IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

The Image Steganography Using LSB And PVD Algorithms

[1]Akshitha S, [2]Ananya Desai S, [3]Aishwarya MS, [4]Sahana S U, [5]Prof.Sridhar R

[1,2,3,4] UG Student, Department of Information Science and Engineering, Global Academy of Technology, Bengaluru.

[5]Assistant Professor, Department of Information Science and Engineering, Global Academy of Technology, Bengaluru.

ABSTRACT:

A method for concealing important information in digital photos without altering their appearance is image steganography. In human history, data privacy has always been significant, whether on a global or personal scale. In past centuries, the confidentiality of data has been significant, whether on a global or personal scale. As digital technologies develop, a wider range of data types and techniques are available. Any information sent over transmission routes can be concealed. It's an art to conceal private information in publicly accessible news. Although cryptography cannot be perceived as its substitute or an alternative to it, steganography is recognised as an extra layer of protection. Picture steganography, which involves hiding hidden messages in the cover image, can be used for secure communication. a method of hiding where the secret information is inserted such that it cannot be seen by unauthorised individuals and cannot be seen by the human eye. For the purposes of secure communication, picture steganography, which comprises concealing secret messages in the cover image, can be employed. a concealment in which the secret data is embedded in such a way that it is impossible for unauthorised persons to view and undetectable to the human eye. Pixel value differencing (PVD) and least significant bit (LSB) replacement are the two most often used techniques for concealing information in photographs. The LSB approach works by swapping a bit of the secret message for each pixel in the cover image's least significant bit. Instead, the PVD method embeds the secret information by calculating the difference between the pixel values of neighbouring pixels. The algorithms are resistant to a variety of assaults, ensuring that the hidden message is kept.

Keywords – Secret picture, cover picture, pixel value differentiating, stegno picture, least significant bit.

1. INTRODUCTION

Photo steganography is an intriguing discipline that blends the skill of hiding information internally inside digital photographs with data security science. In today's interconnected world, were privacy and secure communication are of utmost importance, steganography offers a clever and inconspicuous way to conceal sensitive data. The behavior of embedding secret information or messages into an image while maintaining its visual integrity is the essence of image steganography. The main objective is to protect the embedded data from casual viewers and any other unauthorized individuals. This method makes advantage of the enormous quantity of extraneous or unneeded

data that is available in photographs, such as the fine colour fluctuations, pixel intensity differences, or frequency components of the image.

The process of image steganography involves two crucial components: the cover image and the secret message. The cover image acts as a carrier for the hidden data, while the secret message represents the information to be concealed. By cleverly manipulating the cover image, the secret message is seamlessly incorporated, making it virtually indistinguishable to the naked eye. Various algorithms and methodologies exist to achieve this concealment. Some common techniques include least significant bit (LSB) substitution, where the least significant bits of the pixel values are replaced with the secret message bits.

To incorporate the data in a more resilient and unnoticeable manner, transform domain techniques like the discrete cosine transform (DCT) or wavelet transform might be used. The applications of image steganography are diverse and range from covert communication and information hiding to digital watermarking and authentication. It has found relevance in fields like journalism, law enforcement, military operations, and even digital forensics. However, it's important to note that while steganography can be used for legitimate purposes, it can also be misused for malicious activities, necessitating the need for advanced detection techniques. As technology continues to advance; image steganography remains an intriguing and evolving field Researchers continually explore new techniques and algorithms to enhance the security and robustness of steganographic systems, while also developing sophisticated methods to detect and counteract hidden information. By understanding the principles and intricacies of image steganography, we can appreciate its potential and better safeguard our digital communications and data.

2. LITERATURE REVIEW

"An Improved Image Steganography Algorithm Based on Hybrid-Domain Features and Genetic Optimization" by Guo et al: Based on hybrid-domain characteristics and evolutionary optimization, this research developed a unique picture steganography technique**.** The algorithm used wavelet transform, discrete cosine transforms

(DCT), and singular value decomposition (SVD) to embed secret data in images. The genetic algorithm was used to optimize the embedding process. The proposed algorithm achieved high embedding capacity and good visual quality. However, it had relatively high computational complexity.

A Novel Approach for Image Steganography Using LSB and PVD Techniques with Cryptographic Algorithms: Techniques LSB and PVD Using Cryptographic Algorithms This research suggests a unique way for picture steganography combining cryptographic algorithms with both the LSB and PVD approaches. A high level of security and resilience against many forms of assaults is the aim. The three key stages of the suggested method are embedding, encryption, and extraction.

"Multi-channel PVD-based Steganography with Pixel-level Modification for Text and Image" by Park et al: The secret data is then embedded in each channel of the split cover picture using the suggested method's multi-channel PVD technique. The cover image pixels that have been altered by PVD embedding are then modified at the pixel level to increase security. Finally, a form of scrambling is used to further obscure the stego-image.

"An Improved Image Steganography Algorithm Based on Hybrid-Domain Features and Genetic Optimization" by Guo et al: This research introduced a revolutionary hybrid-domain and genetic optimization-based picture steganography technique. In order to embed hidden data in photos, the method employed wavelet transform, discrete cosine transforms (DCT), and singular value decomposition (SVD). The embedding procedure was optimized using the genetic algorithm. The suggested approach produced good visual quality and a high embedding capacity. But the computational complexity was rather significant.

"A High-Capacity Image Steganography Method Based on DCT and Multi-Level Quantization" by Yang et al: This paper proposed a high-capacity image steganography method based on DCT and multi-level quantization. The method used DCT to transform the cover image, and then quantized the transformed coefficients at multiple levels to hide secret information. The suggested technique produced a high embedding capacity and good visual quality. However, it had relatively low robustness against certain attacks. “Image in image steganography” by Jassim F. and Shuchi Sharma (2021) alleged to use the YIQ color space model and RGBA based cover image. The RGB values of the secret picture pixels are transformed into YIQ colour space before being inserted in the least significant bits of the cover image's colour pixels as well as the alpha channel. Their findings show that it is feasible to conceal one picture within an additional photo while preserving appropriate image resolution.

