Image Steganography based on Histogram Shifting

*Meghana, #Umesh D R

*Student M.tech, #Associate Professor, PES College of Engineering, Mandya, India,

*meghanamahadev22@gmail.com, #umesh.dr.pesce@gmail.com

Abstract: **Image steganography is a sub division of steganography where a secret information is hidden inside an image. In steganography, quality, capacity and time taken to embed the secret data inside an image are important factors. The quality of the images depends on the algorithms implemented for steganography. Here in the paper, we implement different algorithms for different operation like dividing the images into blocks and finding the best blocks to hide the secrete data, we generate histograms for each blocks which is bookmarked and later used to extract the secret data. After extraction, enhancement techniques are implemented to enhance the extracted secret data. Our proposed method is more efficient and requires less time for embedding process.**

Keywords — ***Embedding, Enhancement, Extraction, Histogram, Secret data, Steganography***.

I. Introduction

In today's world, communication is one of the necessity that everyone wants to send message from one location to another. Here privacy and security of the message matters to certain levels. In order to protect the data from intruders two techniques can be used they are, cryptography and steganography. In cryptography, the message is encrypted using a particular key. Only the sender and receiver know this encryption keys. The message cannot be accessed without the encryption keys. However, transferring the encrypted message can be easily detected by the intruders and intruders might violently decrypt the message. Steganography over comes all the drawbacks of cryptography.

The word steganography was derived from Greek word, which means concealed writing. Thus, steganography is not only the art of hiding the data but also a fact of transmission of secret data. Steganography works in a way that it hides the presence of the message in the image. Steganography method is so powerful that it can hide the secret message inside any multimedia like audio, video, images referred as embedding.

Data hiding inside an image can be performed in two methods. They are, spatial domain and Transforms domain methods. Spatial domain technique works with image pixels. The pixel values are changed to achieve the required enhancement while in transformation or frequency domain data is embedded based on the frequency of pixel. The first effort in spatial domain is least significant bit substitution.

In the paper, we have elaborated the content into VI sections; section II contains survey related to the work with steganography. Section III holds the different stages of proposed method, section IV describes the proposed work in algorithmic approach, section V explains the experimental results and calculations. section VI concludes the paper.

II. Related Work

In this section, we briefly explain about the research done on image steganography. In paper [1] at the sender side uncompressed cover image is encrypted using encryption-key later data hider may compress the encrypted image using data hiding-key to create a space so that some additional data can be added, secret data is added to this space. If the receiver has the encrypted-key, they can decrypt the cover image but not the secret message, if the receiver has data-hiding key they can decrypt the secret message but not the cover image. If the receiver has both encrypted-key and data hiding-key both information can be recovered. In paper [2] the secret data is modified before embedding into the host image, genetic algorithm is used to find the best templet in the host image to hide the secret data . In paper [3] spatial domain technique is used which is simple and popular method of embedding secret data in least significant bit of the host image. In paper [4] the secret data is hidden inside the cover image in a ratio 2:2:4 in red, green and blue respectively separating each plane. In paper [5] author, explain about how the edges of the image can be used to hide the secret data, it also explains about edge detection and filter techniques

III. Proposed Work

The proposed work is based on reversible data hiding technique. here, there are three stages embedding, extraction and enhancement. In embedding two images are selected as cover image and secret image, both the images are divided into non overlapping blocks. Histograms are

DOI : 10.35291/2454-9150.2019.0108

generated for each block. Bits of secret image is hidden inside cover image's least significant bit producing stego image. In extraction this secret bits hidden in cover image are decrypted recovering cover image and secret image without any distortions. After extraction of secret data from cover image, secret image enters the enhancement phase. The details of each of the embedding, extraction and enhancement process are explained below.

A. *Embedding process*

In embedding process cover image is selected and checked whether lower bond pixel and upper bond pixel are 1 and 254 respectively, if not they are set to 1 and 254 to decrease overflow and underflow problems. After that cover image is divided into non overlapping blocks. In each block reference pixel is selected and average of other pixels are calculated. This information is bookmarked. Histogram is generated for each blocks. Pixel values in every block are converted into binary values. LSBs of each pixel is set to 0. Secret image is resized and divided into non-overlapping blocks, each pixel value in each blocks are converted into binary values. The binary pixel values of secret image is embedded into the LSB of cover image.

