Efficient and Robust Spatial Domain Image LSB Steganography

Divya Singh[#1],Bhanu Prakash Lohani[*2],Vimal Bibhu[@3]

[#1] Senior Lecturer,Amity University Gr Noida Campus

[1] divya1784@rediffmail.com

[*2] Senior Lecturer, Amity University Gr Noida Campus

[2] bhanuplohani@gmail.com

[@3]Assistant Professor, Amity University Gr Noida Campus

[3] vimalbibhu@gmail.com

Abstract. Steganography is the art of hiding information in some medium. Here we are using image as a means for securing information for data transmission. Spatial domain image Steganography has been used for the work because of its compatibility to images. Objective of the paper is to increase the capacity of hidden data in a way that security could be maintained. This paper discusses the concept of "Digital Image Steganography" and various techniques used in image Steganography in spatial domain. In this paper we will also discuss the difference between image Steganography and watermarking technique. Basically Steganography pay attention to the degree of invisibility while watermarking pay most of its attribute to the robustness of the message and its ability to withstand attacks of removal such as image operation (rotation ,cropping, filtering)audio operation in the case of images of audio files being watermarked respectively. Communication of secret information between two entities can be achieved through steganography. The term being derived from Greek words *Steganos* and *graphia* meaning covered writing. Steganography is an information hiding technique where the secret information to be communicated is embedded into a cover media such as image, video, audio and text files such that the hacker looking at the stego image cannot even think of the existence of the secret information and only it can be retrieved at the destination by an authorized person.

Keywords: Digital, Steganography, audio, video, rotation ,cropping, filtering , digital ,watermarking.

I. INTRODUCTION

Steganography: Steganography is the art of hiding the fact that communication is taking place by hiding information in other information. Many different carrier file formats can be used but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of Steganography techniques some are more complex than others and all of them have respective strong and weak points. The major task is to provide the user the flexibility of passing the information implementing the encryption standards as per the specification and
algorithm proposed and store the information in a form that is unreadable to unauthorized person.

II. STEGANOGRAPHIC CAPACITY

Steganographic capacity refers to the maximum amount (rate) of information that can be embedded into a cover-object
and then can be reliably recovered from the stego-object (or a distorted version), under the constraints of undetectability, perceptual intactness and robustness, depending on whether Wendy is active or passive. Compared to data hiding systems, stegosystems have the added core requirement of undetectability. Therefore, the steganographic embedding operation needs to preserve the statistical properties of the cover-object, in addition to its perceptual quality. On the other hand, if Wendy suspects of a covert communication but cannot reliably make a decision, she may choose to modify the stego-object before delivering it. This setting of steganography very much resembles to data hiding problem, and corresponding results on data hiding capacity can be adapted to steganography **[1].**

III. SPATIAL DOMAIN EMBEDDING

The best widely known steganography algorithm is based on modifying the least significant bit layer of images, hence known as the LSB technique. This technique makes use of the fact that the least significant bits in an image could be thought of

random noise and changes to them would not have any effect on the image. In the LSB technique, the LSB of the pixels is replaced by the message to be sent. The message bits are permuted before embedding, this has the effect of distributing the bits evenly, thus on average only half of the LSB's will be modified. Popular steganographic tools based on LSB embedding [3, 4, and 5], vary in their approach for hiding information. Some algorithms change LSB of pixels visited in a random walk, others modify pixels in certain areas of images, or instead of just changing the last bit they increment or decrement the pixel value [2].

IV. STEGANALYSIS

Steganalysis is the science of attackingSteganography in a battle that never ends. It mimics the already established science of Cryptanalysis. Note that a Steganographer can create Steganalysis merely to test the strength of their algorithm. Steganalysis is achieved through applying different image processing techniques e.g., image filtering, rotating, cropping,translating, etc. More deliberately Steganalysis can involve coding a program that examines the stegoimage structure and measures its statistical propertiese.g., first order statistics (histograms) or second orderstatistics (correlations between pixels, distance,direction). Apart from many other advantages higher order statistics, if taken into account before embedding, can improve the signal-to-noise ratio when dealing with Gaussian additive noise.

V. TECHNIQUES OF IMAGE STEGNORAPHY

Various techniques are used for digital image steganoraphy

A. Spatial Domain based Steganography :It includes LSB (Least Significant Bit) Steganography. The spatial methods are most frequently employed because of fine concealment, great capability of hidden information and easy realization. LSB Steganography includes two schemes: Sequential Embedding and Scattered Embedding. [4]

