https://www.ijsrtm.com
Vol.1 Issue 1 Dec 2021: 1-6
Published online 11 December 2021
E-ISSN: 2583-7141

International Journal of Scientific Research in Technology & Management

Image Steganography for Data Hiding using Dual Layers AES with LSB

Aditya Singh Sikarwar
Electronics & Communication Engineering
University Institute of Technology, RGPV
Bhopal, Madhya Pradesh, India
aditya78618@gmail.com

Vineeta Saxena Nigam
Electronics & Communication Engineering
University Institute of Technology, RGPV
Bhopal, Madhya Pradesh, India
vineetargpv@gmail.com

***Abstract*— The technique for hiding a message within an images cover is called image steganography. You can use an image or a text message but it's much more common and useful to hide text inside an image. To maintain national security or personal dependability in this digital age it is necessary to communicate covertly or transmit the message in a confidential manner. The system in this case is based on the Dual layer Advanced Encryption Standard (AES) and Least Significant Bit (LSB) which is also known as a hybrid technique in which two approaches can be used to improve the systems security patch. AES has been used in this work to encrypt a secret message which has subsequently been concealed in an image using LSB. In this case k-LSB has been used in accordance with the LSB methodology to effectively conceal the secret message within an image without significantly enlarging it. In order to decipher the secret message a region-based detection technique was employed to extract or unhide the hidden box. In order to conceal a message in a complex and arbitrary string and then conceal it in an image in accordance with the standards the system here employs the encryption technique.**

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

I. INTRODUCTION

Steganography means hiding information in Greek. All data is now stored as computerized media using computers and technological advancements that make steganography correspondence channels easy to use. Everyone must remain discreet. The term steganography is divided into two parts: Graphy which means writing (text) and Steganos which means secret or covered (where you need to conceal the mystery messages). Thus data security is provided by two different types of systems: steganography and cryptography. By applying cryptanalysis to the jumbled message the intruder can decipher the secret message in any other way the gatecrasher can alter the coded message. Cryptography entails transforming the message from a clear configuration to an incoherent organization but the encoded message is visible to everyone. The idea behind steganography is to hide sensitive information in any type of media including text images sounds and videos. A different record known as cover media conceals the message to be concealed. Stego is the combination of a cover document and a mystery message. The sender can send the stego to the specified goal via an organization and the collector can receive it. The information may be hidden within pictures pixels. Considering the force of shading each pixel has a whole number value. This value can be converted to a double arrangement such as bytes of 1s and 0s. It is possible to use individual bits from these bytes to hide the information. Bytes pieces can be selected at random and replaced with the privileged data.

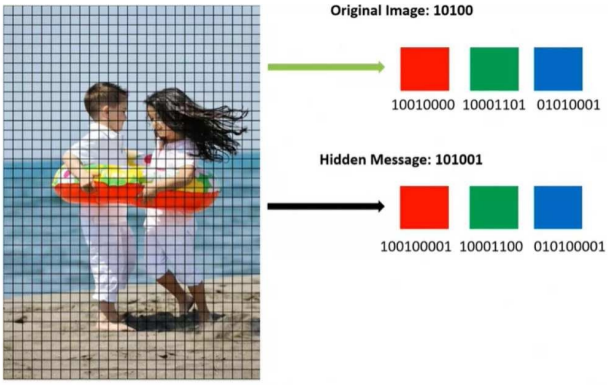

Fig. 1. Image Steganography [2]

