KVL Algorithm: Improved Security & PSNR for Hiding Image In Image Using Steganography

Kamlesh Lakhwani[1], Kiran Kumari[2]

[1] *Dept of Computer Science and Engineering , Suresh Gyan Vihar University,Jaipur,Rajasthan,India*
[2] *Dept of Information Technology, Suresh Gyan Vihar University, Jaipur, Rajasthan, India*

ABSTRACT:

The captivating increase in internet communication in the last few era, guide the necessity of the secure communication of data between two or more remote receivers. Mainly security troubles a lot during transmission of images and videos over internet communication. The methods or technique for secure real time image transmission, in this technique cover (dummy) image will be used as a carrier of secret (main/original) image will be hiding inside the cover image using LSB algorithm. In addition to this a key will be generated with help of Triple DES algorithm using to hide secret image inside the cover image. Secret image is encrypted using the key and then inserted into the cover image. The key is same at the receiver side to release the hidden image inside the cover image.

KEYWORDS: *LSB, DES, RLE, Image Steganography, Secret key, Cover Image, Secret Image.*

I. INTRODUCTION

The existence of internet networks has encouraged new problems with security and confidentiality. Having protected and consistent means for communicating with images and video is satisfying a need and its correlated issues must be carefully considered. Hence, image protection and image encryption have become significant. The image can be considered nowadays, one of the most important practical forms of information. Image and video encryption have applications in various ways like internet communication, mobile communication, and multimedia communication, and telemedicine, military and medical imaging communication.In case of internet and mobile communication the images or videos are transferred hence, the most important complication is speed of procedure. In the digital era nowadays, the protection of digital image has become more and more important because of the advances in multimedia and communication technology. We can appreciate that more and more works have been developed for security issues to protect the data from possible unofficial instructions.

[1.1] Steganography Concept

Steganography refers to the science of “invisible” communication. Steganography is way by which information in hide behind any other in such a way so it looks cool and no differences occurs in original and Stego Information. Steganography basically gives importance to the hiding of information whereas the cryptography based on transforming the information from one form to another based on some steps known as algorithms and unique identifiers known as keys.

The basic structure of Steganography is made up of three components.

- Cover /carrier image
- Message to be hidden (Secret Image)
- Key

Figure 1.1 illustrates Steganography Components.

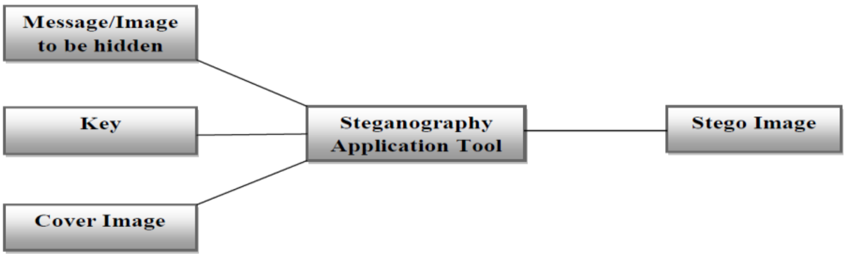


Figure 1.1 Basic Concept of Steganography

[1.2] Steganography Categories

Steganography can be applied to images, text, videos, digital signals as well as continuous signals and other information formats, but the preferred formats are those which repeat the data. Repetition can be in the form of repetition of bits which are responsible to visualize the information [1]. Repeated bits of an object are those bits that can be altered without the alteration being detected easily [2]. Image and video files especially comply with these requirements, while research has also uncovered other file formats that can be used for information hiding.

There are four main categories of file formats that can be used for Steganography shown in figure 1.2 below.

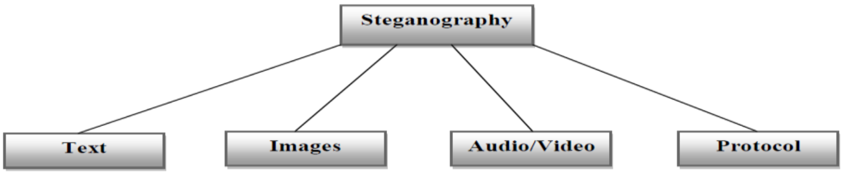


Figure 1.2 Categories of Steganography

[1.3] Image Steganography

Image Steganography is divided into two sub-categories

1) Image Domain Steganography
2) Transform Domain Steganography

Both image and transform domain Steganography further divided into sub categories as shown in figure1.3 given below.

