IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-8, Issue-2, Feb 2020 E-ISSN: 2347-2693

A Robust Hybrid Algorithm for Image Steganography

Divya Soi[1*], Bhupinder[2]

[1,2]Indo global group of colleges, Abhipur, India

**Corresponding Author: divyasoi30oct@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v8i2.5968 | Available online at: www.ijcseonline.org

Accepted: 13/Feb/2020, Published: 28/Feb/2020

***Abstract*-**Image Steganography is the mechanism of hiding the critical information on the segment of the image that can either be least significant or most significant in nature. Image Steganography involves multiple images that are merged together to achieve a common image that is transferred over a digital medium. Proposed system uses slant let transformation to achieve better result of image security in terms of accuracy. Accuracy is achieved by minimising mean square error and improving peak signal to noise ratio.

Keywords: Image Steganography, Slant let Transformation. PSNR, MSE

I. INTRODUCTION

In present days, the assurance and illicit redistribution of advanced media has turned into a noteworthy issue. [1] The advanced Steganography has been utilized to shield computerized data from unlawful redistribution and changes. In advanced water denoting the image has been improved by installing clamour tolerant flag into bearer flag.

Late years have seen a quick development in the accessibility of computerized media content. Today, computerized media archives can be conveyed by means of the World Wide Web to countless without much exertion and cash. Moreover, not at all like conventional simple replicating, with which the nature of the copied content is corrupted, advanced apparatuses can without much of a stretch create extensive measure of ideal duplicates of computerized archives in a brief period. This simplicity of computerized interactive media appropriation over the Internet, together with the likelihood of boundless duplication of this information, debilitates the protected innovation rights like never before. Hence, content proprietors are energetically looking for advances that guarantee to ensure their rights.

In the present period [2], [3]advanced security turns into the most smoking point because of its capacity to decrease the cost related with registering. Computerized registering gives the on request benefits like stockpiling, servers, assets and so on to the clients without physically obtaining them and the instalment is as per pay per utilize. Since image processing gives the capacity, diminishes the overseeing expense and time for association to the client however security and classification turns into the one of the greatest problems before us. To tackle the issue [4] slantlet transformation is used. The real issue with cloud condition is, the quantity of client is transferring their information on distributed storage so now and again because of absence of security there might be odds of loss of privacy. To beat these hindrances an outsider is required to anticipate information, information encryption, and trustworthiness and control unapproved access for information stockpiling to the cloud.

With the fast improvement of equipment and programming computerized security acquires the insurgency the business. It gives assets like computational power, stockpiling, calculation stage promotion applications to client on request through web. A portion of the cloud suppliers are Amazon, IBM, Google, Sales drive, Microsoft and so on. [5]Computerized processing highlights included asset sharing, multi-tenure, remote information stockpiling and so on yet it challenges the security framework to secure, ensure and process the information which is the property of the individual, undertakings and governments. Despite the fact that, there is no prerequisite of information or ability to control the foundation of mists; it is dynamic to the client. It is an administration of an Internet with high adaptability, nature of administration, higher throughput and high processing power. Advanced registering suppliers send normal online business applications which are gotten to from servers through web program. Information security is the greatest issue in computerized security and it is difficult to determine it.

[6], [7]Steganography through the advancement of DWT known as slant let transformation is proposed. The logo image and main image are collaborated together by the use of slantlet transformation. Singular valued decomposition is used to reduce the complexity of operation. The entire image is decomposed into three parts. Matrix indicated with S,V and D. all the colour dissimilarities are denoted with D and intensity mismatch is resolved with singular matrix s and v. Flow of proposed system is given as under.

Basic principal of Steganography is given as under

- Input the image (primary image)

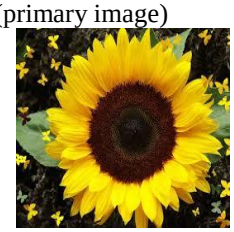

Fig. 1

- Input the logo image(Secondary image)

Fig. 2

- Apply the mechanism of Steganography to merge the two images.

Fig. 3

- Output the Steganography image

Fig. 4

Obtained the parameters such as PSNR and MSE for performance measurement of techniques used.
Next section gives the brief overview of existing security techniques used within the digital systems.

II.TECHNIQUES USED FOR IMAGE SECURITY

To achieve the image security, Steganography and stenography mechanisms commonly followed. The techniques for image security are described as under

LSB Stenography

[8]In LSB stenography, the least significant bits of the image are chosen and replaced with the logo image. The contrast enhancement mechanism is implied in order to change the contrast of both the images so that merged images are clearly visible. Problem with this approach is however those attackers easily can determine the position of the logo and hence attack can easily takes place. In order to tackle the issue, MSB stenography is followed.

MSB Stenography

[9]In MSB stenography, most significant bits are enriched with the logo image and hence merged image is obtained. The assumption is that MSB are less prone to attacks as compared to LSB bits. The mechanism of LSB stenography is performed in this case however MSBs are used in place of LSBs.

Cipher Bits

[10]this is another mechanism to ensure the safeguard of transmitted image over the career. The image meant to be transmitted over the medium however before transmission image is encoded and cipher image is obtained. The key that can be public or private is also generated. This key is transmitted along with the image itself. At the other end decryption mechanism is implied to resolve the problem into desired image formats.

