RESEARCH ARTICLE OPEN ACCESS

Dual Level Image Steganography for Data Hiding using AES & LSB

Rahul Kumar M.Tech. Scholar
Computer Science & Engineering Rabindranath TagoreUniversity Raisen, Madhya Pradesh - India
Devendra Singh Rathore Asst. Professor
Computer Science & Engineering Rabindranath Tagore University Raisen, Madhya Pradesh - India
Mukesh Kumar Asst. Professor
Computer Science & Engineering Rabindranath Tagore University Raisen, Madhya Pradesh - India

ABSTRACT
Image steganography is a technique for hiding a message into the cover of the image. Message can be either in text format or image however concealing message inside the image is considerably more famous and pertinent. In this computerized world; it is needed to convey subtly or passing the message secretly through which a public safety or individual ones unwavering quality can be kept up with. Here the framework depends on Dual layer Advanced Encryption Standard (AES) and Least Significant Bit (LSB) that can be additionally called a half and half strategy where two techniques can be interceded to upgrades the security fix of the framework. In this work a mysterious message has been scrambled utilizing AES and afterward concealing that encoded message in an image by utilizing LSB individually. According to the LSB philosophy; here k-LSB has been sent to conceal the mysterious message in an image productively without expanding the size definitely. Also later for interpreting the mysterious message an area based identification strategy has been utilized to remove or unhide the secret box. Here the framework uses the encryption technique for concealing a message in a confounded and irregular string afterward concealing it into the image according to the benchmarks.

Keywords— Image Steganography, Advanced Encryption Standard, Least Significant Bit, K-LSB, Data Hiding, Region Detection Method.

I. INTRODUCTION

With the lift in computer vision, the web and with the advancement of computerized signal handling, DSP, data hypothesis and coding hypothesis, steganography has gone "advanced". In the domain of this advanced world steganography has made an air of corporate carefulness that has generated different fascinating applications, accordingly Markup Language, XML. An image is addressed as a N*M (in the event of greyscale images) or N*M*3 (if there should be an occurrence of shading images) network in memory, with every passage addressing the power worth of a pixel. In image steganography, a message is inserted into an image by adjusting the upsides of certain pixels, which are picked by an encryption calculation. The beneficiary of the image should know about a similar calculation to know which pixels the individual should choose to remove the message [1].

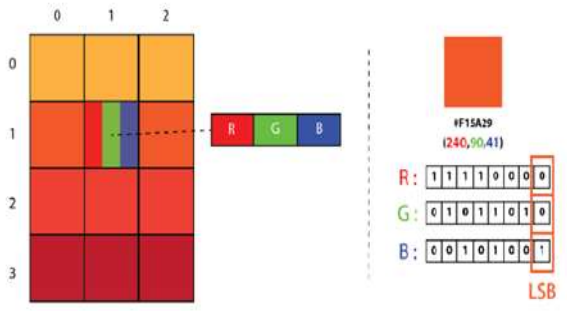


Fig. 1. Image Steganography [2]

Steganography comprises of a variety of mystery associated techniques that stow away the information from being distinguished or seen. For concealing restricted data in the image, there exist countless techniques for steganography strategies some of them are significantly more intricate than outsiders all the graphical UI have there a portion of the free focuses or more grounded focuses. Distinctive application actually needs outright mortality of the restricted intel, while diverse application needs a colossal privileged information its proceeding with development is ensured. Digital wrongdoing is accepted to profit from this computerized upset. Henceforth a quick concern was displayed on the conceivable utilization of steganography by hoodlums. Digital preparation or the "advanced danger" as Lieutenant Colonel Timothy L. Thomas characterized it as being hard to control. Provos and Honeyman examined 3,000,000 images from famous sites searching for any hint of steganography. They have not tracked down a solitary secret message. Notwithstanding the way that they credited a few motivations to this disappointment it ought to be noticed that steganography doesn't exist just in still images. Installing stowed away messages in video and sound documents is likewise conceivable. Models exist for concealing information in music documents, and surprisingly in a less complex structure, for example, in Hyper Text Markup Language , HTML, executable records, .EXE, and Extensible to be covered up.