Image domain also known as spatial domain methods insert messages in the intensity of the pixels directly. Image domain Steganography take in bit-wise methods that apply bit insertion and noise manipulation. Sometimes it is characterized as simple systems. The image formats that are most appropriate for image domain Steganography are lossless Steganography and the techniques are normally dependent on the image format.

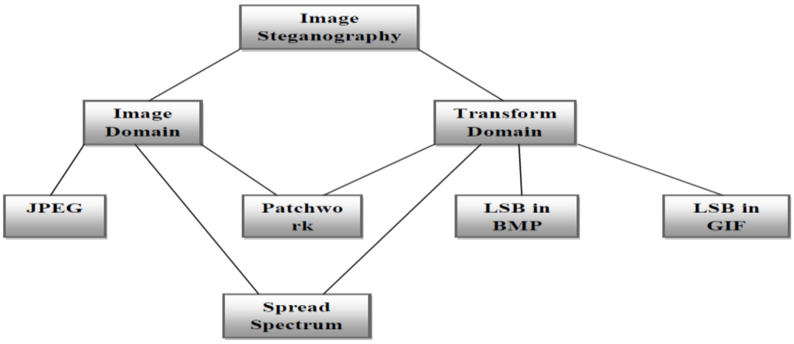


Figure 1.3 Categories of Image Steganography

Transform domain also known as frequency domain Steganography methods. In this method images are first transformed and then the message is inserted in the image. Transform domain Steganography involves the manipulation of image transforms and algorithms.

[1.4] Steganography Techniques

In all the methods of Steganography something is done to conceal a message; naturally, these actions or techniques can be separated and analyzed to learn what is happening during the whole process. There are six techniques of Steganography which are as follows:

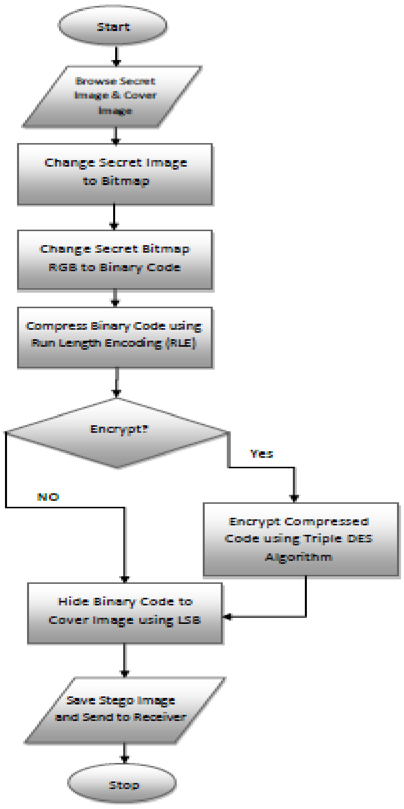
[1] Substitution Techniques
[2] Transform Domain Techniques
[3] Spread Spectrum Technique
[4] Statistical Techniques
[5] Distortion Techniques
[6] Cover Generation Techniques

II. PROPOSED METHODOLOGY

Steganography was previously done on text and images many times using the LSB algorithm. In our methodology we tried to come with a solution which can make it easy and perfect, we tried to provide concept by which lossless communication can take place. As I previously mentioned that Image Steganography is of two types; we have taken the goodness of both in our methodology. Using the Transform domain we changed the Secret image to its RGB color components, converted their values in binary code and then using the RLE (RUN LENGTH ENCDING) compression algorithm compressed the binary code up to 35 percent. To perform the security task we provided encryption module, using the standard Triple DES and Hash code (MD5) Algorithms. Then using the Image Domain Steganography we directly put this encrypted and compressed binary code to the cover/dummy image and produced the Stego Image which is used for the communication over networks.

