REA Steganography and Steganalysis

Ruchika Sharma
PHD Scholar, JaganNath University, Jaipur
Dr. Meenu Dave
Professor, JaganNath University, Jaipur

Abstract: The art and science of finding a covert message is called steganalysis. While steganography hides the existence of secret data within digital media, steganalysis detects and uncovers the presence of such hidden information. To ensure the robustness of the embedded algorithm in a steganographic communication system, steganography and steganalysis work together. The distortion measurements SNR and PSNR are employed in steganography to assess the visual quality of an image, which is affected by the process of data embedding. These measures are useful for evaluating the imperceptibility, capacity and robustness of steganographic systems.

Keywords: Steganography, Steganalysis, Digital Media, SNR, PSNR

1.INTRODUCTION

Steganalysis is the process of detecting hidden information within a seemingly harmless digital cover. It uncovers the existence of concealed data. The practice of identifying a covert message is known as steganalysis. The cover medium is highly likely to retain fragments of the concealed message. A steganalyst aims to identify how the process of hiding information changes the statistical properties of the cover. Steganalysis is the process of detecting hidden secret data. Its main objective is to determine whether or not a concealed message is embedded within the stego cover[1]. The aim of steganalysis is to identify whether a digital cover conceals any secret information and to assess the strength of the embedded steganographic system[2]. Steganalysis aims to uncover details about the image and the hidden message, including the type of embedding algorithm used, the length of the message, its content, and the secret key employed[3]. Steganalysis is classified into two broad groups (a) Passive and (b)Active.:

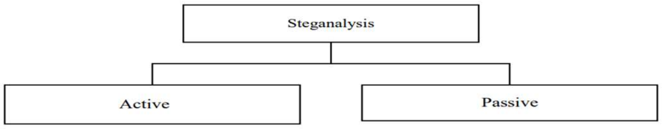

Fig 1: Classification of Steganalysis

Passive steganalysis does not know the actual cover medium. It only speculates on the existence of concealed information. Its purpose is to assess whether a stego cover holds a concealed message and to identify the stego embedding algorithm used. To uncover hidden data, passive steganalysis relies solely on observation and analysis of communication without any interference. In contrast, active steganalysis involves intentionally interfering with the transmission. It estimates the length of the embedded message and identifies the locations of the concealed messages. Additionally, it determines the secret key used for embedding and various parameters of the stego embedding methods. Many steganalysis researchers, such as Neil F. Johnson and S. Jajodia [4,5], have sought to categorize steganalysis attacks that aim to recover, modify, or remove messages. These attacks can be divided into following categories:

- ***Chosen Stego Attack*****:** The steganalyst in this case is aware of the steganographic algorithm that was used to construct the stego medium, thus they attempt to create stego mediums from cover media to match the intercepted stego medium.

Stego Only Attack: : In a stego-only attack, the steganalyst has access solely to the stego medium being examined, with no additional information available.

Known Cover Attack: In a known cover attack, the original cover medium is accessible alongside the stego medium. This allows the steganalyst to identify differences between the two and attempt to ascertain the steganographic method used. This approach is similar to traditional plaintext attacks.

Known Message Attack: A known message attack can be used once the hidden message has been discovered. The steganographer can try to analyze the stego image for potential future attacks by knowing the hidden message.

Chosen Message Attack: The steganalyst generates a stego-object by using a known message and a steganography tool or technique. Using this method, one can find the matching pattern in the stego-object that can be utilized to determine the steganographic tool or methodology.

Stego-system spectrum may differ depending on the domain they are embedded in, such as transform or spatial[6]. The following figure depicts the schematic diagram representing steganalysis approach.

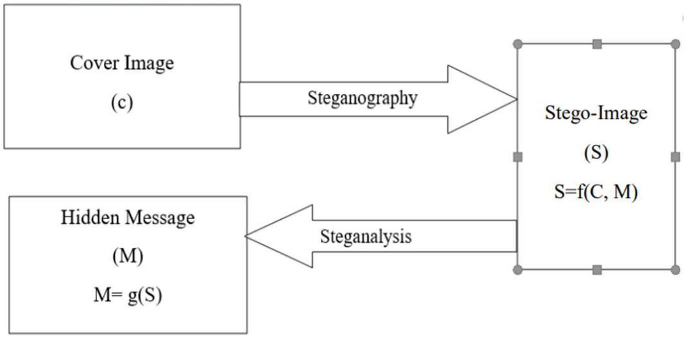

Fig 2: Schematic Diagram Representing Steganalysis Approach

In the above Figure2
C : Cover image.
M : hidden message.
S : stego image.
S= f(C, M) denotes stego image generated by hiding M(hidden message) in C (cover image)
M= g(S) denotes steganalysis is applied on S and hidden message is retrieved.

