IJCAT International Journal of Computing and Technology, Volume 1, Issue 3, April 2014
ISSN : 2348 - 6090
www.IJCAT.org

Extracting Spread-Spectrum Hidden Data from an Image

[1] Ms. Komal B.Bijwe, [2] Dr.G.R.Bamnote

[1,2] Department Of Computer Sci. & Engg
PRMIT,Badnera,Amravati-444604 (M.H)

Abstract - In this paper, we present a novel high bit rate LSB Image data hiding method. The basic idea of the proposed LSB algorithm is data embedding that causes minimal embedding distortion of the host image. Using the proposed two-step algorithm, data hiding bits are embedded into higher LSB layers, resulting in increased robustness against noise addition or image compression. Listening tests showed that the perceptual quality of data hided image is higher in the case of the proposed method than in the standard LSB method.

Keywords **- Higher LSB, Guard Pixels, Stegnography, Multi- carrier, Information hiding,Data Encryption.**

1. Introduction

Steganography 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. The power of steganography is in hiding the secret message by obscurity, hiding its existence in a non-secret file. In that sense, steganography is different from cryptography, which involves making the content of the secret message unreadable while not preventing non-intended observers from learning about its existence1.

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 steganographic 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.

Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication to hide a message from a third party. Steganography 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 Steganography 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. Steganography 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. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them. Generally, in steganography, the actual information is not maintained in its original format and thereby 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 steganography. A good example of this is the relationship between are 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 steganographically embedded into the larger one without impacting the quality. Important domains, besides classic computing, where steganography can be applied are domains using mobil and embedded devices especially mobile phones. In this project we state the fact that steganography can be successfully implemented and used into a next generation of computing technology with image and video processing abilities. The LSB method used for this project which satisfies the requirement of steganogaphy protocols. This research will include implementation of steganographic algorithm for encoding data inside video files, as well as technique to dynamically extract that data as original.

2. Literature Survey

Tung-Hsiang Liu and *Long-Wen Chang* [1] has proposed a simple data hiding technique for binary images in *2004*.The proposed method embeds secure data at the edge portion of host binary image. The Distance matrix mechanism is used to find the edge pixels of host binary image. Then the Weight mechanism is used to consider the connectivity of the neighborhood around changeable pixels for choosing the most suitable one. For the security and quality consideration, a random number generator is used to distribute the embedding data into the overall image. This method not only embeds large amounts of data into host binary image but also can maintain image quality.

In order to improve the capacity of the hidden secret data and to provide am imperceptible stego image quality *H.-C. Wu, N.-I. Wu, C.-S. Tsai* and *M.-S. Hwang* [2] has proposed a novel stenographic method based on Least Significant Bit (LSB) Replacement and Pixel Value Differencing (PVD) methods in *2005*.Pixel Value Differencing (PVD) method is used to discriminate between edge areas and smooth areas of cover image. The secret data is hidden into the smooth areas of cover image by LSB method while using the PVD method in the edge areas. As, the proposed method not only store data in the edge areas but also in the smooth areas; therefore it can hide much larger information and maintains a good visual quality of stego image.

In *2005 M. Carli M.C.Q. Fariasy, E. Drelie Gelascaz, R. Tedesco & A. Neri* [3] has proposed a no-reference video quality metric that blindly estimates the quality of a video. They had used Block based Spread Spectrum embedding method to insert a fragile mark into perceptually important areas of the video frames. They used a set of perceptual features to characterize the perceptual importance of a region that are Motion, Contrast and Color. The mark is extracted from the perceptually important areas of the decoded video on receiver side. Then a quality measure of the video is obtained by computing the degradation of the extracted mark. So, in this way quality of a compressed video is estimated by using simple embedding system on perceptually important areas of the video frame. In *2007 Hsien-Wen Tseng, Feng-Rong Wu*, and *Chi-Pin Hsieh* [4] has proposed a novel method for hiding data in binary images. A Weight mechanism is used to select the most suitable pixel for flipping. Additionally boundary check is performed to improve the visual quality of stego image as well as to prevent boundary distortion. This method achieved a good visual quality for watermarked image and has high capacity of embedding.