Thus various algorithmic techniques can be used to select pixels that are used to store information. To ensure that no outsider can understand how their correspondence is being conducted image steganography takes into account two parties. In picture steganography the enigmatic message is typically hidden in the least important area of the cover

image. The tone of the first image is not altered by changing the LSB of any pixel instead it only changes by 1 bit which would be equivalent shading to unique [1]. Steganography is a collection of secret-related techniques that conceal information so it cannot be identified or seen. Numerous steganography techniques are available for hiding restricted data in images some of these techniques are much more complex than those used by outsiders. All graphical user interfaces have some free or more grounded focuses. Diverse applications require extensive privileged information to be concealed whereas distinctive applications require complete mortality of the restricted information. In this proposal the report outlines the plans to provide a basic overview of image steganography its applications and different techniques. It also adds an extra layer of security to the information in the image and the data that is hidden. By jumbling the data that is transferred within the picture and then encoding the picture with the data again using the AES computation security is made available. This method gives the data a double layer of security. Unpredictable information was immediately sent for verification and its important to note that the component is unstable because it hides the restricted information in the advanced image allowing the guaranteed person to decipher the data and validate the initial image. There are many different methods for hiding information. Its payload limit complexity visual quality and security are what determine how an unstable information-encased calculation is displayed [3].

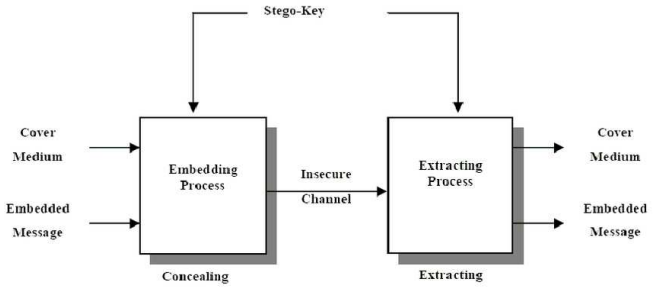

Fig. 2. General Image Steganography System [4]

The security of the framework will be increased since the hacker is unaware of the information hidden in the picture. As a result if the subject approaches consent the intruder can easily access the data. In any event since there won't be any proof of information hidden in the picture he won't have the choice to know the details. The first details and the picture will only be of interest to the verified person. The image and related information can therefore be safely conveyed in a variety of settings using this framework. For example this framework can be used in clinical science where patient reports and their results need to be sent off to the specialist in a safe manner.

II. Related Works

Singh Balvinder and others. [5] suggested a technique that demonstrates how they are hiding the enigmatic text in a cover image without causing any serious damage. Because no one has the 8-digit arbitrary key to determine which pixels have stored data and which have not this cycle makes it difficult for unapproved clients to identify the progressions in the Stego image. On the other hand if someone does notice the progressions they are unable to receive the cryptic message from the Stego image. Additionally the secret data is in a jumbled format which will secure our communication. The suggested method produces a higher PSNR value where a higher PSNR value indicates a better image quality or to put it another way less twisting in a unique image. Additionally these methods of hiding the enigmatic message within the cover image doesnt require any financial outlay. Comparing this strategy to other existing techniques it also hides more bytes of restricted information in the cover image. The goal of this system was to locate a good approach but there are a number of hackers who can change the message or extract the secret message by using modern attacking techniques. Double encryption or a slightly different strategy is necessary to protect the message or the PSNR value may not be sufficiently reflected. Randa Atta et al. An image steganography technique reliant on a sophisticated EMD and neutrosophic set was suggested by [6]. The cover image in the suggested plot is divided into blocks that are categorized as edge and non-edge blocks based on the modified neutrosophic set edge finder (MNSED). In contrast to the existing EMD-reliant steganography methods the suggested approach involves introducing the enigmatic digits into the edge and non-edge blocks using two distinct notational frameworks. Additionally it makes sure that the precise edge regions are evaluated after the enigmatic message is installed avoiding the burden of inserting overhead edge data into the cover image. According to exploratory results the suggested approach outperformed best-in-class plans in terms of installing limit and stego-image quality. The suggested approach is also strongly opposed to the comprehensive analysis. By selecting a more suitable model it is evident that the possibility of further improving the security of the suggested approach at low payloads can be investigated by adaptively selecting the squares for inserting the enigmatic message. Elharrouss Omar and others [7] suggested a method that relies on LSB coding it uses a k-LSB-based approach that hides the image using k least pieces. The secret image is translated by using an area recognition exercise to identify the squares that contain it. An image quality upgrade strategy is used to improve the image goal because it may have an impact on the Stego images objective. They compare the suggested method with some of the state-of-the-art methods to demonstrate its suitability. A. Wael Ibrahim. Almazaydeh et al. In [8] two steganography strategies were proposed: the new method with LSB +KEY and the notable strategy also known as Least Significant Bit. Using the PSNR benefits of individual computations the results implementation has been examined. Regarding the PSNR values it is observed that the LSB + KEY computation provides a better yield. .

