Performance Analysis of Data Encryption Techniques Using Image Steganography

Sunita Devi[1], Arvind Kalia [2]
Department of Computer Science
[1] Research Scholar, Himachal Pradesh University, Shimla, India
[2]Professor, Himachal Pradesh University, Shimla, India

Abstract- *Steganography is defined as the study of invisible communication. It maintains secrecy between two communicating parties. In image steganography, secrecy is achieved by embedding data into cover image and generating a stego-image. Using Steganography techniques on stego image the security can be improved. For improving second level security, different algorithms can be applied on stego image. So that the result in the improvement of security in terms of execution can be achieved. When it comes to the pro and cons of various Steganographic software, many have been designed; each of them has different features and capabilities for data hiding. Hence, this makes it a wide and attractive field for further research, in which the establishment of innovative methods and techniques could be done. The objective is to compare different encryption techniques and validate the results using MATLAB. In order to meet the objective the both theoretical and practical approach has been used. The research methodology used practical approach for performance analysis. The algorithm used for secret communication using steganography and cryptography here steghide tool is used. Steghide technique is implemented in MATLAB. The performance and comparison of these techniques are evaluated on the basis of the different quality measurement parameters mean square error (MSE), peak signal to noise ratio (PSNR), normalized absolute error (NAE), normalized cross-correlation (NCC) and maximum difference (MD).*

Keywords: Encryption Techniques, MSE, PSNR, NAE, NCC, MD.

I. INTRODUCTION

In the past years, several information hiding techniques were used which hides the data inside another object. These days, all the information is stored in a digital form. The other objects can be data, image, audio or video. Images are one of the most important carrying media, which can be used for hiding the information [1]. This process of hiding information into another object is referred to as a stenography. There are two techniques available for transmitting the secret information between the communicating parties. One is cryptography [17], in which the structure of the message is scrambled to make it meaningless and can be reconstructed only by the holder of a key. It offers the ability of transmitting the information between communicating parties in a way that prevents the third party from reading it [5]. When secret message is transmitted, it is observable by anyone means it does not attempt to hide the fact that a message exists. The second technique is stenography, which hides the secret message into another object. It does not alter the structure of the secret message, but hides it inside a cover object so that it cannot be seen by any observer. On the other hand, steganography focuses on making the fact that the secret message does not exist within the system. Figure 1.1 shows the general block diagram of steganography.

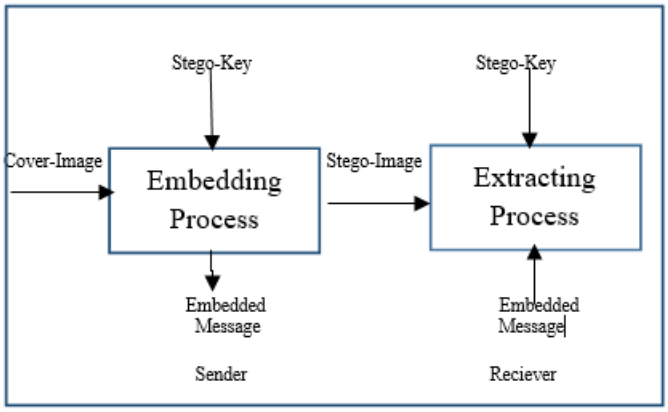

Figure 1.1: General Block Diagram of Steganography.

A. Steganography Terminology

A complete steganography system consists of the cover object, stego object, embedding algorithm, extraction process and secret message and sometime a stego key which is used to extract the message from stego object [3]. Embedding of message is performed in the sender side and extraction process is carried out at recipient side. Only the sender and intended recipient know the secret transmission of information. Explanations of the important terminologies of the stego system are following:

- Cover Object: It is the input medium in which concealment of the secret data is to be performed. It could be an image, video file, audio file or a text file.

- Stego-Object: After the concealment of secret data into the cover medium, the cover object becomes the stego-object.
- Embedding: Embedding is the process of making a stego-object from a cover object. Or we can define as the process of concealment of a secret message into some digital medium.
- Extraction: This is the reverse process of embedding. In this process, the conceded message is recovered from stego-object to read it.
- Message: It is the secret information that is to be embedded in the cover object for safe transmission of data from sender to receiver.