In *2008 Beenish Mehboob* and *Rashid Aziz Faruqui* [5] discussedthe art and science of Steganography in general and proposed a novel technique to hide data in a colorful image using least significant bit. Least Significant Bit or its variants are used to hide data in digital image. This technique chops the data in 8 bits after the header and used LSB to hide data. So, they proved LSB method is the most recommended for hiding data than other techniques which require masking and filtering.

M.B. Ould Medeniand & El Mamoun Souidi [6] has proposed a novel stenographic method for gray level images on four pixel differencing and LSB substitution in *2010*.They used K-bit LSB substitution method for hiding the secret data into each pixel where K is decided by the number of one in the most part of pixel. This method gave best values for the PSNR measure which means that there were no big difference between the original and the stegno image. In *2012 Tasnuva Mahjabin,Syed Monowar Hossain* and *Md. Shariful Haque* [7] has proposed a data hiding method based on PVD and LSB substitution to improve the capacity of the secret data as well as to make stegnalysis a complicated task they made an effort to implement a robust dynamic method of data hiding. An efficient and dynamic embedding algorithm was proposed here that not only hides secret data with an imperceptible visual quality and increased capacity but also make secret code breaking a good annoyance for the attacker. This method achieved an increased embedding capacity and lower image degradation with improved security as compared to LSB substitution method and some other existing methods of data hiding.

Ankit Chaudhary and *JaJdeep Vasavada* [8] has proposed an improved stenography approach for hiding text messages in RGB lossless images in *2012*.The security level is increased by randomly distributing the text message over the entire image instead of clustering within specific image portions. They increased storage capacity by utilizing all the color channels for storing information and providing the source text message compression. The degradation of the images can be minimized by changing only one lease significant bit per color channel for hiding the message, incurring a very

little change in the original image. So, this method increased the security level and improved the storage capacity while incurring minimal quality degradation.

Kousik Dasgupta & J.K. MandalandParamartha Dutta [9] have proposed a secured has based LSB technique for video stenography in *2012*.This technique utilizes cover video files in spatial domain to conceal the presence of sensitive data regardless of its format. After comparing the proposed technique with LSB technique it is found that the performance analysis of proposed technique is quite encouraging. The advantage of this method is that the size of the message does not matter in video stenography as the message can be embedded in multiple frames.

In *2012 Poonam V Bodhak* and *Baisa L Gunjal* [10] has proposed a method to hide data containing text in computer video file and to retrieve the hidden information. This can be designed by embedding the text file in a video file in such a way that the video does not lose its functionality using DCT & LSB Modification method. This method applies imperceptible modification. This proposed method strives for high security to an eavesdropper's inability to detect hidden information.

RigDas and *Themrichon Tuithung* [11] have proposed novel technique for image stenography based on Huffman Encoding in *2012*. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret Image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of the Huffman encoded bit stream and Huffman Table are also embedded inside the cover image, so that the Stego-Image becomes standalone information to the receiver.

In *2013 Ming Li,Michel K. Kulhandjian, Dimitris,A. Pados,,Stella N. Batalama,* and *Michael J. Medley* [12] has considered the problem of extracting blindly data embedded over a wide band in a spectrum (transform) domain of a digital medium (image, audio, video).We develop a novel multicarrier/signature iterative generalized least-squares (M-IGLS) core procedure to seek unknown data hidden in hosts via multicarrier spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available.

3. Proposed Methodology

3.1. Algorithms

Data Hiding:-

1. Select an Image
2. Split an Image into multi-carrier objects.
3. Select a multi-carrier image.
4. Select Secrete data for hiding.
5. Encrypt data with Shifting method
6. Split data into equal number of carrier objects.
7. Apply Higher LSB Method for replacing pixels bits with encrypted data bits by taking one multicarrier image object & secret data segment.
8. Repeat Step 3 & Step 7 until all encrypted data segments not hidden into multi carrier images.
9. Join multi carrier's objects to create single image.
10. Stop

