A Modified Approach for Data Hiding Based On Encryption and Pixel Neighbour Interpolation

Antampreet Kaur[1], Dr. Kanwalvir Singh Dhindsa[2]
[1]*M.Tech Research Scholar, CSE Deptt., Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib*
[2]*Professor & Head (CSE Deptt.), Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib*

Abstract-Data hiding is the process that has been used for secure transmission of secret information by using cover medium. In the process of steganography data hiding has been done on the basis of mean interpolation method and using the artificial intelligence approach so that data can be embedded using the pixels that provide minimum distortion after embedding of data. In this process mathematical data embedding operations have been implemented on the image so that using the log value of the secret information data has been embedded to the pixel. This causes low intensity changes to the image that occurs to minimum mean square error after process of embedding information. To enhance the security of the data embedding modified AES approach has been implemented that use highest common factor so that low computation complexity of the encryption algorithm, takes place and data can be embedded in encrypted manner. This is the reversible process so that at the receiver end secret information as well as cover information can be extracted.

Keywords: *Steganography, AES, Interpolation, BFO PSNR and MSE.*

I. INTRODUCTION

1.1 Steganography

Steganography is the process that has been used in digital information transmitting in a secret manner so that description about the secret information can't be availed during transmission. Ancient time secret information has been transmitted by using the individual credentials for hiding secret information.

In picture steganography the data is shrouded only in pictures. The thought and practice of concealing data has a long history. Steganography varies from cryptography as in where cryptography concentrates on keeping the substance of a message mystery, Steganography concentrates on keeping the presence of a message mystery. Steganography and cryptography are both approaches to secure data from undesirable gatherings yet not one or the other innovation alone is flawless and can be bargained. Once the vicinity of shrouded data is uncovered or even suspected, the motivation behind steganography is part of the way crushed.

1.2 Different types of Steganography

1.2.1 Text Steganography

Text Steganography is the approach that has been used so that secret information can be embedded to text content and transmitted to receiver end. In this process of data hiding secret information has been embedded to nth character of the text lines so that secret information can be extracted without any issue at receiver end. Due to advancements in the technology importance of the text Steganography has been reduced and all operations have been done in digital format.

1.2.2 Image Steganography

Images are used as the popular cover objects for steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key. The resulting stego image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of steno image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message

1.2.3 Audio Steganography

Audio Steganography has been done so that information can be easily transmitted through audio signals in secure manner. In this process information has been embedded on the basis of addition of more louder signal than available in the audio file that are not auditable to human ear.

1.2.4 Protocol Steganography

In the process of protocol steganography various approaches have been used so that data can be embedded with that network protocols that are transmission control protocol (TCP) and internet protocol (IP). Information has been embedded to the header of the protocols and transmitted over the network. Sometimes non-usable slots of protocols have been used so that information can be embedded and transmitted through communication channel.

1.2.5 Video Steganography

Video Steganography is the field to transmit large secret information in a secure manner by hiding content behind the fames of the video file. Due to its size and memory

prerequisites information can be easily embed and transmit over transmission media. The ideas of cryptography and steganography can be used for embedding secret information to cover video that provides more security and data integrity.

1.3 Applications of Steganography

There are various areas where steganography can be applied, some examples are:

