第 48 卷 第 6 期
2021 年 6 月

湖 南 大 学 学 报（自 然 科学版）
Journal of Hunan University（Natural Sciences）

Vol. 48. No. 6.
June 2021

StegoBound: A Novel Image Steganography Technique Using Boundary-Based LSB Substitution

Syed Saad Ahmed[1], Mashal Memon[1], Rabeea Jaffari[2], Moazzam Jawaid[1]

[1] Computer Systems Engineering, Mehran University of Engineering and Technology, Jamshoro, Pakistan

[2] Software Engineering, Mehran University of Engineering and Technology, Jamshoro, Pakistan

Abstract: The safe exchange of private information in the current web age is a significant security concern that has come around after developing steganography as a piece of conspicuous information concealing strategy. Steganography methods guarantee secure information by hiding the transmission channel and are described using three key boundaries: specific strength, implanting limit, and intangibility. The cutting-edge steganography strategies anyway neglect to accomplish an ideal compromise among the key steganographic factors. This research study describes a novel image steganography technique StegoBound based on gradient, which efficiently hides the secret message and produces excellent results for the essential steganographic characteristics. To produce top-notch stego-pictures, StegoBound shrouds the restricted information in the sixth, seventh, and eighth least significant bits (LSBs) of the boundary zone pixels in grayscale cover pictures. The nature of the stego-pictures is assessed through primary closeness file (SSIM), widespread picture quality file (UQI), mean square of error (MSE), Peak Signal to Noise Ratio (PSNR), mean qualities, and histogram investigation. The novel method's effectiveness evaluation is confirmed by calculating MSE, SSIM, PSNR, and UQI. Experimental results and comparative studies reveal that our proposed technique achieves state-of-the-art results in hiding the secret data by providing an optimal trade-off between imperceptibility, embedding capacity, and security.

Keywords: steganography, data hiding, LSB substitution, MSB, boundary.

隐写术界：一种使用基于边界的最低有效位替换的新型图像隐写技术

摘要：在当前的网络时代，隐私信息的安全交换是一个重要的安全问题，它是在将隐写术发展为一种显眼的信息隐藏策略之后出现的。隐写术方法通过隐藏传输通道来保证信息的安全，并使用三个关键边界进行描述：特定强度、植入限制和无形性。无论如何，尖端的隐写术策略都忽略了在关键隐写术因素之间实现理想的折衷。这项研究描述了一种基于梯度的新型图像隐写技术隐写术界，它有效地隐藏了秘密信息，并为基本的隐写特征产生了出色的结果。为了生成一流的隐写图片，隐写术界将受限信息包含在灰度覆盖图片中边界区域像素的第六、第七和第八个最低有效位中。隐写图片的性质通过主要接近度文件、广泛的图片质量文件、误差均方、峰值信噪比、平均质量和直方图调查进行评估。通过计算均方误差、结构相似指数、峰值信噪比和通用图像质量指数来确认新方法的有效性评估。实验结果和比较研究表明，我们提出的技术通过提供不可感知性、嵌入容量和安全性之间的最佳权衡，在隐藏秘密数据方面取得了最先进的结果。

关键词：隐写术、数据隐藏、最低有效位替换、最高有效位、边界。

Received: March 16, 2021 / Revised: April 13, 2021 / Accepted: May 17, 2021 / Published: June 28, 2021

About the authors: Syed Saad Ahmed, Mashal Memon, Computer Systems Engineering, Mehran University of Engineering and Technology, Jamshoro, Pakistan; Rabeea Jaffari, Software Engineering, Mehran University of Engineering and Technology, Jamshoro, Pakistan; Moazzam Jawaid, Computer Systems Engineering, Mehran University of Engineering and Technology, Jamshoro, Pakistan

1. Introduction

Confidential information was once passed down by etching it on the scalps of slaves and servants or hiding it on the backs of wax tablets, rabbits' abdomens, or the backs of wax tablets. With the advent of digitization, automated approaches, such as cryptography and steganography, have replaced the traditional methods and are efficiently used to conceal confidential data. Steganography is a Greek word that signifies "disguised composition." "Steganos" signifies "covered," and "graphy" signifies "composing." The investigation of steganography is the camouflage of information by darkening the transmission or correspondence way [1]. The concealed transmission of hidden data or messages makes steganography different from cryptography. The latter only scrambles the message in an incomprehensible format but does not obfuscate the message's presence, increasing the chance of detection by arousing suspicion. Thus, steganography offers increased benefits over cryptography by concealing the very existence of the message itself, which avoids drawing the interest of unauthenticated users, making it more resilient to the cryptographic approaches [2]. However, for additional security and privacy, steganography and cryptography are often used together [3]. Steganographic techniques are employed in a range of research fields, including but not limited to identifying piracy in digital material, computer forensics, and tracing criminal behavior on the internet. [4].

Steganography works by concealing the private information or the payload inside a transporter (like content, picture, video, or sound); just the sender and beneficiary know about the local intel's quality [5]. The payload message is covered in the transporter/cover medium utilizing a fitting installing capacity to make a stego-transporter vague from the cover medium, keeping away from any doubt. The stego-transporter comprising of the mysterious message is then moved to the beneficiary by the sender. The message is recovered using a removing capacity utilizing a stego-key which is a common mystery between the sender and the beneficiary [6]. The procedure of steganography is depicted in Fig. 1. The most widely used carrier medium for steganography are images where various properties of images such as luminance, contrast, and colors are varied to hide the message [7] and are the main focus of this research study.

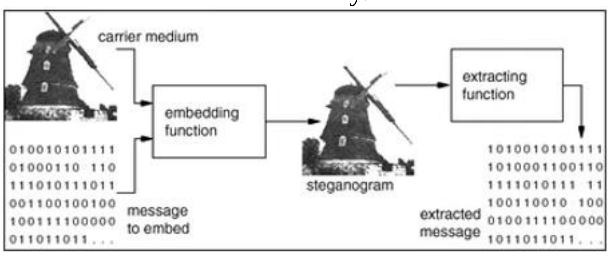

Fig. 1 Steganography process

The success of any steganographic technique can be determined via three parameters, namely: imperceptibility, payload capacity, and robustness. Imperceptibility can be described as the generated stego-image's indistinguishability from the cover image; attackers or stego-analysts find it difficult to uncover the important information in the stego-image. The amount of imperceptibility is commonly expressed in PSNR (Peak Signal to Noise Ratio), with a greater PSNR indicating a higher level of imperceptibility. The amount of message bits that may be securely encoded in the pixels of the cover picture without being statistically detected is referred to as payload capacity. A sufficient payload capacity is required for an efficient steganography process. Finally, resilience assesses the steganographic technique's ability to withstand steganalysis attempts to obtain the secret message. These steganographic parameters have a significant trade-off [5].

Image steganography is partitioned into 2 types: spatial space and transforms/frequency space. After using spatial domain procedures, the important data is straightforwardly concealed in the cover picture. In contrast, transform domain methods are used to hide enormous quantities of data in the frequency space by modifying the amplitude of all transformations of the cover picture. This research study focuses on spatial domain techniques only due to their widespread adoption, high hiding capability, and easy retrieval. However, we refer the readers to the research works in [8], [9], [10] for more information regarding the spatial domain, transforms domain, and steganalysis techniques.

