International Journal of Research and Review
DOI: https://doi.org/10.52403/ijrr.20210948
Vol.8; Issue: 9; September 2021
Website: www.ijrrjournal.com
Research Paper *E-ISSN: 2349-9788; P-ISSN: 2454-2237*

A Comparative Analysis of LSB, MSB and PVD Based Image Steganography

Alade Oluwaseun. Modupe[1], Amusan Elizabeth Adedoyin[2], Adedeji Oluyinka Titilayo[3], Fenwa Olusayo Deborah[4]

[1,2] Senior Lecturer, [4]Associate Professor, Department of Cyber Security Science,
[3]Senior Lecturer, Department of Information System,
Ladoke Akintola University of Technology, Ogbomoso, Oyo State Nigeria

Corresponding Author: Amusan E.A and Adedeji O.T.

ABSTRACT

Steganography is the art and science of hiding information by embedding data into cover media. Numerous techniques are designed to provide the security for the communication of data over the Internet. A good steganographic algorithm is recognized by the performance of the techniques measured with the support of the performance metrics among which are PSNR, MSE, SSIM, robustness and capacity to hide the information in the cover image. In this paper a comparative analysis of Least Significant Bit (LSB), Most Significant Bit (MSB) and Pixel Value Differencing (PVD) image steganography in grayscale and colored images was performed. Three different cover images were used to hide secret message. A comparative performance analysis of LSB, MSB and PVD methods used in image steganography was performed using peak signal to noise ratio (PSNR), Mean square error (MSE) and Structural Similarity index (SSIM) as performance metrics. LSB technique gives higher PSNR and SSIM values than MSB and PVD method with lower MSE than the other two techniques. Future research can be geared towards investigating the embedding capacity, security, and computational complexity of each technique.

Keywords: Least Significant Bit (LSB), Most Significant Bit (MSB), Pixel value differencing (PVD), PSNR, SSIM and MSE,

1. INTRODUCTION

Steganography has to do with a way of hiding communicated data in such a way that it remains private. It supports privacy between two communicating parties. In image steganography, privacy is achieved by embedding data into cover image and producing a stego-image (Alade et al, 2021). Image Steganography techniques can be considered under two domains which are spatial domain and transform domain steganography. The secret information is directly inserted into a cover image in a spatial domain approach. Examples of spatial domain techniques are Least Significant Bit (LSB) substitution, Pixel Value Differencing (PVD), Gray level modification method (GLD), Parity Checker method (PCM), Exploiting modification direction (EMD), Diamond encoding method (DEM), Optimal pixel adjustment process method (OPAP), Adaptive pixel pair matching method (APPM). Transform domain approach is used for hiding a huge amount of data. Steganography is divided into four types which are text, image, audio and Protocol.

Steganalysis is a way of noticing the hidden data from stego-image (Fridrich, Goljan, and Du, 2001). RS analysis, Histogram analysis, Chi-square attack, Weighted-Stego (WS) analysis to mention a few are some of the steganalytic attacks on spatial domains (Subhedar, Mankar, 2014). The effectiveness of any steganographic technique can be measures in terms of capacity, distortion measure, security or attack resistance, and computational

complexity. Maximum amount of data that can be hidden inside the image is called the capacity. It is typically characterized in terms of bits per pixel. The distortion in the stego image can be measured by peak signal-to-noise ratio (PSNR). A higher value of PSNR indicates a lesser distortion of the image. Also a good steganographic technique should be resistant to various steganalysis attacks. Computational complexity refers to the time required to hide the data inside the cover image.

2. LITERATURE REVIEW

Anil and Mohit (2012) presented the evaluation of least significant bit (LSB) and most significant bit steganography in a grayscale or RGB image using mean square error as a performance metrics. The results of LSB based steganography and MSB based steganography was presented.