B. Steganography Types

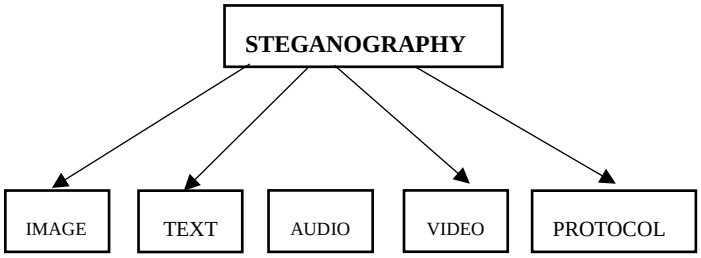

Figure 1.2: Categories of steganography

- Text based Steganography.
- Image based Steganography.
- Audio based Steganography.
- Video based Steganography.
- Protocol based Steganography.

- *Text-based Steganography*

In this, the message that is to be sent is rooted firstly in a text file with formatting. The format it based on line-shift coding, word-shift coding, feature coding etc. Reformatting of the text destroys the rooted content hence the technique is not robust [16].

- *Image-based Steganography*

This Steganography hides the message in the images. This is the most popular technique because of the fact that almost no perceivable changes occur. Some of the commonly used methods of embedding payload in cover image are least Significant Bits (LSB) substitution in which the LSBs of cover image pixel are altered to hide the payload and more data can be hidden in edges [13].

- *Audio-based Steganography*

This Alters audio files so that they contain hidden messages. The techniques are LSB manipulation, phase coding and echo hiding. It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. These methods are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.

- *Video-based Steganography*

Video Steganography is a technique to hide files or information into a digital video format. Video is used as carrier for hidden information. Generally discrete cosine transforms (DCT) which is used to hide the information in each of the images in the video, which is not visible by the human eye. Video Steganography uses, such as Mp4, MPEG, AVI or other video format.

- *Protocol-based Steganography*

The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. In the layers of the OSI network model, there exist covert channels where steganography can be used. It involves hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP etc. as cover object. An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used.

C. Overview of Data Encryption Techniques Using Image Steganography

i. *Cryptography*

Cryptography is that branch of science which is concerned with the mathematical techniques for keeping message secure and free from attacks. Cryptography is the art of achieving security by encoding the data into an unreadable form. Data that can be read and understood without any difficulty is called plain text or clear text [20]. The method of encoding Plain text in such a way as to hide its content is called encryption. Encrypting plain text results in unreadable gibberish called cipher text. You use Encryption to ensure that information is hidden from anyone for whom it is not intended, even those who

can see the encrypted data. The process of reverting cipher text in its original plain text is called decryption [17].Fig. 1.3 shows the encryption and decryption process.

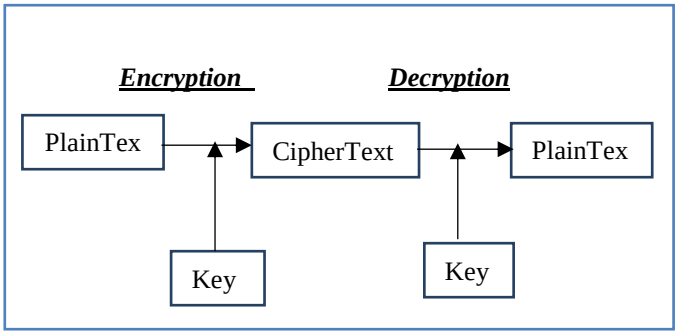

Figure 1.3: Encryption and decryption process

There are two types of encryption algorithms: symmetric encryption algorithm and asymmetric encryption algorithm. In Symmetric key encryption sender and receiver will have the same key for the process of encryption and decryption of data. In asymmetric key encryption algorithm different keys are used in sending and receiving site for encryption and decryption.

II. ENCRYPTION ALGORITHMS

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- Triple Data Encryption Standard
- Blowfish Encryption Algorithm

➢ *Data Encryption Standard (DES)*

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only) [15].The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

- Avalanche effect − A small change in plain text results in the very grate change in the ciphertext.
- Completeness −Each bit of ciphertext depends on many bits of plaintext.

