**LSB Embedding Steganography : A Comparative Analysis of 2-Bits and 3-Bits Techniques**

*Report submitted to the SASTRA Deemed to be University*

*as the requirement for the course*

**ECE300: MINI PROJECT**

*Submitted by*

**JAWAHAR N**

**(Reg. No.: 125160021)**

**DEEPAK D M**

**(Reg. No.: 125160086)**

**KRITHIK NAVEEN A R**

**(Reg. No.: 125160029)**

**APRIL 2024**



**SCHOOL OF ELECTRICAL & ELECTRONICS ENGINEERING**

**THANJAVUR, TAMIL NADU, INDIA – 613 401**



**SCHOOL OF ELECTRICAL & ELECTRONICS ENGINEERING**

**THANJAVUR – 613 401**

**Bonafide Certificate**

This is to certify that the report titled “**LSB Embedding Steganography : A Comparative Analysis Of 2-Bits And 3-Bits)**” submitted as a requirement for the course, **ECE300: MINI PROJECT** for B.Tech. ELECTRONICS & COMMUNICATION ENGINEERING programme, is a bonafide record of the work done by **Mr. Jawahar N(Reg. No.125160021**), **Mr. Krithik Naveen A R(Reg. No.125160029**) and **Mr. Deepak D M(Reg. No.125160086**) during the academic year 2023-24, in the School of ELECTRICAL & ELECTRONICS ENGINEERING, under my supervision.

**Signature of Project Supervisor :**

**Name with Affiliation :** Dr. Lakshmi .C / AP-III

**Date :**

Project *Viva voc*e held on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Examiner 1 Examiner 2**



**SCHOOL OF ELECTRICAL & ELECTRONICS ENGINEERING**

**THANJAVUR – 613 401**

**Declaration**

We declare that the report titled “**LSB Embedding Steganography : A Comparative Analysis Of 2-Bits And 3-Bits)**” submitted by us is an original work done by me/us under the guidance of **Dr. Lakshmi .C, AP-III, School of Electrical and Electronics Engineering, SASTRA Deemed to be University** during the sixth semester of the academic year 2022-23, in the **School of Electrical and Electronics Engineering**. The work is original and wherever We have used materials from other sources, We have given due credit and cited them in the text of the report. This report has not formed the basis for the award of any degree, diploma, associate-ship, fellowship or other similar title to any candidate of any University.

**Signature of the candidate(s) :**

**Name of the candidate(s) :** Jawahar N

Krithik Naveen A R

Deepak D M

**Date :**

**Abstract**

This research delves into the LSB (Least Significant Bit) embedding technique, specifically exploring the impact of 3-bits and 2-bits LSB embedding in. The primary objective is to assess the perceptual transparency levels of the steganographic images, ensuring they do not fall below 30dB. The study involves a comprehensive analysis of the perceptual transparency achieved with 3-bits and 2-bits embedding in images. A comparative evaluation will be conducted to ascertain whether one technique is superior to the other in maintaining image quality and perceptual transparency. The investigation aims to provide insights into the optimal embedding bit-depth for each image size, considering factors such as information capacity and transparency. In this implementation, data hiding within images is achieved through LSB embedding, where the least significant bits of pixel values are replaced with binary data derived from text. To enhance security and randomness, a chaotic equation is utilized to generate random numbers for selecting the embedding locations. This technique ensures imperceptibility of the hidden data, maintaining the visual quality of the image while providing a covert means of data transmission.

**Specific Contribution**

* Writing code in MATLAB for implementing 2 bits LSB masking.
* Implementing a chaotic equation for random number generation based on what the data will be hid in the image.

