMP format. In the future, we intended to extend our system to hide gray scale and color images as secret message and to increase the system ability to deal with geometric and processing attacks.

Based on the research that has been done, it can be concluded that:

1. Method LSB insertion process by replacing the last bit or the far right with bits secret message text.
2. The quality of the digital image is changing after inserted message; this is evidenced by the color histogram analysis of test results to the original digital image to image insertion results in Figure 4.3 and 4.4. Changes in quality depending on the size of the size of the message is inserted. While the size of digital image also changed after the insertion process the message.

Suggestions:

The applications still have disadvantage, then there are some suggestions that may be useful for further development, among others:

1. This application using LSB method, further research recommended to use another method than the LSB or LSB method. It can also combined with steganographic methods, such as Algorithms and Transformation, Redundant Pattern

Encoding, Spread Spectrum method. So it can be a study that measures the quality of each of these methods.

2. To increase the security of message insertion, it is suggested to develop these programs with encryption algorithm that has a security level above the Advance Encryption Standard (AES).

3. For further development, it is recommended to use other web programming languages, such as python, ruby, and others. In order to know this steganography application performance in each of these languages.

4. This application only supports digital image files to the media container, is expected to be developed so that it supports audio files, video, and others as a medium.

VI. REFERENCES

[1]. **N. S. Raghava, Ashish Kumar, Aishwarya Deep and Abhilasha** chahal "Improved LSB method for image steganography using henon chaotic map" open journal of information security and applications volume 1, number 1, June 2014.

[2]. **Prof.Arjun.R.Nichal, Mr.Abhinav.C.Gorle, Mr.Nitin.S.Chavan, Ms.Rohini.R** "Implementation and Performance Analysis of LSB Based Steganography" International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 2 Issue: 4 pp:-885-889, April-2014

[3]. **Marghny H. Mohamed, and Loay M. Mohamed** "High Capacity Image Steganography Technique based on LSB Substitution Method" An International Journal Applied Mathematics & Information Sciences Appl. Math. Inf. Sci. 10, No. 1, pp-259-266, 1-jan-2016

[4]. **A.E.Mustafa, A.M.F.ElGamal, M.E.ElAlmi, Ahmed.BD** "A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit"Research Journal Specific Education Faculty of Specific Education Mansoura University Issue No. 21, April. 2011

[5]. **Siddharth Singh and Tanveer J. Siddiqui** "A security enhanced robust steganography algorithm for data hiding,"IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, PP 131-139, May 2012 .

[6]. **Reyadh Naoum, Ahmed Shihab, Sadeq AlHamouz"** Enhanced Image Steganography System based on Discrete Wavelet Transformation and Resilient Back-Propagation" IJCSNS International Journal of Computer Science and Network Security, VOL.15 No.1, January 2015

[7]. **Akhtar Nadeem, Ambreen Bano, Islam Faraz "**An Improved Module Based Substitution Steganography Method" IEEE 2014 Fourth International Conference on Communication Systems and Network Technologies pages 695-699, April 2014

[8]. **A Tahir, Doegar Amit "**A Novel Approach of LSB Based Steganography Using Parity Checker" International Journal of Advanced Research inComputer Science and Software EngineeringVolume 5, Issue 1, January 2015

[9]. **Das Pallavi, Satish Chandra,C. Kushwaha,Madhupama "** Data Hiding Using Randomizationand Multiple Encrypted Secret Images" the IEEE international conference on communicat ion and signal processing ,pp:0298-0302, April-2015