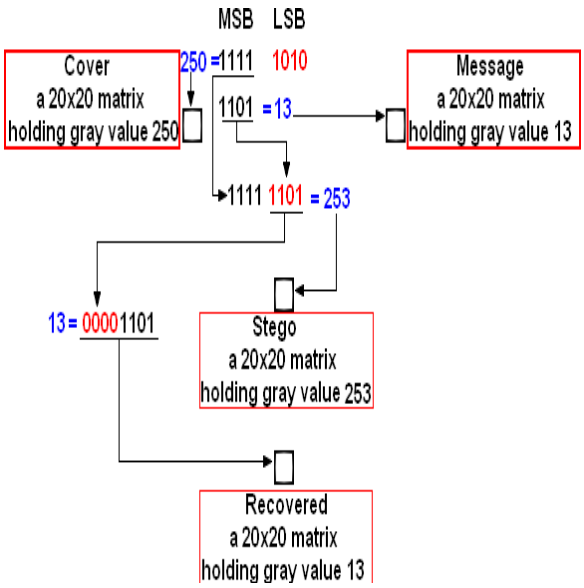
B. Transform Domain based Steganography:The method of transform domain Steganography is to embed secret data in the transform coefficients.

C. Document based Steganography: This method embeds data in documents files by adding tabs or spaces to .txt or .doc files.

D. File Structure based Steganography: This method inserts secrets data in the redundant bits of cover files, such as the reserved bits in the file header or the marker segments in the file format..

E. Steganography in the Image Spatial Domain

In spatial domain methods a steganographer modifies the secret data and the cover medium in the spatial domain, which involves encoding at the level of the LSBs. This method although simpler, has a larger impact compared to the other two types of methods. A general framework showing the underlying concept is highlighted in Fig.below. A practical example of embedding in the 1st LSB and up to the 4th LSB is illustrated in Fig. 11. It can be seen that embedding in the 4th LSB generates more visual distortion to the cover image as the hidden information is seen as “non-natural”. **[4].**



F. **Steganography in the Image Frequency Domain**: Now when the development in IT technology we need more security which is not fulfilled by spatial domain we can achieved more security by using steganoraphy in the image frequency domain. The discovery of the LSB embedding mechanism is actually a big achievement. Although it is perfect in not deceiving the HVS, its weak resistance to attacks left researchers wondering where to apply it next until they successfully applied it within the frequency domain.[6]

G. EZ stego method: EZ stego method is similar to the commonlyused LSB method for 24 bit color images (or 8 bit gray scale images). After the palette colors are sorted by luminance, this method embeds the message in a binary form into the LSB of indices

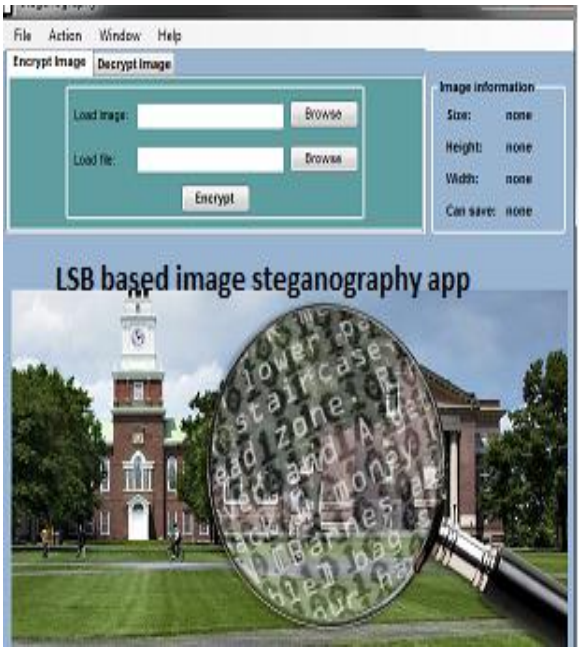
pointing to the palette colors. The detail steps are as follows.[8]
Step 1: Reorder the color in the palette according to the luminance of each palette entry.
Step 2: Find the index of the pixel_s RGB color in the reordered palette.
Step 3: Replace the LSB of the index with one bit of the embedding binary message.
Step 4: Find the new RGB color in the reordered palette referred to by the index.
Step 5: Find the index of the new RGB color in the original palette.
Step 6: Replace the pixel with the index of the new RGB color.
The receiver can simply recover the message by collecting the LSBs of all indices in the image file.A technique for transferring data such that it can be processed as a steady and continuous stream, client does not have to download the entire file to view it. With streaming video, viewers/listeners do not have to download a complete movie or audio before it starts to play. Instead, the movie literally streams in while you play it, comparable with a running water tap.

VI. PRACTICAL APPROACH

Steganography exploiting the Image Format
Steganography: can be accomplished by simply feeding into a Windows OS command window, e.g., Windows XP) the following code: C:\> Copy Cover.jpg /b + Message.txt /b bhanu.jpg What this code does is that it appends the secret message found in the text file 'Message.txt' into the JPEG image file 'Cover.jpg' and produces the stego-image 'bhanu.jpg'. The idea behind this is to abuse the recognitionof EOF (End of file). In other words, the message is packed and inserted after the EOF tag. When bhanu.jpg is viewed using any photo editing application, the latter will just display the picture ignoring anything coming after the EOF tag. However, when opened in Notepad for example, our message reveals itself after displaying some data. The embedded message does not impair the image quality. Neither image histograms nor visual perception can detect any difference between the two images due to the secret message being hidden after the EOF tag. Whilst this method is simple, a range of steganography software distributed online uses it (Camouflage, JpegX, and Data Stash [3]).