AES

[11]Advanced encryption slandered can be used in order to provide encryption of images for security. AES provide 128 bit encryption with 32 distinct segment formats. Keys are generated which are shared with sender and receiver. Keys are used to decode the image which is received at the destination end.

Image Authentication

[12]this is the mechanism in which username and password is allocated to the image. In order to access the image username and password is required to be given. The wrong password ensures de-allocation of resources. Image authentication is least secure since passwords can be easily guessed. In order to overcome this situation, image Steganography mechanism can be used.

The proposed methodology is given in next section

III. PROPOSED METHODOLOGY

[13], [14]Steganography in existing literature is done by the use of discrete wavelet transformation. Advancement in terms of slant let transformation is giving better result in terms of parameters MSE and PSNR. MSE is obtained by the use of following equation

$$MSE = \sum \frac{(X - X_i)^2}{n}$$

Where n I the total number of pixels and x is the actual value of the result. X_i is the result obtained after applying proposed mechanism.
Peak signal to noise ratio is obtained by the use of following equation

$$\text{PSNR}=10 * log(\frac{signal}{Noise})$$

The flow of the proposed system is given in terms of the flowchart as

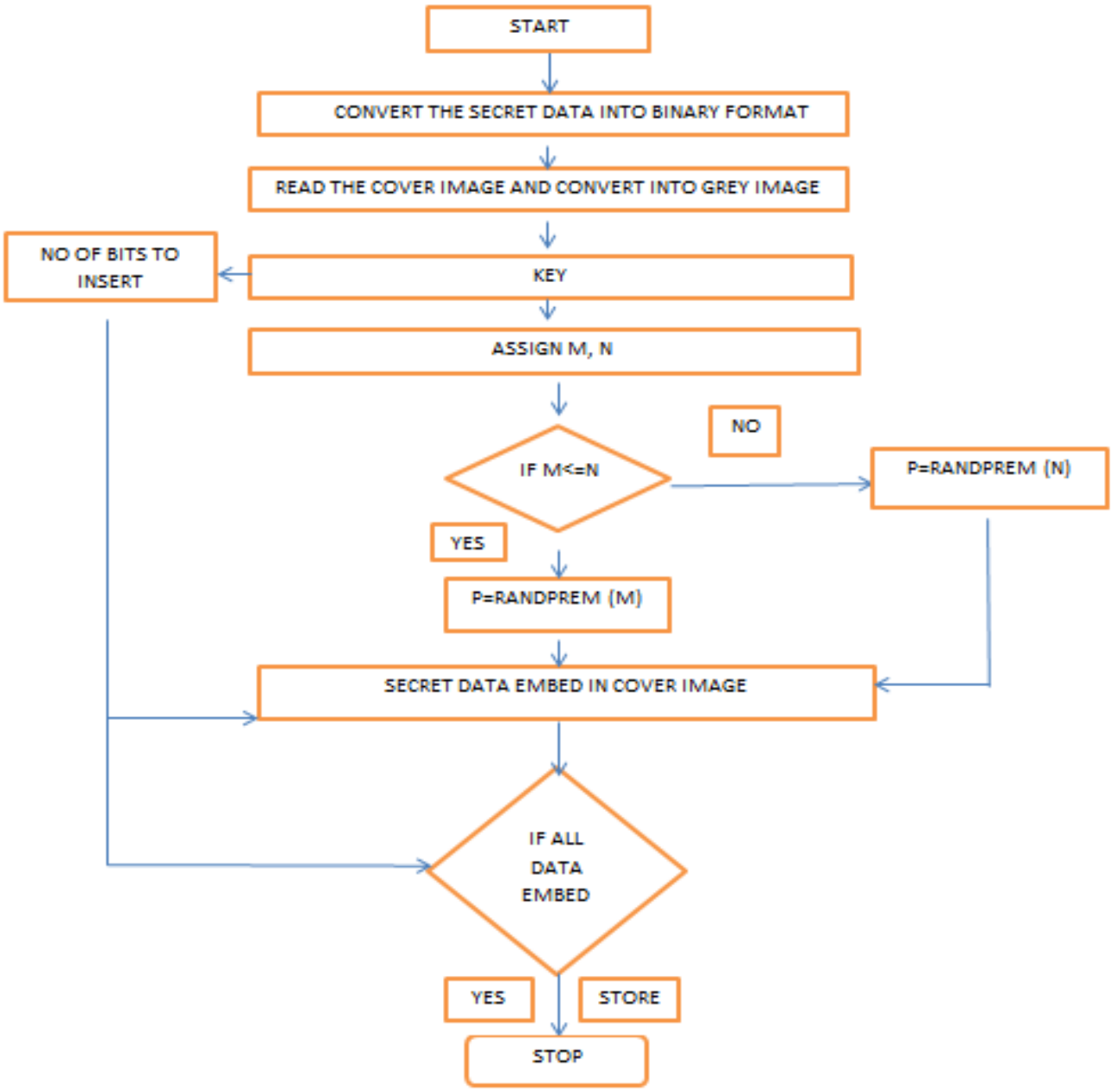

Figure 1: Showing flowchart of proposed system

System being studied takes out the image from source and encrypt message onto the image. Image contain encrypted information. That information along with image is transferred towards the destination. Key for decryption is also transferred along with the image. At the receiver end decryption is performed. Decryption is possible only if valid key is received by the receiver. Recived message is stored within the buffer and algorithm terminates.