3. PROPOSED SYSTEM

The proposed system's two main components are a steganography encoder and a steganography decoder. The steganography encoder must hide the secret message in the cover picture, and the steganography decoder must extract it from the stego image. The proposed technique for adaptive colour picture steganography employs the

concept of neighboring PVD and LSB. The memory allocation and quality of extracted images are compared to find which algorithm is more efficient. To develop and find an effective and robust steganography technique that can hide large amounts of data within images while maintaining high levels of imperceptibility, quality and security against various attacks.

The goal of the system for Image Steganography Using LSB and PVD Algorithms that has been developed is to provide a more effective and secure way to conceal sensitive information inside digital photos. The system seeks to accomplish the following particular goals:

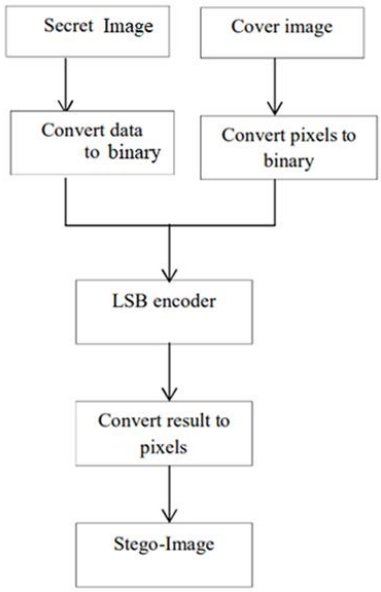
- To provide a safe means of concealing data in digital media.
- To be difficult to detect.
- To be able to hide a variety of data, including text, images, audio, and video.
- Enhanced Data Hiding Capacity.
- Imperceptibility and Robustness.
- Evaluation and Analysis.

4. METHODOLOGY

An approach to spatially adaptable color image steganography envelop LSB substitution and the concept of neighbor PVD. It applies the concept of nearby PVD. To completely use the edge pixels, the approach divides the three planes [red (R), green (G), and blue (B)], into discontinuous blocks of size 3X3. Based on the tolerance capacity of each plane, the technique embeds movable hidden bits. The suggested adaptive colour picture steganography method makes use of the neighbouring PVD and LSB concepts.

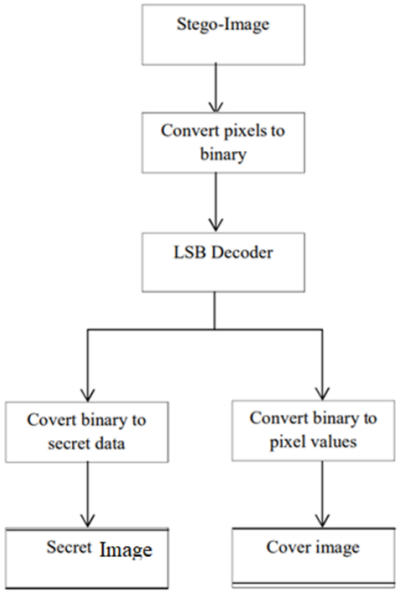
- Memory allocation and image quality are compared to determine which approach is more efficient.
- To create and discover an efficient and resilient steganography approach capable of concealing enormous quantities of data within images while retaining high levels of imperceptibility, quality, and security against diverse assaults.

Steps In LSB Encoder:



1. Enter the secret information, like a picture that has to be isolated.
2. Type in the [256x256] cover (original) picture.
3. Transform each text or pixel's ascii value, which is the confidential data.
4. Transform the cover image's pixel value into binary representation.
5. Use an LSB encoder to hide each text or image bit LSB bit of each cover image's 8-pixel value.
6. The result is reconverted to pixel values in order to produce the stego-image.

Steps In LSB Decoder:



1. Enter the stego picture first.
2. Binary representation of the pixel value.
3. Use the LSB decoder, whose purpose is to recover the hidden information from the stego-image.
4. To obtain the desired result, the hidden picture and the cover picture are separated jointly.

PVD Encoding:

The procedures that are normally taken to use PVD to encrypt the cloistered message are as follows:

1. Divide the cover image into non-overlapping blocks of pixels.
2. Choose the hidden message you want to embed and convert it to binary format.
3. For each block of pixels, select a pixel pair consisting of adjacent pixels with a small difference in their pixel values.
4. If the LSB of the secret message is 1, add a small positive value to the larger pixel value in the pair, and subtract the same value from the smaller pixel value. If the LSB is 0, do the opposite.
5. For every pixel block, repeat step 4 until the full hidden message has been implanted. The PVD technique is effective in steganography because the small changes made to the pixel values are typically imperceptible to the human eye.

Pixel Value Differencing Decoding:

The methods that are often employed used to use PVD to decipher the secret message are as follows:

1. Block the pixels in the steganographic picture so that they don't overlap.

2.For each block of pixels, select a pixel pair consisting of adjacent pixels with a small difference in their pixel values.

3.Calculate the difference between the larger and smaller pixel values in the pair.

4. The LSB of the concealed message is 1 if the difference is positive. The LSB of the concealed message is zero if the difference is negative.

5.Repeat steps 3 and 4 for each block of pixels until the entire hidden message has been extracted.

