International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

A Framework for Data Security using Cryptography and Image Steganography

Balajee Maram, Guru Kesava Dasu Gopisetty, P Srinivasa Rao

ABSTRACT ***Cryptography and steganography are the two research areas which are popular for data confidentiality, data hiding respectively. Steganography hides the data in various multimedia cover files like image, audio and video. This paper handles images for steganography, which have high redundant pixels. In this paper, Lease Significant Bit (LSB) method hides the secret message bits in least significant bits of each pixel. The performance metrics MSE and PSNR are used to check the strength of the proposed algorithm. The proposed algorithm also checks payload capacity, image quality and security of the confidential data by applying cryptography and steganography algorithm and various parameters.***

Keywords: Pixel, MSE, PSNR, LSB, distortion

I. INTRODUCTION

Audio, video and images are mainly used for data hiding and is call steganography. Digital images are more preferable media for hiding the information, because it is able to hide more data. Till now, various researchers are being worked on steganography algorithms using different image formats for hiding more data. The strength of any steganography algorithm can be measured by hiding capacity, distortion and security. The hiding capacity is nothing but maximum number of bits per pixel hiding in image/audio/video. Measuring the distortion is used to check the performance of steganography algorithm. The distortion of image can be calculated by PSNR, Mean square error (MSE), Root mean square error (RMSE) etc.

II. LITERATURE SURVEY

In digital era, the data can be transferred in different ways between sender and receiver through internet. But more threats are existing for confidential data like medical diagnostics, financial, credentials and military data. In order to provide the data security, cryptography is one technique which scrambles the content. Similarly steganography is also provides the data security through data hiding. Steganography uses a cover medium to hide the secret information [2]. For enhancing the data security, there is a need to combine steganography and cryptography. Image steganography can be hiding the unnatural secret message within a carrier image, so the carrier image quality will have a small change, thus no one cannot recognize it [1]. In steganography, vulnerability is more when least significant bit substitution methods are used for data hiding [3].

Manuscript published on 30 September 2019.
***Correspondence Author(s)**
Dr. Balajee Maram, Asso. Prof., Dept. of CSE, GMR Institute of Technology, Rajam balajee.m@gmrit.edu.in
Dr. Guru Kesava Dasu Gopisetty, Professor & HOD, Dept. of CSE, Eluru College of Engineering & Technology, Eluru
Dr P Srinivasa Rao, Associate Professor, Dept. of CSE, MVGR College of Engineering, Vizianagaram

The LSB bits of all the pixels can be formed as LSB array and can be used to hide the secret binary words which enhances the security [4]. Similarly, the bits from four LSB planes can form four LSB arrays that are used to store four parts of the binary message at minimum distortion locations [5]. The three LSB planes can be investigated for increasing the hiding capacity. But it able to hide two bits only from the secret message [6,7].

LSB Steganography method replaces the least significant bits with secret message bits [8]. After insertion of the secret message bits, the values of pixels can be changed up to +1/-1[9]. In LSB methods, the message was present at LSB, and by only picking LSBs, the intruder can access the data.

In image steganographic techniques evaluation, the following parameters plays a vital role that are shown in Fig-1. Those are (i) hiding capacity, (ii) distortion measure and (iii) security check.

Hiding Capacity: The hiding capacity can be measured by the following two parameters:

- Maximum hiding capacity, is the total bits can be hidden in cover image
- Bit-rate, is the capacity of each pixel can hide how many number bits

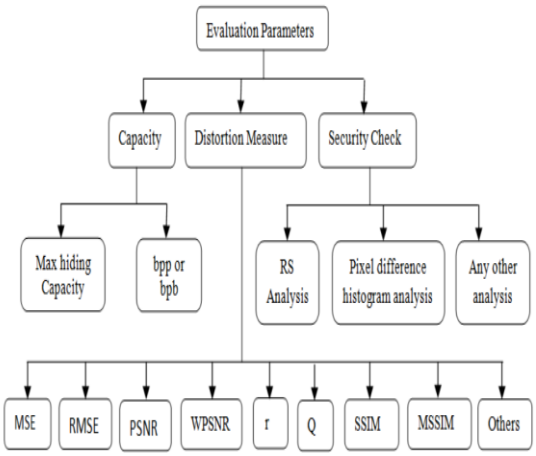


Fig 1: Evaluation parameters for Image

Distortion Measurement: The distortion should not be noticed by the public. The distortion can be measured by various parameters. Peak signal-to-noise Ratio (PSNR), Root Mean Square Error (RMSE), Mean Square Error (MSE) are the parameters play an important role in assessing the performance of the steganography algorithms.

