Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 7, Issue 06, June -2020

IMPROVED IMAGE STEGANOGRAPHY TECHNIQUE USING AES CRYPTOGRAPHY FOR DATA SECURITY

Shivani Sharma[1], Jasvinder Kaur[2]

[1]*Research Scholar, Dept. of Computer Science, PDM University, Haryana, India*
[2]*Assistant Professor, Dept. of Computer Science, PDM University, Haryana, India*

ABSTRACT: *Security has become one of the most challenging aspect in our society. Security is required in every part of the communication. For communication, the sender and receiver play an important role and transfer the data which is very easy to access, so in order to secure the data cryptography was developed.[1] Here the sender utilizes encryption algorithm for encoding the dataand recipient utilizes decoding algorithm for unscrambling the data. But as time goes it became very easy for intruders to access the dataas they can break the code and access the data. So, here we developeda new method that is combined approach of cryptography and steganography. Firstly, we used AES encryption algorithm to encode the data after that the secret-text is converted to cipher-text and lastly, the receiver uses the new algorithm to decode the data.[3] The contents obtained after doing so is secret and its existence is also hidden. This method is tested and it is observed that it prevents steganalysis too as well as parameters like PSNR and MSE are also tested which gave good results.*

KEYWORDS: *Image Steganography, Cryptography, AES, Information Security, PSNR, Stego-image, Secret key*

I. INTRODUCTION: Steganography is defined as the "hidden writing" that helps to hide the presence ofdata. By doing so, it becomequite difficult for intruders to Access the data as it is very difficult to find the difference between the images.[5]The sender is sending a message which is been embedded by a secret key and a stego-image is formed. This process is known as steganalysis, after this the image is further processed and the receiver will extract the image with use of the key. And so, the message will be successfully sent to the receiver.Steganography helps to hide the file in the various form such as image, audio, video, text. And the objective to do this is hiding the availability of data in the cover-picture that is unreadable by humans. Steganography comprise of basic three components which are carrier, message and key.[2] The carrier can be a picture, media player or a TCP/IP packet. And a key is utilized to encode or unscramble a message and the password can be anything, a pattern or a video.[4] The idea driving steganography is if a person wants to transfer a message to other party, the communication between them is constrained by a switch or server. We can watch that one party wants to transfer a message to recipient, so to do so it implants it into a cover picture and obtains a stego picture. In a standard definition, this strategy of typifying message isn't known and is kept as a mystery between the two. Be that as it may, it is seen that the algorithm being used isn't a mystery yet the key is mystery between the two, and it is also known asKerchoff's guideline. It is a technique to secure the touchy information.[6]
The function of combined layer of these two techniques are almost same but the method of achieving it is not same. The following figure shows us the generalized form of steganography, where we can see that we send the image or text by applying encryption algorithm and the receiver receives it using decryption algorithm.[9]

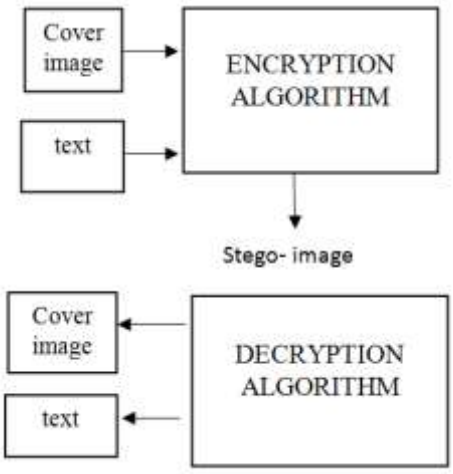

Fig1- Generalized Steganographic Technique

Now, we can define cryptography as the process in which it encrypts the actual message and coverts it into secret message. This message can be retrieved by receiver by using either private key or public key. Also, the message can be encapsulated by using a mathematical equation or algorithm and converts it into a non-readable form which can be any mystery information.[10]Cryptography helps to encapsulate the data in order to protect it from an attacker, whereas steganography helps to conceal the presence of that data from the attacker. So, combination of these two techniques gives superiorcommunication. The aim of this paper is to combine the technologies and have better experience. Some basic terms are as follows:

1) Load: data that requires to be concealed. [12]
2) Carrier file:medium in which the load has to be covered up.
3) Stego-Medium: place where the data has to be covered up.[7]
4) Redundant-bits: the data inside a record, which can be adjusted without harming the document.
5) Steganalysis: The way toward identifying the hidden data which is put away inside a document.[8]

