Proficient Evaluation and Implementation of LSB Based Image Steganography

Deeksha Manjunath, Avani K V H, Rashmi Pai K and C.Gururaj

Abstract.

Abstract— Steganography is the craft of covering the way that correspondence is occurring by encasing information in different information. There are an assortment of transporter record types accessible, yet advanced photographs are the most utilized because of their pervasiveness on the Internet. There are a few distinctive steganographic procedures for concealing secret data in photos, some of which are more troublesome than others and all of which have their own qualities and shortcomings. The steganography strategy used for various applications has changed requirements. A few applications, for instance, may require total imperceptibility of the restricted data, while others might require the disguise of a greater mystery message. Picture Steganography is one such course of disguising data in a cover picture, which may be text, picture, or video.

Keywords- Image Steganography, Least Significant Bit, Data Hiding

1. INTRODUCTION

Image Steganography refers back to the procedure of hiding information inside an photograph file.The image chosen for this design is called the cover image, and the image taken later for steganography (data hiding) is called the steganographic image. It can be carried out in two major steps. In particular, it can be divided into an embedding phase, which hides information in the image (cover) using appropriate calculations and a mysterious key, and an extraction phase, where information is entered. It is extracted from the changed image. It uses a mysterious key to use the opposite calculation. When the stego picture is communicated, it could be plausible that the stego picture gets debased when a third individual captures this picture.

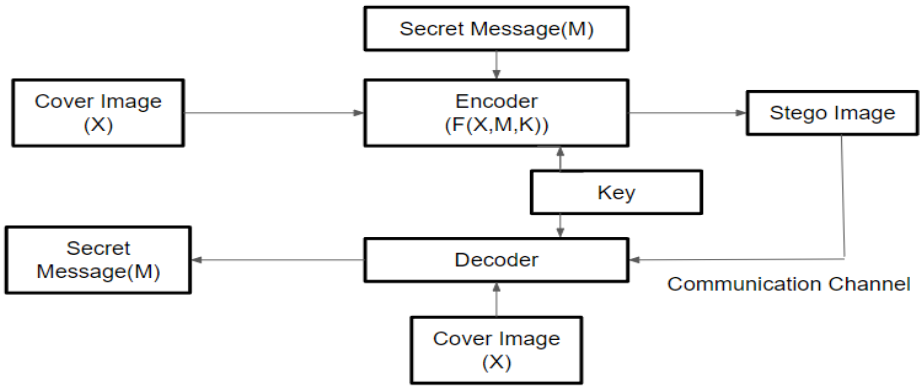

Fig 1: Block diagram of Image Steganography

The fundamental advances associated with picture steganography are displayed in the graph above. The mysterious message or information (X), the cover picture (M) and the mysterious key (K) picked are taken care of to the picture steganography calculation whose capacity is addressed as f(X,M,K). The result of this calculation is an adjusted picture containing the information (stowed away). This altered picture is then communicated to the collector who interprets the got picture with a vital K to separate the information that was covered up.[1]

During the plan of an information concealing framework or picture steganography calculation there are a couple of elements that must be thought of. The elements are subtlety, security, limit or payload, strength and implanting intricacy.

Imperceptibility is the ability of a related technology to transmit data without being seen by humans. If a third party intercepts the image file, the security service determines the resistance of the technology (to prevent third parties from tampering with the image). How much information that can be concealed in the cover picture by the calculation without rolling out the improvements perceptible is characterized by payload or limit. The capacity of the information that is concealed to stay unaltered in any event, when the stego picture is altered by activities like straight or non-direct separating, editing, honing or obscuring, pressure and so forth is characterized by Robustness of the calculation. Embedding complexity measures how complex the algorithm is.

2. BENEFITS AND DOWNSIDES OF LSB BASED IMAGE STEGANOGRAPHY

BENEFITS:

This strategy is exceptionally quick and effectively implementable contrasted with different methodologies of picture steganography.