1.1. Motivation

An in-depth survey of the existing literature reveals that although the state-of-the-art spatial domain steganography methods (LSB and MSB) ensure higher imperceptibility, these techniques have poor payload capacity and robustness due to the use of a fixed embedding function and the uniform number of bits, as well as the fixed bit positions (LSB or MSB), to embed the secret message respectively. These shortcomings make it easier for the stego-analysts to intercept and interpret the stego-images. Improvements and modifications to these techniques attempt to improve the payload capacity and robustness (or both) but fail at achieving higher imperceptibility levels. The mentioned shortcomings of the available steganographic methods motivate this research study.

1.2. Contribution

To address the shortcomings in the available steganography approaches, the contributions of this research study are two-fold, namely:

1. A unique picture steganography approach based on boundary-based LSB replacement achieves a good

balance of imperceptibility, payload capacity, and resilience.

2. Validation of the proposed method on benchmark image data using state-of-the-art results.

The following is how the remaining of this research study is ordered: Section 2 discusses the various steganography strategies and their benefits and drawbacks, section 3 discusses the research methodologies used in this work as well as the suggested steganography technology "Stegobound," and section 4 discusses the proposed methodology's experimental validation and results.

2. Related Works

LSB, MSB, and hybrid approaches are the current state-of-the-art spatial domain picture steganography approaches published in the literature. This section provides a quick summary of various strategies.

2.1. Least Significant Bit (LSB) Technique

To make the stego-picture, most of the writing depends on the Most uncritical Bit (LSB) adjustment approach, which embeds the mysterious message at all huge bit of every byte of the cover picture. The mysterious message and the cover picture are changed over to parallel first, and afterward, the mysterious message is embedded in the cover picture's LSBs. This inserting activity is rehashed until each LSB of the cover picture has been utilized. Until the entirety of the mysterious message, bits have been appropriately implanted in the cover picture. [11]. Despite its modest payload capacity and strong imperceptibility, the conventional LSB is subject to simple assaults. As a result, academics have proposed numerous enhancements to the basic LSB approach to enhance the resilience and payload capacity, such as embedding the important data in the LSBs of the brightest and darkest picture pixels [12] On the other hand, rather than the 1 least significant bit of every byte, the important information may be encoded in the 4 least significant bits of every byte of the cover picture. [13.] Another research suggested by the authors in [14] is to fuse some extra bits with the important message to make the stego-images histogram seem like the first image. In the substitution technique for LSB, this methodology forestalls the histogram attack. The hidden data is embedded in the research described in [15] by utilizing the seventh bit of a picture's chosen pixel as a sign and the seventh bit of the next pixel as a pointer. Two epic steganographic techniques dependent on the substitution of variable length substitution of bits are introduced in [16]. The main methodology hides the least significant bit of personal data per pixel, while the subsequent methodology conceals two bits of important information per pixel utilizing the LSB approach. He et al. utilizes objective examination to compute the implanting profundity with the goal that a versatile number of bits might be disguised in various pixels to expand the number of bits covered in every pixel [17]. The research work in [18] presents a steganographic framework for RGB pictures to upgrade the payload limit and give great intangibility utilizing sorcery LSB replacement and Hash Message Validation Code (HMAC). Message bit subordinate inserting is proposed by Swain and Lenka in [19], where the important message's touch design help in deciding the substituting positions in the pixels of the cover picture.

LSB steganography procedures are utilized related to various cryptographic and different ways to deal with incrementing the framework's power. [20] gives two cryptographic steganographic approaches; the first proselytes the payload picture into an encoded text utilizing an S-DES cryptographic calculation with a mysterious key and afterward hides the scrambled content into the transporter picture utilizing LSB replacement. The subsequent technique changes over the payload picture into an S-DES scrambled picture and afterward utilizes LSB replacement to conceal it in the transporter picture. The methodology portrayed in [21] consolidates two methodologies, MP (Network Example) and LSB (Bolted Symmetric Paired), in which the mysterious message is covered up inside the framework blocks.

Pixel Value Differencing (PVD) [22], [23] and pixel correlation methods [24], [25] are notable tracks in LSB based substitution where a pixel value calculated from 2 consecutive pixels, which are substituted by the bits of the important data as the new difference in the former technique. In contrast, the pixel correlation scheme exploits the connection of a picture element with its neighboring picture elements for embedding the secret message. A productive and dynamic inserting calculation utilizing the PVD strategy is accounted for in [26] that conceals the secret information and makes secret code-breaking a decent disturbance for the aggressor and addresses an extraction calculation that adequately extricates the whole secret message with no deficiency of secret information.

Lastly, the closest LSB track to our proposed approach is to implant the secret message in the cover picture using edge detection algorithms. Youssef Bassil proposes to implant the important data in the three LSBs of every color channel of the edge pixel determined via Canny's edge algorithm. Still, the research work does not report any results via benchmark steganographic parameters [27]. The research works reported in [28] and [29] embed the secret message in LSBs of edge pixels extracted via edges-identification method and hybrid canny edge detection and a fuzzy edge detector with 2k correction method, respectively. However, our research method utilizes the LSBs of boundary pixels instead of edge pixels to embed the secret message and achieves superior performance in all aspects, as discussed in sections 3 and 4. We refer the readers to survey works in [30], [31] for more information on LSB steganography techniques.

2.2. Most Significant Bit (MSB) Technique

As the name implies, the MSB technique uses the most or mean significant bits (higher-order bits) for hiding messages in the cover images. Studies have shown that LSB techniques perform better than MSB techniques [32]. However, MSB techniques can offer better security as stego-analysts are usually aware of the LSBs and design the attacks accordingly to extract the secret messages. In this research work, we briefly discuss the MSB techniques in the chronological order of their publication for better comparison and validation of our proposed technique.

[33] utilizes a 1-cycle MSB in a tumultuous way with the mysterious picture key to conceal the secret message. To compute the following looming place in the picture, 8x8 size framework blocks are browsed the cover picture, with the mysterious key in the main square. [34] depicts a reversible information camouflage methodology dependent on Neighbor Mean Interpolation (NMI) and R-weighted coding. Pixel value differencing (PVD) is used in [35] for implanting the data in the RGB image with a variable number of bits for enhanced security. In [36], the embedding of a secret message occurs in the 4th or 5th MSB of the pixel. The pixels to be utilized for embedding are chosen via three-pixel groups, and OPAP (Optimal Pixel Adjustment Process) is used to lessen distortions that are caused due to the embedding procedure. According to the research in [37], the fifth bit of the cover picture is utilized for concealing the mysterious message by utilizing a technique known as touch differencing on the fifth and sixth bits. If the differencing result isn't indistinguishable from the secret message nibbled, the bit of the cover picture is adjusted. In [38], a strategy is proposed. The slightest bit per pixel is hidden in encoded pictures by preprocessing the picture to sidestep mistakes that redo the nature of changed pictures. The research works in [39] and [40] present improved calculations for disguising the important data in MSBs of the RGB cover picture utilizing pixel esteem pointers. In [39], the green channel fills in as a pixel value marker for concealing the mysterious message in the fifth and sixth bits of the blue or red color plane based on even and odd equalities, while in [40] red channel fills in as the pixel value indicator.