Many new technologies have been developed in recent past to secure data and have a smooth communication system. Here we show the general cryptographic framework where the plain text is converted to cipher text with the assistance of encryption algorithm and again, the cipher text isconverted to plain text with the assistance of decryption algorithm.[11]
Further we will see the steganographic domains and its advantages as well as disadvantages.
This is the figure for cryptography:

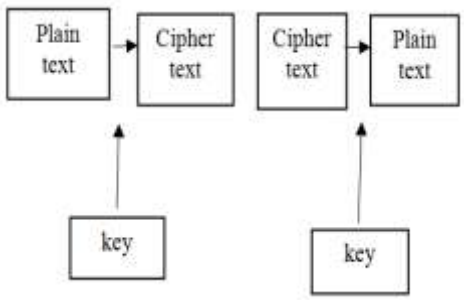

Fig 2: Generalized cryptographic technique

The steganographic technique is divided into two categories which are as follows:
1) Spatial domain- In this kind of domain the work is directly done on the pixels. It deals with the image plane itself. It includes least significant bit method, edge method, pixel value and pixel indicator method. The benefit of this technique is that high quality stego- image and high payload but it is also vulnerable to issues such as JPEG, noise attacks and geometric attacks such as rotation, cropping and resizing etc.[13]
2) Transform domain- In this kind of domain the work is done on space explicit qualities to insert information and to perform to the picture and change it to area like DCT and DWT. Here the information is installed on the changed picture rather than direct picture. The benefit of this technique is that information can be easily encapsulated where it is less exposed to cropping and processing.[17] And here the component of transformed image spread over the whole image so this helps us from any data attack. But it is a quite difficult way of hiding information.
In steganography, two groups work together. The first group makes steganographic algorithms whereas the second one develops counter attacks i.e. steganalysis.Steganalysis is the study of recognizing messages concealed utilizing steganography; this is undifferentiated from cryptanalysis applied to cryptography.[19]
So, now the paper contains part II which has the review and analysis briefly described that are about our proposed technique. Part III describes the presented technique which is followed by results and discussions in part IV. The conclusion and future scope arepresent in part V.

II. LITERATURE REVIEW: We have many algorithms present today for securing the data and sending it efficiently. But each of them has their own advantage anddisadvantage. Let's have a look on some of them:

P Kalamkar, M Gaikwad recommended that Colour Image Visual Cryptography for secret key assurance and it can't break this security with present innovation. This framework will be an aid for the Core Banking Application and the bank clients are feeling free from the secret phrase hacking issues.

N Wu, P Shang, J Fan, Z Yangunderstood the steganography to secure data dependent on the Markov model which has been frequently utilized in normal code handling. Due to some different ways, past related calculations were not completely used or disregardedsignificant ideas, change likelihood, in Markov chains.

Rashad Thabit presents two improved steganography techniques based on SLT and different embedding methods. The first proposed technique embeds secret text in a cover text whereas the second technique encodes binary data in a cover image.[20]

FarshadMiramirkhani, Omer Narmanlioglubuilt up a portable VLC channel dependent on non-successive beam following. For practical displaying, frequency reliance was expressly considered while various kinds of reflections were thought of.[15]

So, the methods discussed above have one or other drawback which we can easily fix by applying a two-layer protection on the data i.e. using both of the technologies together. Results of above method have low quality stego image and also easily detectable image. This present research work solves this problem and proposes a new scheme which gives good quality stego-image as well as increasing security of data while transmission.[14]

III. PROPOSED METHODOLOGY: The proposed work is divided into two steps, firstly data is encrypted and converted into cipher then secondly conceal the information using LSB technique given by the algorithm. The message is hidden into two layers such as first layer conceals it using cryptography and second conceals the message using the new algorithm. This new method is combined with existing technology to build up the security and have smooth communication. Firstly, we encode the data then the message is hidden using algorithm. Simply LSB was not efficient as it was easy to discover so we used combined layer of steganography and cryptography which automatically increased the security and efficiency of data.[20] Even after detecting the steganography attacker needs to decode the new algorithm which is quite difficult to access.

A. *PresentedArchitecture*: Here we show, thedesign of our algorithm.The encryption method which we used here to scramble the information isAES algorithm. The steps are as follows:

1) In this technique, we use bytes instead of bits. There are 128 bits of plain-text hinder as 16 bytes.

2) These bytes are masterminded in 4 lines and 4 segments to fill in as a grid.

3) The no. of rounds is changeable and relies upon the measurement of our key.

4) There are 10 rounds for 128-piece keys, 12 round for 192-piece keys and 14 round for 256 keys.

5) Most of them has distinctivekey that is assessed by unique AES key.

Now, we havediagram showing the functionality of this algorithm. There are two steps in this algo which are substitution and permutation. The 128-bit plaintext goes to pre- round transformation which goes on from1,2,…….N and gives us 128-bit ciphertext.

