Three Level Security Technique of Image Steganography with Digital Signature Framework

Rahul Kamboj[1], Madhav Prasad Khanal[2]

[1]PG Scholar, Department of ECE, Punjab College of Engineering & Technology, Lalru, PUNJAB -140501
[2]Asst. Professor, Department of ECE, Punjab College of Engineering & Technology, Lalru, PUNJAB -140501

Abstract— *Steganography technique is more popular in recent years due to high level security involved in transferring the data. In image stegnography scheme the secret message is hidden inside a digital image by using different techniques. Least significant bit (LSB) is the commonly used technique foe embedding the information inside a cover image. A three level security scheme has been developed by using MATLAB with digital signature framework. The developed technique has a simpler approach as compared to other complex technique involved in secure transmission of data. The results are analyzed for different images using Peak Signal to noise ratio (PSNR) and the results reveals that the average PSNR value is enhanced by 15.83% compared to the reference values.*

Keywords — Image steganography, PSNR, MATLAB, LSB, Digital signature.

I. INTRODUCTION

As the usage of internet is increasing rapidly with digitization the main concern in the field of information technology (IT) and communication is security of data. Stegnography is the art and science of invisible communication. This technology conceal a message or an image within another image making it completely hidden that helps in secure transmission of information over insecure channel [1]. Image stegnography works on concept of hiding information exclusively in the form of images. Stegnography and cryptography techniques are used for security dealing with passing of secured information. Cryptography deals with maintain secrecy of content message whereas stegnography aims on maintain the secrecy of message. Data hiding method by improved LSB substitution process [2] which improves the PSNR with respect to image quality and computation work. The stego image quality can be greatly improved with minimum computational complexity by applying LSB image hiding method. The effectiveness of the proposed method is verified experimentally by achieving the balance between the security and the image quality. Exhaustive literature review of different stenographic techniques and their classification of the passed decade [3] highlighting the visual quality of the image provides a guideline for researchers and scientist. A method for hiding information on billboard display is presented [4] for online hiding of information on the output screen on the output screen of the instrument. Private marking system using symmetric key steganographic techniques and LSB techniques is used for hiding the secret information. Babloo Saha and Suchi Sharma [5] compiled research work in the field of stegnography deployed in spatial, transform and compression domain of digital images and conclude that transform domain techniques make changes in the frequency coefficients instead of manipulating the image pixels directly, leading to the minimum level of distortion thus preferred over spatial domain techniques. Framework to support the concept of image stegnography with structural design signature environment is given by Alam and Islam [6]. The experimental work by the author was conducted on smaller domain with a future plan to perform the experiment on standard data sets to test the effectiveness of framework. Arun Kumar et al. [7] proposed two simple fuzzy filters for the removal of impulse and gaussian noise in gray scale and color images. Hsien-Wei-Yang [8] proposed a reversible data hiding algorithm based on interleaving maximum-minimum histogram. In view of the above discussion the present work incorporates a MATLAB scheme for three level secure transmissions of data with digital signature framework.

II. METHODOLOGY

Following methodology is adopted for carrying out the proposed work as follows:

1. Selection of stego image-1 (SI-1) from the database.
2. Selection of cover image (CI-1) from the database.
3. Hide stego image-1 (SI-1) into cover image (CI-1) using LSB method which is modified by using MATLAB. The MATLAB program is modified in such a manner that instead changing only one bit, the program intends to change more than one bit for security purpose.
4. Apply the digital signature on the cover image-1 (CI-1) after embedding stego image into it.

5. Selection of cover image-2 (CI-2) from the database.
6. Now cover image-1 (CI-1) will act as stego image for cover image-2 (CI-2) providing three level of security.
7. Obtained image from step 6 is the final cover image to transmit.
8. Receiving of CI-2 at the receiver end.
9. Apply the reverse LSB on CI-2 to obtain CI-1.
10. Apply the digital signature on CI-1 to obtain cover image with stego image.
11. Again apply reverse LSB on CI-1 to obtain the stego image.

Now we will compare the proposed work with the work in [6] on the basis of PSNR.

2.1 Simulation Tool

MATLAB R2011a was used for simulation work and computations were done on computer with specifications as shown in Table 1.

