Implementation of Improved Steganography for Hiding Text on Digital Data

Aditi Soni[1], Sujit K. Badodia[2]

[1] SVITS, Indore Sanwer Road, Gram Baroli, Alwasa, Indore (MP), 45311, India

Abstract: ***Data hiding techniques have taken vital role with the hasty growth of exhaustive transfer of multimedia content and secret communications. Steganography is the art of hiding information in ways that prevent recognition. Steganography means hiding a secret message (the embedded message) within a larger one (source cover) in such a way that an observer cannot be able to sense the presence of contents of the hidden message. Lots of different carrier file formats can be used, but digital images are the most popular because of their occurrence on the Internet. In this, data hiding method that utilizes encoding on letters, then compression of that letters and then a new technique is proposed which is combination of two techniques. Results came from the experiment show that the proposed method can bury a large amount of secret data and also keep very high security, when the message is decrypted.***

Keywords: Steganography, Projection, Compression, Data hiding, Angle, Cover, Stego

1. Introduction

Technique to broadcast a secret data from a sender to receiver is called Steganography. It will be done in such a way such that an intruder does not suspect the endurance of the message. Generally this can be done by burrying the secret message within a different digital medium such as text, image, audio or video. Usually, data will appear to be something else: images, articles, shopping lists, or some other “cover-text” and, naturally, the hidden message may be in invisible ink between the observable lines of a private letter. It is a high security technique for long data transmission. Steganography can be used to conceal important data inside another file so that the parties intended to get the message knows the presence of secret message. The general model of data hiding can be described in Fig 1. The embedded data is the message that one wants to send in secret. There is range of methods of steganography

- Least significant bit (LSB) method
- Transform domain techniques
- Statistical methods
- Distortion techniques

The Steganography system scenario is shown in the Figure 1

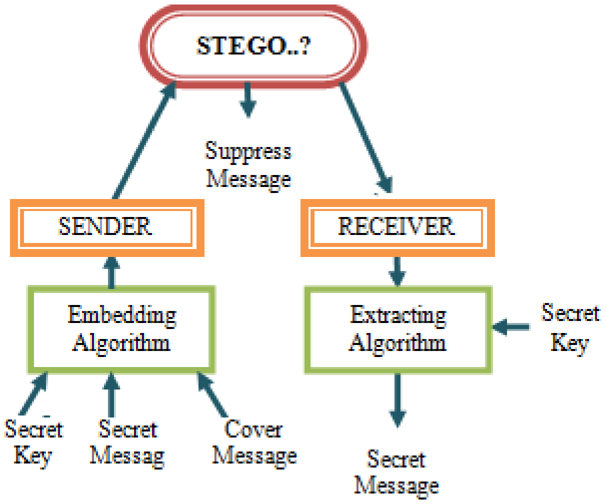


Figure 1: Steganography System Scenario

2. Steganography in Digital Mediums

Depending on the type of the cover object there are lots of suitable steganographic techniques which are followed in order to attain security. It can be shown in Figure 1.

- **Image Steganography:** Taking the cover object as image in Steganography is known as image Steganography. Normally, in this technique pixel intensities are used to conceal the information.
- **Network Steganography:** When taking cover object as network protocol, such as TCP, UDP, ICMP, IP *etc*, where protocol is used as carrier, is known as network protocol Steganography.
- **Video Steganography:** Video Steganography is a technique to hide any kind of files or information into digital video format. Video which is the grouping of pictures is used as carrier for hidden information. Usually discrete cosine transform (DCT) modify values (*e.g.*, 8.667 to 9) which is used to hide the information in each of the images in the video, which is not perceptible by the human eye.
- **Audio Steganography:** When audio is taking as a carrier for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI, MPEG or *etc* for steganography.
- **Text Steganography:** General technique in text steganography, like number of tabs, white spaces, capital letters, just like Morse code and *etc* is used to attain information hiding.

3. Literature Review

Ki-Hyun Jung [2014] proposed the semi-reversible data hiding method based on interpolation and LSB substitution. The interpolation method has been preprocessed before burrying secret data for the purpose of advanced capacity and best quality. Then, the LSB substitution method was applied for embedding secret data. The cover image with the scaled down size and secret data could be extracted from the Stego-image without the need of any extra information. The experimental results showed that the average PSNR was 43.94 dB and the capacity was 393,216 bits when k=2. In the case of k=3, we demonstrated that the PSNR and capacity were 37.54 dB and 589,824 bits, respectively

Mehdi Hussain [2013] gave an overview of different Steganography techniques, its major types and classification of Steganography which have been proposed in the literature during last few years. We have critical analyzed different proposed techniques which show that visual quality of the image is ruined when hidden data increased up to certain limit using LSB based methods. And many of them embedding techniques can be broken or shows indication of alteration of image by careful analysis of the statistical properties of noise or perceptually analysis.

