Hiding Data in Image using Extended Pixel Mapping Method

Miss. Nishigandha P. Mangle
Master of Engineering
Information Tecnology Department
prof. Ram Meghe Institute of Technology & Research
Amravati,India
Nishigandhamanglepapers2014@gmail.com

Prof .Sanjay V. Dhopte
Information Tecnology Department
prof. Ram Meghe Institute of Technology & Research
Amravati,India
sanjaydhopte@gmail.com

Abstract— Internet technologies are currently charring an important role in our day to day life. It has the benefit as well as disadvantages also.This in term generates the needs of data activity technology for maintaining the secrecy of the key information. The steganograpic concept of data hiding is used in this method. The method used spatial domain technique. This algorithm used image as a carrier medium for hiding the data. In this pixel component are used for hiding the data. For achieving this pixel index value and their position are calculated. According to this key will be generated and by using key data is hided.Experimental result shows that the perceptual quality of hided image is high in this technique. The key idea of this project is to hide the data in carrier image and retrieve data from carrier image without affecting without affecting the perceptual transparency of the data hided image. This system provides compression of data so that payload capacity of the system will be increases.

Keywords— *Higher LSB, Guard Pixels, Steganography, Multi- carrier, Information hiding , data Encryption.*

*****

I. INTRODUCTION

Digital communication has become an essential part of infrastructure now a days, a lot of applications are Internet-based and in some cases it is desired that the communication be made secret. Two techniques are available to achieve this goal: one is cryptography, where the sender uses an encryption key to scramble the message, this scrambled message is transmitted through the insecure public channel, and the reconstruction of the original, unencrypted message is possible only if the receiver has the appropriate decryption key. The second method is steganography, where the secret message is embedded in another message. Using this technology even the fact that a secret is being transmitted has to be secret. [10]Data hiding is a technique that imperceptibly hides secret data into cover media, such as digital images, videos, audios, etc. as shown in fig.1.

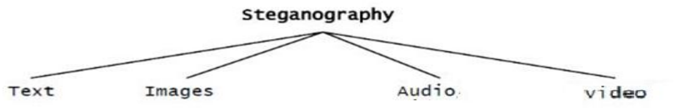

Figure:1.1 classification of Steganographic Techniques

Data hiding is the practice of hiding information "in plain sight". This technique relies on a message being encoded and hidden in a transport layer in such a way as to make the existence of the message unknown to an observer. Importantly, the transport layer the carrier file is not secret and can therefore be viewed by observers from whom the secret message itself should be concealed.[12] The power of privacy of data is hiding the secret message by obscurity, hiding its existence in a non-secret file. In that sense,privacy of data is different from cryptography, which involves making the content of the secret message unreadable while not preventing non-intended observers from learning about its existence. Because the success of the technique depends entirely on the ability to hide the message such that an observer would not suspect it is there at all, the greatest effort must go into ensuring that the message is invisible unless one knows what to look for. The way in which this is done will differ for the specific media that are used to hide the information. In each case, the value of a privacy of data approach can be measured by how much information can be concealed in a carrier before it becomes detectable, each technique can thus be thought of in terms of its capacity for information hiding. There are numerous methods used to hide information inside of Picture, Image and Video files. The desire to send a message as safely and as securely as possible has been the point of discussion since time immemorial. Information is the wealth of any organization. This makes security-issues top priority to an organization dealing with confidential data. Whatever is the method we choose for the security purpose, the burning concern is the degree of security. Privacy of data is to the art of covered or hidden writing.[11] The purpose of privacy of data is convert communication and hide a message from a third party. Privacy of data is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between the two is that privacy of data involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Privacy of data in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture,Video or Image file.[1] What privacy of data essentially does is to exploit human perception; human senses are not trained to look for files that have information hidden inside of them. Generally, in privacy of data, the actual information is not maintained in its original format and there by it is converted into an alternative equivalent multimedia file like image, video or image which in turn is being hidden within another object. This apparent message (known as cover text in usual terms) is sent through the network to the recipient, where the actual message is separated from it. There are many to embed information into a popular media using privacy of data.A good example of this is the relationship between coded song and its lyrics. The image file containing the recording is much larger than the song lyrics stored as a plain ASCII files. Therefore it is probably safe to assume that the smaller file could be privat data embedded into the larger one without impacting the quality. Important domains, besides classic computing, where privacy of data can be applied are domains using mobile and embedded devices especially mobile phones.[10] In this project we state the fact that privacy of data can be successfully implemented and used into a next generation of computing technology with image and video processing abilities. This research will include implementation of privacy of data algorithm for encoding data inside video files, as well as technique to dynamically extract that data as original.