2.3. Hybrid Technique

For image steganography, hybrid approaches often combine LSB and MSB methods. Solomon et al. [41] implant the mysterious message in the cover picture utilizing two bits (one LSB and one MSB). [42] depicts a technique for installing a mysterious message in the MSB of a cover picture by utilizing the LSB of the cover picture as a pointer. The research in [43] recommends a framework where the secret message bits are first encoded utilizing even and odd equalities. Afterward, the important message is implanted in the LSB of the cover picture utilizing the MSBs as the pixel indicator. Though these techniques [42], [43] do not embed the information in the MSB and LSB jointly, they use both the schemes and hence place them under the discussion of hybrid techniques.

2.4. Conclusion

Several spatial domain image steganography techniques were reviewed, such as LSB, MSB, and hybrid techniques. While these techniques have shown acceptable performances, these still do not achieve an optimal trade-off between the key steganographic parameters that are imperceptibility, robustness, and payload capacity [44]. We propose a novel steganography technique in section III, named StegoBound, that resolves this issue and achieves an optimal balance between the steganographic parameters.

3. Stegobound: A Novel Image Steganography Technique Using Boundary-Based LSB Substitution

We propose a new steganography method for implanting the important data in the LSBs of the cover picture’s boundary pixels in this research paper. LSB technique is chosen because it guarantees high imperceptibility as compared to the MSB technique. At the same time, the boundary pixels help increase the payload capacity and the robustness of the proposed technique guaranteeing an optimal trade-off between the key parameters.

The novelty of this research is that the data is being hidden in the boundary region, with 3 bits being used to implant the secret information.

StegoBound technique is essentially a two-step process comprising of image segmentation and LSB substitution. Firstly, thresholding-based image segmentation is used to separate the background region of the cover image from its foreground region for boundary calculation. The boundary region is computed via edge detection. The confidential data is then implanted in the cover picture’s least significant bits as 6th, 7th, and 8th, using LSB replacement. It should be noted that the proposed method only works with grayscale photos. In sub-sections 2.1 and 2.2, the embedding and extraction methods for implanting and extracting the secret information to/from the cover image are discussed.

3.1. Embedding Algorithm

Input: Grayscale cover image, the secret message

Output: Stego-image

1. Select the secret information and the cover picture.

2. Convert the cover image into binary.
3. Separate the foreground region from the background with thresholding-based segmentation in the cover image.
4. Compute the boundary region in the cover image by edge detection.
5. Embed the secret message in the boundary region pixels (indicated by a high gradient value between the foreground and the background) using three LSBs (6th, 7th, and 8th bit) until the end of the secret message is read to generate the final stego-image.

3.2. Extraction Algorithm

Input: Stego-image

Output: Secret Message

1. Read the stego-image and convert it into binary.
2. Separate foreground region from the background with the help of thresholding-based segmentation.
3. Compute the boundary region in the stego-image by edge detection.
4. Extract the secret message by reading the 6th, 7th, and 8th bits of the stego-image from boundary region pixels (i.e., places where high gradients are observed).

The workflow of the embedding and extraction algorithm is presented in Fig. 2 and 3, respectively.

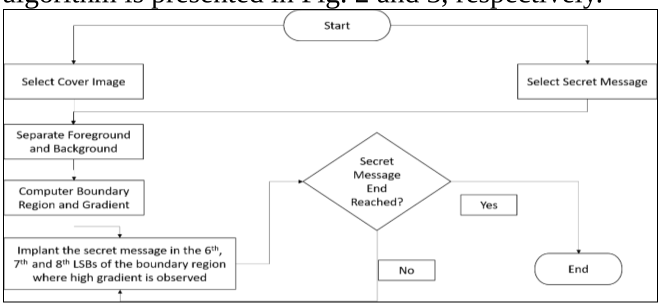

Fig. 2 Workflow of embedding algorithm

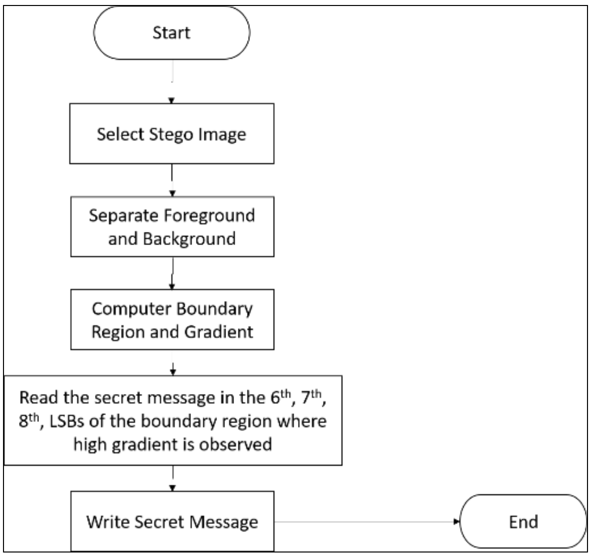

Fig. 3 Workflow of extraction algorithm

4. Results and Discussion

The suggested approach is applied to utilize MATLAB 2017a. Benchmark cover images used to assess the performance of the intended approach are Lena.png, Bluehills.png, Mandrill.png, Boat.png, and House.png, as shown in Fig 4.

The limitation of the results will be if the boundary isn't computed properly, and the foreground and background aren't separated clearly.

The cover images are grayscale png images of size 512x512, 128x256, 512x512, 512x512 and 256x256, respectively.

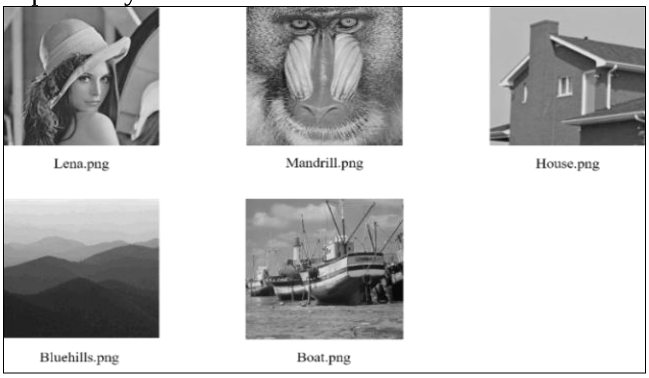

Fig. 4 Benchmark cover images

The stego-images (corresponding to the benchmark cover images) generated via the proposed method StegoBound are depicted in Fig. 5.