Atallah M [2012] proposes a new Steganography technique which was presented, implemented and analyzed. The proposed method hides the secret message based on searching about the matching bits between the secret messages and image pixels values. 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.

Mamta Juneja [2014] proposed technique achieves the goal of an implementation of new steganography approach for images which is the combination of three new techniques a) Hybrid feature (line/edge/boundary/circle) detector technique integrating Canny and Enhanced Hough transform for bifurcating an image into edge and smooth areas b) Two Component based LSB Substitution Technique for hiding encrypted messages in edges of images c) Adaptive LSB substitution technique for hiding messages to smooth areas. It achieves the target of 50% hiding capacity and Imperceptibility (PSNR value) with minimum MSE (mean square error) while hiding more data on edges than smooth areas as edges being high in contrast, color, density, frequency and other noise disturbances can tolerate more changes in their pixel values than smooth areas.

4. Methodology

A data hiding method that is the combination of Projection of the letters, then compression of text and then new technique is introduced, which is the combination of permutation straddling and Matrix Encoding is proposed. The part of projection is done by rotating the letters of the word, one by one by 85°. Contrasting stream media, image files only provide a partial steganographic capacity. In the majority of the cases, a buried message does not require the full Space. That‟s why, a part of the file left as unused. Fig. 2 shows, that the changes focus on the starting segment of the file, and the unused part resides on the end. To avert attacks, the embedding function should use the carrier medium as usual as possible. The embedding density should be the equal everywhere.

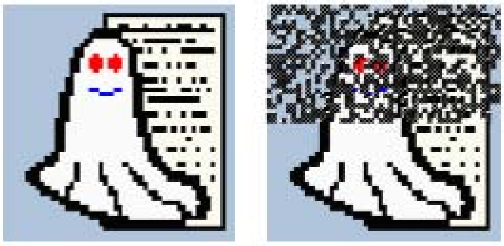


Figure 2: Continuous embedding concentrates changes

First we apply Permutative Straddling. In this, some well-known steganographic algorithms widen out the message over the whole carrier medium. The straddling mechanism shuffles all coefficients using a permutation. Then, embeds into the permuted sequence. The contraction does not change the number of coefficients. It only changes their values. The permutation depends on a key derived from a password. It delivers the steganographically changed coefficients in its original sequence to the Huffman coder. With the correct key, the receiver is able to repeat the permutation. Fig. 3 shows the consistently distributed changes over the whole image.

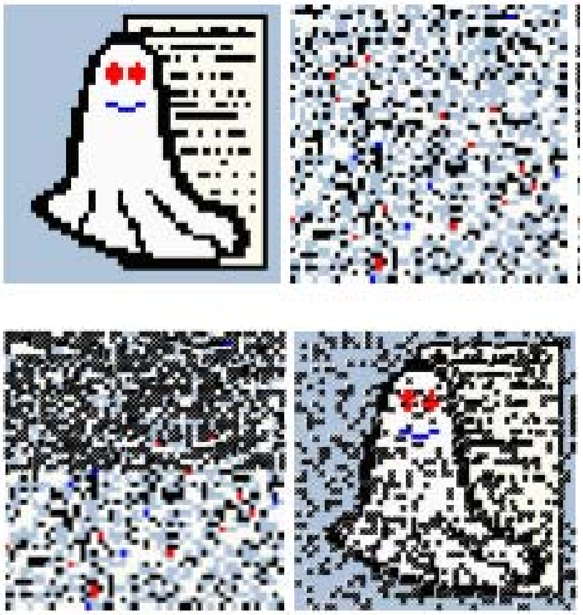


Figure 3: Permutative embedding scatters the changes

And then Matrix Encoding is done. In addition, the original image is not needed to pull out the hidden message. The proposed receiver need only possess a key in order to reveal the secret message. The existence of the hidden information is virtually untraceable by human or computer analysis.