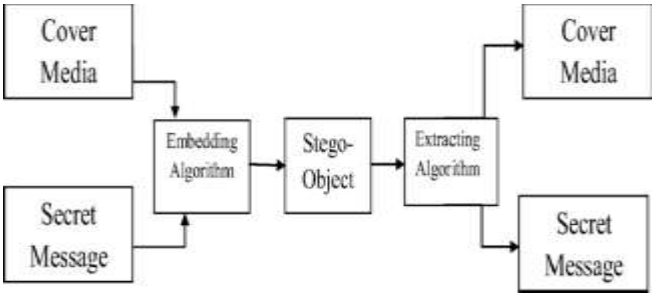


Fig. 2. General Image Steganography System

II. RELATED WORKS

A. Related Works

Shivani et al. [3] et al. proposed a system which is based on zero distortion technique. Zero distortion technique is a clever methodology for performing steganography, in which computerized medium is utilized as a kind of perspectivenotational frameworks into the edge and non-and privileged information is concealed in such a way so that there is no distortion in the cover medium. Srilekha Mukherjee et al. [4] proposed a system which is based on mid position value technique. From there on, Mid Position Value (MPV) technique is executed to insert information bits from the mysterious image inside the mixed cover. Ultimately, converse Arnold change is applied on the above image. The outcomes in a descrambling activity, for example returning the ordinary direction. Hereafter the stego is produced. Every one of the test results examines the result of the full strategy. For this reason, a few quantitative and subjective benchmark examination relating to this methodology have been made. Mohammed Abbas Fadhil et al. [5] proposed a system which is based on Mapping algorithm. In this work, a clever steganography framework was introduced. The principle ventures for applying this framework are clarified. We can finish up the fundamental properties and benefits of this framework through the accompanying focuses: When the framework fabricates the FT from the pixels of the stego-image, and afterward maps these frequencies to the request for frequencies (of the alphabetic English letters). Jia Lui et al. [6] proposed a system which is based on Generative Adversarial Networks. With the generative models, image steganography started to converge with the field of PC vision. Conventional PC vision analysts have likewise begun to concentrate on image steganography. A blend of the exploration fields widens the spaces of image steganography. In addition, the presentation of GANs into the examination thoughts of data concealing will likewise altogether affect the improvement of other data concealing advances, for example, computerized watermarking innovation. In this paper, creators survey image steganography with GAN. Randa Atta et al. [7] proposed a system which is based on neutrosophic set. This paper has proposed an image steganography strategy dependent on edge EMD and neutrosophic set. In the proposed plot, the cover image is separated into blocks which are arranged into edge and non-edge blocks dependent on the changed neutrosophic set edge finder (MNSED). Dissimilar to the current steganography techniques dependent on EMD, the proposed strategy works with inserting the mysterious digits in two unique - ary edge blocks. Additionally, it ensures assessing the specific edge areas subsequent to installing the mysterious message and thus keeps away from the weight of implanting of overhead edge data in the cover image. Vikas Verma et al. [8] proposed a system which is based on Midpoint Circle Approach. As contrasted and the customary Least Significant Bit calculation, the information stowing away steganographic strategy introduced in this paper was viewed as of expanded intangibility to steg analysis assaults on the cover image. Along these lines, this strategy is most appropriate for the reasons for correspondence applications. Omar Elharrouss et al. [9] proposed a system which is based on k-LBS technique. In this paper, an image steganography technique has been introduced for concealing an image into another. Utilizing the k-LSB-based technique the proposed strategy start by blending the cover image and the images to be covered up. To distinguish the area that contains the secret images, a district discovery activity has been introduced utilizing the neighborhood entropy channel. Daxa L. Vasoya et al. [10] proposed a system which is based on classification algorithm. This paper proposed a clever technique for image steganography dependent on DCT and information mining order techniques. Two 8 digit dim level image of size P X Q and M X N are utilized as cover image and mystery image individually. DCT is performed on both mystery image and cover image. Wa'el Ibrahim A. Almazaydeh et al. [11] proposed a system which is based on dynamic symmetric key. This paper shows two techniques for Steganography: the first is the notable technique which is known as Least Significant Bit, and the subsequent one is the new technique with LSB +KEY.The execution of the outcomes have been analyzed utilizing the PSNR values of individual calculations. It is noticed that the LSB +KEY calculation gives better result regarding the PSNR values Hayat Al-Dmour et al. [12] proposed a system which is based on Edge Detection and Hamming Code. In this paper, a proficient clinical image steganography technique is proposed for concealing patient secret data. The proposed technique can be utilized as an effective enhancement to cryptography strategies. It consolidates edge recognition to recognize and implant in high differentiation spaces of the image, and thus, draw in less consideration from interlopers. Shalaw Mshir et al. [13] proposed a system which is based on ASCII embedding technique. This technique has the accompanying qualities: The first image and the Stego