The mean-squared error (MSE) The MSE between the original image (I1 (m,n)) and the stegoimage (I2(m,n)).

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (p_{ij} - q_{ij})^2$$

Here the image contains M number of rows and N number of columns. The p and q are the carrier image pixel and the stego-image pixel value at row and column respectively. The MSE value of any algorithm indicates that when both the carrier and the distorted-image are equal then MSE is 0.
Peak signal-to-noise Ratio (PSNR)
The following formula is for calculating PSNR value for the given image:

$$PSNR = 10 \times \log_{10} \frac{255 \times 255}{MSE}$$

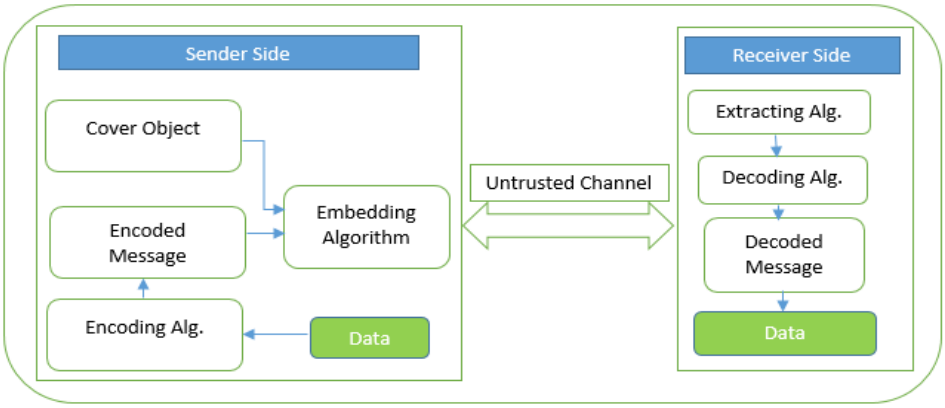
It is a good indicator for comparing the restoration results of the same image but meaningless across images. According to different studies, PSNR is ranked as follows: up to 40 dB = very good; 30 to 40 dB = acceptable; < 30 dB = not acceptable.

III. PROPOSED SYSTEM

Least Significant bit substitution (LSB) method
The LSB substitution technique stores the secret message bits in the least significant bits of the cover file. The cover file could be audio, video or image file.
Least significant bit (LSB) in PNG

As we know, the Graphics Interchange Format (GIF) has only eight (8) bits depth, so, the information hiding capacity is lower compared to BMP. The hiding of information using LSB has the same result in both GIF and BMP. The LSB approach is considered as most effective for embedding a reasonable capacity of information. In the GIF image, the colors used are stored in a palette because it is an indexed image. The use of a GIF image as a carrier for steganography requires some levels of carefulness because of the issue with the palette scheme. The use of a GIF image with an altered LSB as a palette scheme may give different colors due to the change in the color palette index. Whenever there are different neighboring palette entries, there is a remarkable image change, but when there is a similar neighboring palette entry, the change is not remarkable [11]. Generality, applications that deploy LSB approaches on GIF image are characterized with low security due to the possibility of detecting even an average change in the image. Such issues can be solved thus:

- The palette must be isolated if there is a reduced difference between sequential colors.
- An 8-bit grayscale GIF image comprising of 256 gray shades must be used; else, there will be a gradual alteration of the colors.



At the sender-end

Step 1: Apply DRDP method for shuffling the data
Step 2: Convert all pixels in the original image row by row into binary form and put it in image array
Step 3: Length of the message is stored in first pixel
Step 4: Take two characters (16-bits)/UTF-16 UNICODE character and convert it into binary form
Step 5: The step-5 16-bit binary data is stored in next 3 pixels in the following:

- 3-bits in LSB of red component of 1st pixel
- 2-bits in LSB of green component of 1st pixel
- 3-bits in LSB of red component of 2nd pixel
- 2-bits in LSB of green component of 2nd pixel
- 3-bits in LSB of red component of 3rd pixel
- 2-bits in LSB of green component of 3rd pixel
- 1-bit in LSB of blue component of 3rd pixel

Step 6: Repeat Step 4, Step 5 for next pixels till all the bits of secret message are embedded in the image.

