A Least Significant Bit Steganographic Method Using Hough Transform Technique

Dalia Nashat[1], and Loay Mamdouh[2]
[1]Faculty of Computers and Information, Assuit University, Assuit, Egypt
[2]Hurghada Faculty of Computers & Artificial Intelligence, South Valley University, Hurghada, Egypt

Steganography is a data-hiding scientific branch that aims to hide secret data in an image, video, or audio. Image steganography methods try to embed a large amount of data into images with high imperceptibility. However, increasing the number of embedded data in the image decreases its quality. Therefore, in this paper, a new method based on Least Significant Bit (LSB) using Hough Transform is proposed to improve the stego image quality with increasing the amount of embedded data. The LSB is the common embedding steganography method due to its simplicity of implementation and low complexity. The proposed method inverts the LSBs of image pixels to enhance the quality of stego image. First, improved edge detection filter is used to detect edges areas. Then, we invert LSBs for the pixel in edge area pixels. Finally, the LSBs smooth area pixels of the cover image are inverted. The performance of the presented method is evaluated for the stego image quality and the amount of embedded data. The results show that the new method has better performance in comparison with the current methods in terms of Peak Signal-to-Noise Ratio (PSNR) and capacity.

***Index Terms*—Information security, Image processing, Steganography, Data hiding, LSB, Hough Transform**

I. Introduction

The continuous development of communication technology makes data exhibit unauthorized access during transmission over networks. Therefore, many data hiding methods have been used to secure data during transmission over networks such as cryptography, steganography, watermarking, and digital signatures [1] [2] and [3]. Cryptography transforms data into a meaningless form and the user who has the key can only decrypt the encrypted data [4]. Steganography and watermarking are the two main fields of the data hiding science [5]. The goal of steganography is hiding data while watermarking is preserving copyright [6]. Greek terms steganos, which translate to ”covered” or ”hidden,” and graph, which translates to ”write,” are the roots of the term steganography. Thus steganography means ”Hidden writing”. Image steganography aims to hide secret data in an image. The original image which is used to embed secret data is called the cover image. After embedding, the image is known as a stego-image.

Steganography approaches in images use transform domain or spatial domain [6] and [7]. In the transform domain, the cover image is transformed into a frequency domain by using transform methods such as Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Discrete Fourier Transform (DFT) before embedding process [3] [8] and [9]. In the spatial domain, the secret data are hidden directly into the cover image by modifying the image pixels. This can be done by replacing the redundant or insignificant parts of the cover image by secret data bits [8] [10] and [11]. The spatial domain is more widely used in steganography approaches due to its greater quality of imperceptibility and embedding capability [12].

Manuscript received November 12, 2022; revised June 9, 2023. Corresponding author: Dalia Nashat (email: dnashat@aun.edu.eg).

The easiest and most popular approach of steganography methods in the spatial domain is the LSB method. The classical method is known as LSB substitution. This method inserts directly the secret bits instead of the least significant bits for each pixel in the cover image. The advantages of this method are simplicity and high embedding capacity. The main disadvantage is the noticeable distortion in the stego image which attracts any unauthorized attention. Much research have been done to improve the performance of LSB such as the LSB inversion method which reduces the chance of detecting the hidden data [13]. While using this strategy may greatly reduce bit error and raise imperceptibility quality, the stego images are not consistent enough across various cover images and messages [14]. LSB inversion method is the process of inverting the LSBs of pixel of the cover-image based on the secret data values. In this method, the number of pixels that is modified is less than that in the standard LSB method. This improves the quality of stego image and then enhance the PSNR values [15].

Recently, edge detection techniques deployed in data security techniques. Since the hough transform is one of the most promising techniques for line detection, it is used for hiding data in color images like [16] and [17]. The main disadvantage of these methods is that they integrated steganography and encryption methods to hide data which makes them more complex. Also, greyscale images are ideal in image steganography methods since they have fewer color variations because it just uses black or grey [18].

In this paper, we introduce a new steganographic technique based on LSB with hough transform in greyscale images. The main contribution of our method is to increase the capacity of embedded data and enhance the quality of the stego image. It is known that edge areas can tolerate much more changes than smooth areas without making perceptible distortion, so hough transform with Canny Filter are used to obtain edge and smooth areas and then obtain the peaks in edge areas to

embed secret data by inverting LSBs for pixels. The number of secret bits determines the number of LSBs of each pixel that can be used to embed the secret bits. We used standard greyscale images to evaluate the efficiency of our method. The performance of the presented method is evaluated for the stego image quality and the amount of embedded data. The results show that the new method has better performance in comparison with the current methods in terms of Peak Signal-to-Noise Ratio (PSNR) and capacity.