The difference between information and encoded image is negligible.

Rather than implanting the data in just the LSB, we can insert the data in the last two LSBs, along these lines installing much bigger mystery messages.

This technique frames the establishment for other complex calculations.

DRAWBACKS:

LSB based encoding the information is frail as it tends to be handily decoded taking the LSBs of the picture and acquiring the mysterious message in its double structure.

This strategy is old and out of date and other better encryption techniques have been created.

While inserting the mysterious message in more than one LSB, the picture quality decreases relying upon the number of pixels that have changed.

3. IMAGE STEGANOGRAPHY AND ITS TYPES

Image steganography is classified into two categories: Spatial space information stowing away and Transform area information stowing away. Spatial area strategies use procedures dependent on basic controls which create spaces in the cover picture to conceal privileged information where changes can't be effectively distinguished. While in Transform space procedure [9], the pixel esteems in spatial area are changed over into recurrence space esteems by performing two layered changes [11]. The recurrence area esteems or coefficients changed by the restricted information are utilized to conceal the information. Most transform domain techniques are developed from spatial domain approaches.

Spatial domain image steganography can be classified into six categories as mentioned below[5].

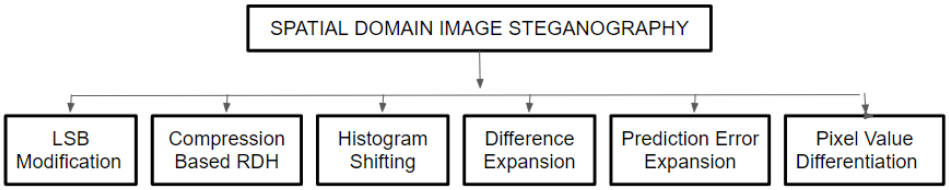

Fig 2: Types of Spatial Domain Image Steganography

LSB Modification: It is a method in which the least extended bit of each pixel in the image is replaced with the message bit intended to be hidden.

Compression based RDH (Reversible Data Hiding): This technique is performed on the bit planes of the cover image to create a gap to cover the data.

Histogram Shifting: This approximation is obtained by taking into account the histogram of the image. Adjusts all pixel values between the peak and null positions, creating enough space to hide the data.

Difference Expansion: This approach relies on the image's redundancy. The disparity between neighbouring pixels is increased, and the data is buried in the resulting space.

Pixel Value Differentiating: The difference between successive pixels in a block determines the number of bits of data to be buried (The cover image is divided into pixel blocks that do not overlap).[2]

Prediction Error Expansion: This approach combines differential expansion with histogram shifting.

Transform Domain Types:

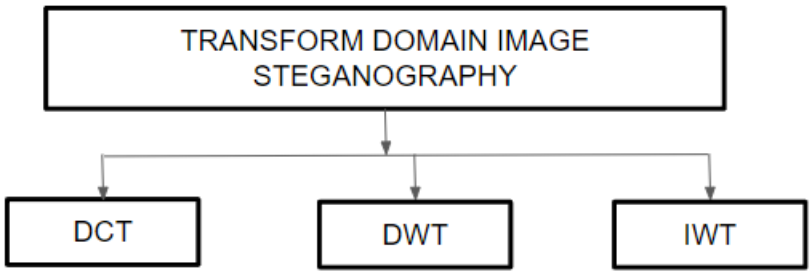

Fig 3: Classification of Transform Domain Types

DCT (Discrete Cosine Transform): DCT is an important aspect of image processing as it helps in JPEG compression. DCT transforms the spatial intensity of pixels into alternating current (AC) and direct current (DC) coefficients, which is the basis for this technology .

DWT (Discrete Wavelet Transform): It simultaneously provides image information in both the spatial and frequency domains [8] LSB or HS-based approaches can be used to implement DWT. Data bits are stored in the LSB position of the quantized coefficients of the DWT sub band when implemented using LSB. The coefficients of the histogram change based on the data bits when HS is used.

