10.48047/jocaaa.2024.32.01.24

Image Steganography Based on Color Pallete

Sonia Thind[1] and Dr. Abdullah[2]
[1] Research Scholar, University Institute of Computing,
Chandigarh University, Gharuan,Mohali. India.
(Email id: sonia.thind24@gmail.com)
[2]Associate Professor, University Institute of Computing,
Chandigarh University, Gharuan,Mohali. India

ABSTRACT
The potential growth of modem infrastructures necessitates more advanced security measures, particularly when using computers. Network security is becoming increasingly important as a result of the enormous number of documents being sent online. To protect documents from unauthorized access, privacy and data dependability are necessary; this led to a frenzied development of the area of data concealing. Data hiding techniques are receiving a lot of attention these days due to concern over encoding facilities achieving illegal activity and patent owners who want to monitor reliable and logical information, patent security, along with illegal entry and practice in electronic things (songs, movies, manuscripts, and programs) done by using digital marks. The secret code safeguard does not maintain next level security, but it may be increased by masking the existence of statistics, which is made feasible via steganography. The suggested approach entails replacing LSB bits in Protection Image (A) with Secret Image (B) to incorporate Secret Image in Protection Image. Stego-object is the resulting copy after applying DCT to transform it from three-dimensional domain to frequency and then compressing it using Huffman compression.

Keyword: Discrete Cosine Transformation, Square Truncation Coding, Least Significant Bit, Compression Ratio, Signal to Noise Ratio

1. INTRODUCTION

Steganography is an encoding technique that ensures statistical categorization. The main drawback of encoding is that anyone can identify the mysterious correspondence passage (memo transient), but it is very difficult to decipher the scrambled information. In contrast, steganography hides the data so that the correspondence passage is invisible, preventing anyone from understanding the statistics or memo distribution. It provides a secret passageway for correspondence that cannot be removed or restored without changing the installation data or information. The most often used Steganography technique involved changing and anticipating the smallest essential Bit of the pixel. Every pixel may store or capture 8 bits of information thanks to the revised piece encoding approach that was used for steganography [3].

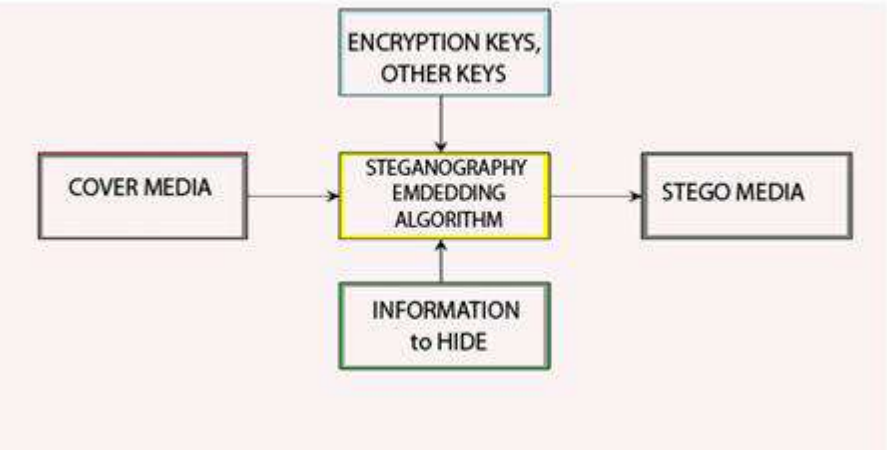

Figure 1: Simple Steganography [3]

There are several modern uses for techniques that embed records in audiovisual and photographic images advance image by obscuring the placement of information in an image, steganography techniques may also produce advancing and opposing similarities.

10.48047/jocaaa.2024.32.01.24

Diverse tactics must continue to be researched and developed to provide individual protection. The greatest initial and following step towards steganography is probably encoding. Steganography isn't as adaptable to use as encoding, which is also frequently seen. Steganography is the knowledge and study of mixing hidden memos such that no one, outside the transmitter and likely receiver, can connect the incident with the memo. It is a form of safety achieved without providing a description. The word "steganography," which has Greek roots, means "hidden composition." The main goal of steganography is to conceal the fact that the note is present in the distributed intermediate [3].