The rest of this paper is organized as follows. Section 2 introduces the related work. Section 3 presents a brief description of the hough transform method and introduces the optimal LSB method. Section 4 explains the presented method in details. In Section 5 the experimental results are demonstrated. The conclusion of the paper is presented in section 6.

II. Related Work

Currently, many steganographic techniques for data hiding are available. Some of these techniques used hough transform with LSB method. Yasmina et al. [19] presented a new technique to hide secret data in a color image based on Steganography and Cryptography. The secret data is encoding using Huffman Coding. hough transform is used to detect Straight Lines in a cover image. The encoded data is embedding in the Straight Lines using (LSB) method. This technique can recover the secret data without the need for the cover image and without losing any letter from the stego image. The PSNR value of this technique is high.

Arman and Farsad [20] proposed a new approach of information security in color images. Advanced Encryption Standard (AES) to encode hidden information is used to enhance the security for resisting against attacks. Canny and hough transform are used for edge detection and smooth areas. LSB two-component method of replacement and adapting for hiding encrypted information is used. This method proves that edge areas can tolerate further changes in the pixels than smooth areas. The method has passed various steganography analysis involving visual and static analysis.

Mamta and Parvinder [16] presented approach aimed to develop and enhance the data hiding technique in RGB color images based on 3 new techniques. In the first, Canny and hough transform are used to divide an image into the edge and smooth areas. Then, encrypted secret bits are embedded in edge areas using Two Component based LSB Substitution Technique. For smooth areas, an adaptive LSB is used. This approach is robust and makes it is difficult for human eyes to detect any data hiding. Also, this method is better in PSNR and capacity while comparison with other existing methods.

Mohammed and Rossilawati [15] introduced a new bit inversion approach of steganography improves the color stego image quality. They proposed two additional levels of security to the standard LSB steganography. The first level is that this method used only two colors green and blue where in the standard LSB, the three colors green, blue and red are used. The second level utilized the new LSB inversion method that reverses the bits of the stego image pixels after applying the standard LSB. The proposed approach increases the capacity and the stego image quality and enhances the weaknesses of the standard LSB steganography.

Rupali and Vaishali [13] proposed a method based on complemented message and inverted bit LSB substitution which provides three levels of security rather than hiding bits directly in the cover image. This method reduced the detection of hidden data. Experimental results show that this method is better than the simple LSB method in PSNR.

Dilip and Chakravarthy [21] presented a new Threshold-LSB based information hiding scheme. This scheme uses the threshold of the pixel in a grayscale image before embedding secret bits. The embedded secret bits are distributed randomly across the image. The main advantage of this scheme that it is difficult for any intruder to extract the secret message even if he has the stego image. The results show the better performance of this scheme in capacity and visual quality of stego image.

Kamaldeep and Rajkumar [22] presented a new method of image steganography blend with cryptography. The combinations of steganography and Cryptography method improved the security of the embedded data. In this method, the authors encrypted the secret message firstly. Then, they embedded it in the image using LSB with Shifting (LSB-S) method. This method provided good values of PSNR and Mean Square Error (MSE) as shown from experimental results.

Kamaldeep and Rajkumar [23] used three bit XOR steganography technique for hiding data into gray images. Any intruder cannot be able to find the meaning of the message if he extracts the last three bits. This approach achieves high accuracy over existing methods.

Authors in [24] proposed an efficient steganographic method to enhance the capacity taking high visual quality into consideration. This method used inverting LSBs and arithmetic operations for embedding by inverting some LSB of the cover image depending on the secret data. The experiments indicate that the proposed method gives high capacity and good imperceptibility in comparison with the previous methods.

The DE-based scheme in [25] enhanced information concealing based on difference expansion and modulus function. The authors take into account both positive and negative difference values to produce hidden data. In comparison to the prior DE-based technique, the suggested DE offers a high capacity while keeping a high degree of resemblance between the cover and the stego images, which amply illustrates its performance.

Authors in [26] proposed a steganography algorithm by using the chaotic map and modified LSB. They applied the tent chaotic map and the two-dimensional piecewise smooth chaotic map. The experimental results demonstrate that the host image's histogram and the stego image's histogram are practically similar.

Mohammed et al. [27] presented an study summarizes the current image steganography techniques in spatial domain, also analyzed different problems and the drawbacks of each method that have been innovated from last few years.