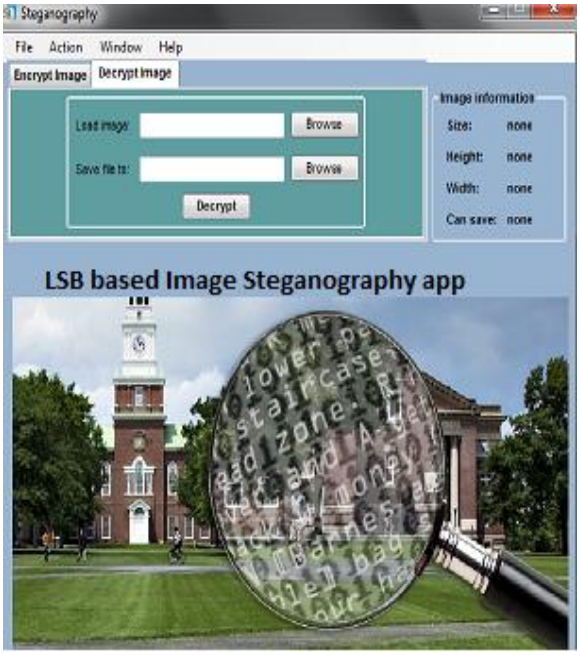
4: Related work -- Proposed steganorapihc system (Model): We have implemented a project in which the algorithms are used follows the concept of LSB based image steganography ,hence we have generated a model for image steganography. In this system we have generated a GUI for steganographic application. In this GUI there are two main functions, one is used for encryption process and another is for the used decryption process. In the time of encryption process we will take one image and another text file which we want to hide and then by following some algorithm this will convert the required file and in the decryption process we will give the encrypted files location and the location where we want to save the decrypted file and we will find the same name file which in encrypted at the given location. In our project we used a header to help with the embedding and extracting of a message from an image. This allows for quick updates to the encoding algorithm, as well as multiple user-specific modes of encoding. It also allows for better Stengagraphic hiding because the header format changes depending on the message type, mode, and length, making it harder to crack and detect my Steganography.The totlal GUI which is implemented by us is shown by the help of diagram (snapshot1 and snapshot 2) .

Encrytion Process:



S1: Encryption Process GUI

Decryption Process:



S2: Decryption process GUI

VII. FUTURE THOUGHTS

Here in the above project done by us it only support the bmp and txt file format so this is the limitation of our project. In future we will add the functionality in which the above project will support all file formats. This allows for a much broader area: one would be able to encode .exe, .doc, .pdf , .mp3 etc. Proposed method is achieving highest capacity among all existing methods without any distortion in image. When proposed method has been performed on different images, it has given constant result but other existing methods gave different results on different images. Proposed method is secure and undetectable because of randomness. In future, techniques to improve security for data hiding by using randomization will be used to extend this work.

VIII. CONCLUSION

In this paper we have discussed the concept of "Digital Image Steganography" and various techniques used in image Steganography in spatial domain. We have also discussed the difference between image Steganography and watermarking technique. Steganography is an information hiding technique where the secret information to be communicated is embedded into a cover media such as image, video, audio and text files such that the hacker looking at the stego image cannot even think of the existence of the secret information and only it can be retrieved at the destination by an authorized person.

References

[1]. P. Moulin and Y. Wang, \New results on steganography," Proc. of CISS,
[2]. T. Sharp, \Hide 2.1, 2001," http://www.sharpthoughts.org**.**
[3]ftp://ftp.funet.fi/pub/crypt/mirrors/idea.sec.dsi.unimi.it/code/s-tools4.zip
[Stella] : http://wwwicg.informatik.uni-rostock.de/~sanction/stella/
http://sourceforge.net/projects/hide-in-picture/
[Revelation]: http://revelation.atspace.biz/
[Camouflage]: http://camouflage.unfiction.com/
[4] P. Alvarez, Using extended file information (EXIF) file headers in digital evidence analysis, InternationalJournal of Digital Evidence, Economic Crime Institute (ECI), 2(3)(2004)1-5.
5] H. Farid, A Survey of image forgery detection, IEEE Signal Processing Magazine, 26(2)(2009)16-25.
[6]Marvel, L.M., Boncelet, C.G., Retter, C.T., 1999. Spread spectrum image steganography. IEEE Trans. Image Process. 8 (8), 1075–1083.
[7] D. Frith, Steganography approaches, options, and implications, Network Security, 2007(8)(2007)4-7.
[8] M.H. Shirali-Shahreza and M. Shirali-Shahreza, A new approach to Persian/Arabic text teganography, in:Proceedings of 5th IEEE/ACIS International conference on Computer and Information Science (ICISCOMSAR 2006), 10-12 July 2006, pp. 310-315.