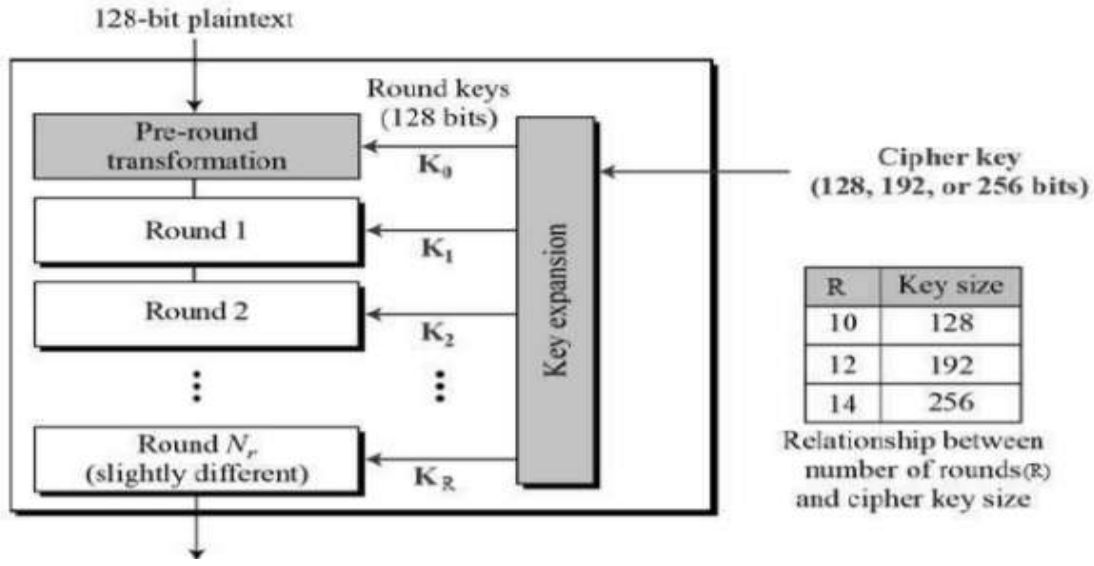

Fig 3: AES Algorithm

Now we begin with the embedding algorithm.

B. *Encryption module*: *Encoding image file to give output asa text.*
The algo is as follows:
Begin
1) Take input as any audio, video, image or text. Here we are taking an image.
2) Select the image where you want to insert another image. And run the program using AES algorithm.
3) Do the encryption process using AES which will create a ciphertext.
4) Now take the cover image and key and perform embedding using the algorithm.
5) Lastly, we obtain result as our stego-image.
Stop.

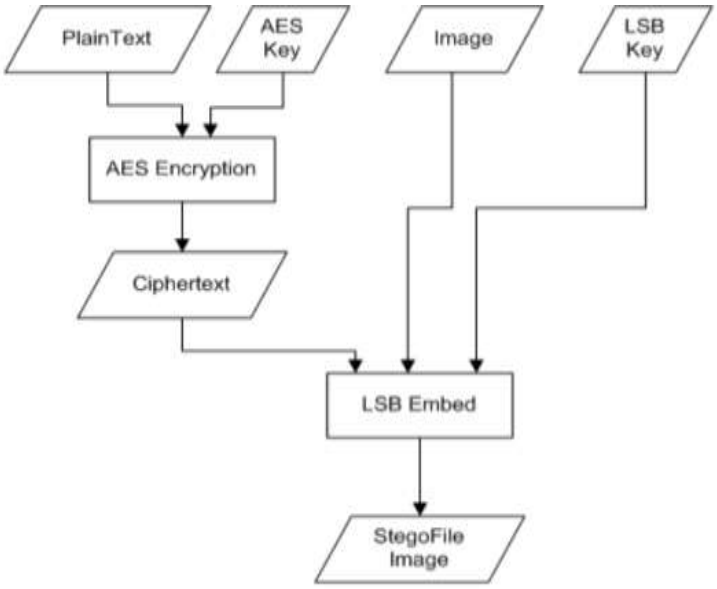

Fig4: Embedding process

C. *Extracting module*: *Extracting image file to give output as plain text.*
The algo is as follows:
Begin
1) Initially we put the stego bmp file and LSB key to do the decoding part.
2) After doing so, we obtain the ciphertext.
3) Lastly, we use the AES key to do the extraction part. This process goes until we obtain plaintext.
End.