Deepak Kumar and others. demonstrates image steganography in [9]. It is difficult for unauthorized clients to identify the stego images progressions but if someone does notice them they are unable to decipher the images enigmatic message because without the 8-digit arbitrary key no one is prepared to identify which pixel contains hidden data. employing a Least Significant Bit (LSB)-dependent YCbCr shading model. Using the least significant bit the privileged information is hidden inside the YCbCr shading space after the image has been converted from RGB to the method suggested in this paper. and which did not. The confidential information is also included. Our interaction will be safer

with a jumbled structure. The suggested method provides higher PSNR values. Return the information to RGB shading space while hiding it. The suggested approach is evaluated through a thorough analysis. Numerous cryptographic techniques are examined. A higher PSNR value indicates a better quality of the. lower twisting in a unique image as one might say. For hiding the enigmatic message within the cover image this method also doesnt require any financial outlay. This. . . . Peak Signal to Noise Ratio (PSNR) and Mean sq. Error (MSE) are used. In contrast to the RGB color model which contains luma components in addition to blue and red difference components the YCbCr color model is slightly different. The hue strategy also hides a greater number of bytes. limited details into the cover image in contrast to others. The intensity range which is 0 to 255 is comparable to RGB. Extracting a hidden message from an image based on YCbCr is a bit. currently used method. The goal of this system was to identify a good. approach but there are several ways for hackers to change the message or extract the secret message using modern attack methods. Double encryption or a slightly different strategy is needed to protect the message or the PSNR value shouldnt be sufficiently reflected. Randa Atta et al. proposed an image steganography method that relies on a neutrosophic set and advanced EMD. Depending on the modified neutrosophic set edge finder (MNSED) the cover image is divided into blocks in the suggested plot which are then categorized as edge and non-edge blocks. Different. YCbCr has a slightly higher luminance than RGB which makes it more difficult to predict due to the natural colors. RGB pictures are unpredictable and rarely show the changed area. Enhancing the encryptions security and data hiding strategy is preferable to altering the images color model. A PSNR value of 50 to 55 is ideal for a system because it preserves both the image quality and the attacker prediction rate because it has little effect on the image and appears to be authentic.

III. Proposed Work

The proposed work is based on two distinct methods. The first is AES which has been used to encrypt the message encryption calculation but has not yet been subject to such provisos when the message is being embedded in an image. The second is LSB which has been employed to conceal the. message within a picture that is unpredictable at the moment intruders end.

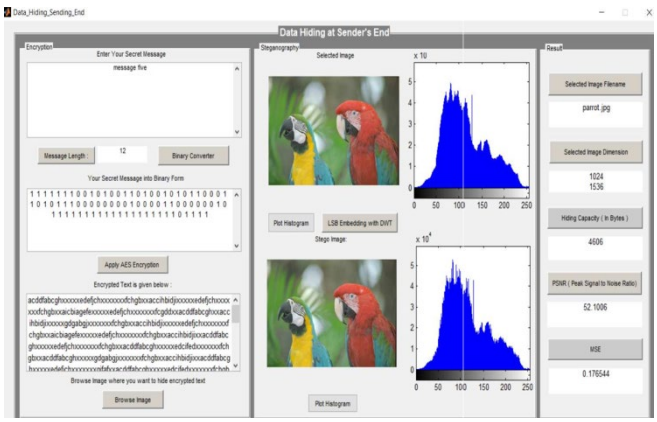

Fig. 3. Sender's End (Proposed)

A good PSNR and MSE value that represent the quality of the image that hasn't been significantly altered and that maintains the aspect ratio are successfully achieved by the proposed system. We use both steganography and cryptography in our work. In order to increase data security we combine both methods. There are two layers in the suggested system specifically. Encryption/Decryption Layer and Steganography Layer.