Steganography provides the authentication over the data using some tag or labeling on some objects like text, audio, video, image. The goal of steganography is to cover the presence of a message and to form a covert channel. The message is hidden in another object as a result the transmitted object are going to be identical wanting to each individual’s eye.[13] Steganoanalysis is that the art of detective work any hidden message on the communicating. If the existence of the hidden message is exposed, the goal of steganography is crushed.

One of the possible ways of categorizing the present steganalytic attacks is on the following two categories

1. Visual Attacks: These methods try to detect the presence of information by visual inspection..

2. Statistical Attacks: These methods use first or higher order statistics of the image to reveal tiny alterations in image.[15]

USES OF STEGANOGRAPHY

1. steganography is used to stored any information in some medium when we want to store some secret information such as military secret information.
2. Steganography can be used to implement watermarking.for eg.IDs embedded into the fingerprint images via steganography.
3. 3.The transportation of sensitive data is another key use of steganography.Such as from E-Mail to images on Internet websites.[14]

II. Literature Survey

2.1.Existing Steganographic Techniques

The steganographic algorithms proposed in literature can broadly be classified into two categories.

1. Spatial Domain Techniques

2. Transform Domain Techniques

Each of these techniques is covered in detail in the next two subsections.

2.2. A Spatial Domain Image Steganography Technique

These techniques use the pixel gray levels and their color values directly for encoding the message bits. These techniques are some of the simplest schemes in terms of embedding and extraction complexity. The major drawback of these methods are amount of additive noise that creeps in the image which directly affects the Peak Signal to Noise Ratio and the statistical properties of the image. Moreover these embedding algorithms are applicable mainly to lossless image-compression schemes like TIFF images.[6]

Ching-Chiuan Lin_atel.[2] This paper proposes in 2008 a data hiding scheme that losslessly embeds a message into a cover image using the two differences between the first and the second pixel as well as between the second and the third pixel in a three-pixel block. Data embedding is done using difference between 1st and 2nd pixel and 2nd and 3rd pixel.Payload capacity 2.08 bpp Drawback of method is that cover medium get injured .*Cheng-Hsing Yang_atel*[3](2008)This paper proposes a new adaptive least significant bit (LSB) steganographic method using pixel-value differencing (PVD) that provides a larger embedding capacity and imperceptible stegoimages. The method exploits the difference value of two consecutive pixels to estimate how many secret bits will be embedded into the two pixels. *Der-Chyuan Lou_atel* [4] The transmission of digitized medical information has become every convenient due to the generality of Internet. Regardless of the prevention of medical fault, the real-time detection of abnormal event, the support of clinical decision, even the model developing of medical service based on patient, Internet has created the biggest benefit to achieve the goals of promoting patient safety and medicine quality The disadvantage of the HIS is the medical staffs can only look up the related check reports in the specific place. This is inconvenient for the data searching. The proposed multiple-layer embedding goes as follows. In the first layer, we use the horizontal scanning method to obtain the pixel pair. *Min-Yen Chiu_atel*[5] Hiding a lot of data into cover image causes serious distortion. Therefore, hiding capacity is limited by maintaining image quality. A method is proposed to solve this problem in this paper. Firstly, we divide cover-image into many non-overlapping blocks. Each block consists of two contiguous pixels. The hiding bits are transformed into decimal format and are separated into two parts. Then, modulus operation is used to hide two parts into the first pixel and the second pixel of a block, respectively. Experiment results prove that the proposed method has higher image quality than pervious literature which is based on pixel value differencing *Weiqi Luo_atel[7]* The least-significant-bit (LSB)-based approach is a popular type of steganographic algorithms in the spatial domain. However, we find that in most existing approaches, the choice of embedding positions within a cover image mainly depends on a pseudorandom number generator without considering the relationship between the image content itself and the size of the secret message. *Ankita Sancheti_atel*[8]In this paper, secure steganography is used to obtain high capacity of image for data hiding. Both color and gray scale images have been used as cover file for PVD method. Then a secret key is used to control the message embedding process. To estimate how many secret bits will be embedded into the pixel, largest difference value between the other three pixels close to the target pixel is used. This makes edge areas of image to be used for higher embedding capacity. *Vijay kumar Sharma_atel*.[9]Steganography is a branch of information hiding. It allows the people to communicate secretly. To ensure the security against the steganalysis attack, a new steganographic algorithm for 8bit(grayscale) or 24 bit (colour image) is presented in this paper, based on Logical operation. Algorithm embedded MSB of secret image in to LSB of cover image. In this n LSB of cover image ,from a byte is replaced by n MSB of secret image. The image quality of the stego-image can be greatly improved with low extra computational complexity.