**Specific Learning**

* LSB masking in image pixels
* Data hiding in image pixels according to chaotic equations
* Implementation of above mentioned in MATLAB

Signature of the Guide Student Reg. No : 125160021

Name : Dr. Lakshmi .C / AP-III Name : Jawahar N

**Abstract**

This research delves into the LSB (Least Significant Bit) embedding technique, specifically exploring the impact of 3-bits and 2-bits LSB embedding in. The primary objective is to assess the perceptual transparency levels of the steganographic images, ensuring they do not fall below 30dB. The study involves a comprehensive analysis of the perceptual transparency achieved with 3-bits and 2-bits embedding in images. A comparative evaluation will be conducted to ascertain whether one technique is superior to the other in maintaining image quality and perceptual transparency. The investigation aims to provide insights into the optimal embedding bit-depth for each image size, considering factors such as information capacity and transparency. In this implementation, data hiding within images is achieved through LSB embedding, where the least significant bits of pixel values are replaced with binary data derived from text. To enhance security and randomness, a chaotic equation is utilized to generate random numbers for selecting the embedding locations. This technique ensures imperceptibility of the hidden data, maintaining the visual quality of the image while providing a covert means of data transmission.

**Specific Contribution**

* Writing code in MATLAB for implementing 3 bits odd rows LSB masking.
* Retrieving the hidden data based on order of the random numbers generated.

**Specific Learning**

* LSB masking in image pixels
* Data hiding in image pixels according to chaotic equations
* Implementation of above mentioned in MATLAB

Signature of the Guide Student Reg. No :125160029

Name : Dr. Lakshmi .C / AP-III Name : Krithik Naveen A R

**Abstract**

This research delves into the LSB (Least Significant Bit) embedding technique, specifically exploring the impact of 3-bits and 2-bits LSB embedding in. The primary objective is to assess the perceptual transparency levels of the steganographic images, ensuring they do not fall below 30dB. The study involves a comprehensive analysis of the perceptual transparency achieved with 3-bits and 2-bits embedding in images. A comparative evaluation will be conducted to ascertain whether one technique is superior to the other in maintaining image quality and perceptual transparency. The investigation aims to provide insights into the optimal embedding bit-depth for each image size, considering factors such as information capacity and transparency. In this implementation, data hiding within images is achieved through LSB embedding, where the least significant bits of pixel values are replaced with binary data derived from text. To enhance security and randomness, a chaotic equation is utilized to generate random numbers for selecting the embedding locations. This technique ensures imperceptibility of the hidden data, maintaining the visual quality of the image while providing a covert means of data transmission.

**Specific Contribution**

* Writing code in MATLAB for implementing 3 bits LSB masking.
* Implementing a chaotic equation for random number generation based on what the data will be hid in the image

**Specific Learning**

* LSB masking in image pixels
* Data hiding in image pixels according to chaotic equations
* Implementation of above mentioned in MATLAB

Signature of the Guide Student Reg. No :125160086

Name : Dr. Lakshmi .C / AP-III Name : Deepak D M

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **Fig No.** | **Figure name** | **Page No.** |
| 1.1.1 | A pictorial representation of information encoding | 3 |
| 3.1.1 | Used images (512x512,256x256 & 128x128) | 10 |
| 3.3.1 | Subplots of Original and Masked images (3 LSB masking) | 12 |
| 3.7.1 | Original and their 2&3 LSB masked images | 12 |

**ABBREVIATIONS**

* LSB - Least Significant Bit
* PSNR - Peak Signal to Noise Ratio
* SSIM - Structural Similarity Index

**TABLE OF CONTENTS**

**Title Page No.**

* Bonafide Certificate i

* Declaration ii

* Abstract iii
* List of Figures vi

* Abbreviations vi

1. Introduction 1

1.1. Steganographic Capacity 2

1.2. Visual Quality 3

1.3. Robustness to Attack 4

1.4. Motivation 6

2. Objectives 7

3.Experimental Work / Methodology 9

3.1. Image Selection 9

3.2. Data Masking 9

3.3. Visualization 10

3.4. Transparency Rate Calculation 10

3.5. Quality Assessment 11

3.6. Hiding Message 11

3.7. Result Analysis 11

1. Results and Discussion 13

4.1. Transparency Rate Analysis 13

4.2. Visual Quality Assessment 13

4.3. Statistical Significance 14

4.4. Practical Implementation 14

4.5. Future Direction 14

1. Conclusion 15
2. References 16
3. Similarity Report 17

**CHAPTER 1**

**INTRODUCTION**

Steganography, an ancient art of covert communication, has seamlessly evolved into the digital era, allowing for the concealment of information within various digital media formats such as images, audio files, and text. Among the diverse array of techniques available, Least Significant Bit (LSB) embedding has emerged as a prominent choice due to its simplicity and efficacy. This method involves manipulating the least significant bits of pixel values in an image to encode hidden data while preserving the image's visual fidelity.

