ISSN 2347 - 3983
Volume 8. No. 4, April 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter63842020.pdf
https://doi.org/10.30534/ijeter/2020/63842020

A Systematic Approach for Data Hiding Using Cryptography and Steganography

Kusuma Priya B[1], Lakshmana Phaneendra Maguluri[2], Dr. T.Srinivasarao[3], T.E.Rao[4]
[1]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fields,Vaddeswaram, Andhra Pradesh 522502, India, boddukusumapriya@gmail.com
[2]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fields,Vaddeswaram, Andhra Pradesh 522502, India, phanendra51@gmail.com
[3]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fields,Vaddeswaram, Andhra Pradesh 522502, India, srinivas123fast@gmail.com
[4]Department of Mechanical Engineering, Koneru Lakshmaiah Education Foundation, Green Fields,Vaddeswaram, Andhra Pradesh 522502, India, terao1@rediffmail.com

ABSTRACT

Information Security has always been a very substantial facet when it comes to hindering unauthorised access, destruction or inspection of confidential data. Today every field in the world makes use of multimedia information like image, video, or audio and the file transmitted. To serve data security cryptography and steganography are mainly used techniques, each of them had a problem. Cryptography is that the art of saving information by encrypting it into an obscure format. On the opposite hand, steganography is that the art and science of secret communication to send messages during a way which hides even the existence of the communication. This paper provides a mixed system design utilizing cryptography and steganography techniques to provide a reliable communication system capable of resisting attackers. The affine cipher is used in this paper to encrypt the hidden text message which provides an effective level of security. After that, combining the techniques of Discrete Cosine Transform (DCT) and Least Significant Bit (LSB) cryptography is utilized to mask encrypted messages inside the image. The achievement of the built structure is measured using the value of Mean Square Error (MSE), Peak signal to noise ratio (PSNR) value, and analysis of histograms. The results indicate the system designed offers a noble security level.

Key words: Affine Cipher, Cryptography, DCT, Histogram, LSB, PSNR, Steganography.

1. INTRODUCTION

Cryptography and steganography are commonly used methods for protecting the privacy, integrity, availability of data. By combining cryptography & steganography modes which provides a strong communication mechanism for exchanging the data over insecure channel.

Cryptography is that the science of protective sensitive info by coding it into associate illegible format. Cryptology or Cryptography may be a word originated by combining two Greek words “crypto” suggests that HIDDEN and “graphe” means that WRITING. In this, Sender will encrypt the secret message in unreadable[16] format by using certain key and this encrypted message is called cipher text then the cipher text will pass to the receiver the secret message will be decrypted by the receiver using key. Cryptography algorithms and ciphers is categorised mainly into two sorts, one is symmetrical key or secret key cryptography rule & alternative one is asymmetric key or public key encryption algorithm. within the case of regular key cryptography one key's utilized by the sender aspect for cryptography method and additionally corresponding key's utilized by the receiver aspect for decipherment method in order that the secretive key will be shared between sender and receiver. In public key cryptography two keys are employed, one is secret key that is employed by the receiver aspect next alternative one is common key that is declare to the public.

Steganography is actually an art of writing[17] masked messages. It is the process of masking a piece of information behind another piece of information that can only be viewed by the receiver. For example, there is one text file which contains hidden message we can hide this text file behind any image file and we can hide this text file behind any mp3 file so it's a same vice-versa we can hide on mp3 file behind any image file and we can hide any image file in any text file. There are many[18] alternative techniques are offered for steganography. LSB is that the most typically used steganography technique which gives high security.

2. RELATED WORKS

J Kadim, B Halloran and J viral [1] have presented a review on existing types of image steganography and the recent contributions in each category in multi-ple modalities. It gives the complete overview of steganography image

including their requirements, general operations, different types of aspects, and evaluation of performance. This review does not provide information about other steganography techniques.

Rashmi N and Jyothi k[2] proposed an approach by combining cryptography and steganography which provide security when confidential information to be sent over an insecure channel. In this they used RC4 algorithm to encrypt the data, It is symmetric key algorithm attackers can easily break this algorithm and get the data.

Alsammak, M Ahmed and A Attaby [3] introduced a new technique called jpeg image steganography to enhance the increasing of Steganographic capacity as well as quality of stego image. They also designed a new algorithm called dct-m3 which is going to reduces the number of changes in the cover image. This algorithm supports only jpeg images.