IWT (Integer Wavelet Transform): The lift system converts information about the pixels of the spatial domain into values in the frequency domain. The lifting strategy is based on computed averages and differences for pairings.

A combination of algorithms [10] can be used to design an algorithm appropriate for the application which depends on the factors described above.

4. LEAST SIGNIFICANT BIT

LSB strategy is a spatial area procedure as the calculation is applied straightforwardly on the spatial space pixel esteems. One of the principle reasons regarding the reason why we decided to perform information concealing utilizing LSB philosophy is a direct result of the speed of execution of this procedure. It's a lot quicker than a large portion of the other picture steganography strategies.

This technique depends on adjusting the last piece[6]. The last piece doesn't convey a ton of content and transforming it won't make a big deal about a distinction[7]. Since changing the last piece doesn't have a significant result it does regularly and consequently can be called as a high recurrence part

In this technique since just the most un-critical piece is adjusted, it is very helpless because of which an extra advance is performed – the crude information is encoded and afterward taken care of to the picture steganography calculation. This extra advance may be tedious however is a fundamental stage to work on the security of the privileged information. This technique is a simple to carry out strategy as it includes supplanting just the last piece of the multitude of pixels of the cover picture or a couple by the scrambled message bits.

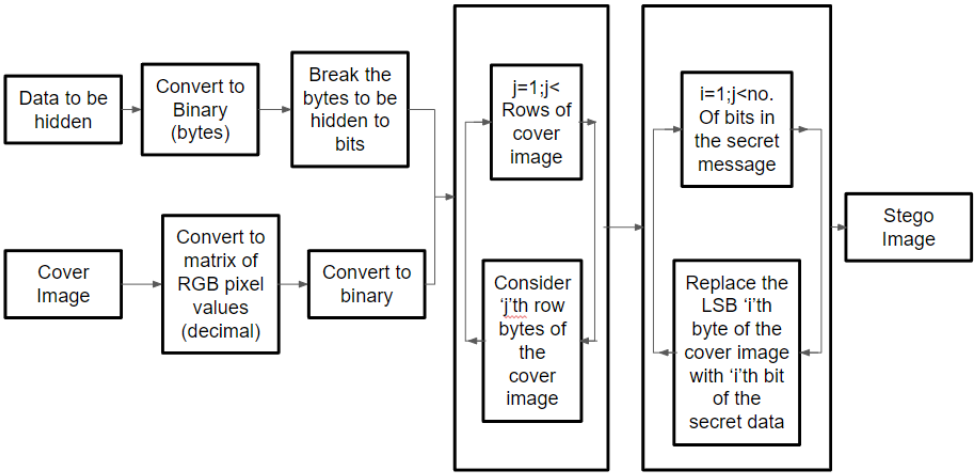

Fig 4: Block Diagram for LSB based Image Steganography

5. EVALUATION METRICS

Bit Error Rate (BER): This performance metric compares the two photos to see how big of a change there is by comparing the bits in the stego picture to the bits in the cover image in the received image

Bit error rate=BE/BC

BC – The total number of bits included inside the grayscale cover picture.

BE – The total amount of bits differing from that of the stego picture.

The bit error rate ranges from 0 to 1, with 0 indicating that the stego image is identical to the cover image and 1 indicating that the brightness of the stego image is significantly different from the cover image.

Mean Square error: Calculates the average squared difference between the estimated and actual values. In this case, the estimated picture is the stego image, while the real image is the cover image.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(Y_i - \hat{Y}_i)^2 \qquad \text{(Eq.1)}$$

Peak Signal-to-noise ratio (PSNR): This ratio is used to compare the quality of an original and a compressed picture. The greater the PSNR, the higher the quality of the compressed or rebuilt image.[4]

$$PSNR = 10 \times log_{10}(\frac{I_{Cmax}^2}{MSE})\ dB$$

(Eq.2)

Icmax – The cover image's maximum pixel value

MSE – Mean square error

Histogram Analysis: A comparison of the stego image histogram and the cover image histogram is performed. If they are comparable, it indicates that the method utilised is effective.