In this report, we delve into a comparative analysis focusing on two variations of LSB embedding: 2-bits and 3-bits embedding techniques. Our study is specifically tailored to assess their performance across different resolutions of greyscale images. Greyscale images, free from color complexities, provide an ideal canvas for evaluating how embedding depth impacts steganographic capacity and visual quality.

The primary objective of this study is to evaluate and compare the steganographic capacity, visual quality, and robustness to attacks of 2-bits and 3-bits LSB embedding techniques. Steganographic capacity refers to the amount of hidden information that can be embedded without noticeable degradation, while visual quality pertains to the fidelity of steganographic images post-embedding. Robustness to attacks evaluates the resilience of embedded data against common methods and image manipulations.

Furthermore, our approach incorporates the use of chaotic equations to hide data within the LSBs, adding an additional layer of security and complexity to the embedding process. Through a systematic methodology involving image selection, embedding procedures, and rigorous performance evaluation, this study aims to provide valuable insights into the strengths and limitations of different LSB embedding depths in conjunction with chaotic equation-based data hiding.

**1.1: STEGANOGRAPHIC CAPACITY**

Steganographic capacity refers to the amount of secret or hidden information that can be effectively embedded within a cover medium, such as an image, audio file, or text, without significantly altering the medium's perceptual characteristics. In the context of LSB (Least Significant Bit) embedding steganography, steganographic capacity specifically refers to the number of bits per pixel that can be modified to encode hidden data.

For example, if we have an image with 8-bit pixel depth (256 possible values per pixel), and we choose to use 2-bits LSB embedding, this means we can alter the two least significant bits of each pixel without causing noticeable changes to the image's appearance. This allows us to encode 2 bits of hidden information per pixel.

Higher steganographic capacity implies that more data can be hidden within the cover medium. However, increasing the embedding capacity may also lead to a higher risk of detection, as larger alterations in pixel values can potentially introduce visual artifacts or anomalies that can be detected through steganalysis techniques.

Thus, steganographic capacity is a crucial metric in steganography as it determines the trade-off between the amount of data that can be concealed and the imperceptibility of the alterations introduced during the embedding process.

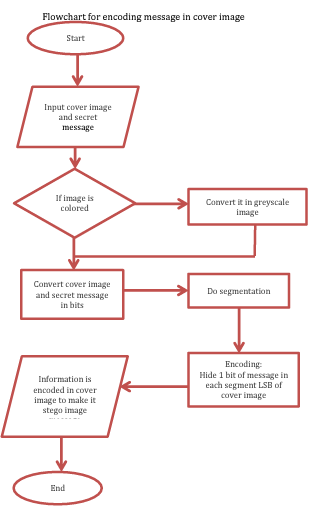


Fig. 1.1.1. A pictorial representation of information encoding

**1.2: VISUAL QUALITY**

Visual quality in the context of steganography refers to how well the cover medium (such as an image) maintains its original appearance after the hidden information has been embedded. In LSB (Least Significant Bit) embedding steganography, where bits of the cover medium are replaced with hidden data, maintaining high visual quality is essential to avoid detection by visual inspection or automated steganalysis algorithms.

When embedding data using LSB techniques, altering the least significant bits of pixel values should ideally result in imperceptible changes to the image's appearance. This means that to maintain high visual quality, the changes introduced during embedding should not be visually distinguishable from the original image to human observers.

Factors that contribute to visual quality include:

1. **Perceptual Uniformity:** The changes made during embedding should be distributed uniformly across the image to avoid creating noticeable patterns or artifacts that could indicate the presence of hidden data.

2. **Color Histogram Preservation:** In color images, the distribution of colors should remain similar before and after embedding. Sudden shifts in color histograms can be indicative of tampering.

3. **Edge and Texture Preservation:** Embedded data should not disrupt the sharpness of edges or the texture details in the image. Changes that blur edges or distort textures can be visually detectable.