5. IMPLEMENTATION

There are several ways to implement picture steganography via the LSB and PVD techniques. Utilising a programme that applies the algorithms is one method. Implementing the algorithms in a programming language is an additional method. We are implementing this project by applying the following modules:

- LSB Encoding and Decoding
- PVD Encoding and Decoding

The implementation begins with the loading of the cover picture, which will be utilised to conceal the hidden message. To prepare the picture for the steganography process, pre-processing activities such as scaling or noise reduction may be conducted. Concurrently, the secret message is prepared by converting it to binary format and representing it as a sequence of bits.

The cover image's individual pixels are then iterated over in order to implement the LSB method. The pixel value is converted to binary, and the corresponding bit from the secret message is swapped for each pixel's least significant bit. The updated stego image with the hidden secret message is created by repeating this process until all of the secret message's bits are added. To increase the capability for data hiding, the PVD algorithm is applied. The revised Stego image is examined, and new bits of the secret message are added by using the differences in pixel values between nearby pixels. To disguise the bits, the pixel values are modified correspondingly. This operation is continued until all of the secret message's bits have been implanted, resulting in an upgraded stego picture with increased data concealing capability.

6. MODULES

User Interface: The user interface part of the system allows the user to communicate with it, input photos, adjust parameters, and get results.

Data Embedding Module: Using PVD and LSB techniques, this module embeds the cover image's hidden message.

The Steganography Quality Evaluation Module assesses the effectiveness of the steganography technique and offers comments on the message's imperceptibility.

Output Module: The output module displays to the user the extracted message and the embedded image in an appropriate format. Storage Module: The storage module safeguards the input and output photos as well as any other pertinent data.

Performance Metrics Module: This module tracks the system's efficiency, including the amount of time it takes to embed a message, its processing power, and the calibre of the message that is ultimately retrieved.

A. LSB Steganography:

The LSB (Least Significant Bit) steganography technique may be used to conceal information by employing the least significant bit of each pixel in a digital picture. It makes use of the fact that changing the least significant portion of a pixel has little impact on the image's overall visual quality, making it a suitable method for covert communication.

B. PVD Steganography:

Utilising the changes in pixel values between consecutive pixels in an image, PVD (Pixel Value Differencing) steganography is a method for hiding hidden information in digital images. Compared to conventional LSB steganography, PVD offers a greater capability for data concealment while yet retaining visual imperceptibility.

7. RESULTS

LSB steganography is shown to decode images less accurately than PVD steganography. It also uses less memory than LSB since the technique directly impacts the data in the cover image. With a distinct secret key array for each algorithm deployment, PVD adds an extra degree of protection. Even aesthetically, PVD obscures pictures more effectively than LSB, where a flimsy hidden image might be seen. The longer time needed to complete the encoding and decoding operations seems to be PVD's primary drawback. However, it may be said that in many aspects, PVD is a superior steganography algorithm to LSB.