Types of Attacks together with Steganography

Steganalysis is the investigation of the spread (carrier), the Stego-picture, and the hidden communication. An assault refers to the many methods used to investigate Stego-pictures and includes:

a. Stego-just here the attacker slants just to the Stego-picture,
b. Known Cover here the attacker approaches just to the deliverer,
c. Known Message where the attacker approaches just to the message,
d. Picked Stego where the attacker approaches together the Stego-picture and Stego scheming
e. Picked message here the attacker makes a Stego-picture from a memo using a calculation, probing for marks that will authorize him to identify other Stego pictures.

Embedding

The secret memo and the spread medium attached to the encoder must be permitted simultaneously as the first step in the installation process for data concealment. To insert the mysterious data into the spread media, a few conventions will be carried out within the encoder. What kind of data you are trying to implant will determine the convention. For instance, data is embedded into photographs using a picture standard. An installation key is commonly needed. This might be an exposed or secret key, and by using your secret key to encrypt an unknown message, the beneficiary will be able to decrypt it using your exposed key. This reduces the likelihood that an outside attacker will grab the Stego article and unravel it in order to find the mysterious data.

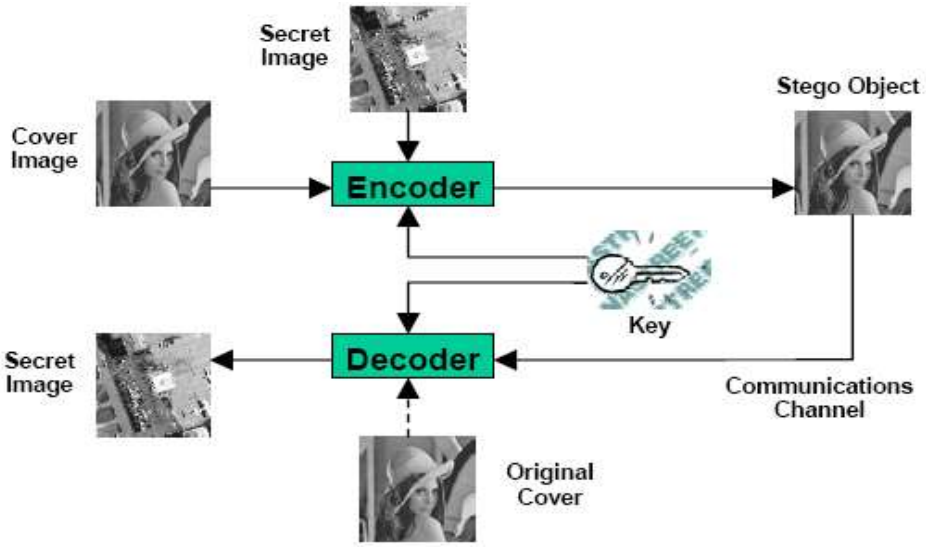

Figure 2: General method of Image Steganography [2]

A Stego item will be provided after passing over the encoder. The first spread article to use the hidden data in it is a Stego entity. If an outside attacker may view implanted data, this piece must appear virtually identical to the distributed item. Once the Stego entity has been delivered, it will then be transmitted to the intended beneficiary for untangling via a specific correspondence route, such as email. To see the mysterious data, the recipient must understand the Stego item. The interpretation process, in contrast to the converting process, is the last step. It is only the extraction of enigmatic data from a Stego entity [2].

Steganography Grouping

10.48047/jocaaa.2024.32.01.24

When we talk about sophisticated steganography, we want to say that computerized media like photos, videos, and procedures are used as legitimate covers for secretly hiding confidential communications. The four primary categories of document arrangements that can be used for steganography are depicted in Figure 3 [3].