image seem to be indistinguishable. The natural eye can't see the distinction on account of the great PSNR result. The technique endeavors to find a mysterious message in the higher layers of the pre-owned image and changes the last layer of the comparing block. This will build the level of heartiness of the Stego investigation techniques. Bit mistake = 0 for generally trial results; the installed secret message is recuperated effectively with no blunders. Elshazly Emad et al. [14] proposed a system which is based on least significant bit and integer wavelet transform. This paper proposes a protected image steganography algo rithm for inserting a mysterious text in computerized images by us ing the IWT technique dependent on the LSB calculation. Four distinct instances of IWT-LSB are proposed, which are IWT LSB-1, IWT-LSB-2, IWT-LSB-3 and IWT-LSB-4. The proposed half and half IWT-LSB calculations are performed us ing the MATLAB programming.

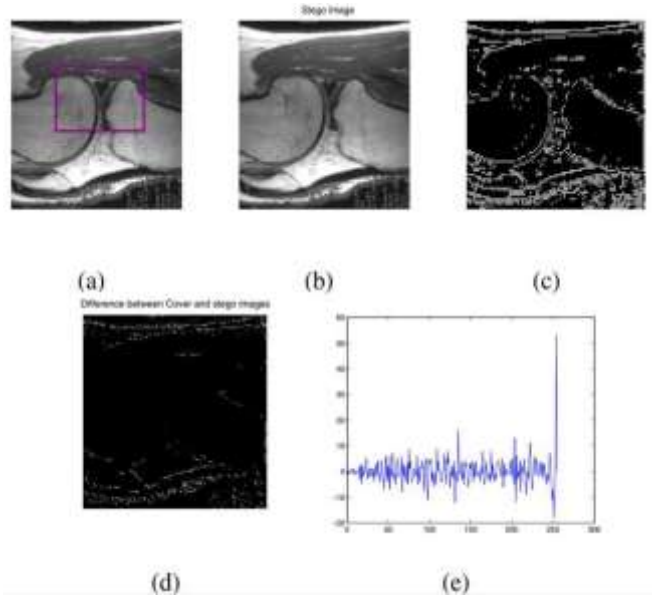


Fig. 3. (a) Cover Image, (b) Stego Image, (c) Edge Detected image, (d) Difference between (a) and (b) & (e) Difference between the cover and stego histograms [14]

Abbas Darbani et al. [15] proposed a system which is based on JPEG embedding technique. In this paper, a steganography technique in JPEG images is proposed. Since a piece of information might be lost after the discretization (or quantization) of recurrence values in the JPEG pressure methodology, in the proposed strategy, the implanted message is added to the image after the discretization stage. The strategy uses two contiguous pixels in the steganography interaction. Reza tavoli et al. [18] proposed a system which is based on LSB. This paper at first examines the various methodologies of steganography in an image . It has shown that the space pixel gives more limit than the recurrence area. Likewise, the sort of an image is viable in accomplishing the ideal outcome in steganography.In correlation with the present proposed techniques in recurrence space; our calculation has the capacity of putting away a bigger measure of data. Pressure prior to concealing advance is more suitable in imperceptibility of the steganography. Besides it expands the image limit with respect to information incorporation. Blending the utilization of a fitting cover with the use of a specific sweep of an image, and also adding a stage of encryption with each, takes into consideration various separate periods of data security.