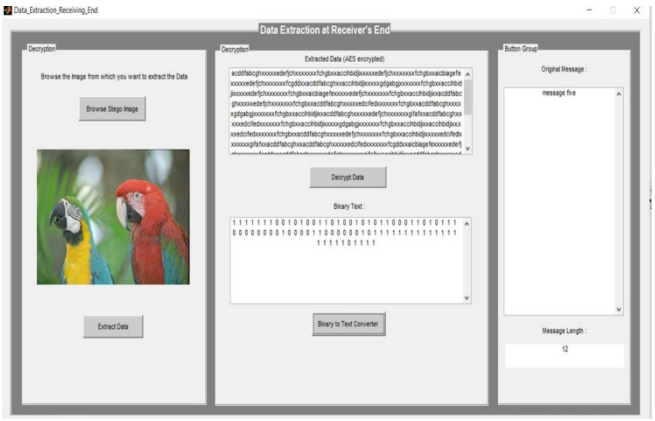

Fig. 4. Receiver's End (Proposed)

A. AES Encryption

Rijindael also known as the Advanced Encryption Standard (AES) is used to retrieve data. These days AES is a widely used symmetric square code that has been extensively studied. For this reason symmetric key encryption or AES uses a key length of 128 bits. AES computations characteristics include high security numerical sufficiency defense against all known attacks high encryption speed overall sovereignty free use and reasonableness across a broad range of hardware and programming. While escape clauses are present in the calculations for DES and 3DES encryption they have not yet been included in the AES calculation.

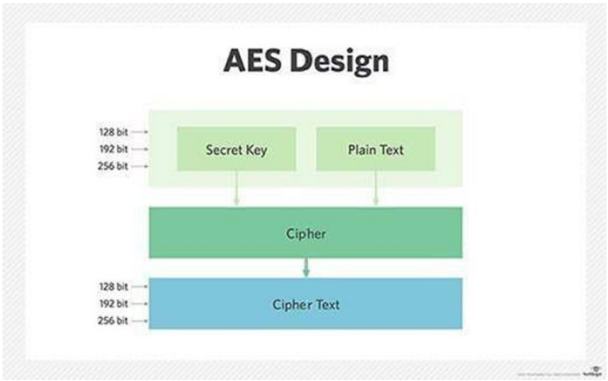

Fig. 5. AES Encryption

B. LSB

The acronym for Least Significant Bit is LSB. The idea behind installing an LSB is that if we alter the final component it will add value. Pixel there wont be any significant changes. shading. For example 0 is dark. Changing the value to 1 wont significantly alter the distinction because it is still dark just a lighter shade. Depending on the parallel number it can be the piece that is farther to the left or the piece that is farther to the right. design. if the LSB is referred to as little-endian. . If. The design is on the right and the LSB is on the left. Large Endian is the classification for engineering. In little-endian

engineering for example the LSB of the double number 00000001 is 1.

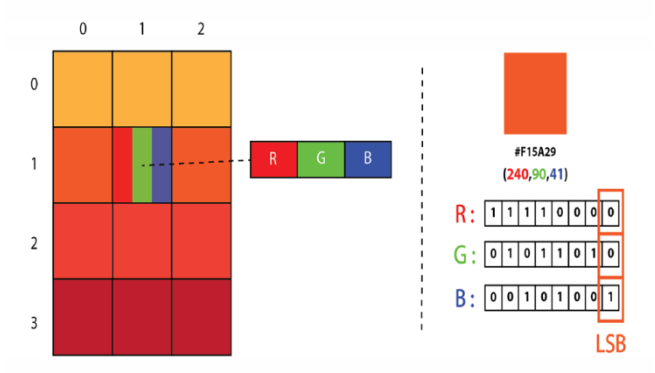

Fig. 6. LSB Steganography

C. Flow Chart

According to the flow diagram shown in fig 7. First a secret message must be written in order to encrypt it. After that it must be converted into binary code and after that AES encryption is started. After the message has been successfully encrypted the system looks for a crypto image which will be used as the input image or cover image. The system then determines whether the image is compatible with the message and whether it can be embedded with it.