B. *Extraction process*

Input of the extraction process is a stego image formed from embedding process. Stego image is divided into non-overlapping blocks. Histogram is generated to every block. In each block reference pixel is chosen this pixel will be the same one, which was chosen in embedding process, average difference between the chosen pixel, and the remaining pixel of the block is calculated. LSB of each pixel value is checked. If the LSB of pixel is 0, 0 is recorded if the LSB is 1, 1 is recorded as secret image pixel value and the process continues and checks all the stego image pixel extracting secret image from cover image. The output of this phase will be extracted secret image and restored cover image.

C. *Enhancement phase*

After the completion of extraction process, the extracted secret image goes through enhancement phase. Gaussian filters is one of the method through which noise of the image can be removed. Gaussian filters helps in smoothing the image. In one dimension, the Gaussian function is:

$$G(x)=\frac{1}{2\pi\sigma^{2}}e^{-\frac{x^{2}}{2\sigma^{2}}}$$

Where σ is the standard deviation of the distribution. The distribution is assumed to have a mean of 0.

Flow of proposed work

As shown in figure 1 two images are selected as cover image and secret image, as a first step cover image is checked, whether the lower and upper bond pixel values are 1 and 254 respectively. If not they are set to 1 and 254. In the next step cover image is divided into non overlapping blocks. Block difference of each block is calculated. Different histograms are generated for each block. Simultaneously secret image is also divided into blocks and histograms are generated. Secret image values are embedded into cover image's least significant bit, which gives a stego-image. Now in extraction process, this stego-image is taken as input and divided into blocks. Again the block difference is calculated, different histograms are generated and shifts back the pixel values which extracts the secret image from cover image.

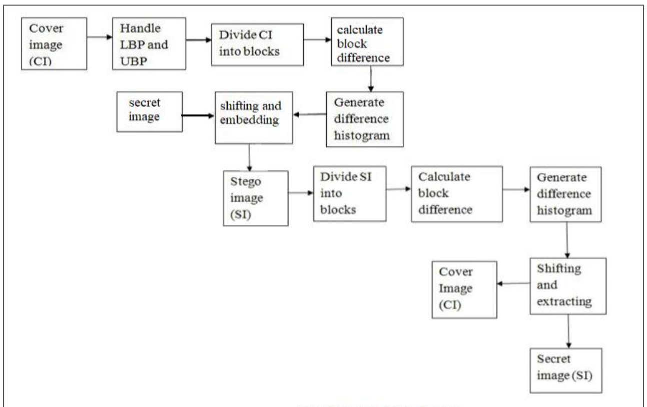

Fig 1: Flow of proposed work

IV. ALGORITHMIC APPROACH

Algorithmic approach is an effective method of expressing within a finite amount of space and time. Starting from an initial input proceeds through a finite number of steps and eventually producing output .In the section we have explained all the algorithms used in the project, there are different algorithms, which performs different operations in each step of the process.

A. Main module

Input: Grayscale image
Output: Enhanced secret-image and restored cover-image

Step 1: Begin
Step 2: Read the cover-image
Step 3: Divide the image into blocks
Step 4: Generate the difference histogram
Step 5: Shift the histogram and embed the secret bits
Step 6: Generate the stego-image by embedding secret bits into cover-image
Step 7: Read the stego-image
Step 8: Divide the stego-image into non-overlapping-blocks
Step 9: Generate the difference histogram

DOI : 10.35291/2454-9150.2019.0108

```
Step 10: Shift the histogram back to extract the secret-image and cover-image
Step 11: Enhance the extracted secret image using Gaussian filters.
Step 12: End.
```

B. Embedding module

Input: Grayscale host-image and secret-image

Output: stego-image

```
Step 1: Begin
Step 2: Read the input images
Step 3: Check whether the lower bound pixel and upper bound pixel is 1 and 254
Step 4: Partitions the cover-image into smaller blocks
Step 5: For each block, select a pixel as maximum and take the difference between the maximum pixel and remaining pixel.
Step 6: Generate the difference histogram
Step 7: Shift the histogram and embed the secret bits
Step 8: End
```