Structural Similarity Index (SSIM): This approach is used to detect similarities between the cover picture and the stego image. As it assesses picture deterioration induced by image processing processes, this method is said to be perceptual.[3]

$$SSIM(I_c, I_s) = \frac{(2\mu_{I_c}\mu_{I_s} + k_1)(2\sigma_{I_cI_s} + k_2)}{(\mu_{I_c}^2 + \mu_{I_s}^2 + k_1)(\sigma_{I_c}^2 + \sigma_{I_s}^2 + k_2)}$$

(Eq.3)

6. RESULTS

A simple interactive interface (shown in fig 5) is created with 2 options:

1) to encode any text message to an image

2) to decode any text message from an image.

On choosing the option to encode, the user is asked to upload the text that has to be hidden and the image in which it is to be hidden (an example of this is shown in fig 5).

The decoding procedure can be performed by uploading the encoded image to obtain the original text message (shown fig 6)

```
--LSB Image Steganography--
1: Encode
2: Decode
1
Enter Source Image Path
rashmi.jpeg
```

```
Enter Message to Hide
Steganography is the practice of concealing a message wi
oncealment of information within computer files. In digi
coding inside of a transport layer, such as a document f
ographic transmission because of their large size. For e
e color of every hundredth pixel to correspond to a lett
cifically looking for it is unlikely to notice the chang
Enter Destination Image Path
rashmiencoded.png
Encoding...
Image Encoded Successfully
```

Fig 5: Encoding the hidden message into the Source Image

```
--LSB Image Steganography--
1: Encode
2: Decode
2
Enter Source Image Path
rashmiencoded.png
Decoding...
Hidden Message: Steganography is the practice of concealing a
y includes the concealment of information within computer file
e steganographic coding inside of a transport layer, such as a
ideal for steganographic transmission because of their large s
le and adjust the color of every hundredth pixel to correspond
e who is not specifically looking for it is unlikely to notice
```

Fig 6: Decoding the Source Image to access the concealed text

Below are the Mean Square Error (MSE) and Structural Similarity Index (SSIM) values.

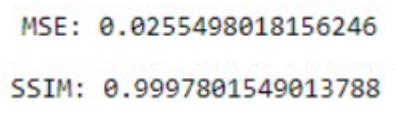

Fig 7: MSE and SSIM values

7. FUTURE SCOPE

Increased integration should be pursued while retaining anonymity. Using this technique, we can hide a text file the size of an image. Text files larger than images should be hidden. The secret key must be known to both the sender and the recipient. There are no keys on the lid, they must be prepared separately. You can create a system to secretly create and release these keys. If you need additional security, you can use the domain transfer technique. Steganography in combination with cryptography offers an incomparable technique to protect communication networks.

ACKNOWLEDGMENT

We wish to express our sincere acknowledgement to management, B.M.S. College of Engineering for sponsoring this work.

REFERENCES

[1] Mohammed A. Saleh, Image Steganography Techniques - A Review Paper, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 7, Issue 9, September 2018. https://ijarcce.com/wp-content/uploads/2018/10/IJARCCE.2018.7910.pdf

[2] Hsien-Wen Tseng, Hui-Shih Leng, "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number", Journal of Applied Mathematics, vol. 2013, Article ID 189706, 8 pages, 2013. https://doi.org/10.1155/2013/189706

[3] Stoyanova V, Tasheva Zh, Research of the characteristics of a steganography algorithm based on LSB method of embedded information in images, International Scientific Journal "Machines. Technologies. Materials." https://stumejournals.com/journals/mtm/2015/7/65.full.pdf