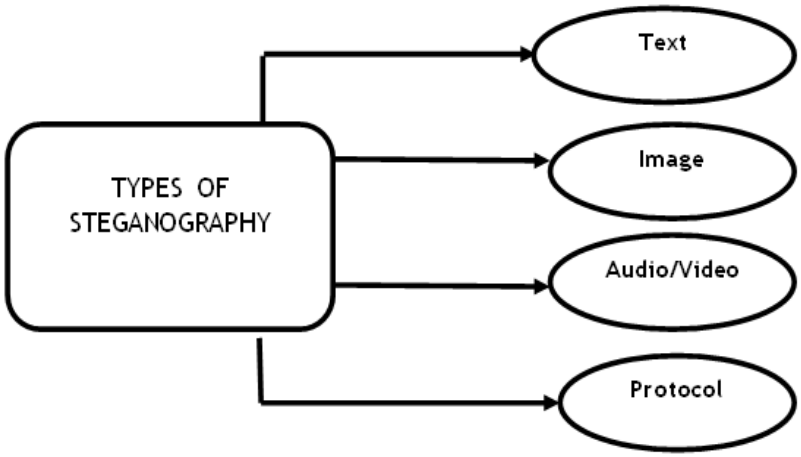

Figure 3: Categories of Steganography [3]

Image Steganography

The secret insertion of information into computerized images is known as picture steganography. Although steganography may encrypt data in any computerized medium, sophisticated photos are the most often used carrier due to their frequent usage online. The image document's variable size allows it to conceal large amounts of data. The normal image and the image with hidden information cannot be distinguished by HVS. Additionally, as modern images now include a significant amount of extra data, they have become the most often used materials for steganography. Therefore, this investigation uses a photograph as a distributed document [1] [3] [8].

Trials in Steganography

The substantial problems of fruitful steganography are:

- **Security of Unseen Message**

The cloaked material must be imperceptibly and demonstrably invisible in order to avoid raising the suspicions of nosy neighbors while avoiding the meticulous demonstration of technique recognition. Steganography techniques should produce a high-quality, blurry Stego-picture.

- **Extent of Payload**

Steganography concentrates on covered memoranda and, unlike water markings, which must implant a sufficient number of patent figures, in this approach typically requires proper installation limits. Higher payload requirements and secure correspondence requirements sometimes conflict. Depending on the specific application circumstances, an exchange off must be sought for.

- **Sturdiness**

Stego-picture should support image manipulation techniques like compression, cutting, resizing, and so on. For instance, when any of these operations are carried out on Stego-picture, secret information shouldn't be completely destroyed. There is currently no steganography technique that provides all three items at a meaningful level. Here, there is a debate between the implanted information's capacity for attack and its limit, while still giving due consideration to the Stego-medium's capable perception. Expecting to achieve high heartiness to flag changes and high addition limit at the same time is ludicrous [6, 8].

2. RELATED WORK

Shadi AlZubi et al., (2011) another extension of wavelet change, curvelet change aims to handle fascinating wonders occurring along bends. Curvelet change is a particularly nerve-wracking task when using low-light CT filters to organize human organs. The author demonstrated an expert use of Curvelet change for noise