- Steganography has been a best solution to transmit secure information in such a manner so that information that is secret like news can be transmitted without any intercepting and tracing between the transmission channels.
- Steganography can be used for as an alternative to watermarking process. In the process of watermarking cover source has been extended by embedding extra information for the purpose of ownership. On the basis of purpose of ownership, the content that has been embedded in watermarking creates issues to cover media that changes integrity and quality of cover media that has been used for data embedding process. So, to avoid this issue in watermarking Steganography can be used so that information can easily embedded to the data and used for transmission over transmission channel.
- Steganography can be used in hybrid manner for information security to provide hidden exchange. Government has been involved in two various types of secret communication that deals with national security concerns and with civil concerns. Digital Steganography can be used in both types of communication so that reliable communication can be done and used for data security and embedding. In business purpose for trading and new product launching steganography can be used so secure transmission of data.
- In steganography data can be easily embedded at a particular location so that information can be different information can be revel for different purposes at different places. For example, in cover media banking information as well as military related information has been hided at different locations. At receiver end if banking information has been reveled from the cover data then that has no information about the military information embedded to cover media. In today marketing scenario E-commerce is largest area for business marketing that has various user that access their information on the basis of username and password basis. There is no such method is available that can be used for integrity and authenticity of the user that a user who is accessing the information is actual user that is genuine card holder. In this process steganography plays important role that combines fingerprint scanned images data with the session id's of user so that secure access can be used and information and user authentication will not harm.
- Steganography is major useful for transmission of sensitive information over the channel so that information can't be traced and intercepted. Cryptography had been used for transmission of secret information, but changes in cover media has a drawback that represents that any sensitive information has been embedded to the cover media. Steganography allows the user to transmit information without representing any information has been embedded to the cover media. Steganography can be easily done to content that has been transmitted through E-mail messages.

II. REVIEW OF LITERATURE

Kaur and Soni[1] discussed about processing of data transmission in the network communication, various methods of data transmission have been used. Using wired connection through data transmission based on co-axial cables is the best method, but having slow rate of data transmission. Optic fiber is the latest technology that can be used for data transmission with high rate of data transmission so that better data delivery and secure transmission of information can be achieved. In this paper data transmission from source to destination has been done on the basis of encryption strategy. Data has been encrypted and then transmitted by using optics fiber cables that have low data leakage due to prone to various attacks during data transmission. In this paper various approaches of data encryption process have been analyzed and implemented for the process of data encryption in the sake of security. AES, RSA and DES were the approaches that have been simulated in this paper and their results have been compared so that optimum approaches can be extracted for the process of data encryption and secure transmission of data.

Islam *et al.*[2]discussed about the approach that has been used for process of data hiding using the cover medium so that information can be transmitted in secure manner from source to destination. In this paper various constraints and issues of the data hiding that are PSNR, data capacity has been improved using the best approach based on most significant bits difference for data hiding. In this process of data hiding the difference between the most significant bits that are located at 5^{th} and 6^{th} places in the binary conversion of the cover image pixel value. The computed difference has been matched with the secret information value if that is similar no change has been made to 5^{th} bit else 5^{th} bit has been changed and after that cover image has been formed after processing for all the pixels available in the cover image. On the basis of pixel differencing approach better PSNR value and data capacity has been achieved.

Prashanti et al. [3]used combination of data embedding and data encryption for better security and secrecy of the critical information. In this paper an approach has been used for the process data encryption that is public key based encryption

approach that has been used based key sharing between receiver and sender. After the process of encryption encoded information has been embedded to cover images pixels using least significant bits based data embedding approach so that least bits of the cover image pixel have been XOR with the secret information bits and the new pixel value has been formed using logical truth values. The information has been transmitted and extracted at receiver end. The information has been decoded using the secret public key that has been available at receiver end for security sake. This approach validated the process of data hiding but the major issue in this approach causes to low data capacity for data hiding that must be improved in latest research.

Sharma and Sejwar[4]states that information sharing and its integrity is the vast area of research in digital communication. All the information that has been used in recent actions has been stored and transmission using digital communication channels. Due advancement in the data communication technology intruders are increased that captured important information for illegal use purposes. In this paper author has designed an improved approach for secure and authenticate information sharing approach that is based on the QR codes based validation system. In this paper a three layers based security approach has been developed that is based on QR code scanning based process. At the receiver end a code has been transmitted and the user scan the code and after scanning a secret key has been given as input that has been matched with stored information in the QR code. After this process data can be extracted and receiver end.