Zeena et al. [28] proposed algorithm encrypted secret text data using the simple and traditional Caesar method, but in an innovative way based on the coordinates of the central circular shape that the algorithm finds to reduce the number of keys exchanged between the sender and the recipient and to increase the level of security and confidentiality.

A novel signature steganography technique for color image in YUV domain is proposed in [29]. The LSB of the Y channel and the bits of the stego key are bitxored to determine the channel in which the Beta elliptic signature bits will be buried. This technique guarantees PSNR greater than 90db and SSIM exceeds 0.99.

A distinction grade value (DGV) with LSB method is presented in [30] to achieve a robust steganography scheme. Authors used encryption, Huffman compression algorithm and Fibonacci-based image transformation to improve the imperceptibility, security, robustness and capacity of their scheme.

Authors in [31] suggest two enhanced RDH-based methods. The first method is the better dual image-based least significant bit (LSB) matching with reversibility, and the second is n-rightmost bit replacement (n-RBR) with modified pixel value differencing (MPVD). A dual images Reversible Data Hiding (RDH) approach is developed by combining the modified LSB matching method with EMD in [32]. This method improved the quality of stego images to achieve average PSNR 51.14db and average SSIM 0.9975.

III. Background

A. Hough Transform

The Hough Transform (HT) is an incredible technique used in computer vision, image analysis, and digital image processing. The goal of this technique is to find imperfect instances of objects within a certain class of shapes by a voting procedure [33]. The simplest and the most popular application of HT were concerned with the detection of lines in the image [34], but later the HT was extended to detect positions of circles or ellipses.

The straight lines are the classical case of HT. The HT is defined as a transformation of a point in two dimensions space to a parameter space. The parameter space demonstrates the shape of the object [35]. The straight line, in general, is described in the x-y plane as follows [36]:

$$y = ax + b \tag{1}$$

This equation in the Cartesian coordinate system, where a and b are the parameters of the line. This form can be represented as a point (b,a) in the parameter space. Because the vertical lines to the x-axis can give rise to unbounded values of the parameter a which is the slope, lines can be represented in terms of theta θ and ρ such that [35]:

$$\rho = x\cos\theta + y\sin\theta \tag{2}$$

where ρ is the distance from the origin to the closest point on the straight line, and θ (theta) is the angle as shown in Figure.1.

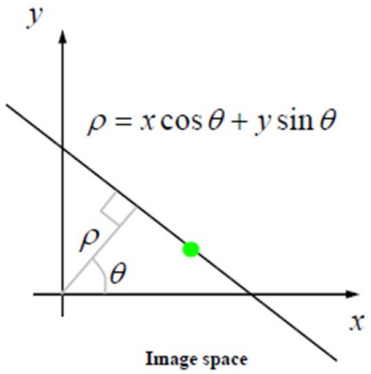


Fig. 1: ρ, θ line parameterization [35].

A unique sinusoidal curve in the $(\rho,\theta?)$ plane is produced. This curve is produced from all straight lines passing through a single point in the plane [35].

B. The Optimal Lest Significant Bit (LSBs) Technique

The quality of the stego image is enhanced by the optimal LSBs method. This method is obtained by improving the simple LSBs method. The optimal LSBs method applies an optimal pixel adjustment process (OPAP). For each pixel, three candidates are selected and compared to get the closest value to the original pixel value which has the secret data. The best candidate is then called the optimal pixel and is used to hide the secret data in it [37] [38] and [39]. The algorithm of the optimal LSBs is explained as follows:

- Suppose I_i is the value of the original pixel in the cover image and x is the number of bit(s) of the secret data to be embedded.
- Embed x bit(s) into I_i by using the LSBs method. The stego pixel $I_i^{'}$ can then be produced.
- Adjust the$(x+1)$-th bit of $I_i^{'}$. As a result of this adjustment another two pixel values $I_-^{'}$ and $I_+^{'}$ will be generated and can be calculated as follows:

$$\left(I_+^{'}, I_-^{'}\right) = \begin{cases} I_+^{'} = I_i^{'} + 2^x \\ I_-^{'} = I_i^{'} - 2^x \end{cases} \tag{3}$$

  The hidden data in $I_-^{'}$ and $I_+^{'}$ are identical to $I_i^{'}$ because the last x bits of them are the same.
- The optimal candidate $I_i^{''}$ is the most approximate to the original pixel value and can be found as follows:

$$I_i^{''} = \begin{cases} I_i^{'}, if \left|I_i - I_i^{'}\right| \le \left|I_i - I_-^{'}\right| \le \left|I_i - I_+^{'}\right| \\ I_+^{'}, if \left|I_i - I_+^{'}\right| \le \left|I_i - I_i^{'}\right| \le \left|I_i - I_-^{'}\right| \\ I_-^{'}, if \left|I_i - I_-^{'}\right| \le \left|I_i - I_i^{'}\right| \le \left|I_i - I_+^{'}\right| \end{cases} \tag{4}$$

- Finally, replace all the optimal candidates $I_i^{''}$ with the original pixel values I_i.