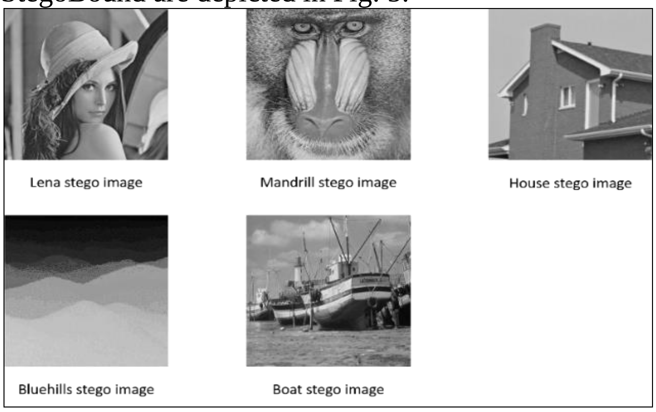

Fig.5 Stego images generated via StegoBound

The generated stego-pictures are entirely identical to the benchmark cover images (shown in Fig. 4) and are unidentifiable by the naked eye, as shown in Fig. 5. That implies that the quality of the images is not altered by implanting the secret message. Moreover, the use of 3 LSBs, i.e., 6th, 7th, and 8th bit for hiding the secret message delivers high payload capacity to this technique, and the use of boundary pixels guarantees better security. The validation findings of the proposed StegoBound methodology are shown and evaluated in terms of imperceptibility, robustness, and payload capacity.

4.1. PSNR and MSE

Imperceptibility of the generated stego-images is evaluated in terms of PSNR values, where a higher PSNR signifies a superior quality stego-image. The

PSNR is, in turn, calculated based on MSE (Mean-squared error) values. The MSE and PSNR values for the stego-images can be mathematically calculated using eq (1) and eq (2), respectively.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (1)$$

where mx n denotes the rows and columns of noise-free grayscale stego-image. I and K refer to the original image and the stego picture (processed image). With MSE being calculated, PSNR (in db) is calculated as:

$$PSNR = 20.\log_{10}(MAX_I) - 10.\log_{10}(MSE) \quad (2)$$

4.2. Payload Capacity

The payload or the embedding capacity of this steganography method can be determined mathematically using Eq. (3).

$$Payload\ Capacity = \text{Number of boundary pixels x 3} \quad (3)$$

The PSNR, MSE, and Capacity values obtained for the stego-images generated via StegoBound (depicted in Fig. 5) are summarized in Table 1.

Table 1 PSNR, MSE, and capacity values for stego-images generated via StegoBound

S.#	Stego Image	PSNR	MSE	Capacity
1	Lena	64.154	0.0125	4755
2	Mandrill	72.439	0.0037	7668
3	House	72.552	0.0036	2856
4	Bluehills	68.047	0.010	2178
5	Boat	64.6688	0.0221	6522

Table 1 shows that the PSNR and MSE values of StegoBound are very good as the PSNR is above 45 decibels (db), and the MSE values are nearly zero. Moreover, the payload capacity of StegoBound is also sufficiently good due to the use of 3 LSBs.

4.3. SSIM and UQI

The Structural Similarity Index (SSIM) is a perceptual measure that measures picture quality debasement because of preparing like information pressure or transmission misfortunes. It is a full reference measure that requires two pictures—a reference picture and a processed picture—from a similar picture catch. Utilizing eq, SSIM might be resolved mathematically (4).

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (4)$$

Universal Image Quality Index (UIQI) is a proportion of how great a picture is in the wake of inserting. UQI utilizes loss of a relationship, luminance contortion, and differentiation twisting to evaluate picture quality. UQI can be determined numerically via Eq. (5).

$$UQI = \frac{4\,\sigma_{xy}\,\bar{x}\,\bar{y}}{(\sigma_x^2 + \sigma_y^2)\,[(\bar{x})^2) + (\bar{y})^2)]} \quad (5)$$

SSIM and UQI are given in Table 2

Table 2 SSIM and UQI values for stego-images generated via StegoBound

S.no	Image	SSIM	UQI
1	LENA (512x512)	0.9953	0.9998
2	MANDRILL (512x512)	0.9985	0.9998
3	HOUSE (256x256)	0.9956	0.9998
4	BLUEHILLS (128x128)	0.9984	0.9996
5	BOAT (512x512)	0.9968	0.9998

The results of SSIM and UQI obtained from the StegoBound technique are of high quality as both the SSIM and UQI for every stego image formed by StegoBound is approximately 1. 1 means that the stego image and original image are the same.

4.4. Comparison

A comparison of the PSNR findings achieved via StegoBound (Table 1) with the PSNR values of other steganography techniques can validate the superiority of the intended StegoBound approach over other state-of-the-art techniques (discoursed in section 2). Table 3 indicates the outcomes of the comparison analysis.

Table 3 Comparative analysis of StegoBound with state-of-the-art techniques in terms of PSNR

S.#	Technique	Category	Image	Type	PSNR
1	[15]			Grayscale	49.37
2	[16] 1-bit scheme			Color	51.63
3	[16] 2-bit scheme			Color	49.90
4	[19]			Color	50.93
5	[21]	LSB		Color	46.64
6	[22]			Color	43.63
7	[23]			Color	47.51
8	[28]			Color	47.5897
9	[29]			Grayscale	40.81
10	[34]		Lena (512x512)	Color	39.566
11	[35]			Grayscale	42.26
12	[36]			Color	42.447
13	[37]	MSB		Grayscale	51.17977
14	[38]			Grayscale	57.58
15	[39]			Color	53.7317
16	[40]			Color	48.0002
17	[42]	Hybrid		Color	54.27
18	[43]			Color	62.73
19	StegoBound	LSB		Grayscale	64.154

S.#	Technique	Category	Image	Type	PSNR
20	[15]			Grayscale	49.38
21	[16] 1-bit scheme			Color	51.64
22	[16] 2-bit scheme			Color	49.88
23	[21]			Color	40.26
24	[22]	LSB		Color	38.33
25	[23]			Color	45.13
26	[26]			Gray	32.6719
27	[28]		Mandrill	Color	36.3637
28	[29]			Grayscale	41.74
29	[34]			Color	39.573
30	[36]			Color	42.451
31	[37]	MSB		Grayscale	51.1803
32	[39]			Color	53.7882
33	[40]			Color	61.7972
34	StegoBound	LSB		Grayscale	72.439
35	[22]	LSB		Color	41.22
36	[23]		House	Color	46.77
37	StegoBound	LSB		Grayscale	72.552
38	[22]	LSB		Color	41.30
39	[23]		Boat	Color	46.42
40	StegoBound	LSB		Grayscale	64.6688
41	[33]	MSB	Bluehills	Grayscale	41.367
42	StegoBound	LSB		Grayscale	68.047

Table 3 reveals that our proposed StegoBound technique achieves the best PSNR values for the generated stego-images compared to all the techniques.

4.5. Robustness

StegoBound is also strong against statistical strikes and offers better security against steganalysis attacks. By evaluating the means values of the original cover photos and the generated stego-images, as well as through histogram analysis, the security of StegoBound may be verified. Better security is ensured by a little difference in the mean values of the two photos. Table 4 shows the mean values of the original cover images and the stego-images generated utilizing StegoBound.