A cover image and hidden message are shown as input in the above figure. Some approach is then applied to produce a stego image with an embedded hidden message.

Steganalysis judges the performance of the embedding algorithm on different factors i.e. capacity, perceptibility and robustness [7].

II. PARAMETERS DETERMINING QUALITY OF EMBEDDING ALGORITHM

To guarantee the robustness of an embedded algorithm in a steganographic communication system, steganography and steganalysis work in tandem.

The embedding algorithm should be tested based on few parameters which ensures the strength of the algorithm. The parameters are capacity, robustness and perceptibility[16]. The following figure presents the parameters of steganalysis.

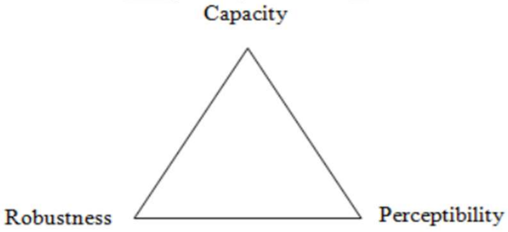

Fig 3: Parameters of Steganalysis

Robustness: It is the amount of alteration the stego cover may sustain before being destroyed by an adversary.

Capacity : The quantity of information that may be concealed in a particular digital cover depends on this component[8].

Perceptibility: It is the determinant of whether the stego retains the original digital cover's likeness or not. Greater resemblance suggests that it is less likely to be mistaken for stego[9].

In any steganographic system, the quality of the embedding algorithm is determined by these three parameters. The embedding algorithm should consider all the above factors and produce an optimized solution.

III. STUDY OF REA STEGANOGRAPHY

Recursive equation approach is used for hiding information. It is used as key to hide information in a digital cover[10]. The adopted methodology uses secret information, digital image as cover and a recursive equation to find the random place to hide the secret information. Recursive equation iterates within itself. Only one initial value is required and then recursive equation approach is used as a key to randomly locate hidden information, making it nearly impossible for an intruder to find because the likelihood of correctly identifying the difference between the cover and stego image is negligible[11]. Even if someone attempts to break into the stego image, it would be impossible to access the hidden information because it is stored at a very great distance and at random locations generated by recursive equation.

The REA steganography algorithm works on two factors:

3.1 Selecting the location in a BMP and PNG Image to hide Secret Information:

The location of hidden secret information in BMP and PNG images is determined by the REA steganography. Using a single recursive equation with starting condition can determine many places in images where secret information can be hidden. Recursive equations strengthen algorithms by generating the next place to conceal hidden information based on the previous position as they cycle through themselves.

In order to determine the randomized locations to conceal secret information, the method takes into account two different forms of recursive equations: linear and higher order recursive equations.

3.2 Strength of Approach

Recursive equations are used by the REA steganography algorithm to strengthen the algorithm in terms of capacity, robustness, and imperceptibility[12]. Since the information is hidden from one another at great distances, it is nearly impossible for an intruder to find out that it is hidden.

The pixel position can hardly be found, which makes it difficult for a third party to discover the any concealed message using REA steganography. To protect privacy and security, the REA steganographic approach is tested for imperceptibility, distortion, and security against recovery of hidden communications.

IV. PERFORMANCE MEASURES

A number of widely used metrics, such as the Peak-Signal-Noise Ratio (PSNR) and Signal-to-Noise Ratio (SNR), are used to evaluate the efficacy of the REA steganography. These metrics are useful for evaluating the robustness, capacity, and imperceptibility of steganographic needs. One can assess an image's imperceptibility using SNR and PSNR[13].

4.1 Signal-Noise Ratio

In the domains of image and video coding, distortion metrics such as the signal-to-noise ratio (SNR) and peak-signal-to-noise ratio (PSNR) are frequently employed. These measures are employed in steganography to assess how the data concealing process affects the image's visual quality. SNR is the measurement of the signal to noise power ratio.