Rohit Garg and Tarun Gulati (2012) focused on the comparison of LSB and MSB Based Steganography in Gray-Scale Images. The results were presented using MSE and PSNR as a performance metrics. The author concluded that LSB based steganography is much better than MSB based steganography for hiding the message.

Rejani, Murugan and Deepu (2015) conducted brief analysis and comparison of different spatial domain image steganography techniques. The author concluded that the modern secure image steganography presented a challenging task of transferring the embedded information to the destination without being detected.

Yu Yu Wai and Ei Ei Myat (2018) presented the comparison of LSB, MSB and new Hybrid (NHB) steganography in digital image. The difference of embedding the data in an image using LSB, MSB and new Hybrid steganography was presented in the paper. Many different secret data formats (txt, docx, xlsx, pdf) were embed in cover image. The image quality was measured with Mean Square Error (MSE) and Peak Signal Ratio (PSNR).

Darwis, Pamungkas and Wamiliana (2020) compare the LSB, Modulus Function (MF), and PVD methods to serve as alternatives to the use of steganography techniques. The results of the study concluded that the LSB method had the best image quality compared to the MF and PVD methods. PVD algorithm had a better capacity than the LSB and MF methods in terms of storage capacity.

Alade et al. (2021) presented firefly algorithm for finding best positions inside cover image in order to embed text message into cover image using Pixel Value Differencing (PVD) technique. The author evaluated the stego image and cover image using Peak Signal to Noise Ratio (PSNR) and Mean square Error (MSE) and concluded that firefly algorithm with PVD technique produced a promising result for image steganography.

In this paper a comparative analysis of LSB, MSB and PVD based image steganography was conducted in grayscale and colored images. Three different cover images were used to hide secret message. A comparison between the results of LSB, MSB and PVD was done in terms of Peak to Signal ratio (PSNR), Mean square error (MSE) and Structural Similarity index SSIM.

3. METHODOLOGY

3.1 Selected Image Steganography Techniques

1. Least Significant Bit Method (LSB)

Least significant bit is the popular method for hiding the message in a digital image. (Chan and Cheng 2004) The message in the least significant bits (LSB‟s) of pixel values of an image is hidden and the binary equivalent of the secret message is distributed among the LSBs of each pixel. It is the common technique used when dealing with images.

Least Significant Bit Algorithm adopted from Chan and Cheng (2004) is given as follows

Algorithm to embed text message:-

Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace LSB of the cover image with each bit of secret message one by one.
Step 5: Write stego image.
Step 6: Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.
Algorithm to retrieve text message:-
Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 8 bit into character.

Advantages OF LSB Technique

- It is used for insertion of data.
- Countless techniques use this method because implementation is very simple.
- Original Image is very similar to stego image.
- There is fewer change for distortion of the original image.
- More data can be embedded into an image.
- Less suspicious to human eyes.

Disadvantages

- Easily retrieved by illegal person.
- Less robust, the concealed data can be lost with image compression.
- Three weakness- Robustness, Tamper and Resistance.
- Very sensitive to any kind of filtering.
- Scaling, Rotation, Cropping, adding extra noise lead to destroy the secret message.

2. Most Significant Bit (MSB) Steganography

Most significant bit is a slight modification of the LSB steganography. In this technique the most significant bit is changed instead of changing the least significant bit. The embedded value is stored in the most significant bits of the image.

Most Significant Bit Algorithm adopted from (Anil and Mohit, 2012) was given as follows

Algorithm to embed text message:-
Step 1: Read the cover image and text message, which is to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Calculate MSB of each pixel of cover image.
Step 4: Replace MSB of the cover image with each bit of secret message one by one.
Step 5: Write stego image.
Step 6: Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.
Algorithm to Retrieve Text Message:-
Step 1: Read the stego image.
Step 2: Calculate MSB of each pixel of stego image.
Step 3: Retrieve bits and convert each 8 bit into character.

Advantage

- MSB makes the system more secure.
- It has greater PSNR and better Payload capacity which can be used to hide more data in a single cover image.

