EFFECTIVENESS OF PERFORMANCE EVALUATION PARAMETERS IN CONTRAST WITH IMAGE STEGANOGRAPHY

[1]ROHIT KAPOOR

[1]ASST PROFESSOR, LUCKNOW PUBLIC COLLEGE OF PROFESSIONAL STUDIES

KEYWORDS

STEGANOGRAPHY, COMMUNICATIONS, LEAST SIGNIFICANT BIT, STRUCTURAL SIMILARITY INDEX, QUALITY ASSESSMENT

ABSTRACT

Steganography, in particular regarding images files, has arisen in this era of important digital communication as the requisite to firm safety information. In this study, performance evaluation metrics have been implemented on various image steganography algorithms to evaluate their performance. It also discusses the trade-off among invisibility of embedded data, payload efficiency, and immunity to attacks. Aim: To present a complete assessment of multiple steganography methods, with an emphasis upon the vital performance parameters determining their robustness.

1. INTRODUCTION

As the demand for secure communications and the number of cyber threats have proliferated, so too has research into steganography, a technique for hiding data within other data. Since picture files are very widely used in digital communication, image steganography has also become one of the most popular forms of steganography. By analyzing significant variables such processing efficiency, resilience, payload capacity, and imperceptibility, this study aims to compare the effectiveness of performance evaluation criteria in contrast to image steganography. Steganography is a sophisticated technique of hiding text in an image, in a way that ensures secure transmission of information while not exposing that such information is being passed. The word steganography is based on two Greek roots, steganós, “covered,” and graphein, “writing,” so

steganography means covered writing, and that's exactly what it is. Compared to the cryptography, which concerns the process to make one's data nonsensical without an associated key, using steganography we are focusing on hiding the existence of the information, which is why it is an alternative on a dirty communication it is hidden in plain sight. With the rise of digital culture, ensuring the safeguarding of sensitive information is essential and image steganography has some major use cases to offer. It is used in such domain as digital rights management, cybersecurity, military intelligence. In the cyber-security milieu, it is used to protect sensitive data, embedding it into graphics that may appear harmless but conceal sensitive data, as well as preventing unauthorized access. Steganography is used to communicate encrypted messages discreetly in military operations, avoiding detection of sensitive information exchanged. This technique could also be used by activists and dissidents to attack significant information without detection

2. BACKGROUND

The focus of picture steganographic element is to conceal information from unwanted eyes by inserted it inside of graphic file in undetectable way. These techniques generally fall under mask-based methods, transform-domain methods, and LSB (Least Significant Bit) insertion. Each of these methods has advantages and disadvantages that influence their effectiveness. The field of secure communications has seen great interest in a technique known as image steganography, which involves hiding secret data within an image file. These methods are comprehensively assessed using a diverse set of performance criteria to evaluate efficiency, quality, and safety. Here, we present a review of literature that synthesizes major findings from more recent work that tests steganographic systems on critical aspects on payload capacity, image quality metrics and security mechanisms.

- **PERFORMANCE INDICATORS**

The field of steganography is mostly evaluated in terms of its PSNR and MSE parameters. Akhtar et al. The proposed methods in (2013) were improvements over the least significant bit (LSB) method which showed better peak signal to noise ratio (PSNR) values against regular implementations. They showed that using one of the existing algorithms of 'bit-inversion' could increase the invisibility of hidden data when high quality images were used. Dou et al. in a comparative study,

demonstrate that the PSNR provided by BMP images is typically superior to the one provided by JPEG and PNG from a specific image (2019). One.

Apau et al. performed an extensive organised benchmark (2024) examined several image steganography systems, and their robustness to statistical steganalysis attacks. This test verified that performance measures like PSNR and MSE play an important role in evaluating the embedded information's invisibility while delivery quality of picture is preserved at the ideal level [4]. Four. Advanced methods, such as machine learning or deep learning, are becoming more relevant thanks to their enhanced performance in preserving image quality along with a increase in security rates as shown by the results.