When referring to images, It describes how the extra noise distorts the original image. After reconstruction, an image's quality is assessed using the SNR and PSNR[14]. The reconstruction of image is considered good if the values of SNR and PSNR are higher.

The ratio of signal power level to noise power level is known as the signal to noise power ratio (S/N).

$$\frac{S}{N}(dB) = 10 * \log\frac{P_S}{P_N}$$

Where PS is the signal power and PN is the noise power.

4.2 Peak-Signal-Noise-Ratio

The original data is the signal whereas Noise is the result of compression-induced error. When comparing compression, PSNR serves as an approximation of the human visual system's (HVS) reconstruction quality. It is measured in decibels (dB). To calculate PSNR, the following mathematical formula is used:

$$PSNR = 20 * \log_{10}(\frac{L-1}{RMSE})$$

L represents the total number of intensity levels possible in an image, with the minimum intensity level set at 0.

MSE is the mean squared error & it is defined as:

$$MSE = \frac{1}{rs}\sum_{p=0}^{r-1}\sum_{q=0}^{s-1}\left(X(p,q) - Y(i,j)\right)^2$$

Where X represent the matrix data or pixel value of original image. Y represents the matrix data or pixel value of stego image. r represents the number of rows of pixels and p represents the index of that row of the image. s represents the number of columns of and q represents the index of that column of the image[15].

RMSE is the root mean squared error.

$$RMSE = \sqrt{MSE}$$

V. EXPERIMENTAL RESULTS

This section presents some experimental results to illustrate the efficacy of the proposed approach. The performance of the proposed method is evaluated on 24- bit BMP image format.

In Figure 4, a selection of the images used to test the algorithm are displayed. The stego image is displayed in Figure 5 after embedding the secret message into the cover object. All of these test images are 300* 300 pixel size.

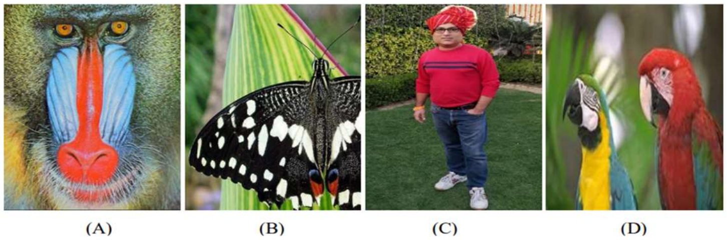

Fig 4:Cover Images (A) baboon1.bmp (B) butterfly.bmp (C) Chander.bmp (D) parrot stego5.bmp

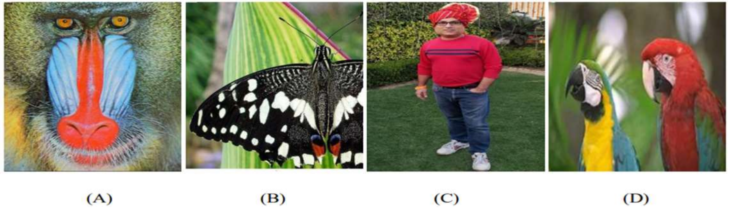

Fig 5 : Stego Images (A) baboon1stego.bmp (B) butterflystego.bmp (C) Chanderstego.bmp (D) parrot stego10.bmp

The above images are testing for Imperceptibility.Imperceptibility determines whether or not the cover can be altered after a message has been implanted. When utilizing an image as a cover, the main metrics used to assess imperceptibility are signal to noise ratio and peak signal to noise ratio. An acceptable threshold for preserving the similarity between the cover and stego images is considered to be a PSNR value of 30dB or higher. The comparison of the alterations in cover and stego image is shown in below table:

Cover Image	Stego Image	PSNR(db)
parrot stego5.bmp	parrot stego10.bmp	49.79
butterfly .bmp	butterflystego.bmp	45.02
chander. bmp	chanderstego.bmp	42.33
baboon1 .bmp	baboon1stego.bmp	46.79

Table 1: Comparison of the Alterations in Cover and Stego Image by Generating Peak Signal to Noise Ratio

The PSNR outcome of changes to the cover and stego images is displayed in the above table. The outcome clearly indicates that in every situation, the stego image's imperceptibility is higher than 30 dB. All PSNR assessments are more than 30 dB. A PSNR value of more than 30 dB is considered to be a trustworthy indicator for preserving the cover and stego image similarity. Because of this, the proposed method has good imperceptibility.