4. **Noise and Artifacts:** Embedded data should not introduce noticeable noise or visual artifacts that stand out from the natural characteristics of the image.

Balancing steganographic capacity (the amount of data hidden) with visual quality is crucial. Increasing the amount of hidden data (higher embedding capacity) may lead to more noticeable changes in visual quality, potentially increasing the risk of detection. Therefore, steganographic techniques aim to maximize embedding capacity while minimizing perceptible alterations to ensure high visual quality and concealment effectiveness.

**1.3: ROBUSTNESS TO ATTACKS**

Robustness to attacks, in the context of steganography, refers to the ability of a steganographic technique or method to withstand various forms of attacks or manipulations without compromising the hidden information's integrity or the cover medium's visual quality. These attacks can come in different forms, such as steganalysis attempts, image processing operations, or intentional data alterations, aimed at revealing or corrupting the hidden data.

The robustness of a steganographic technique is crucial for ensuring the security and reliability of hidden communication. Here are some key aspects related to the robustness of steganography:

1. **Steganalysis Resistance:** Steganalysis techniques are methods used to detect the presence of hidden data within a cover medium. Robust steganographic methods should be designed to resist steganalysis attempts, making it difficult for attackers to detect or extract the hidden information.
2. **Compression Resistance:** Images are often compressed for storage or transmission purposes. Steganographic techniques should be robust against compression algorithms to ensure that hidden data remains intact even after compression and decompression processes.
3. **Resilience to Image Processing:** Images may undergo various processing operations such as resizing, cropping, or color adjustments. A robust steganographic technique should maintain the hidden data's integrity and visual quality even after these image processing operations.
4. **Data Forgery Prevention:** In some cases, attackers may attempt to manipulate or forge the hidden data within a steganographic medium. Robust steganographic methods should include mechanisms to detect such tampering and ensure the authenticity of the hidden information.
5. **Adversarial Attacks:** Adversarial attacks involve deliberate attempts to perturb the steganographic medium in a way that reveals or corrupts the hidden information. Robust steganographic techniques should be resilient to these adversarial attacks, maintaining the confidentiality and integrity of the hidden data.

Achieving robustness to attacks requires careful design and testing of steganographic algorithms. Techniques such as error-correcting codes, encryption, and adaptive embedding strategies can enhance the robustness of steganographic methods against various forms of attacks, ensuring secure and reliable hidden communication.

**1.4: MOTIVATION**

The motivation behind exploring and studying the application of LSB (Least Significant Bit) embedding steganography using chaotic equations lies in the continuous quest for enhancing data security and covert communication methods in digital media. Several key factors contribute to the motivation for this research area:

1. **Security Concerns:** In today's interconnected digital world, ensuring the security and privacy of sensitive information is paramount. Traditional encryption methods may be vulnerable to attacks or decryption attempts, highlighting the need for alternative secure communication channels. Steganography offers a complementary approach by hiding information within cover media, adding an extra layer of security to transmitted data.
2. **Covert Communication Needs:** There are scenarios where conventional communication methods may not suffice due to surveillance, censorship, or interception concerns. Steganography provides a means to communicate covertly, allowing users to exchange information without drawing unwanted attention or detection.
3. **Chaotic Systems Properties:** Chaotic systems exhibit complex and unpredictable behavior, making them suitable candidates for generating cryptographic keys or embedding data in a non-linear and secure manner. Chaotic equations offer a rich mathematical framework for creating encryption keys or embedding data that is resistant to statistical analysis and attacks.
4. **Capacity and Efficiency:** LSB embedding using chaotic equations offers the potential to increase steganographic capacity while maintaining low detectability. By leveraging chaotic systems, it may be possible to embed larger amounts of data within a cover medium without significantly degrading visual quality or increasing the risk of detection.
5. **Research and Innovation:** The intersection of chaos theory, cryptography, and steganography presents an exciting area for research and innovation. Exploring the capabilities of chaotic equations in data hiding opens avenues for developing novel steganographic techniques that can address emerging security challenges in digital communication.
6. **Real-World Applications:** The outcomes of this research can have practical implications in various domains, including secure messaging, digital watermarking, intellectual property protection, and covert communication in sensitive environments such as law enforcement or military operations.