ALGORITHM OF THE PROPOSED SYSTEM

1. Begin
2. Input: Cover Image, Secret Message, Secret Key;
3. Transfer Secret Message into Text File;
4. Message Text File;
5. Convert Text File to Binary Codes;

6. Convert Secret Key into Binary Codes;
7. Set Bits Per Unit to Zero;
8. Encode Message to Binary Codes;
9. Add by 2 unit for bits Per Unit;
10. Output: Stego Image;
11. End

The flow of the algorithm is given by the following figure:-

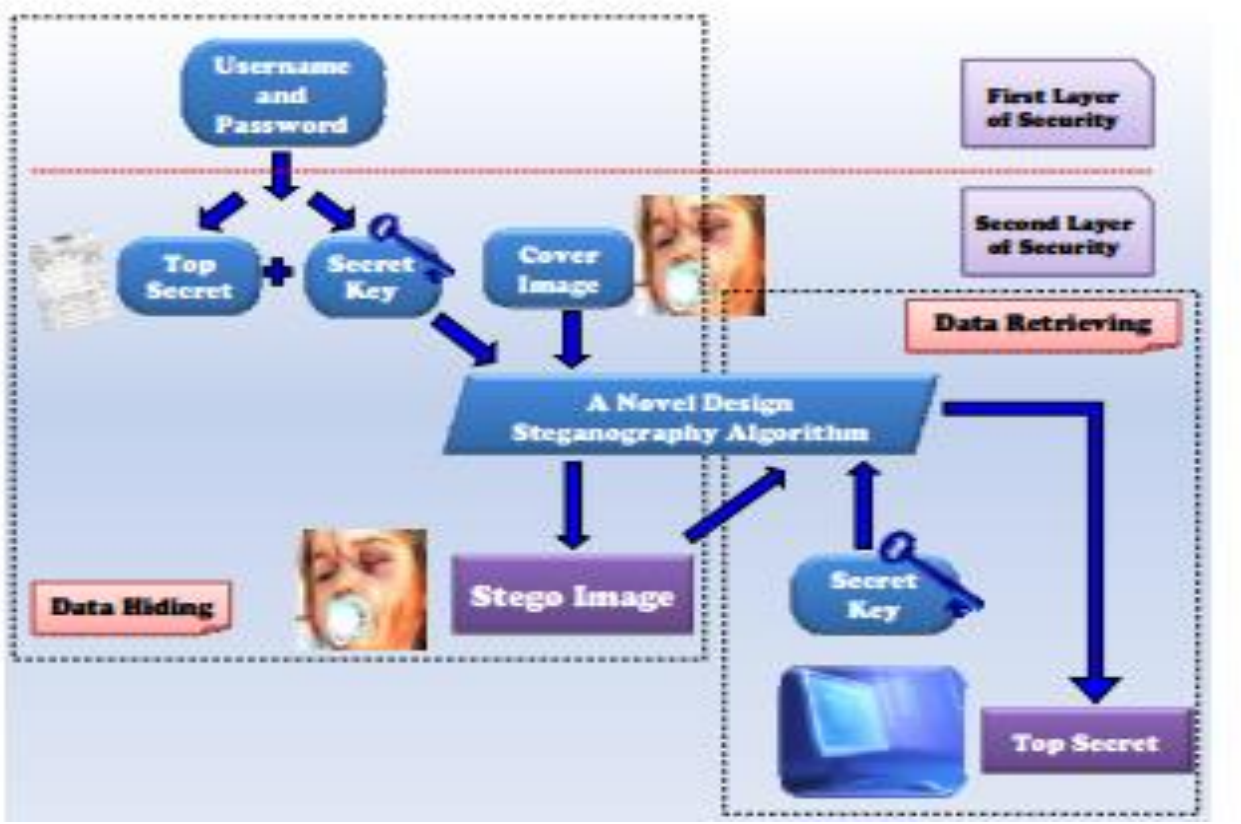

Figure 6: The framework for the system

IV. PERFORMANCE ANALYSIS AND RESULTS

In order to analyze the performance of the system parameters such as PSNR, MSE, CR and BPP are used. The results are attained by the use of both colored and Black and white images. In almost all the cases results for the purposed system comes out to be better. Results are depicted as under

Parameter- PSNR

Table 1: Comparison of PSNR metric with existing and proposed system

BASE PAPER	Proposed System with Colored Images	Proposed system with Black and White images
24.782	10.233	12.6399
35.8314	6.9233	9.07644
33.2008	12.1523	13.6909
24.4253	10.3552	11.7566