10.48047/jocaaa.2024.32.01.24

filtering and clinical image division. A correlation analysis of numerous adjustments is accomplished, and the results show that curvelet alterations exhibit a perfect representation of the region of fascination with greater accuracy and less agitation. **Dr. Mohammed Nasser Hussein Al-Turfi, (2012)** Despite what might be expected, a notable picture will be used exists on the two sides of the channel and an instant message containing important information will be transmitted. This is how the steganography system will be implemented, but on a different level because the important information won't be covered up in a picture or moved through the correspondence channel inside a picture. We can re-blend and re-make the source image with the right exercises. The computation was done in MATLAB7, and it demonstrates that it has a great capacity for completing tasks involving diverse types and sizes of images. The receiving side completed pristine reproduction. The formula that ensures picture transmission, however, sends no pictures at all, which is what I find most intriguing. **Saleh Saraireh, (2013)** One of the biggest concerns in information communication nowadays is data security. As a result, it becomes an identical piece of information correspondence. Encoding and steganography are combined to communicate about matter. The secured correspondence system put out by this author makes use of steganography and encoding computations. This combination creates a strong and sturdy communication foundation that can fend off aggressors. The channel group figure is used in this work to scramble the secret instant memo, giving it a higher value for safety, flexibility, and quickness. From this point on, a distinctive steganography focused on wavelet variations is used to change the wavelet coefficients in order to hide the encoded memo in the distributed picture. Top sign to commotion ratio (PSNR) and histogram analysis are used to evaluate the suggested framework's presentation. The outcomes of the reenactment demonstrate that the suggested framework provides a high level of security. **Mazhar Tayel and Hamed Shawky, (2014)** In the correspondence frameworks, information security has grown to be a serious problem. A secret note is concealed through the use of steganography. The author suggested a modified Steganography computation based on the combined degradation criteria of secret memo and covert image. Before implanting a Stego entity in the spread image, a fuzzification is used in the mystery memo to simplify the deteriorating elements. A component that determines an appropriate incentive for the implanting quality factor to receive a sufficient debasement was also known as the tradeoff factor. Additional histogram measures that relate to the relative recurrence occurrence of the various photographs are suggested in order to examine and evaluate the revised computation and any Steganography calculations. **Hon-Hang Chang et al., (2015)** Due to its low computational cost and ease of implementation, Square Truncation Coding (STC) is one of the most used pressure processes in the image information concealment. There are now three sets of large mean and small mean per three bitmaps in a shading image. The degree of pressure cypher can be spared by using a regular bitmap. By changing big mean and small mean conversion arrangements, the author created an information concealment strategy to cover mystery information into the BTC pressure code. The intended technique aims to include more cryptic information into the BTC pressure cipher's color scheme. The author offered a creative method for encoding the component '1"s measure. If the total is a large amount, the information is deduced to be a mystery bit '0'; nevertheless, it will ultimately be deduced to be a mystery bit '1'. Additionally, the mystery information may be inserted using the lower amount important Bit (LSB) of both the big and small mean sets. All things considered, each square in the suggested technique conceals at least 10 mystery pieces. **Jigar Makwana et al., (2016)** enhancing information security by double steganography is the main focus. In double steganography, a mystery message is first put into one media, followed by the installation of a Stego-item into a different medium. The cited study also provides a methodical evaluation of double steganography by comparing the mean square error (MSE) and subsequent increase in the top sign to noise ratio (PSNR) between original host papers and newly produced stenographic recordings. **A. Soria-Lorente et al., (2017)** presents a unique steganography technique based on an entropy thresholding approach and the pressure standard recommended by the Joint Photographic Expert Group. In order to construct a parallel grouping of pseudorandom integers that indicate where the elements of the twofold arrangement of a mystery message will be inserted, the Steganography computation uses one open key and one private key. The inclusion in the modified DCT region assumes the end position at the first seven AC coefficients. **Kamaldeep Joshi et al., (2018)** A method for picture coding that hides the data along a chosen pixel and on the next estimation of the chosen pixel, pixel + 1, is advised. The tiniest portion is concealed at the selected pixel, and the succeeding portion is concealed on the pixel+1 value. A scientific capability is applied to the seventh pixel of an image based on the seventh pixel, which results in the creation of an ephemeral variable (pixel + 1). For data extraction and covering up, the seventh piece of the chosen pixel and the seventh piece of pixel

10.48047/jocaaa.2024.32.01.24

+ 1 are both used. **Eugenijus Margalikas and Simona Ramanauskaitė, (2019)** proposed a revolutionary picture steganography method that relies on shading space's shifting shading palette. By using images with a fixed or flexible color palette and smoothing, it is possible to increase the pixel and shading capabilities, but this will increase the likelihood of recognizable proof being implanted.

3. PROPOSED WORK

Assumptions

1. A: Cover image
   B: Secret Image
   A & B are can be of any size.
2. Secret Image (B) is embedded in LSB's of Cover Image (A)

Involvement: Shelter Image (A), Secret Photo (B)

Production: Coded Stego Object (S)

Loop

1. Scan first byte of Cover Image (A) & Secret Image (B)
2. Run LSB ()
3. Calculate DCT ()
4. Do Quantization ()
5. Save the outcome as Stego Object (S).

