

Edge-based Image Steganography using Edge Least Significant Bit (ELSB) Technique

Vinolin V

*Department of Applied Electronics,
St.Xavier's Catholic College of Engineering
Kanyakumari, Tamil Nadu, India
v.vinolin@gmail.com*

Vinusha S

*Department of Applied Electronics,
Regional Centre of Anna University
Tirunelveli, Tamil Nadu, India
s.vinu89@gmail.com*

Abstract: Image steganography is defined as a process of conceal a secret message into a larger media file. Media files are ideal for steganography system since it has larger size and such media files are termed as audio, video and image. The advantage of steganography over cryptography is that the intended secret message does not attract attention to itself as an object of scrutiny. In this paper, the edge based image steganography system is developed using threshold selection and edge least significant bit technique. The main purpose of this system is to enhance the security and imperceptibility of the system. The proposed methodology constitutes of threshold selection, embedding process and extraction process. Initially, the edges are determined from the cover image by the edge detector. Here, the canny edge detection algorithm is utilized for edge selection with the aid of threshold selection. Thus, the edge pixels are obtained for the embedding process. Then, the secret message is entrenched into the edge pixel of the original image using the Edge Least Significant Bit (ELSB) technique which acquires the embedded image. At the receiver side, the secret message is retrieved from the watermarked image using ELSB technique. The experimental results are evaluated and performance is analysed with the parameters are Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The outcome of the proposed system attains the higher PSNR of 78dB which ensures the security of the image steganography method.

Keywords: Steganography, Threshold selection, Embedding and Extraction process, ELSB technique, PSNR.

1. Introduction

Image steganography is the branch of information security technique which is used to conceal the secret information into media files or cover image. Initially, we employ some image steganographic techniques like invisible ink, microdots character arrangement etc. Nowadays, due to modernization of the technology, some media files have the source for the image steganography method. Such media files are text, audio and video and also several digital medium like floppy disk, radio waves, hard drives etc [2]. The main objective of steganography is to embed the secret message into the original image which is unable to detect by any intruder. Several factors of the message are employed to transmit the information securely over the channel. The factors are content adaptability, smaller size of images and visual resilience [1]. Due to residing the data into cover image, it leads to generate distortions in the original image. However, the distortion may not be visible to the human beings but, the secret image is detected by the distortion in the steganalysis method [3]. Thus, the image steganography is widely used for video and image communication in multimedia systems.

In image steganography method, the steganographic terms are named as cover image, secret message, watermarked image, secret key, embedding process and extraction process [10]. Image steganography technique is categorized into two types viz., i) spatial domain and frequency domain based approach. In spatial domain, the intensity of the pixel value in the original image is changed since the secret message is entrenched. Whereas in the frequency domain, several transform is used to obtain the transform coefficients where the information is embedded [5]. Some of the spatial domain approaches are LSB based approach and PVD based approach. In LSB based technique, the embedding process is done by replacing the least significant bit of the cover image with the message bit. In pixel value difference (PVD) approach, higher the pixel difference in the cover image is undergone for the embedding process. Thus, the pixel difference is estimated by one pixel and its neighbour [8]. The frequency domain

approaches are discrete wavelet transform, discrete cosine transform, singular value decomposition, etc. The transform function is utilized to obtain its coefficients where the message is hidden [7].

The security of the steganographic technique is validated based on the selection of pixels for embedding process. Then, we consider the edge pixels and texture area of the cover image for the embedding process. Thus, the message is embedded significantly in the edge portion rather than the smoother area of the original image. Due to changes of intensity in the edge pixel, it is critical to detect the message by the imposer [1]. The embedding rate increases greatly by using more edge pixels and then the smoother region of the image remains unaltered [14]. The edges are selected by the Sobel edge detection or canny edge detection algorithm. Then, the secret message is embedded into the edges by its threshold value. If the difference between the edge pixel and its neighbour pixel is greater than the threshold, then the data is embedded into edge locations [13]. The three major prerequisite are considered while evaluating the performance of the steganography method. The requirements are robustness of the system, imperceptibility of the image and data embedding rate [4].

2. Literature Review

Anastasia Ioannidou *et al.* [1] presented an edge detection technique for the image steganography method. The secret message was embedded into the edges of the original or cover image. The proposed technique was based on the edge pixels in the original image. A hybrid edge detector was used for the edge detection. Furthermore, the high payload technique was also employed. Then, the steganographic algorithm was produced by incorporating these two techniques. Finally, the higher peak to signal noise ratio (PSNR) was achieved using the MATLAB implementation.