The results in terms of plot is given as under

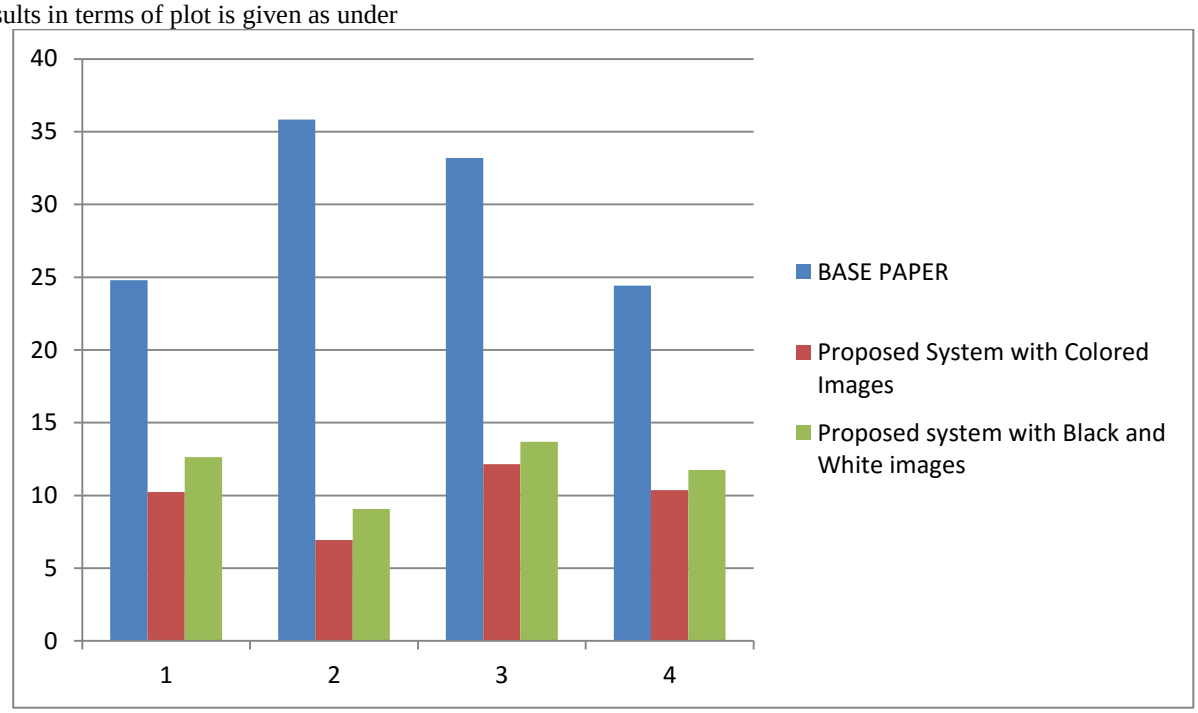

Figure 7: Plots corresponding to PSNR

Line chart for the PSNR parameter obtained is as under

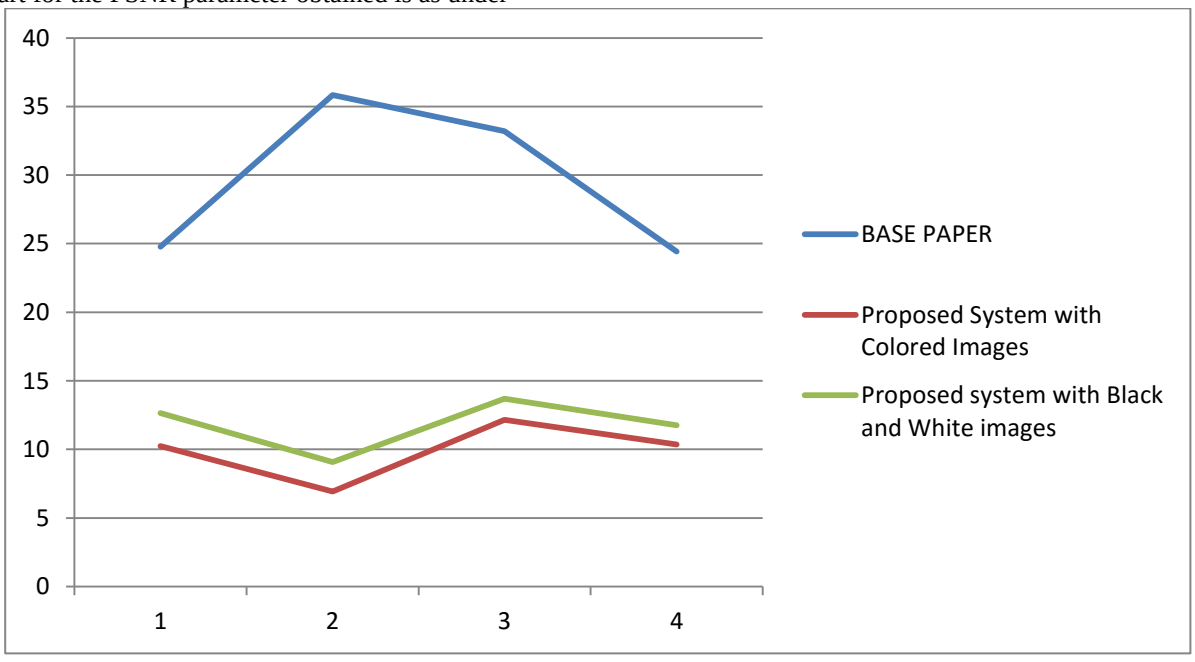

Figure 8: Line chart corresponding to PSNR

Peak signal to noise ratio is required to be enhanced which is obtained by dividing signal with noise present within the image. The PSNR is considerably increased through the proposed literature through the application of Stegnography. Peak signal to noise ratio needs to be maximized. The formula to attain PSNR is listed as under

$$PSNR = 10 * LOG_{10}(\max_i/mse)$$

Maxi is the maximum signal range and mse is mean square error obtained through the noise value.