Now, we present an example to explain how the distortion that caused by the simple LSBs method can be decreased by the optimal LSBs method. Assume $I_i = 9$, $x = 3$, and the three secret data bits are 111. By using the simple 3-LSBs method, the stego pixel $I_i^{'} = 15$ is produced. Adjusting the 4-th bit of $I_i^{'}$ to generate another two pixel values $I_-^{'} = 7$ and $I_+^{'} = 23$. The last three bits of pixel values $I_i^{'} = 15$, $I_-^{'} = 7$ and $I_+^{'} = 23$ are identical. The optimal candidate is $I_-^{'} = 7$ because it is the closest to the original pixel value $I_i = 9$. This example demonstrates that the stego image quality can be enhanced by using the optimal LSBs method.

IV. The Proposed Method

This section will describe the presented method in details. This method is based on HT and inverting the LSBs of pixels. We use HT along with Canny Filter which provide better results in detecting edges [40]. Canny Filter in the industry is the standard edge detection algorithm [20]. In our method, the receiver should know the cover image that used to embed data into it. Also, the receiver should know the algorithm that used for embedding and the length of hidden data. The presented method consists of two parts. The first part is the embedding procedure which explains the steps of embedding data into the image. The second part is the extracting procedure which a retrieval process of the embedding procedure. We will describe the equation of the used image. Then we will discuss the embedding and extracting procedures in detail.

For any gray image I, $I = \{P_1, ..., P_N\}$ which consists of set of pixels. Each pixel consists of 8 bits:

$$P_i = \{b_1, ..., b_8\}, b_j \in \{1, 0\} \tag{5}$$

Let N is the image size. It is estimated as:

$$N = H \times W \tag{6}$$

Where H, W are height and width for the image respectively. Assume M is the secret data bits and n is its length,

$$M = \{m_1, m_2, ..., m_n\}, where\, m_i \in \{1, 0\} \tag{7}$$

The maximum hiding capacity h in the image I in terms of bits is:

$$1 \leq h \leq (N \times 8). \tag{8}$$

A. The Embedding Procedure

We use standard grayscale images and a series of pseudo-random data in the form of a binary system as input in the embedding procedure. The output of this procedure is the stego image. Hough Transform with Canny Filter is used to obtain edge areas. Then the peaks in edge areas are obtained to embed secret data. We invert n-LSBs of each edge pixel corresponding this peaks and $(n-1)$-LSBs bits of all the rest of the pixels (what's left of edge pixels and all smooth pixels) in the cover image where n=3, 4, 5. Note that, n is determined according to the amount of secret data bits which is wanted to be embedded. We apply the optimal LSBs method to improve the results. The algorithm as follows:

- Convert the secret data into the binary system.
- The secret bits are treated as a bit string of n-bit segmentation. Convert each n-bit segmentation into a decimal number. The corresponding decimal integer for a bit string of length n is supposed to fall in the range of [0, $(2^n - 1)$]. For example, if n = 4, the decimal value is range from 0 to 15.
- Obtain the edge areas of the cover image using Canny detector and Hough Transform.
- Find the peaks using Hough peak at threshold=0.1 or 0.2 or 0.3 or 0.4 or 0.5.
- Find the pixels in the cover image corresponding to a particular Hough Transform peak.
- For edge pixel in a peak, convert the pixel into binary. if the decimal value for n-bit string greater than $(2^n/2)-1$, then subtract the decimal value from $(2^n - 1)$ and treat with the result as our decimal value. Invert the last LSB (n-LSB) of the pixel. if the decimal value less than or equal $(2^n/2)-1$, don't invert the bit.
- According to the decimal value we will invert the bits of the pixel. For example, assume d is the decimal value and n=4, then the 1^{st}, 2^{nd} and 3^{rd} LSBs will be inverted as follows (note that n represents the bit segmentation and the number of LSBs of each pixel which will be used to embed secret data bits):
  - If $d = 0$, then don't invert any bits.
  - If $d = 1$, then invert 1^{st} LSB.
  - If $d = 2$, then invert 2^{nd} LSB.
  - If $d = 3$, then invert 1^{st} and 2^{nd} LSBs.
  - If $d = 4$, then invert 3^{rd} LSB.
  - If $d = 5$, then invert 1^{st} and 3^{rd} LSBs.
  - If $d = 6$, then invert 2^{nd} and 3^{rd} LSBs.
  - If $d = 7$, then invert 1^{st}, 2^{nd} and 3^{rd} LSBs.
- Apply the optimal LSBs method to the pixel obtained in the previous step.
- Repeat steps from 5 to 8 for all edge pixels corresponding to Hough Transform peaks.
- After that, repeat the previous steps from step 6 for all the rest of the pixels (what's left of edge pixels and all smooth pixels) in the cover image but note that n will be $(n-1)$.