During the last few years, cryptanalysis has found some weaknesses in DES when key selected are weak keys. These keys shall be avoided. DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.

➢ *Advanced Encryption Standard (AES)*

The most popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES.A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack [7]. Triple DES was designed to overcome this drawback, but it was found slow.
The features of AES are as follows −

- Symmetric key symmetric block cipher.
- 128-bit data, 128/192/256-bit keys.
- Stronger and faster than Triple-DES.
- Provide full specification and design details.
- Software implementable in C and Java.

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES have been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches. However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

➢ *Triple DES*

The speed of exhaustive key searches against DES after 1990 began to cause discomfort amongst users of DES. However, others did not want to replace DES as it takes an enormous amount of time and money to change encryption algorithms that are widely adopted and embedded in large security architectures. The pragmatic approach was not to abandon the DES completely, but to change the manner in which DES is used. This led to the modified schemes of Triple DES (sometimes known as 3DES). Incidentally, there are two variants of Triple DES known as 3-key Triple DES (3TDES) and 2-key Triple DES (2TDES).

The encryption-decryption process is as follows −

- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.

- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the cipher text.
- Decryption of a cipher text is a reverse process. User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1.

Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

➢ *Blowfish Encryption Algorithm*

Blowfish was designed in 1993 by Bruce Scheier as a fast, alternative to existing encryption algorithms such AES, DES and 3 DES etc. [17]. Blowfish is a symmetric block encryption algorithm designed in consideration with:

- Fast: It encrypts data on large 33-bit microprocessors at a rate of 36 clock cycles per byte.
- Compact: It can run in less than 5K of memory.
- Simple: It uses addition, XOR, lookup table with 33-bit operands.
- Secure: The key length is variable, it can be in the range of 33~448 bits: default 138 bits key length.
- It is suitable for applications where the key does not change often, like communication link or an automatic file Encryptor.
- Unpatented and royalty-free.

III. RELATED WORK

Shrivastava et al. [18] explained the various techniques based on a combination of steganography and image compression approach. The aim was to calculate the effectiveness of the compression. The most often used factor for this purpose is compression ratio (CR), which expresses the ability of the compression method to reduce the amount of disk space needed to store the data. During the study, it was found that image compression minimizes the size in bytes of a graphics file without degrading the quality of the image to an unacceptable level. *Katoch et al. [8]* explained the two main techniques, first is cryptography and second is Steganography. The main objective of the study was to boost up the security related to data over the internet. Both are used for data security purpose. In this paper, a technique is used which combines these two methods to provide a more efficient and effective result. Therefore, different cryptographic algorithms are compared on the basis of Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The goal of the study was to implement two techniques like Steganography and Cryptography for confidential communication between the two entities and also deals with security and privacy. *Vyas et al. [19]*have presented, implemented and analyzed a new Steganography technique. The basic idea was to get good image quality. It was seen in their work that the proposed method was compared with the LSB benchmarking method for hiding the secret message which hide the secret message directly in the least two significant bits of the image pixels. The future work on this study was to improve the compression ratio of the image to the text. The main intention of the survey was to develop a steganographic application that provides good security. *Khan et al. [9]* discussed that the steganography promises confidentiality of data being transmitted between two parties by hiding the very existence of the data. It helps to achieve secure transmission of data over a network. They also provided a technical introduction of image steganography and its implementation using Least Significant Bit (LSB) technique with Huffman Coding. It focused on the use of Huffman Coding Algorithm to minimize the amount of bits to be embedded into the carrier in order to achieve efficient image steganography. *Khan et al. [10]*have described the secure steganography for digital images. The main aim of the study was to observe the reliability of proposed solution which can be appreciated by observing the differences between cover, preprocessed cover and Stego object. Proposed scheme was equally good for color as well as gray scaled images. Another interesting aspect of this research was that it implicitly presents a fusion of cover and information to be hidden in it while taking care of passive attacks on it. Matlab simulation software was used for technical analysis. They concluded that it was equally suitable for gray scaled, and as well as for colored images. *Singh et al. [16]* has described the concept of steganography, its various techniques, its advantages and disadvantages, applications; it's merging with cryptography techniques. The main goal of the study was to secure the data so that no unauthorized person can access it. So that various steganography powerful security tools were used. They can hide a secret message inside an object. The object can be a text, image, audio or video. *Kaur et al. [7]* have studied that steganography refers to the data hiding. The main purpose of steganography is to hide the data behind the images. It means that it encrypts the text in the form of an image a day's in data transfer over the network, the security is the main issue concerned with this. In order to. The steganography is done when the communication takes place between sender and receiver. Now secure the data while transmission steganography is used. Before the development of the steganography, Security of the data is the main concern of research for the researchers. *Rao et al. [14]* have studied that steganography helps in the communication of secured data in several carries like images, videos and audio. It undergoes many useful applications and well known for ill intentions. It was mainly proposed for the security techniques in the increase of computational power, in order to have security awareness