Bailey and Curran[5]proposed various use cases for data hiding has been discussed that can be used for color image pixelsbased steganography. In the process of pixel based data hiding primary color based pixels have been used for data embedding process. In the process Red, Green and Blue that are primary colors in the RGB color space model of a digital image. In this phase on data embedding three different models have been discussed for the process of data embedding. On the basis of these process of data embedding R, G and B based pixels has been used for extraction of bits for data embedding so that based on these bots data can be embedded and transmitter using transmission channel. Second approach is that that can be used combination of two color pixel values that is based on RG, GB, RB based pixel detection approach. On the basis of these model 9 uses can be developed that can be used for data embedding process. In the third phase single RGB based component can be used for embedding of secret information behind the cover media pixels. The major drawback of the third model is data capacity has been reduced by 40% for secret information embedding. In this process that data embedded has been distributed in the all content of the image that is not an easy process to extract without knowledge of pixels in which data has been embedded.

Zhu et al. [6]discussed robust data hiding approach that can be used for communication over the lossy channels. In the previous data hiding information approaches data has been transmitted over the network using lossless channels. On the basis of interpolation process scaling of the image has been done and the reverse process has been done at the receiver end so that cover image and secret information can be extracted at the receiver end. Reverse interpolation process is most reliable approach from the attacks because of robust information about the pixels that has been used for secret information hiding process. On the basis of this process image has been divided into various sub-blocks that has been used for addition of new pixels based of neighbor pixel values and the scaling of the cover image has been done at this level of interpolation. After this the various mathematical operations have been implemented on the interpolated pixels so that secret information can be embedded to the pixels that can be extracted art receiver and after removal of the interpolated pixels original cover image can be verified. This approach has been verified and implemented in many phases and outperforms to existing approaches in the process of interpolation based data hiding.

Hussain and Hussain[6]described steganography as the art of concealing a message signal to have signal, with no bending in the facilitated sign. Utilizing steganography, data can be covered up in facilitated transporter, for example, pictures, features, and sounds records, content documents, and information transmission. In picture steganography, to enhance the limit of concealed information into facilitated picture without creating any factually noteworthy adjustment has a real concern. Numerous novel information concealing strategy taking into account Least Significant Bits (LSB) and Pixel Value Differencing (PVD) to build the concealing limit have been proposed with subtle quality. In this paper we have enhanced the Modified Kekre's Algorithm (MKA) which is taking into account LSB system. The enhanced plan builds the implanting limit while holding the great nature of stego-picture (convey concealed information) as good as MKA. Trial results demonstrate that the enhanced plan outflank the first near plan particularly in limit of concealed information bits.

III. METHODOLOGY

In the process of data hiding various image pixels have been used so that data can be easily embedded behind the cover image pixels. On the basis of this data hiding process secret information has been embedded to the cover image pixels using various bits of the cover image pixel value. In the process of data hiding the basic concept is that minimum distortion must be occurred in the image and maximum data can be embedded behind the cover media. On the basis of this principal a method has been developed that provide minimum distortion and maximum data capacity of data embedding so that information can be embedded to the image pixels.

These approaches have major drawback of minimum data capacity and complexity in data hiding process.

In this process mean neighbour interpolation has been used for the process of data embedding so that based on neighbour pixel values new interpolated pixels can be generated that can be used for data attachment based on log value of the secret information. Column based pixel difference has been computed by using the cover image pixels and these difference values have been used for computation of no. of bits that can be embedded to the cover image pixels.

- **Modified Neighbour mean interpolation**

In the process of modified neighbor interpolation bacterial forging optimization has been used that works on the principal of fitness function so the best region from the image can be extracted that can be used for interpolation and data embedding phase in the process of data embedding. Based on neighbour pixel value new average pixel value has been computed that has been used for the process of data embedding and these interpolated formation of pixel at receiver end has been undergoes reverse interpolation so that original image can extracted at receiver end.

In the proposed work data hiding has been done on the basis of interpolation process. In this process image of 512* 512 has been used as original image that has been reduced to size of 256*256 using image toolbox in MATLAB. After this process the image that has been generated undergoes the process of interpolation so that new proximate pixels can be easily generated. On the basis of pixel generation new rows and columns have been inserted in the blocks of the images and new pixel values have been estimated using different interpolation equation. The whole process of interpolation has been illustrated below through an example.