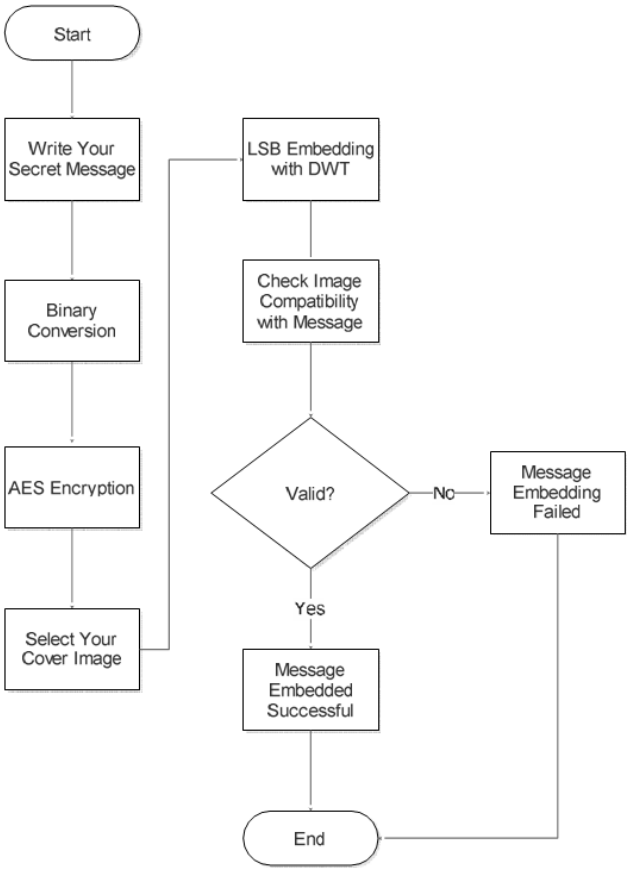

Fig. 7. Sender's End (Flow Chart)

This indicates that the system intended it to do so. In order to determine the resolution of the picture whether the image is too high or too low or whether it has a valid extension. Once the system determines that the image is appropriate it can be hidden in a cover image that the sender has chosen. The message can be sent to the rightful recipient after it has been indulged or concealed with the cover image. There it can be further decrypted unhidden and read with a high degree of validity. The recipient must first choose the target Stego image. The system will then determine whether the message is present in the image and if it is extract the encrypted message. Once the encrypted message has been located the system can successfully decrypt it. The message will then be converted into binary code and after the binary code has been extracted the system will convert the binary image to text which must be the secret message that was sent by the sender. The system has been trained to secure a message with two levels of security with what is known as a hybrid method also called a compound method which hides the message in an image and secures a secret message without significantly altering the PSNR value. The proportion between a signals most extreme possible value and the ability to distort noise that affects how it is portrayed is known as the Peak Signal to Noise Ratio (PSNR).