VI. CONCLUSION

Steganalysis involves detecting hidden information embedded within an otherwise normal-looking cover, exposing the existence of concealed data. This paper explains the application of steganalysis and the various factors that influence the quality of embedding algorithms. It highlights the key parameters that affect the robustness of the algorithm. The study of the REA algorithm outlines the effectiveness of the recursive equation approach in identifying optimal locations within image files for embedding secret information. The Proposed REA algorithms discussed in this paper preserve the image quality even after embedding secret information within the cover. The imperceptibility is tested using PSNR values. The algorithm is considered to have good strength as there is very less probability of finding secret information.

REFERENCES

[1] Niels, P. and Honeyman, P. (2003). Hide and seek: An introduction to steganography, IEEE Security and Privacy, vol. 1, no.3, pp. 32-44.

[2] Ker, A.D. (2006). Fourth-order structural steganalysis and analysis of cover assumptions. Delp, E.J., Wong, P.W. (eds.) IS&T/SPIE Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents VIII, pp. 60720301–60720314. SPIE, San Jose.

[3] Li, Pei & Li, Yeli & Wang, Hongjuan & Liu, Chang. (2021). Research on Steganalysis of Digital Image Based on Deep Learning. 528-534. 10.1109/AEMCSE51986.2021.00114.

[4] Johnson, N.F. and Jajodia, S. (1998). Exploring Steganography: Seeing the Unseen‘. IEEE Computer, February, pp. 26-34.

[5] Johnson, N.F. and Jajodia, S., (1998, April). _Steganalysis of Images Created Using Current Steganography Software‘. Proceedings of the Second Information Hiding Workshop, Portland, Oregon, USA, Vol. 1525, pp 273-289.

[6] Li, B., He, J., Huang, J., & Shi, Y. Q. (2011). A survey on image steganography and steganalysis. Journal of Information Hiding and Multimedia Signal Processing, 2(2), 142-172.

[7] Chandramouli, R., Kharrazi, M., Memon, N.(2004). Image steganography and steganalysis concepts and practice. Kalker, T., Cox, I., Ro, Y.M. (eds.) IWDW 2003. LNCS, vol. 2939, pp. 35–49. Springer, Heidelberg.

[8] Lin T. and Delp J.(1999). A Review of Data Hiding in Digital Images. In Proceedings of the Image Processing, Image Quality, and Image Capture Conference, Georgia, pp. 274-278.

[9] Sharma. Ruchika, Kumar. Vinay. (2020). Information Hiding using Linear Recursion. In IJSER Volume 11, Issue6, ISSN: 2229-5518.

[10] Sharma Ruchika, Kumar Vinay. (May 2015). Implementation of Steganogrphy Using Recursive Equation Approach. IJCMS Vol. 4, Special Issue.

[11] Sharma. Ruchika, Kumar. Vinay, (2022). Hiding secret data in an image using a higher order recursive equation as key. In Caraivéti Volume 5, Issue 2(JanuaryJune 2022), ISSN : 2456-9690.

[12] Swanson, M.D., Zhu, B., Tewfik, A.H. (1996). Transparent robust image watermarking. Proc. IEEE International Conference on Image Processing (ICIP96), Piscataway, NJ. IEEE Press, vol. III, 1996, pp. 211- 214.

[13] Salomon, D. (2004). Data compression: the complete reference. Springer Science & Business Media.

[14] Krishna Raj, Kapil Dev Tiwari, Vipul Goel, Pragya Gautam (July 2017).Variational Techniques for Image De-noising: A Review. International Journal for Research in Applied Science and Engineering Technology ISSN: 2321-9653,Vol. 5, Issue VII, pp.2168-2172.

[15] M. Cadik and P. Slavik(2004).Evaluation of two principal approaches to objective image quality assessment. 8th International Conference on Information Visualisation, IEEE Computer Society Press, pp. 513-551.

[16] Sharma. Ruchika, Kumar. Vinay, (2022). Recursive Equation Approach of Information Hiding for Authentication of Digital Data in Journal of Algebraic Statistics , Volume 13, Issue 2, pp. 813-819