# EFFECTIVENESS OF PERFORMANCE EVALUATION PARAMETERS IN CONTRAST WITH IMAGE STEGANOGRAPHY

**Mr. Rohit Kapoor[1] Assistant. Professor,**

**Lucknow Public College of Professional Studies Lucknow, U.P., India.**

**Mr. Ajay Kr Gupta[2] Assistant. Professor,**

**Lucknow Public College of Professional Studies Lucknow, U.P., India.**

**Prof. Ajay Kr Bharti[3] Professor,**

**Department of Computer Science and Engineering,**

**Babu Sunder Singh Institute of Technology and Management, Lucknow, U.P., India.**

**KEYWORDS**

STEGANOGRAPHY, PAYLOAD, ROBUSTNESS.

**ABSTRACT**

Steganography refers to the act of hiding information within another medium in such a way that its existence is undetectable to the naked eye. Within the realms of computers and electronics, a file, communication, pictures, or video may be hidden inside of secondary medium. Steganography's primary objective is to ensure that the message's contents are not discernible to anybody other than the intended receiver. This concealed information may be written, visual, auditory, or any combination thereof. The data's privacy may be considerably enhanced by adjusting steganography settings. These settings are designed to be as stealthy as

possible while yet allowing for safe information concealing through a carrier image. When employing image Steganography, the size of the carrier picture is the primary consideration. More information may be concealed in a bigger picture. The quantity of storage space required, however, should not be ignored. If the picture is too tiny, it may not save all the information, jeopardising data security. The second variable is the nature of the information that has to be concealed. In order to conceal their true nature from prying eyes, many forms of data need unique steganographic approaches. Although it's simple to conceal text and pictures inside an image's pixels, more complex methods may be required to conceal audio and video information. The third factor is the robustness of the encryption scheme used to conceal the information. This is crucial because it assures that the concealed information will stay safe in the event that the carrier image is compromised. A powerful encryption method, such as AES or RSA, should be employed to safeguard the information. The amount of data security required is the fourth factor to think about. Multiple levels of encryption and steganography settings may be required to assure data security, depending on the sensitivity of the data. The term "payload" is used to describe the concealed information in a steganographic picture or message. The payload might be anything from text to a picture to a movie. The payload is concealed by manipulating the image's least important bits. How much information may be concealed in a picture is proportional to its size and

quality. More information may be concealed in a picture if it is both bigger and of better quality. Finally, the amount of time and energy required to retrieve the secret data should be taken into account to prevent it from being recovered or decoded by an unauthorised party. Digital signatures and authentication tokens are two examples of potential extra security measures that may be needed. Using a picture Steganography procedure with the right settings, the information may be safely concealed inside an unassuming picture. Using this method, sensitive data may be sent safely and effectively. The goal of picture steganography is to conceal data inside an image in a manner that evades conventional analysis. Methods including encryption, watermarking, and digital signatures are used to secretly insert the data into the picture. In this study, we'll look at the several metrics that may be used to assess an image steganography scheme's efficiency. The capability of the picture steganography technique is the primary variable to examine. This measures how much information can be cloaked in one picture. The capacity of the scheme varies substantially depending on the nature of the data being concealed and the degree of protection required. The greater the amount of information that can be concealed inside a picture, the safer the system is expected to be. The scheme's resilience is the second important factor. This relates to how well the scheme holds up against common assaults like compression, noise, and cropping. A strong scheme can defend against these kinds of assaults while still

protecting the confidentiality of the secret information. The scheme's security is the third factor to think about. This relates to how well the strategy guards the secret information from prying eyes. Examining the kind and strength of encryption used may provide us some insight into this. The more robust the encryption, the harder it will be for an adversary to decipher the secret information. The scheme's practicality is the fourth important factor. This relates to how simple it is to embed and extract data from a picture using the technique. Users are more likely to embrace a user-friendly scheme, increasing the system's effectiveness in hiding data. The scheme's price tag is the fifth and last factor to think about. The expense of enacting and continuing to run the plan is meant here. Users are more inclined to accept a strategy that is also cost-effective. In conclusion, picture steganography is a reliable strategy for concealing information in visual media. The efficiency of an image steganography scheme may be evaluated using the parameters mentioned in this work, allowing the user to choose a scheme that provides the level of security they need.

## 1. INTRODUCTION

Steganography, or the practice of concealing information in an image, is frequently used for both privacy and security reasons. The objective of steganography is to secretly transmit data by altering a picture. Hidden information is embedded into digital photos without altering their appearance. As far as the naked eye is concerned, the embedded data shouldn't be there. The best steganographic methods will keep the image's aesthetic appeal while concealing sensitive information.