Table 4 The mean values of StegoBound stego-images and original cover images

S.#	Image	Original Image	Stego Image
1	Lena image	124.0504	124.0502
2	Mandrill image	138.7426	138.7425
3	House image	137.9846	137.9855
4	Bluehills image	124.1266	124.1108
5	Boat image	129.7079	129.7077

The mean values of the stego-images and original images are practically identical and do not differ much, implying that StegoBound delivers greater security, as shown in Table 3. StegoBound is also resistant to histogram steganalysis, as seen in Figs. 1 and 2, where the histograms of the cover picture Lena and the generated stego-image are nearly similar and show no noticeable variations. 6–7

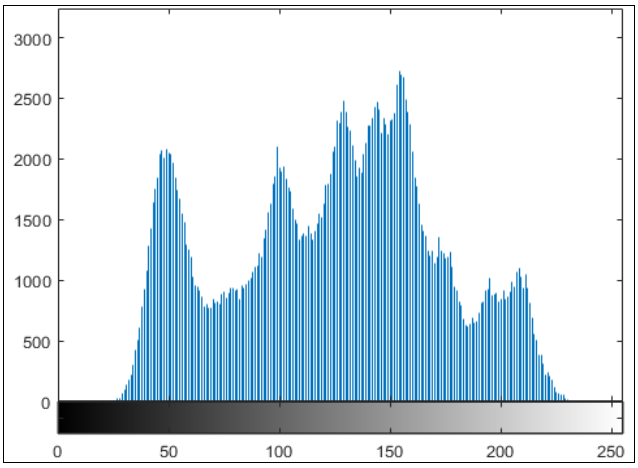

Fig. 6 Histogram of cover image Lena

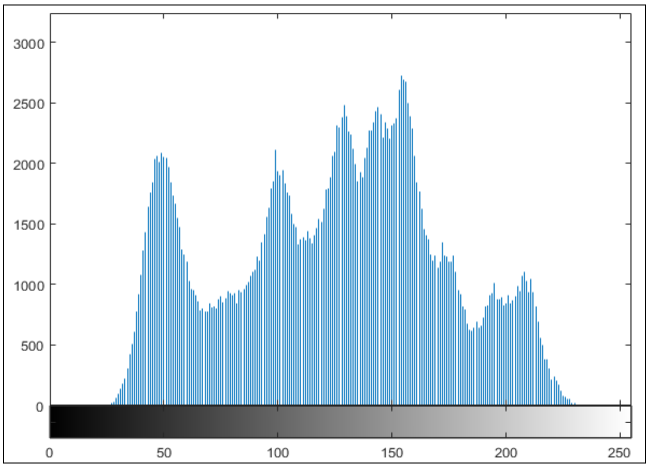

Fig. 6 Histogram of stego image Lena

5. Conclusion and Future Works

We introduced a new steganographic methodology in this study paper. With 3 LSBs, StegoBound used boundary-based LSB replacement to insert the hidden message in the cover image. Our proposed technique achieves an optimal trade-off for the key steganographic parameters. It delivers state-of-the-art results with high imperceptibility, payload capacity, and robustness compared to other existing methods.

In the future, we intend to extend StegoBound for RGB images and explore MSB and hybrid substitution techniques for embedding the secret messages.

References

[1] DULUTA A., MOCANU S., PIETRARU R., MEREZEANU D., and SARU D. Secure Communication Method Based on Encryption and Steganography. *2017 21st International Conference on Control Systems and Computer Science*. Institute of Electrical and Electronics Engineers, Piscataway, USA, 2017: 453-458. https://doi.org/10.1109/CSCS.2017.70

[2] MISHRA R., & BHANODIYA P. A Review on Steganography and Cryptography. *2015 International Conference on Advances in Computer Engineering and Applications*. Institute of Electrical and Electronics Engineers, Piscataway, USA, 2015: 119-122. https://doi.org/10.1109/ICACEA.2015.7164679

[3] CHALLITA K., & FARHAT H. Combining Steganography and Cryptography: New Directions. *International Journal on New Computer Architectures and Their Applications*, 2011, 1: 199-208. http://oaji.net/articles/2015/544-1430753335.pdf

[4] SAJEDI H., & JAMZAD M. Cover Selection Steganography Method Based on Similarity of Image Blocks. *2008 Institute of Electrical and Electronic Engineers 8th International Conference on Computer and Information Technology Workshops*. Institute Of Electrical And Electronics Engineers, Piscataway, USA, 2008: 379-384. https://doi.org/10.1109/CIT.2008.Workshops.34

[5] JOHNSON N. F., DURIC Z., and JAJODIA S. *Information Hiding: Steganography and Watermarking-Attacks and Countermeasures*. Springer Science & Business Media, Berlin, Germany, 2001. https://link.springer.com/book/10.1007/978-1-4615-4375-6

[6] BAILEY K., & CURRAN K. An Evaluation of Image Based Steganography methods. *Multimedia Tools and Applications*, 2006, 30: 55-88. https://doi.org/10.1007/s11042-006-0008-4

[7] WESTFELD A., & PFITZMANN A. Attacks on Steganographic Systems. *International Workshop on Information Hiding*, 1999: 61-76. https://doi.org/10.1007/10719724_5

[8] CHANU Y. J., TUITHUNG T., and SINGH K. M. A Short Survey on Image Steganography and Steganalysis Techniques. *2012 3rd National Conference on Emerging Trends and Applications in Computer Science*. Institute of Electrical And Electronics Engineers, Piscataway, USA, 2012: 52-55. https://doi.org/10.1109/NCETACS.2012.6203297

[9] KAUR S., BANSAL S., and BANSAL R. K. Steganography and Classification of Image Steganography Techniques. *2014 International Conference on Computing for Sustainable Global Development*. Institute of Electrical And Electronics Engineers, Piscataway, USA, 2014: 870-875. https://doi.org/10.1109/IndiaCom.2014.6828087

[10] SHARMA A., PORIYE M., and KUMAR V. A Review of Image Steganography Techniques: Development Trends to Enhance Performance. *International Journal of Advanced Research in Computer Science*, 2017, 8(5): 1852-1855. https://doi.org/10.26483/ijarcs.v8i5.3962

[11] THANGADURAI K., & DEVI G. S. An Analysis of LSB Based Image Steganography Techniques. *2014 International Conference on Computer Communication and Informatics*. Institute of Electrical and Electronics Engineers, Piscataway, USA, 2014: 1-4. https://doi.org/10.1109/ICCCI.2014.6921751

[12] SWAIN G., & LENKA S. K. A Hybrid Approach to Steganography Embedding at Darkest and Brightest Pixels. *2010 International Conference on Communication and Computational Intelligence*. Institute of Electrical and Electronics Engineers, Piscataway, USA, 2010: 529-534. https://ieeexplore.ieee.org/document/5738786

[13] RACHAEL O., MISRA S., AHUJA R., ADEWUMI A., AYENI F., and MMASKELIUNAS R. Image Steganography and Steganalysis Based on Least Significant Bit (LSB). *Proceedings of International Conference on Emerging Trends in Information Technology 2019*. Springer, New-York, USA, 2020: 1100-1111. http://dx.doi.org/10.1007/978-3-030-30577-2_97

[14] GHAZANFARI K., GHAEMMAGHAMI S., and KHOSRAVI S. R. LSB++: an Improvement to LSB+ Steganography. *2011-2011 Instiute of Electrical and Electronic Engineers Region 10 Conference*. Institute Of Electrical And Electronics Engineers, Piscataway, USA, 2011: 364-368. https://doi.org/10.1109/TENCON.2011.6129126

[15] JOSHI K., GILL S., and YADAV R. A New Method of Image Steganography Using 7th bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image. *Journal of Computer Networks and Communications*, 2018, 2018: 1-10. https://doi.org/10.1155/2018/9475142

