Image Steganography based on Quantization Error

Akanksha Tripathi
M.tech Researcher,
Galgotia College of Engineering and Technology

Sachin Kathuria
Assistant Professor,
Galgotia College of Engineering and Technology

ABSTRACT
This paper designs a technique that hides the text in a image such that the modified (stego) image have same or enhanced quantized variance as compared to the original image. The algorithm hides the text in the higher frequency component of transformed image only if the image quantized variance needs the improvement at that pixel. This results in the enhanced image with hided data. The results are analysed over various images by using the parameters like PSNR, MSE and the quantized variance.

Keywords
Quantization error, PSNR, jpeg, stego image.

1. INTRODUCTION
The Steganography is used to hide the data under a cover media. The most important characteristic of the Steganography is the imperceptibility i.e. there is no difference between the original and stego cover media. The rise of digital images corresponded with the well-known availability of image editing software led an image forger to easily alter in a visually realistic manner. These softwares can be used to alter the image. The most common is to compress the image. The jpeg compression of the image changes the image properties. It is necessary to maintain the quantization ratio to maintain the image properties [1][2].

The primary goal of digital image forensics is the identification of images and image regions which have undergone some form of manipulation or alteration. The common properties of the histograms of unaltered images led to building a model of an unaltered image's pixel value histogram. The methods for detecting generally forms globally and locally applied contrast enhancement, as well as a method for identifying the use of histogram equalization, a commonly used form of contrast enhancement [3][4]. This paper uses the concept of jpeg compression anti forensics to hide the data inside the image.

2. RELATED WORK
Various work done by researchers are as follow: Fridrich, A. Jessica, B. David Soukaland A. Jan Lukáš [5],in 2003 demonstrated that images can be manipulated with editable software's. and identified the Problem of copy-move forgery.

Manimurugan.S, Athira B.Kaimal [6] 2012 Prevent a medical image compression history by using unnoticeable forgeries. Unnoticeable forgeries can by detect by estimation, examination and alteration. Böhme, Rainer, and Matthias Kirchner [7] 2013 shows that the Counter-forensics is first defined in a formal decision-theoretic framework. This framework is then interpreted and extended to encompass the requirements to forensic analyses in practice, including a discussion of the notion of authenticity in the presence of legitimate processing. The work which is compared with the present work is as follow: In this work the input is an color image. The R, G, B component are extracted from the image. The extracted components are converted in to the binary format. Then the binary array is reshaped to the block of 8 bit. The secret message is hided to blue component of the image by replacing the LSB of the each block by one bit. The decryption process is the reverse of the encryption process. The data is hided to the blue component of the image that makes system imperceptible. The work is modified by using the forward quantization error concept given in the next section.

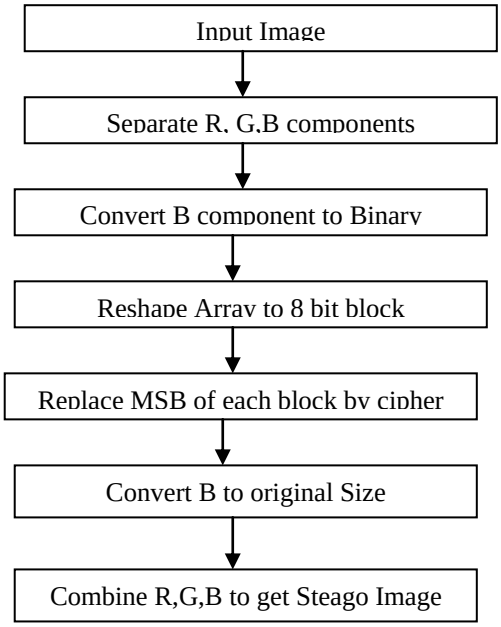

Figure 1: Existing Flowchart

3. PROPOSED ALGORITHM
This work is based on jpeg compression anti forensics which calculates the forward quantization error to determine whether the given image is jpeg compressed or not. The information loss due to the quantization can be given as: $loss = I - int32(I/q) * q$ where q is the quantization step and the int32 converts the number in double to the integer i..e quantize the value. The variance of the loss can be calculated as:

$$var(loss) = \sum_{i=1}^{n} loss_i / n$$

Where n is the number of pixels in the image. If the value of loss variance is less than a threshold then the image is compressed otherwise uncompressed. It can be given as

$$\begin{cases} var(loss) < t & compressed \\ var(loss) \geq t & uncmpressed \end{cases}.$$