like individuals, groups, agencies, etc. The factors that are separated from cryptography and watermarking are data is not detectable; capacity of hidden data is unknown and robustness of the medium. The steganography provides different methods existing and guidelines.

III. OBJECTIVES

The main objective of the study is to boost security of important and confidential data over internet. This can be achieved by using the different encryption algorithm for hiding text or image in digital files. Then the sender and receiver can use the tools to hide and extract the secret text or image in digital files. The specific objectives of the study are:

- To study and evaluate the various data encryption algorithms used in image steganography using different image format.
- To compare the performance analysis of data encryption techniques using image steganography.
- To test the efficiency and accuracy of data hiding through different algorithms for data hiding.

IV. SCOPE AND METHODOLOGY

The transmission of the important data over the network is very risky these days. To secure such data mostly the tool is used, that is steganography tool. As the hackers are better known that the data over the internet is encrypted and they know that the encryption is done by using some mathematical methods and they can decrypt that data using the mathematical calculations or by using hit and trial methods. Only cryptography is not the solution, steganography can refine and increase the security levels and data, information can be secured very efficiently rather than using of cryptography alone. To refine the security levels using it is important to find the drawbacks of cryptography and steganography, it is also important to study that how they work and how we can use them? The main issue is to combine the cryptography and steganography and maintain the integrity of the secured channel and data to be secured. In order to meet the objective the both theoretical and practical approach has been used. The research methodology used theoretical approach for the study and selection of tool for the objective which includes literature survey, articles, books, research paper and internet. Practical study configures, implements, tests and evaluates the images for performance and modified. After applying all these techniques on image data it results in an encryption method which is highly secure. For the implementation, Matlab is used as a simulator to implement the techniques of steganography.

V. ANALYSIS

For the purpose of analysis and comparison of the algorithms, the algorithms are simulated in Matlab. This paper presents the experimental results for the steghide method for the color images. For this study PSNR, MSE, NCC, NAE and MD are considered for analysis. In this present implementation Armytank and Flower 2096 × 2096 images has been taken as cover image as well as Lena and baboon 128 × 128 images has been taken as secret images and the results are presented in figures 4.2 and 4.3. The estimating parameters of the two stego covers have been performed using indigenous Matlab code in Intel Core i3 CPU processor @ 2.27 GHz, 3GB RAM.
Following are the factors that determine how efficient and Powerful a technique is.

- *PSNR (Peak Signal to Noise Ratio):*

It is defined as the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. This ratio measures the quality between the original and a compressed image. The higher value of PSNR represents the best quality of the compressed image [10].

$$PSNR = 10 \log_{10} \left(\frac{I_{\max}^2}{MSE} \right) dB$$

Where" I_{max}" is the intensity value of each pixel which is equal to 255 for 8 bit grayscale images.

- *MSE (Mean Square Error):*

It is defined as the average squared difference between a reference image and a distorted image. The smaller the MSE, the more efficient the image steganography technique. MSE is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count.

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(X_{i,j} - Y_{i,j} \right)^2$$

Where M and N denote the total number of pixels in the horizontal and the vertical dimensions of the image Xi, j represents the pixels in the original image and Yi, j, represents the pixels of the stego image.

- *NCC (Normalized Cross Correlation):*

  NCC is computed to quantify the correlation between the original and extracted image. It is used to comparing the similarity between the cover image and the stego image and it also check the correctness of the result.

- *NAE (Normalized Absolute Error):*

  It is a network performance function and it measures the network performance as the mean of absolute errors.

