

Performance of Logarithmic Magnitude of Centre-Element-Based Steganography over OFDM constituted Wireless Communication Channel

Mukund D. Maid¹, Pratik R. Hajare²

¹PhD Scholar, Mansarovar Global University, Bhopal, Madhya Pradesh

²Professor, Mansarovar Global University, Bhopal, Madhya Pradesh
mukundmaid@gmail.com¹, pratikhajare8@gmail.com²

Article History:

Received: 29-07-2024

Revised: 20-09-2024

Accepted: 01-10-2024

Abstract:

Hiding crucial information is today's utmost concern and transmitting through wired or wireless medium is another attentive subject. Quality secret hiding requires robustness and better perceptual visuals of the host image. Also, a secret embedding mechanism should offer higher immunity to noises. The work proposes a robust and efficient patch-based secured steganography (P-BSS) mechanism. The stego image is transmitted over an orthogonal frequency division multiplexing (OFDM) based Wireless Communication system governed by 802.11 WLAN. The steganography framework uses center element (CE) information to embed secret bits in its 3x3 neighborhood. The strategy is based on the magnitude and natural logarithm of the center element. The statistical operation on the center element defines the position in the neighborhood from where the embedding process should be initiated. The secret binary information is then hidden using the LSB embedding approach. The stego image when transmitted over a Binary phase shift keying (BPSK) modulated OFDM wireless communication system, the stego image was immune to Additive White Gaussian Noise (AWGN) above 10 dB. The proposed logarithmic magnitude of the center-element-based steganography (LM-CEB-S) framework maintains a proper balance between imperceptibility and security.

Keywords: *Patch-based secured steganography, stego image, orthogonal frequency division multiplexing, center element, natural logarithm, LSB embedding, BPSK, AWGN.*

1. Introduction

The privacy and security of crucial information are concerns with increasing data transmission over the internet. This has been a crucial issue as far as intruders are concerned [1]. Unseen and unknown parties attack the sender's information by several means, possibly leading to malicious threats and activities, and eavesdropping [2]. The most commonly used techniques to prevent such malicious attacks include watermarking, steganography, and cryptography schemes. These are commonly adopted by many researchers to ensure security and privacy [3]. Watermarks are visually perceived, and secret information changes in cryptography. However, Steganography hides the secret details within the host using a key at the sender end. Due to this steganography is preferred over watermarking and cryptography. The host medium can include an image, a voice signal, a video sequence, or a protocol. A common code is used to encode secret information at the transmitter and the receiver in case of cryptography. Whereas, watermarking offers confidentiality by sending the secret details using host data [4].

The significant part that provided the steganography upper hand over the other two approaches is its large data embedding capacity and easier data embedding process. Also, it offers better resistance to an intruder to notice the hidden information [5]. However, due to the high volume of data, there is a trade-off between payload, imperceptibility, and security. It implies that an increase in data would decrease the level of security and vice versa. Besides this, an increase in secret information gradually decreases the imperceptibility [6]. Therefore, the objective concerned in steganography is to hide secret information, preserve the perceptual quality, and make it difficult for an intruder to extract the secret details. Also, the approach used should be cost-effective and robust to prevent loss of information against deterioration. The challenge is to incorporate better mathematical modeling for embedding secret bits that will offer minimum contamination and provide a lossless de-embedding process.

The article's contribution can be summarized as follows:

1. A secured data embedding technique LM-CEB-S using LSB embedding is introduced which offers higher security and imperceptibility.
2. The secret byte is embedded in the host image patch which is governed by the logarithmic magnitude of the center-element. The magnitude value defines the initial embedding position in the patch neighborhood for clockwise embedding.
3. The performance of the steganography mechanism is evaluated using a BPSK-OFDM-based wireless communication system
4. The proposed LM-CEB-S offers a higher peak signal-to-noise ratio and structural similarity.