1.Menu page

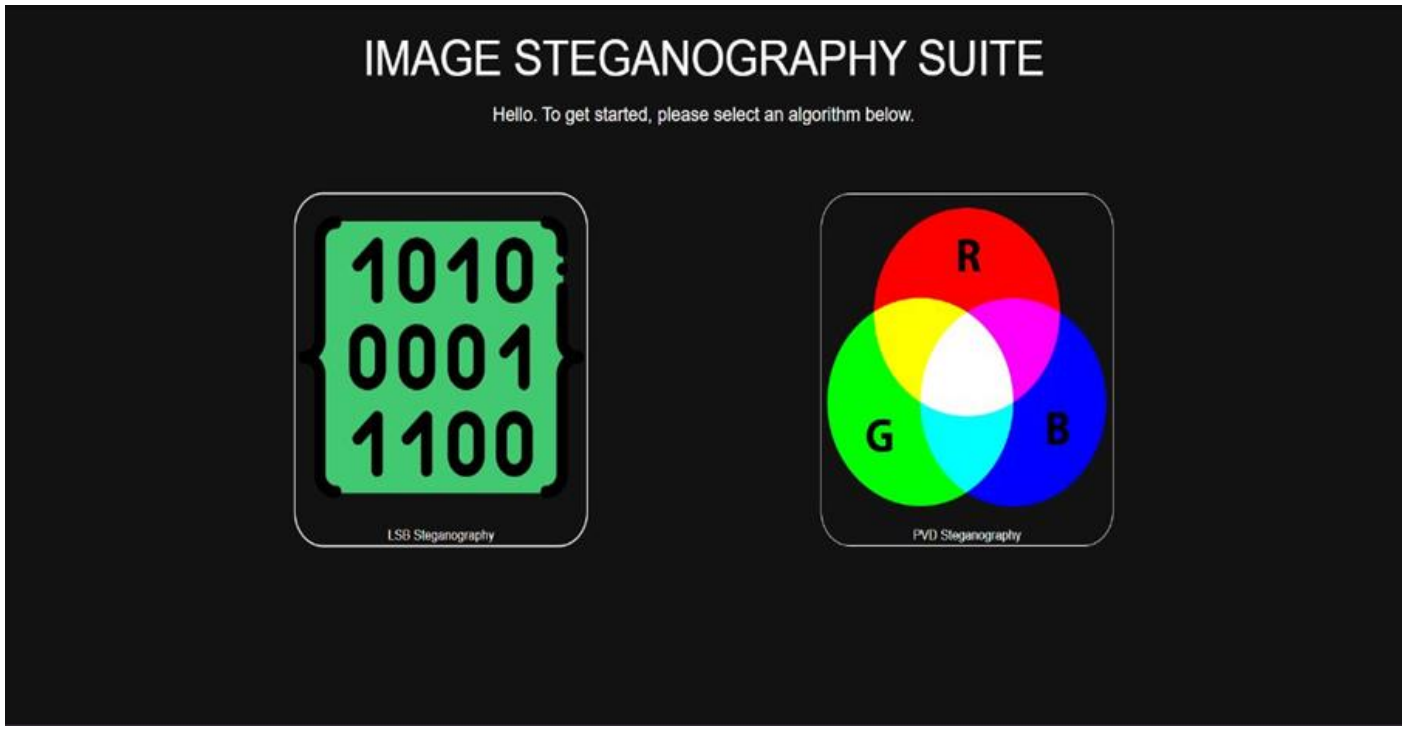


Figure 7.1: Menu Page

2.LSB Steganography

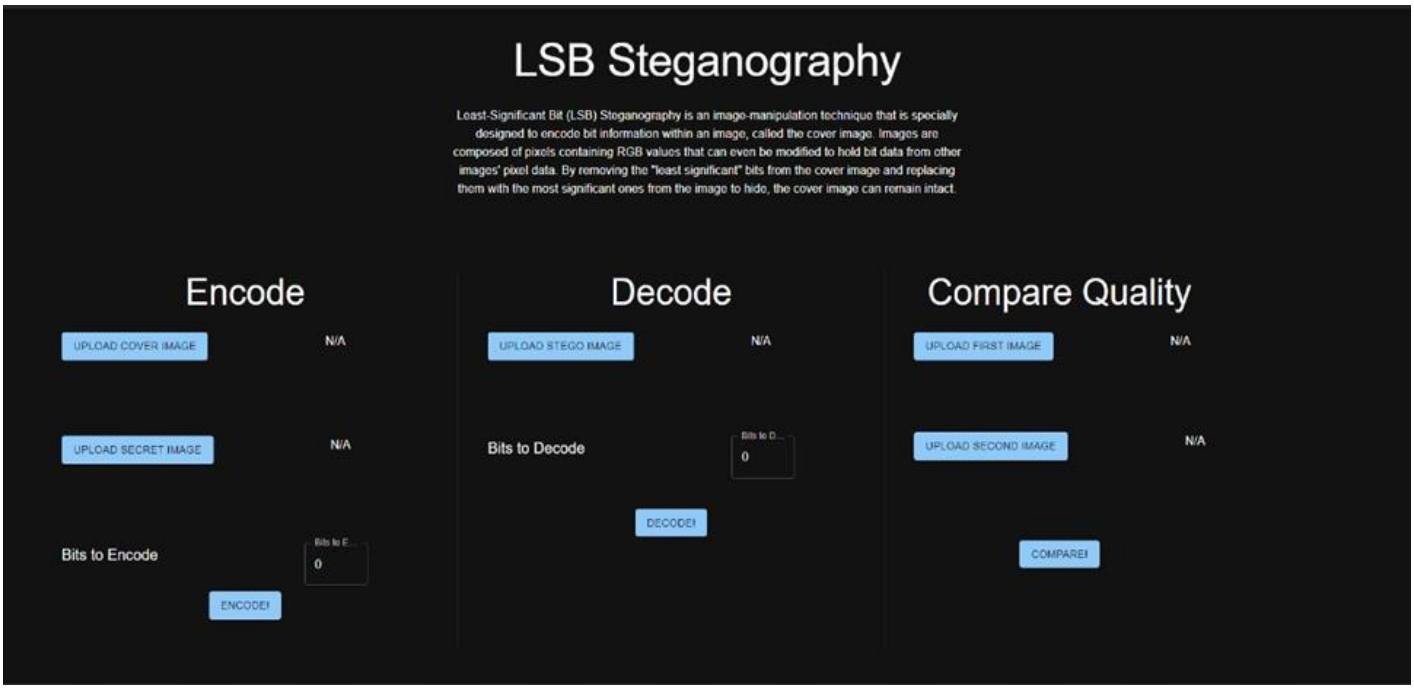


Figure 7.2: LSB Steganography

3.LSB Encoding

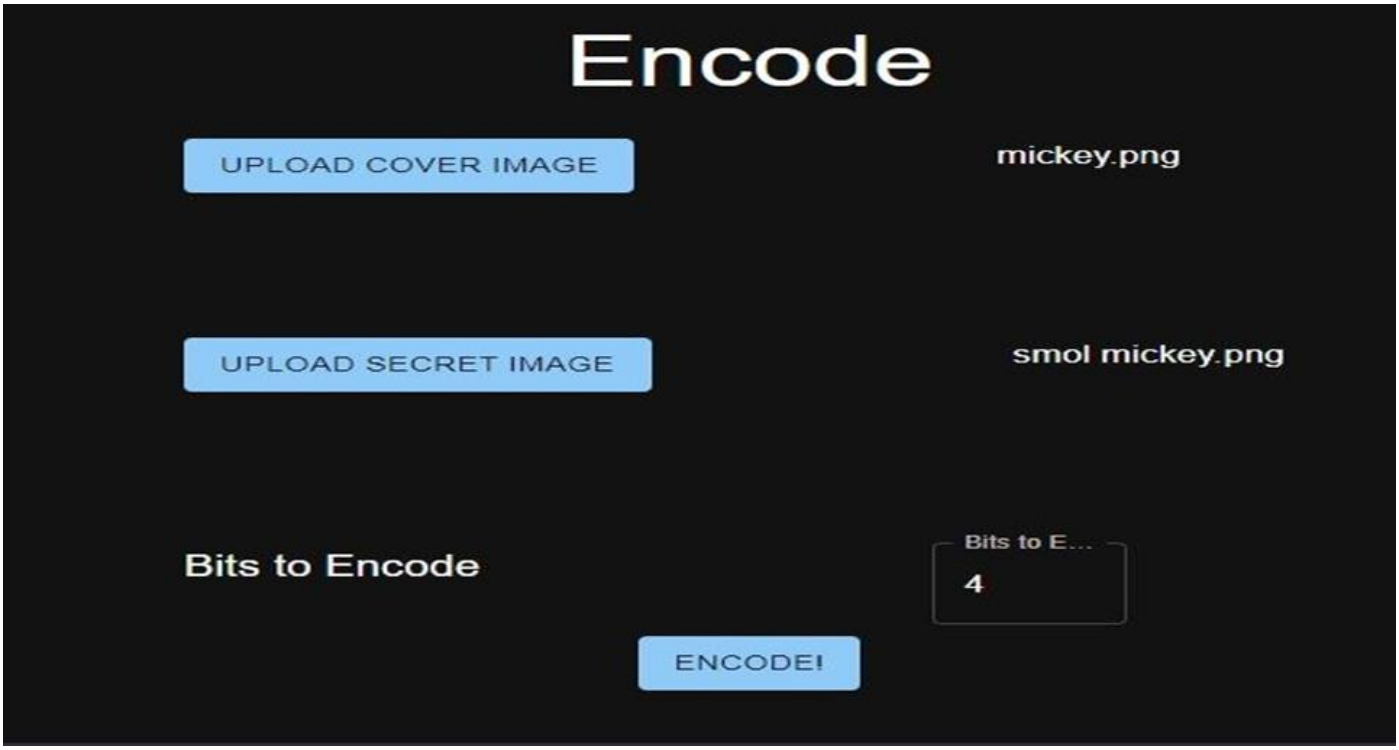


Figure 7.3: LSB Encoding

4.LSB Decoding

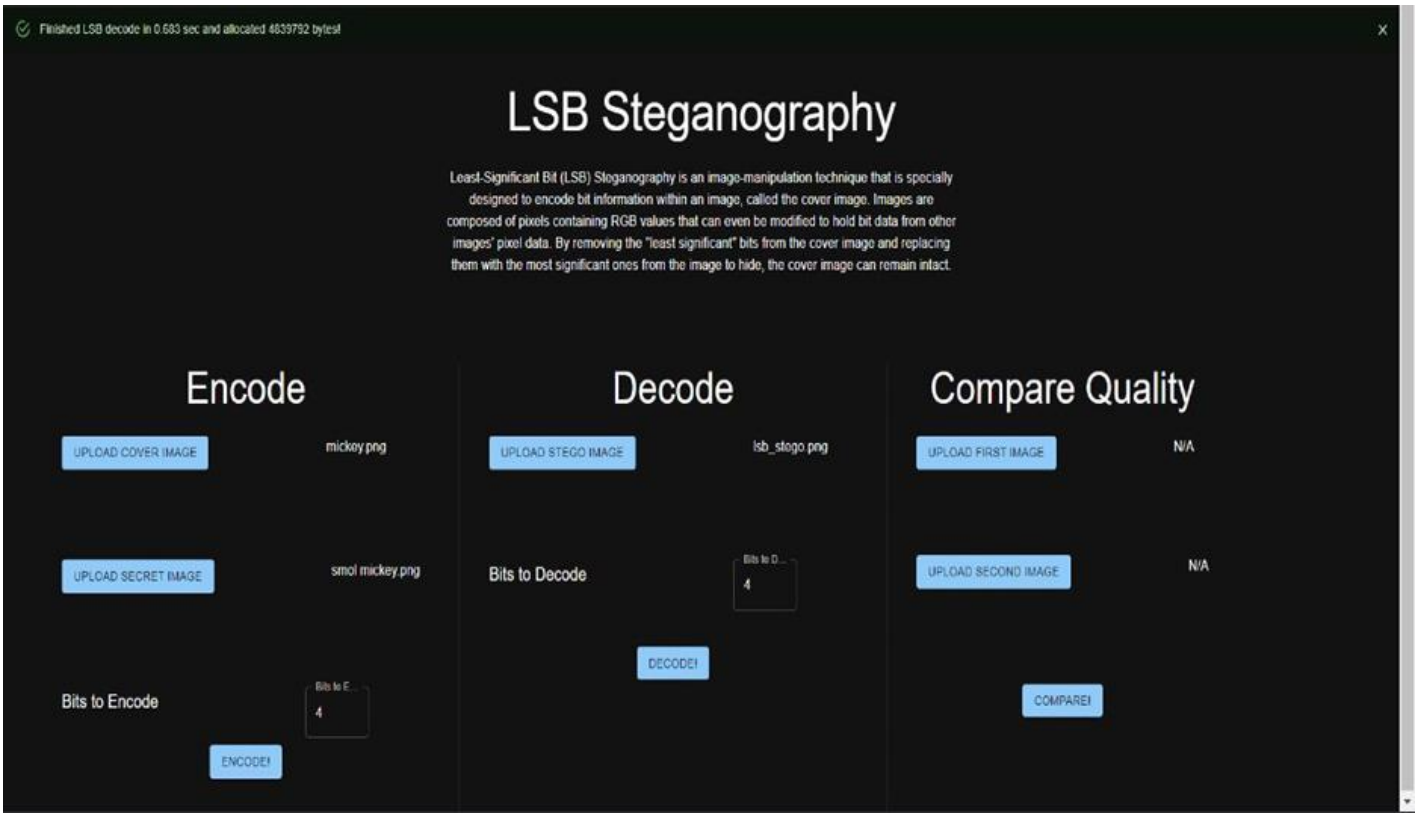


Figure 7.4: LSB Decoding

5.LSB quality Comparison

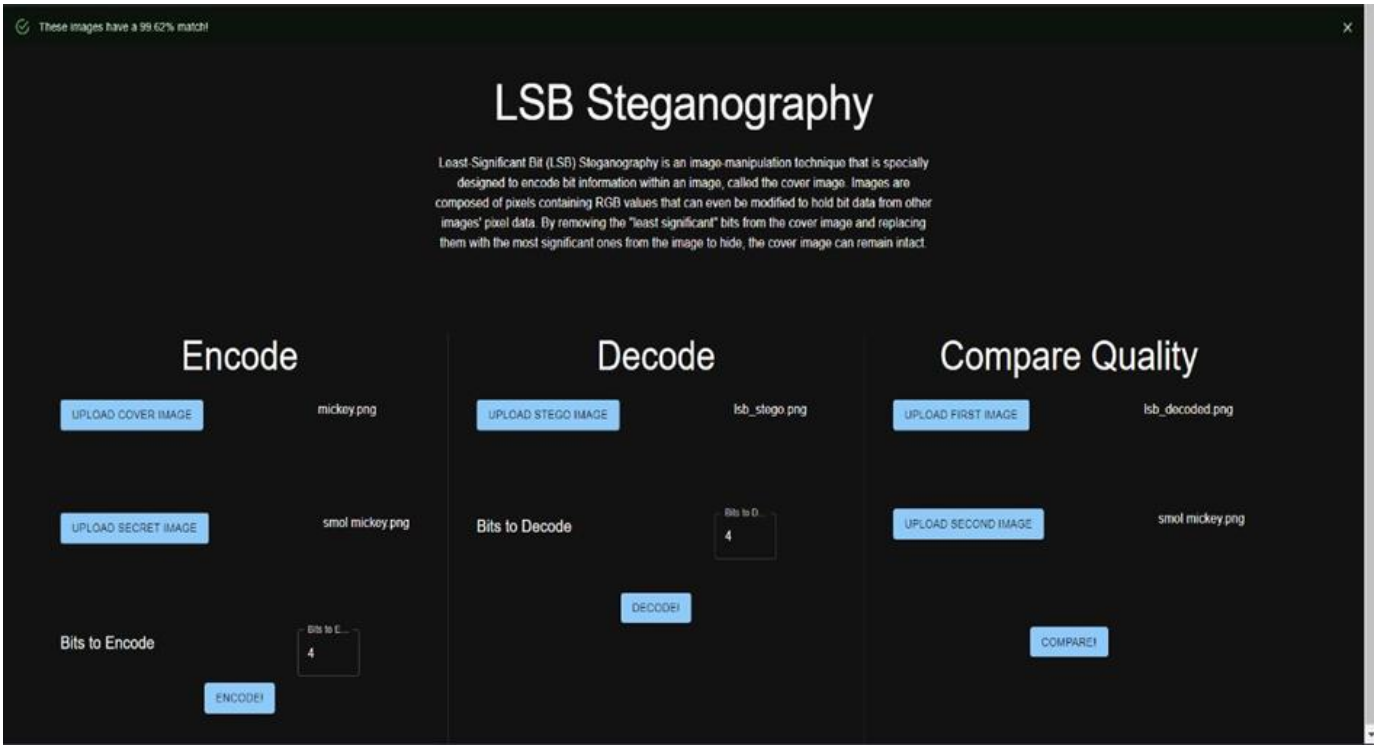


Figure 7.5: LSB quality Comparison

6.PVD Steganography

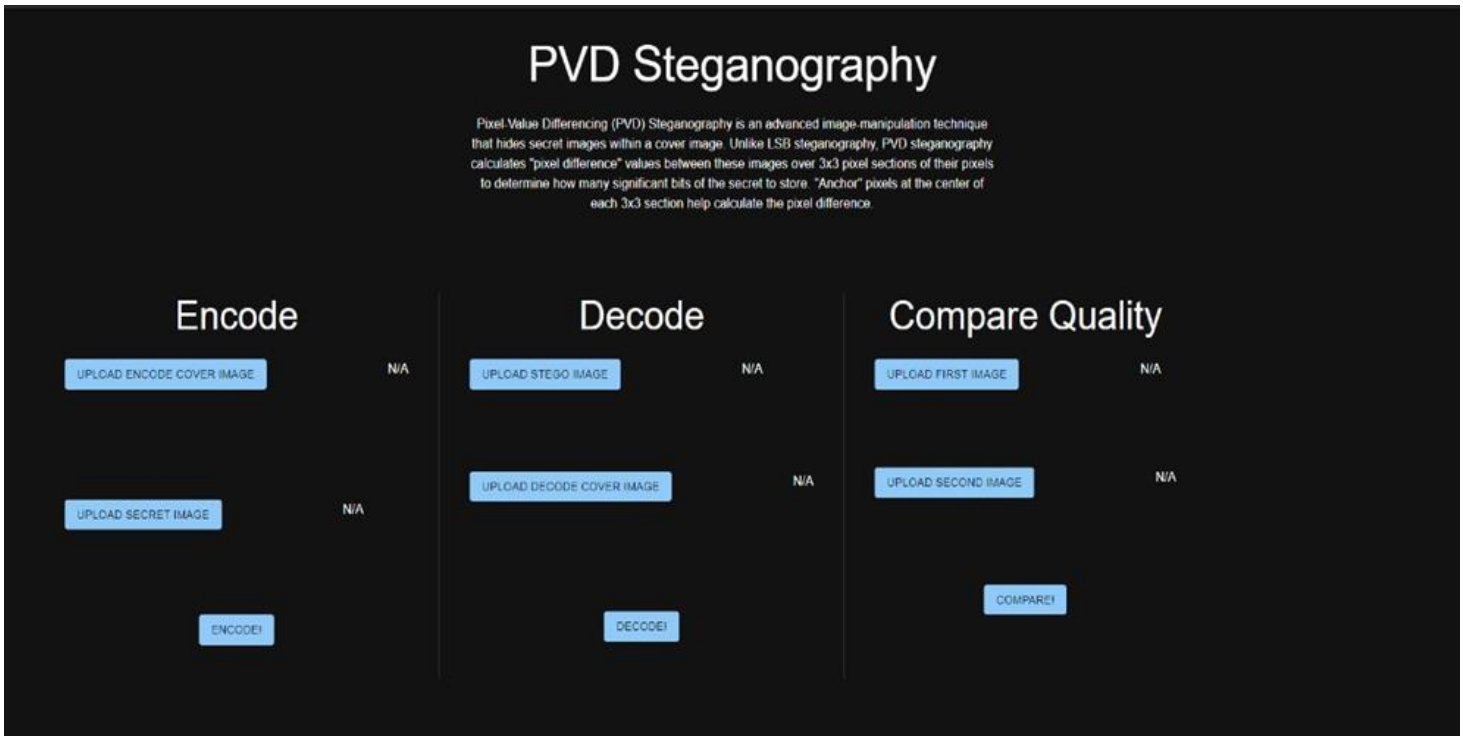


Figure 7.6: PVD Steganography

7.PVD Encoding



Figure 7.7: PVD Encoding

8.PVD decoding

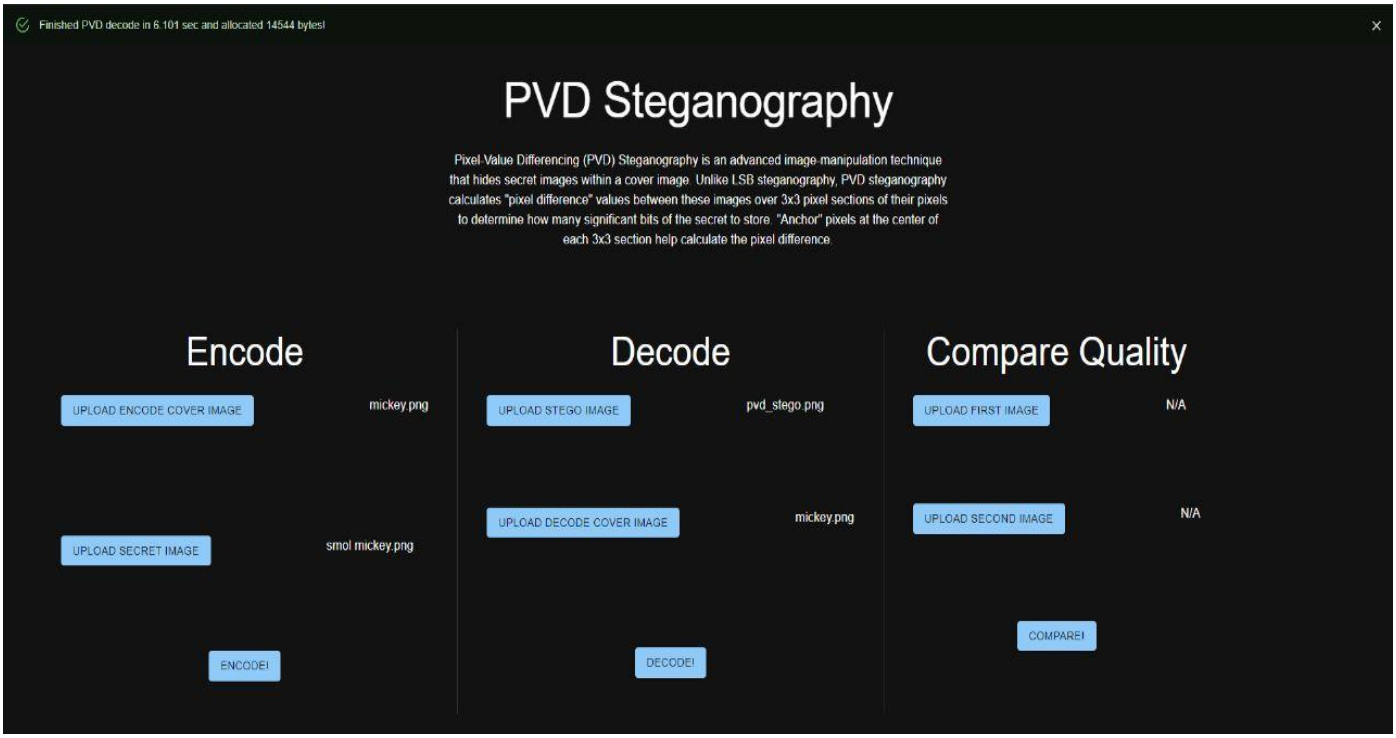


Figure 7.8: PVD decoding

9.PVD quality comparison

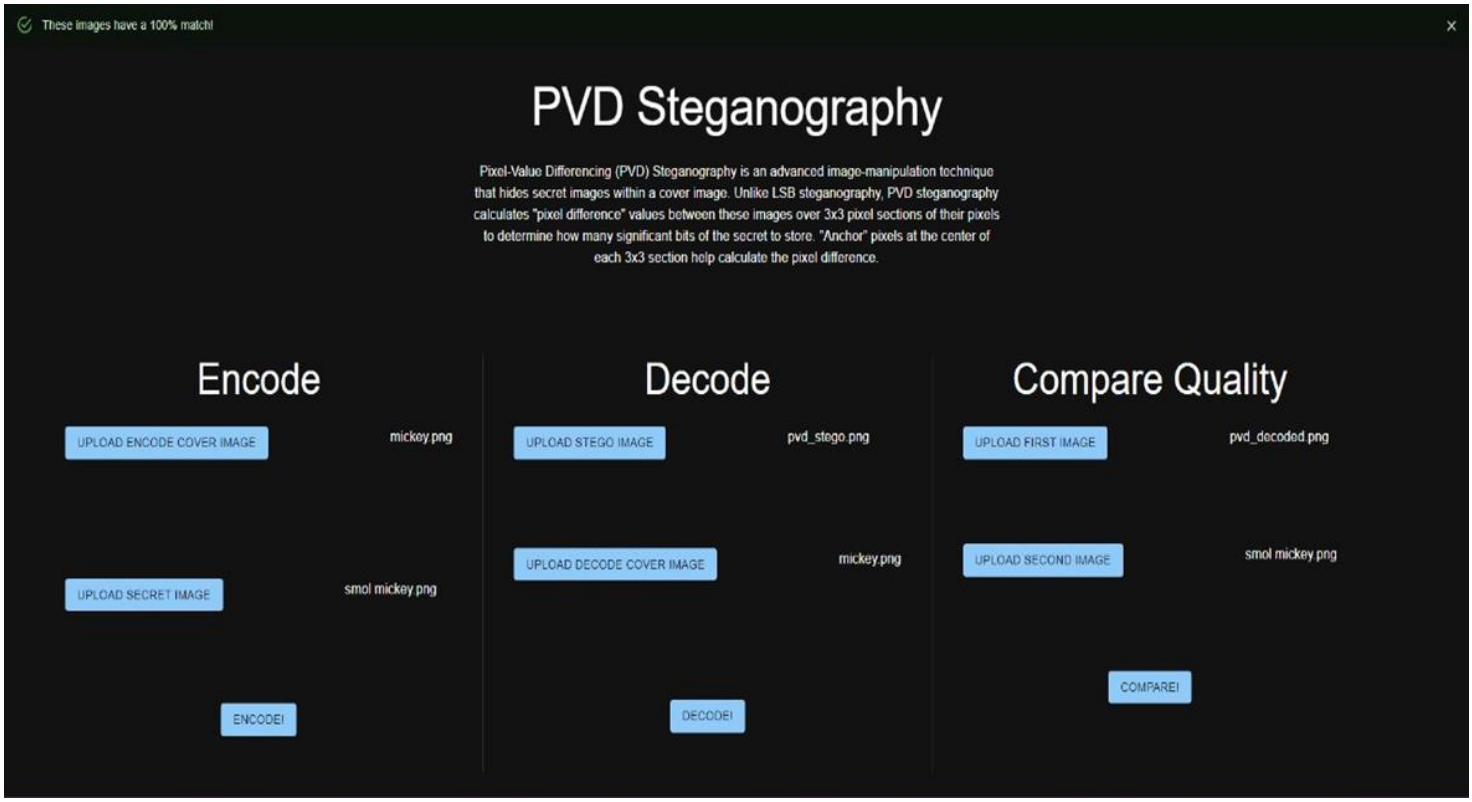


