Using SBR Algorithm To Hide The Data Into The JPEG Image

Ashwini Palimkar *palimkarashwini@gmail.com*
M.Tech (stud of CSE)
Bharati Vidyapeeth University COE
Pune, 411043, Maharashtra, India.

Dr.S.H.Patil *shpatil@bvucoep.edu.in*
Professor & Head Dept of CSE
Bharati Vidyapeeth University COE
Pune, 411043, Maharashtra, India.

Abstract

Data hiding is the art of hiding data for various purposes such as--- to maintain private data, secure confidential data. Well known technique is the Steganography; Steganography has evolved into a digital strategy of hiding a file in some form of multimedia, such as an image, an audio file or even a video file. This paper presents a new Steganography technique in spatial domain for encoding extra information in an image by making small modifications to its pixels. The proposed method focuses on one particular popular technique, Least Significant Bit (LSB) Embedding. Instead of using the LSB-1 of the cover for embedding the message, LSB-2 has been used to increase the robustness of system. and protect the message against the external influences such as noise, filter, compression…etc.[Using SBR Algo].

For more protection to the message bits a Stego-Key has been used to permute the message bits before embedding it. An experimental result of the modified method shows that this paper helps to successfully hide the secret data into the image file with minimum distortion made to the image file.

Keywords: Steganography, Data Hiding, Embedding Data, SBR Algo, Least Significant Bit.

1. INTRODUCTION

With the digitization of data and networking of communications, communications security over the Internet is becoming more and more crucial. With the growth in the communication and so is in the data transmission rate across the various medium it is utmost important to have secure transmission of confidential and proprietary information. Steganography is an art to hide a message within an object so that eavesdropper is unaware of the message presence. Steganography works by replacing bits of unused data bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. Steganography can be applied on various digital objects like audio files, video files, images and text files. Digital images area preferred media for hiding information due to their high capacity and low impact on visibility. For the different image file formats, different steganographic algorithm exists. Most earliest is a Least Significant Bit Hiding (LSB) Scheme that is the easiest way of hiding information in an image. It uses LSB of the pixels to replace it with the message to be.

The basic terminologies used in Steganography systems are: the carrier, the secret data, and the stego key. The carriers such as a digital image, an mp3, even a TCP/IP packet among other things. Secret data is the information which is needed to be hidden in the suitable digital media. A stego key is used to decode the hidden message.

In history, the Nazis invented several Steganographic methods during WWII such as Microdots, invisible ink and null ciphers. As an example of the latter a message sent by a Nazi spy that read: "Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suet's and vegetable oils."

. Using the 2nd letter from each word the secret message reveals:

.Pershing sails from NY June 1.

In steganography, before the hiding process, sender must select an image file, secret data to be hidden and stego key used as password. This paper proposes a new second bit replacement algorithm to hide data in a JPEG image using steganographic method. In this we have used Compression method to increase the hiding capacity. We have used java application as front end And SQL query processor as back end for implementing this project.

2. IMAGE STEGANOGRAPHY

Image steganography takes the advantage of limited power of HVS.Images are the most popular object used for steganography.

2.1 Image Definition

Image is the collection of numbers that constitute different light intensities in different areas of image .This numeric representations forms a grid and the individual points are known as pixels .most images on the internet consists of rectangular map of images pixels, these pixels displayed R by R horizontally.

There are 8 bits used to define the color of each pixel. Digital color image is stored in 24 bit files & uses RGB color model as represents red[8 bit],green[8 bit],blue[8 bit].

2.2 Image Compression

When working with larger images, images tend to become too large to transmit over a std internet connection. To display an image in a reasonable amount of time ,techniques must be used to reduce the image's file size, these techniques use of mathematical formulas to analyze and condensed image data, resulting in smaller file size, this process is called compression.

2.3 Direct Cosine Transformation

Using DCT we can hide data. The DCT algorithm is used extensively in video and image(JPEG).Most of the techniques uses JPEG image as vehicle to embed their data.JPEG compression uses DCT to transform successive sub image blocks[8 x 8] Pixels into 64 DCT coefficients. This is a very simple method and while it works well in