Second parameters which is evaluated through the proposed and existing system is MSE. Results are listed as under

Table 2:Comparison in terms of MSE with existing and proposed system

Base Paper	Proposed with Colored Image	Proposed with Black and White Images
34.1887	7.53252	6.50848
35.5882	3.48089	2.12638
32.9193	21.1494	16.4359
33.7493	2.89472	2.61182

Plots in terms of bar chart and line chart of MSE is as under

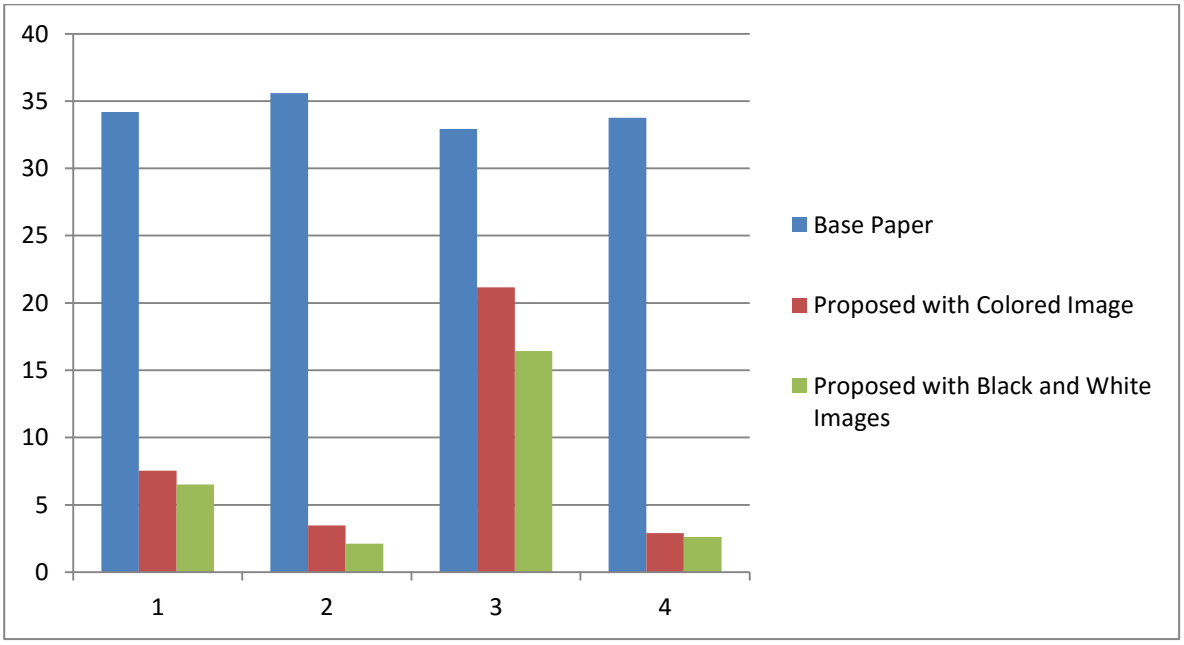

Figure 9: Plot of comparison of MSE

Line chart for MSE is as under

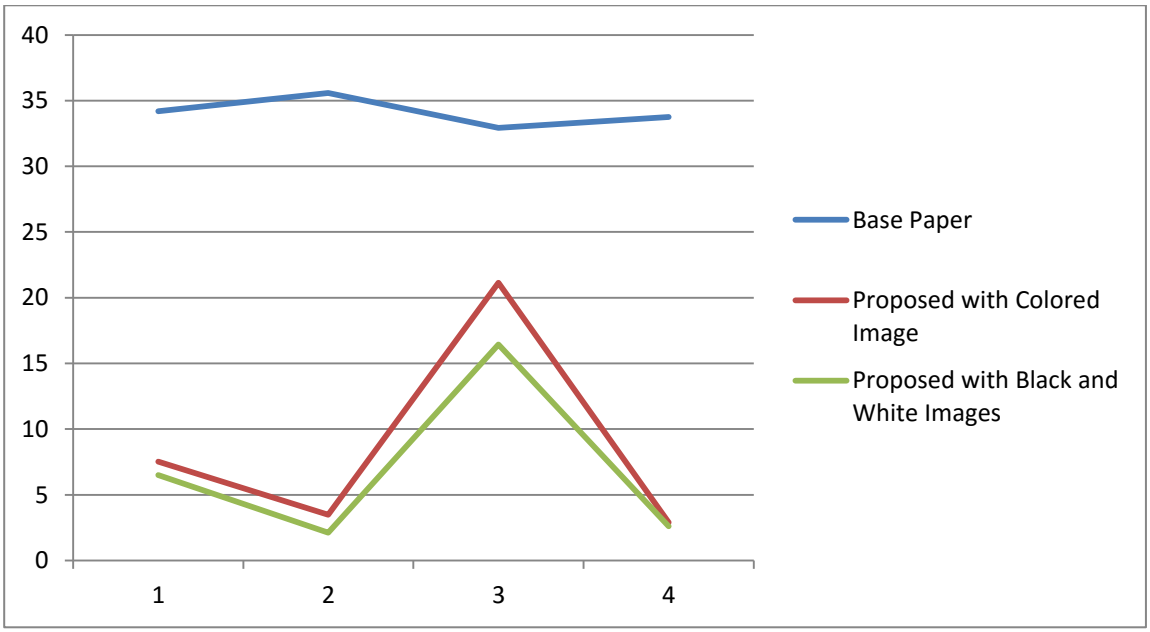

Figure 10 : Line chart demonstration of base and proposed system

MSE should be minimized which is accomplished with the help of proposed literature. Mean square error is also reduced as the noise from within the image is reduced. MSE is obtained using the formula listed as under

$$MSE = avg(x - x_a)^2$$

Through the avg function mean value is obtained. X is the actual value and xa is the approximate value obtained from simulation. Result variation gives mean square error. Proposed literature subsequently decreases MSE from within the transmitted images.