Figure 7.9: PVD quality comparison

8. FUTURE SCOPE

Steganography is a real-world invention that enables anonymous information transfer via a communications channel. A staggered picture is created by fusing the carrier image with the overlooked image. Without retrieval and an explicit retrieval method, the hidden image is hard to find. Future research into the use of PVD for the steganography of other forms of material, such as audio and video, is accessible.

9.CONCLUSION

The fact that PVD decodes pictures more accurately than LSB was successfully found. Since the approach directly affects the data in the cover picture, it requires less RAM to function properly than LSB. PVD increases security by providing a unique secret key array with each algorithm deployment. However, it may be said that in many aspects, PVD is a more accurate steganography algorithm than LSB.

REFERENCES

[1] Ahani, S., and S. Ghaemmaghami. 2015. Colour image steganography method based on sparse representation. IET Image Processing 9 (6):496–505. doi:10.1049/iet-ipr.2014.0351.

[2] Cancelli, G., and M. Barni. 2009. Mpsteg-color: Data hiding through redundant basis decomposition. IEEE Transactions on Information Forensics and Security 4 (3):346–58. doi:10.1109/TIFS.2009.2024028.

[3] Dande, S. C., S. S. Agrawal, and S. R. Hirekhan. 2016. Implementation of colour image steganography using LSB and edge detection technique: A labview approach. In Proceeding of 2016 International Conference on Communication and Signal Processing (ICCSP), IEEE, 1466–1470.

