iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** V **Month of publication:** May 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Secure Image and Text Steganography Technique

Amitoz Singh Rathore[1], Sur Singh Rawat[2]
[1,2] *Department Of CSE, JSSATE*
Noida, U.P.,India

Abstract - Steganography is the art or practice of hiding image data or file within another image data or file. The aim of steganography is to insert secret data inside a piece of impressionable information. The outcome of steganography is dependent on the secrecy efficiency of the cover signal. After the steganographic carrier is known, the security is dependent on the robustness of the algorithm and the cryptographic techniques used. In order, to gain secrecy, either the carrier must be made more robust against steganalysis or new and better carriers must be discovered. The method presented in this paper aims to secure the data.
Keywords- Steganography, Hidden, Secure, Key, Image.

I. INTRODUCTION

In today's world of leading technology security is very important. With the increase in cyber crimes and hacking providing only network security is not sufficient to transfer information. To secure important images like blue print of company projects , secret images of concern to the army or of company's interest, using image steganography to secure data is beneficial. The message should be encrypted and embedded in the part of image so that it is difficult to detect. More over the secret message should be broken down into parts and then it should be sent so it becomes difficult for the attackers to get access to all the parts of the message at once. The data should not be sequentially embedded but randomly inserted to get the security of a much needed higher level. This makes it highly difficult for the intruder to detect the embedded data and decode it.

II. LITERATURE SURVEY

Current state of the world says that everything that can be thought off can be done with the help of the internet. Right from shopping for clothes to buying a house. The transactions are all done using personal information, credit card numbers etc. With the amount of internet users increasing every day, everything that is transferred over the internet is under threat by some malicious attack of another person. In order to provide security and integrity to the data that is being send across the system network security is not enough. With the increasing technology the attackers have also kept themselves updated with technology and ways to attack. In order to have security the only idea would be not letting the attackers know about the existence of important information in your transaction. Many methods have been developed to do so like digital watermarking and visual cryptography were used before image steganography. Researchers have also developed methods to embed data or another image within the image. There are various techniques for data hiding like the spatial domain, frequency domain, and compressed data domain. In spatial domain the image pixels are kept in order to incorporate the data to be embedded. This technique is simple to implement. It gives a high hiding capacity. The quality of the image in which the data insertion is done can be easily controlled. In frequency domain data embedding the images are first converted into frequency domain, and then data is inserted by manipulating the changed coefficients of the frequency domain. In compressed domain data hiding technique since the data is transmitted over the network is always in the compressed form so this information is used for inserting the data in compressed domain where the compressed data coefficients are manipulated to insert data. The Visual cryptography is the technique in which encryption could be done with a mechanical operation without the use of any computer. Cryptography secures the contents of the message whereas steganography protects both messages and the communicating parties. This is a visual secret sharing scheme and recovering scheme, where an image was broken up into n parts a person with access to all n shares could decrypt the image, while any n-1 shares revealed no information about the original image.

©IJRASET 2015: All Rights are Reserved

III. PROPOSED METHOD

In order to hide data we will apply a randomized approach as in earlier approaches data has been sequentially embedded so it was easy for the attackers to access the embedded data. But we will follow a pseudo random approach to insert and extract data. Also we will select certain essential area on the image in which insertion is done so that it cannot be easily manipulated. The data will be encrypted and inserted into the cover image at the sender end and at the receiver end data will be extracted and decoded.

A. The Proposed Encoding Algorithm

Inputs: Cover Image, Image file or Text file, Key
Output: Cover Image with Embedded data.
Begin
Check the type of the message.
If message is in text form convert from ASCII to integer values
If message is in image form convert the message to integer value representation.
Check that enough space is in the cover image.
Input for the key value to be used for embedding data.
Input the seed for randomization.
Check the size of the cover image and the size of the data to be embedded.
If the size of cover image is smaller
Return
Else
Start sub-iteration 1
Convert the set of bits of the message to be embedded in the encrypted form by
performing the xor operation between the message bits and the key that is provided.
Select Area on the image and arrange the pixels of that area randomly
Insert the data in the randomly arranged pixel
End sub-iteration 1.
End