- **SECURITY CONSIDERATIONS**

One of the main concerns in steganography is the security (degree of robustness of techniques against discovery). Soni et al. (2015) analysed various steganographic techniques and their vulnerabilities to steganalysis. Traditional methods like LSB are increasingly challenged by detection algorithms, and this has rendered the need for the development of more secure alternatives. Two. Their findings highlighted the importance of further investigation into resilient concealment strategies that are resistant to modern detection techniques.

Hemalatha et al. (2012) introduced a secure concealment process using an Integer Wavelet Transform (IWT) within the high-frequency sub-bands of images. This approach demonstrated improved PSNR values and high-intensity resistance against noise and signal processing operations, representing a suitable solution for the increase of both capacity and security. Two.

- **COMPARATIVE ANALYSES**

This comparative assessment is crucial in order to understand the advantages and disadvantages of various types of steganographic techniques. Rafiqi et al. (2022) stated that the literature review mainly described the numerous encryption techniques based on various algorithms whose performance has been assessed according to parameters, such as peak signal to noise ratio (PSNR), mean squared error (MSE), and structural similarity index (SSIM). Although conventional LSB methods are preferred because of their simple implementation, wavelet transforms and machine learning based solutions give much better performance in terms of security and capacity [16, 18]. Furthermore, Punidha et al. In 2022, Model proposed a reversible data hiding using integer wavelet transformations, which is

more significant than the other reversible data hiding methods on visual quality and storage capacity. The continuous requirement for advancement in steganography to overcome your future informatSecurity is emphasized in this comparative study.

2.1. IMAGE STEGANOGRAPHY

The goal of picture steganography is to conceal data from prying eyes by inserting it into a graphic file in an undetectable manner. Common approaches include mask-based techniques, transform-domain methods, and Least Significant Bit (LSB) insertion. There are benefits and drawbacks to each of these methods that affect how well they work

2.2. PERFORMANCE EVALUATION PARAMETERS (PEM)

Image steganography, which involves hiding information within digital images, faces a number of challenges that can affect its efficiency and reliability. It is important to understand these challenges because they affect the selection of data hiding techniques as well as the security of the data being protected. The following PEP

- **EMBEDDING CAPACITY**

Providing a high capacity of embedding without degrading the quality of the cover image is one of the main problems in the area of image steganography. How much data can be hidden in an image depends on the size and format of the image. Most techniques that enhance embedding capacity also cause visible distortions in the image that can make the embedded data more easily detected.

As noted by Ghoul et al. (2023), there exists a fine balance between embedding capacity, imperceptibility, and security, improvement of one aspect generally degrades another, leading to a tough trade-off for practitioners.

- **IMPERCEPTIBILITY**

Preserving imperceptibility, meaning steganography requires the hiding of data while not changing the way the cover looks, is critical.

Steganography's aim as a means of secret communication is lost if the alterations to the image are too visible. Although very simple, common techniques, such as Least Significant Bit (LSB), can be relatively easy to find if not executed well. The other challenge is to embed information to make it so that it is invisible to the naked human eye but also is robust against detection algorithms.

- **SECURITY**

But there is other serious concern — security of hidden texts. In addition to hiding data, image steganography must also keep data safe from various types of attacks like statistical analysis, steganalysis, etc., which try to find hidden messages. Although, multiple ways to improve the security including randomization and encryption techniques have been introduced (Subhedar & Mankar, 2015), this provides extra complexity in the embedder and can impact performance.

- **ROBUSTNESS AGAINST ATTACKS**

Steganographic algorithms=/techniques have to be strong enough to resist against many types of attacks software, such as compression, cropping, and/or other image processing techniques that would uncover or alter the hidden data. The challenge is to create methods that remain robust under these conditions whilst still achieving strong data hiding. Many modern techniques are known to lack robustness [4], especially against common lossy compression algorithms used in image formats (e. g. JPEG.

- **COMPLEXITY OF IMPLEMENTATION**

Developing efficient steganographic methods can be significantly harder than what it may seem, as it demands in-depth know-how of data encoding procedures, as well as the digital visual aspect. Errors that will occur on the implementation that will set steganography process ineffective comes from this complexity. Also, with the technological advances, the nature of image processing is changing continuously thus the method after some time becomes obsolete and detection technique are changing too Which again increases the task of the professionals to keep up with the latest techniques.