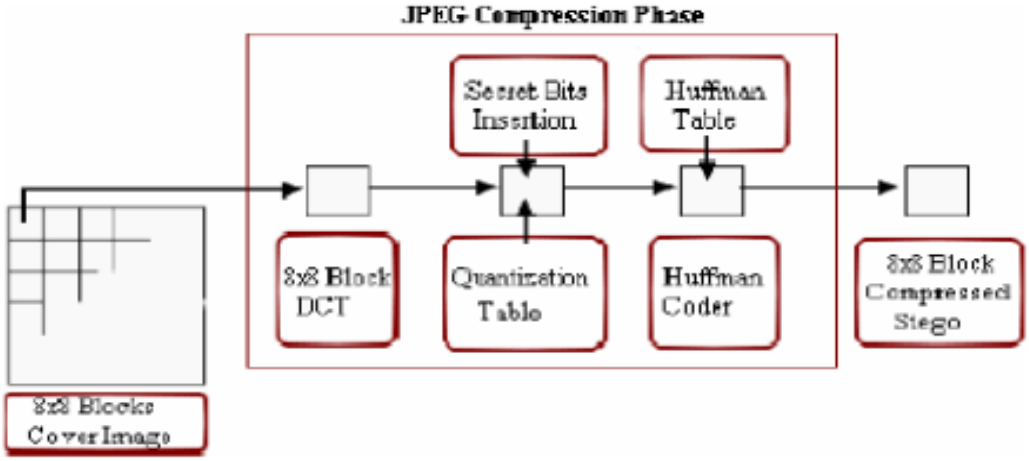


FIGURE1: Data flow diagram showing process of embeddingKeeping down distortions, it is vulnerabletonoise.

2.4. Categories of Image Steganography

Steganography can be applied to images, text, videos, digital signals as well as continuous signals and other information formats, but the preferred formats are those which repeat the data. Repetition can be in the form of repetition of bits which are responsible to visualize the information .Repeated bits of an object are those bits that can be altered without the alteration being detected easily.

Image domain also known as spatial domain methods insert messages in the intensity of the pixels directly. Image domain Steganography take in bit-wise methods that apply bit insertion and noise manipulation. Sometimes it is characterized as simple systems. Transform domain also known as frequency domain Steganography methods. In this method images are first transformed and then the message is inserted in the image

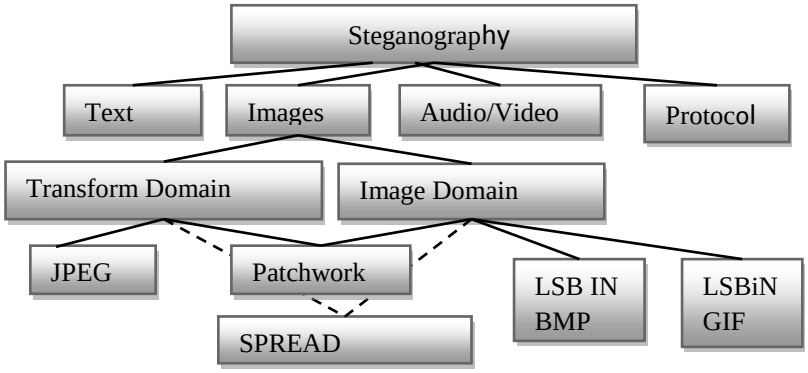


FIGURE2: Categories of Image Steganography.

2.5 Applications of Steganography

1. Image Steganography allows for two parties to communicate secretly and covertly [on the internet].
2. It allows for copyright protection on digital files using the message as a digital watermark.
3. For the transportation of high-level or top-secret documents between international governments.
4. Remarkable use in Military Applications

5. It can also be quite nefarious. It can be used by hackers to send viruses and Trojans to compromise machines, and also by terrorists and other organizations that rely on covert operations to communicate secretly and safely.

3. PROPOSED SYSTEM

I have chosen to implement LSB second bit replacement algorithm (SBR algorithm).

In this method, color image has been used as a cover. So, we can hide a data up to 65536 bytes. The data is embedded in the LSB-2 of the cover to increase the robustness of the system and protect the message against the external influences such as noise, filter, compression…etc. The embedding process is very easy, which only replaces the permutated bits of the message by the LSB-2 set of the cover to obtain the new stego-image array

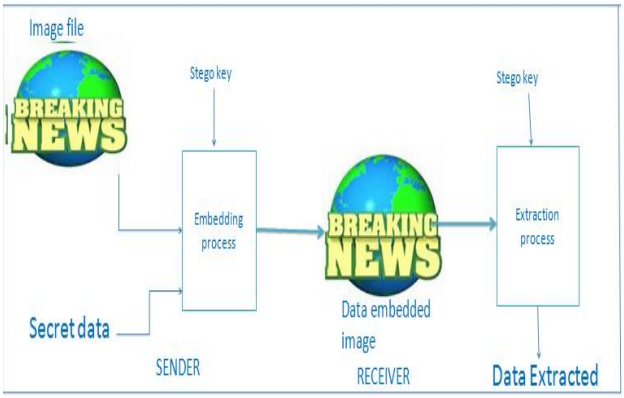


FIGURE 3: Proposed System.