Weiqi Luo *et al.* [2] proposed a more secure steganography method based on the adaptive pixel value differencing. Initially, the cover image was divided into small regions which were then rotated according to the degrees of 0, 90, 180 or 270. The resultant image was further partitioned into non-overlapping embedding units. The three consecutive pixels were obtained and the middle pixel was exploited for the message embedding. For embedding, three pixels were sorted to obscure the local statistical feature. Thus, the embedded bits were dependent on the differences among three pixels. Experimental results for the adaptive PVD technique were validated which ensured the better security.

Hayat Al-Dmour and Ahmed Al-Ani [3] described an image steganography algorithm which composed of edge detection and XOR coding. Edge detection was mainly used to detect the edges where the message was embedded since it caused the less degradation of the original image quality. The edge detection was applied here to both cover image and message. Then, the XOR coding mechanism was used to reduce the differences between the original image and data. The proposed method required the four bits of the cover image which was used for the embedding process. In order to embed the data, no more than two of the four bits was changed in the cover image. Thus, the message was entrenched using edge detection and XOR coding. The experimental results ensured that attained the high imperceptibility and sustained a better security level when applied a textual feature algorithm.

Rina Mishra *et al.* [4] explained a technique for data transmission over the insecure channel. Here, the compression and encryption was utilized in this technique. Initially, the secret information was compressed using the LZW algorithm. Then, the size of data was compressed to the concise format. After compression, the data was encrypted with the aid of key to improve the security level. Here, the canny edge detector was utilized. Thus, the edges of the secret message was extracted for entrench data into the original image. The experimental results were evaluated and the performance was analysed in the MATLAB implementation. Finally, the outcome of the proposed technique attained low distortion in the embedded image.

Hedieh Sajedi and Mansour Jamzad [5] discussed a method for computing embedding capacity of cover images. The capacity constraint was used to embed the secure data rather than the embedder did not know about the prior knowledge of how much data to be hidden. Initially in the proposed approach, an ensemble system was employed to evaluate the security limits for the embedding in the cover images by the steganalyzer units. In this system, the units were calculated from the different steganalyzer with respect to the different payloads that leads to determine the upper bound of embedding rate for the image. Thus, the embedding capacity minimized the risk of detection in the embedding process. The experimental results showed the relation between complexity and embedding capacity which enhanced the security level of the stego images.

Fangjun Huang *et al.* [6] proposed an edge adaptive image steganography based on the LSB matching revisited image. This scheme was used to select the embedding location with regard to the size of secret image and difference of the two consecutive pixels in the original image. Only the sharper edge regions were used for lower embedding rate. Thus, more edge regions were selected adaptively for data

hiding while increased the embedding rate. The experimental results were validated using 6000 natural images with three specific and four universal steganalytic algorithms. Thus, the results proved that the proposed scheme could enhance the security level significantly when compared to the existing system like LSB based approach and pixel value differencing based approach.

Saiful Islam and Phalguni Gupta [7] described a steganographic method based on pixel intensity to embed the secret message into the gray scale image. Thus, the edge pixels in the original image were used as the embedding locations. The number of edge pixels was selected adaptively according to the size of payload. Thus, the experimental results of the proposed steganographic method achieved the better security performance when compared to the existing systems.

Jeng Shyang Pan *et al.* [8] presented an image steganography method which was composed of compressive sensing and subsampling. Initially, the cover image was compressed by the transform domain. The main characteristics of compressive sensing, dimensional reduction and random projections were utilized to embed the secret message into compressed original image. Then, the measurement matrix was created using the secret key that was employed in both embedding and extraction process. The embedded image was acquired which was then reconstructed at the receiver side using the Total Variation (TV) minimization algorithm. Subsampling was utilized in this paper to attain different transform coefficients from sub images. Finally, the bit correction rate parameter was used to determine the accuracy between the original secret image and extracted message. Thus, the experimental results of the steganography method were validated in MATLAB which leads to attain the high security level of information.