Such problems indicate the importance of continuous research and development work over image steganography domain. It is necessary to address these issues for better implementation of steganographic techniques for secret data embedding.

- **QUALITY ASSESSMENT TECHNIQUES FOR EVALUATING IMAGE QUALITY AFTER STEGANOGRAPHY**

One primary problem is determining how to maintain the visual integrity of digital photographs after data embedding, which is important for image steganography, a process that consists of embedding hidden data into images. Several methods are employed after steganography to estimate the picture quality; two of the most

common are the Structural Similarity Index Measure (SSIM) and the Peak Signal-to-Noise Ratio (PSNR).

- **PEAK SIGNAL-TO-NOISE RATIO (PSNR)**
  PSNR is a widely used metric for comparing the quality of the original cover pictures and the reconstructed pictures. It is represented by following parameters: -

$$\text{PSNR} = 10 \cdot \log_{10} \left(\frac{MAX^2}{MSE} \right)$$

- **MEAN SQUARE ERROR-**
  MSE measures the squared pixel difference between the original image and the stego image. Since the embedding process adds less distortion, a larger PSNR means better quality. But PSNR may not suffice to capture all the subtle differences humans perceive.

$$\text{MSE} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} [I(i,j) - K(i,j)]^2$$

  -

- **SSIM STANDS FOR STRUCTURAL SIMILARITY INDEX MEASURE**.
  One important metric that measures picture quality by evaluating the amount of structural information thought to have changed is SSIM. Unlike PSNR, which simply looks at the individual difference in pixels, SSIM considers structural information, contrast and brightness for a more comprehensive view of image quality. Specifically, SSIM has a range of -1 to 1, where a value of 1 indicates a perfect structural similarity between the original (or preliminary) and the stego images. It is a great metric for evaluating visual quality since it is closer to how humans perceive visual information. The SSIM can be evaluated using the mentioned formula:-

$$\text{SSIM}(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

- **RELEVANCE OF VISUAL INTEGRITY MAINTAIN THE EMBEDDING DATA**

When embedding data, keeping the visual quality high is extremely important for several reasons:

- **Resistance to Detection:** if the changes made to introduce data are too visible and attention-seeking they may be revealed by steganalysis tools. Steganography, though it also involves hiding information, has a different objective, as high quality stego images are less likely to be marked as suspicious, thus keeping the information hidden.
  When applying steganography for secure communication or digital watermarking, keeping visual quality is better addressed and results in user experience leading to the enhanced input. Correct, users expect to see embedded hidden/check data for the visual delights.
- **Robustness against Attacks:** Images that maintain their fidelity post-embedding have improved resilience against various forms of attacks, including compression and cropping. This resilience ensures that embedded data remains unaltered and accessible, even with potential refreshes.
- **Evading Detection**: If the changes made to the embedded data are too obvious, it could attract attention and result in their identification by steganalysis tools. Because of this, high-quality stego photos are seldom flagged as suspicious, while the hidden information remains hidden.
  In apps that use steganography for secure communication or for digital watermarking, the user experience is enhanced when visual quality is preserved. Users expect hidden information to
- **Legal and Ethical Issues:** Maintaining the integrity of visuals while adding data is essential in areas such as copyright protection and digital rights management for compliance with ethical and legal guidelines.
  Several quality evaluation tools, such as PSNR and SSIM, are essential to determine the working of picture steganography techniques. If professionals take care to maintain visual quality when embedding, steganographic systems can become more secure, more user-friendly and the probability of their discovery lowered. From copyright protection to digital rights management, maintaining a sense of visual fidelity whilst weaving together information is crucial in adhering to legal norms and moral principles.
- **Various Methods of Image Steganography**

Image steganography refers to hiding of secret information in digital images.

This ensures that unauthorised users cannot detect the information being hidden.

This article explores various methods of picture steganography, focusing on its mechanisms, advantages, and disadvantages.

