TISA: Text and Color Image based Steganography Algorithmic Approach

Deepti Upadhyay[1], Dr. Satyaranjan Patra[2], Ms. Smita Rani Biswal[3]

[1,2,3]*Computer Science& Engineering*

[1]*Bhopal Institute of Technology & Science,* [2]*Bhopal Institute of Technology & Science, Bhopal*

[3]*Padmanava College of Engg., Rourkela*

Abstract - The goal of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. The proposed work is dedicated to design and develop strong steganography based cryptographic approach. In this research work, we proposed Text and Colour Images based Steganography Algorithmic Approach i.e. TISA which incorporates data security by means of digital images. In this approach we hide and recover data using images steganography technique where we encryption and decryption perform using Triple DES algorithm. Our proposed approach is simplified yet efficient algorithm that can implemented for end user application that strictly enforce the data integrity over the communication channel. The performance of the proposed system is measures in terms of time, memory, MSE and PSNR for image quality

Keyword —Steganography, Images, Cryptography, triple DES, Blowfish, Information Security, Data Hiding.

1. INTRODUCTION

For the perception of data security it is more important to protect data from outside the privilege area. Internet had eased the way of transferring data and communicating with other users. In this digital world, a user's personal/banking information may need to be shared with other internet users via the social applications. This information, if not secured, can be intercepted by malicious users vulnerable to illegal use. Also, the security of the secret information in defense and other applications is of major concern. Therefore to protect information from an unauthorized access, we need robust security mechanisms. In this manner security of data is of foremost importance in today's world. Security has become one of the most important factors in communication and information technology [1] [2].

The desire to send a message as safely and as securely as possible has been the point of discussion since time immemorial. Information is the wealth of any organization. This makes security-issues top priority to an organization dealing with confidential data. Whatever is the method we choose for the security purpose, the burning concern is the degree of security. Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication to hide a message from a third party [3].

In this paper we present text and colour image based encryption technique which is implement steganography for information security. Basically encryption algorithms are mathematical model which is used for manipulation of data, to hide required information.

This paper has been organized in four sections. Section II describe relative backgrounds details of the work. III provide our proposed work of this paper. Section V illustrates the performance of the developed system. Section VI summarizes the whole work i.e. conclusion.

2. BACKGROUND

Since the inception of internet the security of information is the most vital factor in information technology and communication. Therefore, the background of a study is an important part of our research paper. It provides the context and purpose of the study. Hence there is need for background study that contribute to prepare proposed system.

2.1 What is Steganography?

Steganography is the idea of hiding private or sensitive data or information within something that appears to be nothing out of the normal. The word steganography comes from the Greek Steganos, which mean covered or secret and –graphy mean writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected [4] and a communication is happening [5]. Secret information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges.

2.2 Different Types of Steganography

Increased use of internet, information becomes available on-internet, a person who possesses an internet can easily get data from internet for information that they want [6]. The use of steganography techniques can be broadly classified in four types which is depict in given diagram:

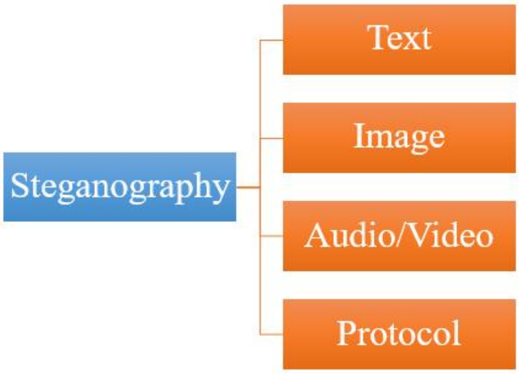

Figure 1. Categories of steganography

Use Text: Hiding information in text is historically the most important method of steganography. An obvious method was to hide a secret message in every nth letter of every word of a text message.

Image: Given the proliferation of digital images, especially on the Internet, and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography.

Audio/Video: To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably

Protocol: The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission [7].