End Loop

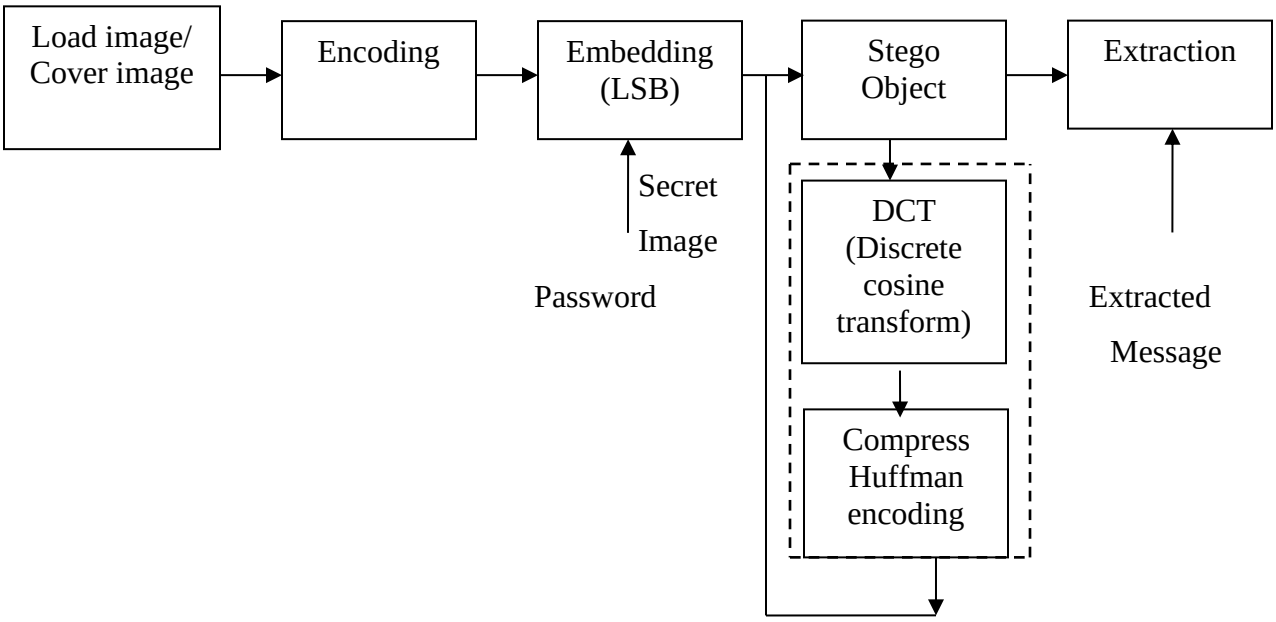

Figure 4: Planned Design of Steganography

1. Cover Image: any graphical image (bmp, jpeg, png) file can be used as cover image.
2. Encoding: both the Cover Image and Secret Image are transformed into the unit8 encoding.
3. Embedding: Three features in data hiding schemes are:
Capacity: It is amount of data that can be hiding in the Cover Image
Security: It is the failure to identify unseen data
Robustness: It is time Stego-object can survive before an opponent can abolish unseen data.
LSB (Least Significant Bit) Embedding: In this every bitmap of photograph is converted into the binary value and facts are secreted into the tiniest important location of the binary value of the bitmap of the photograph in a way, this will not abolish the truthfulness of the Shelter photograph.
Password acknowledged as Stego-Key, receiver that conforming decrypting key can only mine the Secret Image from a Shelter Image.
4. Stego Object: A Stego Object looks alike original Cover Image with the Secret Image inserted within it.

10.48047/jocaaa.2024.32.01.24

DCT (Discrete Cosine Transforms): This function that converts electronic media from the three-dimensional to the frequency dominion. Subsequently converting the photograph in rate of recurrence domain, the facts are inserted in the tiniest important bits of the intermediate frequency components.

Algorithm:

Step 1: Divide image into 16 x 16 blocks of pixels.