The proposed system consists of :

3.1 Embedding Process

Inputs: Image file, secret data, stego key
Output: Data embedded image
Step 1: Scan the Original image and encode it in binary form and store it in the array called Pixel-array
Calls the compression function
Step 2: select secret data convert it in binary and store it in the array Mi.
Step3: select the image file and find number of pixels, set LSB-1=Ai array.
Step4: select the image file and find number of pixels, set LSB-2=Bi array.
Step 5: Encode Stego key in binary and store it in the array
Step 6: check the length of secret data and length of image file.
Step 7: Choose first pixel
Step 8: Start picking bit from the beginning of the key array, and LSB bit form first byte of pixel.
Step 9: Apply AND function& SHIFT operator.
Step 10: Start Loop1
If bit of data to be hidden is=1& Bi = 0
Then 1.replace value of Bi
2. Ai=0
3. Set as minus 1 pixel value
End
Step 11: For second byte of image file
Start Loop2
If bit of data to be hidden is=0& Bi = 1
Then 1.replace value of Bi

2. Ai=1
3. Set as increase 1 pixel value

End

Step12: Replace necessary bits as defined by Compression ratio in each pixel, Store information about bits Embedded in binary file.
Step13: Repeat step8, step9, step10, step11, step12 6 till all the bits of image file has been embedded.
Step 14: Set the image with new values and save it
Step 15: End

3.2. Extraction Process

Inputs: Embedded image file, Secret key
Output: Secret data
Step 1: Select the folder in which you want to extract the hidden data
Step 2: Choose the embedding image file.
Step 3: Provide security key.
Step4: Convert the binary file into human readable form.

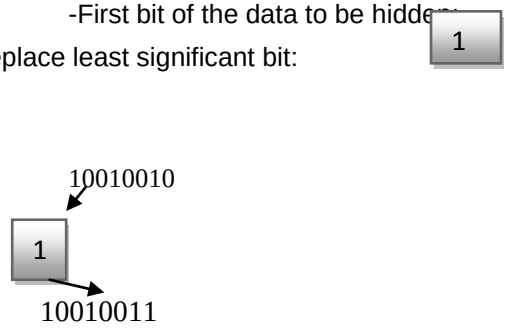
4. EXPERIMENTAL RESULTS AND DISCUSSIONS

Experimental results are given in this section, we used standard image to apply the proposed algorithm, consider that we have to hide the secret data "A" in image files:

Step1: Convert the data from decimal to binary.
Data-----.>10000001
Step 2: Read image file.
Step3: Convert the image file from decimal to binary.
Step4: Break the byte to be hidden into bits.
10000001 ---------- 10000001
Step5: Take first byte of original data from the image file.

CASE1 LSB-1 REPACEMENT

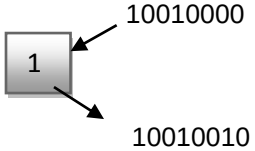
Step6: Replace the least significant bit by one bit of the data to be hidden.
- First byte of original data from the Cover Image: 10010000
-First bit of the data to be hidden:
-Replace least significant bit:



Repeat the replace for all bytes of Cover Image

CASE2: ROBUST LSB-2 REPLACEMENT

step6: Replace LSB2 by one bit of the data to be hidden.
A- Select First byte of original data from the image file
- First bit of the data to be hidden is: 1
- Replace the LSB2:



- In our proposed method if the bit of the data to be hidden = = 1 and

LSB2= =0 then

1. We change LSB1 of image to 0 after replacement.
   10010010
2. we subtract 1
   10010000

So we have no change image file

B- Second byte of original data from the image file: 10010010

-2nd bit of the data to be hidden

0

- Replace the LSB2:

10010010

0

10010000

In our Proposed Method if the bit of the data to be hidden = = 0 and LSB2= =1

1. We change LSB1 of image to 1 after replacement. 10010011
2. Increase one 10010010

So we have No change in data embedded image

Repeat the replace for all bytes of image

The system is tested using the images as shown in **FIGURE**4&5

Example1

FIGURE4 (a): Sports Image.

FIGURE4 (b): Data Embedded Image.

Fig (a) shows the original sports image the data is embedded in it. Fig (b) shows the data embedded in the image. It should be noted that original sports image and data embedded sports image are exactly same.

Secret data used in our method is shown below", using steganography (way of hiding data) and SBR algorithm, we can 100% detect the guilty agent. Here Stego key used in this algorithm, Is as USERNAME (which is Unique).

In this, Guilty agent leaks the sports news from the BNN news channel, this agent name is ashwini.

Using proposed method the admin detect this agent as shown below,

"sports_INDASHWINI", So here guilty agent is "ASHWINI."
Example2

FIGURE5 (a):Hindi_news Image.

FIGURE5 (b): Data Embedded Image.

Fig (a) shows the original hindi_news image the data is embedded in it. Fig (b) shows the data embedded in the image. It should be noted that original hindi_news image and data embedded sports image are exactly same.

Secret data used in our method is shown below", using steganography (way of hiding data) and SBR algorithm, we can 100% detect the guilty agent. Here Stego key used in this algorithm, Is as USERNAME (which is Unique).