B. The Proposed Decoding Algorithm

This algorithm "reveals" hidden messages by reversing the processing steps completed by the Encoding algorithm.
The embedded data is extracted and then decoding of the extracted data is done get the message. As data is inserted randomly so the same sequence of pixels that was used for embedding should be generated to extract the data.
Inputs: Image that has embedded or hidden data or message that is to be extracted, key.
Output: This output file will either be an image or a hidden text file that was embedded into the image at the sender end.
Begin:
Input the cover file that has embedded data and convert to get the pixel values.
Input from user about the type of data embedded text or image.
Depending upon the input from the user we can assess the kind of embedded
data and kind of bits to be extracted.
Select the area on the image at which insertion was done
Input the key used for encoding data.
Input seed used for initialization of randomization.
Extract the embedded bits.
Now execute the XOR operation on the bits extracted using the key.
Thus the extracted data is used to get the data which is hidden or embedded data.
End

IV. ANALYSIS

The algorithm is tested using PSNR (Peak Signal to Noise Ratio). PSNR is used to test the quality of the stego images. The higher

©IJRASET 2015: All Rights are Reserved

Volume 3 Issue V, May 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

the value of PSNR the better is the Stego image quality .
Calculate the MSE(mean square error) between the Cover image and Stego Image.

$$MSE = 1/MN \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} (C(p.q) - S(p,q))^2$$

$PSNR=10\log_{10}MAX^2/MSE$
MAX is the maximum pixel value of images.
The figures represent the cover image fig 1 image to be hidden fig 2 and the stego images with the hidden data fig 3



Fig.1 Cover Image



Fig.2 Image to be hidden



Fig 3 Stego Image

The figures represent the cover image fig 4 document to be hidden fig 5 and the stego image with the hidden data fig 7



Image



Text document



Stego Image

TABLE 1

Comparison of Psnr values of different values of cover images and Data shown in table1

Cover data	**Size of cover**	**Message Hidden**	**Size of message Hidden**	**PSNR**
Animal.jpg	800Kb	Text	8kb	82.14
		Image	100kb	62.15
Lenna.jpg	500Kb	Text	10kb	80.02
		Image	50kb	61.83
Sweet.jpg	410kb	Text	15kb	81.14
		Image	40kb	60.51