Step 2: Apply DCT to every pixel of each block from top-left to bottom-right of the Cover Image.

Step 3: Store DCT Coefficient for every pixel in data block.

Step 4: Quantized each DCT coefficient with a reference quantization table.

Step 5: Now replace these quantized DCT coefficient by a bit from Secret Image.

Step 6: Apply encoding to every reformed quantized DCT coefficient to create compacted Stego Object.

Compress Huffman Encoding: It eliminates duplicate codes from the image, compresses the image file and effectively rebuilt it. It also raises the inserting capability [6].

5. Extraction: The receiver must decipher the Stego Object to see the Secret Image. It is the opposite of the converting procedure.

4 RESULTS AND DISCUSSION

Figure 5: Cover Image

Figure 5 shows the Cover Image this is used embed Secret Image in iteself.

Figure 6: Secret Images to be Hiding

Figure 6 shows three Secret Imageries that need to be unseen in RGB plane.

10.48047/jocaaa.2024.32.01.24

Figure 7: Stego Images (Stego ImageR, Stego ImageG, and Stego ImageB)

Figure 7 shows Stego Images achieved after inserting the Stealthy photographs within shelter image.

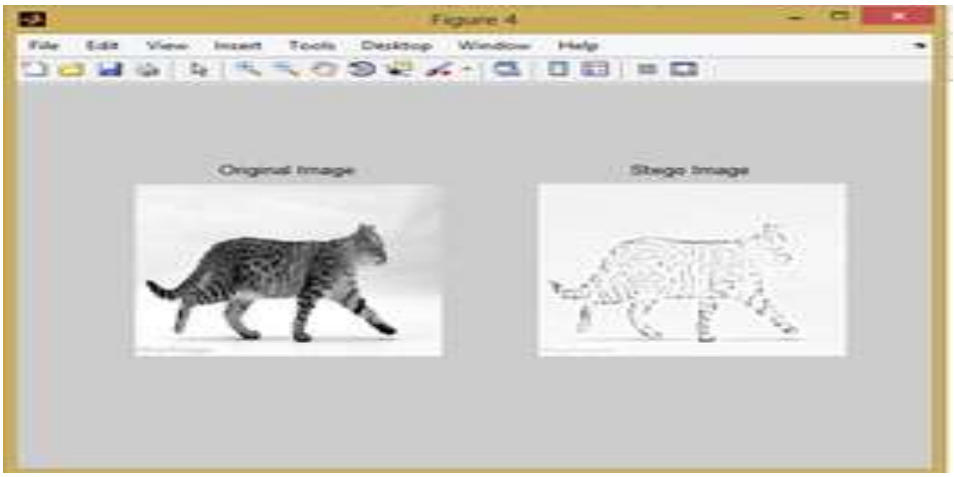

Figure 8: Cover Photograph and Stego Image

Figure 8 shows the Original and Stego Image

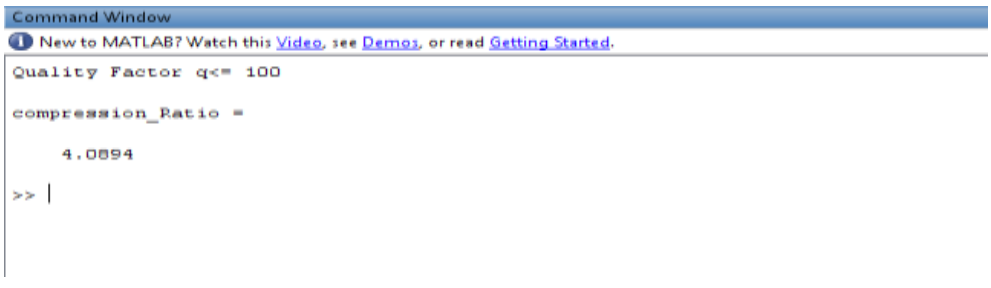

Figure 9: Quality Factor vs. Compression Ratio

Figure 9 shows how compression Ratio affects Image quality.