- **Least Significant Bit (LSB) Substitution**
  Insert lsb is one of the common method in image steganography. The least meaningful bit of each pixel of the cover image is replaced by bits of the hidden message using this technique. This method is considered simple and practical for implementation. However, since it modifies the least significant bits, it is also susceptible to detection by a statistical analysis that can fairly easily be performed.
- **Transform Domain Methods**
  Transform domain method embeds data into the frequency coefficients of an image rather than directly changing pixel values in the spatial domain. Common techniques include:
  DCT (Discrete Cosine Transform) is used in steganography to change the coefficients of DCT blocks in JPEG images, which significantly improves imperceptibility and robustness against compression attacks compared to the LSB (Least Significant Bit) method.
  Data can be embedded in low and high-frequency components using the Discrete Wavelet Transform (DWT) thus ensures high-level security and low visibility.
- **Statistical„...Techniques**
  Statistical approaches include altering the statistical characteristics of a picture to insert confidential information without perceptible alterations to the visual quality. These methodologies often encompass:The spread spectrum method disperses the cover image's hidden data across a broad frequency range, making it difficult to identify.
  The adaptive approaches make better use of the space provided and reduce visual artefacts by adjusting their embedding strategy according to the local properties of the cover picture.
- **Machine Learning-Based Approaches**
  Deep learning approaches greatly improved the modern steganography techniques CNN-based methods automatically learned the optimal characteristics to embed hidden data into images to improve payload capacity and visual quality. They have outperformed much more conventional methods.

- **Hybrid approaches** can employ their strengths and reduce their weaknesses by combining multiple steganographic approaches LSB has a good- capacity but tissue data it is sensitive for detection, So combining DCT or DWT with LSB gives better results with data capacity and detection less. These hybrid techniques are increasingly popular as the enhance both the security and visual quality. 4. Machine Learning Aided/Facilitated Approaches

Machine learning methods have notably enhanced the recent steganography techniques:

CNN-based methods automatically determine how to embed hidden data into photographs to make the best use of payload capacity and visual quality. They also showed much better performance than more conventional procedures.

Technique	**Domain**	**Payload Capacity**	**Robustness Against Attacks**	**Complexity**	**Image Formats Supported**
Least Significant Bit (LSB)	Spatial	High	Low	Low	All formats (JPEG, BMP, PNG)
Random Pixel Embedding (RPE)	Spatial	Moderate	Moderate	Moderate	All formats
Pixel Value Differencing (PVD)	Spatial	High	High	Moderate	All formats
Discrete Cosine Transform (DCT)	Transform	Moderate	High	High	JPEG, BMP

Discrete Wavelet Transform (DWT)	Transform	Moderate	High	High	JPEG, BMP
Spread Spectrum	Statistical	Low	Very High	High	All formats

TABLE 1: TABULAR FORM COMPARISON OF VARIOUS IMAGE STEGANOGRAPHY TECHNIQUES

Parameters/Technique	Description	Advantages	Challenges	References
1. Peak Signal-to-Signal-to-Noise Ratio (PSNR)	Measures the ratio between the maximum possible power of a signal and the power of corrupting noise.	Simple to calculate; widely used for assessing image quality post-steganography.	Does not correlate well with perceived visual quality; sensitive to noise.	Huynh-Thu & Ghanbari (2008)
2. Structural Similarity Index Measure (SSIM)	Assesses perceived changes in structural information between two images.	More aligned with human visual perception than PSNR; considers luminance and contrast.	Computationally intensive; requires careful interpretation of results.	Wang & Bovik (2006)
3. Image Steganography Techniques	Methods for hiding data within images (e.g., LSB, PVD).	Allows secure communication; can be integrated into various applications.	Risk of detection; potential quality degradation of cover images.	Subhedar & Mankar

4. Adaptive Steganography	Techniques that adjust embedding based on image content to optimize quality and capacity.	Enhances security and imperceptibility by adapting to the cover image's features.	Increased complexity in embedding process; requires advanced algorithms.	Ghoul et al. (2023) DOI:

Analysis of performance evaluation metrics and image steganography methods. This comparative exploration demonstrates the variety of performance evaluation metrics and image steganography techniques, each approach with its strengths and challenges. Performance evaluation methods help in evaluating how valuable an employee is to an organization and how effectively that organization or an employee is performing, while steganography methods simply aim at hiding data in an image without degrading quality.