3. Problem Statement

The edge based image steganography method is used to conceal the secret message into the edge pixels of the cover image. In [1], the bits in the pixel are flipped when its size is not equal to the size of message. Here, the edge pixels are determined by the canny edge detection algorithm. The edge map is created by the six most significant bits of the cover image. Thus, the time consumption is more due to generate the edge map and permuted the pixel randomly for the embedding process.

4. Proposed Methodology: Edge least significant bit for edge based image steganography

The main objective of this paper is to enhance the security of the image steganography method using edge based LSB technique. The idea behind the edge based image steganography method is to embed the secret image into the edge location of the cover image. The proposed methodology constitutes of three steps. The steps are i) Threshold selection, ii) Embedding process and iii) Extraction process. Initially, the edge portion of the original image is selected using the canny edge detection algorithm. Then, the sharper edges are determined by the threshold selection method. This method is used to detect the edges by high threshold, low threshold and width of the Gaussian kernel. Subsequently, the secret image is embedded into the edge portion of the cover image using Edge least significant bit technique (ELSB). This technique is employed to replace the last two bits of the edge pixel with the first two bits of the message. Thus, the embedded image is obtained at the sender side. Then, at the receiver side, the message is retrieved efficiently from the embedded image using the edge based least significant bit (ELSB) technique. Figure 1 depicts the block diagram of the proposed methodology.

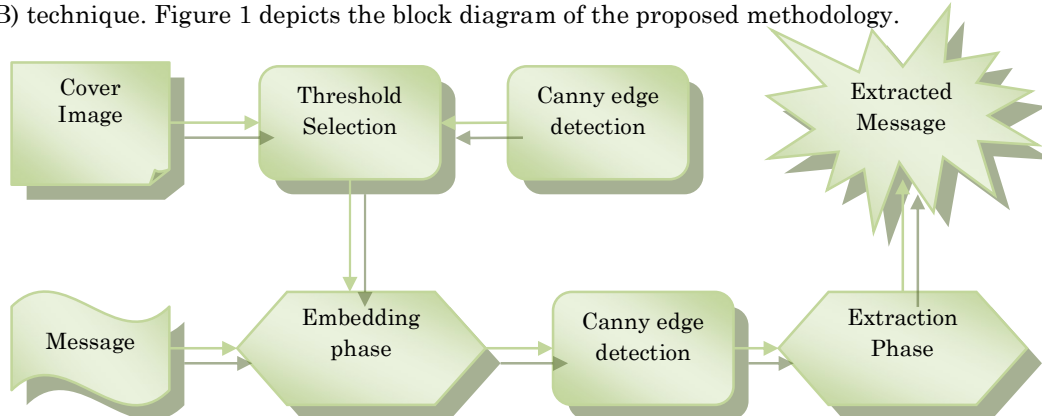


Figure1. Block diagram of the proposed methodology

4.1 Threshold selection

Initially, the input image is fed into the canny edge detection algorithm to select the edge pixels for the embedding process. The edge pixels are determined using the threshold selection. Here, we consider the three parameters to detect the edges, which are high threshold (t_h), lower threshold (t_l) and width of Gaussian kernel. The threshold t_h refers to identify the strong edges whereas the t_l threshold determines the weaker edges of the cover image. The high threshold provides the enough number of edges according to the message size to entrench the secret message into the cover image. Similarly, the low threshold is evaluated by $t_l = 0.4 \times t_h$. Then, the noise sensitivity in the edge detection algorithm is controlled by the width of the kernel. Thus, the kernel width is set to be constant to obtain the lower and higher threshold. The threshold selection for the image steganography is expressed as below.

i) Initially, in the threshold selection, the minimum threshold is set to be 0 and maximum threshold value is set to be 1. Then also, the width of the Gaussian kernel is fixed randomly. It is represented as:

$$\begin{aligned} t_{\min} &\leftarrow 0 \\ t_{\max} &\leftarrow 1 \end{aligned} \quad (1)$$

ii) The high threshold value is determined by the minimum and maximum threshold value. Thus, the value lies between zero to one. The high threshold is formulated by,

$$t_h = \frac{t_{\max} + t_{\min}}{2} \quad (2)$$

where, t_h is the higher threshold value for the embedding process.

iii) Let l_e be the obtained number of edge pixels using canny edge detection algorithm. When the number of pixels and the length of the secret message are same, we cannot determine the threshold value for embedding. It is defined by,

$$l_e = \text{edge}(I) \quad (3)$$

where, I be the input image and l_e is the number of edge pixels.