In this, Guilty agent leaks the sports news from the BNN news channel, this agent name is JOHN Using proposed method the admin detect this agent as shown below,

"Hindi_newsJOHN",So here guilty agent is "JOHN."

Minimum distortions take place in data embedded image due to embedding small amount of data using proposed method. the results shows that the proposed method is much more secure than LSB.

5. CONCLUSION

The proposed algorithm used in this paper, encrypts the secret data before embedding it in the image file with minimum distortions. We have also used an compression technique. We have developed system in java based on proposed algorithm.

Here we have tested several JPEG images with secret data hidden and we can concluded that resulting data embedded image do not have any noticeable changes.

This method is essential for construction of accurate targeted and blind steganalysis methods for JPEG, BMP and PNG images. In this paper we have identified the use the concept of SBR hide the given secret data into the image file.

6. REFERENCES

[1] A.E.Mustafa, A A. M.Elgamal, M.E.Elami, Ahmad bd, "A proposed Algorithm For Steganography in Digital image Based On LSB"Research Journal Specific Education Faculty of specific Education, MansouraUniversity, Issue no. 21, April. 2011.

[2] Vijay Kumar Sharma, Vishal Shrivastava'Steganography algorithms for hiding image in image by improved lsb substitution by minimize detection ',in Journal of Theoretical and applied Information Technology15th February 2012. Vol. 36 No.1.

[3] Alain, C. Brainos, A Study of Steganography and the Art of Hiding Information, East Carolina

university.

[4] Desoky, A. (2009):A novel Noiseless Steganography paradigm, Ph.D., Department of Computer Science and electrical engineering, Faculty of the Graduate School, university of Maryland, Baltimore County.

[5] Christopher, T. (2007): Compression Aided feature Based steganalysis of Perturbed Quantization steganography in Jpeg image, M.Sc. s, Department of science in Electrical and Computer Engineering, University of Delaware.

[6] Xiang-yang, L. , Dao-shun., Ping, W., Fen-lin, L.((2008): a review on Blind Detection for Image Steganography, journal of Signal Processing, Vol(88),Issue(9).

[7] Samer, A.(2006):A New Algorithm for Hiding Gray Images using Blocks, Information , Security Journal, The hashemite University, Jordan, Volume (15), Issue (6).

[8] Kaushal M. Solanki, 2005, Multimedia Data Hiding: From fundamental Issues to Practical Techniques, PhD, electrical and Computer Engineering, university of california, Santa Barbara.

[9] Sanjeev, M.et.al (2008): Customized and Secure Image Steganography, Journal of Signal Processing, Vol (1), Issue (1).

[10] Hengfu, Y., Xingming S., Guang S(2009): A High- capacity Image Data Hiding Scheme Using adaptive LSB substitution, Journal of radio engineering, vOL. (18), NO. (4).

[11] Lee, L.(2004) :LSB Steganography :Information within Information, Journal of Computer Science, Vol (265), N(5).

[12] Amirthanjan, R.Akila, R & Deepika chowdavarapu,a Comparative Analysis of Image steganography', 2010.

[13] Bandyopadhyay, S.K., 2010. An Alternative Approach of Steganography Using Reference Image.international Journal of Advancements in Technology, 1(1), pp.05-11.

[14] Kaur, R. Dhir, & G. Sikka. (2009). A new image steganography based on first component alteration technique. International Journal of Computer Science and Information Security (IJCSIS), 6, 53-56.

[15] TMorkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the fifth Annual Information Security South Africa Conference,(ISSA2005), Sandton, South Africa, june/July 2005.

[16] Robert Krenn, " Steganography and steganalysis", Internet Publication, March 2004.

[17] Johnson, N.F. & Jajodia, S., ''Exploring Steganography: Seeing the Unseen'', Computer Journal, February 1998.

[18] Petit colas, Fabien A.P., ''Information Hiding: Techniques for Steganography and Digital Watermarking.'', 2000.

[19] Alain, C. Brainos, A Study Of Steganography And The Art Of Hiding Information, East Carolina University.

[20] J.L.Dugelay and S.Roche, ''Information Hiding: Techniques for Steganography and Digital Watermarking'', S.Katzenbeisser and F.A.P.Petitcolas (eds.), Norwood, MA: Artech

House, pp. 121-148,

[21] Ajanthaa lakkshmann, Puja u.dharia, Fairy Gandhi, An adaptive image steganography technique using LSB and MSB international research journals V3, n1, 2013, ISSN 1839-6518.

[22] Jain, Sachin Mesh ram, Shikha Dubey, Image Steganography Using LSB and Edge detection Technique", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231- 2307, Volume-2, Issue-3, July 2012.

[23] TMorkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005.

[24] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.

[25] Yang, C.-H.: 'Inverted pattern approach to improve image quality of information hiding by LSB Substitution', 2008.