An example to explain the proposed modified neighbour mean interpolation method for scaling the original image of size 3×3 is shown in figure 4.1. Initially, in the proposed work one blank row and one column has been added between two adjacent rows and columns, respectively, as shown in Figure 4.2 and assign original pixel values to the old locations as follows: T(0, 0) = I(0, 0), T(0, 2) = I(0, 2), T(0,4) = I(0, 4), T(2, 0) = I(2, 0), T(2, 2) = I(2, 2), T(2, 4) = I(2, 4), T(4, 0) = I(4, 0), T(4, 2) =I(4, 2), and T(4, 4) = I(4, 4). It then calculates the center pixel values of T(1, 1), T(1, 3), T(3,1), and T(3, 3) with the help of original image pixels. It is basically the average value of all the surrounding pixels. After calculating the center pixel values, the value of the other pixels like T(0, 1), T(1, 0), T(0, 3), T(1, 2), T(1, 4), T(2,1), T(3, 0), T(2, 3), T(3, 2), T(3,4), T(4, 1), and T(4, 3) are calculated i.e., 28, 32, 31, 28, 26, 35, 52, 25, 32, 46, 49, and 52,respectively. The scaled up pixel values of the last row and column are computed with the help of the pixel values of the previous rows and columns, respectively as shown in figure 4.3 This process can be repeated for the entire image to get the final scaled up image.

I(0,0)=19	I(0,1)=35	I(0,2)=29
I(1,0)=46	I(1,1)=21	I(1,2)=23
I(2,0)=62	I(2,1)=39	I(2,2)=72

Fig 4.1 original image of size 3×3

The figure 4.1 represents original image block that has been used for interpolation process so that new pixels can be easily generated through interpolation. On the basis of interpolation, a new row and column has been added to the all the adjacent pixels that are available in the original image and the values that are available ate original image block has been located at new places that has been represented in figure 4.2

I(0,0)=19		I(0,2)=35		I(0,4)=29
I(2,0)=46		I(2,2)=21		I(2,4)=23
I(4,0)=62		I(4,2)=39		I(4,4)=72

Fig 4.2 interpolated image of size 5×5

All the values from the original block has been generated so that new block can be formed that has been illustrated below. O (i,j) represents original image pixel value that has been replaced with C (i,j) so that cover image block can be generated.

$$\begin{cases} T(0,0) = I(0,0) \\ T(0,2) = I(0,2) \\ T(0,4) = I(0,4) \\ T(2,0) = I(2,0) \\ T(2,2) = I(2,2) \\ T(2,4) = I(2,4) \\ T(4,0) = I(4,0) \\ T(4,2) = I(4,2) \\ T(4,4) = I(4,4) \end{cases} \quad (1)$$

$$\begin{cases} T(1,1) = \frac{I(0,0)+I(0,2)+I(2,0)+I(2,2)}{4}; \\ T(1,3) = \frac{I(0,2)+I(0,4)+I(2,2)+I(2,4)}{4}; \\ T(3,1) = \frac{I(2,0)+I(2,2)+I(4,0)+I(4,2)}{4}; \\ T(3,3) = \frac{I(2,2)+I(2,4)+I(4,2)+I(4,4)}{4}; \end{cases} \quad (2)$$