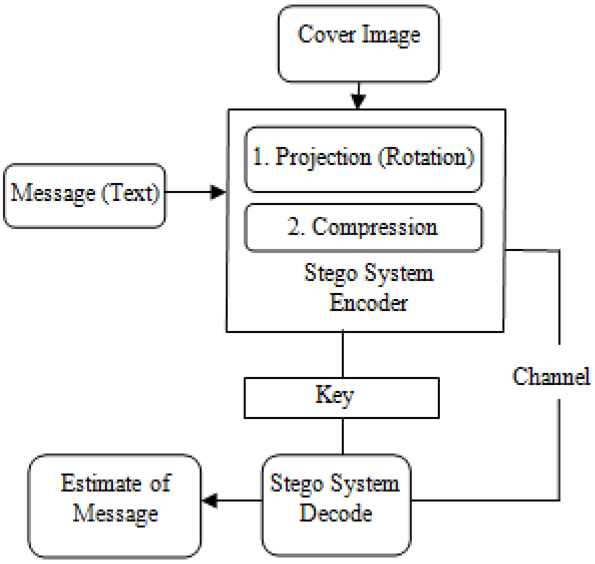
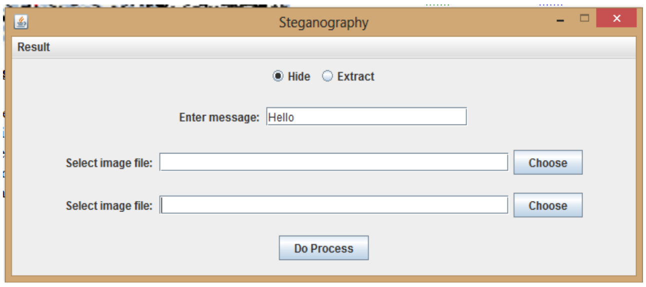


Figure 4: Block Diagram of Proposed System

Fig 4 shows that the sender initiates the message as text for appending on the cover image then it processed with the help of the projection which means that it will be rotated by 85^0 so that letters are slanted. It will helpful for our method and after this compression will be done. This data uploaded or merge with the cover image and that image not distorted in any manner. Send it to the receiver with the secure channel and at the end of the receiver key used for the decryption of the data and successfully receive the data.

5. Results and Discussion

In this Experiment, first we have to select the option whether we want to hide the data or extract the hidden data. Lets just take the condition in which we are going to hide the data in the image. So in this, we have to enter the text or message, which is to be hide in the image. Lets take an example, we hide the word "Hello"in the image as shown in fig 5



Steganography

Result

● Hide ○ Extract

Enter message: Hello

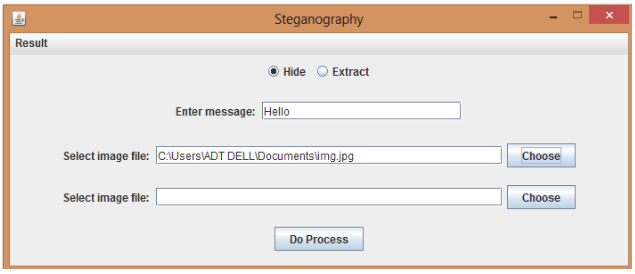
Select image file: Choose

Select image file: Choose

Do Process

Figure 5: Enter the message whch is to be hide

Then select the image in which we want to hide the text. Let"s just take an example, in which data is to be hidden in image named img.jpg as shown in fig 6. Then generate the new image file in which the data is hidden. This image is sent to the receiver from which data is to extracted. Lets just take, the new image which is to be generated named hello.jpeg as shown in fig 7



Steganography

Result

● Hide ○ Extract

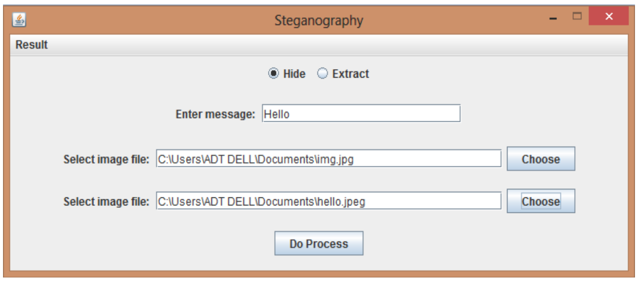
Enter message: Hello

Select image file: C:\Users\ADT DELL\Documents\img.jpg Choose

Select image file: Choose

Do Process

Figure 6: Select the image



Steganography

Result

● Hide ○ Extract

Enter message: Hello

Select image file: C:\Users\ADT DELL\Documents\img.jpg Choose

Select image file: C:\Users\ADT DELL\Documents\hello.jpeg Choose

Do Process

Figure 7: Generate the image

When we click on the "Do Process" Button, the text which is to be hide in the image will be rotated. And we get the Rotated message which is difficult to recognize by the intruder. The result rotated message will be shown as it is shown in fig 8