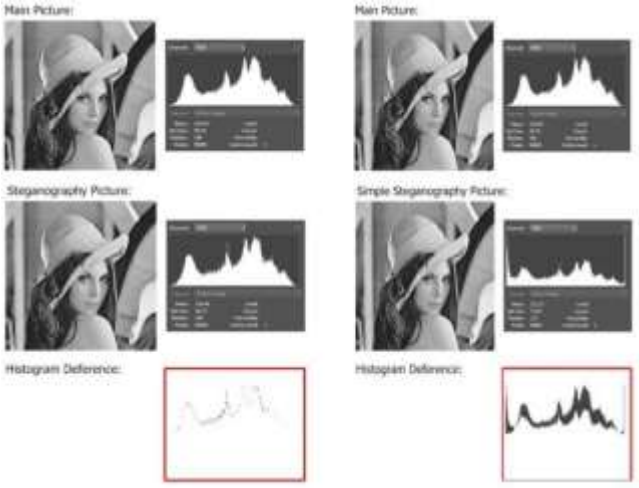


Fig. 4. Histogram Comparison [18]

Sumeet Kaur et al. [19] proposed a system which is based on hybrid hiding model. In this examination, image steganography framework has been proposed and executed for concealing a classified image in a host image. Wei Lu et al. [20] proposed a system which is based on histogram of structure element. In this paper, author proposed a new measurable model dependent on the histogram of SEs to address double images. We examined PMMTM exhaustively, talked about the connection between the histogram of SEs and the co-event grid of SEs (sub SEs) exhaustively, and presumed that the previous can supplant the last option in the errand of double image steganalysis. Vipul Sharma et al. [21] proposed a system which is based on LSB. This paper proposed a new steganographic calculation for concealing text documents in images. Here we have likewise utilized a fundamental pressure calculation with greatest pressure proportion of 8 pieces/pixel. We have fostered a framework in java dependent on the proposed calculation.

III. PROBLEM IDENTIFICATION

Deepak kumar et al. [21] presents an image steganography strategy utilizing YCbCr shading model dependent on Least Significant Bit (LSB). In this paper proposed technique convert the image from RGB to YCbCr shading space then privileged information is concealed inside YCbCr shading space utilizing least significant bit and subsequent to concealing the information, convert it back to RGB shading space. Various methods of cryptography are looked at utilizing Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). YCbCr Color Model is bit differ from RGB color model where luma component along with blue

and red difference components are present. The color intensity range is similar as RGB which is 0 to 255. Extracting hidden message from YCbCr based image is bit possible as compare to the RGB image because the luminance is quietly more visible in YCbCr instead of that RGB is bit complex for prediction because of natural colors. RGB images are not predictable and hardly find the altered region. Instead of changing the color model of the image; it is better to improve the security of the encryption as well as data hiding approach. For ideal system PSNR value should between 50 to 55 which maintains the quality of the image and also maintain the prediction rate for attackers because it does not much affect the image and it seems to be an original image.

IV. PROPOSED WORK

Proposed work is based on two different approaches first one is AES which has been used for encrypting the message at the time of embedding the message in an image and second one is LSB which has been used for hiding the message in an image that can not be predicted at the intruders end. Proposed system is successfully designed to achieve the good PSNR and MSE value that reflect the quality of the image that has not been modified a lot and the aspect ration is also maintained. In our work we utilize both cryptography and steganography. In order to get more security to the data we combine both the technique. Proposed System consists of two layers, namely Steganography Layer and Encryption/Decryption Layer.

A. Sender's End

As First of all; a secret message has to be written for encrpting the secret message, once the message has been writted then it will futher convert into binary code and once the binary conversion has been done then AES encryption has been initiated. The more well known and broadly took on symmetric encryption calculation prone to be experienced these days is the Advanced Encryption Standard (AES). It is figured out something like six opportunity quicker than triple DES. A trade for DES was required as its key size was excessively little. With expanding registering power, it was viewed as helpless against thorough key hunt assault.

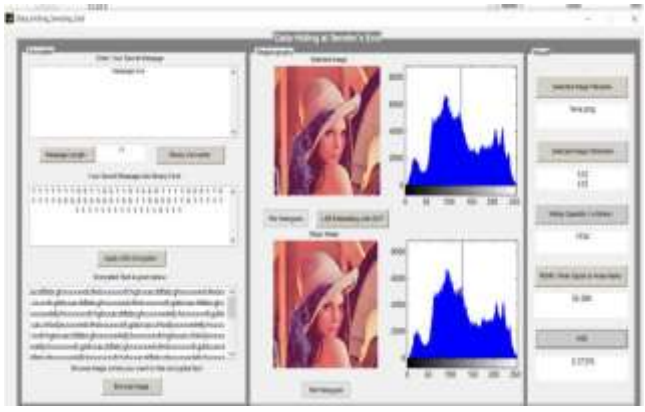


Fig. 5. Sender's End (Proposed)