©IJRASET 2015: All Rights are Reserved

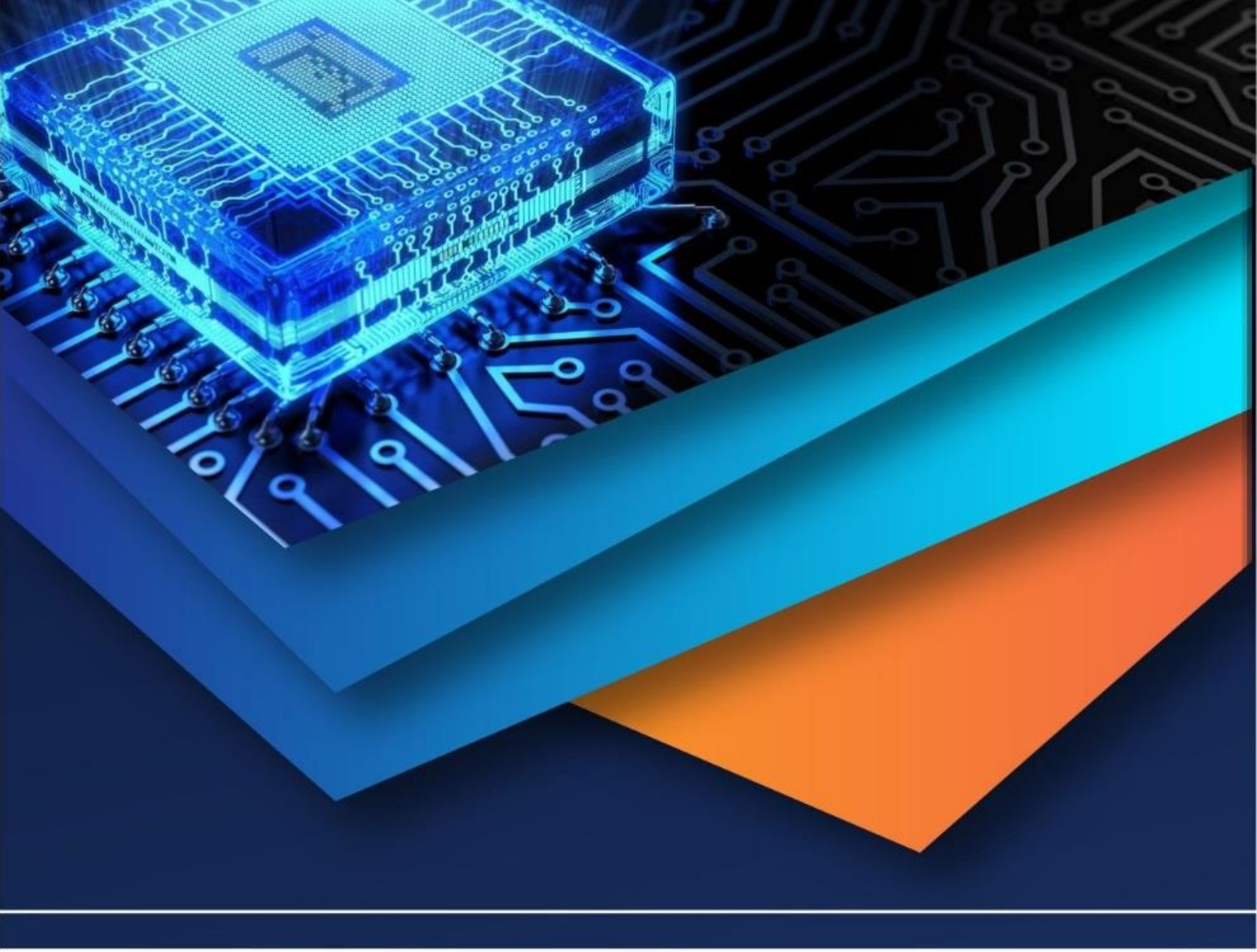
V. CONCLUSION

This paper has presented a novel system for data encryption and hiding into image. The data is hidden in a randomized way in the selected area of the image. The method has put forth a new system which combines cryptography and image steganography which could be proven a highly secured method for data transactions in the near future. The procedure is compatible with pay load capacity of cover image. Any type of data, text or image can be easily embedded into suitable cover image at sender end and extracted at receiver end.

REFERENCES

[1]Acharya, U.D., Hemalatha, S., Priya Kamath, R. and Renuka A., 2013.A secure and high capacity image steganography technique. Signal & Image Processing: An International Journal (SIPIJ), Vol.4, No.1, pp. 83-89.
[2]Ge Huayong A.B., Huang M. and Wang Q., 2011.Steganography and steganalysis based on Digital Image.4th International Congress on Image and Signal Processing. Vol.1, pp. 252-255.
[3]Tsung-Yuan Liu,2010 Student Member, IEEE, and Wen-Hsiang Tsai, Senior Member, IEEE.Generic lossless visible watermarking a new approach. IEEE transactions on image processing, Vol. 19, No. 5, pp. 1224-1235.
[4]Weiqi Luo, Member, IEEE, Fangjun Huang, Member, IEEE, and Jiwu Huang, Senior Member,IEEE,2010.Edge Adaptive Image Steganography Based on LSB Matching Revisited., IEEE Transactions on Information Forensics and Security,Vol.5.,No.2, pp.201-214.
[5]] Batra, S. Sharma, H.R. and Singh, P., 2007. Steganographic methods based on digital logic. Proceedings of the 6th WSEAS International Conference on SIGNAL PROCESSING, Dallas, Texas, USA, March 22-24, pp. 157- 162.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)