iv) To resolve this problem, we define the terminating condition with respect to the l_e and length of secret message L . The condition is defined by the difference between the number of edge pixels and length of message L that is represented as $d = l_e - L$ and limit is set to be upper bound on l_e which is expressed as $0.01 \times L$. When the difference is greater than the limit, the threshold t_h has to be selected as the median threshold value. Similarly, if the l_e is greater than the L , then the median threshold is set to maximum threshold. Thus, it is derived as:

$$\begin{aligned} t_{\min} &\leftarrow t_h; \quad \text{if } d > \text{limit} \\ t_{\max} &\leftarrow t_h; \quad \text{if } d < 0 \end{aligned} \quad (4)$$

This process is repeated until the difference between the number of edge pixels and L , is less than the limit i.e., $0.01 \times L$. Thus, the edge pixels are obtained using the threshold selection for embedding and extraction process of the image steganography.

4.2 Embedding process using ELSB technique

After the edge pixels are obtained using threshold selection, the secret message is then entrenched into the edge pixel of the original or cover image. Here, the edge based least significant bit (ELSB) technique [9] is utilized in this paper. Let I be the cover image with the size of $m \times n$ i.e., m number of rows and n number of columns and M be the secret message. In ELSB technique, the masked image is generated by masking the last two LSB bits in the cover image. Then, the edge pixels are selected by the threshold selection based on the canny edge detection algorithm. Then, the secret data is embedded into the LSB bits of the edge pixels in the cover image. Thus, the ELSB technique is deliberated below.

i) The cover image I and the secret message M is considered as input for the embedding process. In order to sustain the edges before and after embedding, the two LSB bits of the original image is masked. The information does not change by masking the least significant bit of the cover image. Then, the mask image is defined as,

$$I'(i, j) = \text{mask}(\{2\text{LSB}[I(i, j)]\}) \quad (5)$$

where, $I(i, j)$ is the pixel of the original image, $I'(i, j)$ represents the pixel value of the mask image and 2LSB denotes two least significant bits of the image.

ii) After the mask image is obtained, the canny edge detector [1] based threshold selection is utilized. This detector is used to select the edges where the secret message is entrenched. Thus, the edges in the cover image is selected by,

$$l_e = \text{canny}(I', t_h, t_l, w) \quad (6)$$

where, l_e is the number of selected edge pixels in the cover image using canny edge detection algorithm, t_h and t_l are the high and low threshold value which is determined using the threshold selection and w is the width of the Gaussian kernel.

iii) The secret message consists of m number of characters which is embedded into the resultant edge pixel of the cover image. Thus, the first two bits of each character are entrenched into the edge pixels of the mask image. Then, the next two bits of the character are embedded into the next edge pixel value. Similarly, this process is repeated until all the message character is embedded into the cover image.

$$W(i, j) = E[I'(i, j)] + k(i, j) \quad (7)$$

where, $E[I'(i, j)]$ represents the edge pixel of the masked cover image and $k(i, j)$ denotes each character of the secret message. Then, all the characters in the message is embedded into the selected edge pixels of the cover image. Thus, the embedded image or watermarked image W is obtained at the sender side. Then, the embedded image is transmitted to the receiver side via the communication channel.

4.3 Extraction Process

At the receiver side, the message is retrieved from the embedded image using the Edge least significant bit method [9]. The embedded image is also masked at the two least significant bits. Then, the canny edge detector based threshold selection is utilized to select the edge pixels of the embedded image. Thus, we determine the edge pixels where the data is hidden. After getting each character, then we apply the XOR operation between each character. Finally, the receiver retrieves the secret message significantly.

i) After obtaining the embedded image at the receiver side, we retrieve the message using ELSB technique. Then, the embedded image is masked at the least two significant bits. Then, the edge pixels are selected by the canny edge detector where the receiver extracts the secret data. It is formulated as:

$$W'(i, j) = \text{mask}\{(2\text{LSB})[W(i, j)]\} \quad (8)$$

where, $W(i, j)$ is the pixel value of the embedded image where the two LSB bits are masked.