- *MD (Maximum Difference):*

It is used to calculate the maximum intensity of the cover image and stego image.

A. Performance Analysis

The above mentioned techniques are implemented in MATLAB. The procedure is applied on both the .bmp and .jpg images of different sizes. An image is considered to be a carrier object for data embedding. Cover object is subject to be 'original image' whereas the Stego object is termed as 'embedded image'. During the analysis, data is used in kilobytes i.e. 5KB of a text file as well as 128* 128 of image size as secret messages. The cover image and secret image have been compared with available algorithm methods and the results are tabulated in Table 1.1 and Table 1.2. The PSNR, MSE, NCR, NAE, MD used as the parameters of image quality.

Table 1.1: Performance Analysis of all the methods used in image steganography (. JPG)

	Cover Images	Secret Message	MSE	PSNR	NCC	NAE	MD
AES	Armytank.jpg	lena.jpg	0.0559	60.6568	1.0000	2.9801 e-004	2
		smessage.txt	0.0069	69.7159	1.0000	3.7064 e-005	2
DES	Armytank.jpg	lena.jpg	0.0558	60.6653	1.0000	2.9747 e-004	2
		smessage.txt	0.0066	69.9494	1.0000	3.5140 e-005	2
TRIPLE DES	Armytank.jpg	lena.jpg	0.0557	60.6753	1.0000	2.9680 e-004	2
		smessage.txt	0.0065	69.9739	1.0000	3.4920 e-005	2
BLOW FISH	Armytank.jpg	lena.jpg	0.0553	60.7068	1.0000	2.9466 e-004	2
		smessage.txt	0.0067	69.8545	1.0000	3.5911 e-005	2

Table 1.2: Performance Analysis of all the methods used in Image steganography (. JPG)

	Cover Image	Secret Message	MSE	PSNR	NCC	NAE	MD
AES	Flower.bmp	baboon.bmp	0.0712	59.6068	1.0000	3.6853 e-004	2
		smessage.txt	0.0067	69.8937	1.0000	3.4595 e-005	1
DES	Flower.bmp	baboon.bmp	0.0707	59.6354	1.0000	3.6591 e-004	3
		smessage.txt	0.0064	70.0372	1.0000	3.3467 e-005	1
TRIPLE DES	Flower.bmp	baboon.bmp	0.0712	59.6090	1.0000	3.6823 e-004	2
		smessage.txt	0.0063	70.1368	1.0000	3.2711 e-005	1
BLOW FISH	Flower.bmp	baboon.bmp	0.0712	59.6031	1.0000	3.6871 e-004	3
		smessage.txt	0.0064	70.0911	1.0000	3.3057 e-005	1

After all the analysis, these ratios present the change that has been occurring in the images. Comparing the MSE (Mean Square Error) and the PSNR (Peak signal noise ratio) of original and embedded image it has been clear that lower the MSE and Higher the PSNR improves the Stego image quality

For .JPEG images, Figure 1.4(a) and 1.4(b) shows the visual appearance of the cover image and stego image. Similarly for .bmp images, Figure 1.4(c) and 1.4(d) shows the visual appearance of the cover image and stego image. It is clear from the Figure 1.5&1.6 that visual appearance of the stego images is very good. Steghide technique is applied on two images and results of these images are presented here.

Figure 1.4(a): cover image (armytank.jpg)

Figure 1.4 (b): Secret image (lena.jpg)

Figure 1.4(c): cover image (flower.bmp)

Figure 1.4(d): Secret image (baboon.bmp)