B Samir kumar, M Upasana and B Datta[4] used a technique in which confidential data does not embedded directly within the cover file but the intensity of cover pixcel are adjusted so that at the receiver side by performing binary addition actual target bits are extracted from stego image.

H Abdulzahra Atee, A Robiah, N Mohd and hmad[5] developed a new mechanism by combining cryptography and steganography which is used to hide a secret message. A new encryption schema is tested and merged with two Steganographic methods named Simple LSB and color image-based data (CIBDH) hiding in order to prove its effectiveness and performance. In this they used single public key at the time of encryption which is vulnerable to attacks.

S subhedra and H Mankar[6] gives a review on fundamental concepts, Seurity aspects evaluation measures of strganography system, various spatial and transform domain embedding schemes. In addition, for the analysis of stego images, image quality metrics are used. This research only focused on image steganography.

Saleh Saraireh[7] introduced a new system which is a combination of cryptography and steganography techniques. In this to encrypt the data filter bank encryption algorithm is used and to hide encrypted data within the image discrete wavelet transforms based steganography technique used. Discrete wavelet transforms algorithm is more robust to attacks.

Roopali Soni and Pria Bharti [8] proposed a new algorithm by merging of cryptography and steganography techniques, this is used for embedding data in images. This algorithm can embed data within the images without discarding it and it is efficient for small data. This proposed system works only on encryption process.

Mohit g[9] used a text steganography method which used to hide sensitive data within the html report. In this they first encrypt the data and then hide the data within the html files. The benefit of using html files is that the sensitive data will not be suspicious because they are fundamental elements of the web. This proposed work only gives support to the text steganography system.

Mir A.H and Arooj N [10] presented that steganalysis is the concept detecting the confidential data inserted in digital media by using stseganography. B. Priya and Sastry [16] In this survey they arrange various methods that have been designed for steganalysis and some methods are also identified for statistical steganalysis.

T Wei-Liang, C Chin-Chen, and Y Chia-Ming [11] presented a histogram modification used for reversible data hiding. They solved the issue of peak points communicating pair by using binary tree structure and histogram shifting model is employed to prevent from overflow and underflow.

Mohammad Ali and Aman J [12] introduced a traditional steganography approach for data hiding.
zeros and ones form of confidential information is used to rewrite the LSB of each byte within the encrypted image randomly. The results shows that the encrypted image deacy and interaction values before insertion and after insertion are similar. They used single public key for encryption.

Yuan-Hui Y, Iuon-chang L and Chin-Chen C[13] proposed a Steganography method for inserting a grayscale picture within a true color picture. In this presented method three types of obscure pictures can be carried. First one is color obscure picture covering second is palette-based 256-color obscure picture covering and third is grayscale picture covering in a true color picture.

Tao Z, Mingwu s, Yan Z and Xijian P[14] presented that picture smoothness is defined as allocation of the variation between the current pixel value and its neighbourhood average pixel value is statistically modelled, Kim,S. Jihyun and Minsoo[17] and then the variance of this statistical distribution.

Alvaro M, Gadiel S and Guillermo S[15] are experimentally performed survey on if stego-images, bearing a confidential data, are statistically “natural.” For this purpose they have used results on some steganography methods and the statistics of natural pictures.

3. PROPOSED SYSTEM

3.1 Over View of the Proposed System

This paper is to provide a strong connection among sender and receiver over unsecure channel. The proposed method explained two steps for hiding secret message. The first one is

changing from plaintext to ciphertext by using an affine cipher, in some cases sending an encrypted message causes impression whereas invisible message won't do so. The second one is hiding the ciphertext in an image by using the merging of LSB technique and DCT technique.

Affine cipher is a monoalphabetic substitution cipher where each letter is replaced by others. It is the mix of Ceaser cipher and productive cipher which uses two keys for encryption and decryption process named K1 and K2. The whole action depends on operating modulo m that is the length of the alphabet. In affine cipher letter of the associate alphabet of size m mapped to integers within the scope zero to m-1.K1 should be chosen relatively prime to m.

3.2 Framework of the planned system

The planned technique primarily has the subsequent schema. It depicts the essential flow of each the embedding and extraction method of the planned schema as shown in figure one and figures two severally. figure [1] exhibits the method of canopy a secret info within the image. Figure [2] describes the method of extracting hidden info from the image.