[16] SWAIN G. Digital Image Steganography Using Variable Length Group of Bits Substitution. *Procedia Computer Science*, 2016, 85: 31-38. https://doi.org/10.1016/j.procs.2016.05.173

[17] HE J., TANG S., and WU T. An Adaptive Image Steganography Based on Depth-Varying Embedding. *2008 Congress on Image and Signal Processing*. Institute Of Electrical And Electronics Engineers, Piscataway, USA, 2008: 660-663. https://doi.org/10.1109/CISP.2008.189

[18] HLAING A. T., & THANT K. M. Color Image Steganography Using Cryptography and Magic LSB Substitution Method. *2018 Joint International Conference on Science, Technology and Innovation*. Mandalay Technological University, Mandalay, Myanmar, 2018. https://www.researchgate.net/publication/334646919_Color_Image_Steganography_using_Cryptography_and_Magic_LSB_Substitution_Method_M-LSB-SM

[19] SWAIN G., & LENKA S. K. A Technique for Secret Communication Using a new Block Cipher with Dynamic Steganography. *International Journal of Security and Its Applications*, 2012, 6: 1-12. http://article.nadiapub.com/IJSIA/vol6_no4/2.pdf

[20] SHARMA V. Two New Approaches for Image Steganography Using Cryptography. *2015 Third International Conference on Image Information Processing*. Institute Of Electrical And Electronics Engineers, Piscataway, USA, 2015: 202-207. https://doi.org/10.1109/ICIIP.2015.7414766

[21] NILIZADEH A., and NILCHI A. R. N. A Novel Steganography Method Based on Matrix Pattern and LSB Algorithms in RGB Images. *2016 1st Conference on Swarm Intelligence and Evolutionary Computation*. Institute Of Electrical And Electronics Engineers, Piscataway, USA, 2016: 154-159. https://doi.org/10.1109/CSIEC.2016.7482107

[22] WU D.-C., & TSAI W.-H. A Steganographic Method for Images by Pixel-Value Differencing. *Pattern Recognition*

Letters, 2003, 24: 1613-1626. https://doi.org/10.1016/S0167-8655(02)00402-6
[23] TSENG H.-W., & LENG H.-S. A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number. *Journal of Applied Mathematics*, 2013, 2013: 1-8. https://doi.org/10.1155/2013/189706
[24] CHANG C.-C., & TSENG H.-W. A Steganographic Method for Digital Images Using Side Match. *Pattern Recognition Letters*, 2004, 25: 1431-1437. https://doi.org/10.1016/j.patrec.2004.05.006
[25] SWAIN G., & LENKA S. K. Steganography Using Two Sided, Three Sided, and Four Sided Side Match Methods. *Computer Society of India Transactions on Information and Communication Technology*, 2013, 1: 127-133. https://doi.org/10.1007/s40012-013-0015-3
[26] MAHJABIN T., HOSSAIN S. M., and HAQUE M. S. A Block Based Data Hiding Method in Images Using Pixel Value Differencing and LSB Substitution Method. *2012 15th International Conference on Computer and Information Technology*. Institute Of Electrical And Electronics Engineers, Piscataway, USA, 2012: 168-172. https://doi.org/10.1109/ICCITECHN.2012.6509770
[27] BASSIL Y. Image Steganography Based on a Parameterized Canny Edge Detection Algorithm. *International Journal of Computer Applications*, 2012, 60(4): 35-40. https://doi.org/10.5120/9682-4112
[28] JUNEJA M., & SANDHU P. S. An Improved LSB Based Steganography Technique for RGB Color Images. *International Journal of Computer and Communication Engineering*, 2013, 2: 513. http://www.ijcce.org/papers/238-W1028.pdf
[29] KAUR A., & KAUR S. Image Steganography Based on Hybrid Edge Detection and 2k Correction Method. *International Journal of Engineering and Innovative Technology*, 2012, 1: 167-170. http://dx.doi.org/10.1063/1.4897776
[30] JOIS A., & TEJASWINI L. Survey on LSB Data Hiding Techniques. *2016 International Conference on Wireless Communications, Signal Processing and Networking*. Institute Of Electrical And Electronics Engineers, Piscataway, USA, 2016: 656-660. https://doi.org/10.1109/WiSPNET.2016.7566214
[31] ASHWIN S., RAMESH J., KUMAR S. A., and GUNAVATHI K. Novel and Secure Encoding and Hiding Techniques Using Image Steganography: A Survey. *2012 International Conference on Emerging Trends in Electrical Engineering and Energy Management*. Institute Of Electrical And Electronics Engineers, Piscataway, USA, 2012: 171-177. https://doi.org/10.1109/ICETEEEM.2012.6494463
[32] GARG M. R. Comparison Of LSB & MSB Based Steganography In Gray-Scale Images. *International Journal of Engineering Research and Technology*, 2012, 1(8): 1-6. https://www.ijert.org/research/comparison-of-lsb-msb-based-steganography-in-gray-scale-images-IJERTV1IS8630.pdf
[33] SATHISHA N., MADHUSUDAN G., BHARATHESH S., BABU K. S., RAJA K., and VENUGOPAL K. Chaos Based Spatial Domain Steganography Using MSB. *2010 5th International Conference on Industrial and Information Systems*. Institute Of Electrical And Electronics Engineers, Piscataway, USA, 2010: 177-182. https://doi.org/10.1109/ICIINFS.2010.5578711
[34] YALMAN Y., AKAR F., and ERTURK I. An Image Interpolation Based Reversible Data Hiding Method Using R-Weighted Coding. *2010 13th Institute of Electrical and Electronics Engineering International Conference on Computational Science and Engineering*. Institute Of Electrical And Electronics Engineers, Piscataway, USA, 2010: 346-350. https://doi.org/10.1109/CSE.2010.52
[35] MANDAL J., & DAS D. Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain. *International Journal of Information Sciences and Techniques*, 2012, 2: 17-24. https://doi.org/10.5121/IJIST.2012.2408
[36] GUPTA P. K., ROY R., and CHANGDER S. A Secure Image Steganography Technique with Moderately Higher Significant Bit Embedding. *2014 International Conference on Computer Communication and Informatics*. Institute Of Electrical And Electronics Engineers, Piscataway, USA, 2014: 1-6. http://dx.doi.org/10.1109/ICCCI.2014.6921726
[37] ISLAM A. U., KHALID F., SHAH M., KHAN Z., MAHMOOD T., KHAN A., MAHMOOD T., KHAN A., ALI U., and NAEEM M. An Improved Image Steganography Technique Based on MSB Using Bit Differencing. *2016 Sixth International Conference on Innovative Computing Technology*. Institute of Electrical And Electronics Engineers, Piscataway, USA, 2016: 265-269. https://doi.org/10.1109/INTECH.2016.7845020
[38] PUTEAUX P., TRINEL D., and PUECH W. High-Capacity Data Hiding in Encrypted Images Using MSB Prediction. *2016 Sixth International Conference on Image Processing Theory, Tools and Applications*. Institute of Electrical and Electronics Engineers, Piscataway, USA, 2016: 1-6. https://doi.org/10.1109/IPTA.2016.7820991
[39] AHMED S., JAFFARI R., and THEBO L. A. Data Hiding Using Green Channel as Pixel Value Indicator. *International Journal of Image Processing*, 2018, 12: 90-100. https://www.cscjournals.org/manuscript/Journals/IJIP/Volume12/Issue3/IJIP-1169.pdf
[40] SHARMA A., PORIYE M., and KUMAR V. A Secure Steganography Technique Using MSB. *International Journal of Emerging Research in Management and Technology*, 2017, 6: 208-214. https://doi.org/10.23956/ijermt.v6i6.270
[41] AKINOLA S. O., & OLATIDOYE A. A. On the Image Quality and Encoding Times of LSB, MSB and Combined LSB-MSB Steganography Algorithms Using Digital Images. *International Journal of Computer Science & Information Technology*, 2015, 7: 79-91. http://dx.doi.org/10.5121/ijcsit.2015.7407
[42] DHANNOON B. N. An Indirect MSB Data Hiding Technique. *Life Science Journal*, 2013, 10: 263-266. http://www.lifesciencesite.com/lsj/life1011s/046_21081life1011s_263_266.pdf
[43] KUMAR M. A., & KAHAR M. Variant of LSB Steganography Algorithm for Hiding Information in RGB Images. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 2017, 10(1): 35-48. http://dx.doi.org/10.14257/ijsip.2017.10.1.05
[44] JAFFARI R., HASHMANI M. A., TAIB H., ABDULLAH N., and RIZVI S. S. H. A Novel Image-Based Framework for Process Monitoring and Fault Diagnosis of Mooring Lines. *Journal of Hunan University Natural Sciences*, 2020, 47(10): 100-114. http://jonuns.com/index.php/journal/article/view/453