$$\begin{cases} T(0,1) = \dfrac{I(0,0)*2 + I(0,2)*2 + T(1,1)}{5}; \\ T(1,0) = \dfrac{I(0,0)*2 + I(2,0)*2 + T(1,1)}{5}; \\ T(0,3) = \dfrac{I(0,0)*2 + I(0,4)*2 + T(1,3)}{5}; \\ T(1,2) = \dfrac{I(0,2)*2 + I(2,2)*2 + T(1,3)}{5}; \\ T(1,4) = \dfrac{I(0,4)*2 + I(2,4)*2 + T(1,3)}{5}; \\ T(2,1) = \dfrac{I(2,0)*2 + I(2,2)*2 + T(3,1)}{5}; \\ T(3,0) = \dfrac{I(2,0)*2 + I(4,0)*2 + T(3,1)}{5}; \\ T(2,3) = \dfrac{I(2,2)*2 + I(2,4)*2 + T(3,3)}{5}; \\ T(3,2) = \dfrac{I(2,2)*2 + I(2,4)*2 + T(3,3)}{5}; \\ T(3,4) = \dfrac{I(2,4)*2 + I(4,4)*2 + T(3,3)}{5}; \\ T(4,1) = \dfrac{I(4,0)*2 + I(4,2)*2 + I(3,1)}{5}; \\ T(4,3) = \dfrac{I(4,2)*2 + I(4,4)*2 + I(3,3)}{5}; \end{cases} \quad (3)$$

On the basis of above defined equations (1), (2) and (3) a cover image block has been generated so that data can be easily embedded behind these blocks.

T(0,0)=19	28	T(0,2)=35	31	T(0,4)=29
32	30	28	27	26
T(2,0)=46	35	T(2,2)=21	25	T(2,4)=23
52	42	32	39	46
T(4,0)=62	49	T(4,2)=39	52	T(4,4)=72

Figure 4.3 cover image block of size 5×5 with proximate pixels

- On the basis of interpolation process the data has been embedded behind the cover image using embedding process that is based on pixel differencing approach. On the basis of pixel difference number of bits has been computed that can be used for data embedding.
- **Embedding Phase**

After the process of interpolation cover media has been generated so that data can be embedded behind the cover pixels. To do so image has been sub-divided into sub-groups of 2X2.

After division of the image in non-overlapping blocks various steps have been carried out in repetition manner so that data can be embedded with cover image pixels.

Input: Cover image I_c of size N*2 X M*2 where N: height and M: Width

Output: Stego Image S_m

a. Divide cover image I_c to non-overlapping block of 2by2.

b. Compute absolute difference values such that $D_{(i,1)} = |T_i(1,1) - T_i(0,1)|$ and $D_{(i,2)} = |T_i(1,1) - T_i(1,0)|$

c. On the basis of difference value embedding bits have been computed using upper bound and lower bound limits. Such that $U_{(i,1)}, L_{(i,1)}$ and $U_{(i,2)}, L_{(i,2)}$ are the upper and lower limits for difference $D_{(i,1)}$ and $D_{(i,2)}$respectively. By using these limits n has been computed that is the number of bits that can be embedded. $n_{(i,1)} = \log_2(U_{(i,1)} - L_{(i,1)} + 1)$ and $n_{(i,2)} = \log_2(U_{(i,2)} - L_{(i,2)} + 1)$.

d. Compute two different values using lower limits and secret bits integer value that has been generated on the basis of conversion from bits to integer value S. where $d_{(i,1)} = |L_{(i,1)} + S_{(i,1)}|$ and $d_{(i,2)} = |L_{(i,2)} + S_{(i,2)}|$. $S_{(i,1)}$ and $S_{(i,2)}$ are the integer values w.r.t $n_{(i,1)}$ and $n_{(i,2)}$ respectively.

e. For generation of new pixel value that contain secret data embedded with the cover image pixel values using $m_{(i,1)} = |D_{(i,1)} - d_{(i,1)}|$ and$m_{(i,2)} = |D_{(i,2)} - d_{(i,2)}|$. On the basis of these values new pixel values can be generated so that stego image can be formed.