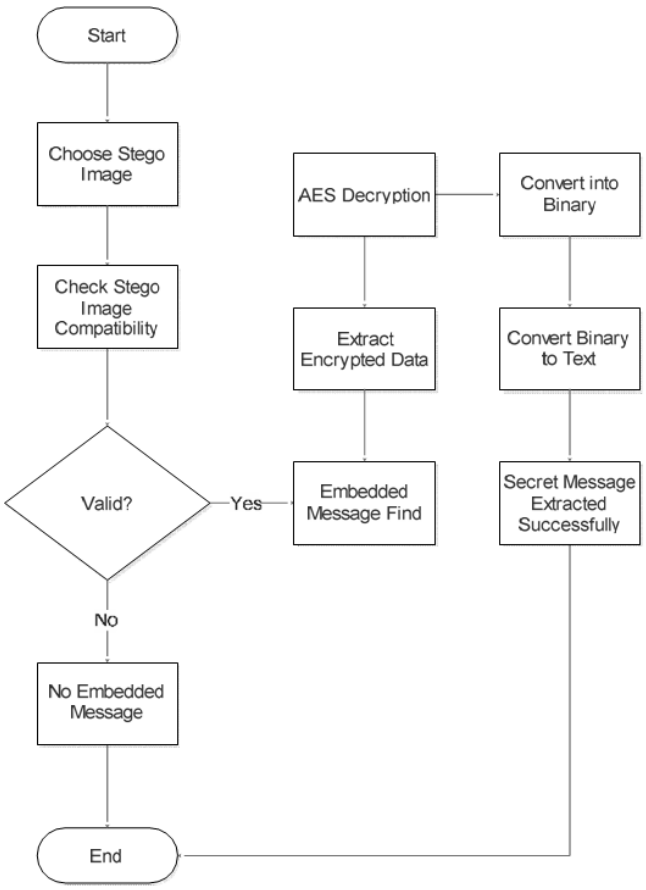

Fig. 8. Receiver's End (Flow Chart)

D. Dual Layer AES & LSB 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;

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

Encrypted message {
76A2F63499FFDD4B39654A6C41505228 }

Step 5: Select an image for LSB steganography

if $M_i < 1$ **then**

No Message for Embedding;

end else

Embedded the secret message in target image;

end else

end if

Step 6: Send stego image to the receiver

Step 7: End

E. Dual Layer AES & LSB Algorithm (Receiver)

INPUT: A ← Stego Image as two dimensional matrix andSecret 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;

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

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

IV. 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 50 to 55 for maintain the aspect ratio and quality of the image. Due to the remarkably broad dynamic range of many signals (the ratio of the largest to the smallest possible gains of a variable amount) the PSNR is typically expressed as far as the logarithmic decibel scale. Improving the visual aspects of an advanced image or enhancing it can be subjective. A technique that produces a picture of superior quality may vary from person to person. Building up quantitative and observational measures to examine the effects of image enhancement for the computations on picture quality is therefore crucial. Diverse image improvement calculations can be purposefully measured using similar text image types to determine whether a particular calculation produces superior results. The peak signal to noise ratio is the measurement under examination. It can more accurately assume that a calculation is superior if it can demonstrate that a calculation or series of calculations can improve a degraded image or upgrade a degraded image.