III. PROPOSED WORK

This contribution we present an extension of PMM method which is based on special domain with the help of different images.We have used different images in our work,which have been collected frome image database and those images which are used in researchers.The input message can be adopted as digital character format.The ASCII to binary canversion take place.Bits are used for embedding in separate pixel and selection of embedding pixel depends upon mathematical function which also construct by us.The selection technique is based on pixel intensity value and pixel position on image.Mapping of secret data in embedding pixel is based on intensity value.Extraction process starts again by selecting the same reverse process required during embedding process.At the receiver side other different reverse operation has been carried out to get back the original information.

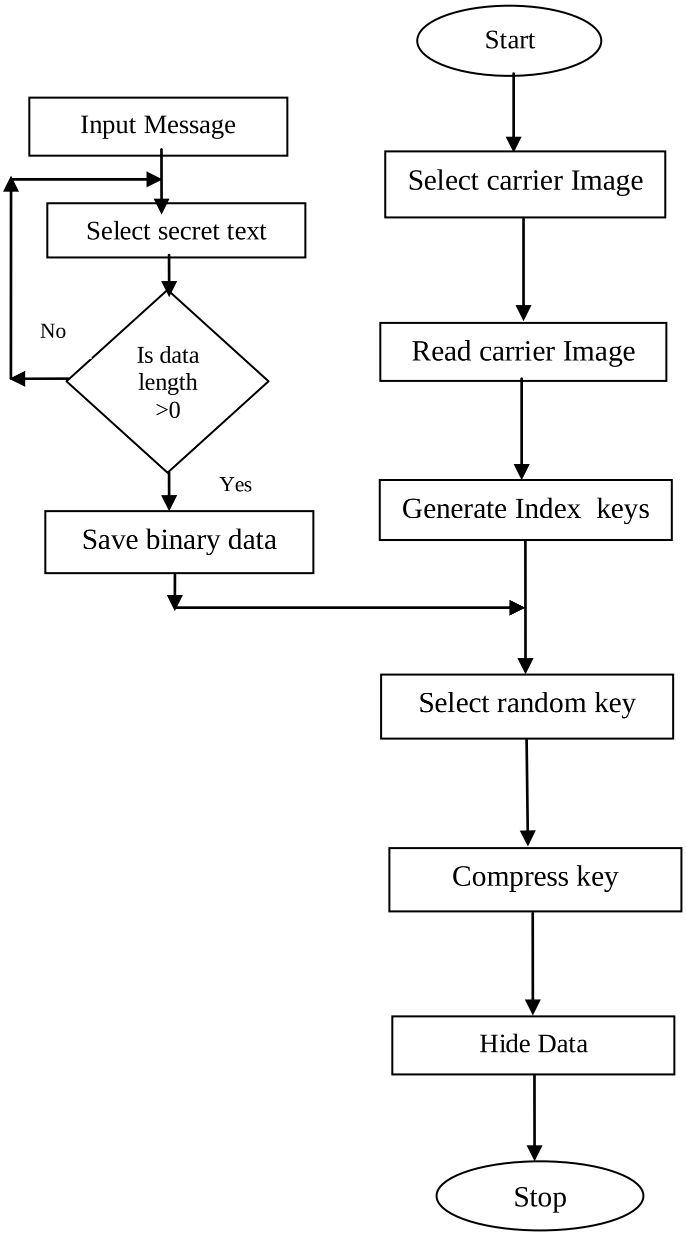

Fig. III.I: Flowchart for Data Hiding

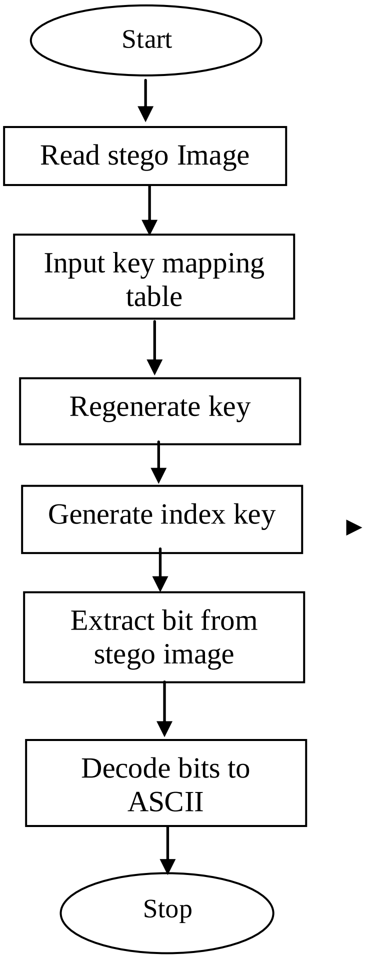

Fig.III.II:Flowchart for Data Extraction

Proposed Methodology has been divided in 2 Phases:

1) Data Hiding
2) Data Extraction

Algorithm for Data hiding:-

1. Select an Image for hiding.
2. Read carrier Image
3. Select secret data either from file or by writing.
4. Data length is calculated and convert it to binary code.
5. Generate Index keys.
6. Select random key using mathematical function.
7. Key get compress and compress key is generated.
8. Stop

Algorithm for Data Extraction:-

1. Select a stego Image.
2. Read stego image dimention.
3. Input key mapping table.
4. Regenerate key using key mapping table.