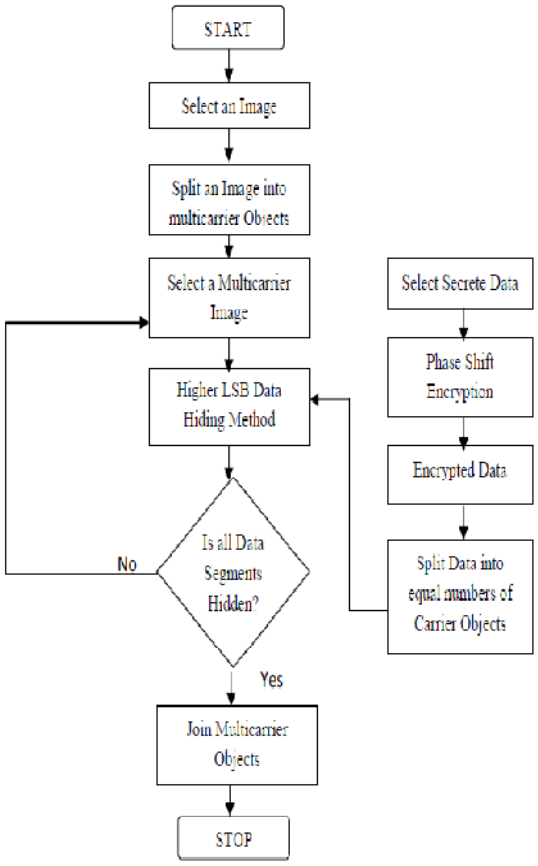


Fig 1: Data Hiding in an Image

Data Extraction:-

1. Select a Stego Image.
2. Split stego Image.
3. Apply Higher LSB Extraction algorithm.
4. Select length Key.
5. Extract data bits from 1 to 5 LSB color pixels bits.
6. Generate Data.
7. Decrypt Data.
8. Stop

3.3 Selection of Guard Pixels Region

Problem may occurred for loss of secrete information when we join multi carrier images with selection of proper guard pixels region.

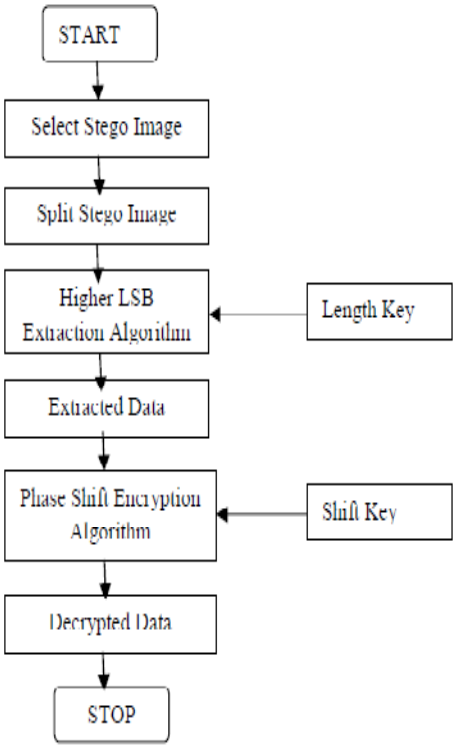


Fig 2: Data Extraction Form Image

3.2 Splitting Carrier Image into Multi Carrier Objects

In a Proposed Method, We split a carrier image as shown below

Fig 3: Original Image with its Four Multi Carrier Objects

Carrier object can be represented with

$$Im = \int_1^2 (O1 + O2)\ ) \ || \int_3^4 (O3 + O4) \quad (1)$$

Where,

O1,O2,O3,O4 =Image Objects

|| =Veritcal Join

+=Horizontal Join

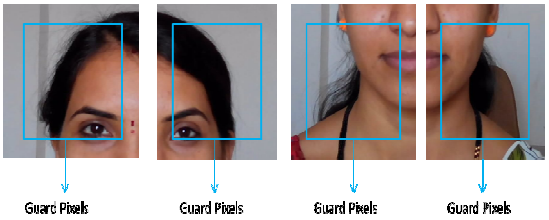


Fig 4: Guard Pixel Region in each Carrier Objects

We avoid mutual collison between two objects at their boundry lines. Thus guard pixels region of an indivisual object can be represented with

$$Gpx = (H - 2)X(W - 2) \quad (2)$$

Where

H=Height of an Object Image

W=Width of an Object Image

Over all guard pixels region can be represented with an equation

Initially *Gp=0*

$$Gp = Gp + \sum_{i=1}^{4} Gpi \quad (3)$$

Where,

Gp=Over all guard pixels count.