ii) The canny edge detection algorithm is also utilized at the receiver side. Thus, the detection algorithm is applied to the embedded image. Since we employ the same masked image to compute the edge pixels, the same edge pixels are obtained at the sender and receiver side. Thus, the edge pixels are determined as,

$$l_e' = \text{canny}(W', t_h, t_l, w) \quad (9)$$

where, l_e' is the acquired edge pixels at the receiver side with regard to the mask watermarked image, width, high and low threshold.

iii) The message is retrieved by the difference of embedded image and the original or cover image. The receiver reads the last two bits from each edge pixel of the embedded image. Thus, the character is retrieved from edge pixel is represented by,

$$k(i, j) = E[W'(i, j)] \oplus I(i, j) \quad (10)$$

where, k is the character of message which is extracted from the edge pixels of the embedded image with respect to the original image. Then, the secret message R is obtained by the XOR operation [9] of all the characters. It is expressed as:

$$R = k_1 \oplus k_2 \oplus k_3 \oplus \dots \oplus k_m \quad (11)$$

where, R represents the extracted message. Thus, the receiver extracts the message from the embedded image securely.

5. Results and Discussion

This section presents the experimental results and the performance analysis of the edge based image steganography method. The performance is analysed by the parameters are Mean Square Error (MSE) and Peak to Signal Noise Ratio (PSNR).

5.1 Experimental Setup

a) Evaluation parameters: The performance of the edge based image steganography method is analysed using MSE and PSNR parameters. Then, the performance is compared with the existing systems

i) *MSE*: The Mean Square Error is evaluated by the original message and extracted message. The MSE is used to measure the distortion of the image which ensures the security level of the secret message. The MSE is calculated by,

$$MSE = \frac{1}{x \times y} \sum_{k=1}^x \sum_{l=1}^y (M_{kl} - R_{kl})^2 \quad (12)$$

where, x and y are the number of rows and columns in the message, M_{kl} represents the pixel value of the original message and R_{kl} is the pixel of retrieved message.

ii) *PSNR*: The Peak to Signal Noise Ratio is used to measure the quality of the images. The better quality of the image is determined by the high PSNR value. Thus, the PSNR is calculated by the ratio between the cover image and embedded image. It is expressed as:

$$PSNR = 20 \log_{10} \frac{I_{\max} \times m \times n}{\sum \sum (I(i,j) - W(i,j))^2} \quad (13)$$

where, m is the number of rows and n be the number of columns in the cover image, $I(i,j)$ is the pixel of the original image and $W(i,j)$ represents the watermarked image pixel.

5.2 Performance analysis

The performance is analysed for the two images using the MSE and PSNR parameter. Then, the analysed performance is compared with the existing edge based image steganography method. Thus, the performance is apparently described below.

a) MSE

The figure 2 depicts the MSE performance analysis for the two images. The MSE is the measure which is computed between the watermarked image at the sender side and watermarked image at the receiver side. Thus, lower the error in the image ensures to retrieve the message efficiently. The MSE performance for the image 1 is shown in figure 2.a. When the SNR is 30dB, the existing 2LSB technique achieves 0.26 MSE error value. But, the proposed ELSB technique attains the minimum error of 0.17 values which is demonstrated in the figure 2.a. Similarly, the mean square error for the proposed system is gradually decreased while increasing the SNR value. Then, the figure 2.b shows the MSE performance analysis for the image 2. The MSE of existing system obtains 0.25, 0.23, 0.19, 0.16 and 0.13 error by varying the SNR value. However, the proposed work acquires the MSE of 0.23 when the signal to noise ratio is 10dB. Further, the mean square error is moderately decreased to 0.07 while increasing the SNR value which is represented in figure 2.b. Thus, the minimum error is obtained using the proposed ELSB technique which proves the robustness of the system.