参考文:

[1] DULUTA A., MOCANU S., PIETRARU R., MEREZEANU D., 和 SARU D. 基于加密和隐写术的安全通信方法。 2017 年第 21 届控制系统和计算机科学国际会议。美国皮斯卡塔韦电气和电子工程师协会, 2017: 453-458. https://doi.org/10.1109/CSCS.2017.70
[2] MISHRA R., 和 BHANODIYA P. 隐写术和密码学综述。2015年计算机工程与应用进展国际会议。美国皮斯卡塔韦电气和电子工程师协会, 2015: 119-122. https://doi.org/10.1109/ICACEA.2015.7164679
[3] CHALLITA K., 和 FARHAT H. 结合隐写术和密码术：新方向。新计算机体系结构及其应用国际期刊, 2011, 1: 199-208. http://oaji.net/articles/2015/544-1430753335.pdf
[4] SAJEDI H., 和 JAMZAD M. 基于图像块相似度的封面选择隐写方法。 2008 年电气与电子工程师学会第 8 届计算机与信息技术研讨会国际会议。美国皮斯卡塔韦电气和电子工程师协会, 2008: 379-384. https://doi.org/10.1109/CIT.2008.Workshops.34
[5] JOHNSON N. F., DURIC Z., 和 JAJODIA S. 信息隐藏：隐写术和水印 - 攻击和对策。施普林格科学与商业媒体, 柏林, 德国, 2001. https://link.springer.com/book/10.1007/978-1-4615-4375-6
[6] BAILEY K., 和 CURRAN K. 基于图像的隐写术方法的评估. 多媒体工具和应用程序, 2006, 30: 55-88. https://doi.org/10.1007/s11042-006-0008-4
[7] WESTFELD A., 和 PFITZMANN A. 对隐写系统的攻击。信息隐藏国际研讨会, 1999: 61-76. https://doi.org/10.1007/10719724_5
[8] CHANU Y. J., TUITHUNG T., 和 SINGH K. M. 关于图像隐写术和隐写分析技术的简短调查。2012第三届全国计算机科学新兴趋势和应用会议。美国皮斯卡塔韦电气和电子工程师协会, 2012: 52-55. https://doi.org/10.1109/NCETACS.2012.6203297
[9] KAUR S., BANSAL S., 和 BANSAL R. K. 图像隐写技术的隐写术和分类。2014计算促进全球可持续发展国际会议. 美国皮斯卡塔韦电气和电子工程师协会, 2014: 870-875. https://doi.org/10.1109/IndiaCom.2014.6828087
[10] SHARMA A., PORIYE M., 和 KUMAR V. 图像隐写技术回顾：提高性能的发展趋势。国际计算机科学高级研究杂志, 2017, 8(5): 1852-1855. https://doi.org/10.26483/ijarcs.v8i5.3962
[11] THANGADURAI K., 和 DEVI G. S. 基于最小二乘位的图像隐写技术分析。2014年计算机通信和信息学国际会议。电气和电子工程师学院，皮斯卡塔韦，美国, 2014: 1-4. https://doi.org/10.1109/ICCCI.2014.6921751
[12] SWAIN G., 和 LENKA S. K. 在最暗和最亮像素处嵌入隐写术的混合方法。2010年国际通信和计算智能会议。电气和电子工程师学院，皮斯卡塔韦，美国, 2010: 529-534. https://ieeexplore.ieee.org/document/5738786
[13] RACHAEL O., MISRA S., AHUJA R., ADEWUMI A., AYENI F., 和 MMASKELIUNAS R. 基于最低有效位的图像隐写术和隐写分析。2019年信息技术新兴趋势国际会议论文集。美国纽约施普林格, 2020: 1100-1111. http://dx.doi.org/10.1007/978-3-030-30577-2_97
[14] GHAZANFARI K., GHAEMMAGHAMI S., 和 KHOSRAVI S. R. 最低有效位++：对最低有效位+隐写术的改进。2011-2011电气和电子工程师学会区域10会议。电气和电子工程师学院，皮斯卡塔韦，美国, 2011: 364-368. https://doi.org/10.1109/TENCON.2011.6129126
[15] JOSHI K., GILL S., 和 YADAV R. 通过在灰度图像中引入连续临时像素，以像素的第7位作为指示符的图像隐写术新方法。计算机网络与通信杂志, 2018, 2018: 1-10. https://doi.org/10.1155/2018/9475142
[16] SWAIN G. 使用可变长度位替换组的数字图像隐写术。普罗西迪亚计算机科学, 2016, 85: 31-38. https://doi.org/10.1016/j.procs.2016.05.173
[17] HE J., TANG S., 和 WU T. 基于深度变化嵌入的自适应图像隐写术。2008年图像和信号处理大会。电气和电子工程师学院，皮斯卡塔韦，美国, 2008: 660-663. https://doi.org/10.1109/CISP.2008.189
[18] HLAING A. T., 和 THANT K. M. 使用密码学和魔术最低有效位替换方法的彩色图像隐写术。2018年科学、技术与创新联合国际会议。曼德勒科技大学，曼德勒，缅甸, 2018. https://www.researchgate.net/publication/334646919_Color_Image_Steganography_using_Cryptography_and_Magic_LSB_Substitution_Method_M-LSB-SM
[19] SWAIN G., 和 LENKA S. K. 使用具有动态隐写术的新块密码进行秘密通信的技术。国际安全杂志及其应用, 2012, 6: 1-12. http://article.nadiapub.com/IJSIA/vol6_no4/2.pdf
[20] SHARMA V. 两种使用密码学的图像隐写术新方法。2015第三届图像信息处理国际会议。电气和电子工程师学院，皮斯卡塔韦，美国, 2015: 202-207. https://doi.org/10.1109/ICIIP.2015.7414766
[21] NILIZADEH A., 和 NILCHI A. R. N. 一种基于矩阵模式和红绿蓝图像中最低有效位算法的新型隐写术方法。2016年第一届群体智能与进化计算会议. 电气和电子工程师学院，皮斯卡塔韦，美国, 2016: 154-159. https://doi.org/10.1109/CSIEC.2016.7482107
[22] WU D.-C., 和 TSAI W.-H. 通过像素值差分的图像隐写方法。模式识别字母, 2003, 24: 1613-1626. https://doi.org/10.1016/S0167-8655(02)00402-6
[23] TSENG H.-W., 和 LENG H.-S. 基于像素值差分和完全平方数的隐写方法。应用数学杂志, 2013, 2013: 1-8. https://doi.org/10.1155/2013/189706
[24] CHANG C.-C., 和 TSENG H.-W. 使用侧面匹配的数字图像隐写方法。模式识别字母, 2004, 25: 1431-1437. https://doi.org/10.1016/j.patrec.2004.05.006
[25] SWAIN G., 和 LENKA S. K. 使用双面、三面和四面匹配方法的隐写术。印度计算机学会信息和通信技术交易, 2013, 1: 127-133. https://doi.org/10.1007/s40012-013-0015-3