10.48047/jocaaa.2024.32.01.24

Parameters to Measure the Quality of Recovered Secret Image

1. Compression Ratio: Quality of recovered secret image depends on compression ratio used to create Stego Image as shown in table 5.1. Quality of image decreases as the compression ratio increases. We get 100% quality at compression ratio 5.9823.

2. Signal to Noise Ratio: Sharpness of recovered secret image is controlled by SNR parameter. We get 100% quality for image restoration at SNR 21.1475

Table 1: Quality Measurements of Recovered Secret Image

Parameters	Quality Vs C.R		Quality Vs SNR	
	10	70.6207	10	21.0982
	20	53.0084	20	21.1634
Proposed	30	44.0233	30	21.1699
Technique	40	38.1689	40	21.1823
	50	33.7931	50	21.1785
	60	30.090	60	21.1855
	70	25.2062	70	21.1930
	80	19.7101	80	21.2020
	90	12.7271	90	21.1929
	100	5.9823	100	21.1475

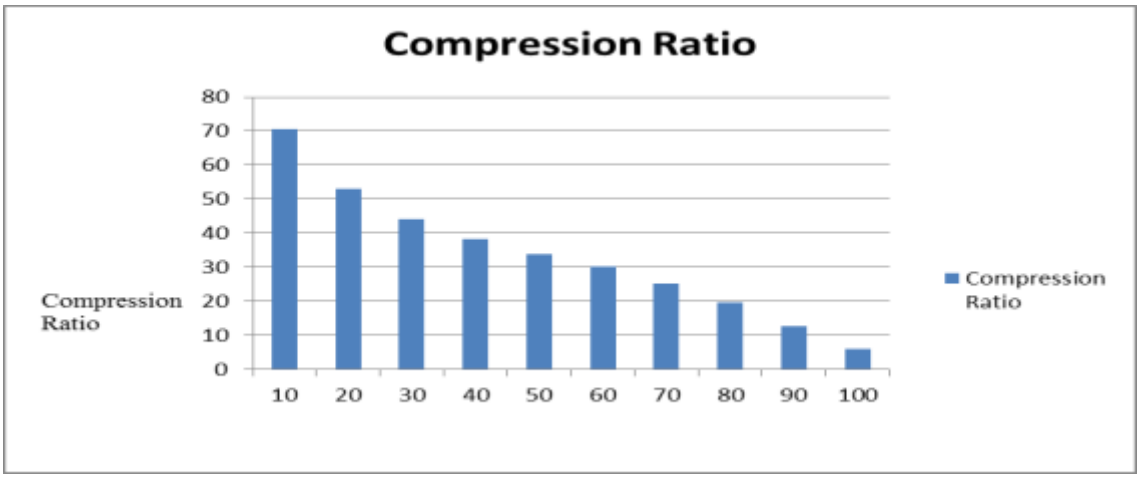

Figure 10: Quality of Recovered Secret Image vs. Compression Ratio

10.48047/jocaaa.2024.32.01.24

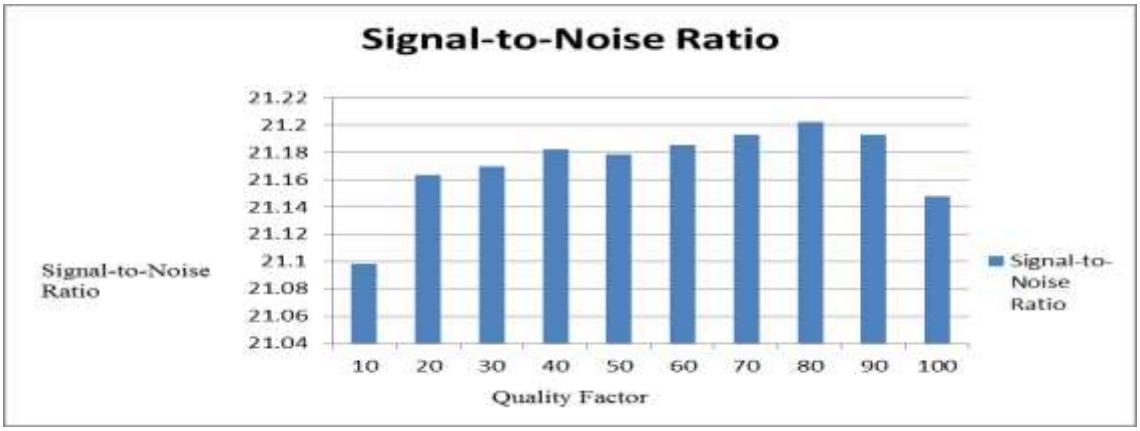

Figure 11: Quality of Recovered Secret Image vs. Signal-to-Noise Ratio

CONCLUSION AND FUTURE SCOPE

Modern advanced correspondence has grown to be an important component of architecture; many purposes are Internet-based, and occasionally it is desired that the correspondence be made safe. To achieve this goal, two techniques are available: steganography and cryptography. In this demonstration, many sophisticated Steganography techniques are used to create a hidden inserted representation that is undetectable from the original snapshot taken with natural eyes. A close study is conducted to demonstrate the planned system's feasibility. The Quality Factor, Compression Ratio, and Signal-to-Noise Ratio have been used to assess the suitability of the presented solutions. To accommodate the largest load, the LSB technique has been used. To get Stego Entity, the entire load is inserted into the shelter image. DCT transforms the Stego Entity into a recurrence region in the three-dimensional planetary. Using track size encoding, a secure Stego object is gathered and packaged. Change (DCT) of Cover Picture includes the installation procedure. These actions provide sufficient safety. Then it uses Huffman encoding for security. Future study will involve increasing the approach for audiovisuals that has been suggested and altering the strategy that has been put forward to enhance image quality by raising SNR and lowering MSE. In order to improve the security of the message, we must develop steganography procedures that allow us to embed information that is equal to or more than that available through present techniques without sacrificing the quality of the Stego image.