Where t is the threshold value determined on experimental basis. Here, the value of t is taken as 5. This process find the pixel where the loss variance is less than the threshold value and hides the data in those pixels resulting enhanced loss variance. This process enhance the image quality and removes the traces f the jpeg compression. Moreover, the value of PSNR must be high with no visual difference in the

stego image as compared to original image. The process can also be understood by following algorithm:

1. Text=Read the input text.
2. Text=Convert double(text) to binary.
3. Input image.
4. If length(size(image))==3 then

   Convert image to gray scale

   End
5. Calculate loss as

$$loss = I - int32(I/q) * q$$
6. Calculate the loss variance

$$var(loss) = \sum_{i=1}^{n} loss_i / n$$
7. Transform the image into frequency domain

   [ll lh hl hh]=dwt2(I,'db2')

   Here db2 represents the wavelet transform used.
8. Convert the high frequency component i.e. hh to vector form say hh2.
9. For each bit of btext
10. If var(loss(hhr(current_pixel)))<t

    Then hide the pixel in the image hh2

    End if

    End for
11. Take idwt to get the image in time dmain.

    Ri=idwt2(ll lh hl hh2,'db2')

The ri is the reshaped stego image resultant of the algorithm. The process is also given in the flowchart shown in figure 2. The loss variance, psnr and the mean square error of the resultant image can be calculated over various images by using MATLAB described in next section.

4. RESULT AND DISCUSSIONS

The implementation of the proposed work is carried out on images downloaded from the internet. The proposed algorithm is implemented on various images. The figure 3 shows a original image before hiding the data into the image while the figure 4 shows the image after hiding the data inside it. It can be seen that there is no visual difference between two images.

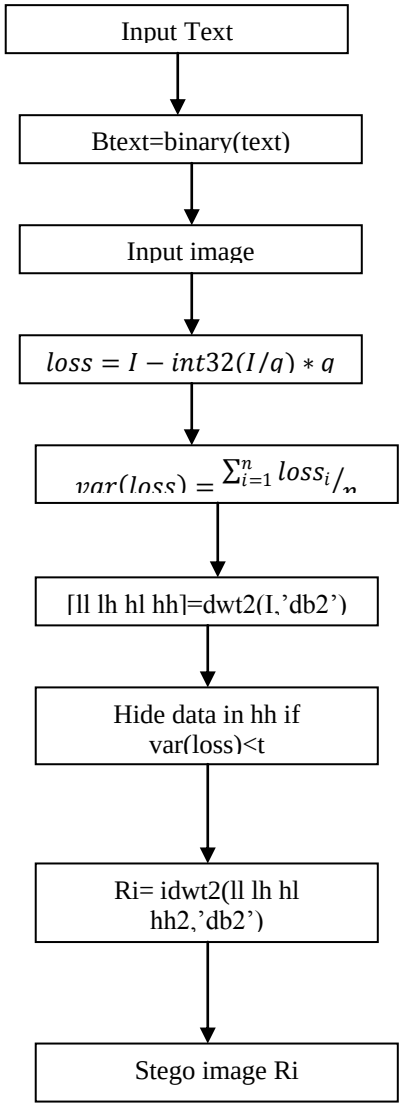

Figure 2: Proposed Flowchart

Figure 3: Original Image

Figure 4: Stego Image

The figure 5,6 shows the histogram of the original and stego image respectively. It can be analysed that both histogram are same. It means no difference can be determined even by analysing the histograms of the original and stego image.

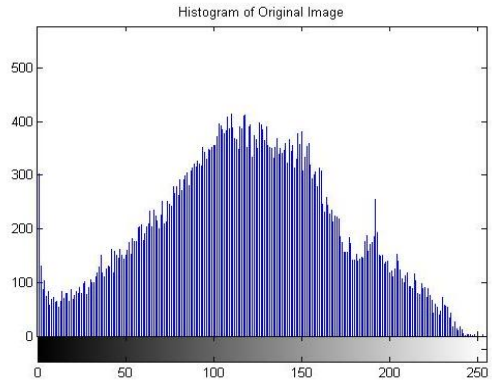

Figure 5: Histogram of original image

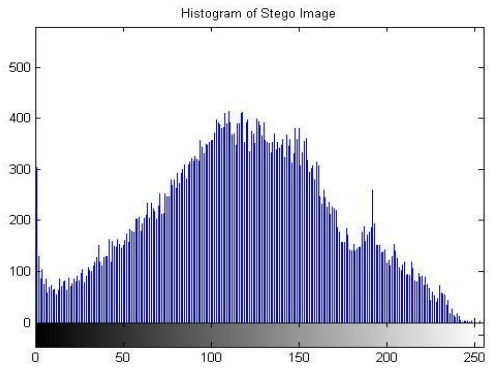

Figure 6: Histogram of the stego image.