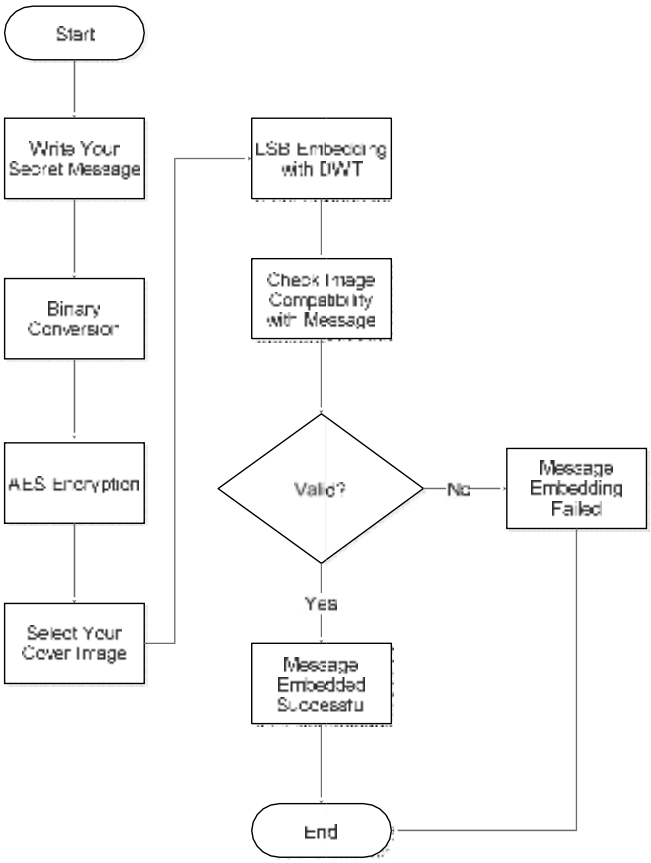


Fig. 6. Sender's End (Flow Chart)

Triple DES was intended to beat this downside however it was seen as sluggish. Once the message has been successfully encrypted the message then system attains for crypto image which will be considered as the input image or cover image then system will check the compatibility of the image whether it can be embedded with the message or not, it means that system intended to find the image resolution whether it is too low or too high or image has valid extention or not and once the system find the image suitable then it can be ready to be hide in a cover image which has been selected by the sender. Once the message has been indulge or hidden with the cover image then it can be send to the legitimate reciever and at the receiver's end it can be further decrypted and unhide the message and can read the confidential one with great level of authenticity.

B. Receiver's End

At the reciever end reciver has to select the target stego image and then system will futher check whether message is available in the stego image or not, and if message is embedded in the image then it can be extracted the encrypted message and once the encrypted message has been find then system can decrypt the message successfully and then then message will further convert into binary code and once the binary code has been extracted then system convert the binary image to text and that text must be the secret message which has been sent by sender. The system has been trained to secure a message with two level of security that can be called as hybrid method which is also

called a compound method for securing a secret message and hiding the message in an image without much affecting the PSNR value. The term Peak Signal to Noise Ratio (PSNR) is an articulation for the proportion between the most extreme conceivable value of a signal and the power of distorting commotion that influences the nature of its portrayal. Since many signals have an exceptionally wide dynamic range, (proportion between the biggest and smallest potential upsides of a variable amount) the PSNR is normally communicated as far as the logarithmic decibel scale. Image enhancement or working on the visual nature of an advanced image can be subjective. A technique gives a superior quality picture could fluctuate from one individual to another.

Fig. 7. Receiver's End (Proposed)