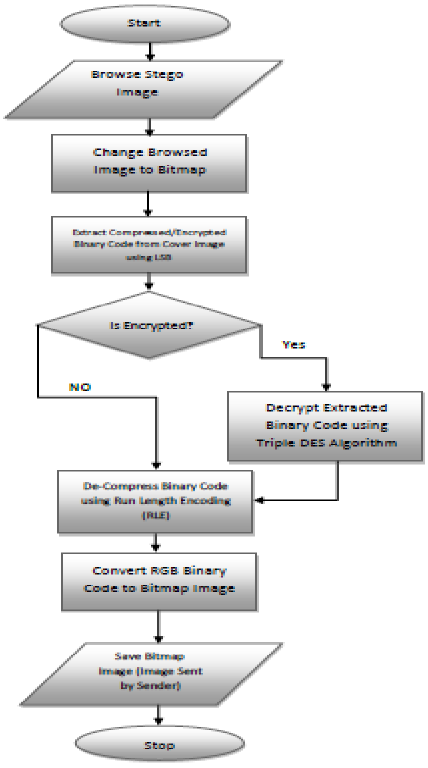
[2.1] Flow Chart

[2.1.1] Image Hiding


Start
Browse Secret Image & Cover Image
Change Secret Image to Bitmap
Change Secret Bitmap RGB to Binary Code
Compress Binary Code using Run Length Encoding (RLE)
Encrypt?
Yes
NO
Encrypt Compressed Code using Triple DES Algorithm
Hide Binary Code to Cover Image using LSB
Save Stego Image and Send to Receiver
Stop

Flow-Chart of Image Steganography: Image Hiding

[2.1.2] Image Extraction


Start
Browse Stego Image
Change Browsed Image to Bitmap
Extract Compressed/Encrypted Binary Code from Cover Image using LSB
Is Encrypted?
Yes
NO
Decrypt Extracted Binary Code using Triple DES Algorithm
De-Compress Binary Code using Run Length Encoding (RLE)
Convert RGB Binary Code to Bitmap Image
Save Bitmap Image (Image Sent by Sender)
Stop

Flow-Chart of Image Steganography: Image Extraction

[2.2] Algorithm

[2.2.1] Image Hiding

```
Hide (secret, cover, key)
[1]  Start
[2]  Resize Secret and Cover Image in 1:9
[3]  Read Secret Image as Bitmap
[4]  Read Cover Image as Bitmap
[5]  Change Secret Image Pixel RGB component values to Binary Code
[6]  Compress Binary Code using RLE Compression Algorithm
[7]  Check for Key
[8]  If Key is not blank
[9]  Apply Triple DES Encryption using the key
[10] Embed Encrypted Binary Code in to the Cover Image Pixel Components using LSB Algorithm
[11] Save Stego Image to Computer
[12] Transfer it over the Network with the shared key
[13] Stop
```

[2.2.2] Image Extraction

```
Extract (stego_image, key)
[1]  Start
[2]  Read Stego Image as Bitmap
[3]  Extract Secret Image Encrypted Binary Code from the Stego Image using LSB Algorithm
[4]  If Key is not blank
[5]  Apply Triple DES Decryption using the key
[6]  Decompress Binary Code using RLE Compression Algorithm
[7]  Convert RGB Binary Code to Secret Image RGB Component
[8]  Save Secret Image to Computer
[9]  Stop
```

III.COMPARATIVE ANALYSIS

Figure 3.1 Lena Cover Image

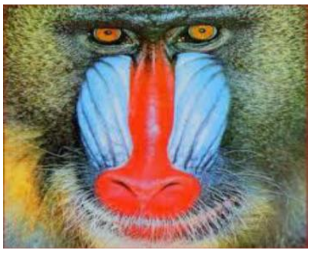


Figure 3.2 Baboon Secret Image

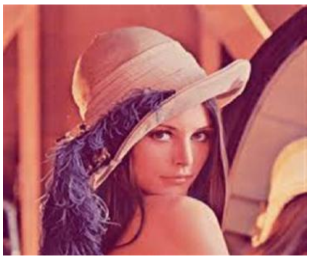


Figure 3.3 Lena Stego Image

Lena Image	LSB3	Jae Gilyu	First component alteration technique	Improved LSB	KVL Method
PSNR	37.92	38.98	46.11	46.65	51.98

Table 3.1 Comparative study of various techniques with proposed Method

The results are then compared with various steganography methods as shown in the table 3.1[3, 4]. Experimental result had shown the strong point of this method as compare to other methods [3, 4]. For this method we embedded the secret image in cover image and get stego image. The PSNR Peak Signal to Noise Ratio) of stego-image is calculated and compared with previous work.