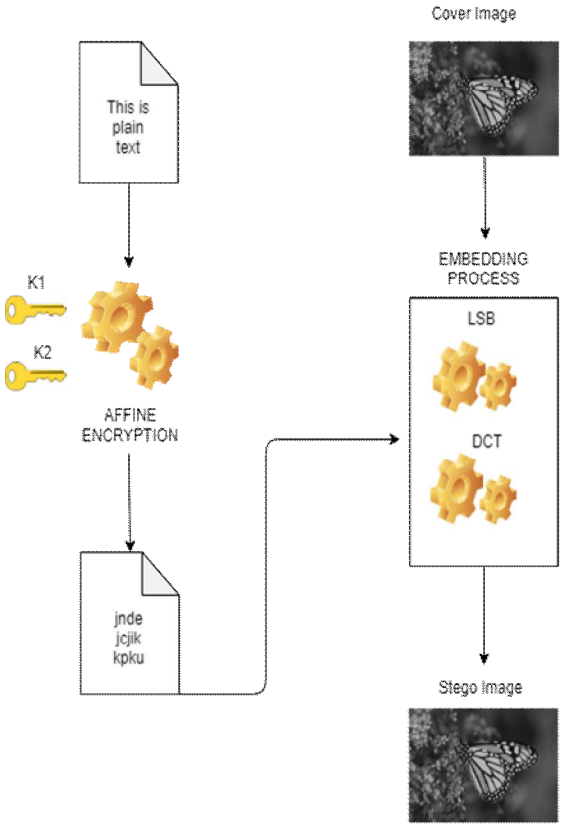


Figure 1: Hiding Mechanism

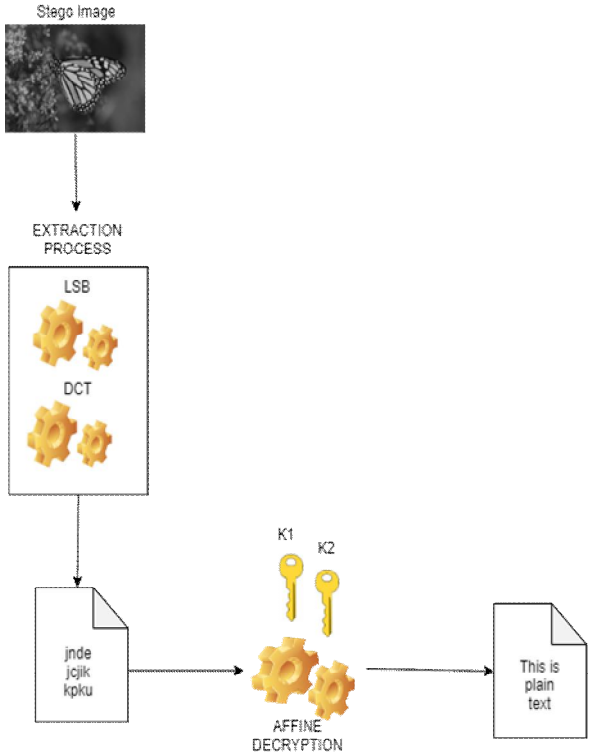


Figure 2: Extraction Mechanism

3.3 Embedding and extraction process

Algorithm

Input: Secret message which should be in readable format.
Output: Secret message which should be in unreadable format.

Data Encryption
Step 1: Create Cipher Text variable named C.
Step 2: The chosen keys should be less than or equal to 26, otherwise there is an error.

If K1>26 && K2>26
Error="wrong key used"

Step 3: If the keys are less than 26 calculate the length of the PlainText.

For i=1:1: length (PlainText)

Step 4: Next find the index value of the PlainText using find function.

P=find (index==PlainText (i))

Step 5: Then calculate the CipherText value.

C=mod (K1*(P-1) + K2, 26)

Step 6: The obtained CipherText value is in numeric format, convert numeric format to character format by using char function.

Cipher=char(C)

Data Decryption
Step 1: Create PlainText variable named P.
Step 2: Calculate the length of CipherText.

Step 3: Next find the index value of the CipherText using find function.
Step 4: Then calculate the PlainText value.

P=mod (K1_inverse*(C-1) - K2, 26)

Step 5: The obtained PlainText value is in numeric format, convert numeric format to character format by using char function.

For hiding data in images a combined mechanism of LSB and DCT are implemented to improve hiding capacity and peak signal noise ratio.

Steganography Based on Lsb:-

Algorithmic approach to embed text message:-
Input: input image.
Output: Image which hides secret information.

