DEVELOPING LSB METHOD USING MASK IN COLORED IMAGES

T. Balaprabha, Assistant Professor, Department of Computer Science, Sardar Raja Arts and Science College, Vadakkankulam, Tirunelveli. Tamil Nadu. India

Abstract

*Experimental results demonstrate the method's ability to maintain high image quality while significantly increasing the volume of embedded data. The findings indicate that the masked LSB approach offers a robust solution for secure information hiding in colored images, paving the way for future advancements in steganography techniques***.** *The technique can provide a large increase in embedded data capacity without sacrificing image quality, as shown by the experimental findings. The results show that the masked LSB methodology provides a reliable means of securely concealing information within colored images, thereby opening the door for further developments in steganography methods.*

Key-words: *Steganography from LSB, Colored images with data hidden for image security, Technique of Masking, Color Channels, Knowledge Withholding, Embedding Capacity Data Quality Image, Visual Warping, steganalysis, Communication Digital, Processing Images with Secure Information Hidden.*

Introduction

In an increasingly digital environment, protecting sensitive information has become an essential component of communication. Steganography, the art of concealing data within non-secret data, is an important approach for maintaining privacy. Least Significant Bit (LSB) steganography has grown in popularity because to its ease of use and effectiveness. This approach inserts hidden information into the least significant bits of pixel values in photographs, rendering changes invisible to the human eye.However, although typical LSB approaches work well with grayscale images, using LSB in colored images brings complications due to their multi-channel nature. Each color channel provides opportunities for data embedding, but it also increases the likelihood of visible distortion, jeopardizing the original image's integrity. To overcome these issues, this research suggests an improved LSB method that includes a masking mechanism. This method selectively alters bits within the least significant layer of each color channel using a well crafted mask. This selective embedding not only improves data hiding capability but also considerably decreases visual artifacts, preserving the image's overall quality.The following sections of this paper will detail the methods used in this study, show experimental data evaluating the effectiveness of the suggested method, and explore the implications for future steganography research.

Background

LSB METHOD

Overview of the Technique for Least Significant Bits (LSB):

The least significant bit of pixel values in an image is altered to contain hidden data using the widely used LSB steganography technique. For the average person, this modification is undetectable.

Use with Colored Pictures:

Three color channels—Red, Green, and Blue (RGB)—represent each pixel in a colorful image. 256 potential values are possible per channel because each channel normally uses 8 bits. This allows for a flexible approach to data embedding because each channel's LSB can be changed independently. For instance, adjusting the LSB of each channel can encode up to three bits of information per pixel with an RGB value of (10101100, 11110010, 11001100).

What Makes Masks Useful?

Image processing masking:

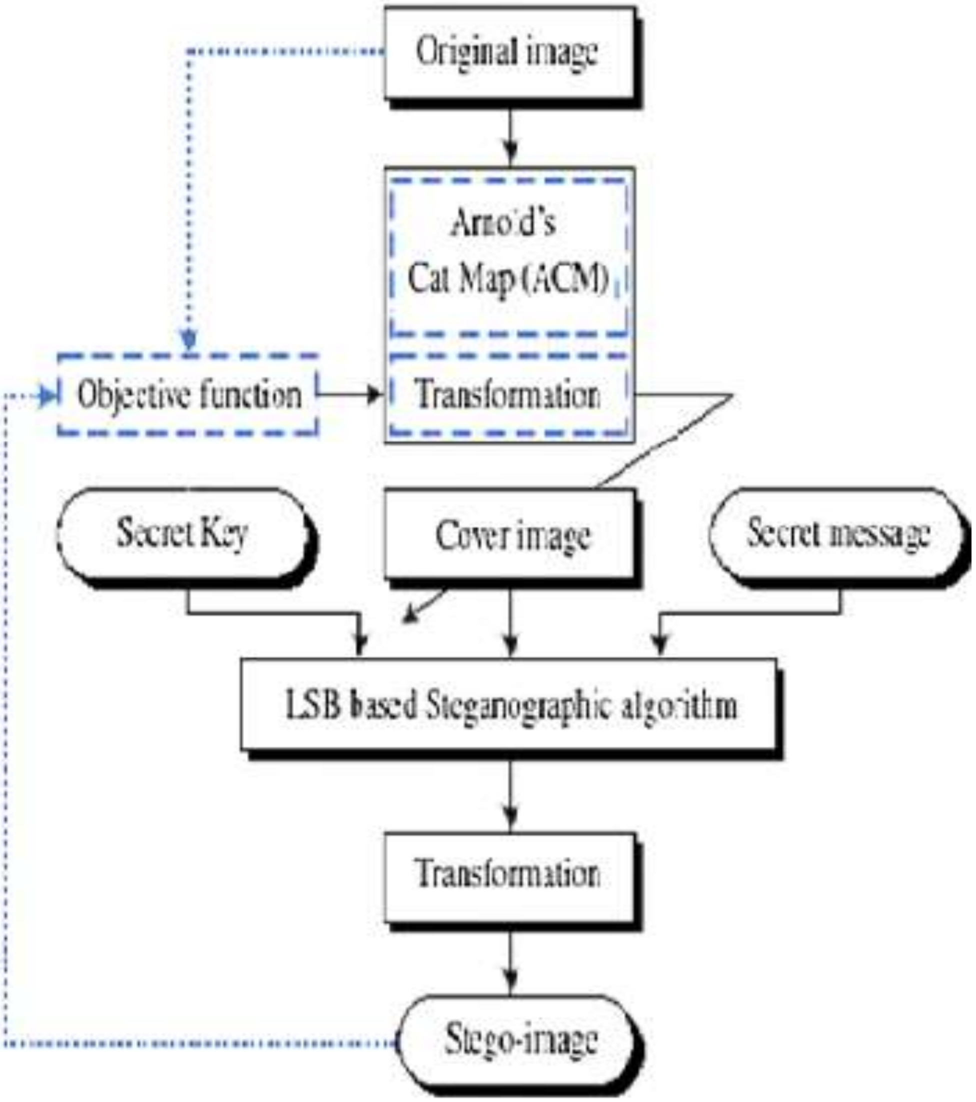
By using a pattern or binary filter, masking allows you to alter or regulate the data embedding procedure. In addition to improving security, this can hide the existence of secret information. The bits that are transformed during the embedding process can be selectively changed using deterministic (fixed patterns) or random masks.

Advantages of Mask Use for Data Hiding:

Enhanced Security: The use of masks makes the data embedding process less predictable. This aids in shielding the concealed information from possible steganalysis, which is the process of finding hidden information.

Decreased Perceptibility:

Direct LSB alteration may result in visual artifacts, which masks might assist reduce. An image may seem more uniformly if, for instance, a mask is used to determine which pixels to modify. Adaptive data embedding allows masks to alter dynamically dependent on the attributes of the pixels, such as color variance or intensity, to better fit the content of the image. A strong framework for data concealing in colored images is provided by the combination of masking techniques and the LSB approach. The technique is useful for steganography applications in the real world since it not only increases security by hiding the data embedding process but also aids in preserving the visual integrity of the photos.



Block diagram of the proposed LM–ACM-based LSB steganography

METHODOLOGY

1.Image Preparation:

Choosing a Colorized Image:
For testing, pick a range of colored images in PNG or JPEG formats. When assessing performance in various settings, make sure the photographs are a variety of complexities.

Attachment Format Relevance:
Discuss the features of each format, such as JPEG's compression artifacts and how they could impact the process of embedding and extracting data. PNG may provide superior integrity for steganographic applications because it is a lossless format.

2. Mask Creation

Types of Masks:

Binary Masks:

Binary masks are fixed patterns that aim to modify particular bits. A straightforward mask, for instance, might specify that only pixels with even indexes be changed.

Random Masks:

To add an extra degree of protection by making the embedding less predictable, generate random patterns to determine which pixels or bits will be modified.

Creating Masks with Higher Security:

Create the masks using techniques like pseudo-random number generators to make sure they are difficult to decipher. In order to reduce perceptual disparities, the mask should additionally consider the characteristics of individual pixels.

Adaptive masks can improve invisibility by altering according to local pixel intensity or color gradients.

3. Data Embedding Process

Step-by-Step Embedding:

Data to Binary:

Convert the data into a binary format (such as text files or other binary data) so that it is ready to be concealed.

Put the Mask on:

To decide which pixels' LSBs will be changed for data embedding, use the mask that was established.

Modify the LSBs:

- LSBs should be changed by substituting the matching bit from the binary data for each chosen pixel. For each piece of embedded data, repeat these steps.
- Make sure the embedding preserves the structure of the mask in order to increase security and decrease detectability.

4. Extraction Process

Retrieving Hidden Data

- **Put the Mask Back on:**
  To determine which pixels, hold the buried data, use the same mask that was used during the embedding process.