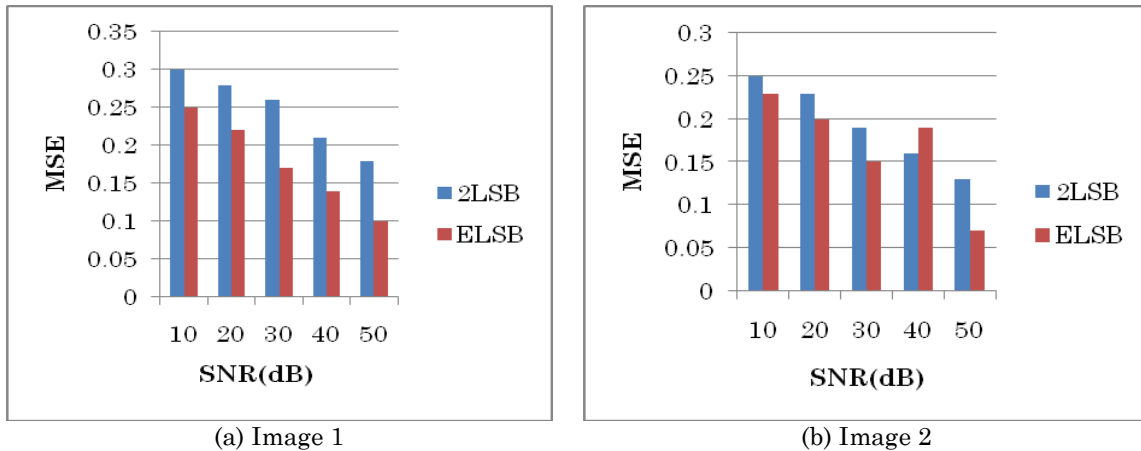


Figure 2. MSE performance analysis

b) PSNR

The figure 3 demonstrates the PSNR performance analysis for the existing and proposed work. The Peak Signal to Noise Ratio is employed to measure the quality of the image which tends to retrieve the secret message significantly. The figure 3.a depicts the PSNR performance for the image 1. Lower the MSE value which leads to attain the higher PSNR value. The existing least two significant bits achieves the PSNR value of 63dB when the signal ratio is 10dB. Then, the PSNR is increased to 69.3dB when the SNR is 50dB. Subsequently, the proposed work attains the 71 dB PSNR at 10 dB of signal to noise ratio. Furthermore, the PSNR is gradually increased to 78dB while increasing the SNR value which is shown in figure 3.a. The MSE performance analysis for the image 2 is deliberated in figure 4.b. When the signal to noise ratio is 20dB, the existing system achieves the 65.1 dB PSNR, whereas 72.3dB PSNR is obtained for the proposed system. Similarly, the 68.5 peak signal to noise ratio is attained in the existing system. But, in the figure 3.b, the proposed ELSB technique acquires the 76.8 dB PSNR value rather than the 2LSB technique when the SNR is 40dB. Finally, the proposed work achieves the higher PSNR of 78dB for the edge based image steganography method.