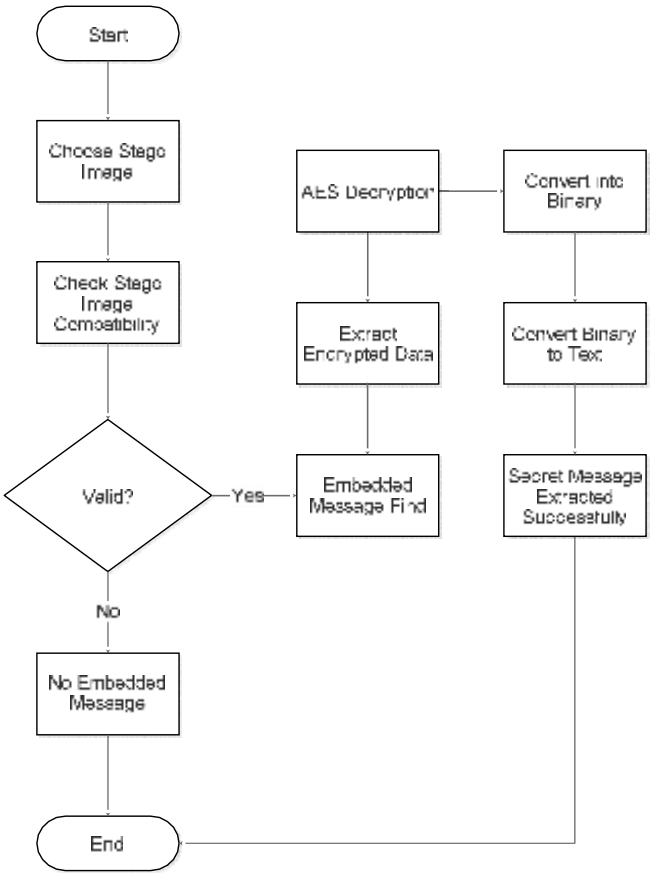


Fig. 8. Receiver's End (Flow Chart)

Consequently, it is important to build up quantitative/observational measures to look at the impacts of image enhancement for the calculations on picture quality. Utilizing similar kind of text images, diverse image improvement calculations can measure up deliberately to distinguish whether a specific calculation delivers better outcomes. The measurement being scrutinized is the peak signal to noise ratio. If it can show that a calculation or set of calculations can upgrade a degraded image or enhance a degraded image then more intently take after the first, then, at that point, it can all the more precisely presume that it is a superior calculation.

C. AES-LSB Dual Level Algorithm (Sender)-

INPUT: A ← Secret Message, Cover Image as two dimensional matrix and Secret Key

OUTPUT: C_t ← Stego Image

Step 1: Input secret message

Step 2: Calculate the Length of the message as M_i

Step 3: Convert message to Binary code

if message = "abc" **then**

binary code { 101010111100}

end if

Step 4: Convert binary to encrypted message through AES

Declare Key size = 128;

Declare Secret 16 bit key;

$$\begin{bmatrix} a1 & a2 & a3 \\ a4 & a5 & a6 \\ a7 & a8 & a9 \end{bmatrix} \longrightarrow \begin{bmatrix} b1 & b2 & b3 \\ b4 & b5 & b6 \\ b7 & b8 & b9 \end{bmatrix}$$

Encrypted message {
76A2F63499FFDD4B39654A6C41505228 }

Step 5: Select an image for LSB steganography

if $M_i < 1$ **then**

No Message for Embedding;

else

Embedded the secret message in target image;

end else

end if

Step 6: Send stego image to the receiver

Step 7: End

D. AES-LSB Dual Level Algorithm (Receiver)-

INPUT: A ← Stego Image as two dimensional matrix and Secret Key

OUTPUT: S_m ← Secret Message

Step 1: Input Stego Image

Step 2: Extract Secret Message M_j

Step 3: if stego image contains message **then**

Extract encrypted message;

else { No message found}

end else

end if

Step 4: Decrypt message through AES

Declare Key size = 128;

Declare Secret 16 bit key;

$$\begin{bmatrix} b1 & b2 & b3 \\ b4 & b5 & b6 \\ b7 & b8 & b9 \end{bmatrix} \longrightarrow \begin{bmatrix} a1 & a2 & a3 \\ a4 & a5 & a6 \\ a7 & a8 & a9 \end{bmatrix}$$

Decrypted message {
76A2F63499FFDD4B39654A6C41505228 }

Step 5: Convert decrypted message to binary

Binary code {101010111100}

Step 6: Convert binary code to text message

Secret message = "abc";

Step 7: End

V. RESULT ANALYSIS

Here the system has been validated with certain input cover images and secret message as per the base paper tested the dataset. Each cover image has been embedded with secret message at the sender's end and then it further decrypted at the receiver's end successfully. Each traversing pertains hiding capacity, PSNR value and MSE value.