5. Generate index key.
6. Extract bit from stego image.
7. Decode bits to ASCII
8. Generate Data.
9. Stop

IV. RESULTS AND ANALYSIS

In this section,we describe the experimental results of method which based on some techniques to calculate data hiding performance.Capacity of data hiding and image quality of stego image,these two techniques are used here for performance metric.The quality of stego image produced by the proposed method has been tested based on various images..Figure----shows the graphical representation of calculated value of various images.The techniques are described below:

Compression ratio:Data compression ratio is defined as the ratio between the *uncompressed size* and *compressed size.*

$$\text{Compression Ratio} = \frac{\text{Uncompressed Size}}{\text{Compressed Size}}$$

Here we have tested the system for number of images of different format and different size.In this stego images are generated by help of our algorithm and some parameter are calculated.The figure shows the graphical analysis of some images.Fig.IV.1 shows that as the image size increases the data hiding capacity of image increases.As image size increase secret data length also increases but the time for hiding the bits also increases respectively. Algorithm calculate the key depend upon the secret data length.The generated key length is equals to the secret data length as shown in figIV.2.Fig.IV.3 shows as secret data length increases compression key length decreses i.e compression ratio decreses.The fig IV.4 shows compression ratio increases upto 50%.As the compression ratio increases data hiding capacity of algorithm increases.