Step 7: Set the image with the new values and save it.
Step 8: End

At the receiver-end

Step 1: Convert all pixels in the original image row by row into binary form and put it in image array
Step 2: Length can be extracted from first pixel
Step 3: Next three pixel gives the 2-character (16-bits)/UTF-16 UNICODE character data in the following:

- 3-bits in LSB of red component of 1st pixel
- 2-bits in LSB of green component of 1st pixel
- 3-bits in LSB of red component of 2nd pixel
- 2-bits in LSB of green component of 2nd pixel
- 3-bits in LSB of red component of 3rd pixel
- 2-bits in LSB of green component of 3rd pixel
- 1-bit in LSB of blue component of 3rd pixel

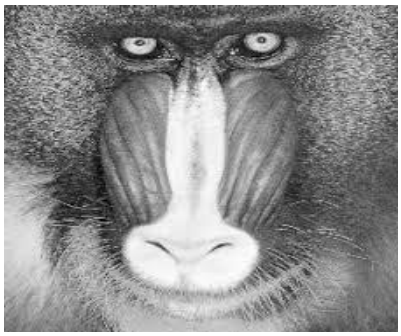
Step 4: Repeat Step-3 for next pixels in the stego-image
Step 5: Decode all the extracted bits using DRDP method to get the plain message.
Step 6: End
Using encoding algorithm, the stego-image can be prepared which hides the given message, transfer the stego-image to the destination. In destination end, the hidden message can be extracted and decoded using DRDP method. Then the original message can be shown to the user.

Retrieval Number: J11480881019/19©BEIESP
DOI: 10.35940/ijitee.J1148.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

IV. RESULTS AND DISCUSSION

The performance of the proposed system can be measured with two parameters PSNR and MSE. The proposed algorithm has been applied on the following 256X256 pixel grayscale images for 2KB, 4KB, 6KB, 8KB, 10KB and 12KB data.



The proposed algorithm hides 2KB data using above grayscale images and the results are shown in Table-1.

Table 1: The results of the proposed method using (256∗256) image for 2KB data

Image name	PSNR	MSE
Lena.png	52.02567405554823	0.40786172839506174
Lady.png	52.10998923428396	0.40001975308641974
Baboon.png	52.01873862476182	0.4085135802469136
Mother_baby.png	52.04316683245441	0.4062222222222222
Photographer.png	52.08070772173965	0.40272592592592593
Mountains.png	52.352312640282996	0.3783111111111111

The proposed algorithm hides 4KB data using above grayscale images and the results are shown in Table-2.

Table 2: The results of the proposed method using (256∗256) image for 4KB data

Image name	PSNR	MSE
Lena.png	50.4794738257217	0.5822814814814815
Lady.png	50.55272092383845	0.5725432098765432
Baboon.png	50.59896536679627	0.566479012345679
Mother_baby.png	50.64984257765515	0.5598814814814815
Photographer.png	50.44089830107775	0.5874765432098765
Mountains.png	50.90267753089074	0.5282172839506173

The proposed algorithm hides 6KB data using above grayscale images and the results are shown in Table-3.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table 3: Performance analysis of the proposed method using (256∗256) image for 6KB data

Image name	PSNR	MSE
Lena.png	49.373761743656	0.7511111111111111
Lady.png	49.45317609213536	0.7375012345679013
Baboon.png	49.476151912875395	0.7336098765432099
Mother_baby.png	49.53075274575315	0.7244444444444444
Photographer.png	49.127118833681834	0.7950024691358024
Mountains.png	49.78105789120015	0.6838716049382716

The proposed algorithm hides 8KB data using above grayscale images and the results are shown in Table-4.

Table 4: The results of the proposed method using (256∗256) image for 8KB data

Image name	PSNR	MSE
Lena.png	48.56807556629448	0.9042172839506173
Lady.png	48.5726318997976	0.9032691358024691
Baboon.png	48.56940400318278	0.9039407407407407
Mother_baby.png	48.65421580192646	0.8864592592592593
Photographer.png	48.01843125808709	1.0262123456790124
Mountains.png	48.80416223818523	0.8563753086419753

The proposed algorithm hides 10KB data using above grayscale images and the results are shown in Table-5.

Table 5: The results of the proposed method using (256∗256) image for 10KB data

Image name	PSNR	MSE
Lena.png	47.90099372469009	1.0543407407407408
Lady.png	47.84569355727929	1.0678518518518518
Baboon.png	47.83133723209605	1.0713876543209877
Mother_baby.png	47.94178589803764	1.044483950617284
Photographer.png	47.187395189755854	1.2426271604938273
Mountains.png	48.03879258055392	1.0214123456790123

The proposed algorithm hides 12KB data using above grayscale images and the results are shown in Table-6.

Table 6: The results of the proposed method using (256∗256) image for 12KB data

Image name	PSNR	MSE
Lena.png	47.310063251040766	1.2080197530864198
Lady.png	47.19229954563354	1.2412246913580247
Baboon.png	47.24822612347714	1.225343209876543
Mother_baby.png	47.297795137340174	1.211437037037037
Photographer.png	46.5193871665294	1.4492444444444443
Mountains.png	47.39308623431002	1.1851456790123456

The proposed method has been applied on the above grayscale images for 8KB data and the results are compared with existing technologies like Classic LSB method, SSC method, PIR, FMM and CST methods. The comparative results are shown in Table-7.