Table No. I Result Analysis

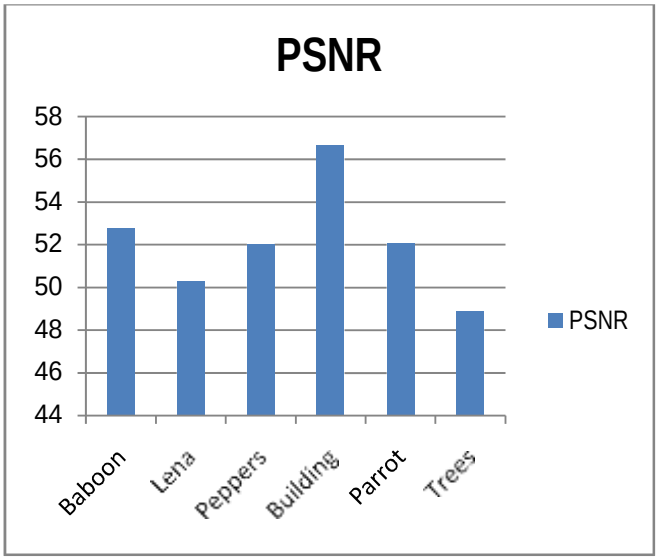
Image Name	Image dimension	Hiding capacity	PSNR value	MSE
baboon.jfif	1620 * 1080	3238	52.77	0.10997
lena.png	512 * 512	1534	50.286	0.37376
peppers.png	722 * 850	2548	52.042	0.18146
building.jpg	1200 * 1920	5758	56.664	0.048438
parrot.jpg	1024 * 1536	4606	52.101	0.17654
trees.png	200 * 200	598	48.888	0.60231

Table No. II Result Comparison

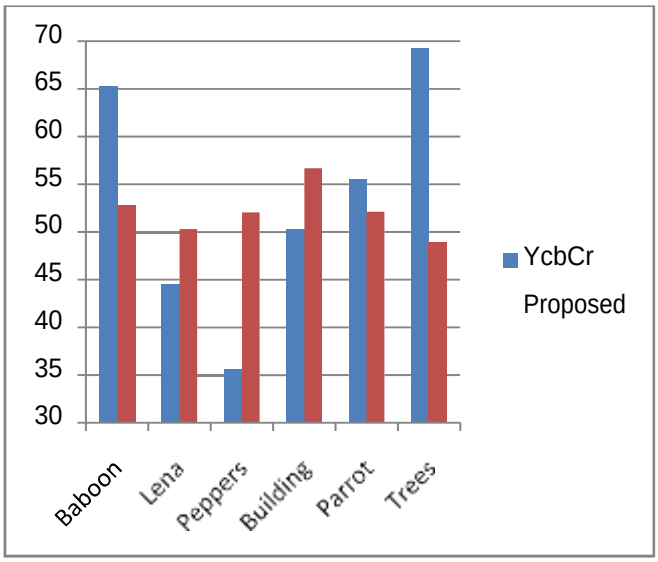
Image Name	YcbCr Method (PSNR Value)	AES & LSB –DWT Proposed Method (PSNR Value)
baboon.jfif	65.2584	52.77
lena.png	44.5215	50.286
peppers.png	35.621	52.042
building.jpg	50.2455	56.664
parrot.jpg	55.5214	52.101
trees.png	69.2352	48.888

Table No. I shows the result outcomes of the proposed system where image name, image dimension, hiding capacity, PSNR value and MSE value have been represented. Table No. II shows the result comparison with the previous methodology which is YcbCr. PSRN value should between 30 to 50 for maintain the aspect ratio and quality of the image.

Graph No. I Result Analysis



Graph No. II Result Comparison for PSNR Value



VI. CONCLUSION & FUTURE SCOPE

Here the proposed system is able to encrypt the message using AES and successfully embedded the message in a cover image using LSB algorithm at the sender's end and successfully decrypted the data and extract the secret message at the receiver's end. System pertain better PSNR value as compare to the base paper. The quality of the image has not been much affected and prediction level is bit low for illegitimate users. Here the system can be enhanced in future with more precise PSNR value which should be 30 to 50 and should not be exceeding as per the ideal system.

System may also choose another data hiding method that fewer affect the quality of the image and maintain the aspect ratio and MSE value too.

REFERENCES

[1] https://www.geeksforgeeks.org/image-steganography-in- cryptography/

[2] https://medium.com/swlh/lsb-image-steganography-using-python- 2bbbee2c69a2

[3] Shivani, Shivani & Kumar, Virendra & Batham, Saumya. (2015). A Novel Approach of Bulk Data Hiding using Text Steganography. Procedia Computer Science. 57. 10.1016/j.procs.2015.07.457.