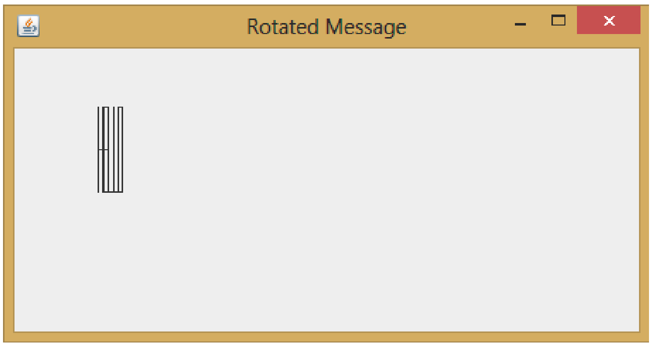
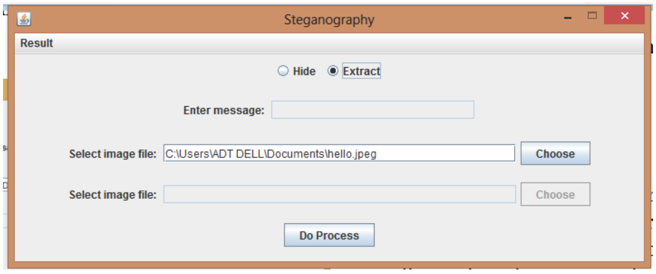


Figure 8: Result Rotated Image

Now, we have to select the option to extract the hidden data. Select the image from which we want to extract the text. Select the image hello.jpeg from the document or wherever you save the image. And click on the button "Do Process" as shown in fig 9.



Steganography

Result

○ Hide ● Extract

Enter message:

Select image file: C:\Users\ADT DELL\Documents\hello.jpeg Choose

Select image file: Choose

Do Process

Figure 9: Select the image

When we click on the "Do Process" Button, the text which is to hidden in the image will be rotated again. And we get the Inverse Rotated message. The message is easily understood by the receiver now. The result inverse rotated message will be shown as it is shown in fig 10

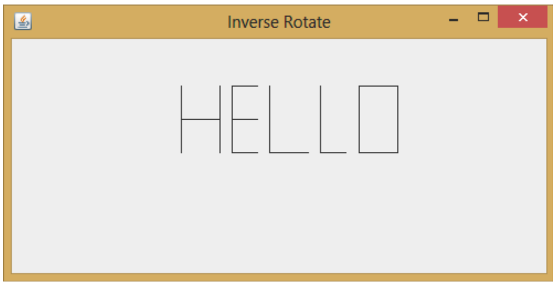


Figure 10: Result Inverse Rotated Image

When we click on the result button which is located on the top of the screen, we get the dropdown option as „Graph‟ as shown in Fig 11. When we click on Graph option, we get four graphs.

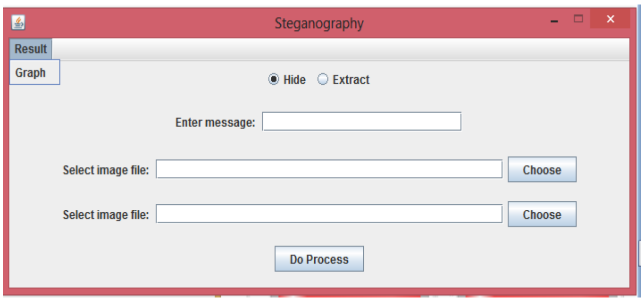


Figure 11: Dropdown option for Graph

First two graphs are for hiding process. In Fig 12, first graph is between message length and time and second graph is between File size and time. We can clearly see that there is least amount of difference between the old record and new record.

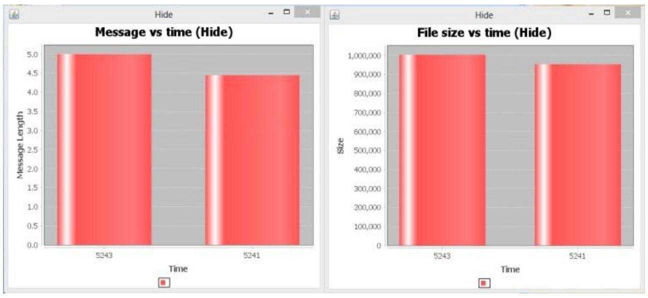


Figure 12: Graphs for Hiding Process

The other two graphs are for extracting process. In Fig 13, same criteria are taken. We can clearly see here also least amount of difference between the old record and new record.

