Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 04, April-2020

Hiding Compressed and Encrypted Data by using a Technique of Steganography

Amrita Bhatnagar
Dept of computer science & Eng.
IPEC Ghaziabad,India

Shweta Chaku
Dept of computer science & Eng.
IPEC Ghaziabad,India

Monica Sainger
Dept of computer science & Eng.
IPEC Ghaziabad,India

Abstract:- The steganography is a technique which hide the text data in the color and gray images .We can use different type of steganography techniques. Some Techniques are used in spatial Domain Technique. Some techniques are used in frequency Domain. Some steganography techniques are very popular like LSB, MSB and 7 bits in hiding the invisible information in various file formats images. In this paper, Steganography and Cryptography is combined for hiding and unhiding a text file into an image file. Data Compression is also used in this technique. LSB insertion technique is used for Steganography and LZ algorithm is used for Data Compression. Cryptography is done with RSA algorithm

Keywords: LSB insertion technique, RSA Algorithm, LZ Algorithm, compression ,encryption

I. INTRODUCTION

In current scenario secret messages can be send by hiding in a image or a text so nobody other than sender and receiver can read or see the message.With the help of Steganography Confidential data can be send over the computer networks safely. So hiding and unhiding of data is known as steganography. In steganography the Image which hide the data is known as Cover Image because it covers the secret message and after hiding the data image is known as stego image.In Steganography LSB insertion is a very popular and commonly applied technique for embedding data in a cover file. The LSB embedding technique suggests that data can be hidden in such a way that even the naked eye is unable to identify the hidden information in the LSBs of the cover file. It is a spatial domain technique.

Cryptography is method which convert the text in codes so that intruder is successful in finding the secret message it can not be readable by intruder.So if we apply steganography and crptography then it will provide double layer of security.Image compression is used to reduce the size of messge so that message easily hide.In this paper we are lossless compression technique named LZ algorithm.

II. PROPOSED TECHNIQUE

In the proposed method, Steganography and cryptography is used to send the compressed secret message at the side of sender and at receiver side message is decrypted ,decompressed and extracted from the stego image.

LSB Encoding Algorithm

LSB Encoding algorithm works in binary data so firstly we have to convert our image in binary format and then embedded the message bits with cover image pixel. Each pixels least significant bit will be replaced by message bit . In this way data will be hide in cover image.

.Hiding Data

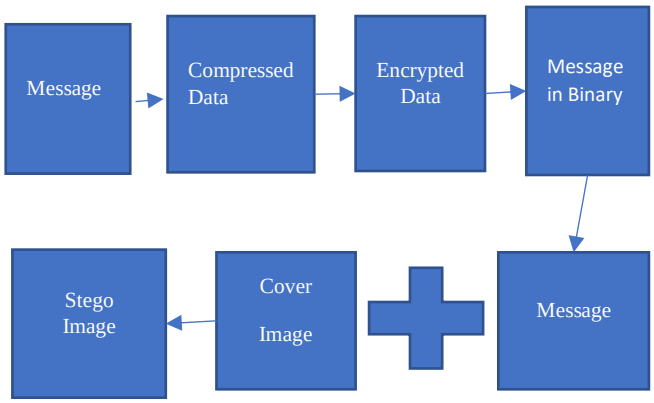

Fig-1 Hiding the secret Data

LSB Decoding Algorithm

LSB Decoding technique is used for extract the secret message form cover image .After extraction of message ,this message is decompressed and decrypted by secret key and original message is find out.

Unhiding Data

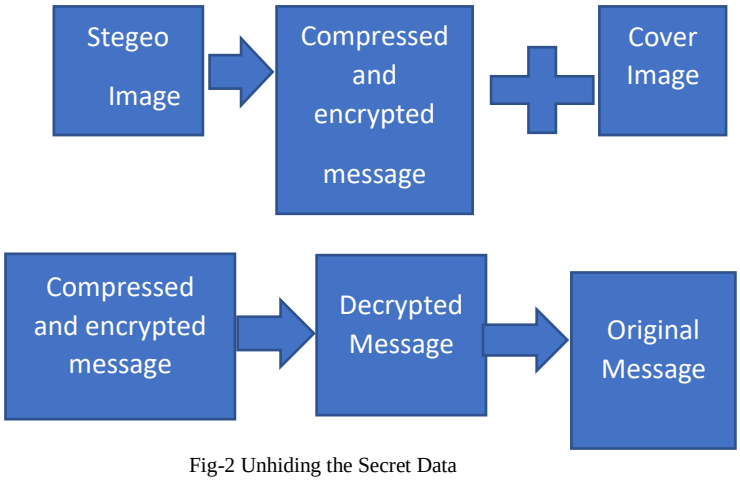

Fig-2 Unhiding the Secret Data

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 04, April-2020

III Experimental Work And Results

Now we will compare both images cover and stego by using MSE,PSNR and Corelation. We will use three Image formats bmp ,gif, png.