B. The Extracting Procedure

In the extracting procedure, the required input is the original and stego images. The output of this procedure is the secret data. The receiver needs to compare the stego image with the original image to recover the secret data. The following are the steps for the extracting procedure:

- Obtain the edge areas of the original image using Canny detector and Hough Transform.
- Find the peaks using Hough peak.
- Find the pixels in the original image corresponding to a particular Hough Transform peak.

- Compare n-LSBs of each edge pixel in the original image with the corresponding in the stego image. Determine which bits are inverted and based on that estimate the decimal value.
- When the last LSB is inverted, subtract the decimal value from $((2^n - 1)$ to obtain the original decimal value.
- Repeat the previous steps from 3 to 5 for all edge pixels corresponding to Hough Transform peaks.
- After that, repeat the previous steps 4 and 5 for all the rest of the pixels (what's left of edge pixels and all smooth pixels). Note that n will be $(n-1)$.
- Convert the decimal numbers to a binary system. Note that, every decimal value must consist of n bits in the case of edge pixels corresponding to Hough Transform peaks or $(n-1)$ bits in the case of all the rest of the pixels (what's left of edge pixels and all smooth pixels). If the decimal number consists of less than that, then add $0^{'}$s left the bits.
- With this manner, all the secret data bits will be retrieved completely.

V. Experimental Results

Several experiments are performed to evaluate the presented method. Seven standard grayscale images "Lena", "Baboon", "Peppers", "Cameraman", "Barbara", "Elaine" and "Tiffany" each of size 512×512 are used as cover images. We use gray images since color images are large, which attracts attention although they have more space for hiding data [14]. A series of pseudo-random data are embedded into the cover images. We used Matlab 2017 to execute our method. The performance of the presented method is estimated from the two main evaluating factors: the visual quality of stego images and the embedding capacity. The quality of the stego image is estimated by using PSNR which is the most common measurements of steganography performance. In our approach, we used PSNR to estimate the similarity between the stego images and the original images. PSNR has a large value when the original image and the stego image are similar. This means that the stego image has less image distortion and high visual quality. The PSNR is evaluated in decibel scale (dB) and known as follows [41] and [21]:

$$PSNR = 10 \cdot \log_{10} \frac{255^2}{MSE} (dB) \tag{9}$$

Where MSE is the Mean Square Error between the cover and stego images. MSE and PSNR are inversely proportional. For a cover image with height H and width W, MSE is defined as:

$$MSE = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} \left(I_{ij} - I_{ij}^{'} \right)^2 \tag{10}$$

Where I_{ij} and $I_{ij}^{'}$ are the pixel values of the cover and stego images respectively.

For capacity which is the second evaluating factor, capacity is the number of secret data bits that can be hidden into a pixel which is measured in bits per pixel (bpp). It is used to evaluate the effectiveness of the data embedding methods. A large value of capacity means that the cover image can carry more secret data bits. The embedding capacity is estimated as follows [41] and [21]:

$$C = \frac{\|S\|}{H \times W} (bpp) \tag{11}$$

where $\|S\|$ represents the total number of secret bits embedded into a cover image with size $H \times W$ pixels. There is an inverse relationship between capacity and PSNR. This means that increasing the capacity increasing the MSE and this affects inversely on the PSNR. Therefore, it should be a trade-off between capacity requirements and PSNR

TABLE I: Experimental Results

Cover Images	e =4 & s =3		e =5 & s =4	
	Capacity	PSNR	Capacity	PSNR
Lena	807774	40.5871	1069918	34.3994
Baboon	832703	39.7345	1094847	34.7204
Peppers	808003	40.5687	1070147	36.0981
Cameraman	807353	40.6131	1069497	33.3830
Barbara	813402	40.3876	1075546	34.1777
Elaine	808469	40.5478	1070613	33.3312
Tiffany	806165	40.6601	1068309	33.4615

TABLE II: Comparison of proposed method and Ref. [25].