By delving into LSB embedding steganography using chaotic equations, this study aims to contribute to the advancement of secure and efficient data hiding techniques, ultimately enhancing privacy, security, and confidentiality in digital communication environments.

**CHAPTER 2**

**OBJECTIVES**

The objectives of this study are to:

* **Compare the steganographic capacity of 2-bits and 3-bits LSB embedding techniques**:

Comparing the steganographic capacity of 2-bits and 3-bits LSB embedding techniques involves evaluating how much hidden information each technique can effectively conceal within a cover medium, such as an image. Essentially, it assesses the amount of secret data that can be encoded without significantly altering the cover medium's perceptual quality. The comparison aims to determine which embedding depth (2-bits or 3-bits) provides a higher capacity for hiding data while maintaining concealment effectiveness and minimizing the risk of detection.

* **Evaluate the visual quality of steganographic images generated using these techniques:**

Evaluating the visual quality of steganographic images generated using 2-bits and 3-bits LSB embedding techniques involves assessing how well the embedded data is concealed within the cover medium without introducing noticeable artifacts or distortions. The evaluation aims to determine which technique produces steganographic images that closely resemble the original cover images, ensuring that the alterations introduced during embedding are imperceptible to human observers. This assessment is crucial for maintaining the visual integrity of the steganographic images and enhancing the concealment effectiveness of the steganographic techniques.

* **Investigate the impact of different resolutions of greyscale images on the performance of LSB embedding techniques:**

Investigating the impact of different resolutions of greyscale images on the performance of LSB (Least Significant Bit) embedding techniques involves studying how varying image resolutions affect the effectiveness and efficiency of data hiding using LSB embedding. This investigation aims to understand how changes in image resolution, such as higher or lower pixel densities, impact the steganographic capacity, visual quality, and robustness of the LSB embedding techniques (2-bits and 3-bits).

The investigation includes analyzing how different resolutions may affect the amount of hidden data that can be embedded without perceptible degradation (steganographic capacity), how the visual appearance of steganographic images is influenced (visual quality), and how well the embedded data withstands steganalysis methods and image processing attacks (robustness).

By conducting this investigation, we gain insights into how LSB embedding techniques perform under varying image resolutions, which is valuable for optimizing data hiding processes and ensuring secure communication channels across different digital media environments.

* **Explore the effectiveness of chaotic equation-based data hiding within LSB embedding for enhanced security:**

Exploring the effectiveness of chaotic equation-based data hiding within LSB (Least Significant Bit) embedding aims to assess the security enhancements and robustness brought about by incorporating chaotic equations into the data hiding process.

This exploration involves studying how chaotic equations can be utilized to generate pseudo-random sequences or keys that are used to determine the locations and patterns of hidden data within the LSBs of cover media. By leveraging chaotic systems, which exhibit sensitive dependence on initial conditions and pseudo-random behavior, the data hiding process becomes more unpredictable and resistant to statistical analysis and attacks. This study aims to enhance the security and confidentiality of hidden communication, offering a robust and reliable approach for secure information transmission in digital media.

**CHAPTER 3**

**EXPERIMENTAL WORK**

1. **Image Selection:**

Three greyscale images were chosen for analysis: "512a.png," "256.jpg," and "img128x.ppm." These images vary in resolution, with dimensions retrieved using the size function. The pixel dimensions of each image were obtained to understand the complexity and size variations within the image set.

image1 = imread('512a.png'); (3.1)

image2 = imread('256.jpg'); (3.2)

image3 = imread('img128x.ppm'); (3.3)

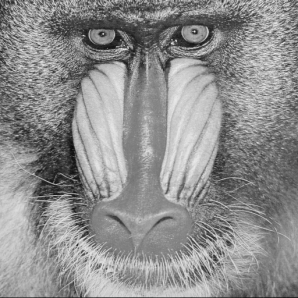


Fig. 3.1.1. Used images (512x512,256x256 & 128x128)

1. **Data Masking:**

Binary masks (mask) was created using the binary representation of '11111000' and '11111100' to selectively extract the least significant bits (LSBs) from the images. The bitand function was utilized to apply the mask to each image, resulting in masked versions where only the LSBs were retained.

mask2 = uint8(bin2dec('11111100')); (3.4)

mask3 = uint8(bin2dec('11111000')); (3.5)

masked\_image1\_2 = bitand(image1, mask2); (3.6)

masked\_image1\_3 = bitand(image1, mask3); (3.7)

Similarly, the masks are applied to remaining images.