[4] Mukherjee, Srilekha & Roy, Subhajit & Sanyal, Prof(Dr.) Goutam. (2018). Image Steganography Using Mid Position Value Technique. Procedia Computer Science. 132. 461-468. 10.1016/j.procs.2018.05.160.

[5] Al-Husainy, Mohammed. (2010). A Novel Steganography- Cryptography System. Lecture Notes in Engineering and Computer Science. 2186.

[6] J. Liu et al., "Recent Advances of Image Steganography With Generative Adversarial Networks," in IEEE Access, vol. 8, pp. 60575-60597, 2020, doi: 10.1109/ACCESS.2020.2983175.

[7] Singh, Balvinder & Kataria, Sahil & Kumar, Tarun & Shekhawat, Narpat. (2014). A Steganography Algorithm for Hiding Secret Message inside Image using Random Key. International Journal of Engineering Research and. V3 10.17577/IJERTV3IS120844.

[8] Atta, Randa & Ghanbari, Mohammed & Elnahry, Ibrahim. (2021). Advanced image steganography based on exploiting modification direction and neutrosophic set. Multimedia Tools and Applications. 80 10.1007/s11042-021-10784-5.

[9] Verma, Vikas & Poonam, & Chawla, Rishma. (2014). An enhanced Least Significant Bit steganography method using midpoint circle approach. 105-108. 10.1109/ICCSP.2014.6949808.

[10] O. Elharrouss, N. Almaadeed and S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 2020, pp. 131-135, doi: 10.1109/ICIoT48696.2020.9089566.

[11] D. L. Vasoya, V. M. Vekariya and P. P. Kotak, "Novel approach for image steganography using classification algorithm," 2018 2nd International Conference on Inventive Systems and Control (ICISC), 2018, pp. 1079-1082, doi: 10.1109/ICISC.2018.8398970.

[12] W. I. A. Almazaydeh and H. S. Sheshadri, "Image Steganography Using a Dynamic Symmetric Key," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2018, pp. 1507-1513, doi: 10.1109/ICOEI.2018.8553778.

[13] H. Al-Dmour and A. Al-Ani, "Quality optimized medical image steganography based on edge detection and hamming code," 2015 IEEE 12th International Symposium on Biomedical Imaging (ISBI), 2015, pp. 1486-1489, doi: 10.1109/ISBI.2015.7164158.

[14] S. Mshir and A. Varol, "A New Model for Creating Layer Planes Using Steganography for Text Hiding," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019, pp. 1-5, doi: 10.1109/ISDFS.2019.8757498.

[15] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," in Journal of Systems Engineering and Electronics, vol. 29, no. 3, pp. 639-649, June 2018, doi: 10.21629/JSEE.2018.03.21.

[16] A. Darbani, M. M. AlyanNezhadi and M. Forghani, "A New Steganography Method for Embedding Message in JPEG Images," 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI), 2019, pp. 617-621, doi: 10.1109/KBEI.2019.8735054.

[17] Tavoli, Reza & bakhshi, Maryam & Salehian, Fatemeh. (2016). A New Method for Text Hiding in the Image by Using LSB. International Journal of Advanced Computer Science and Applications. 7. 10.14569/IJACSA.2016.070416.

[18] Kaur, Sumeet, Savina Bansal and Rakesh Kumar Bansal. “Image steganography for securing secret data using hybrid hiding model.” Multim. Tools Appl. 80 (2021): 7749-7769.

[19] W. Lu, R. Li, L. Zeng, J. Chen, J. Huang and Y. -Q. Shi, "Binary Image Steganalysis Based on Histogram of Structuring Elements," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 9, pp. 3081-3094, Sept. 2020, doi: 10.1109/TCSVT.2019.2936028.

[20] Sharma, Vipul & Kumar, Sunny. (2013). A New Approach to Hide Text in Images Using Steganography. International Journal of Advanced Research in Computer Science. 3. 701-708.

[21] D. kumar, "Hiding Text In Color Image Using YCbCr Color Model: An Image Steganography approach," 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2019, pp. 1-5, doi: 10.1109/ICICT46931.2019.8977644.