2.3 Image Cryptography

In these days as multimedia data transferred over insecure channel, it becomes an important issue to encrypt image with a suitable image encryption algorithms. An image encryption is different from text due to large processing, pixels definition, time to encrypt and size. This is also a different approach due to different type of attacks possible on text and image data. With the ever-increasing growth of multimedia applications, important issue for communication and storage of images is security, and encryption is one the technique to ensure security. encryption techniques convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the confidential message without a key for decryption [8].

Image cryptography algorithms attempt to convert original images to other images that are difficult to understand in order to keep the image confidentiality between users. In other words, it is important that without a key for decryption, nobody could get to know the content. Majority of traditional algorithms are basically used for encryption of text data; however they do not fit for the multimedia data particularly images due to their huge size. Furthermore, decrypted text result should be similar to the original text, while decrypted image is not required to be similar with original image [9].

3. PROPOSED WORK

This section provide the detail methodology and basic functional aspects of the proposed image cryptography approach and in the next section summarized steps of in algorithmic form.

The working of the proposed image steganography technique is given and explained in details in this section. To understand the core concept of the proposed methodology by using given figure description:

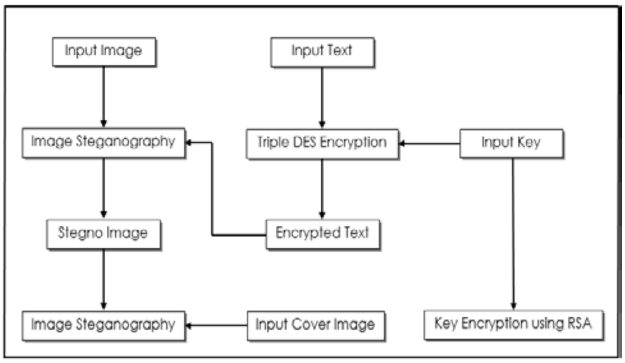

Fig. 2. Data Hiding Process

3.1 Description of the Proposed Flow Diagram

The given flow diagram 2 and 3 depicts image steganography process. Figure 2 show data hiding process and 3 shows data recovery process. Here we are individually describe function flow of both diagram.

In data hiding or encryption process, used LSB steganography technique in which firstly input Stegno image, text data, input key and cover image and processed algorithm by using these four inputs. After input image, we input text which is have to be secure using image. Like an example we input text “You are Awesome” On this input text, we have applied triple DES algorithm for encryption process. For this encryption process simultaneously we input random key. As an example we input key “12345” to triple DES algorithm. By individually on this input key we apply RSA encryption algorithm for the purpose of key encryption is process is an independent. To process input key, we got the encrypted text which is pass to the LSB based steganography approach. After completion of this step we got stegno image. On this stegno image again we have applied LSB steganography technique by using input cover image. Therefore, again new stegno image is produced. Finally, the data have been hide in image successfully and got encrypted stegno image.

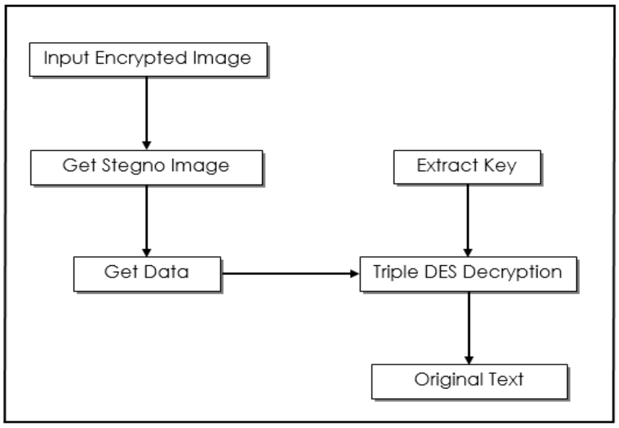

Fig. 3. Data Recovery Process

Figure 3 shows the decryption process. In this phase, we input encrypted image on this encrypted image we apply steganography technique and got stegno image. By this stegno image we get cipher-text. For getting original data, this encrypted data is pass to the triple DES algorithm for decryption process. For this decryption algorithm we also pass extract key by default input process. This process will also know as data recovery process.