Evaluating the efficiency of the image's steganography methods utilised is vital for assuring the security and secrecy of the concealed data. Comprehensive assessment criteria must be used for any examination of picture steganography techniques to be considered complete. Common measures take into account things payload, reliability, invisibility, and safety. Payload refers to the quantity of info that can be effectively disguised in a picture. Images are considered robust if they can survive being subjected to a wide range of methods of image processing without losing any of the concealed information. The level of imperceptibility achieved by a given steganographic technology is a measure of how much of a change in perception it induces. Security refers to the capacity of the steganographic mechanism to withstand a variety of efforts made by unauthorised parties to gain access, such as assaults launched by cybercriminals or malicious software. Careful evaluation of these characteristics is vital in ensuring the efficiency of picture steganography methods, which may offer high-security protections for highly sensitive information.

## 2. NEED OF IMAGE QUALITY PARAMETERS

Image quality metrics are essential in the research, development, and assessment of algorithms for digital image processing. In order to quantify the efficacy of picture steganography methods, a number of assessment factors have been developed. The use of assessment criteria to measure and enhance the performance of picture steganography algorithms is becoming more important. In terms of the information concealment method known as steganography, the quality and resilience may be determined with the use of evaluation parameters. Capacity, stego-image quality, stego-image security, message concealment and extraction speed, and file-format compatibility are all crucial assessment aspects in picture steganography. The efficacy of the picture steganography technology cannot be determined without assessment criteria. In addition to improving our understanding and development of picture steganography, parameters allow us to evaluate and contrast various approaches. Safe and efficient transfer of sensitive information through digital pictures relies heavily on the usage of assessment criteria.

Hidden data embedding has the potential to degrade picture quality, however. In steganography, it's important to think about the following aspects of picture quality:

The total size of the stego-image is dependent on the amount of concealed data. Steganography attempts to conceal images while leaving as little of a trace as possible. Lossless compression and other methods may be used to shrink the size of the secret information.

Image artefacts such as noise and distortion might be introduced during the embedding process. It is crucial to control these factors and make sure the embedded data does not negatively affect the picture's visual integrity so as to preserve image quality.

## 3. QUALITY PARAMETERS & ITS TYPES

Steganography refers to the technique of secretly transmitting information by embedding it in a picture or other kind of media. In order to preserve picture quality while embedding hidden data, there are a number of factors to think about while working with steganography in photos. Some crucial considerations include:-

Payload: The quantity of secret information that may be kept inside a picture is known as its "embedding capacity or Payload". Increasing the capacity for embedding hides more information but may dramatically reduce the picture quality. It is critical to strike a balance between storage space and final picture quality.

Format of the Image: Some picture formats are found more resistant to steganographic methods than others. In contrast to lossy formats like JPEG, which create compression artefacts that may impact both the apparent picture quality and the hidden data, lossless formats like PNG or BMP are able to maintain the embedded data without any loss.

The resolution of a picture is the number of horizontal and vertical pixels per inch that make up the image. When information is embedded in a picture with a greater resolution, it may be possible to make less obvious adjustments. Bigger photos,

however, have bigger file sizes, which might signal malicious intent. The image's resolution is the total number of individual pixels. For the purposes of data concealing, higher resolution photos are favoured due to their superior visual quality. Using a high-resolution image allows for greater room to incorporate concealed data while still maintaining a natural appearance. High-resolution photographs have the potential drawback of being more cumbersome to transmit due to their greater file sizes.

Method of Encoding There is a wide range of steganographic algorithms and methods available, each with its own potential impact on picture quality. Depending on the technique, the least important bits of a picture may be changed, the colour scheme may be adjusted, or the spatial frequency domain may be shifted. The quality of the concealed information and the picture as a whole may be affected by the method used. The effectiveness of the embedding process is an additional consideration. In order to be useful and efficient, the time it takes to hide information inside a picture must be acceptable

Robustness or Tolerance for Background Noise and picture Manipulation:- The term "robustness" is used to describe how well the concealed information holds up after being subjected to a number of transformations during image processing. A strong steganographic method will be able to withstand these manipulations without compromising the quality of the concealed data or the picture. A successful steganographic method will remain resilient in the face of background noise and picture manipulations like cropping, resizing, and compression. Standard image processing techniques should not affect the concealed information. To preserve picture quality, it is essential that obvious distortions brought about by embedding be kept to a minimum.

Qualities of the Human Visual System (HVS): Designing steganographic approaches that are less likely to be discovered requires an understanding of the limits and features of the human visual system. Data may be hidden with little influence on

picture quality by taking advantage of human perception's flaws, such as our inability to notice subtle shifts in colour channels.

One must strike a fine balance between data concealing and picture fidelity preservation in order to achieve high grade steganography. The amount of privacy required, the nature of the data to be hidden, and the final use of the steganographic picture all play a role in determining the exact parameters to be taken into account.