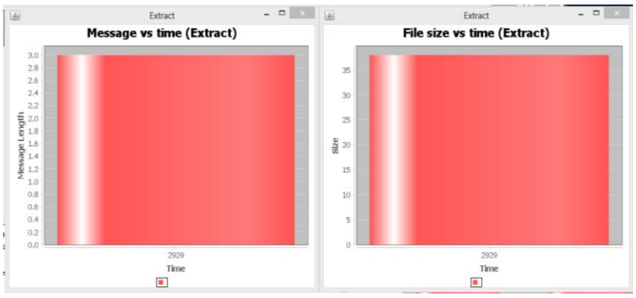


Figure 13: Graphs for Extracting Process

6. Conclusion

In this paper, planned data hiding method that utilizes Projection of the letters, then compression of that letters and then Hiding the data with Permutation Straddling and Matrix Encoding. Also give an overview of different types of Steganography techniques, classification of Steganography which have been proposed in the journalism in last few years. Experimental results show that the proposed method can implant a huge amount of secret data while keeping very high security, as when the message is decrypted. Resistant to statistical attacks.

References

[1] Ki-Hyun Jung , Kee-Young Yoo "*Steganographic method based on interpolation and LSB substitution of digital images*" Springer Science+Business Media New York 2014 DOI 10.1007/s11042-013-1832-y.

[2] Stefan Katzenbeiser & Fabien A.P.Petitcolas(1999), Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Computer Security series, Boston, London.

[3] Chan CK, Cheng LM (2004) Hiding data in images by simple LSB substitution. Pattern Recogn 37:469–474

[4] Chang CC, Lin MH, Hu YC (2002) A fast and secure image hiding scheme based on LSB substitution. Int J Pattern Recog 16(4):399–416.

[5] Johnson, Neil F., "Steganography", 2000, URL: http://www.jjtc.com/stegdoc/index2.html

[6] Huang LC, Tseng LY, Hwang MS (2013) A reversible data hiding method by histogram shifting in high quality medical images. J Syst Software 86:716–727

[7] Johnson NF & Jajodia S (1998) Exploring steganography: seeing the unseen. Comput Pract 26–34

[8] Jung KH, Yoo KY (2009) Data hiding method using image interpolation. Comput Standards Interfaces 31: 465–470

[9] Jung KH & Yoo KY (2013) Data hiding using edge detector for scalable images. Multimedia Tools and Appl doi:10.1007/s11042-012-1293-84

[10] Lee CF, Huang YL (2012) An efficient image interpolation increasing payload in reversible data hiding. Expert Syst Appl 39:6712–6719

[11] Lee YP, Lee JC, Chen WK, Chang KC, Su IJ, Chang CP (2012) High-payload image hiding with quality recovery using tri-way pixel-value differencing. Information Sciences 191:214–225

[12] Lehmann TM, Gonner C, Spitzer K (1999) Survey: interpolation methods in medical image processing. IEEE Trans Med Imaging 18(11):1049–1075

[13] Mielikainen J (2006) LSB matching revisited. IEEE Signal Processing Letters 13:285–287

[14] Ni Z, Shi YQ, Ansari N, Su W (2006) Reversible data hiding. Circ Syst for Video Technol IEE 16:354–362

[15] Swanson M, Kobayashi M, Tewfik A (1998) Multimedia data embedding and watermarking technologies. Proc IEEE 86(6):1064–1087

[16] Mehdi Hussain and Mureed Hussain (2013) A survey of Image Steganography Techniques. International Journal of Advanced Science and Technology Vol. 54.

[17] Atallah M. Al-Shatnawi A New Method in Image Steganography with Improved Image Quality. Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 391

[18] Mamta. Juneja, and Parvinder S. Sandhu An Analysis of LSB Image SteganographyTechniques in Spatial Domain International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 1, Issue 2 (2013) ISSN 2320–401X (Print)

Author Profile

Aditi Soni is persuing MTech(Final Year) in Software Engineering from Sri Vaishnav Institute of Technology and Sciences, Indore. And completed Bachelor of Engineering in Information Technology from Shri Ram Institute of Technology, Jabalpur. She has publushid her papers in International Journal Of Engineering Sciences & Research Technology, International Journal of Engineering Research and General Science, International Journal for Scientific Research & Development.