Steganalysis Technique on Gray scale Image by Varying Message Length using Adaptive Histogram Equalization Attack

Anuj Kumar
Research Scholar
Department of Computer Science
CT inst. Of Engg. Management technology

Shivani Khurana
Assistant Professor
Department of Computer Science
CT inst. Of Engg. Management technology

ABSTRACT
Steganography considered as a technique for secret communication without knowing the others and only an authorized user can access the information which is embedding in the cover medium. Steganalysis is the process to detect of presence of Steganography and to destroy, extract it. In this Paper There is Adaptive Histogram Equalization Technique that performed on the Stego Image that is category of the Histogram Equalization attack and measuring the quality of Image after applying the Attack.

General Terms
Detection, Destruction

Keywords
Least Significant Bit, Steganography, Secret Information, Adaptive histogram equalization.

1. INTRODUCTION
"Steganography" is a Greek origin word which means "hidden writing". Steganography word is created from two forms: Steganos which means "secret or covered" (where you want to hide the secret messages) and the graphic which means "writing" (text). [1]It was started by the Greeks by shaving the slave's hair heads and writing the message on their heads, after the hair had been grown, they were sent to their allies in order to communicate with them without the enemies' knowledge. As well as, the invisible ink used for hiding the secret messages by the American revolutionaries during the USA Revolution. It was also used in both World Wars by German army [1]. Another Steganography technique is the Spam Mimic software which developed by Wayner in (2003), this software was developed to detect and hide the secret messages in text file based on set of protocols. [1]

Steganalysis is a technique to detect the Steganography. It is used to detect whether media contain Stego data or not. There are two types of attack one is Visual attack and second is Statistical Attack. In Visual Attack a set of Stego images are compared with original cover images and the visible difference is notified. The process of finding these distortions is called Statistical Steganalysis and in Statistical attack to detect the Steganogram chi-square attack is used.

There are several types of attacks based on the information available for analysis. [6]

2. STEGANALYSIS ATTACKS

2.1 Known carrier attack
The original and Stego media both are available for analysis. [10]

2.2 Steganography only attack
In this type of attacks, only Stego media is available for analysis. [10]

2.3 Known message attack
Secret message is known in this case. [10]

2.4 Known Steganography attack
The Cover media, Stego media as well as the steganography tool or algorithm, are known. [10]

2.5 Chosen Stego attack
The Stego algorithm and Stego-object are available for analysis. [10]

3. STEGANALYSIS USING ADAPTIVE HISTOGRAM EQUALIZATION ATTACK
Here, Adaptive histogram equalization used as an attack for Steganalysis in spatial domain. That applied on LSB technique to destroy the secret message which is embedded in the cover media. Adaptive histogram equalization (AHE) improves on this by transforming each pixel with a transformation function derived from a neighborhood region.

4. METHODOLOGY FOR STEGANALYSIS
Here is the methodology for Steganalysis is shown in figure as below:

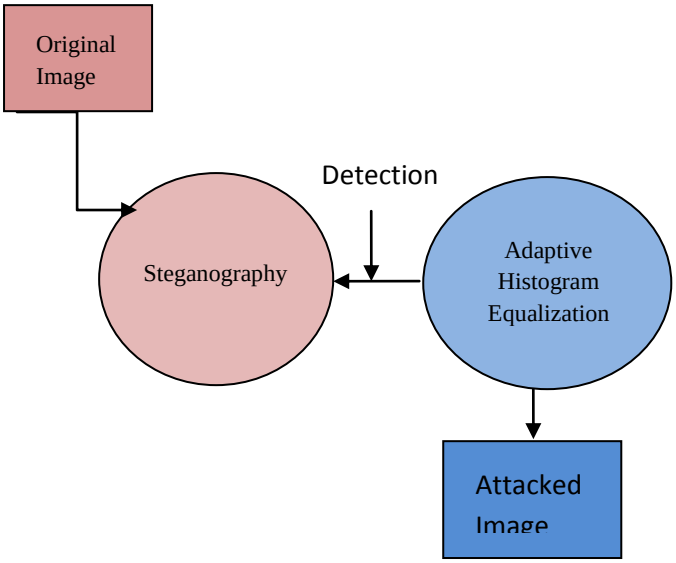

Fig 1: Steganalysis by Adaptive Histogram Equalization

First of all apply the histogram attack to detect whether the image is stego or not that is to detect the steganography. Here BMP image is used as cover media. In which histogram of stego image created and original image were created, and then to obtain the difference from histogram. If difference occur then the image is stego if not occur then image is not stego. This is called detection of Steganography. Once the steganography is detected then adaptive histogram equalization attack on the stego image is applied to destroy the secret image from the cover media. At last comparing them by calculating the loss rate for checking which is better among them.