TABLE 1
SPECIFICATIONS OF TOOL USED

Computer	Core 2 Duo or higher
RAM	3 MB
Platform	Windows 7
Other hardware	Keyboard, Mouse
Software	MATLAB 2011a

III. RESULTS AND DISCUSSION

Experimental investigation was conducted by creating different scenarios by using various set of images. The input to the MATLAB scheme was provided with three images for providing security with the help of stegnography. On running the developed scheme a window will be open from which we select the host image 1 from the data base and then a new window will open by which we select the host image 2 that will act as stego image and will hide in host image 1. Finally the last image as message image is selected that is to be encrypted, this image will hide in the host image 2 and to retrieve the message at the receiver end we apply a digital signature for decryption process to start and thus receiving the message image at the receiver end. The image quality was measured by using peak signal-to-noise ratio (PSNR). As images of different schemes are compared in terms of the PSNR which is estimated in decibel (dB) and higher PSNR value indicate a better image quality and is defined as:

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \tag{1}$$

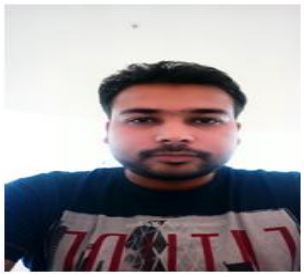
Where MSE (Mean Square Error) is defined as

$$MSE = \frac{1}{wh} \sum_{i=1}^{w} \sum_{j=1}^{h} (h_{ij} - s_{ij})^2 \tag{2}$$

where w and h are the width and height of the image respectively and h_{ij} and s_{ij} are the pixel values of host and stego image at $[i, j]$ respectively..

Images used in the present work for different scenario is shown in Table 2, where the first column represents images as Host 1, second column represents the images as Host 2 and third column represents the message images taken for four different scenarios and comparative analysis of present work and reference work [6] is shown in Table 3.

TABLE 2
IMAGES USED FOR DIFFERENT SCENARIOS

Scenarios	Column 1(Host 1)	Column 2(Host 2)	Column 3(Message Image)
1			
2			
3			
4			

To compare the present results with the result of previous experimental studies the performance factor (PSNR) found in literature are summarized in Table 3. The literature review reveals that the analysis using three level securities with digital signature framework employed in the analysis has not been performed previously. So it is difficult to make direct comparison of the present study with the result obtain in previous study. However commonly used parameter for measuring image quality is peak signal to noise ratio (PSNR) is used in the present work.

TABLE 3
COMPARATIVE ANALYSIS FOR PSNR VALUES

Scenario	Host-1	Host-2	Message Image	Proposed Work	Reference Work [6]	Percentage Enhancement in PSNR Values
1	Rahul1	Bird	Objects	44.0736	38.04	15.86
2	Rahul2	Rahul1	Cameraman	44.7862	38.67	15.81
3	Rahul2	Rahul3	Rahul4	44.7875	38.57	16.12
4	Butterfly	Pepper	Rahul2	44.7858	38.79	15.45

IV. CONCLUSION

A scheme has been developed for secure transmission of high quality data with minimum distortion in the image. The developed scheme saves the computational time and reduces the complexity of the problem as compared to other techniques like DCT (Discrete cosine transform), DWT. The enhancement in the PSNR values for different scenarios from highest to lowest are: Scenario 3 (16.21%), Scenario 1 (15.86%), Scenario 2 (15.81%) and Scenario 4 (15.45%). Thus the result shows that the developed algorithm ensures higher quality of data and high encryption level.

ACKNOWLEDGEMENTS

I am greatly thankful to principal and the management of Punjab College of Engineering & Technology, Lalru, PUNJAB for motivation, encouragement and providing facility to carry out this research work.

REFERENCES

[1] Ms.G.S.Sravanthi, Mrs.B.Sunitha Devi, S.M.Riyazoddin & M.Janga Reddy "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method." Intertional Journal of Computer Application volume 5-No.7 October 2009.

[2] Vijay Kumar Sharma, Vishal Shrivastava, "A Steganography algorithm for hiding image in image by improved LSB substitution by minimizes detection". Journal of Theoretical and Applied Information Technology (JATIT), Vol. 36 No.1.

[3] Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques. International Journal of Advanced Science and Technology" Vol. 54, May, 2013.

[4] Shashikala Channalli, Ajay Jadhav, "Steganography An Art of Hiding Data. International Journal on Computer Science and Engineering" Vol.1 (3), 2009, 137-141.

[5] Babloo Saha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images". Defense Science Journal, Vol. 62, No. 1, January 2012, pp. 11-18.

[6] Fahim Irfan Alam, Md. Mohaiminul Islam, "An Investigation into Image Hiding Steganography with Digital Signature Framework". IEEE, Vol. 6, No. 13, pp. 978-1-4799- 400, 2013.

[7] S.Arunkumar, Ravi Tej Akula, Rishabh Gupta & M.R.Vimala Devi, "Fuzzy Filters to the Reduction of Impulse and Gaussian Noise in Gray and Color Images". International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[8] Hsien-Wei Yang, "Interleaving Max-Min Difference Histogram Shifting Data Hiding Method". Journal of software, VOL. 5, NO. 6, JUNE 2010.