$$(T'_i(1,1), T(0,1)) = \begin{cases} (T_i(1,1) - \left\lceil \frac{m_{(i,1)}}{2} \right\rceil, T_i(0,1) + \left\lfloor \frac{m_{(i,1)}}{2} \right\rfloor) \ ford_{(i,1)} = 1 \\ (T_i(1,1) - \left\lfloor \frac{m_{(i,1)}}{2} \right\rfloor, T_i(0,1) + \left\lfloor \frac{m_{(i,1)}}{2} \right\rfloor) \ ford_{(i,1)} = 0 \end{cases} \quad (4)$$

$$(T'_i(1,1), T'_i(1,0)) = \begin{cases} (T_i(1,1) - \left\lceil \frac{m_{(i,1)}}{2} \right\rceil, T_i(1,0) + \left\lfloor \frac{m_{(i,1)}}{2} \right\rfloor + m_{(i,2)}) \ ford_{(i,2)} = 1 \\ (T_i(1,1) - \left\lfloor \frac{m_{(i,1)}}{2} \right\rfloor, T_i(1,0) + \left\lfloor \frac{m_{(i,1)}}{2} \right\rfloor + m_{(i,2)}) \ ford_{(i,2)} = 0 \end{cases} \quad (5)$$

f. On the basis of equation (4) and (5) value of $T'_i(1,1)$ has been computed that must be similar so that values can be generated.

g. Repeat these steps do that secret data can be embedded behind the cover image so that stego image S_m is generated.

By using above defined methodology secret data has been embedded so that stego image has been formed. Stego image has been transmitted to the receiver end so that data can be extracted at receiver end.

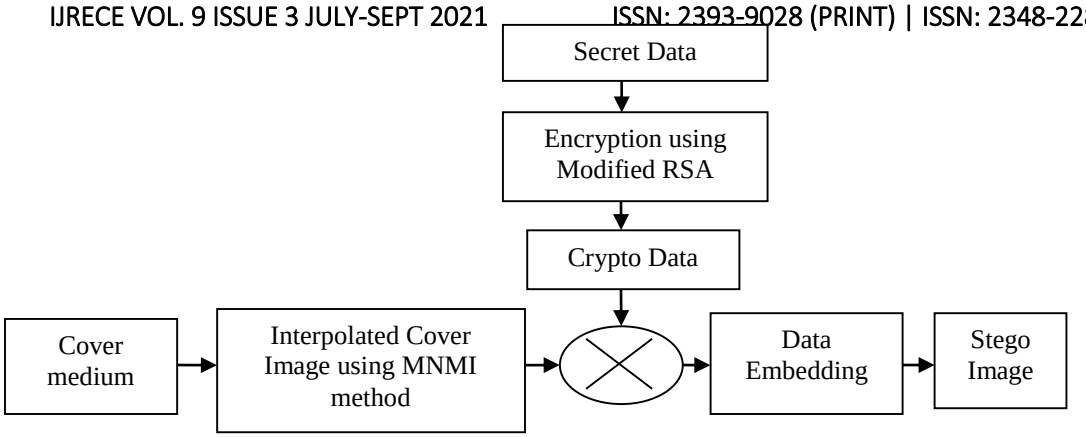

Fig 4.4 Block diagram of crypto data embedding using proposed method

In this example, firstly, secret data is encrypted using Modified RSA algorithm. Then, hide crypto data bit stream $(10010101010)_2$ into the modified cover image using modified interpolation method. For embedding this encrypted data bits stream, divided the cover medium into 1×4 non-overlapping blocks (column wise).The pixels are represented by$(1,1) = 72,(2,1) = 81,(3,1) = 125,(4,1) =$ 179 Then Absolute Difference (AD) is calculated $AD_{(i,1)} = |179 - 125|= 54$ and$AD_{(i,2)} = |179 - 81| = 98$. After that, the number of embedding crypto data bits are calculated using $nb_{(i,1)} = log_2|63\text{-}32+1|=5$ and $nb_{(i,2)} = log_2|127\text{-}64+1|= 6$ with the assist of lower bound and upper bound of range table. Furthermore, evaluate the New Difference (ND) as $ND_{(i,1)} = |32 + 18|= 50$ and $ND_{(i,2)} = |64 + 42| = 106$ where 32 and 64 are lower bound of range table. In order to get the new pixel values calculates $k_{(i,1)} = |50 - 54| = 4$ and$k_{(i,2)} = |106 - 98| = 8$. Then, evaluate the new pixel pair values using $\left(I_i^{'}(4,1), I_i^{'}(3,1)\right) = (179 - 2, 125 + 2), \left(I_i^{'}(4,1), I_i^{'}(2,1)\right)$ $=(179 - 2, 81 - 2 + 8)$. In this way, stego block of processed image is attained such as pixel values of processed image are as$(1,1) = 72, (2,1) = 87, (3,1) = 127, (4,1) = 177.$ This process is repetitive until all the 1×4 non-overlapping blocks are not processed and crypto data is not embed into the cover image.