Table 5.1:Size of Image and secret data length

Name of Input Image	Size of Input Image	Secret data length
Img1.jpg	57x89	80
Img2.jpg	81x99	88
Img3.jpg	82x140	112
Img4.jpg	99x81	128
Img5.jpg	104x99	184
Img6.jpg	123x145	216
Img7.jpg	123x156	296
Img8.jpg	142x152	472
Img9.jpg	169x230	660
img10.jpg	230x169	752
Img11.bmp	234x280	800
Img12.bmp	1024x768	832
Img13.gie	1024x758	884

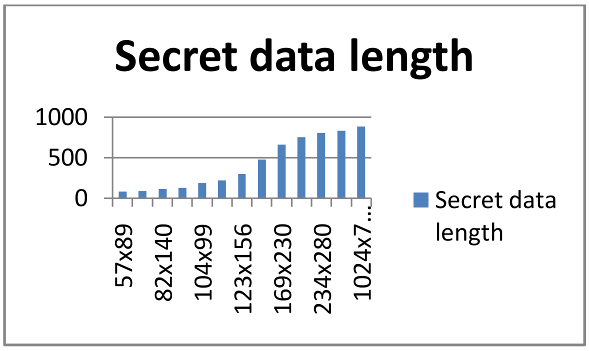

Fig.IV.1 Image size and secret data length\

Table 5.2:Secret data length and compress Key length

Name of Input Image	Size of Input Image	Secret data length	Compress key length
Img1.jpg	57x89	80	58
Img2.jpg	81x99	88	46
Img3.jpg	82x140	112	46
Img4.jpg	99x81	128	74
Img5.jpg	104x99	184	84
Img6.jpg	123x145	216	89
Img7.jpg	123x156	296	144
Img8.jpg	142x152	472	184
Img9.jpg	169x230	660	251
img10.jpg	230x169	752	384
Img11.bmp	234x280	800	400
Img12.bmp	1024x768	832	410
Img13.gie	1024x758	884	424

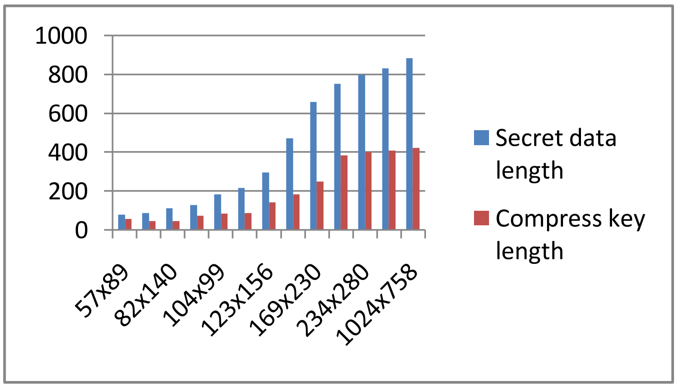

Fig.IV.3 Relationship between secret data length and compress key length

Name of Input Image	Size of Input Image	Secret data length	Compress key length	compression ratio
Img1.jpg	57x89	80	58	45.65
Img2.jpg	81x99	88	46	48.64
Img3.jpg	82x140	112	46	57.81
Img4.jpg	99x81	128	74	45.33
Img5.jpg	104x99	184	84	52.27
Img6.jpg	123x145	216	89	41.2
Img7.jpg	123x156	296	144	48.64
Img8.jpg	142x152	472	184	38.98
Img9.jpg	169x230	660	251	38.03
img10.jpg	230x169	752	384	51.06
Img11.bmp	234x280	800	400	50
Img12.bmp	1024x768	832	410	49.27
Img13.gie	1024x758	884	424	47.96

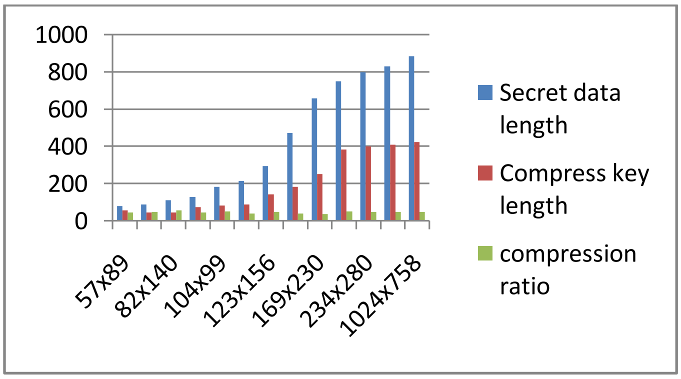

Fig. IV.4 Relationship between compress key length and compression key length.