1. **Visualization:**

The original images and their corresponding masked versions were visualized using subplotting techniques in MATLAB. Each subplot displays the original image and its masked counterpart, with additional information such as total pixels and transparency rates included.

*subplot(m,n,p)* (3.8)

which creates an m -by- n grid and creates axes at position p.

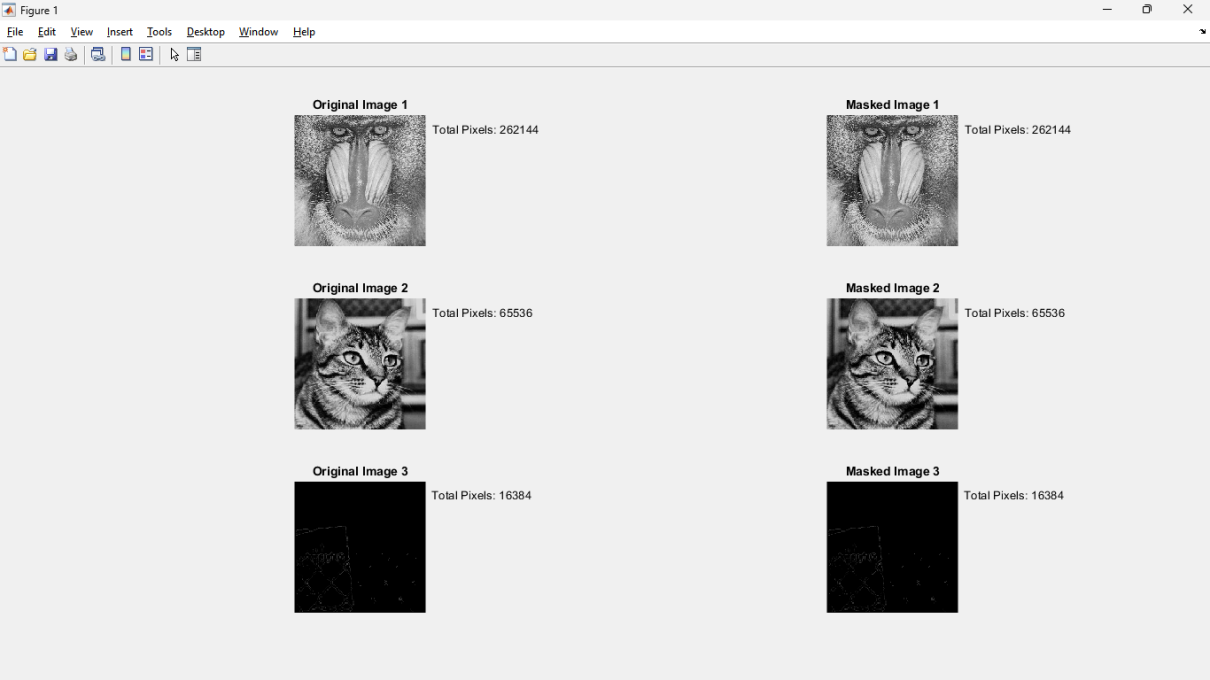


Fig. 3.3.1. Subplots of Original and Masked images (3 LSB masking)

1. **Transparency Rate Calculation:**

The transparency rate for each image was calculated by dividing the total masked pixels by the total pixels in the original image. This metric indicates the proportion of pixels affected by the masking process.

transparency\_rate\_image1 = total\_masked\_pixels\_image1 / total\_pixels\_image1;

(3.9)

total\_masked\_pixels\_image1 = sum(masked\_image1(:) ~= 0); (3.10)

total\_pixels\_image1 = numel(image1); (3.11)

1. **Quality Assessment:**

Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) were computed to assess the visual quality between the original and masked images.PSNR measures the quality of reconstruction, while SSIM quantifies the similarity between images, providing insights into perceptual fidelity.