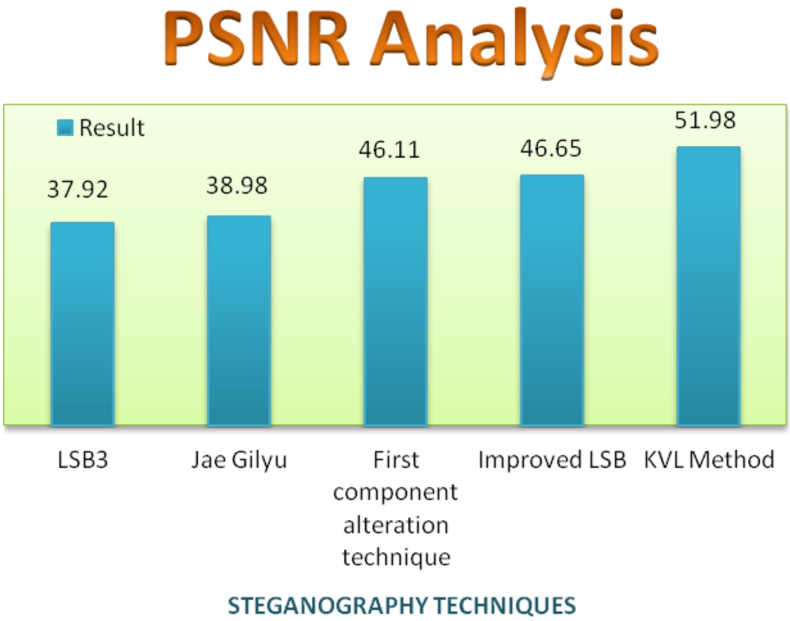


Figure 3.4 PSNR Analysis of different Steganography techniques

Comparative result in table 3.1shown that the PSNR will increase in proposed work so there is no difference in visible quality of cover (original) image and stego image. This method is applicable for both 24-bit color image and 8-bit grayscale image.

IV. CONCLUSION

We have proposed KVL Algorithm for image hiding in image using the LSB based algorithm. In this least significant bit of cover image are used and secret image most significant bits of color components are hidden in them. 3 RGB Pixels are used to hide 8 bit information. Our technique gives the image quality of high standards and with the necked eyes it is impossible to find the variations in the Stego image. The result comparisons also support the statement strongly. Experimental result shows the effectiveness of the proposed method. The results obtained also show significant improvement in PSNR than the method proposed in ref. [3, 4] with respect to image quality and computational efficiency.

V. FUTURE WORK

KVL Algorithm shown great commitment in the still images; the quality it managed for the cover, stego and extracted images are of extreme level. Now we are having a hope and going to implement this algorithm in video-streaming also. Video is a collection of frames which are streamed at particular streaming rate measured at a specific frame per second rate. We can collect pick any frame from the image and can use it as cover/dummy image to hide the secret information or images. This will definitely give a great extend to the security standards in the network based communication.

REFERENCES

[1] Currie, D.L. & Irvine, C.E., “Surmounting the effect of lossy compression on Steganography”, 19th National Information System Security Conference, 1996.

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

[3] Amanpreet Kaur1, Renu Dhir2, and Geeta Sikka3. “A New Image Steganography Based On First Component Alteration Technique” (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No.3, 2009.

[4] Vijay Kumar Sharma, Vishal Shrivastava, “A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimize Detection”, (JATIT) Journal of Theoretical and Applied Information Technology, Vol.36 No.1, February 2012.

[5] Mrs. Richa Raja Gautam, Prof Rakesh Kumar Khare, “Real Time Image Security For Mobile Communication Using Image Steganography” (IJERT) International Journal of Engineering Research & Technology, Vol. 1 Issue 8, October 2012.

[6] Sonia Sharma, Anjali Dua, “Design and Implementation of an Steganography Algorithm Using Color Transformation”, (IJRTE) International Journal of Recent Technology and Engineering, Vol.1, Issue 2, June 2012.

[7] Himanshu Gupta, Prof. Ritesh Kumar, Dr. Soni Changlani, “Enhanced Data Hiding Capacity Using LSB- Based Image Steganography Method”, International Journal of Engineering Technology and Advanced Engineering, Vol 3, Issue 6, June 2013.

[8] Ravinder Reddy Ch, Roja Romani A, “ The Process of Encoding and Decoding of Image Steganography using LSB Algorithm”, IJCSET, Vol 2, Issue 11, November 2012.

[9] Priya Thomas, “Literature Survey on Modern Image Steganographic Techniques”, International Journal of Engineering & Technology, Vol. 2 Issue 5, May 2013.

[10] Shikha Sharda, Sumit Budhiraja, “Image Steganography: A Review”, International Journal of Emerging Technology and Advanced Engineering, Vol. 3 Issue 1, January 2013.