Next parameter to be evaluated is BPP. The tabular representation for the same is as under

Table 3:Comparison in terms of BPP

Base Paper	Proposed with Colored images	Proposed with Black and White images
14400	77562	77562
9216	58320	58320
12544	58266	58266
576	77562	77562

Plots of BPP which should be maximized as achieved with the help of proposed system is shown as under

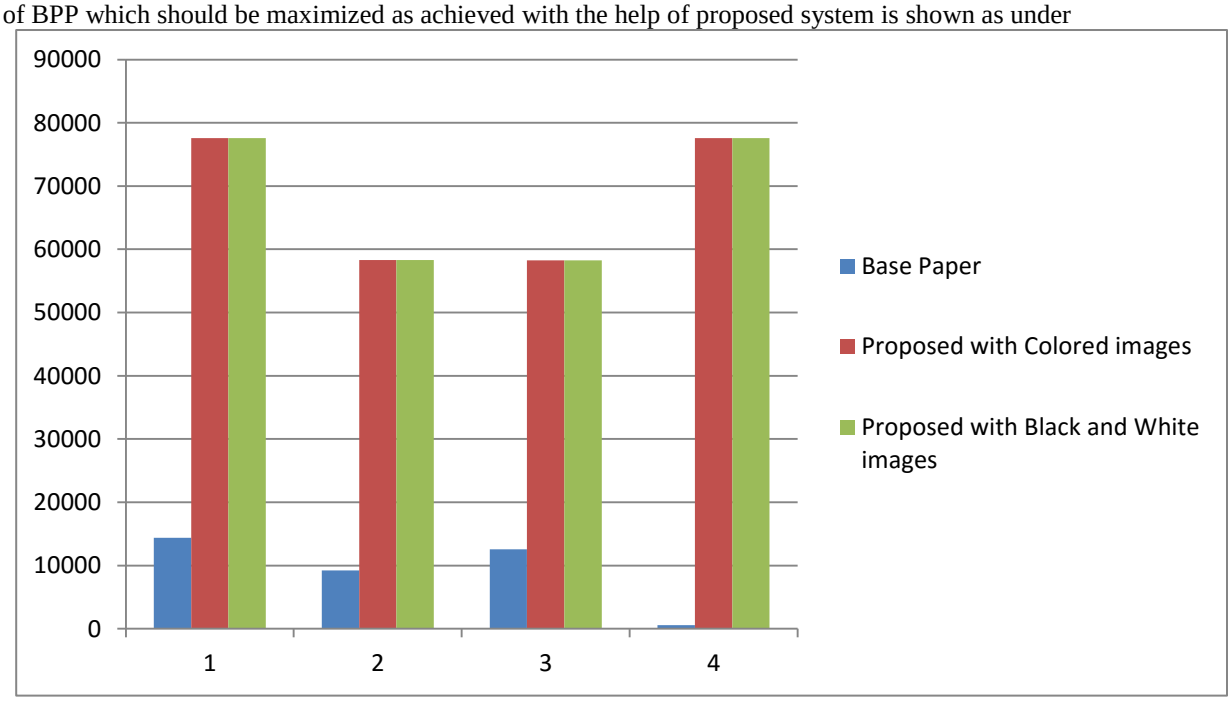

Figure 21: Plot showing comparison of BPP

BPP is increased as the applications of proposed literature. BPP depends upon size and noise from within the image. BPP is enhanced as noise is reduced and size is reduced to fit within the axis of MATLAB. BPP is calculated using the formula listed as

$$BPP = 2^k$$

Where k refers to number of gray levels present within the images.
Line Chart for the BPP is as under