Gpi=Individual guard pixels count.

3.4 Higher LSB Method for Data Embedding.

We proposed a novel method for data hiding that achieves high data hiding capacity along with great robustness. Let Consider as shown

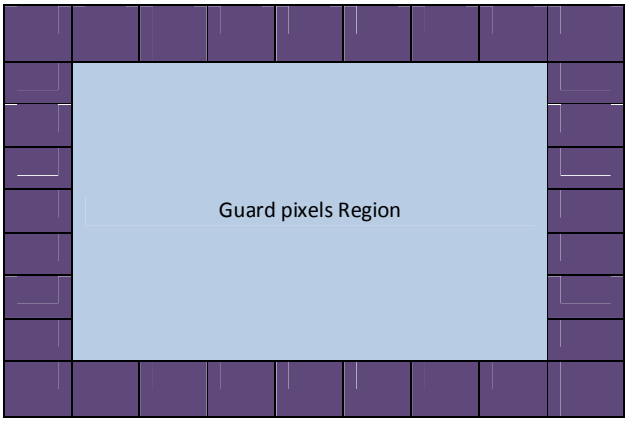


Fig 5: Images with Pixels Block

An individual pixel is represented with 24 Bits in RGB format as shown

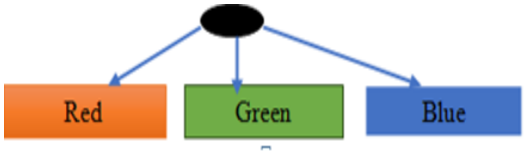
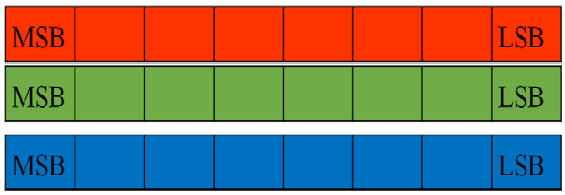


Fig 6: Pixels with Red, Green & Blue component

In above shown diagram, each color component is represented with 8 bits pixels as



In proposed methodology, we replace 5 bits from LSB side with data bits as shown

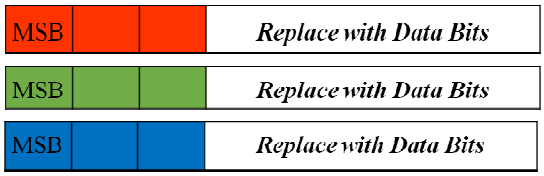


Fig 7: Replacing 5 LSB bits of Red,Green & Blue component

Thus total data hiding capacity in terms of bits is represented with

$$Hc = Gp * 15 \quad (4)$$

Where

Hc=Data Hiding Capacity

Through proposed method, quantization error of 32 occurs which may affect image intensity but preserves inns' quality.

Higher LSB Algorithm

Step1:Select Pixels.
Step 2:Select R,G,B componants.
Step 3: if ((R + 32)>255) ||(R-32)<0), ((G + 32)>255) || (G-32)<0), ((B + 32)>255) ||(B-32)<0), then descard pixel componants else replace its 5 LSB side bits with data bits.
Step 4: Repeat step 2 to 3 until all guard pixel region not scanned.
Step 5:Stop

Table 1. Data Hiding Result

Sr. No	Image Size	Guard Region Size	Data bits	Data Hided	Result Image Size	PSNR
1	100 X 100	96 X 96	500	√	100 X 100	70.57
2	150 X 150	146 X 146	500	√	150 X 150	75.2143
3	200 X 200	196 X 196	500	√	200 X 200	80.237
4	250 X 250	246 X 246	500	√	250 X 250	67.2382
5	300 X 300	296 X 296	500	√	300 X 300	76.2342

Table.2 .Data Hiding Result (Change in data hiding bits quantity)

