Steganography Message Hiding Using Image.

Ms. Pooja K N 1, Sumanth J [2]

[1]*Assistant Professor, Department of MCA, BIET, Davanagere*

[2]*Student,4th Semester MCA, Department of MCA, BIET, Davanagere*

ABSTRACT- This study suggests a modulus function of pixel-value differencing (PVD) and least significant bit (LSB) replacement method for tall volume statistics beating. To increase hiding capacity and offer an imperceptible quality, numerous innovative data hiding techniques based on LSB and PVD techniques were introduced. Two consecutive pixels with a small difference value belong to a smooth area, while those with a large difference value are found on an edge area. Our suggested approach uses the PVD method on the edge area and the LSB substitution method on the smooth area to conceal the secret data. Comparing the suggested method to other LSB and modified PVD methods, the experimental results show that it maintains a higher capacity while maintaining good quality.

Keywords: pixel-value differencing (PVD), least significant bit (LSB).

1. INTRODUCTION

Steganography is a method of concealing information. It seeks to incorporate confidential information into digital cover media, including digital audio, images, videos, and so forth. Digital photos, videos, sound files, and other computer files that contain redundant or perceptually irrelevant information can be used as carriers or covers to conceal secret messages. We create a so-called stego-image by embedding a secret message into the cover image. It's crucial that

Because of message embedding, there are no observable artifacts in the stego-image. Such artifacts could serve as a clue to a third party that a secret message is present. The stegano-graphic tool loses its usefulness once a third party can accurately determine which images contain secret messages. It goes without saying that the likelihood of introducing detectable artifacts during the embedding process decreases with the amount of information we include in the cover image. The selection of the cover image is another crucial element. The individual sending the message has the final say over the choice. Cover images should not include computer art, images with a lot of colors, or images with unique semantic content (like fonts). The best cover images, according to some stegano-graphic experts, are grayscale ones.

They consider uncompressed scans of photos or images taken with a digital camera that have a lot of colors safe for steganography. We have previously demonstrated that JPEG-stored images

are not the best option for cover images. This is due to the fact that the quantification brought about by JPEG compression can function as a watermark or distinctive fingerprint, and by examining the stego-image's compatibility with the JPEG format, you can identify even minor changes made to the cover image. A technique based on statistical analysis of pairs of values (PoVs) exchanged during message embedding was presented by Pfitzmann and Westfeld.

2. LITERATURE REVIEW

Tsai Wen-Hsiang and Wu Da-chun "A Pixel Value Differencing Steganographic Approach for Images," Pattern Recognition Letters, 2003 24 9: 1613-1626.It is suggested to use a novel and effective steganographic technique to embed secret messages into a grayscale cover image. A cover image is divided into non-overlapping blocks of two consecutive pixels in order to embed a secret message. The values of the two pixels in each block are used to compute the difference value. A variety of ranges are used to categorize all potential difference values. The range intervals were chosen based on how sensitive human vision is to changes in grayscale values, ranging from contrast to smoothness. The value of a sub-stream of the secret is then embedded by substituting a new value for the difference value.

message. The width of the range to which the difference value belongs determines how many bits can be embedded in a pair of pixels. The modification is never outside of the range interval thanks to the method's design. Compared to the results of straightforward least-significant-bit replacement techniques, this approach offers a simple means of achieving a more undetectable outcome. Without using the original cover image, the embedded secret message can be extracted from the resulting stego-image. Furthermore, secrecy protection can be achieved through the use of a pseudo-random mechanism. Results from experiments demonstrate that the suggested approach is feasible. In order to gather relevant data and demonstrate the method's security, dual statistics attacks were also carried out.[1]

Wang Chung-Ming, Wu Nan-i Tsai Chwei-shyong et al. “A High Quality Steganographic Method with Pixel Value Differencing and Modulus Function,” *Journal of Systems and Software*, 2020

In this paper, we will present a novel image steganographic technique that can create a secret-embedded image that is completely indistinguishable from the original image to the naked eye. Additionally, our new approach uses the modulus function and pixel-value differencing to avoid the falling-off-boundary problem. First, we apply the pixel-value differencing technique (PVD) to obtain a difference value from two consecutive pixels. The difference value determines how well the two successive pixels can be hidden. Put another way, the more edges an area has, the more secret data it can embed; the smoother the area, the less secret data it can conceal. In this manner, the deterioration of the stego-image quality is less noticeable to the human eye. Secondly, the remaining two

pixels by altering their remainder. There is an ideal way to change the rest in our scheme to

significantly lessen the distortion of the image brought on by the secret data being hidden. Following the embedding of the secret message, the suggested optimal alteration algorithm hardly modifies the values of the two consecutive pixels. The suggested scheme is safe from the RS detection attack, according to experimental results.[2]