Step 1: Read the input image.
Step 2: Convert the image to the grayscale image.
Step 3: Size the image needed to size.
Step 4: Convert the message to its binary format.
Step 5:Initialize output image identical as associate degree input image.
Step 6: Traverse through every picture element of the image.
Step 7: Convert the image constituent worth to binary.
Step 8: Get subsequent little bit of the message to be embedded.
Step 9: produce a variable temporary worker called temp.
Step 10: If message bit = LSB little bit of the constituent then set temp=0.
Step 11: If the message bit! = LSB little bit of the constituent then, set temp=1.
Step 12: This setting of temporary worker are often done by taking XOR of the message bit and therefore the LSB of the constituent.
Setp 13: Update the constituent of the output image to input image constituent worth +temp.
Step 14: Keep change the output image till all the bits within the image are embedded.
Step 15: Finally, write input image also as output (or stego) image to the native system.

Algorithmic approach to retrieve text message:-
Step 1: Read Output(stego) image.
Step 2: Traverse through the image every picture element.
for i=1: height & for j=1: width
Step 3: Convert image pixel values to binary.
Step 4: Calculate the LSB of every pixels of output image.
Step 5: Restore those bits.
Step 6: The string is obtained by Converting each bit into character.
Step 7: Display the textString.

Steganography Based on DCT:-

Algorithmic approach to insert text message:-
Step 1: Browse input image.
Step 2: Convert the image to grayscale image.
Step 3: Read confidential data and change to its binary format.
Step4: Broke the input picture to 8×8 block of picture element.
Step 5: Acting from prime to bottom, left to right figure 128 in every block of pixels
Step 6: Apply DCT to each block of the picture element.
Step 7: Compress each block by using quantizaation table.
Step 8: Find Least Significant Bit of every Discrete Cosine coefficient and alter with every bit of secret information.
Step 9: Write Output image.

Algorithmic approach to restore text message:-
Step 1: Browse Output image.
Step 2: Broke stego image into 8×8 blocks of picture element.
Step 3: Acting from prime to bottom, left to right deduct 128 in every block of pixels.
Step 4: Implement DCT to every block.
Step 5: Compress every block by using qantization table.
Step 6: Determine Least Significant Bit of every Discrete Cosine coefficient.
Step 7: Retrieve every eight bit and convert it into character.

4. RESULTS AND ANALYSIS

In this paper for analyzing the operating of the planned system, 5 completely different cowl pictures were utilized to insert associate encrypted secret message. During this initial, the key data is encrypted, then encrypted data is hidden in a picture and sent to the receiver. At the recipient aspect, hidden secret data is initial extracted then decrypted. This represents a hybrid system that could be a combined technique of cryptography and steganography algorithms for developing the dependability of the information and concealing capability of the image. This mixture is tested using MSE, PSNR and histogram analysis.

MSE ought to be as less as possible. If the input image and output image square measure an equivalent then MSE is zero. The MSE of the designed structure using distinct pictures was measured exploitation equation [1], and also the results are sumarized in Table one.

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

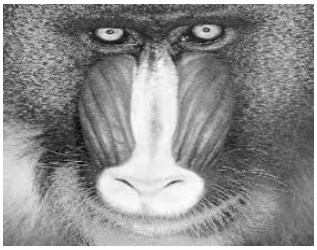
PSNR is a measure of distortion within the stegano image. it's measured in decibels (dB). If the PSNR worth of the grayscale image larger than 36dB then, humans can't notice between the input image and output image. The PSNR of the designed system using completely different pictures was computed applying equation [2], and therefore the outcome results are summarized in Table one.

$$psnr = 10 \times log_{10}\left(\frac{255 \times 255}{mse}\right) \quad (2)$$

Table 1: MSE and PSNR Results

COVER IMAGE	MSE	PSNR
Baboon	0.98	48
Butterfly	1	46
House	0.74	49.4
Wolf	1.16	47.9
Peppers	1	47

The histogram analysis is employed to judge the flexibility of the projected technique. If the bar graph remains a similar as once embedding the data, then the planned algorithm is effective. The bar graph of the input pictures before & once the embedding method was plotted as shown in figures [5] and figure [6]. Note that the histograms of the input pictures and stegano pictures do not have any notable difference.