5. ALGORITHM

5.1 Embedding

- Choose cover Image and secret message.
- Convert decimal value of pixel of an image in binary value.
- Embed secret message at least significant bit of each pixel's binary value.
- Convert each pixel's binary value in decimal value.
- Reconstruct the Image.

5.2 Detection

- Create histogram of original Image**.**
- Create histogram of Stego Image.
- Subtract Stego histogram from original histogram.
- If difference occur Image is Stego otherwise not Stego.

5.3 Destruction

- Apply Adaptive histogram equalization on Stego image.
- Create histogram of attacked image.
- Subtract it from original image.
- Calculate PSNR and MSE for quality measure.

6. RESULTS AND DISCUSSION

Here it shows the original image and Stego image and shows the histogram of both images to presents the difference occur after Steganography.

Fig 2: Original image

Fig 3: Stego image

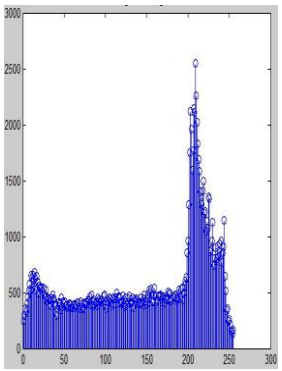

Fig4: Histogram of Original image

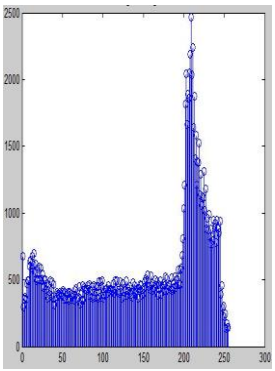

Fig 5: Histogram of stego Image

Here the attacked Image Fig (g) is obtained after applying the adaptive histogram equalization on the Stego Image. And the Histogram of Attacked Image is represented by Fig (h).

Fig 6: Attacked image

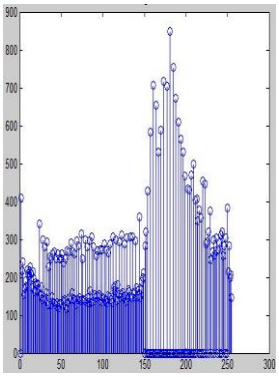

Fig 7: Histogram of Attacked image

6.2 Histogram Differencing

The Histogram distribution may be used to discriminate stego images from natural images. Zhang et al. proposed the difference image histogram method that generates a difference Image D, calculating the difference value between two adjacent pixels of the image as given by

$$D(i, j) = I(i+1, j) - I(i, j)$$

Error Image Occur after Differencing the Stego Image From Original Image. And obtain the Difference Histogram by generating the Histogram of Error Image.

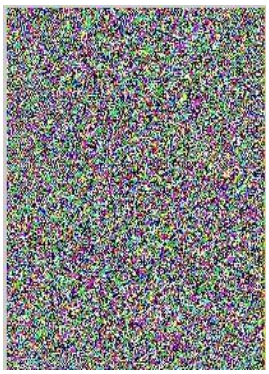

Fig 8: Error Image

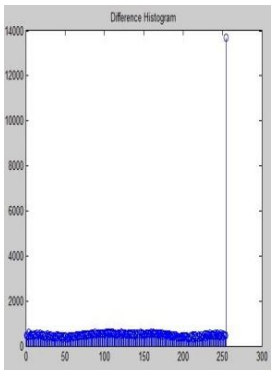

Fig 9: Difference Histogram

Error Histogram Occur after Differencing the Adaptive Histogram Equalized Image Histogram From Original Image Histogram.

Fig 10: Error Image

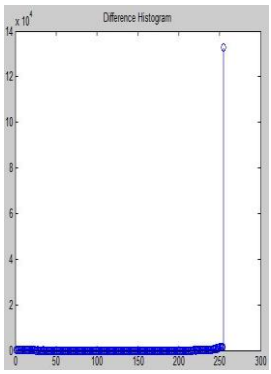

Fig 11: Difference Histogram

6.3 QUALITY MEASURE

Quality measured after the Steganography to check the quality of image. Here, the various tests are performed by varying the message length to check the quality of image at which level the quality is affected by varying the message length and to check how much the loss rate and noise occur in the image.