Moreover, two parameters i.e. MSE and PSNR are also analyzed given as follow:

4.1 MSE

MSE is given by taking the mean of the squared value of the original image pixel and the resultant image pixel. It can be calculated as follow:

$$MSE = \frac{1}{IJ}\sum_{m=0}^{I-1}\sum_{n=0}^{J-1} e(m,n)^2$$

The comparison of the MSE is shown in figure 7:

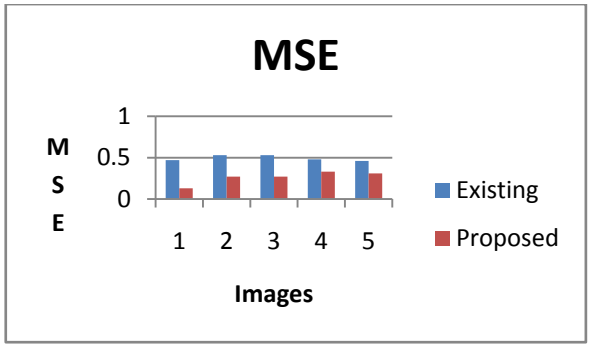

Fig 7: MSE Comparison

It can be seen that the MSE value get decreased for every image.

4.2 PSNR

PSNR (Peak Signal-to-Noise Ratio compares the quality of the similarity between the original and reconstructed image. The higher the value of the PSNR more is the similarity. PSNR can be calculated as:

$$PSNR = 20log\frac{S}{\sqrt{MSE}}$$

The comparison of the PSNR is shown in the figure 8:

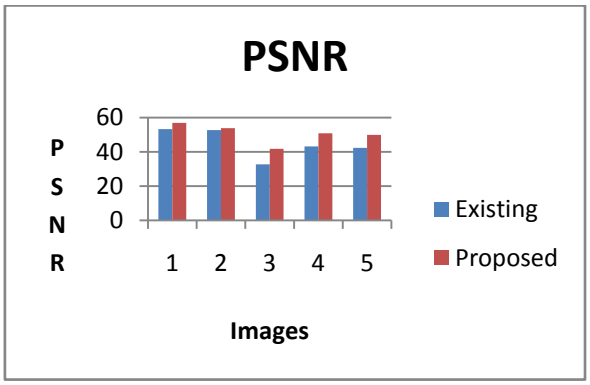

Fig 8: PSNR Comparison

The above analysis shows that the PSNR of the proposed method is better than the existing method. The Increase in the PSNR and the decrease in the MSE confirm the benefits of the proposed work.

5. CONCLUSION

This work enhances the performance of the existing Steganography technique by using the forward quantization error concept. The work hides data in the transformed domain only if the loss variation is low in that particular region. The concept enhances the imperceptibility while maintaining the loss variance of the image. This work can be extended to used more media to hide the data.

6. REFERENCES

[1] Matthew C. Stamm, Steven K. Tjoa, W. Sabrina Lin, and K. J. Ray Liu. 2010. Anti-forensics of JPEG compression", In Acoustics Speech and Signal Processing (ICASSP), pp. 1694-1697.

[2] Matthew C. Stamm, Student Member, IEEE, and K. J. Ray Liu, Fellow, IEEE. 2011. Anti-forensics of digital image compression", IEEE Transactions on Information Security, Vol. 6 No. 3, pp. 1050-1065, September.

[3] Stamm, M. C., & Liu, K. R, 2010. Forensic detection of image manipulation using statistical intrinsic fingerprints, IEEE Transactions on Information Forensics and Security, Vol.5 No.3, pp. 492-506.

[4] Fridrich, A. Jessica, B. David Soukal, and A. Jan Lukáš. 2003. Detection of copy-move forgery in digital images. In Proceedings of Digital Forensic Research Workshop.

[5] Lukáš, Jan, and Jessica Fridrich. 2003 Estimation of primary quantization matrix in double compressed JPEG images. Proc. Digital Forensic Research Workshop.

[6] Manimurugan.S (2012) A Tailored Anti-Forensic Approach for Bitmap Compression in Medical Images", IOSR Journal of Computer Engineering

[7] Böhme, Rainer, and Matthias Kirchner. 2013. Counter-forensics: Attacking image forensics. Digital Image Forensics. Springer New York. 327-366.