3.2. Proposed Algorithm

The last section provides the understanding about the processes involved in the proposed cryptographic technique. This section provides the summarized steps of the process for both the action. This proposed model contains the two major modules first the data hiding process and seconds the recovery of actual text message. Both the phases of system is described using the table 1 and table 2.

Table (1) Data Hiding Process

```
Input: Text$T_i$, Image $I_i$ , Cover Image $I_C$, Key $K_i$
Output: Steganographic Image $I_s$
Process:
1:$\mathrm{I_i} = \mathrm{readInputImage}$
2:$\mathrm{T_i} = \mathrm{InputText}$
3:$\mathrm{K_i} = \mathrm{Inputkey}$
4:$\mathrm{EncK} = \mathrm{RSA.encrypt}\ (\mathrm{K_i})$
5:$\mathrm{EncD} = \mathrm{tripleDES.encrypt}\ (\mathrm{T_i}, \mathrm{K_i})$
6:$\mathrm{stegnoImg_1} = \mathrm{LSBsteganography.hide}\ (\mathrm{I_i}, \mathrm{EncD})$
7:$\mathrm{I_c} = \mathrm{readCoverImage}$
8:$\mathrm{steganoImg_2} = \mathrm{LSBSteganography.hide}\ (\mathrm{I_i}, \mathrm{I_c})$
9:$\mathrm{I_s} = \mathrm{steganoImg_2}$
10:Return $\mathrm{I_s}$
```

Table (2) Data Recovery Process

```
Input:Steganographic Image $I_s$, $EncK$;
Output: Original Text $T_o$
Process:
1:$\mathrm{steganoImg_1} = \mathrm{LSBsteganography.encrypt}\ (\mathrm{I_s})$
2:$\mathrm{EncD} = \mathrm{LSBsteganography.extract}\ (\mathrm{steganoImg_1})$
3:$\mathrm{K_i} = \mathrm{RSA.decrypt}\ (\mathrm{EncK})$
4:$\mathrm{T_o} = \mathrm{tripleDES.decrypt}\ (\mathrm{EncD}, \mathrm{K_i})$
5:Return $\mathrm{T_o}$
```

4. BACKGROUND

The proposed Image steganography technique is implemented successfully and for justifying the results and efficiency of the proposed technique. This section includes the results analysis and performance of the system in terms of their performance parameters.

4.1 Time Consumption

The amount of time required to process the algorithm using couple of encryption and decryption is known as the time consumption (complexity). This can be computed using the following formula:

$$\mathrm{Time\ Consumed} = \mathrm{End\ Time} - \mathrm{Start\ Time}$$

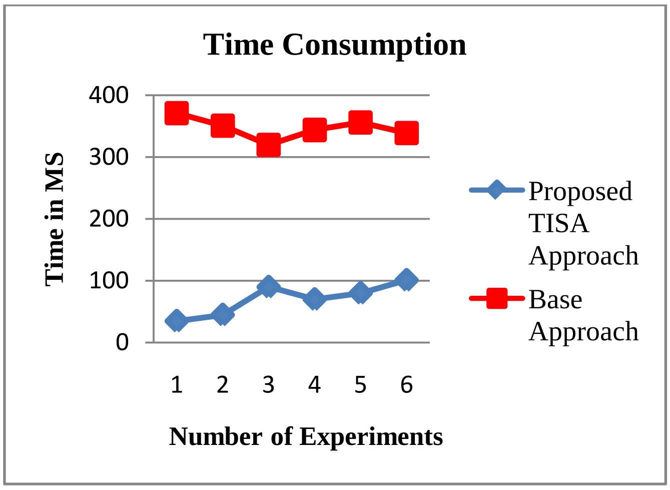

Fig. 4. Time Consumption

The time consumption of the proposed and base approach is given using figure.4. In this figure the X-axis contains number of experiments and the Y axis contains consumed time in terms of milliseconds. According to the comparative results and their analysis the performance of the proposed approach minimize the time requirement to process the algorithm. But the amount of time is increases in similar way as the amount of data for analysis is increases in respective manner.