IV. RESULTS

In the process of image steganography data hiding has been done on the basis of bacterial forging optimization with interpolation that has been hybrid with modified AES encryption approach.

(a) Mean Square Error (MSE)

The MSE is measurement of the cumulative squared error between original image and processed image. The mathematical formula for calculating the MSE is given as [42]:

$$MSE = \frac{1}{X \times Y}\sum_{i=1}^{X}\sum_{j=1}^{Y}(L(i,j) - M(i,j))^2 (4)$$

Where $L(i,j)$ and $M(i,j)$ are the i^{th} row and j^{th} column pixels of cover image L and stego image M, and $X \times Y$ signify the size of the cover image.

(b) Peak Signal to Noise Ratio (PSNR)

The PSNR is used to measure the quality of image. It is the ratio between square of maximum pixel value of the image and MSE. The mathematical formula for calculating the PSNR is given as [42]: $\text{PSNR} = 10\log_{10}\left(\frac{255^2}{\text{MSE}}\right)$ (5)

(c) Structure Similarity Index (SSIM)

The Structure Similarity Index is the ratio of original image and processed image. If the value of SSIM is one then it means there is no difference between processed and cover image otherwise both are totally different. From Table 4.1, it has been concluded that the Structure Similarity Index Matching (SSIM) of the original image and processed image is almost close to 1 using equation 6

$$SSIM = \frac{(2\mu_L\mu_M + C1)(2\sigma_{LM} + C2)}{(\mu_L^2 + \mu_M^2 + C1)(\mu_L^2 + \mu_M^2 + C1)} (6)$$

Where μ_L represent the mean of original image and μ_M represent the mean of stego image. μ_L^2 Represent the variance of original image L and μ_M^2 represent the variances of stego image M. σ_{LM} is the covariance of two images and $C1, C2$ are the two variables.

(d) Entropy

It measures the randomness associated with a random variable in the image. The mathematical formula for calculating the entropy is given as

$$Entropy = \sum_i P_j \log_2 P_j (7)$$

P_i is the probability.

4. Experimental Results

Experimental results achieved the better values of Image Quality Measuring (IQM). The performance evaluation of the proposed method is measured using a variety of Image Quality measures (IQM) like MSE, Entropy, PSNR, SSIM and Correlation are summaries in Table 5.1. PSNR is very critical parameter for measuring the image quality. PSNR more than 40 db represent the best quality of image. The proposed method attains more than 40 db PSNR of image that is represented in Table 4.1. Smaller value of MSE represents smaller mean square error between the two images. The proposed method of data hiding obtains very smaller value of MSE.

Table 4.1
Experimental results of the proposed method in terms of Peak Signal to Noise Ratio, Correlation, Entropy, Mean Square Error and Structure Similarity Index Matching.

Image	PSNR	MSE	Entropy	Correlation	SSIM
Lena	42.86	3.36	5.03	0.9993	0.9617
Baboon	33.17	30.63	4.78	0.9915	0.9764
Airplane	44.30	2.41	3.61	0.9975	0.9467
Boat	40.39	5.93	4.75	0.9986	0.9796
Pepper	41.45	4.64	5.22	0.9992	0.9755

From Table 4.1, it has been concluded that mean value and standard deviation of original image and processed image is almost same and represents the minor changes between the original image and processed image. Comparison of the proposed method with existing techniques [3, 5, 13, 19, 20] in term of PSNR using different images is shown in Table 4.2 and Bar chart is also shown in Figure 4.1. From Table 4.2 and Figure 4.1 it has been concluded that proposed method is better than other existing methods of data hiding such as NMI, ENMI, INP, IMNP and MNMI in term of visual quality of image.