MSE

In statistics, MSE is known as mean square error. It should be less for cover image and stegeo image

The MSE between cover file and stego file is calculated as per

$MSE=\sum_{M,N}(I_1(m,n)-I_2(m,n)]^2/M*N$

M and N are the number of rows and columns in the input images

PSNR

PSNR between cover image and stego image is calculated by given equation . A higher PSNR indicates that the quality of the stego image is similar to the cover image.

$PSNR=\log10(R^2/MSE)$

In the previous equation, R is the maximum fluctuation in the input image data type.

Correlation

Correlation, a best known method, not only evaluates the degree of closeness between two functions but also determines the extent to which the cover image and the stego image are close to each other even after embedding data.

The MSE, PSNR and Correlation values for various image file formats are shown in the Table

Table : Quality Metrics for various Image File Formats

Cover Image	Stego Image	MSE	PSNR	Correlation
Cover_abc.bmp	Stego_abc.bmp	3.67	46.1	0.998
Cover_Barbara.bmp	Stego_Barbara.bmp	4.01	49.4	0.998
Cover_Baboo.gif	Stego_Baboo.gif	2.18	44.7	0.999
Cover_Home.gif	Stego_Home.gif	3.84	47.4	0.998
Cover_Peper.png	Stego_Pepers.png	3.04	44.3	0.997
Cover_Aeroflight.png	Stego_Aerolflight.png	2.65	42.15	0.9981

The results show that MSE, PSNR and correlation are in comparison with already existing results. The MSE obtained for different file formats varies from 2.6 to 4.0 and PSNR varies from 42.15 to 49.42 dB and 99.98% of correlation is obtained with the proposed technique.

IV. CONCLUSIONS

When we send a secret message on internet it is very risky .But this technique is very useful to send the data safely. In proposed method only sender know how the hide data and only receiver know how unhide the data. Besides these two person nobody knows about the secret message so data is send safely. With images.Cover image and stegeo image are simllar in quality .Nobody can see the message with naked eye.

REFERENCES

[1] Sultana, S., Khanam, A., Islam, M.R., Nitu, A.M., Uddin,M.P., Afjal, M.I., Rabbi, M.F.: A Modified Filtering Approach of LSB Image Steganography Using Stream Builder along with AES Encryption, HBRP Recent Trends in Information Technology and its Applications, Volume 1 Issue 2, pp. 1-10 (2018).

[2] G. Swain and S. K. Lenka, "A novel steganography technique by mapping words with LSB array," International Journal of Signal and Imaging Systems Engineering, vol. 8, pp. 115-122, 2015.

[3] A. Sharif, M. Mollaeefar, and M. Nazari, "A novel method for digital image steganography based on a new threedimensional chaotic map," Multimedia Tools and Applications, vol. 76, pp. 7849-7867, 2017.

[4] S. Mishra, P. Pandey, "A Review on Steganography Techniques Using Cryptography", International Journal of Advance Research In Science And Engineering, Volume 4, Special Issue (01), 2015.

[5] N. Singh, "Survey Paper on Steganography", International Refereed Journal of Engineering and Science (IRJES), Volume 6, Issue 1, 2017.

[6] A. Rashid and M. Rahim, "Critical Analysis of Steganography "An Art of Hidden Writing"", International Journal of Security and Its Applications, Volume 10, No. 3, 2016. [

[7] S. Swathi, P. Lahari and B. Thomas," Encryption Algorithms: A Survey", International Journal of Advanced Research in Computer Science & Technology (IJARCST), Volume 4, Issue 2, 2016.

[8] S. Asbeh, H. Al-Sewadi, S. Hammoudeh and A. Hammoudeh, "Hex Symbols Algorithm for AntiForensic Artifacts on Android Devices", International Journal of Advanced Computer Science and Applications (IJACSA), Volume 7, No. 4, 2016.

[9] K. Rahmani, K. Arora and N. Pal, "A CryptoSteganography: A Survey", International Journal of Advanced Computer Science and Applications (IJACSA), Volume 5, No. 7, 2014.

[10] P. Joseph and S. Vishnukumar, "A Study on Steganographic Techniques", Proceedings of Global Conference on Communication Technologies (GCCT), IEEE, 2015.