C. LBP and UBP handling module

Input: Grayscale image

Output: LBP =1 and UBP=254

```
Step 1: Begin
Step 2: Read the input image
Step 3: Check whether LBP=0 and UBP=255 if it is then set LBP=1 and UBP=254
Step 4: End
```

D. Block division module

Input: Grayscale image

Output: Image divided into blocks

```
Step 1: Begin
Step 2: Read the input image
Step 3: Divide the image into non-overlapping-blocks
Step 4: For every block, select maximum reference pixel
Step 5: Take the difference-between chosen maximum pixel and remaining pixels in the block.
Step 6: End.
```

E. Extraction module

Input: stego-image

Output: secret image and restored cover image

```
Step 1: Begin
Step 2: Read the input images
Step 3: Partitions the input image into non-overlapping-blocks
Step 4: In each block select the maximum pixel value as reference pixel. This reference pixel is the same pixel selected in embedding process.
Calculate the average btw reference and remaining pixel.
Step 6: Generate the different histogram
Step 7: Shift the histogram back and extract secret bits
Step 8: End
```

F. Enhancement module

Input: Secret image

Output: Enhanced secret image

```
Step 1: Begin
Step 2: Read the input image
Step 3: Enhance the secret image using Gaussian filters
Step 4: End
```

V. PERFORMANCE ANALYSIS

Performance analysis is a section where it is checked whether the proposed method reached the expectation. Here we evaluate the proposed system with reference to the previous approaches. In the project, we have taken Peak signal noise ratio and Mean square error to measure the performance of the proposed system.

a. Result analysis

In image steganography, we hide the secret image inside another image, which can be called as cover image where quality of both secret image and cover image is an important factor. Peak signal noise ratio (PSNR) measures the quality of the image. High the PSNR value represents the better image quality and less probability of identifying the presence of secret data. As the PSNR value of the image increases, it gets difficult to detect the presence of secret image in cover image.

b. Peak signal noise ratio (PSNR)

In image steganography quality of the images are one of the important factors. Quality of the image before embedding and after extraction are compared to evaluate the capacity of the algorithms implemented. Here PSNR performs this investigation.

$$\text{PSNR}=10^{*}\log_{10}(255^{2})/MSE$$

c. Mean square error (MSE)

After embedding secret image in cover image, the cover image and stego image are compared to check the pixel value differences in both the images. MSE performs the compression between cover image and stego image with the given formula below.

$$\text{MSE}=1/(w*h)\sum_{i=1}^{w}\sum_{j=1}^{h}(mij-nij)^{\wedge}2$$

- w and h are width and height of the host image
- Mij is the pixel value of the cover image

- Nij is the pixel value of the stego image

Table 1 shows the calculations of PSNR and MSE values. Column one holds the names of the secret image which is embedded into the column two of images.

TABLE 1 MSE and PSNR of the proposed work

Secret image	Cover image	MSE	PSNR
Baboon	Resized desert	8.39	36.075
Code	Charlie	6.37	36.216
Terrorist	Koala	10.82	36.050
Baboon	Barbara	7.99	36.069
Hydrangeas	Jelly fish	6.39	36.118

VI. Conclusion

In the paper, for the process of steganography multiple algorithms are implemented. By using this algorithm, we achieve better efficiency and quality of steganography. In the paper we divide the images into blocks which helps in finding best template for embedding and also requires less time to embed the secret image. In proposed method the secret data is hidden in the LSB of the cover image hence there will be tiny amount of changes in the pixels which cannot be identified by necked eyes hence stego image appears same as the cover image. The stego-image at the receiver side is divided into cover image and secret image using extraction techniques. The extracted secret image is implemented to enhancement techniques, which enhances the secret image. The proposed method performs enhancement of the secret image which gives a clear picture of the secret data.

References

[1] X.zhang, separable reversible data hiding in encrypted image. ieee trans. inf. forensics security, vol. 7, no. 2, pp. 826–832, apr. 2012

[2] Rashidy kanan,h.,& nazeri, b(2014) a novel image stegnography scheme with high embedding capacity and tunable visual image quality based on a gentic algoritm. expert system with application,41,6123-6130.