Cover Images	Ref. [25]		Proposed Method	
	Capacity	PSNR	Capacity	PSNR
Lena	0.0958	54.5336	807774	40.5871
Baboon	0.0389	58.2953	832703	39.7345
Pepper	0.0807	55.1808	808003	40.5687
Elaine	0.0673	56.2007	808469	40.5478

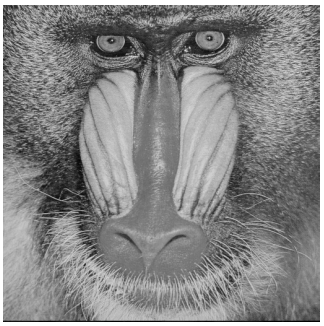
Table I shows the results of the presented method at threshold=0.2 in terms of embedding capacity (in bits) and PSNR value. In this table e pointing to the number of LSB for edge pixels corresponding to hough peaks and s pointing to the number of LSB for all the rest of the pixels (what's left of edge pixels and all smooth pixels) in the cover image. The results of this table indicate that our method can embed a large amount of data with high PSNR values. The average value of PSNR is greater than 40.44, this means that the original and stego images are very similar and it is difficult for the human eye to distinguish between them.

Figure 2 and Figure 3 show the stego images created by our presented method at threshold=0.2 and various values of e and s. These figures demonstrate that the distortion resulted from the embedding is imperceptible to the human vision.

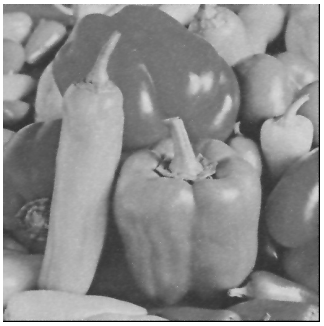
Table II and Table III show a comparison between the presented method with Maniriho and Ahmad [25] and our previous work [24] at threshold=0.2, e =4 and s =3. Results show that the presented method can embed data much more than these methods. This indicates that our method has high embedding capacity. It is noticed that increasing the capacity increasing the MSE and this affects inversely on the PSNR as we mentioned before.

Table IV shows another comparisons between our experiments at threshold=0.2, $e = 4$ and $s = 3$ with Sahu and

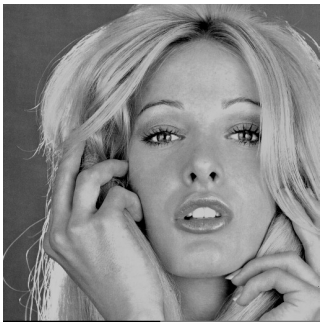
(a) Lena



(b) Baboon



(c) Peppers



(d) Tiffany

Fig. 2: Four stego images at threshold=0.2 and (e =5 & s =4).

(a) barbara

(b) elaine

(c) Cameraman

Fig. 3: Three stego images at threshold=0.2 and (e =4 & s =3).

TABLE III: Comparisons of proposed method and Ref. [24].

Cover Images	Ref. [24]		Proposed Method	
	Capacity	PSNR	Capacity	PSNR
Lena	1048568	36.8362	1069918	34.3994
Baboon	1048568	36.8239	1094847	34.7204
Pepper	1048568	36.8434	1070147	36.0981
Cameraman	1048568	36.9462	1069497	33.3830
Barbara	1048568	36.8712	1075546	34.1777
Elaine	1048568	36.8815	1070613	33.3312
Tiffany	1048568	36.6712	1068309	33.4615

Swain [31] method in terms of capacity and PSNR. It is

TABLE IV: Comparison of proposed method and Ref. [31]

Cover Images	Ref. [31]		Proposed Method	
	Capacity	PSNR	Capacity	PSNR
Lena	524288	51.15	807774	40.5871
Baboon	524288	51.16	832703	39.7345
Pepper	524288	51.17	808003	40.5687
Barbara	524288	51.16	808469	40.5478

clear from this table that the embedding capacity for the presented method is better than Ref. [31]and this means that the presented method can hide a large amount of data.

From the previous comparisons, we notice that our pre-

sented method provides a large embedding capacity and high stego image quality. This indicates the good balance between the size of data that can be hidden in the stego image and its visual quality. As a result, our method is safe to carry data over networks.

VI. Conclusion

In this paper, a new method of data hiding based on LSB and Hough Transform is presented. Our method considers the feature of edge areas which can tolerate much more changes than smooth areas without making perceptible distortion. In this method, Hough Transform is used to obtain the edge areas after that peaks can be obtained. LSBs are inverted to enhance the quality of stego image. Lastly, the optimal LSBs method is used to improve the results. The algorithm is tested on many different standard images with different capacity. The experimental results show the efficiency of our presented method which provides a large capacity and high imperceptibility.