Sr. No	Image Size	Guard Region Size	Data bits	Data Hided	Result Image Size	PSNR
1	100 X 100	96 X 96	500	√	100 X 100	65.57
2	150 X 150	146 X 146	1000	√	150 X 150	71.234
3	200 X 200	196 X 196	1500	√	200 X 200	79.1231
4	250 X 250	246 X 246	2000	√	250 X 250	61.2342
5	300 X 300	296 X 296	2500	√	300 X 300	72.345

4. Conclusion

We presented a reduced distortion algorithm for LSB image steganography. The key idea of the algorithm is data hiding bit embedding that causes minimal embedding distortion of the host image. visualisation tests showed that described algorithm succeeds in increasing the depth of the embedding layer from 1th to 5LSBlayer without affecting the perceptual transparency of the data hided image signal. The improvement in robustness in presence of additive noise is obvious, as the proposed algorithm obtains significantly lower bit error rates than the standard algorithm. The steganalysis of the proposed algorithm is more challenging as well, because there is a significant cryptography provided for data security.

References

[1] Tung-Hsiang Liu and Long-Wen Chang, "An Adaptive Data Hiding Technique for Binary Images", *Proc.IEEE 17th Int.Conf. On Pattern Recognition (ICPR'04)* 2004.

[2] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang," Image steganographic scheme based on pixel-value differencing and LSB replacement methods", *IEE Proc.-Vis. Image Signal Process.*, Vol. 152, No. 5, October 2005.

[3] M. Carli , M.C.Q. Fariasy, E. Drelie Gelascaz, R. Tedesco, A. Neri, "QUALITY ASSESSMENT USING DATA HIDING ON PERCEPTUALLY IMPORTANT" *IEEE* AREAS0-7803-9134-9/05/$20.00 ©2005.

[4] Hsien-Wen Tseng, Feng-Rong Wu,and Chi-Pin Hsieh," Data Hiding for Binary Images Using Weight Mechanism",*IEEE* 2007.

[5] Beenish Mehboob and Rashid Aziz Faruqui," A StegnographyImplementation", *IEEE* 2008

[6] M.B. Ould MEDENI, El Mamoun SOUIDI," A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution "*IEEE* 2010

[7] Tasnuva Mahjabin, Syed Monowar Hossain, Md. Shariful Haque," A Block Based Data Hiding Method in Images Using Pixel Value Differencing and LSB Substitution Method", *IEEE* 2012.

[8] Ankit Chaudhary, JaJdeep Vasavada,"A Hash Based Approach for Secure Keyless
Image Steganography in Lossless RGBImages" , *IEEE* 2012.

[9] Kousik Dasgupta1, J.K. Mandal2 and Paramartha Dutta3," HASH BASED LEAST SIGNIFICANT BIT TECHNIQUE FOR VIDEO STEGANOGRAPHY (HLSB)", *International Journal of Security, Privacy and Trust Management (IJSPTM)*, Vol. 1, No 2, April 2012.

[10] Poonam V Bodhak, Baisa L Gunjal," Improved Protection In Video Steganography Using DCT & LSB", *International Journal of Engineering and Innovative Technology (IJEIT)* Volume 1, Issue 4, April 2012.

[11] RigDas, Themrichon Tuithung," A Novel Steganography Method for Image Based on Huffman Encoding", *IEEE* 2012.

[12] Ming Li, Michel K. Kulhandjian, Dimitris A. Pados, Stella N. Batalama, and Michael J. Medley," Extracting Spread-Spectrum Hidden Data From Digital Media", *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,* VOL. 8, NO. 7, JULY 2013.

Ms.Komal B.Bijwe received B.E in Computer Science & Engineering From H.V.P.M College of Engineering & Technology, Amravati; in 2007 and pursuing M.E in Computer Science & Engineering From Prof.Ram Meghe Institute of Technology & Research, Bandera, Amravati.

Prof.Dr.G.R.Bamnote received PhD in Computer Science & Engineering in 2009. He is now working as a Head of Department (CSE) in Prof.Ram Meghe Institute of Technology & Research, Bandera, Amravati.