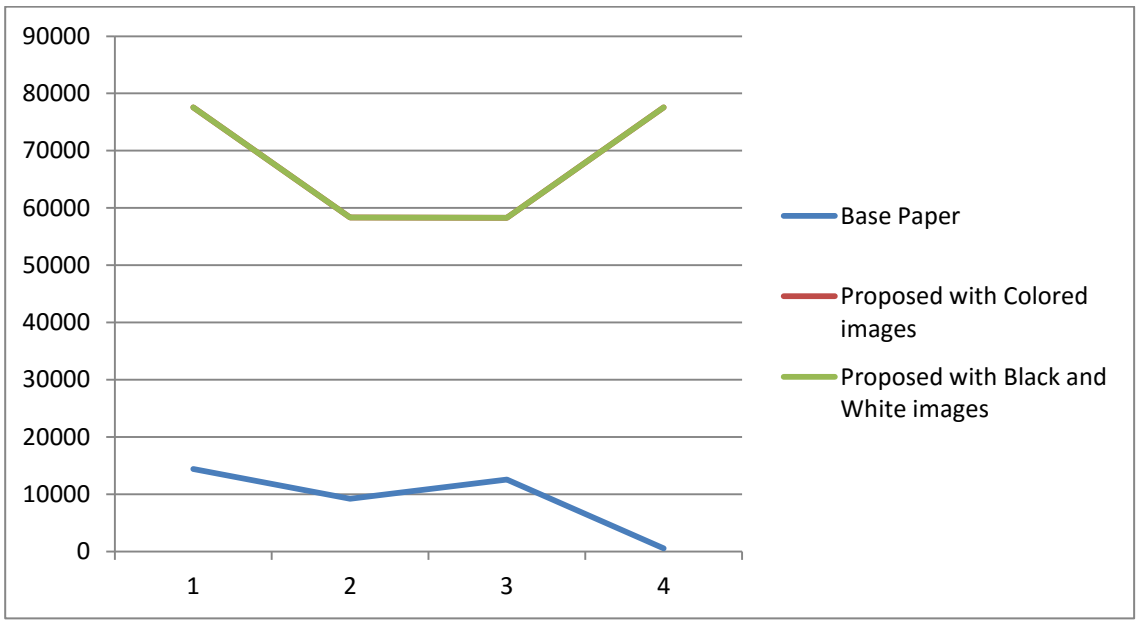

Figure 32: Showing comparison of BPP

Last parameter evaluated is CR. It should be maximized. Tabular representation is as under

Table 4:Comparison of CR in terms of proposed and existing system

Base paper	Proposed with Colored image	Proposed with Black and White image
0.0940245	0.719424	0.719424
0.0324321	0.6944444	0.694444
0.028149	0.60241	0.60241
0.632394	0.719424	0.719424