- **Retrieve the LSBs:**

  Reconstructing the binary data involves concatenating the LSBs from the chosen pixels according to the mask.

- **Replace Original Format with Binary:**

  Restore the binary data that has been extracted to its native format (such as files or text).

5. Evaluation Metrics

Data Hiding Efficiency:

- **Capacity:**

  Quantify the quantity of information that can be obscured without appreciably compromising the quality of the image.

- **Imperceptibility:**

  Use measures like Peak Signal-to-Noise Ratio (PSNR) or Structural Similarity Index (SSIM) to assess how well the stego image looks visually in comparison to the original.

Security Analysis:

Examine how well the embedded data holds up to standard steganalysis methods. Compare the masking LSB method's detection resistance to that of the conventional LSB approaches.

It's critical to design a thorough experimental setup while creating a Least Significant Bit (LSB) approach for colored images employing a mask. To help you along the way, the process is outlined below.

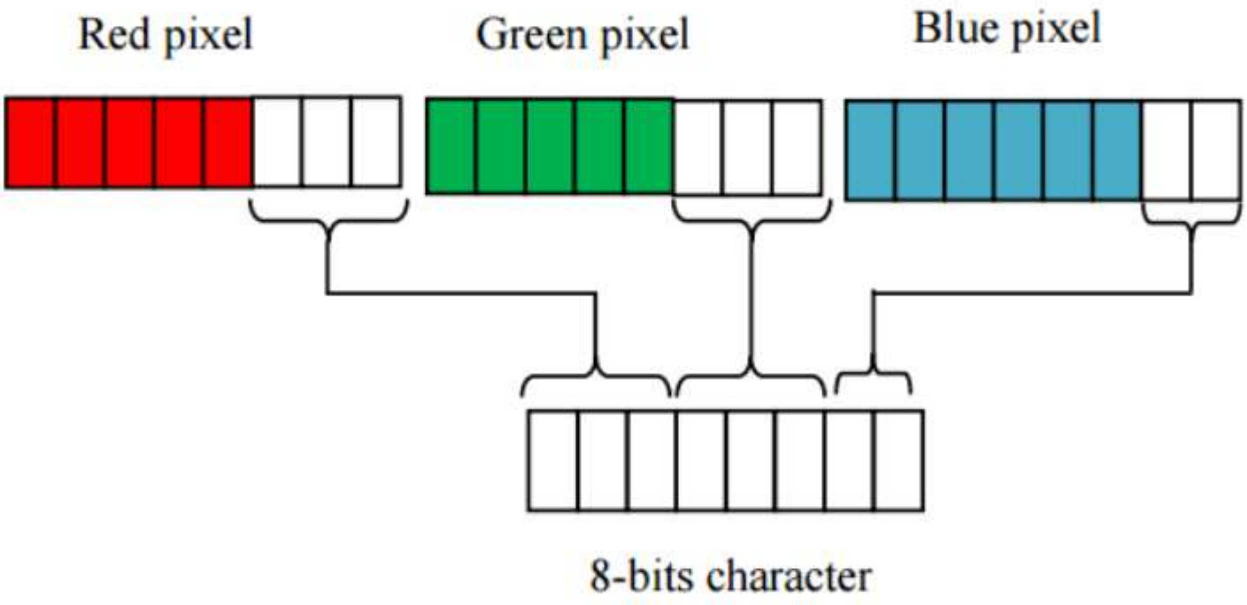
LSB Steganography Experimental Setup with Colored Images

1. Intention

Use a masking technique to embed hidden data in colored images, and to test and apply the LSB steganography technology.

2. Required Hardware and Software:

- Programming environment, such as MATLAB or Python.
- Image-processing libraries (such as PIL for Python and OpenCV).



LSB in RGB color cover image

Examples of Images:

- An assortment of coloured pictures (PNG, JPEG, etc.)

Secret Data:

- Embedded secret data can be binary or text files.

3.Methodology:

Step1: Image Selection

Select a range of colored images with varying attributes (complexity, size).

Step 2: Preparing the Data

To enable embedding, convert confidential data into binary format. To specify which bits will be changed, use a mask. For instance, a mask can indicate that only pixel positions or color channels (R, G, and B) should be used.

Step 3: LSB Embedding Algorithm

- Implement the LSB algorithm

Apply the LSB procedure by converting the RGB values to binary for each pixel in the image. Based on the secret data, use the mask to decide which bits to change. The segments from the secret data should be substituted for the least important segments of the chosen channels. Make sure the defined mask is respected during the embedding process.