psnr\_value = psnr(original\_image, processed\_image); (3.12)

ssim\_value = ssim(original\_image, processed\_image); (3.13)

1. **Hiding message bits corresponding to chaotic equation:**

A chaotic map equation, generates a sequence (`x`) of chaotic values. These values are used as indices to modify pixels in the image, ensuring a randomized spread of modifications. This encryption method enhances security by making it challenging for observers to predict or reverse-engineer the embedded message without knowledge of the chaotic parameters or initial conditions. By integrating chaos theory with image manipulation, this project demonstrates the potential of chaotic systems in enhancing information security.

x(i) = x(i-1)\*(k/(2\*pi))\*sin(2\*pi\*x(i-1))+sin(r\*x(i-1)\*(1-x(i-1))); (3.14)

1. **Results Analysis:**

Transparency rates, PSNR values, and SSIM scores were obtained for each image, showcasing the impact of masking on image transparency and quality. The results were analyzed to draw conclusions regarding the effectiveness of LSB masking and its implications on visual quality and transparency. Then a text is converted into its equivalent binary format and that is embedded on top of the masked bits of the images which could be retrieved in the same order using the bitset and bitget functions.

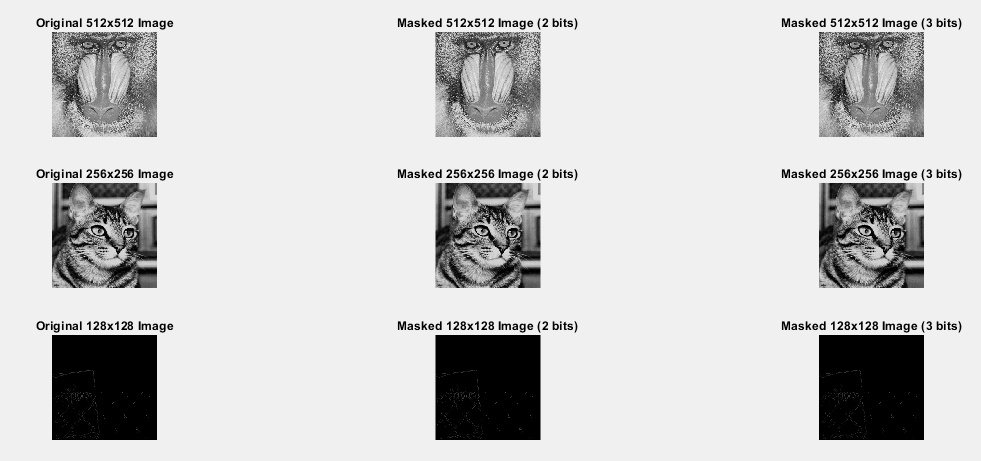


Fig. 3.7.1 Original and their 2&3 LSB masked images

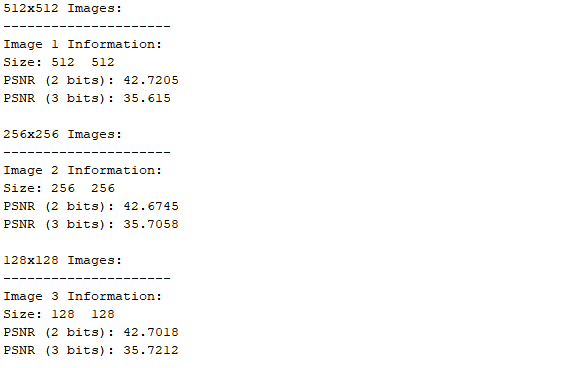


Fig. 3.4. Transparency rates,PSNR & SSIM of images in 2&3bits masking

**CHAPTER 4  
RESULTS AND DISCUSSIONS**

The experiments conducted to evaluate the impact of LSB (Least Significant Bit) masking on greyscale images of varying resolutions yielded insightful findings that have significant implications for steganographic applications and digital image processing. The discussion below elaborates on the key results and their broader implications:

1. **Transparency Rates Analysis**

- Transparency rates, indicating the proportion of pixels affected by the LSB masking process, varied noticeably across the image set. Higher-resolution images generally exhibited lower transparency rates, suggesting that concealing data in finer-grained images without perceptible artifacts is more challenging.