4.1 Memory Consumption

Memory consumption of the system also termed as the space complexity in terms of algorithm performance. This can be calculated using the following formula:

$$\text{Memory Consumption} = \text{Total Memory} - \text{Free Memory}$$

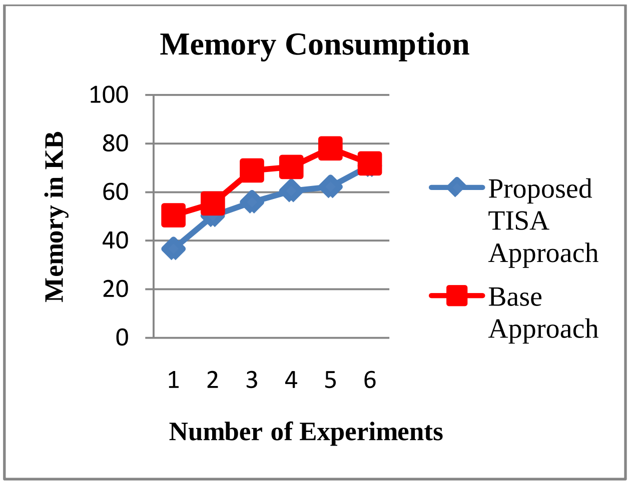

Fig. 5. MemoryConsumption

The amount of memory consumption depends on the amount of data reside in the main memory, therefore that affect the computational cost of an algorithm execution. The performance of the implemented proposed text and colour image steganography approach and base approach is illustrating using figure 5. For reporting the performance the X axis of figure contains the different number of times code execution to and the Y axis shows the respective memory consumption during execution in terms of kilobytes (KB). Additionally, red and blue line shows the base and proposed TISA approach respectively. According to the achieved performance the algorithm demonstrates similar behaviour while we executing the system repeated, but the amount of memory consumption is decreases with the amount of data.

4.3 Mean Square Error (MSE)

The mean squared error (MSE) of an estimator is one of many ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated. MSE is a risk function, corresponding to the expected value of the squared error loss or quadratic loss.

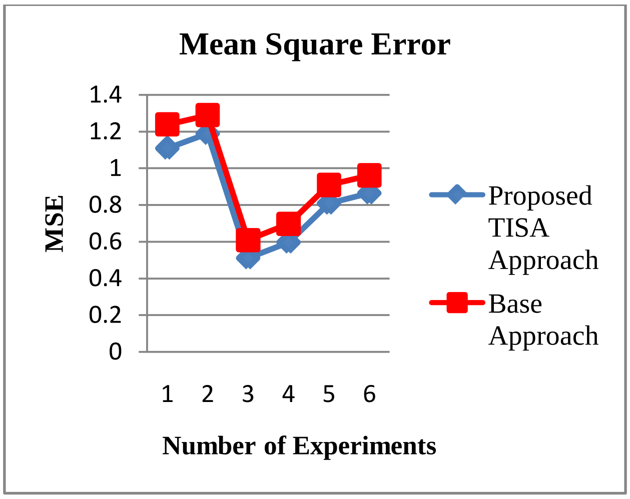

Fig. 6. MSE

In given figure 6, depiction of mean square error of input data images for proposed and base method. The Mean Square Error is defined as the square of the difference between the pixel values of the original image and the Stego image and then dividing it by size of the image. The proposed TISA approach indicated by blue line and base method depict by red line. The lower value of Mean Square Error (MSE) signifies lesser error in the Stegno image in other words better quality.