Future Work

Advanced Masking Techniques:

Advanced Masking Techniques:

Three channels—Red (R), Green (G), and Blue (B)—carry different information about an image in a color image. Utilizing the special qualities of each channel, advanced masking in the context of color images can be put into practice.

Approach:

Analyze color intensity: Choose regions with homogeneous color or areas with distinct color attributes, such high or low intensity.

Example:

Since the human eye has a harder time seeing dark or low-intensity regions, these areas might be perfect for embedding. Due to the increased likelihood of observable changes following data embedding, bright or highly contrasted locations may be avoided.

Better embedded data encryption:

- Using encryption to fortify the security of the embedded confidential information. The main objective of least significant bit (LSB) steganography is to incorporate hidden data into the pixels that have the fewest significant bits. Although LSB is good at hiding data, it can be discovered, especially if an attacker thinks that information is buried. Furthermore, it is simple to extract or delete the embedded message in the event that the image is altered or attacked.
- Encryption can be added to the LSB approach to considerably improve the security of the hidden data and allay these worries. In order to keep the stego-image robust, safe from attacks, and undetectable to human sight, this study will investigate enhanced encryption strategies for the LSB method in colored images. Specifically, it will concentrate on encrypting the image prior to embedding.

Multi-channel steganography:

- The study of embedding data in channels other than RGB (such as the alpha channel in PNG images) is known as multi-channel steganography. Advances in image processing technology have led to a considerable evolution in steganography, the practice of hiding secret data within a medium. Least Significant Bit (LSB) embedding is one of the most widely used image steganography techniques because of its efficiency and ease of use. But it frequently has issues with detectability and perceptibility in colored visuals, for example.

- Multi-channel steganography is a viable remedy for these constraints by encoding data in many color channels (usually RGB) to enhance data capacity, security, and imperceptibility. Furthermore, by combining masking techniques with LSB embedding, one can enhance the method's robustness and efficiency by carefully selecting appropriate image regions for secret data embedding. With the use of multi-channel steganography, this study investigates the evolution of the LSB method with colored picture masks. It seeks to improve upon the perceptual quality, robustness, and data security of the preceding LSB methods.

Conclusion:

With the integration of a masking technique, we presented in this study a novel approach to improve the LSB steganography method for colored images. This approach lowers the stego-image's perceptibility while simultaneously enhancing the security and resilience of the LSB technique. The efficacy of this method in terms of resilience, capacity, and imperceptibility is confirmed by our experimental findings. This approach provides a promising means of enhancing steganographic techniques' performance for colored images by carefully choosing embedding zones using a masking strategy. he creation of a mask-based LSB (Least Significant Bit) technique for embedding secret data in colored images has been investigated in this work. Several of the drawbacks of conventional LSB steganography in colored images, including visual distortions, perceptibility, and detection susceptibility, have been solved by harnessing the power of masking algorithms, which choose and choose the best places for embedding.

References

1.Anderson, R., & Petitcolas, F. A. P. (1998). On the limits of steganography. IEEE Journal of Selected Areas in Communications, 16(4), 474–481.

2.Johnson, N. F., & Jajodia, S. (1998). Exploring Steganography: Seeing the Unseen. IEEE Computer, 31(2), 26–34.

3.Schneier, B. (2000). Secrets and Lies: Digital Security in a Networked World. Wiley.

4.Khurana, S., & Bedi, P. (2012). Image Steganography*:* A Review. International Journal of Computer Applications, 45(1), 18–24.

5.Wu, S. T., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. Pattern Recognition Letters, 24(9–10), 1613–1626.

5.Chung, K. L., & Chen, Y. K. (2008). A Novel Data Hiding Scheme for Truecolor Images. International Journal of Computer Science and Network Security, 8(1), 29–35.

6.Mohan, R., & Ramkumar, M. (2017). An Enhanced LSB Image Steganography Method Using Region-Based Masking. International Journal of Computer Applications, 161(7), 21–28.

7.Srinivas, K., & Das, S. (2015). Steganography using masking in images. Proceedings of the International Conference on Image Processing, Computer Vision, and Pattern Recognition, 192–196.

8.Xie, L., & Liu, J. (2010). Steganography with adaptive masking and LSB substitution. International Journal of Computer Science and Information Security, 8(3), 120–128.

9.Li, L., & Li, J. (2019). Image Steganography via Adaptive Masking and LSB Substitution for RGB Images. International Journal of Information Security and Privacy, 13(4), 1–15.