V. CONCLUSION

In this technique varied format of the images are often taken as carrear medium.The data is hidden secrectly and retrieve at recever side by using key mapping table Experimental results of the method supported some techniques evaluate assess, the hiding performance capability of hiding knowledge and physical property of the image. the standard of image made by the planned technique has been tested..Experimental result's calculated using varied image and of various format.The result analysis can shows that because the size of image will increase the information hiding capability are increases.The compression ratio are will increase and data hiding capability will increase. This technique could be a robust technique.

REFERENCES

[1] Arvind Kumar,Km. Pooja," Steganography- A Data Hiding Technique" International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010

[2] Ching-chiuan Lin,Nien-Lin Hsueh"A lossless data hiding scheme based on three-pixel block differences",scienceDirect, the journal of the pattern recognition society.2007

[3] Cheng-Hsing Yang,chi-yao Weng,shiuh-Jeng Wang,Member,IEEE,and Hung-Min Sun," Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems",IEEE TRANSACTION ON INFORMATION FORENSINCS AND SECURITY,VOL.3,NO.3,SEPTEMBER 2008

[4] Der-Chyuan Lou, Ming-Chiang Hu, Jiang-Lung Liu," Multiple layer data hiding scheme for medical images"scienceDirect,computer standards and interface(2008)CSI-02585

[5] Min-Yen Chiu, Yu-Sheng Liao," Improved Steganographic Technique for the Image Quality of PVD",International Conference on Advanced Information Technologies(AIT)2010.

[6] Ms.G.S.Sravanthi, Mrs.B.Sunitha Devi, S.M.Riyazoddin& M.Janga "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method",Global journal of computer science and technology graphics and vision volume 12 Issue15 version,2012.

[7] Weiqi Luo, Member, IEEE, Fangjun Huang, Member, IEEE, and Jiwu Huang, Senior Member," Edge Adaptive Image Steganography Based on LSB Matching Revisited" , IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 2, JUNE 2010

[8] Ankita Sancheti," Pixel Value Differencing Image Steganography Using Secret Key",International Journal of Innovative Technology and Exploring Engineering(IJITEE)ISSN:2278-3075,VOL-2,Issue-1,December 2012

[9] Vijay Kumar Sharma ,Vishal Shrivastava," A STEGANOGRAPHY ALGORITHM FOR HIDING IMAGE IN IMAGE BY IMPROVED LSB SUBSTITUTION BY MINIMIZE DETECTION",Journal of Theoretical and Applied Information Technology,vol.36,2012.

[10] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav," Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, pp. 338-341

[11] Satish Singh Verma , Ravindra Gupta , Gaurav Shrivastava," A Novel Technique for Data Hiding in Audio Carrier by Using Sample Comparison in DWT Domain", 2014 Fourth International Conference on Communication Systems and Network Technologies.

[12] Saravanan, A. Neeraja,"Security Issues in Computer Networks and Stegnography", International Conference on Intelligent Systems and Control (ISCO 2013) ©2012 IEEE

[13] Richard E. Woods & Rafael C. Gonzalez"Digital ImageProcessing" Book.

[14] Arvind Kumar, Km. Pooja," International Journal of Computer Applications", (0975 – 8887)Volume 9– No.7, November 2010.

[15] Ms. Megha B. Goel, 2Mr. M. S. Chaudhari, 3Mrs. Shweta A. Gode "A Review on Data Hiding using Steganography & Visual Cryptography", © 2014 IJEDR | Volume 2, Issue 1 | ISSN: 2321-9939