Steganalysis methods use statistical analysis of an image's characteristics to reveal any concealed information. Steganography techniques should make the stego-image's statistical features almost identical to those of the original, unmodified picture in order to avoid detection.

The effectiveness of the embedding process is an additional consideration. In order to be useful and efficient, the time it takes to hide information inside a picture must be acceptable.

It's important to remember that various steganographic methods place varying amounts of emphasis on various aspects of picture quality. Researchers and experts in the field of steganography are always trying to find new ways to enhance the practice's efficacy and safety

Image steganography is a process of hiding text, files, or images within an image without changing the original image's visual appearance. Evaluation of steganographic techniques is necessary to ensure their effectiveness in terms of image quality, message capacity, robustness, security, and detection-resistance. Evaluation parameters for steganography techniques in images include capacity, distortion, security, robustness, and complexity. Capacity is the amount of data that can be hidden in an image with minimum distortion[1]. Distortion is the difference between the original and the stego image. Security is the likelihood of discovering the hidden message. Robustness refers to the sensitivity level of the steganographic method to changes like compression, cropping, or resizing. Complexity is the level of effort needed to embed a message and extract it from the stego image. The

evaluation of steganographic techniques is a crucial process to determine their effectiveness in reliably transmitting hidden messages with minimum distortion while ensuring strong protection against unauthorized access or detection.

## 4. MAIN HIGHLIGHTS OF MSE

The Mean Squared Error (MSE) or Mean Squared Deviation (MSD) calculates the average value of the squared errors. The error can be defined as the discrepancy between the estimated outcome and the estimator. The function in question pertains to risk and involves the evaluation of the expected value of the squared variable**.**The Mean Squared Error (MSE) is widely recognized as the predominant estimator for quantifying image quality metrics. The metric in question is a comprehensive reference measure, with lower values indicating superior performance.

### 4.1. MAIN HIGHLIGHTS OF PSNR

- PSNR is based on pixel-by-pixel comparison of two images, which may not reflect the human perception of image quality.
- PSNR does not capture structural distortions in images, such as blurring, blocking, ringing, etc.
- PSNR can be easily fooled by changes in brightness and hue that have little impact on visual quality.
- PSNR depends on the maximum possible pixel value of the image. For 8-bit images, this is 255. For other bit depths, this value changes accordingly.
- PSNR is widely used in image processing research and applications, such as image compression, restoration, denoising, super-resolution, etc.

## 5. COMPARATIVE ANALYSIS OF DIFFERENT IMAGE QUALITY METRICS

In this study, we present a new approach to evaluating image quality using structural similarity at the mean edge. The MESSIM method addressed the limitations of MSSIM on blurred and Gaussian noise images by placing a greater emphasis on edge resemblance during structural similarity measurement. Through improved

consistency with subjective perception, experimental study has demonstrated the superior quality of MESSIM images over a broad spectrum of kinds.

**TABLE 1**

| Steganography Scheme | Capacity | PSNR(dB) |
|---|---|---|
| Wu & Tsai [2] | 1234394 | 41.25 |
| Yang & Wang | 199608 | 41.58 |
| Mandal & Das [3] | 1234394 | 40.21 |
| Swain [4] | 1341192 | 46.17 |