REFERENCES

[1] Hon-Hang Chang, “A High Payload Steganography Scheme for Color Images Based on BTC and Hybrid Strategy”, Taiwan, ROC, 2015

[2] G. Arun Karthick, K. Kavitha, V. Sivakumar, D. Surender, “A Hybrid Method for Covert Communication Using Steganography and Image Fusion”, International Journal of Advances in Engineering & Technology, Vol. 7, No. 2, pp. 410-415, 2014

[3] Mazhar Tayel and Hamed Shawky, “A Proposed Assessment Metrics for Image Steganography”, International Journal on Cryptography and Information Security (IJCIS), Vol. 4, No. 1, 2014

[4] Saleh Saraireh, “A Secure Data Communication System Using Cryptography and Steganography”, International Journal of Computer Networks & Communications (IJCNC) Vol. 5, No.3, 2013

[5] Kiran Parmar and Rahul Kher, “A Comparative Analysis of Multimodality Medical Image Fusion Methods”, Sixth Asia Modeling Symposium, 2012

[6] Dr. Mohammed Nasser Hussein Al-Turfi, “Text Realization Image Steganography”, International Journal of Engineering (IJE), International Journal of Engineering (IJE), Vol. 6, No. 1, 2012

[7] Shadi AlZubi, Mhd Saeed Sharif, Naveed Islam, and Maysam Abbod, “Multi-Resolution Analysis using Curvelet and Wavelet Transforms for Medical Imaging”, IEEE, 2011

[8] Jigar Makwana, S.G Chudasama, "Dual Steganography: A New Hiding Technique for Digital Communication", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 5, No. 4, 2016

[9] A. Soria-Lorente, S. Berres, "A Secure Steganographic Algorithm Based on Frequency Domain for the Transmission of Hidden Information", Hindawi Security and Communication Networks Vol. 2017, Article ID 5397082, 2017

10.48047/jocaaa.2024.32.01.24

[10] Kamaldeep Joshi , Swati Gill, "A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image", Hindawi Journal of Computer Networks and Communications Volume 2018, Article ID 9475142, 2018
[11] Eugenijus Margalikas and Simona Ramanauskaitė, “Image steganography based on color palette transformation in color space”, EURASIP Journal on Image and Video Processing, 2019