Bar Chart and line chart showing the comparison of CR is given s under

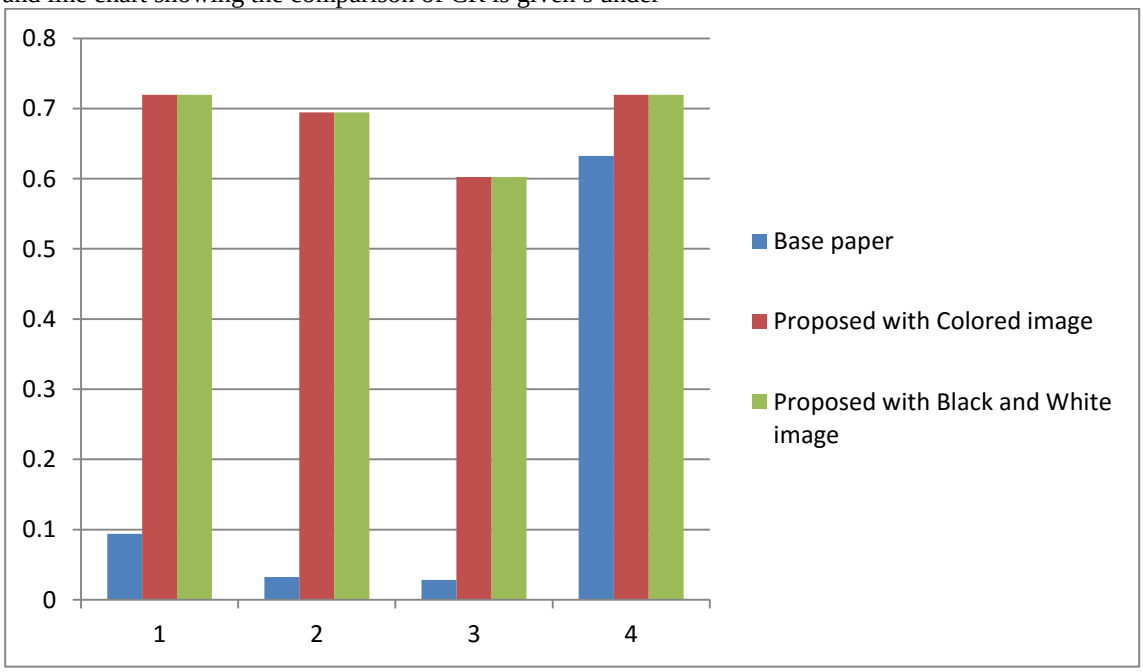

Figure 43: Bar chart showing comparison of CR with existing and proposed system

Line chart comparison is as under

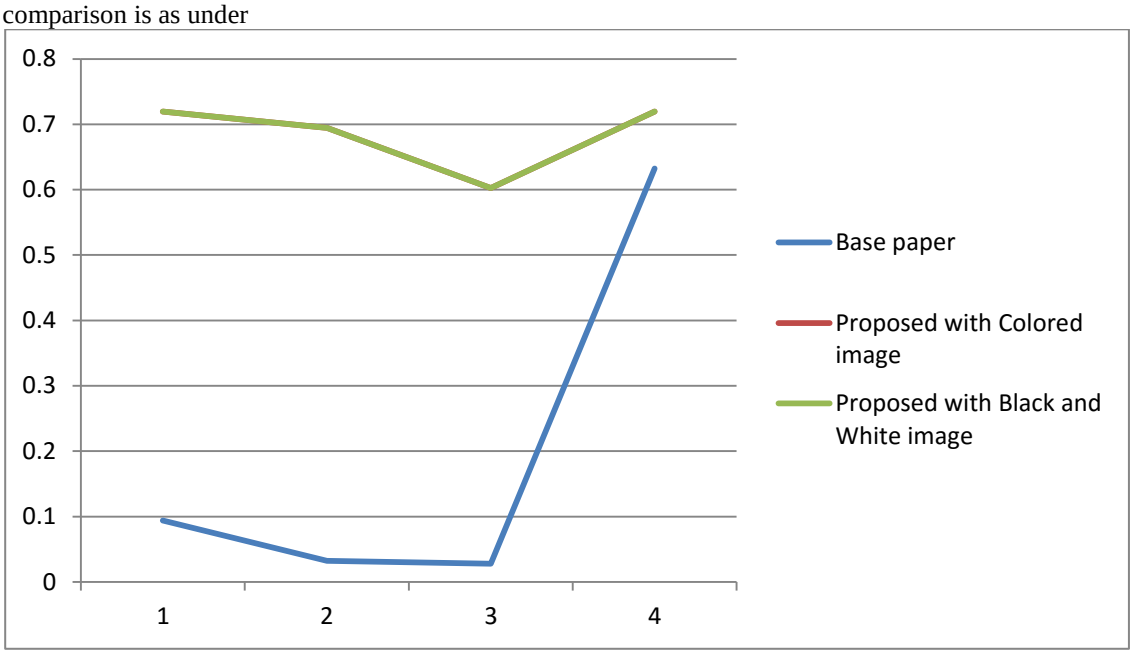

Figure 54: Line chart showing comparison of CR

CR depends upon resolution of the image. Resolution is number of pixels horizontally and vertically present without distortion. Since noise free image is present hence CR enhances. CR is calculated through the following mechanism

$$CR = K_r * R^i + K_g * G^i + K_b * B^i$$

Where R, G and B are three primary colors and values of K is derived from RGB intensity values. by combining any of the above colors any color can be formed and corresponding value of CR varies.

All the parameters have been optimized by the use of proposed system. This result and performance analysis indicates that proposed approach is optimal in nature proving worth of study.

V. CONCLUSION

Data Transmission through digital media is regular now days. As transmission through digital media is expanding so does the assaults. At the season of transmission this data may get influenced by clamor, or some outsider tries to get that data and alter it. This can be forestalled utilizing digital Steganographs. The sender who needs to send mystery or private picture to some other individual will install the mystery picture in another picture with the assistance of a key and send it through the Internet. The beneficiary will get that picture and concentrates the concealed Steganograph from that picture with the assistance of the mutual key.

Security of data and picture will be of prime concern. Improving security is proficient by the utilization of number of systems for this reason encryption and unscrambling instruments are fundamental. Encryption is usually performed on content data the scrambled content is normally known as figure content. The programmers may assault the encoded data since encryption systems are usually utilized. So as to upgrade the security Steganograph appears. The proposed approach improving the security by presenting lucidity of picture encryption and decoding through inclination let changes. The SLT decrease the span of the picture by disintegrating it. By doing as such LSB and MSB bits of the picture can undoubtedly be obliged. The outcomes acquired through the proposed approach are superior to the current one.

REFERNCES

[1] C. Science and S. Engineering, “Steganography Digital Images : A Hybrid Approach,” **vol. 5, no. 5,** pp. 1778–1785, **2015.**

[2] P. Parmar and N. Jindal, “Image Security with Integrated Steganography and Encryption 1 1 2,” **vol. 9, no. 3**, pp. 24–29, **2014.**

[3] T. Bathinda, “Invisible Video Multiple Steganography Using Optimized Techniques,” **2016.**

[4] R. T. Mohammed and B. E. Khoo, “Image Steganography using slantlet transform,” *ISIEA 2012 - 2012 IEEE Symp. Ind. Electron. Appl.*, pp. 281–286, **2012.**

[5] R. K. Sheth and V. V. Nath, “Secured digital image Steganography with discrete cosine transform and discrete wavelet transform method,” *2016 Int. Conf. Adv. Comput. Commun. Autom.*, **pp. 1–5, 2016.**

[6] R. V Mahule, “Analysis of Image Security Techniques using Digital Image Steganography in Spatial Domain,” no. Nckite, pp. **19–26, 2015.**

[7] Z. J. Xu, Z. Z. Wang, and Q. Lu, "Research on Image Steganography Algorithm based on DCT," **vol. 10**, pp. 1129–1135, **2011.**

[8] A. U. Islam, F. Khalid, M. Shah, Z. Khan, T. Mahmood, A. Khan, U. Ali, and M. Naeem, "An improved image steganography technique based on MSB using bit differencing," *2016 6th Int. Conf. Innov. Comput. Technol. INTECH 2016*, **pp. 265–269, 2017.**

[9] V. Saravanan and A. Neeraja, "Security issues in computer networks and stegnography," *7th Int. Conf. Intell. Syst. Control. ISCO 2013*, **pp. 363–366, 2013.**

[10] P. Singhai and A. Shrivastava, "An efficient Image Security mechanism based on Advanced Encryption Standard," no. 13, **2015.**

[11] S. S. Gonge, "An Integration of SVD Digital Image Steganography with AES Technique for Copyright Protection and Security of Bank Cheque Image," **pp. 769–778, 2016.**

[12] Q. Chen, H. Hu, and J. Xu, "Authenticated Online Data Integration Services," **pp. 167–181.**

[13] J. Singh and A. K. Patel, "An Effective Telemedicine Security Using Wavelet Based Steganography," **pp. 2–7, 2016.**

[14] M. Rizal, M. Isa, and S. Aljareh, "A Steganography technique to improve the security level in face recognition systems," *Multimed. Tools Appl.*, **2016.**