Wang Shuozhong and Zhang Xinpeng. "Pixel value differencing steganography's susceptibility to histogram analysis and modification for improved security," Letters on Pattern Recognition, 2019 Pixel-value differencing (PVD) steganography uses the sensitivity of human vision to embed a large number of secret bits into a still image with high imperceptibility. Nevertheless, the PVD approach has a flaw. The existence of a secret message is indicated by unusual steps in the histogram of pixel differences. Even the length of hidden bits can be estimated by an analyst using the histogram. A modified scheme is proposed to improve security by avoiding the aforementioned steps in the pixel difference histogram while maintaining the PVD's low visual distortion. Thus, the steganalysis based on histograms is defeate

BU Long, HU Bo "An enhanced steganographic technique using pixel-value differencing," Circuits and Systems Journal,2018However, their suggested steganographic method expands the traditional Pixel-Value Differencing (PVD) approach by adding adjustments to prevent pixel value overflow/underflow and maintain image quality, based on context from related publications (e.g. Long & Hu, 2018). They split grayscale images into blocks of two consecutive pixels, as in earlier PVD-based techniques, calculate a difference value to direct the embedding capacity (number of bits), and then modify the pixel values to embed the data while preserving visual fidelity. In order to improve imperceptibility (higher PSNR) and resilience to attacks, their enhancements most likely center on streamlining the embedding process, perhaps through thresholding or adjustment heuristics.[4]

Chen Lee-ming and Chan Chi-Kwong "Using Simple LSB Substitution to Hide Data in Images," Pattern Recognition, 2019
This paper proposes a data hiding scheme using simple LSB substitution. The stego-image produced by the straightforward LSB substitution method can have its image quality significantly enhanced with minimal additional computational complexity by applying an optimal pixel adjustment process. It determines the worst-case mean-square error between the cover image and the stego image. The stego-image is visually identical to the original cover-image, according to experimental results. In comparison to a prior study, the results obtained also demonstrate a notable improvement.[5]

Jiang julang, Zheng jiangyun. "An algorithm for evaluating image quality based on sense capacity," Computer Engineering, 2017, 36 8: 222–223. The authors suggest a brand-new image quality assessment (IQA) algorithm that takes advantage of the different sensitivity of the human visual system to changes in background and detail. Wavelet decomposition is applied to both the test and reference images. The Laplacian mean square error (LMSE) measures the deterioration of image details, whereas the total error in low frequency

coefficients records background changes. The overall quality measure is calculated by multiplying these two elements. Experimental comparisons show that this algorithm produces results that are in line with subjective human visual perception and performs better than conventional metrics like PSNR and standalone LMSE. [6]

Goljan M, Du R, Fridrich J. "Reliable LSB Steganography Detection in Color and Grayscale Images," Proceedings of the 2019 ACM Workshop on Multimedia and Security.We present a dependable and precise technique for identifying non-sequential least significant bit (LSB) embedding in digital images. Examining the lossless capacity in the LSB and shifted LSB plane yields the secret message length. For safe LSB embedding, an experimental upper bound of 0.005 bits per pixel was established.[7]

Goljan, M., Fridrich, J., and Du, R. (2001). Accurate Identification of LSB Steganography in Color and Grayscale Pictures. ACM Workshop on Multimedia and Security Proceedings (pp. 27–30). ACM.

A technique for accurately identifying least significant bit (LSB) steganography in color and grayscale images is presented in this paper. In order to detect minute changes brought about by data embedding in the LSB plane, the authors suggest statistical methods. Their method compares embedding patterns and noise characteristics, which vary predictably when data is hidden using LSB techniques. Even when tiny amounts of data are concealed, the detection algorithm exhibits high sensitivity and estimates the message length. In terms of accuracy and robustness, the approach performs noticeably better than conventional histogram-based detection.[8]

3. EXISTING SYSTEM

The least-significant-bit (LSB)-based approach is a popular type of steganographic algorithms in the spatial domain. However, we find that in most existing approaches, the choice of embedding positions within a cover image mainly depends on a pseudorandom number generator without considering the relationship between the image content itself and the size of the secret message. Thus the smooth/flat regions in the cover images will inevitably be contaminated after data hiding even at a low embedding rate, and this will lead to poor visual

quality and low security, particularly for images with a lot of smooth areas, according to our analysis and thorough testing. A steganographic technique based on the pixel-value differencing (PVD) method and least-significant-bit (LSB) replacement is introduced. First, the PVD method is used to obtain a different value from two consecutive pixels. A smooth area can have a small difference value, while an edged area has a large one. The LSB technique conceals the secret data in the cover image's smooth regions while utilizing