[4] Priyandanu Filzasavitra, Tito Waluyo Purboyo and Randy Erfa Saputra, 2019. Analysis of Steganography on PNG Image using Least Significant Bit (LSB), Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE), Journal of Engineering and Applied Sciences, Year : 2019 Volume: 14 Issue: 21 Page No. 7821 - 7827 DOI: 10.36478/jeasci.2019.7821.7827

[5] Ahmad Shaik, V. Thanikaiselvan and Rengarajan Amitharajan, 2017. Data Security Through Data Hiding in Images: A Review Journal of Artificial Intelligence,
Year: 2017 Volume: 10 Issue: 1 Page No.: 1-21 DOI: 10.3923/jai.2017.1.21

[6] [6] K. Thangadurai and G. Sudha Devi, "An analysis of LSB based image steganography techniques," 2014 International Conference on Computer Communication and Informatics, 2014, pp. 1-4, doi: 10.1109/ICCCI.2014.6921751

[7] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia,"Application of LSB Based Steganographic Technique for 8-bit Color Images, World Academy of Science, Engineering and Technology, 2009. 38. 427-429.

[8] Veena Nayak, Sushma P.Holla, AkshayaKumar K. M., C. Gururaj, "Automatic number plate recognition", International Journal of Advanced Trends in Computer Science and Engineering, Vol.9, No. 3, pp 3783 – 3787, ISSN 2278-3091, May – June 2020, DOI: 10.30534/ijatcse/2020/195932020

[9] C Gururaj, Satish Tunga, "AI based Feature Extraction through Content Based Image Retrieval",Journal of Computational and Theoretical Nanoscience, February 2020, volume 17, Issue 9-10, pp.4097-4101, ISSN: 1546-1955 (Print): EISSN: 1546-1963 (Online), DOI: 10.1166/jctn.2020.9018

[10] Maneesha K, Neha Shree, Pranav Datta R, Sindhu S K, C.Gururaj, "Real Time Face Detection Robot", 2nd IEEE International Conference on Recent Trends in Electronics, Information &Communication Technology (RTEICT-2017), ISBN: 978-1-5090-3704-9,19 th – 20 th May 2017 , pp 58-64, SVCE, Bengaluru. DOI: 10.1109/RTEICT.2017.8256558

[11] V Meghana, Manasa Suresh, S Sandhya, R Aparna, C Gururaj, "SoC implementation of network intrusion detection using counting bloom filter", IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology (RTEICT-2016), ISBN: 978-1-5090-0774-5,20 th – 21 st May 2016 , pp 1846-1850, SVCE, Bengaluru. DOI: 10.1109 / RTEICT .2016.7808154

BIOGRAPHIES

Deeksha Manjunath is pursuing her Bachelor's degree in telecommunication engineering from B.M.S. College of Engineering. Her research areas include digital signal processing and image processing. She extends her interest in the field of machine learning and deep learning.

Avani K V H is pursuing her Bachelor's of Engineering undergraduate degree in Electronics and Telecommunication Engineering from B.M.S. College of Engineering, Bangalore. She will be graduating in 2022. Her areas of research include Image processing, Cryptography, Digital Electronics, Machine Learning and Deep Learning.

Rashmi Pai K is pursuing her Bachelor's of Engineering undergraduate degree in Electronics and Communication Engineering at B.M.S. College of Engineering. She is very interested in signal processing, digital and analogue electronics. She is also fascinated with image processing, machine learning, and blockchain.

Dr. C Gururaj received his B.E. degree in Electronics and Communication and MTech degree in Electronics, both from Visvesvaraya Technological University, Belagavi his PhD from Jain University, Bengaluru. He is currently working in the department of Electronics and Telecommunication Engineering, BMS College of Engineering, Bengaluru. He has more than 50 publications to his credit with high citations that are indexed in portals such as Scopus, Web of Science, Google scholar, Vidwan etc. He has received multiple awards and grants throughout his 18 years career. His areas of interest are Image Processing, VLSI Design, Machine Learning, Deep Learning, Artificial Intelligence and Engineering Education