[26] MAHJABIN T., HOSSAIN S. M., 和 HAQUE M. S. 使用像素值差异和最低有效位替换方法的图像中基于块的数据隐藏方法。2012年第15届计算机与信息技术国际会议。电气和电子工程师学院，皮斯卡塔韦，美国, 2012: 168-172. https://doi.org/10.1109/ICCITECHN.2012.6509770

[27] BASSIL Y. 基于参数化精明边缘检测算法的图像隐写术。国际计算机应用杂志, 2012, 60(4): 35-40. https://doi.org/10.5120/9682-4112

[28] JUNEJA M., 和 SANDHU P. S. 一种改进的基于最低有效位的红绿蓝彩色图像隐写技术。国际计算机与通信工程杂志, 2013, 2: 513. http://www.ijcce.org/papers/238-W1028.pdf

[29] KAUR A., 和 KAUR S. 基于混合边缘检测和两千校正方法的图像隐写术。国际工程与创新技术杂志, 2012, 1: 167-170. http://dx.doi.org/10.1063/1.4897776

[30] JOIS A., 和 TEJASWINI L. 最低有效位数据隐藏技术调查。2016年无线通信、信号处理和网络国际会议。电气和电子工程师学院，皮斯卡塔韦，美国, 2016: 656-660. https://doi.org/10.1109/WiSPNET.2016.7566214

[31] ASHWIN S., RAMESH J., KUMAR S. A., 和 GUNAVATHI K. 使用图像隐写术的新型安全编码和隐藏技术：一项调查。2012年电气工程和能源管理新趋势国际会议。电气和电子工程师学院，皮斯卡塔韦，美国, 2012: 171-177. https://doi.org/10.1109/ICETEEEM.2012.6494463

[32] GARG M. R. 灰度图像中最低有效位和基于最高有效位的隐写术的比较。国际工程研究与技术杂志, 2012, 1(8): 1-6. https://www.ijert.org/research/comparison-of-lsb-msb-based-steganography-in-gray-scale-images-IJERTV1IS8630.pdf

[33] SATHISHA N., MADHUSUDAN G., BHARATHESH S., BABU K. S., RAJA K., 和 VENUGOPAL K. 使用最重要比特的基于混沌的空间域隐写术. 2010 第五届工业和信息系统国际会议。电气和电子工程师学院，皮斯卡塔韦，美国, 2010: 177-182. https://doi.org/10.1109/ICIINFS.2010.5578711

[34] YALMAN Y., AKAR F., 和 ERTURK I. 一种基于图像插值的可逆数据隐藏方法，使用日加权编码。2010年第13届电气与电子工程研究所计算科学与工程国际会议。电气和电子工程师学院，皮斯卡塔韦，美国, 2010: 346-350. https://doi.org/10.1109/CSE.2010.52

[35] MANDAL J., 和 DAS D. 基于空间域像素值差异的彩色图像隐写术。国际信息科学与技术杂志, 2012, 2: 17-24. https://doi.org/10.5121/IJIST.2012.2408

[36] GUPTA P. K., ROY R., 和 CHANGDER S. 具有中等高有效位嵌入的安全图像隐写技术。2014年计算机通信和信息学国际会议。电气和电子工程师学院，皮斯卡塔韦，美国, 2014: 1-6. http://dx.doi.org/10.1109/ICCCI.2014.6921726

[37] ISLAM A. U., KHALID F., SHAH M., KHAN Z., MAHMOOD T., KHAN A., MAHMOOD T., KHAN A., ALI U., 和 NAEEM M. 基于使用位差分的最高有效位的改进图像隐写技术。2016第六届创新计算技术国际会议。电气和电子工程师学院，皮斯卡塔韦，美国, 2016: 265-269. https://doi.org/10.1109/INTECH.2016.7845020

[38] PUTEAUX P., TRINEL D., 和 PUECH W. 使用最高有效位预测隐藏在加密图像中的高容量数据。2016第六届图像处理理论、工具和应用国际会议。电气和电子工程师学院，皮斯卡塔韦，美国, 2016: 1-6. https://doi.org/10.1109/IPTA.2016.7820991

[39] AHMED S., JAFFARI R., 和 THEBO L. A. 使用绿色通道作为像素值指示器的数据隐藏。国际图像处理杂志, 2018, 12: 90-100. https://www.cscjournals.org/manuscript/Journals/IJIP/Volume12/Issue3/IJIP-1169.pdf

[40] SHARMA A., PORIYE M., 和 KUMAR V. 使用最高有效位的安全隐写技术。国际管理与技术新兴研究杂志, 2017, 6: 208-214. https://doi.org/10.23956/ijermt.v6i6.270

[41] AKINOLA S. O., 和 OLATIDOYE A. A. 使用数字图像的最低有效位、最高有效位和组合最低有效位-最高有效位隐写算法的图像质量和编码时间。国际计算机科学与信息技术杂志, 2015, 7: 79-91. http://dx.doi.org/10.5121/ijcsit.2015.7407

[42] DHANNOON B. N. 间接最高有效位数据隐藏技术。生命科学杂志, 2013, 10: 263-266. http://www.lifesciencesite.com/lsj/life1011s/046_21081life1011s_263_266.pdf

[43] KUMAR M. A., 和 KAHAR M. 用于在右绿蓝图像中隐藏信息的最低有效位隐写算法的变体。国际信号处理、图像处理和模式识别杂志, 2017, 10(1): 35-48. http://dx.doi.org/10.14257/ijsip.2017.10.1.05

[44] JAFFARI R., HASHMANI M. A., TAIB H., ABDULLAH N., 和 RIZVI S. S. H. 一种新型的基于图像的系泊缆过程监控和故障诊断框架。湖南大学自然科学学报, 2020, 47(10): 100-114. http://jonuns.com/index.php/journal/article/view/453