3. Pixel value differencing Method (PVD)

In Pixel-value differencing steganography technique, the difference value between two consecutive pixels in a block was used to determine how many bits of text could be embedded. The pixel value differencing (PVD) method suggested by (Wu and Tsai, 2003) provides both high embedding capacity and outstanding imperceptibility for the stego-image. The pixel value differencing (PVD) technique segments the cover image into non overlapping blocks comprising two connecting pixels and modified the pixel difference in each block (pair) for data embedding.

Pixel Value Differencing Algorithm adopted from (Darwisa, Pamungkasa and Wamiliana, 2020) was given as follows:
Algorithm to embed text message:-

Step 1: Convert the message to an 8-bit binary number.
Step 2: Calculate the difference between the two neighboring pixels on the cover image
Step 3: Specify the lower limit value and the number of bits n.
Step 4: Take n bits of the message, then convert it to decimal (b)
Step 5: Calculate the difference between the new pixel values.
Step 6: Save the new image as a stego-image

Algorithm to extract Text Message:-
Step 1: Calculate the difference in neighboring pixel values in the stego-image
Step 2: Specify the lower limit value and the number of bits n.
Step 3: Calculate the decimal value (b)
Step 4: Convert the value of b (decimal) to binary n bits
Step 5: Fetch Message = bit n.

Advantages of PVD technique

- High capacity embedding and outstanding imperceptibility of the stego-image

Disadvantages

- Each part of the cover image is divided into non overlapped blocks that has two connecting pixels and changes to different pixel in every one block (pair) for data Embedded.
- A larger difference in the original pixel values allows an extent modification.

This section examined the techniques (LSB, MSB and PVD) using three different colored and gray scale cover images of Lena, Baboon and Peppers. Each techniques was evaluated using peak signal to noise ratio (PSNR), mean square error (MSE) and Structural similarity index (SSIM). Gray scale and colored cover images of Lena, Baboon and Peppers was used for the experiment. Mean square error was used to compute how well the methods perform; PSNR measured the quality between the original and a compressed image. SSIM was used for measuring the similarity between two images.

The peak signal to noise ratio (PSNR) measured in dB was calculated using equation 1

$$PSNR = 10\log_{10}\frac{Max^2}{MSE} \quad (1)$$

Mean Square Error measured in percentage was calculated using equation 2

$$MSE = \frac{1}{M*N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[I(i,j) - I_o(i,j)\right]^2 \quad (2)$$

Where Io is the cover image before embedding, I is the stego-image after embedding and M x N represents the size of these images.

SSIM gives the similarities rate of cover and stego image. SSIM was calculated using equation 3

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c1)(\sigma_x^2 + \sigma_y^2 + c2)} \quad (3)$$

4. RESULTS AND DISCUSSIONS

Table1: Comparison of LSB, MSB and PVD techniques for color cover images

Cover Image (512x512)	LSB			MSB			PVD		
	PSNR	MSE	SSIM	PSNR	MES	SSIM	PSNR	MSE	SSIM
Lena	50.656	0.0062	0.9998	40.273	0.0082	0.9975	49.283	0.0076	0.9981
Baboon	50.654	0.0065	0.9997	40.253	0.0087	0.9943	48.829	0.0072	0.9945
Peppers	50.619	0.007	0.9998	39.998	0.0090	0.9967	48.934	0.0079	0.9980

Table2: Comparison of LSB, MSB and PVD Techniques for gray scale cover images

Cover Image (512x512)	LSB			MSB			PVD		
	PSNR	MSE	SSIM	PSNR	MSE	SSIM	PSNR	MSE	SSIM
Lena	50.141	0.0072	0.9960	40.073	0.0092	0.9890	49.417	0.0079	0.9728
Baboon	50.148	0.0075	0.9987	40.053	0.0098	0.9897	48.529	0.0891	0.9876
Peppers	50.140	0.008	0.9963	39.559	0.0105	0.9888	48.392	0.0901	0.9748