Table 4.2
Comparison of the proposed method with existing approaches in term of Peak Signal to Noise Ratio using different images.

Image	INP [13]	ENNM [5]	IMDP [20]	MNI [3]	PINP
Lena	30.6	33.4	32.1	37.4	42.8
Baboon	22.1	24.4	24.0	31.5	33.1
Airplane	28.7	33.3	30.8	35.3	44.3
Boat	26.7	30.9	28.3	34.5	40.3
Pepper	29.1	35.2	30.9	37.0	41.4

Table 4.3
Comparison of the proposed method with existing approaches in term of Mean Square Error using different images.

Image	INP [13]	ENNM [5]	IMDP [20]	MNI [3]	PINP
Lena	56.5	29.2	39.8	11.62	0.84
Baboon	394	232	256	45.66	9.1
Airplane	86	29.9	54	18.85	0.73
Boat	137.3	52.4	94	22.65	1.33
Pepper	79.8	19.2	52.7	12.94	1.47

V. CONCLUSION & FUTURE SCOPE

In the proposed work image steganography has been used so that data can be easily embedded behind the cover image with minimum distortion in cover media. This cipher text has been embedded behind the cover image so that data can be transmitted in secure manner. Interpolation based approach has been used for generation of new pixels and pixel difference has been used for embedding of secret information that has been encrypted. Whole information has been embedded to the pixels of the image and new image has been formed. In the proposed work various parameters have been analyzed for performance evaluation of proposed work. These parameters are PSNR, MSE, SSIM and Correlation. On the basis of these parameters one can conclude that proposed approach provides better image steganography as compare to existing approaches.

In the future reference proposed approach can be used in real world application for data security and transmission. In the

future new approaches that are based on artificial intelligence that can be used for images steganography so that regions from the images can be extracted in which data can be embedded at high capacity with minimum distortion.

V. REFERENCES

[1] A. Kaur and G. Soni, "Optical stegnography to enhance speed of analog transmission with security enhancement through image encryption," *2017 9th International Conference on Computational Intelligence and Communication Networks (CICN)*, 2017, pp. 165-168, doi: 10.1109/CICN.2017.8319378.

[2] A. U. Islam *et al*., "An improved image steganography technique based on MSB using bit differencing," *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, 2016, pp. 265-269, doi: 10.1109/INTECH.2016.7845020.

[3] G. Prashanti, B. V. Jyothirmai and K. S. Chandana, "Data confidentiality using steganography and cryptographic techniques," *2017 International Conference on Circuit,Power and Computing Technologies (ICCPCT)*, 2017, pp. 1-4, doi: 10.1109/ICCPCT.2017.8074276.

[4] S. Sharma and V. Sejwar, "Implementation of QR Code Based Secure System for Information Sharing Using Matlab," *2016 8th International Conference on Computational Intelligence and Communication Networks (CICN)*, 2016, pp. 294-297, doi: 10.1109/CICN.2016.64.

[5] Bailey, K., Curran, K. "An evaluation of image based steganography methods." *Multimedia Tools Appl* 30, 55–88 (2006).

[6] L. Zhu, X. Luo, Y. Zhang, C. Yang and F. Liu, "Inverse Interpolation and Its Application in Robust Image Steganography," in *IEEE Transactions on Circuits and Systems for Video Technology*, doi: 10.1109/TCSVT.2021.3107342.

[7] M. Hussain and M. Hussain, "Pixel intensity based high capacity data embedding method," *2010 International Conference on Information and Emerging Technologies*, 2010, pp. 1-5, doi: 10.1109/ICIET.2010.5625723.

.