(i) Baboon cover picture

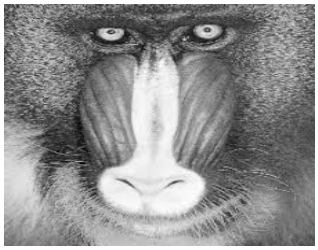
(ii) Butterfly cover picture

(iii) House cover picture

(iv) Wolf cover picture

(v) Peppers cover picture

Figure 3: Dataset of cover images



(i) Baboon stego picture

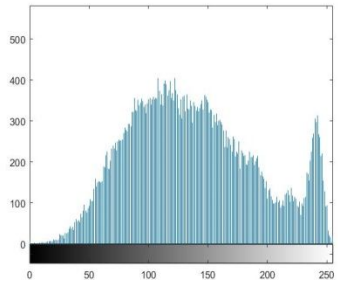
(ii) Butterfly stego picture

(iii) House stego picture

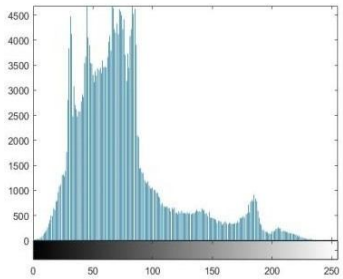
(iv) Wolf stego picture

(v) Peppers stego picture

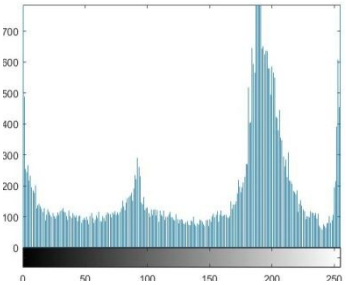
Figure 4: Dataset of stego images



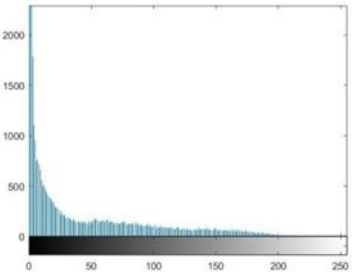
(i) Histogram of Baboon cover picture



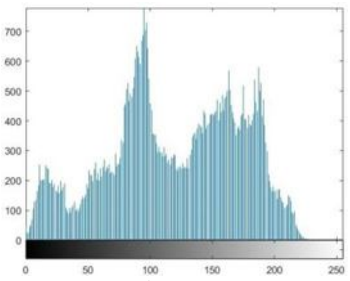
(ii) Histogram of Butterfly cover picture



(iii) Histogram of House cover picture

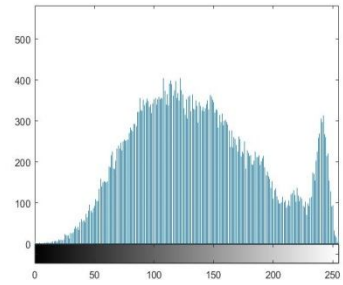


(iv) Histogram of Wolf cover picture

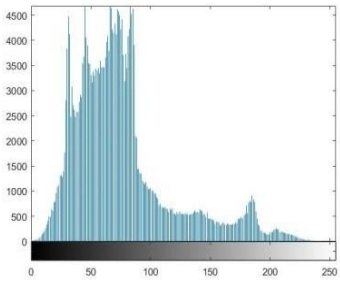


(v) Histogram of Peppers cover picture

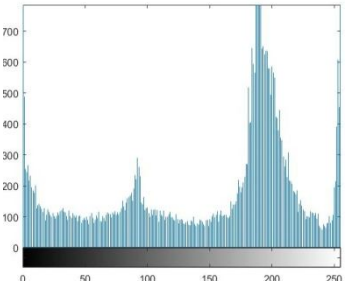
Figure 5: Dataset of histogram cover images



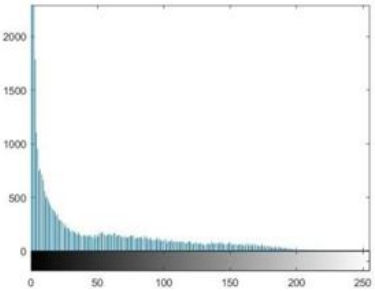
(i) Histogram of Baboon stego picture



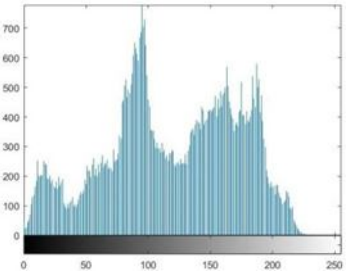
(ii) Histogram of Butterfly stego picture



(iii) Histogram of House stego picture



(iv) Histogram of Wolf stego picture



(v) Histogram of Peppers stego picture

Figure 6: Dataset of histogram stego images

5. CONCLUSION

This paper proposes a high-security model that uses both steganography and cryptography techniques. Affine cipher is a technique of cryptography, used for data encryption. Affine cipher is a symmetric processor; it offers high security, flexibility, and agility. Using steganography techniques such as the (DCT) and (LSB) the encrypted information is inserted into a cover picture. MSE, PSNR, and histo-gram have been used to find the operation of the planned algorithmic rule. The result showed that the MSE values area unit low and PSNR of the purposed system is high, which ensures the invisibility of the covert info through the masked image. Also, the histogram diagrams of the stegano image and input(cover) image are extremely near to one another, which confirms the resistant of the purposed system against the attacks.