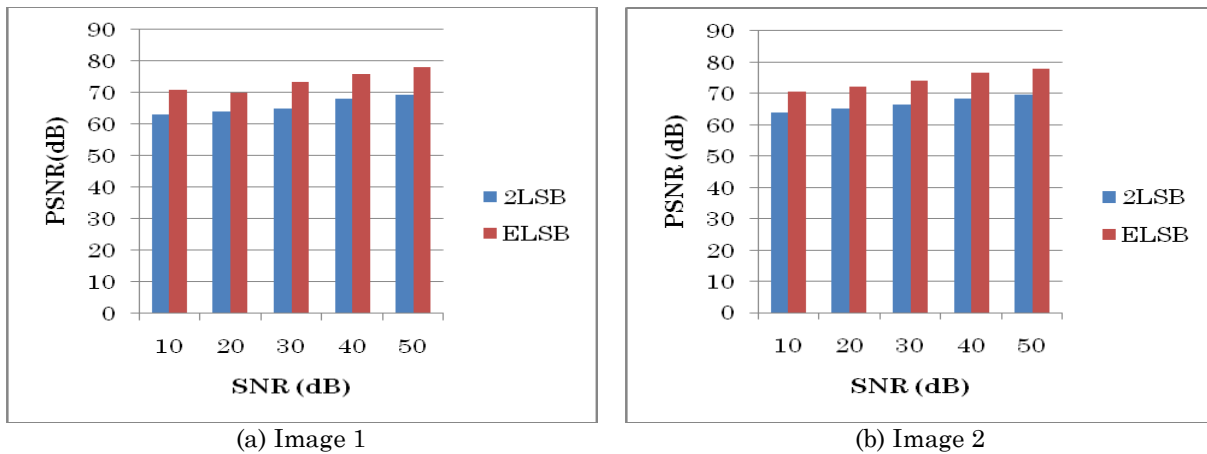


Figure 3. PSNR performance analysis

6. Conclusion

The edge based image steganography was developed using the Edge Least Significant Bit (ELSB) technique. Initially, the threshold selection was employed to detect the edges of the cover image. Here, the canny edge detection algorithm was employed to determine the edges. Also, the high threshold, low threshold and width of the kernel were required to select the edges. In the embedding process, the cover image was masked and the canny edge detection was employed to detect the edge pixels. Then, the secret message was embedded into the edge pixels of the original image. Thus, the watermarked image was obtained at the sender side. Consequently, in the extraction process, the embedded image was masked at the two least significant bits and then evaluates the edge pixel by threshold selection. Thus, the receiver retrieved the secret message securely from the edge pixels of the embedded image. The experimental results were validated and the performance was analysed by the evaluation metrics such as MSE and PSNR. The outcome of the proposed system achieved the higher PSNR of 78dB value which proved the high security of the steganography method.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

- [1] Saiful Islam, Mangat R Modi and Phalguni Gupta, "Edge-based image steganography", EURASIP Journal on Information Security, vol.8, pp. 1-14, 2014.

- [2] Deepali Singla and Mamta Juneja, "An Analysis of Edge Based Image Steganography Techniques in Spatial Domain", In proceedings of IEEE 2014 Recent Advances in Engineering and Computational Sciences (RAECS), pp. 1-5, March 2014.
- [3] Saiful Islam and Phalguni Gupta, "Robust Edge based Image Steganography through Pixel Intensity Adjustment", In proceedings of 2014 IEEE 11th Intl Conf on Embedded Software and System, vol. 771-777, August 2014.
- [4] Rina Mishra, Atish Mishra and Praveen Bhanodiya, "An Edge Based Image Steganography with Compression and Encryption", In proceedings of IEEE International Conference on Computer, Communication and Control (IC4-2015), pp. 1-4, September 2015.
- [5] Anastasia Ioannidou, Spyros T. Halkidis and George Stephanides, "A novel technique for image steganography based on a high payload method and edge detection", Expert Systems with Applications, vol. 39, no. 14, pp. 11517-11524, October 2012.
- [6] P.U.Deshmukh and T.M.Pattewar, "A Novel Approach for Edge Adaptive Steganography on LSB Insertion Technique", In proceedings of IEEE 2014 International Conference on Information Communication and Embedded Systems (ICICES), pp. 1-5, February 2014.
- [7] Hedieh Sajedi and Mansour Jamzad, "Secure steganography based on embedding capacity", International Journal of Information Security, vol. 433, no.8, December 2009.
- [8] Weiqi Luo, Fangjun Huang and Jiwu Huang, "A more secure steganography based on adaptive pixel-value differencing scheme", Multimedia Tools and Applications, vol. 52, no. 2, pp. 407-430, April 2011.
- [9] K. Naveen BrahmaTeja, Dr. G. L. Madhumati and K. Rama Koteswara Rao, "Data Hiding Using EDGE Based Steganography", International Journal of Emerging Technology and Advanced Engineering, vol. 2, no. 11, pp. 285-290, November 2012.
- [10] Hayat Al-Dmour, Ahmed Al-Ani, "A Steganography Embedding Method Based on Edge Identification and XOR Coding", Expert Systems With Applications, vol. 46, pp. 293-306, March 2016.
- [11] Weiqi Luo, Fangjun Huang and Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics And Security, vol. 5, no. 2, pp. 201- 214, June 2010.
- [12] Jeng-Shyang Pan, Wei Li, Chun-Sheng Yang and Li-Jun Yan, "Image steganography based on subsampling and compressive sensing", Multimedia Tools and Applications, vol. 74, no. 21, pp. 9191-9205, November 2015.
- [13] Mehran Iranpour, "A Novel Steganographic Method Based on Edge Detection and Adaptive Multiple Bits Substitution", In proceedings of IEEE 2013 18th International Conference on Digital Signal Processing (DSP), pp. 1-6, July 2013.
- [14] Wen-Jan Chen, Chin-Chen Chang and T. Hoang Ngan Le, "High payload steganography mechanism using hybrid edge detector", Expert Systems with Applications, vol. 37, no. 4, pp. 3292-3301, April 2010.
- [15] Li Fan, Tiegang Gao and Yanjun Cao, "Improving the embedding efficiency of weight matrix-based steganography for grayscale images", Computers & Electrical Engineering, vol. 39, no. 3, pp. 873-881, April 2013.