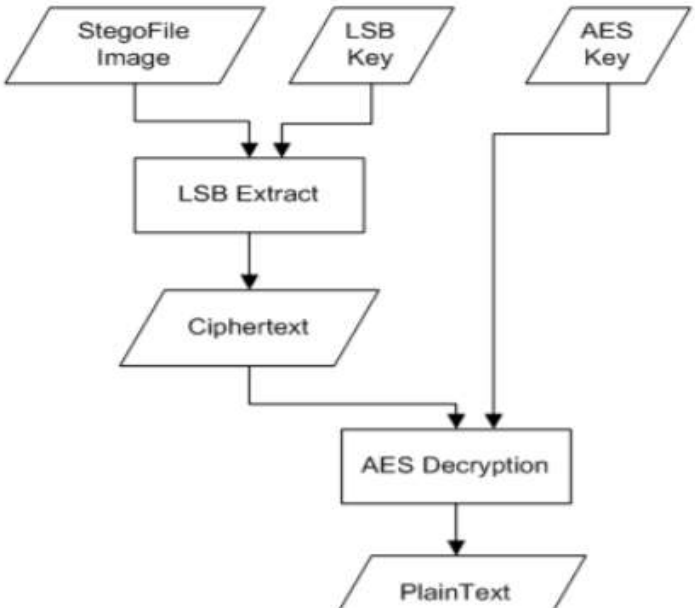

Fig5: Extracting process

IV. RESULTS& DISCUSSION: The proposed calculation was actualized utilizing MATLAB. This area presents the trial results and shows the estimations of PSNR and MSE determined for stego and carrier picture utilizing formulas are given beneath.
A. *PSNR*: PSNR is the Peak Signal to Noise Ratio which helps in getting to the nature of Stego picture as for the first picture. It ascertains the subtlety of the Stego picture. It helps to compare two pictures and helps to determine the closeness between them.[21]The more is the PSNR of the image the more it will be accurate. The formula for PSNR is depicted beneath.

$PSNR = 10\log_{10}[\frac{I^2}{MSE}]$

B. *MSE:* MSE is defined as Mean Square Errorthat helps in ascertaining theerror in the first picture and stego picture. The contrast among the estimations of unique and stego picture are multiplied and afterward their normal is determined.It is utilized essentially if there should arise an occurrence of huge mistakes since it gives generally high weight to these blunders. In this way, RMSE is extremely requesting when huge blunders are unfortunate in the image. The little is the estimation of RMSE, the more will be the nature of framework. Formula to compute MSE is as follows:

MSE $=\frac{1}{(R*C)^2}\sum_{i=1}^{N}*\sum_{j=1}^{M}(Xij-Yij)^2$

Where:

I = max estimation of the pixel. The maximum incentive for gray scale picture is 255.

R and C are the no. of lines and segment in the spread picture.

C. *Performance analysis:* So, by performing execution of the presented work, calculation is investigated based on PSNR and MSE. Fig6depicts the original and stego picture of Lena. Table 1 depicts the exhibition of the technique to show the values of PSNR and MSE.

D. *Results of Lena image*: Below we can see the original image and stego image of Lena.

Fig6: original and stego image of Lena

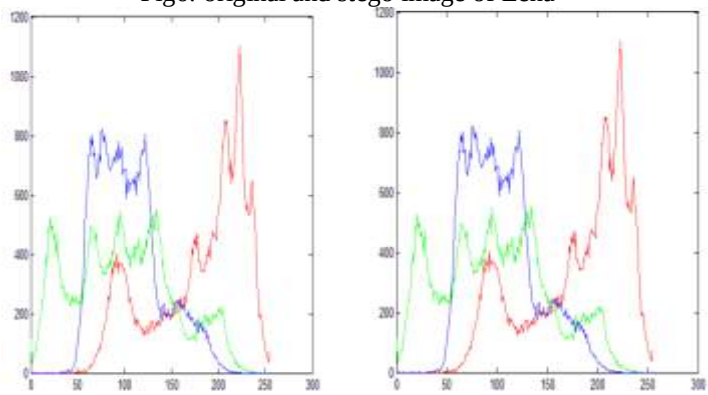

Fig7: histogram of lena image

TABLE1: *Performanceof proposed techniquewith lena image*

Image size	**Message size**	**PSNR**	**MSE**
256*256	1024 bits	73.6312	0.0623
256*256	2048 bits	71.3452	0.3481
256*256	4096 bits	69.6542	0.2134

V. CONCLUSION: In this paper, we intended combined approach for image steganography which overcomethe limitation of existing methods. This approach used them as a combination of layers and are implemented in MATLAB. The results obtained provide us a better security and privacy of data and enhances communication. This also overcome the problem of steganalysis. This method improved the quality of stego-image as well as gave a good PSNR and RSE values. This method creates multiple barriers in front of the attacker so it is impossiblefor intruder to extract the data.