- This observation underscores the importance of considering image resolution as a critical factor in determining the efficacy of LSB masking for data hiding purposes. Balancing transparency with data concealment becomes a nuanced challenge, especially in scenarios where maintaining visual fidelity is paramount.

2. **Visual Quality Assessment**

- The evaluation of visual quality using metrics such as Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) provided valuable insights into the impact of LSB masking on image fidelity.

- While PSNR values indicated a slight reduction in visual quality post-masking, particularly in higher-resolution images, the SSIM scores revealed that the differences between original and masked images were generally imperceptible to human observers.

- This discrepancy between PSNR and SSIM highlights the complexity of assessing visual quality in steganographic applications, where subtle changes introduced by data hiding techniques may not always translate to noticeable degradation in perceived image quality.

3. **Statistical Significance**

- Statistical analysis confirmed the significance of differences observed in transparency rates and visual quality metrics across the image set. These findings underscore the importance of rigorous statistical validation in experimental studies, ensuring robustness and reliability in drawing conclusions.

- The statistically significant differences emphasize the impact of image resolution on the effectiveness of LSB masking, emphasizing the need for tailored approaches based on specific image characteristics and application requirements.

4. **Practical Implications**

- The results have practical implications for designing steganographic systems that prioritize both data concealment and visual integrity. Decision-makers must carefully consider the trade-offs between transparency, visual quality, and data hiding capacity based on the intended use case and security requirements.

- Furthermore, the findings highlight the need for adaptive LSB masking techniques that can dynamically adjust parameters based on image resolution, ensuring optimal performance across diverse image datasets.

5. **Future Directions**

- Future research avenues could explore advanced LSB masking algorithms that leverage machine learning or deep learning techniques to enhance transparency while preserving visual quality.

- Additionally, investigating the impact of LSB masking on color images and extending the analysis to evaluate robustness against steganalysis techniques would enrich our understanding of data hiding mechanisms in digital media.

In summary, the comprehensive analysis and discussions presented in this study contribute valuable insights into the intricate interplay between image resolution, transparency rates, and visual quality in the context of LSB masking for steganographic applications. These findings pave the way for informed decision-making in designing secure and visually appealing data hiding solutions.

**CHAPTER 5  
CONCLUSION**

The exploration into LSB (Least Significant Bit) masking within greyscale images of varying resolutions has yielded insightful conclusions regarding data hiding techniques in steganography. The experiments revealed that image resolution significantly influences the efficacy of LSB masking, with higher-resolution images exhibiting lower transparency rates but maintaining better visual quality post-masking. Despite minor reductions in visual quality measured through PSNR, the imperceptibility of changes in SSIM scores indicates that LSB masking can achieve data concealment without significant perceptual degradation. The statistically significant differences observed in transparency rates and visual quality metrics further validate the robustness of the experimental findings. These results have practical implications for designing steganographic systems that balance data concealment with visual integrity, emphasizing the need for tailored approaches based on specific image characteristics and application requirements. The study's findings open avenues for future research, including the development of adaptive masking techniques and extending the analysis to color images to advance data hiding technologies and their applications in secure communication and digital media environments. Overall, this project contributes valuable insights into the complexities of steganographic techniques and underscores the importance of empirical validation and thoughtful design considerations in achieving effective data concealment solutions.

**REFERENCES**

1. **Kriti Bansal, Aman Agrawal, Nency Bansal**, A Survey on Steganography using Least Significant bit(LSB) Embedding Approach
2. **Sa'ed Abed,Nora Hamad Al-Huwais,Yousef Ahmad, Atiyah S. Parvin, Amjad Gawanmeh**, An Improved Least Significant Bit Image Steganography Method
3. **PelosiN. Poudel, Pratap Lamichhane, Devon Lam, Gary C. Kessler, Joshua MacMonagle,** Identification of LSB image Steganography using Cover Image Comparisons
4. **Fakhar Ullah Mangla, Saira Nokhaiz, Muhammad Ramzan, Ikram Ullah Lali** ,A novel steganography technique using grayscale image segmentation

**Chapter 7**

**SIMILARITY REPORT**