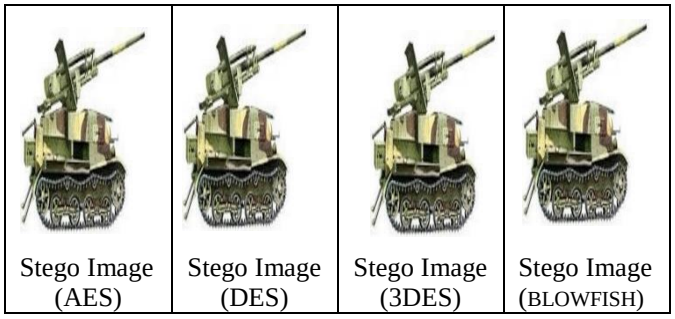

Figure 1.5: Stego images (.jpg) using Steghide Technique

Figure 1.6: Stego images (.bmp) using Steghide Technique

B. Histogram

An image histogram is one of the types of histogram. It specified as a graphical representation of the digital image. It plots the number of pixels in each image block. Image histograms are used in many modern digital cameras. Photographers used them to show the distribution of tones captured, and the image detail has been lost to blown-out highlights or blacked-out shadows. The horizontal axis of the graph described the tonal variations; the vertical axis represents the number of pixels in a particular tone. The left portion of the horizontal axis represents the black and dark areas, the middle portion represents a medium gray and the right hand side represents light and pure white areas [12]. The vertical axis describes the size of the area that is captured in each of these zones. Thus, the histogram for a very dark image will have the majority of its data points on the left side and the Centre of the graph.

A histogram is a measure of the number of occurrences of pixels with respect to particular pixel value [9]. During embedding pixel value changes, hence the number of pixels having a particular pixel value change. These changes can be used to detect steganography. The histograms for both the color image (.jpg, .bmp) with size of (2048 x 2048) for all the four the algorithms have been taken separately.

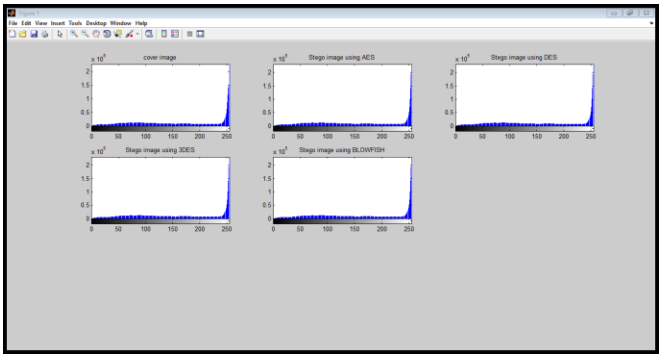

Figure 1.7: Screenshot of the Histograms of stego-images (.jpg) produced by Steg-hide using different algorithms where secret message is .jpg.

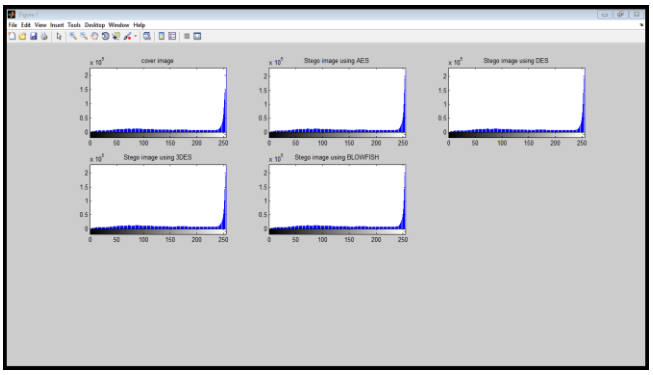

Figure 1.8: Screenshot of the Histograms of stego-image (.jpg) produced by Steg-hide using different algorithms where secret message is .txt file.

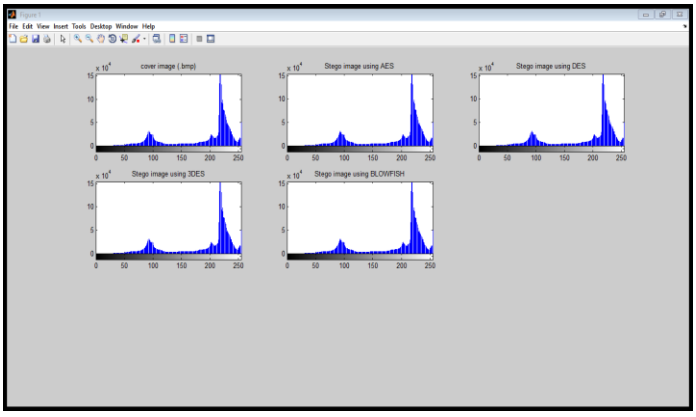

Figure 1.9: Screenshot of the Histograms of stego-image (.bmp) produced by Steg-hide using different algorithms where secret message is a .bmp