3. CONCLUSION

Performance evaluation parameters are used to evaluate the quality and security of images containing hidden data using image steganography. Some of those metrics can be payload capacity, image quality measures, and security measures. By considering metrics such as Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM), techniques such as Least Significant Bit (LSB) achieve higher payload and acceptable image quality. Peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM) are used to assess visual fidelity of stego images. Security is a crucial aspect of this process because methods that preserve maximum images quality while encoding data are less expose to being detected. Steganography is challenged by the trade-off between payload capacity, image quality, and security. More advanced metrics that capture perceptual differences and increases robustness against attacks should be the focus of future research.

4. REFERENCES

- Akhtar, N., Johri, P., & Khan, S. (2013). Performance Evaluation of Secret Image Steganography Techniques Using LSB Method for Data and Image Security. *International Journal of Computer Science Trends and Technology*, 6(2), 30-35. DOI: 10.14445/22312803/IJCST-V6I2P30

- Soni, H., Acharya, U.D., & Renuka (2015). A Study and Literature Review on Image Steganography Techniques. *International Journal of Computer Science and Information Technology*, 6(1), 152-158. DOI: 10.5120/ijcsit20150601152
- Rafiqi, M., & others (2022). Quality Evaluation of Image Steganography Techniques: A Heuristics-based Approach. *Journal of Theoretical and Applied Information Technology*, 100(5), 1414-1420.
- Apau, J., & others (2024). Image Steganography Techniques for Resisting Statistical Steganalysis Attacks: A Systematic Literature Review. *Journal Name*, DOI: 10.xxxx/xxxxxx
- Ghoul, S., Sulaiman, R., & Shukur, Z. (2023). A Review on Security Techniques in Image Steganography. *International Journal of Advanced Computer Science and Applications*, 14(6). http://dx.doi.org/10.14569/IJACSA.2023.0140640
- Subhedar, K., & Mankar, V.H. (2015). Current status and key issues in image steganography: A survey. *ResearchGate*. https://doi.org/10.1109/ICGCIoT.2015.7405888
- Wang, Z., & Bovik, A.C. (2006). Mean Squared Error: Love It or Leave It? A Perspective on Image Quality Assessment. IEEE Transactions on Image Processing, 13(4), 600-612. DOI: 10.1109/TIP.2006.871899
- Huynh-Thu, Q., & Ghanbari, M. (2008). Scope of Validity of PSNR in Image Quality Assessment. Electronic Letters, 44(13), 800-801. DOI: 10.1049/el:20081012
- Wang, Z., & Bovik, A.C. (2003). A Universal Image Quality Index. IEEE Signal Processing Letters, 9(3), 81-84. DOI: 10.1109/LSP.2002.1017620
- Avcıbaş, I., Memon, N., & Sankur, B. (2003). Steganalysis Using Image Quality Metrics. IEEE Transactions on Image Processing, 12(2), 221-229. DOI: 10.1109/TIP.2003.809197
- Huynh-Thu, Q., & Ghanbari, M. (2008). Scope of Validity of PSNR in Image Quality Assessment. *Electronic Letters*, 44(13), 800-801. DOI: 10.1049/el:20081012
- Wang, Z., & Bovik, A.C. (2006). Mean Squared Error: Love It or Leave It? A Perspective on Image Quality Assessment. *IEEE Transactions on Image Processing*, 13(4), 600-612. DOI: 10.1109/TIP.2006.871899

- Subhedar, K., & Mankar, V.H.(2015). Current status and key issues in image steganography: A survey, *ResearchGate*. DOI: 10.1109/ICGCIoT.2015.7405888
- Ghoul, S., Sulaiman, R., & Shukur, Z.(2023). A Review on Security Techniques in Image Steganography,*International Journal of Advanced Computer Science and Applications*, 14(6). DOI: 10.14569/IJACSA.2023.0140640