the PVD technique in the bounded regions. Due to the variable range width and the difficulty of guessing the area where the secret data is hidden by the LSB or PVD method. to calculate the approximate number of secret bits that will be incorporated into the two pixels. A k-bit LSB substitution method is used to embed pixels in the

edge areas, where the value of k is greater than that of the pixels in the smooth areas. Adaptively, the range of difference values is separated into three levels: lower, middle, and higher. The k-bit LSB substitution method embeds both pixels for any consecutive pair of pixels. The level to which the difference value belongs determines the adaptive value k. The majority of Current steganographic techniques typically presume that the LSB of natural covers is negligible and sufficiently random, allowing for the free selection of the pixels or pixel pairs for data hiding using a PRNG. This presumption isn't always accurate, though, particularly for pictures with a lot of smooth areas.

3.1 DISADVANTAGES

3.1.1 Complexity in Implementation:

- Combining both LSB and PVD techniques makes the algorithm more complex.
- Adaptive range division and calculation of pixel differences require additional computation and logic.

3.1.2 Edge Detection May Be Inaccurate:

- The effectiveness of PVD depends heavily on accurate detection of edge and smooth areas.
- Misclassification can lead to noticeable distortions or inefficient embedding.

4. PROPOSED SYSTEM

In this paper, we consider dig-ital images as covers and investigate an adaptive and secure data hiding scheme in the spatial least-significant-bit (LSB) domain. LSB replacement is a well-known steganographic method. In this embedding scheme, only the LSB plane of the cover image is overwritten with the secret bit stream according to a pseuo random number generator (PRNG). As a result, some structural asymmetry (never decreasing even pixels and increasing odd pixels when hiding the data) is introduced, and thus it is very easy to detect the existence of
hidden message even at a low em-bedding rate using some reported steganalytic algorithms, such as the Chi-squared attack, regular/singular groups (RS) analysis , sample pair analysis, and the general framework for structural steganalysis
. This paper presents a novel steganographic algorithm based on the spatial domain: Selected least Significant Bits (SLSB). It works with the least significant bits of one of the pixel color components in the image and changes them according to the message's bits to hide. The rest of bits in the pixel color component selected are also changed in order get the nearest color to the original one in the scale of colors. This new method has been compared with others that work in the spatial domain and the great difference is the fact that the LSBs bits of every pixel color component are not used to embed the message, just those from pixel color component selected.

4.1 ADVANTAGES

Better Visual Quality (Low Distortion): After embedding, the rest of the bits in the selected component are adjusted to achieve a color closest to the original.This minimizes visible changes and preserves the image's visual appearance, which is important for perceptual invisibility. Adaptive Embedding: Instead of blindly embedding into every LSB, the method selectively targets LSBs in specific color components (e.g., R, G, or B), improving both adaptability and flexibility based on image characteristics.

System Architecture

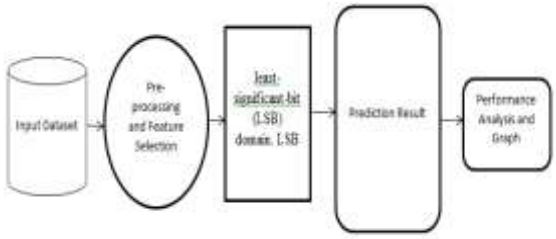

Fig 4.1.1 System Architecture

5. MODULE DESCRIPTION

5.1 Image Preprocessing Module

Purpose: Prepare the cover image for data embedding.

Functions: Load and validate the input image (ensure it's in a lossless format like BMP or PNG).Convert the image into pixel array format for easier manipulation.

Determine each pixel's Red, Green, and Blue (RGB) components.

Identify potential embedding regions (based on smoothness or texture if extended).

5.2 Secret Message Handling Module

Purpose: Prepare the secret message for embedding.

Functions: Accept text or binary data as input.Convert the message into a binary bitstream.Optional: Encrypt or compress the message for added security or efficiency.

5.3 Component Selection Module (SLSB Core)

Purpose: Determine which color component (R, G, or B) to use for embedding.

Functions: Use a pre-defined rule or randomness (e.g., PRNG with key) to select one color component per pixel.Maintain consistency so that the extraction process can correctly identify the selected components.

5.4 Data Embedding Module (Selected LSB with Color Approximation)

Purpose : Embed the secret data into selected color components using the SLSB approach.

Functions: Embed secret bits only into the LSBs of selected color components of pixels.Adjust the higher bits of the same component to maintain visual similarity (find the nearest valid color after embedding).

- Avoid modifying all color components or using fixed LSB patterns to improve stealthiness.