2. Related Work

Several methodologies have been suggested to compensate for these challenges and maintain proper trade-offs between parameters. Work introduced in [7-8] uses the efficient LSB-embedding technique where LSB with certain encryption methods was used. Authors in [9] partitioned the host image into two regions based on texture analysis. They named them sensitive and non-sensitive regions. The latter regions were used to cover the majority of secret information while the former region was used to hide remaining secret details. Their adaptive LSB embedding approach [9] achieved a high payload and provided better imperceptibility. The work suggested in [10] used LSB and the secret key and processed using Ex-OR operation. The key was converted to a single-row vector and Ex-OR-ed with the secret information. The embedding was performed using a single LSB and 3-LSB on color and grayscale images. A minimum cost and storage scheme offering higher visual security was introduced in [11]. A sparse matrix was generated using wavelet transform over the image. Further, it was encrypted with a scrambling mechanism and a cipher image was obtained through compression and quantification. A PNG (portable network graphics) image alpha channel was then used to convert the cipher to a stego image.

A randomly selected channel from a color image was used to hide secret bits in [12]. The host bits were selected using a logistic map and conducted experiments over ten different images. They claimed that their scheme offered higher security regarding attacks. A two-level security mechanism was incorporated in [13]. The AES algorithm was to encrypt the secret key and later the encrypted message was down sampled using Huffman coding. High capacity and imperceptibility were the objectives of the work in [14] where the authors used LZW coding to compress the message information. The compressed info bits were then embedded on the edges of the host image. Since the edge pixel spatial

coordinates keep varying as a function of the host image, the embedding host pixel locations were kept in a separate file which was processed by the receiver.

LSB embedding schemes suffer from payload capacity problems. Advanced research as per the literature concentrated on mitigating the payload problem using Deep-Learning and Artificial Intelligence. General Adversarial Networks (GAN) introduced in [15] comprises two networks including the generator followed by a discriminator. The use of GAN in steganography was to enhance the payload capacity of the host image. The result obtained using the GAN generator network for the data input was approximately equal to the source image. This way ensured 1:1 bit capacity during the embedding process at the cost of computational complexity. The class of the resultant images was determined by the discriminator network. But, the cost of training before steganography proved to be a curse. The training process was simplified in [16-17] which was based on DCGAN similar to the work suggested in [18-19]. The steganography GAN consists of 4-fractional convolutional layers followed by a functional layer. This increased the prediction complexity due to the dependency of the network on eavesdropping on the generator. For the improvement, S-GAN was introduced to a low-complexity network with 3 layers. Using pixel-based segmentation, they succeeded in reducing the process complexity at the cost of increased network losses.

As an extension to watermarking, the authors in [20] incorporated phase drift-based drift correction in PSK or QAM in the dirty constellation. For wireless covert channel. Using discrete wavelet and cosine transforms, a secret image was hidden in the color and intensity part of the host image [21]. An algorithm with higher tolerance to channel behavior called chaotic Baker map was used for encryption. The performance of the steganography system was evaluated using an OFDM-based channel equalization system.

3. Method & Material

The proposed LM-CEB-S framework holds a capacity to embed 9:1 bytes (cover: secret). The secret image is resized to a dimension that is $1/3^{\text{rd}}$ of the carrier image. The dimensions of the secret image are ensured either by resizing the image or by adding or deleting extreme rows and columns from the cover image. A bilinear interpolation is used to resize the secret image which is governed by the following expressions (1) and (2).

If C represents the host image and S represents the secret image,

$$C \rightarrow \left\lfloor \frac{r}{3} \right\rfloor \text{ and } \left\lfloor \frac{c}{3} \right\rfloor = 0 \quad (1)$$

Where, $\left\lfloor \frac{x}{y} \right\rfloor$ is the modulus operator, r and c are the height and width dimension parameters of the host image.

$$S \rightarrow \left\lfloor \frac{R}{r} \right\rfloor \text{ and } \left\lfloor \frac{C}{c} \right\rfloor = 0 \quad (2)$$

Where R and C are the height and width dimension parameters of the secret image.

For embedding a byte in a patch of the cover image, LM-CEB-S considers the center element (C_E) as a significant element in the 3x3 patch for finding the right byte to start the LSB embedding. To find the initial index in the 8-element neighborhood around the (C_E), the natural logarithmic value of the C_E is computed. Since the neighborhood has 8 elements, the maximum value of C_E is 255 (for intensity image). A 3x3 patch is shown in the Figure 1 below. The center element value and the values in its

neighborhood are shown. The number sequence outside the 3x3 patch denotes the normal sequence of embedding secret bits of the secret byte in the clockwise direction. That is, if the center element value is 0, the embedding follows the sequence to embed the secret bits with LSB first. However, if the center element takes any different value in the range [0 255], the initial index of embedding is calculated using the following expression (3).