Table 1: Quality Measure after Steganography

Message Length	Mean Square Error (MSE)			Peak Signal Noise Ratio (PSNR)		
bits	Red	Green	Blue	Red	Green	Blue
32	0.00011	0.00000	0.00000	139.46856	Infinity	Infinity
6560	0.02205	0.00000	0.00000	116.53429	Infinity	Infinity
41,632	0.13712	0.00000	0.00000	108.59785	Infinity	Infinity
76,704	0.16641	0.08593	0.00000	107.75715	110.62728	Infinity
1,09,584	0.16641	0.16615	0.02844	107.75715	107.76387	115.42929
1,51,160	0.16641	0.16615	0.16558	107.75715	107.76387	107.77891

Here, the various tests are performed by varying the message length to check the quality of image at which level the quality is affected by varying the message length. To check how much the loss rate and noise occur in the image after histogram equalization attack and we got the quality is slightly affected by varying the message length and image look like as original.

Table 1: Quality Measure after Adaptive Histogram Equalization

Message Length	Mean Square Error (MSE)			Peak Signal Noise Ratio (PSNR)		
bits	Red	Green	bits	Red	Green	bits
32	241.18352	241.18352	241.18352	76.14545	76.14545	76.14545
6560	241.16122	241.16122	241.16122	76.14585	76.14585	76.14585
41,632	241.20519	241.20519	241.20519	76.14506	76.14506	76.14506
76,704	241.29065	241.29065	241.29065	76.14352	76.14352	76.14352
1,09,584	241.29065	241.29065	241.29065	76.14352	76.14352	76.14352
1,51,160	241.29065	241.29065	241.29065	76.14352	76.14352	76.14352

7. CONCLUSION

Steganography is a technique for secret communication. Here BMP image is used as cover image and embedded the secret message by using substitution technique. In substitution LSB technique is used which is mostly used for embedding the message in cover image. Here the difference in image is obtained after Steganography using Histogram attack and then we performed the Adaptive Histogram Equalization technique on the Stego Image in which the quality is slightly degraded after Adaptive histogram equalization attack and image is look like as original that is by preserving the quality of image. Hence the enhanced Image is obtained with destruction of Secret message.

8. REFERENCES

[1] Atallah M. Al-Shatnawi(2012) "A New Method in Image Steganography with Improved Image Quality." Al-albayt University, Vol. 6, 2012, no. 79, 3907 - 3915.

http://www.m-hikari.com/ams/ams-2012/ams-77-80-2012/alshatnawiAMS77-80-2012.pdf

[2] Ankita Agarwal(2012)" Security Enhancement Scheme for Image Steganography using S-DES Technique ". International Journal of Advanced Research in Computer Science and Software Engineering , April 2012/volume 2 issue 4/V2I400162.

http://www.ijarcsse.com/docs/papers/April2012/Volume_2_issue_4/V2I400162.pdf

[3] Nazanin Zaker , Ali Hamzeh(2011)"A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram"Shiraz University, 25 january 2011. http://connection.ebscohost.com/c/articles/73762949/novel-steganalysis-tpvd-steganographic-method-based-differences-pixel-difference-histogram

[4] Arpan Ghorai, Dibyendu Chowdhury, Satyajit Das(2011)," Design and Implementation of Public Key Steganography," International Journal of Soft Computing and Engineering (IJSCE)

http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1095&context=computerelectronicfacpub&sei

[5] Dr. N. Meghanathan, " Least Significant Based (LSB) Steganography ,"Jackson State University.

http://www.jsums.edu/cms/tues/docs/Steganography/LSB-Steganography.pdf

[6] "Peak signal to noise ratio".

http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio

[7] V. Sharma, S. kumar, "A New Approach to Hide Text in Images Using Steganography"ijarcsse, 4 april 2013, V3I40401 volume 3.

http://www.ijarcsse.com/docs/papers/Volume_3/4_April2013/V3I4-0401.pdf

[8] A. Kumar and Km. Pooja, "Steganography : A Data Hiding technique," International journal of computer Application(0975-8887),vol-9 no.7,november 2010.

http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.206.5754

[9] Kevin O'Bryant, "Principle of steganography".

http://www.math.ucsd.edu/~crypto/Projects/MaxWeiss/steganography.pdf

[10] Introduction to Stegnography. http://io.acad.athabascau.ca/~grizzlie/Comp607/menu.htm