4.4Peak Signal to Noise Ratio (PSNR)

The PSNR measures the peak signal-to-noise ratio between two images. This ratio is often used as a quality measurement between the original and a compressed image. Higher the PSNR means better the quality of the compressed or reconstructed image. The PSNR value can be calculated as:

$$\text{PSNR} = 10\log_{10}\left(\frac{\text{R}^2}{\text{MSE}}\right)$$

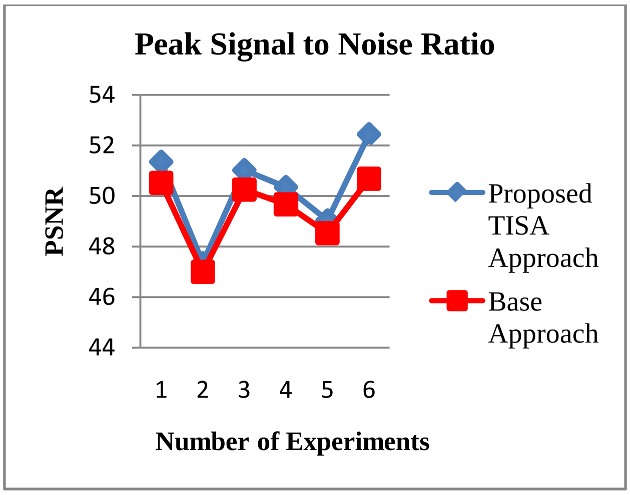

Fig. 7. PSNR

Peak signal to noise ratio of both for both approaches are given using figure 7. In this diagram the X axis shows the different experiments and the Y axis shows the obtained

PSNR ratio. In this figure contains the red and green line to show the performance of the base and proposed respectively. The amount of computed PSNR is fluctuating with the image quality therefore that is not depends on the image size that is depends on the quality of image.

5. CONCLUSION

Information security is greatly essential over the unsecured shared medium. Due to the exponential growth of internet users, unauthorized access of information has become one of the most significant problems. Therefore, to provide more security to the information at the time of communication over unsecured channel, image steganography, an advance technique for data security is needed.

In this security mechanism, the intention of the entire research work is to enhance security of user confidential data by proposing of image steganography technique. In the proposed TISA approach, two input data are required first the test image which is required to hide and the second text data on which basis key is entered and the data is required to be hide. In this approach, we have proposed cryptographic based steganographic algorithm which is based on pure encryption and decryption process by means of triple DES. Additionally, in this we have used RSA algorithm for key encryption. The final outcome of the approach is used for network transmission or other task. Similarly the decryption operation required to recover the original data.

ACKNOWLEDGMENT

The preferred spelling of the word “acknowledgment” in American English is without an “e” after the “g.” Use the singular heading even if you have many acknowledgments. Avoid expressions such as “One of us (S.B.A.) would like to thank.” Instead, write “F. A.

REFERENCES

[1] KshetrimayumJenita Devi, “A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique”, B.Tech. Project Thesis May 2013, available online at: http://ethesis.nitrkl.ac.in/4626/1/109CS0608.pdf

[2] KetkiThakre and NehalChitaliya, “Dual Image Steganography for Communicating High Security Information”, International Journal of Soft Computing and Engineering (IJSCE), Volume-4, Issue-3 July 2014.

[3] Komal Patel and SumitUtareja, “Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm”, International Journal of Computer Applications (IJCA), Volume 63– No.13, February 2013.

[4] Mirza AbdurRazzaq and Mirza Adnan Baig, “Digital Image Security: Fusion of Encryption, Steganography and Watermarking”, (IJACSA) International Journal of Advanced Computer Science and Applications, Volume 8, Number 5, 2017

[5] R. Popa,”An Analysis of Steganographic System”, The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, May 25, 1998.

[6] Anderson, R.J. &Petitcolas, F.A.P., “On the limits of steganography”, IEEE Journal of selected Areas in Communications, May 1998.

[7] Ahsan, K. &Kundur, D., “Practical Data hiding in TCP/IP”, Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002.

[8] S. V. Kamble and B.G. Warvante, “A Review on Novel Image Steganography Techniques”, IOSR-JCE-2004

[9] Nitin Rawal and ManojDhawan, “A Survey Report on Image Encryption Techniques”, International Journal of Engineering Research & Technology (IJERT), Volume 2, October 2013.