VI: REFERENCES:

[1] Ammad Ul Islam, Faiza Khalid, Mohsin Shah, Zakir Khan, Toqeer Mahmood, Adnan Khan, Usman Ali, Muhammad Naeem "An Improved Image Steganography Technique based on MSB using Bit Differencing", The Sixth international conference on Innovative Computing technology (2016)

[2] Ian McAteer, Ahmed Ibrahim, Guanglou Zheng, Wencheng Yang and Craig Valli "Integration of Biometrics and Steganography: A Comprehensive Review" (2019)

[3] Ying Zou, Ge Zhang, Leian Liu "Research on image steganography analysis based on deep learning" (2019)

[4] Ra'ad A. Muhajjar, Farah A. Badr "Secure Data Communications using Cryptography and IPv6 Steganography", International Journal of Engineering &Technology, (2019) 163-168

[5] Ning Wu, Poli Shang JinFan, Zhongliang Yang, Weibo Ma, henru Liu "Research on Coverless Text Steganography Based on Single Bit Rules",IOP Conf. Series: Journal of Physics: Conf. Series 1237 (2019) 022077

[6] U. A. Md. EhasnAli, Md. Sohrawordi, Md. Palash Uddin "A Robust and Secured Image Steganography using LSB and Random Bit Substitution",American Journal of Engineering Research (AJER) 2019 Volume-8, Issue-2, pp-39-44

[7] Rasha Thabit "Improved Steganography Techniques for Different Types of Secret Data" (2019)

[8] Manisha Verma, Hardeep Singh Saini "Analysis of Various Techniques for audio Steganography in Data Security", IJSRNSC Volume-7, Issue-2(2019)

[9] PranayKalamkar, MrunaliGaikwad, Sumit Gore, Dhananjay Sonule, Prof. VidyaBodhe "A Review on ImplementationVisualCryptographyand Steganography" (2019) IJSRST, Volume 6, Issue 2

[10] AditiSharma, MonikaPoriye, Vinod Kumar "A Secure Steganography Technique Using MSB", International Journal of Emerging Research in Management&Technology 2017, Volume-6, Issue-6

[11] Farshad Miramirkhani, Omer Narmanlioglu "A Mobile Channel Model for VLC and Application to Adaptive System Design", IEEE communications letters, vol. 21, no. 5, may 2017

[12] Akram AbdelQaderand FadelAlTamimi "A novel image steganography approach using multi-layers dct features based on support vector machine classifier", The International Journal of Multimedia& Its Applications (IJMA) Vol.9, No.1, February 2017

[13] Soumendu Chakraborty&Anand Singh Jalal&CharulBhatnagar "LSB based non blind predictive edge adaptiveimage steganography", Multimed Tools Appl (2017) 76:7973–7987

[14] ApoorvaShrivastavaandLokesh Singh "A new hybrid encryption and steganography technique: a survey",International Journal of Advanced Technology and Engineering Exploration, Vol 3(14) 2016

[15] AnupriyaAryaand SaritaSoni "A Literature Review on Various Recent Steganography Techniques", International Journal on Future Revolution in Computer Science & Communication Engineering Volume: 4 Issue: 1 (2018)

[16] B. Sudhir, R. Rahul, and Y. Rajkurnar "Insertion of message in 6th, 7th and 8th bit of pixel values and its retrieval in case intruder changes the least significant bit of image pixels" International Journal of Security and Its Applications, Vol. 4, No. 3, July, 2018

[17] Y. Rajkumar, R. Rishi, and S. Batra, "A New Steganography Method for Gray Level Images using Parity Checker," Int. J. Comput. Appl., vol. II, no. II, pp. 18-24,2017.

[18] K R. Babu, D. S. U. Kumar, and D. A. V. Babu, "A Survey on Cryptography and Steganography Methods for Information Security," Int. 1. Comput. Appl., vol. 12, no. 3, pp. 13-17,2017.

[19] K Muhammad, M. Sajjad, I. MeInnood, S. Rho, and S. W. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," Multimed. Tools Appl.,2015.

[20] K.-H. Jung and K-Y. Yoo, "Data hiding method using image interpolation," Comput. Stand. Interfaces, vol. 31, no. 2, pp. 465-470, 2019.

[21] M. Aziz, M. H. Tayarani-N, and M. Msar, "A cycling chaos-based cryptic-free algorithm for image steganography," Nonlinear Dyn., vol. 80, no. 3, pp. 1271-1290(2015).