Table 1 showed the PSNR, MSE and SSIM results obtained by the three techniques for three different colored cover images. The experimental results showed that LSB has higher peak signal to noise ratio compared to others. All the three techniques have a reasonable value for SSIM which indicate a good similarity rate between cover image and stego image. Table 2 presented the PSNR, MSE and

SSIM results obtained by the three techniques for three different gray scale cover images. PVD technique produced a lesser similarity index compared to the other two techniques

CONCLUSION AND FUTURE WORK

In this paper, comparative performance analysis of LSB, MSB and PVD methods used in image steganography was performed. LSB technique gives higher PSNR and SSIM values than MSB and PVD method with lower MSE than the other two techniques. Future research can be geared towards investigating the embedding capacity, security, and computational complexity of each technique.

Acknowledgement: None

Conflict of Interest: None

Source of Funding: None

REFERENCES

1. Alade O.M, Amusan E.A, Adedeji O.T and Alo O.O (2021): Image steganography using Pixel Value differencing (PVD) based on Firefly Algorithm. Journal of Scientific Research & Reports 27(7): 80-86.
2. Fridrich J, Goljan M, Du R.(2001): Reliable detection of LSB steganography in grayscale and color images. ACM Workshop on Multimedia and Security. 2001: 27-30.
3. Subhedar MS, Mankar VH. (2014): Current status and key issues in image steganography: A survey. Computer science review. 2014: 95-113.
4. Anil Khurana, 2B. Mohit Mehta (2012): Comparison of LSB and MSB based Image Steganoraphy; International Journal of Computer Science And Technology Vol. 3, Issue 3, July- Sept 202
5. Rohit Garg and Tarun Gulati (2012): Comparison Of Lsb & Msb Based Steganography In Gray-Scale Images: International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October-2012 pp 1-6
6. Rejani, Murugan and Deepu (2015): Comparative Study of Spatial Domain Image Steganography Techniques. Int. J. Advanced Networking and Applications Volume: 07 Issue: 02 Pages: 2650-2657 (2015) ISSN: 0975-0290
7. Yu Yu Wai and Ei Ei Myat (2018): Comparison of LSB, MSB and New Hybrid(NHB) of Steganography in Digital Image. International Journal of Engineering Trends and Applications (IJETA)-Volume 5 Issue 4, Jul-Aug 2018
8. D Darwisa,b N B Pamungkasa, Wamiliana (2020):Comparison of Least significant bit, Pixel value differencing, and modulus function on steganography to measure image Quality, Storage Capacity, and Robustness. Journal of Physics: Conference Series 1751 (2021) pp1-12.
9. Chan, C. K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. Pattern Recognition, 37(3), 469-474.
10. Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. Pattern Recognition Letters, 24(9-10), 1613-1626.
11. Kamaldeep (2013) "Image Steganography Techniques in Spatial Domain, their Parameters and Analytical Techniques: A Review Article" IJAIR Vol. 2 Issue 5 ISSN: 2278-7844
12. M. Hussain, A.W.A Wahab, Y.I.B. Idris, A.T. Ho, K.H. Jung, "Image steganography in spatial domain: A survey", Signal Processing: Image Communication, Vol 65, pp 46-66, 2018.
13. Z. Wang, E. P. Simoncelli, A.C. Bovik, "Multiscale structural similarity for image quality assessment". In The Thrity-Seventh Asilomar Conference on Signals, Systems & Computers, Vol. 2, pp. 1398-1402, 2003.

How to cite this article: Modupe AO, Adedoyin AE, Titilayo AO et.al. A comparative analysis of LSB, MSB and PVD based image steganography. *International Journal of Research and Review*. 2021; 8(9): 373-377. DOI: *https://doi.org/10.52403/ijrr.20210948*

******