5.5 Stego Image Generation Module

Purpose:
Generate and save the final image with embedded data.

Functions: Merge the modified RGB components back into pixel format.Save the subsequent copy as the stego-image.Ensure no metadata or visible difference reveals the hidden content.

5.6 Data Extraction Module

Purpose: Retrieve the concealed message after the stego-image.

Functions: Accept the stego-image and the original embedding key (if used).Re-identify the selected color components based on the same strategy used during embedding.Extract the LSBs from the identified components.Reconstruct the original message bitstream.

5.7 Security & Steganalysis Resistance Module

Purpose: Enhance and verify the resistance to common attacks.

Functions: Apply techniques to reduce structural asymmetry (e.g., adjusting even/odd balance).Randomize embedding positions where applicable.Perform self-tests against known steganalysis methods like: Chi-squared test,RS analysis,Sample pair analysis

5.8 User Interface (Optional Module)

Purpose: Provide a user-friendly interface for image and message input/output.

Functions: Allow users to load images and messages via GUI.Provide options to view stego-image and extracted message.Visual feedback on embedding success and image quality.

6.RESULT

The proposed steganographic system significantly improves upon the existing approach in terms of visual quality, embedding efficiency, and resistance to detection. While the existing system relies on a mixture of Slightest Important Minute spare and Pixel Worth Differencing it often leads to noticeable distortion in smooth regions of images, reducing both imperceptibility and security. This is because it does not fully consider the local content characteristics during embedding, relying heavily on pseudorandom selection. In contrast, the proposed system introduces a Selected Smallest Important Minute method that adaptively chooses which pixel color components to modify, and further adjusts surrounding bits to preserve the original pixel color as much as possible. This results in greatly enhanced image quality, with minimal visual degradation even at higher embedding rates. Additionally, the adaptive selection strategy in the proposed method increases resistance against common steganalysis techniques like Chi-squared analysis and RS attacks. Overall, the proposed system offers better payload capacity, enhanced security, and superior visual fidelity compared to traditional LSB and PVD-based methods.

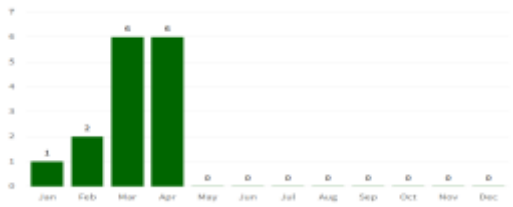

Fig 6.1 Graph

7.CONCLUSION

In conclusion, the proposed steganographic method based on Designated Smallest Important Minutes (SLSB) offers a more secure, adaptive, and visually imperceptible approach to statistics beating in numerical descriptions compared to traditional LSB and PVD techniques. By intelligently selecting specific pixel color components and fine-tuning their values to closely match the original color, the method significantly reduces distortion, especially in smooth regions where traditional methods often fail. Additionally, the adaptive nature of the embedding process enhances resistance to various steganalysis attacks, thereby improving the overall refuge of the concealed statistics. The results clearly demonstrate that the proposed SLSB technique achieves a better balance between embedding capacity, image quality, and steganographic security, making it a additional healthy and reliable solution for secure image-based communication.

8.REFERENCES

[1]. Wu Da-chun, Tsai Wen-Hsiang "A Steganographic Method for Images by Pixel Value Differencing," *Pattern Recognition Letters*, 2024

[2]. Wang Chung-Ming, Wu Nan-i Tsai Chwei-shyong et al. "A High Quality Steganographic Method with Pixel Value Differencing and Modulus Function," *Journal of Systems and Software*, 2020

[3]. Zhang Xinpeng, Wang Shuozhong. "Vulnerability of Pixel Value Differencing Steganography to Histogram Analysis and Modification for Enhanced Security," *Pattern Recognition Letters*, 2019

[4]. BU Long, HU Bo "An improved steganographic method by pixel-value differencing," *Journal of circuits and systems*, 2018

[5]. Chan Chi-Kwong, Chen Lee-ming ""Using Simple LSB Substitution to Hide Data in Images," The pattern *Recognition*, 2019

[6]. Zheng jiangyun, Jiang julang. "Image quality assessment algorithm based on sense capacity," *Computer engineering*, 2017

[7]. Fridrich J, Goljan M, Du R. "Reliable Identification of LSB Steganography in Color and Grayscale Images," Proceedings of the ACM Workshop on Multimedia and

security, 2019.

[8]. Fridrich, J., Goljan, M., & Du, R. (2001). *Reliable Detection of LSB Steganography in Grayscale and Color Images*. In Proceedings of the ACM Workshop on Multimedia and Security (pp. 27–30). ACM.