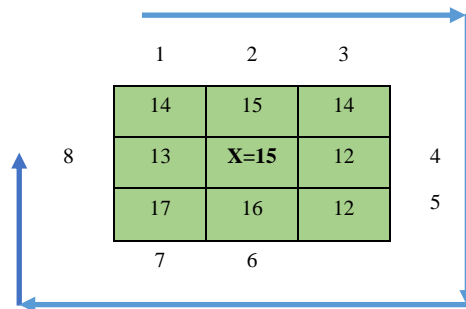


Figure 1 – 3x3 block from the patch image

$$\text{Starting Embedding Index } (I) = \text{round} \left(\frac{\log C_E}{\log 2} \right) \tag{3}$$

From Figure 1, $C_E = 15$, therefore $I = 3.906 \approx 4$. Therefore, the embedding of the LSB bit starts at index 4 and continues in the clockwise direction. The D_0 bit of the secret bit will be placed in the neighborhood byte at index 4, D_1 at index 5, D_2 at index 6, D_3 at index 7, D_4 at index 8, D_5 at index 1, and so on. The maximum value that C_E can hold for an intensity image is 255. In that case, the value of $I = 7.994 \approx 8$ which means the LSB (D_0) bit will be placed in the byte at index 8, D_1 at index 1, D_2 at index 3, and so on. Thus, the initial index is the function of the center element value. However, the rounding operation in expression (3) leads to an overlapping initial index. For $C_E = 0$ and 1, the value of I was set to 1 to avoid invalid inputs. For the remaining values of C_E from 2 to 255, the starting index takes the computed values using expression (3). To compensate for the invalid inputs, expression (3) is modified to expression (4) as:

$$I = \begin{cases} 1 & C_E == 0 \\ 1 & C_E == 1 \\ \text{round} \left(\frac{\log C_E}{\log 2} \right) & \text{otherwise} \end{cases} \tag{4}$$

Table 1 below indicates the value of C_E and the separation distance between values of C_E and cluster members. It is seen that the separation for lower values is small concerning higher values. For the first three values (0-2), the starting index is at index 1, for 3-5 the starting index is 2, and so on. The analysis regarding the cluster members based on C_E concludes that any drift in the values in the lower range would cause misdetection of the starting index. A small distortion in C_E would shift the starting index resulting in a wrong representation of the transmitted or embedded byte. The range of values that can cause such wrong representation is 0-11. Therefore, high-contrast host images will provide better immunity against unwanted attacks.

The value of C_E in each patch remains unchanged during the embedding operation and considering the change in the LSB bit of every neighborhood byte of the host image due to the secret bit, the perceptual quality remains unaffected mostly. That is, if 50% LSB of host bytes are modified, the imperceptibility would be more than 50% adding the no effect of C_E . The following Figure 2 shows how the bits are

covered in the host image 3x3 patch. The bytes in the neighborhood are represented by N_x . The secret byte is given by ‘s’.

Table 1 – Value of C_E , starting index, and separating distance.

C_E	Starting Index	Cluster members
0-2	1	3
3-5	2	3
6-11	3	5
12-22	4	11
23-45	5	23
46-90	6	45
91-181	7	91
182-255	8	74