Table 7: The performance comparison of proposed and existing methods through PSNR[12] by hiding 8KB of data in images of resolution (256∗256)

Image Name	Classic LSB method	SCC method	PIT	FMM	CST	Proposed Method
Lena.png	42.51	42.60	42.30	43.57	55.92	48.57
Baboon.png	54.73	47.97	46.89	44.55	48.95	48.57
House.png	52.04	52.89	51.07	67.55	51.17	48.57
Couple.png	48.40	47.91	46.58	46.25	55.91	48.65
Tree.png	56.27	49.76	48.60	46.12	38.54	48.37
Moon.png	56.02	47.26	46.39	45.82	47.49	48.90

The results of the parameters PSNR and MSE of the proposed system are shown in Table-7. These values are compared with existing methods. The Table-7 shows the comparison of PSNR value of the proposed system and the existing algorithms [13]. The proposed method tries to overcome the drawbacks of all these methods.

V. CONCLUSION

In cryptography and steganography, various algorithms have been designed by many researchers in the world. Many algorithms are able to handle ASCII data only and steganography algorithms are based on LSB technique using images. Very few algorithms are using DRDP method for shuffling the data with simple mathematical operations. When we observe the performance analysis, the Encryption-Time and Decryption-Time are same. The encoded data can be hidden in to the cover file using LSB steganography technique. In the proposed system, the original image and stego-image are looking similar and distortion is also very less. It is proved by two parameters like MSE and PSNR. These values are better than the existing methods.

REFERENCES

1. Moerland, T., “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science, Silman, J., “Steganography and Steganalysis: An Overview”, SANS Institute, 2001 Jamil, T., “Steganography: The art of hiding information is plain sight”, IEEE Potentials, 18:01, 1999
2. 2.Ron Crandall, Some Notes on Steganography, Posted on Steganography Mailing List, 1998.
3. J Fridrich, M Goljian, R Du, “Detecting LSB steganography in color and gray-scale images”. Magazine of IEEE Multimedia Special Issue on Security, Vol.8, No.4, pp.22-28, 2001
4. G. Swain, S.K. Lenka, “A novel steganography technique A novel steganography technique by mapping words with LSB array”, International Journal of Signal and imaging Systems Engineering, vol.8, no.1, pp.115-122, 2015.
5. G. Swain, S. K. Lenka, “LSB array based image steganography technique by exploring the four least significant bits”, Global Trends in Information Systems and Software Applications, Communications in Computer and Information Science, vol.270, pp.479-488, 2012.
6. G. Swain, S. K. Lenka, “A technique for secret communication using a new block cipher with dynamic steganography”, International Journal of Security and Its Applications, vol.6, no.2, pp.1-12, 2012.
7. G Swain, S K Lenka, “A robust image steganography technique using dynamic embedding with two least significant bits”, Advanced Materials Research, vols. 403-408, pp.835-841, 2012
8. N. F. Johnson and S. Jajodia, “Exploring steganography: seeing the unseen,” IEEE Computer, vol. 31, no. 2, pp. 26–34, 1998.

9. R. J. Anderson, "Stretching the limit of steganography in information hiding," Springer Lecture Notes in Computer Science, vol. 1174, pp. 39–48, 1996.
10. M. Khan, S. Muhammad, M. Irfan, R. Seungmin, and B. W. Sung, A Novel Magic LSB Substitution Method (M-LSBSM) Using Multilevel Encryption and Achromatic Component of an Image, Springer, Berlin, Germany, 2015.
11. Balajee M., Narasimham C., Ramesh Kumar Y. (2012) Data Security for Virtual Data Centers by Commutative Key. In: Proceedings of the International Conference on Information Systems Design and Intelligent Applications 2012 (INDIA 2012) held in Visakhapatnam, India, January 2012. Advances in Intelligent and Soft Computing, vol 132. Springer, Berlin, Heidelberg
12. Dr Balajee Maram, Dr J M Gnanasekar, Gunasekaran Manogaran, M. Balaanand "Intelligent Security Algorithm For Unicode Data Privacy And Security In IoT", Service Oriented Computing and Applications (SPRINGER), ISSN: 1863-2386 (Print) 1863-2394 (Online),
13. Balajee Maram, Gnanasekar JM (2015) Light weight cryptographic algorithm to improve avalanche effect for data security using prime numbers and bit level operations, International Journal of Applied Engineering Research (IJAER) 10(21):41977–41983. ISSN 0973-4562.