References

[1] W. S. Sari, E. H. Rachmawanto, C. A. Sari, *et al.*, "A good performance otp encryption image based on dct-dwt steganography," *Telkomnika*, vol. 15, no. 4, pp. 1987–1995, 2017.

[2] R. D. Ardy, O. R. Indriani, C. A. Sari, E. H. Rachmawanto, *et al.*, "Digital image signature using triple protection cryptosystem (rsa, vigenere, and md5)," in *Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS), 2017 International Conference on*, pp. 87–92, IEEE, 2017.

[3] A. Winarno, D. Setiadi, A. Arrasyid, C. Sari, and E. Rachmawanto, "Image watermarking using low wavelet subband based on 8× 8 sub-block dct," in *International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang*, 2017.

[4] L. Kothari, R. Thakkar, and S. Khara, "Data hiding on web using combination of steganography and cryptography," in *Computer, Communications and Electronics (Comptelix), 2017 International Conference on*, pp. 448–452, IEEE, 2017.

[5] G. Ardiansyah, C. A. Sari, E. H. Rachmawanto, *et al.*, "Hybrid method using 3-des, dwt and lsb for secure image steganography algorithm," in *Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2017 2nd International conferences on*, pp. 249–254, IEEE, 2017.

[6] Y. P. Astuti, E. De Rosal Ignatius Moses Setiadi, H. Rachmawanto, and C. A. Sari, "Simple and secure image steganography using lsb and triple xor operation on msb,"

[7] G. Chugh, "Image steganography techniques: A review article.," *Acta Technica Corvininesis-Bulletin of Engineering*, vol. 6, no. 3, 2013.

[8] B. Yang and B. Deng, "Steganography in gray images using wavelet," *Proceedings of ISCCSP*, 2006.

[9] A. Setyono *et al.*, "Stegocrypt method using wavelet transform and one-time pad for secret image delivery," in *Information Technology, Computer, and Electrical Engineering (ICITACEE), 2017 4th International Conference on*, pp. 203–207, IEEE, 2017.

[10] A. U. Islam, F. Khalid, M. Shah, Z. Khan, T. Mahmood, A. Khan, U. Ali, and M. Naeem, "An improved image steganography technique based on msb using bit differencing," in *Innovative Computing Technology (INTECH), 2016 Sixth International Conference on*, pp. 265–269, IEEE, 2016.

[11] E. H. Rachmawanto, C. A. Sari, *et al.*, "A performance analysis stegocrypt algorithm based on lsb-aes 128 bit in various image size," in *Application for Technology of Information and Communication (iSemantic), 2017 International Seminar on*, pp. 16–21, IEEE, 2017.

[12] D. R. I. M. Setiadi, "Improved payload capacity in lsb image steganography uses dilated hybrid edge detection,"

[13] R. Bhardwaj and V. Sharma, "Image steganography based on complemented message and inverted bit lsb substitution," *Procedia Computer Science*, vol. 93, pp. 832–838, 2016.

[14] N. Akhtar, S. Khan, and P. Johri, "An improved inverted lsb image steganography," in *IEEE International Conference on Issues and challenges in Intelligent Computing techniques (ICICT)*, pp. 7–8, 2014.

[15] M. A. Majeed and R. Sulaiman, "An improved lsb image steganography technique using bit-inverse in 24 bit colour image.," *Journal of Theoretical & Applied Information Technology*, vol. 80, no. 2, 2015.

[16] M. Juneja and P. S. Sandhu, "A new approach for information hiding in color images using adaptive steganography and hybrid feature detection with improved psnr and capacity," *International Journal of Engineering and Technology (IJET)*, vol. 5, no. 2, pp. 1853–1862, 2013.

[17] S. Singh and A. Datar, "Improved hash based approach for secure color image steganography using canny edge detection method," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 15, no. 7, p. 92, 2015.

[18] F. U. Mangla, S. Nokhaiz, M. Ramzan, and I. U. Lali, "A novel steganography technique using grayscale image segmentation," *International Journal of Advanced and Applied Sciences*, vol. 6, no. 5, pp. 84–91, 2019.

[19] Y. M. Abdalnour, A. S. Huwedi, and K. A. Bozed, "Image steganography approach based on straight line detection," in *Sciences and Techniques of Automatic Control and Computer Engineering (STA), 2016 17th International Conference on*, pp. 317–327, IEEE, 2016.