[4] Fridrich, J., M. Goljan, and R. Du. 2001. Reliable detection of LSB steganography in color and grayscale images. Multimedia and Security 3657:27–30.

[5] Garcia-Hernandez, J. J., C. Feregrino-Uribe, R. Cumplido, and C. Reta. 2011. On the implementation of a hardware architecture for an audio data hiding system. Journal of Signal Processing Systems 64 (3):457–68. doi:10.1007/s11265-010-0503-8.

[6] Hussain, M., A. Wahid Abdul Wahab, N. Javed, and K.-H. Jung. 2016. Recursive information hiding scheme through LSB, PVD shift, and MPE. IETE Technical Review 35 (1): 53–63. DOI: org/10.1080/02564602.2016.1244496.

[7] Johnson, N. F., and S. Jajodia. 1998. Exploring steganography: Seeing the unseen. Computer Magazine 2 (2):26–34. doi:10.1109/MC.1998.4655281.

[8] Jung, K.-H., and K.-Y. Yoo. 2014. Three-directional data hiding method for digital images. Cryptologia 38 (2):178–91. doi:10.1080/01611194.2014.885817.

[9] Kalita, M., and T. Tuithung. 2016. A novel steganographic method using 8-neighboring PVD (8NPVD) and LSB substitution. In Proceedings of International Conference on Systems, Signals and Image Processing. Vol. 1, IWSSIP, IEEE, 15.

[10] Kutter, M., and F. A. P. Petitcolas. 1999. A fair benchmark for image watermarking systems. Electronic Imaging 3657:25–7. Lee, C.-F., and H.-L. Chen. 2010. A novel data hiding scheme based on modulus function. Journal of Systems and Software 83 (5):832–43. doi:10.1016/j.jss.2009.12.018.