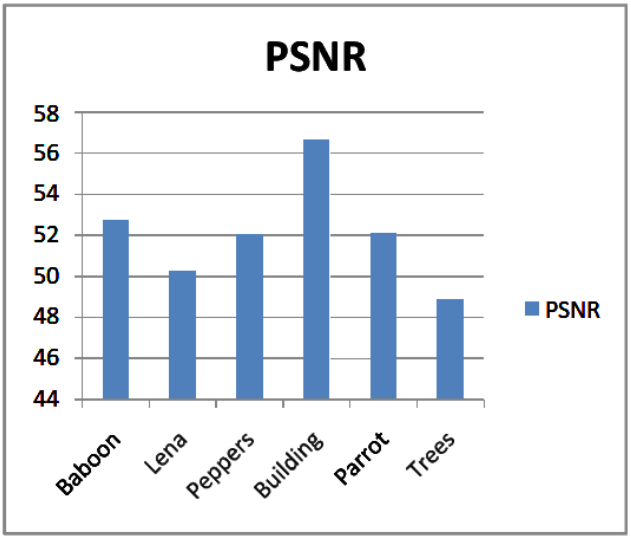

Fig. 9. Result Analysis

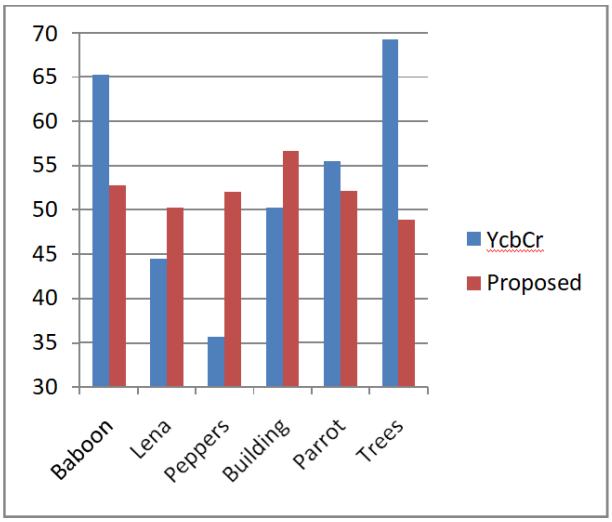

Fig. 10. Result Comparison for PSNR Value

V. Conclusion

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 50 to 55 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] 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.

[2] https://3jxr3314n6nx3lpucsnla08e-wpengine.netdna-ssl.com/wp-content/uploads/2020/05/Image-Steganography-Kids-at-the-

[3] Beach.png

[4] Animesh Kumar, Deepak Idnani, Kaushal soni, Nitin Taneja, Rounak Shrivastava, Steganography Using AES Algorithm, 2019 IJRAR June 2019, Volume 6, Issue 2.

[5] Bandyopadhyay, Samir & Paul, Tuhin & Avishek, Raychoudhury. (2010). A Novel Steganographic Technique Based on 3D-DCT Approach. Computer and Information Science. 3. 10.5539/cis.v3n4p229.

[6] Balvinder Singh et al. , "A Steganography Algorithm for Hiding Secret Message inside Image using Random Key", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERT, Vol. 3 Issue 12, December-2014.

[7] 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.

[8] 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.

[9] Bloisi, Domenico Daniele, and Luca Iocchi. "Image based steganography and cryptography." VISAPP (1). 2007.

[10] Nemati, Hamid. "Information Security and Ethics: Concepts, Methodologies." (2008).

[11] El-Emam, Nameer N. "Hiding a large amount of data with high security using steganography algorithm." Journal of Computer Science 3.4 (2007): 223-232.

[12] M. Warkentin, M.B. Schmidt, E. Bekkering, Steganography and steganalysis, Premier reference Source–Intellectual Property Protection for Multimedia Information technology, Chapter XIX, 2008, pp. 374- 380.

[13] Chen, Po-Yueh, and Wei-En Wu. "A modified side match scheme for image steganography." International Journal of Applied Science and Engineering 7.1 (2009): 53-60.

[14] Wu, Da-Chun, and Wen-Hsiang Tsai. "A steganographic method for images by pixel-value differencing." Pattern Recognition Letters 24.9-10 (2003): 1613-1626.

[15] Kunal Ashok Shinde , Omkar Rajendra Gandhi , Somanath Rohidas Langute, Nagaraj V. Dharwadkar , "ADAPTIVE IMAGE STEGANOGRAPHY USING PIXEL INTENSITY DIFFERENCE", IJIERT - International Journal of Innovations in Engineering Research and Technology, ICCCES-16, ISSN : 2394-3696, Page No.

[16] Muhammad, Khan, et al. "A novel image steganographic approach for hiding text in color images using HSI color model." arXiv preprint arXiv:1503.00388 (2015).

[17] Ibraheem, Noor A., et al. "Understanding color models: a review." ARPN Journal of science and technology 2.3 (2012): 265-275.

[18] Celik, Turgay, and Hasan Demirel. "Fire detection in video sequences using a generic color model." Fire Safety Journal 44.2 (2009): 147-158.

[19] Huang, X. Q., et al. "Study on color image quality evaluation by MSE and PSNR based on color difference." Acta Photonica Sinica 36 (2007): 295-298.

[20] Hore, Alain, and Djemel Ziou. "Image quality metrics: PSNR vs. SSIM." 2010 20th International Conference on Pattern Recognition. IEEE, 2010. Huynh-Thu, Quan, and Mohammed Ghanbari. "Scope of validity of PSNR in image/video quality assessment." Electronics letters 44.13 (2008): 800-801.