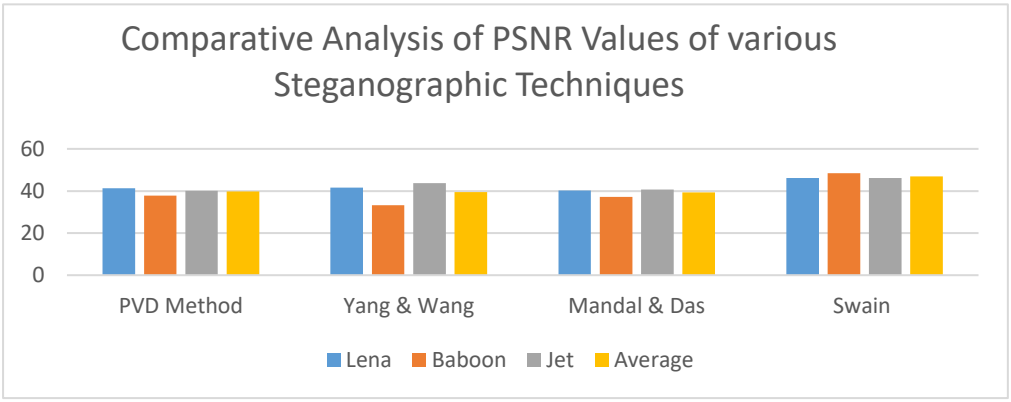


**FIGURE 1 COMPARATIVE ANALYSIS OF PSNR**

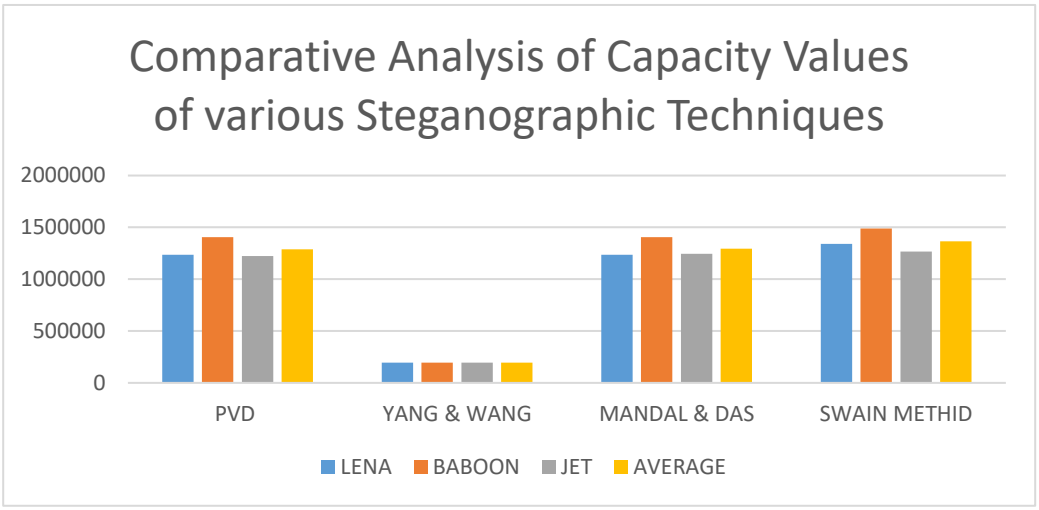


**FIGURE 2 COMPARATIVE ANALYSIS OF CAPACITY VALUES**

## 6. CONCLUSION

The goal of this research was to investigate and evaluate the effectiveness of a variety of image quality criteria that are currently in use. The estimation of various image quality metrics, such as PSNR, SNR, and MSE, is a crucial task in digital image processing. This is because these estimations give a more effective method for evaluating image quality and finding ways to improve it. Methods for evaluating the quality of an image are still in development; they are intrinsically tied to the reason for doing so, and so can only answer specific questions, such as how reliable the image generation system is, how the image will be perceived by a human observer, or what kinds of disturbances are introduced in the image through compression, transmission, or processing.

At the present time, there is no universal system of image quality parameters that can be observed. Image quality factors are closely related to how well an imaging system works, but they can't be used instead because the human visual system is too complicated. One of the most important factors that go into determining image quality is the HVS performance analysis that is done. Image quality is typically believed to be a measure of overall visual impact; nevertheless, the way in which individuals interpret visual information is contingent upon a wide variety of elements, including sharpness, contrast, colorfulness, and individual preferences. The perceptual gap has been quantified using a number of scales, including PSNR, SSIM, and the picture histogram[5].

PSNR has been utilised extensively in numerous sorts of image processing studies around the world, making it a popular measurement tool. However, PSNR has a limitation as a signal-fidelity gauge because of how strongly it correlates with opacity in steganographic pictures. Tests conducted for this study show that SSIM, which is based on the visual system of humans, is more sensitive than PSNR to detecting distortions brought on by the insertion of messages into steganographic colour images.

## 7. REFERENCES


- U. Sara, M. Akter, and M. S. Uddin, “Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study,” *J. Comput. Commun.*, vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.
- D. C. Wu and W. H. Tsai, “A steganographic method for images by pixel-value differencing,” *Pattern Recognit. Lett.*, vol. 24, no. 9–10, pp. 1613–1626, 2003, doi: 10.1016/S0167-8655(02)00402-6.
- J. K. Mandal, “Steganography Using Adaptive Pixel Value Differencing(APVD) of Gray Images Through Exclusion of Overflow/Underflow,” pp. 93–102, 2012, doi: 10.5121/csit.2012.2211.
- S. G. Pradhan Anita, “Adaptive PVD steganography using horizontal, vertical, and diagonal edges in six-pixel blocks,” *Secur. Commun. Networks*, vol. 2017, 2017, doi: 10.1155/2017/1924618.
- Z. Wang and A. Bovik, “Structural similarity based image quality assessment,” *Digit. Video Image Qual.*, 2005, [Online]. Available: http://ece.uwaterloo.ca/~z70wang/publications/SSIM_Chap.pdf.
- [G. Swain and S. K. Lenka, “Steganography using two sided, three sided, and four sided side match methods,” *CSI Trans. ICT*, vol. 1, no. 2, pp. 127–133, 2013, doi: 10.1007/s40012-013-0015-3