[3] Soleimanpour, M., Talebi, S. & Azadi-Motlagh, H. (2013). A Novel Technique for Steganography Method Based on Improved Genetic Algorithm Optimization in Spatial Domain. Iranian Journal of Electrical & Electronic Engineering, 9(2), 67-75.

[4] Amritpal Singh, Harpal Singh. An Improved LSB based Image Steganography Technique for RGB Images. *IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pp. 1- 4, 2015.

[5] Saeed Ahmed Sohag, Dr. Md. Kabirul Islam, Md. Baharul Islam. A Novel Approach for Image Steganography Using Dynamic Substitution and Secret Key. *American Journal of Engineering Research (AJER)*,Vol. 2, Issue 9, pp-118-126, 2013

[6] Carvajal-Gamez, B.E., Gallegos-Funes, F.J., & Rosales-Silva, A.J.(2013). Color local complexity estimation based steganography (CLCES) method. Expert Systems with Applications, 40(4), 1132-1142

[7] Chen, W.-J., Chang, C.-C., & Le, T. (2010). High payload steganography mechanism using hybrid edge detector. Expert Systems with Applications, 37(4), 3292-3301.

[8] Ioannidou, A., Halkidis, S.T., & Stephanides, G. (2012). A novel technique for image steganography based on a high payload method and edge detection. Expert Systems with Applications, 39(14), 11517-11524.

[9] Naor, M., & shamir, A. (1995). Visual cryptography, Advaces in cryptology EUROCRYPT'94. Berlin Heidelberg: Springer.

[10] Sajedi, H., & Jamzad, M. (2010). BSS: Boosted steganography scheme with cover image preprocessing. Expert Systems with Applications, 37(12), 7703-7710.

[11] Qian Mao (2014). A fast algorithm for matrix embedding steganography. Digital Signal Processing 25, 248-254.

[12] Chen, W.-Y. (2008). Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques. Applied Mathematics and Computation, 196(1), 40-54.

[13] Chu, R., & et al. (2004). A DCT-based image steganographic method resisting statistical attacks. IEEE international conference on acoustics, speech, and signal processing, 2004. Proceedings. (ICASSP'04) (Vol.5).IEEE.

[14] Jafari, R., Ziou, D., & Rashidi, M. M. (2013). Increasing image copression rate using steganography. Expert Systems with Applications, 40(17), 6918-6927.

[15] Liu, T. & Qiu, Z. –D. (2002). A DWT-based color image steganography scheme. In 6th International conference on signal processing, 2002 (Vol. 2). IEEE.

[16] Noda, H., Niimi, M., & Kawaquchi, E. (2006). High-performance JPEG steganography using quantization index modulation in DCT domain. Pattern Recognition Letters, 27(5), 455-461.

[17] Duric, Z., Jacobs, M., & Jajodia, S. (2005). Information hidng: Steganography and steganalysis. Handbook of Statistics, 24, 171-187.

[18] Luo, X.-Y. et al. (2008). A review on blind detection for image steganography. Signal Processing, 88(9), 2138-2157.

[19] Nissar, A., & Mir, A. H. (2010). Classification of steganalysis techniques: A study. Digital Signal Processing, 20(6), 1758-1770.

[20] Ziou, D., & Jafari, R. (2012). Efficient Steganalysis of images: Learning is good for anticipation. Pattern Analysis and Applications, 1-11.

[21] Rashidy Kanan, H., & Nazeri, B. (2014). A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert systems with Applications, 41, 6123-6130.

[22] Liu, G., Zhang, Z. & Dai, Y. (2009). GA-based LSB-matching steganography to hold second-order statistics. Proceedings of MINES'09 Los Alamitos IEEE Computer Society, 510-513.

[23] Liu, X. X. & Wang J. J. (2007). A steganographic method based upon JPEG and swarm optimization algorithm, Information Science, 177(15), 3099-3109.

[24] Xu, H., Wang, J. & Kim, H., J. (2010). Near-optimal solution to pairwise LSB matching via an immune programming strategy. Information Sciences, 1201-1217

DOI : 10.35291/2454-9150.2019.0108