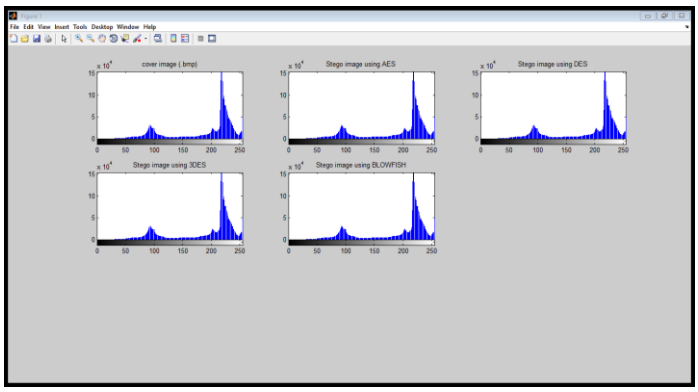

Figure 1.10: Screenshot of the Histograms of stego-image (.bmp) produced by Steg-hide using different algorithms where secret message is .txt file

The observed results of Steghide technique are represented graphically as shown in figure 1.11&1.12. This figure shows the parametric evaluation based on both the stego images, i.e. armytank.jpg and flower.bmp by using different algorithms.

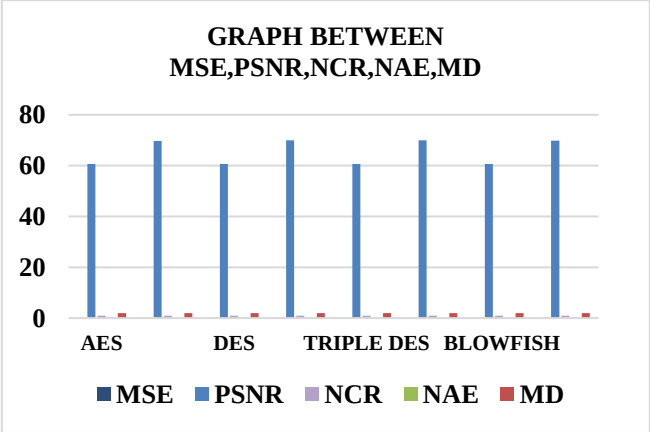

Figure 1.11: Comparison of stego images (.jpg) based on different parameters.

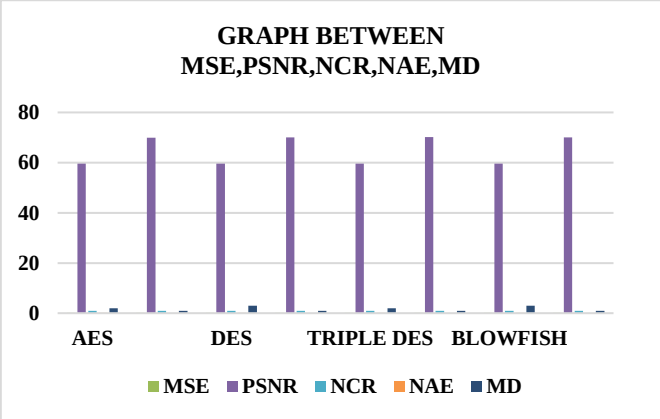

Figure 1.12: Comparison of stego images (.bmp) based on different parameters.

After obtaining all the results, the analysis of the graphs and tables obtained show that the overall performance of Blowfish is much better than that of other three algorithms used in steghide technique. Also, the Blowfish is much secure free alternatives than the other algorithms. The algorithm is unique and a stronger security tool using the steganography with jpeg image. This gives the two phases of security one is at the cryptography used and one is the data is embedded into a JPEG image medium.

VI. CONCLUSION & FUTURE SCOPE

This paper presents a study and performance analysis of different algorithms used in the image steganography technique. The main concern of the study was the performance of the above said algorithms under different parameters when different types of images are used. In this study PSNR, MSE, NCC, NAE and MD are considered for analysis and the popular secret key algorithms including DES, AES, triple DES, Blowfish, were implemented and their performance was compared by encrypting input files of varying contents and sizes. The algorithm was implemented in Matlab, using their standard specifications and was tested on two different types of images (.jpg and .bmp), to present the comparison and the results are compared. In the comparisons it has been found that there is no difference between the original cover image and the steganography image. The histograms are also compared but there are no differences.