REFERENCES

[1] J. Kdhim, P. Premaratne, P. J. Vial and B. Halloran. **Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research**, Neurocomputing, 2019, pp.299-326. https://doi.org/10.1016/j.neucom.2018.06.075

[2] N. Rashmi and K. Jyothi. **An Improved Method for Reversible Data Hiding Steganography Combined with Cryptography**, In Proc. International Conf. on Inventive Systems and Control, 2018, pp.81-84. https://doi.org/10.1109/ICISC.2018.8398946

[3] A Attaby, F. M. Mursi ahmed and K. Alsammak. **Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3**, Ain Shams Engineering Journal, 2017. https://doi.org/10.1016/j.asej.2017.02.003

[4] B. Datta, M. Upasana and B. S. Kumar. **LSB Layer Independent Robust Steganography using Binary Addition**, In Proc. International Conf. on Computational Modeling and Security Procedia Computer Science, Vol.85, 2016, pp.425-432. https://doi.org/10.1016/j.procs.2016.05.188

[5] H. A. Atee, R. Ahmad and N. Mohd Noor. **Cryptography and Image Steganography Using Dynamic Encryption on LSB and Color Image Based Data Hiding**, Middle-East Journal of Scientific Research, Vol.23, No.7, pp.1450-1460, 2015.

[6] M. S. Subhedar and V. H. Mankar. **Current status and key issues in image steganography: A survey**, computer science review, 2014.

[7] S. Saraireh. **A Secure Data Communication System Using Cryptography and Steganography**, International Journal of Computer Networks & Communications, Vol.5, No.3, 2013 pp.125-137.

[8] P. Bharti and R. Soni. **A New Approach of Data Hiding in Images using Cryptography and Steganography**, International Journal of Computer Applications, Vol.58, No.18, 2012,pp.1-5.

[9] G. Mohit. **A Novel Text Steganography Technique Based on Html Documents**, International Journal of Advanced Science and Technology, Vol.35, 2011, pp.129-138.

[10] Nissar and A. H. Mir.**Classification of steganalysis techniques: A study**, Digital Signal Processing, 2010, pp.1758-1770. https://doi.org/10.1016/j.dsp.2010.02.003

[11] T. Wei-Liang, Y. Chia-Ming and C. Chin-chen. **Reversible Data Hiding Based on Histogram Modification of Pixel Differences**, IEEE Transactions On Circuits And Systems For Video Technology, Vol.19, No.6, 2009, pp.906-910.

[12] M. A. Youns and A. Jantan. **A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion**, IJCSNS International Journal of Computer Science and Network Security, Vol.8, No.6, 2008,pp.247-254.

[13] Y. Yuan, C. Chin and L. Iuon. **A new steganographic method for color and grayscale image hiding**, Computer Vision and Image Understanding, Vol.107, 2007, pp.183-194. https://doi.org/10.1016/j.cviu.2006.11.002

[14] Z. Tao, Z. Yan, P. Xijian, S. Mingwu. **Detection Of Lsb Steganography Based On Image Smoothness**, In Proc. IEEE International Conf. on Multimedia and Expo, 2006.

[15] Martin, G. Sapiro and G. Seroussi. **Is Image Steganography Natural**, IEEE Transactions On Image Processing, Vol.14, No.12, 2005, pp.2040-2050.

[16] B. Priya and Sastry. **Assessment of Website Quality based on Appearance**, International Journal of Emerging Trends in Engineering Research, 2019. https://doi.org/10.30534/ijeter/2019/017102019

[17] M. L. Phaneendra and R.Ragupathy. **A New sentiment score based improved Bayesian networks for real-time intraday stock trend classification**, International Journal of Emerging Trends in Engineering Research, 2019.

[18] M. Syamala and N.J.Nalini. **A Deep Analysis on Aspect based Sentiment Text Classification Approaches**, International Journal of Emerging Trends in Engineering Research, 2019. https://doi.org/10.30534/ijatcse/2019/01852019