[20] A. Nejahi and F. Z. Boroujeni, "The improvement of steganography function based on the least significant bit in rgb color," *American Journal of Software Engineering and Applications*, vol. 5, no. 3-1, pp. 1–4, 2016.

[21] D. K. Nayak and C. Bhagvati, "A threshold-lsb based information hiding scheme using digital images," in *Computer and Communication Technology (ICCCT), 2013 4th International Conference on*, pp. 269–272, IEEE, 2013.

[22] K. Joshi and R. Yadav, "A new lsb-s image steganography method blend with cryptography for secret communication," in *Image Information Processing (ICIIP), 2015 Third International Conference on*, pp. 86–90, IEEE, 2015.

[23] K. Joshi and R. Yadav, "New approach toward data hiding using xor for image steganography," in *Contemporary Computing (IC3), 2016 Ninth International Conference on*, pp. 1–6, IEEE, 2016.

[24] D. Nashat and L. Mamdouh, "An efficient steganographic technique for hiding data," *Journal of the Egyptian Mathematical Society*, vol. 27, pp. 1–14, 2019.

[25] P. Maniriho and T. Ahmad, "Information hiding scheme for digital images using difference expansion and modulus function," *Journal of king saud university-computer and information sciences*, vol. 31, no. 3, pp. 335–347, 2019.

[26] A. Karawia, "Medical image steganographic algorithm via modified lsb method and chaotic map," *IET Image Processing*, vol. 15, no. 11, pp. 2580–2590, 2021.

[27] M. Hashim, M. S. MOHD RAHIM, and A. A. ALWAN, "A review and open issues of multifarious image steganography techniques in spatial domain.," *Journal of Theoretical & Applied Information Technology*, vol. 96, no. 4, 2018.

[28] Z. N. Al-Kateeb, M. J. Al-Shamdeen, and F. S. Al-Mukhtar, "Encryption and steganography a secret data using circle shapes in colored images," in *Journal of Physics: Conference Series*, vol. 1591, p. 012019, IOP Publishing, 2020.

[29] A. Zenati, W. Ouarda, and A. M. Alimi, "A new digital steganography system based on hiding online signature within document image data in yuv color space," *Multimedia Tools and Applications*, vol. 80, pp. 18653–18676, 2021.

[30] M. S. Taha, M. S. M. Rahem, M. M. Hashim, and H. N. Khalid, "High payload image steganography scheme with minimum distortion based on distinction grade value method," *Multimedia Tools and Applications*, vol. 81, no. 18, pp. 25913–25946, 2022.

[31] A. K. Sahu and G. Swain, "High fidelity based reversible data hiding using modified lsb matching and pixel difference," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 4, pp. 1395–1409, 2022.

[32] H.-W. Tseng and H.-S. Leng, "A reversible modified least significant bit (lsb) matching revisited method," *Signal Processing: Image Communication*, vol. 101, p. 116556, 2022.

[33] P. V. Hough, "Method and means for recognizing complex patterns," Dec. 18 1962. US Patent 3,069,654.

[34] P. Mukhopadhyay and B. B. Chaudhuri, "A survey of hough transform," *Pattern Recognition*, vol. 48, no. 3, pp. 993–1010, 2015.

[35] M. Rizon, Y. Haniza, S. Puteh, A. Yeon, M. Shakaff, S. Abdul Rahman, M. Sugisaka, Y. Sazali, M. M Rozailan, and M. Karthigayan, "Object detection using circular hough transform," 2005.
[36] R. K. Murmu and M. Jhaniya, *Image Segmentation Using Hough Transform*. PhD thesis, 2009.
[37] C.-K. Chan and L.-M. Cheng, "Hiding data in images by simple lsb substitution," *Pattern recognition*, vol. 37, no. 3, pp. 469–474, 2004.
[38] N.-I. Wu and M.-S. Hwang, "Data hiding: current status and key issues.," *IJ Network Security*, vol. 4, no. 1, pp. 1–9, 2007.
[39] M. H. Mohamed and L. M. Mohamed, "High capacity image steganography technique based on lsb substitution method," *Applied Mathematics & Information Sciences*, vol. 10, no. 1, p. 259, 2016.
[40] M. Juneja and P. S. Sandhu, "Performance evaluation of edge detection techniques for images in spatial domain," *International journal of computer theory and Engineering*, vol. 1, no. 5, p. 614, 2009.
[41] C.-C. Chang, Y.-C. Chou, and T. D. Kieu, "Information hiding in dual images with reversibility," in *Multimedia and Ubiquitous Engineering, 2009. MUE'09. Third International Conference on*, pp. 145–152, IEEE, 2009.