After obtaining all the results, the analysis of the graphs and tables obtained shows that the overall performance of Blowfish is much better than that of other three algorithms used in steghide technique. Also, the Blowfish is much more secure, free alternatives than the other algorithms. The algorithm is unique and a stronger security tool using the steganography with JPEG image. This gives the two phases of security one is at the cryptography used and one is the data is embedded into a JPEG image medium. In future, steganography is implemented on the 3d multimedia images and videos. Work can be done to make the steganography reliable, secure and easily available to provide more security and more authenticity.

REFERENCES

[1] Bender, W., D. Gruhl, and N. Morimoto, Techniques for data hiding, IBM Systems Journal, vol. 35, no. 34, 1996, pp. 131-336.

[2] Chae J.J. & Manjunath S.B., “A Robust Embedded Data from Wavelet Coefficients”, SPIE: Storage and Retrieval

for Image and Video Databases VI, 3312, San Jose, CA, Jan. 1998, 308-317

[3] Chavan Suryakant Neelam, Image Steganography – An Overview. International Journal of Recent Scientific Research, Vol. 6, Issue, 6, pp.4800-4804, June, 2015.

[4] Fridrich J.,Goljan M. and Hogea D., New methodology for breaking steganographic techniques for JPEGs, Proceedings of SPIE, vol.5020, pp.143-155, 2003.

[5] Hemalatha S, Acharya U Dinesh, Renuka, A Comparison Of Secure And High Capacity Color Image Steganography Techniques In RGB And YCbCr Domains, International Journal of Advanced Information Technology (IJAIT) Vol. 3, No. 3, June 2013

[6] Kaur Amandeep, Kaur Rupinder, Kumar Navdeep, A Review on Image Steganography Techniques, International Journal of Computer Applications (0975 – 8887) Volume 123 – No.4, August 2015.

[7] Kaur Ratinder, Banga K.V., "Image Security using Encryption based Algorithm" International Conference on Trends in Electrical, Electronics and Power Engineering (ICTEEP 2012) July 15-16,2012 Singapore.

[8] Katoch Munish, Jaswal Reenu, Image Steganography: A Review, International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 4, April 2016.

[9] Khan Farhan Rafat, Muhammad Junaid Hussain, Secure Steganography for Digital Images, International Journal of Advanced Computer Science and Applications, Vol. 7, No. 6, 2016.

[10] Khan Tariq Hamza, Saleem Heebah, Improved Image Steganography Algorithm using Huffman Codes, International Journal of Computer Applications (0975 – 8887), Volume 147 – No.12, August 2016.

[11] Kundra Shivani, Madaan Nishi, A Comparative Study of Image Steganography Techniques, International Journal of Science and Research (IJSR).

[12] Mihir H Rajyaguru, Combination of Cryptography and Steganography With Rapidly Changing Keys, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 10, October2012.

[13] Parmar Ajit, Kumar Maganbhai, A Study and literature Review on Image Steganography, International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 6 (1), 2015, 685-688.

[14] Rao Kameswara M, Reddy Pradeep K. and Saranya Eepsita, K. Security Enhancement in Image Steganography a MATLAB Approach, Middle-East Journal of Scientific Research 23 (2): 357-361, 2015 ISSN 1990-9233, © IDOSI Publications, 2015.

[15] Singh Ajit, Malik Swati, A review on cryptography and steganography, International Journal of Advanced Research in Computer Science and Software Engineering 3(5), May - 2013, pp. 404-409

[16] Singh Rashi, Chawla Gaurav, A Review on Image Steganography, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, May 2014.

[17] Singh Shailendra Deepak, Metri Mrunali, Image Authentication Using Cryptography and Steganography in Network Security, International Journal of Innovative Research in Computer and Communication Engineering.

[18] Shrivastava Pranjal, Singh Pratap Sandeep, A Survey on Image Steganography Techniques using Compression, International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 5, Issue 2, February 2016.

[19] Vyas Krati, Pal B.L., A Proposed Method in Image Steganography to Improve Image Quality with LSB Technique, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014.

[20] William, Cryptography and Network Security principles and practices, William Stallings, pearsons education, first Indian reprint 2003.