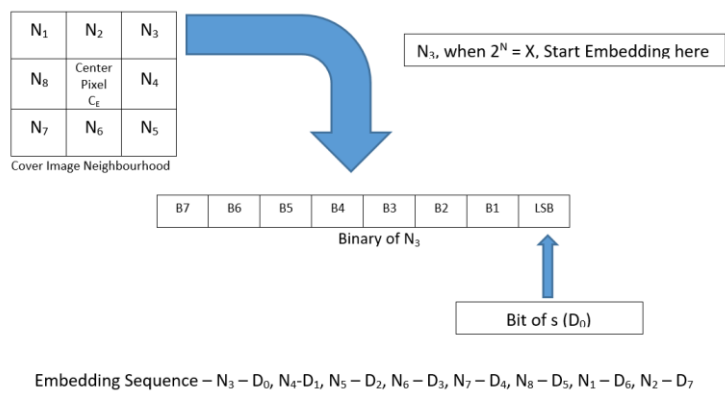


Figure 2 – The LM-CEB-S Embedding scheme

The computational complexity of the embedding mechanism is low since the process involves a division operation followed by a round-off operation. However, converting bytes from decimal to binary and back consumes time. The flowchart for the LM-CEB-S scheme is shown in Figure 3. It shows the covering mechanism of a byte in the 3x3 host patch. Figures 4 and 5 show the results of the LM-CEB-S scheme on images obtained from the IndoorCVPR_09 dataset [22]. Figure 4 depicts the host image, the secret image, and the stego image using the proposed LM-CEB-S embedding scheme. The peak signal-to-noise ratio (PSNR) between host image C and secret image S is 51.6630. The value of PSNR will always be greater than 50 as discussed earlier. Figure 6 shows the recovered image by de-embedding the secret image from the cover image. The PSNR is infinite, which means that the recovered secret image and the original secret image are similar. The complete time required from resizing operation to de-embedding is 0.381 seconds. The original dimensions of both images are 198 x 280 x 3. All the secret frames (RGB) are embedded in the respective frames of the modulating image.

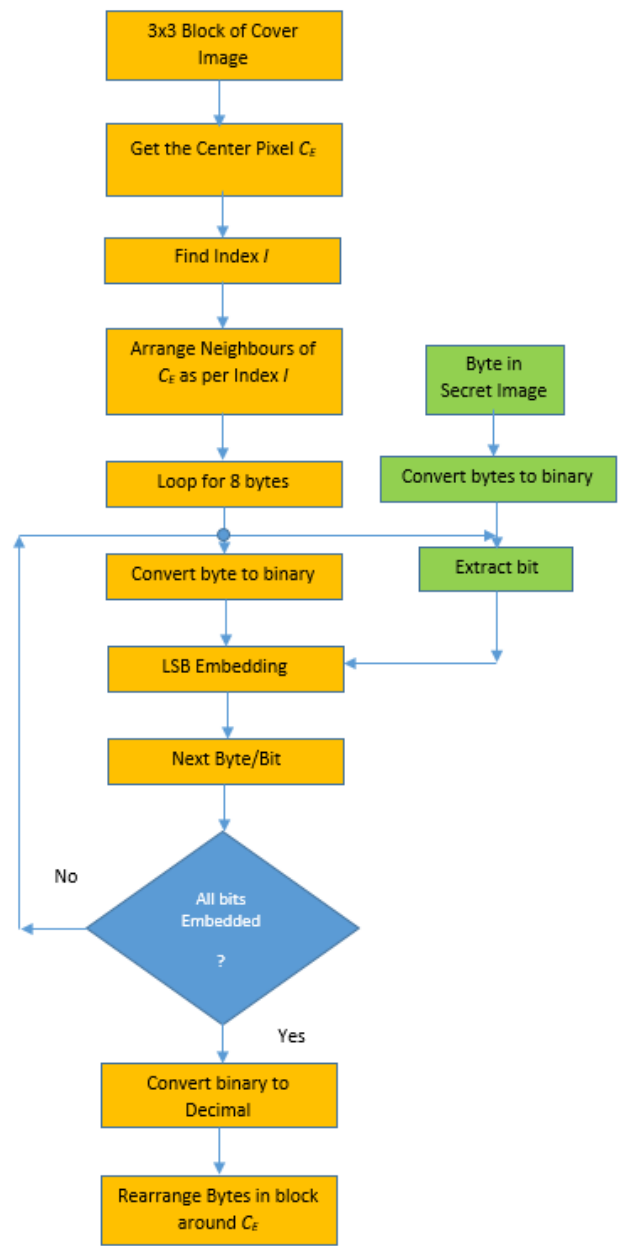


Figure 3 – The LM-CEB-S Embedding scheme



Figure 4 – Cover image, secret image, and stego image (IndoorCVPR_09 dataset). PSNR (C-S) = 51.6630.



Figure 5 – The recovered secret image. PSNR (S-Stego) = Inf. Time Elapsed = 0.381 seconds)

Visual perception of the cover image and the stego image in Figure 4 shows that the imperceptibility is high. The stego image shows no perceptible distortion concerning the modulating image.

The robustness of the LM-CEB-S scheme is verified by transmitting the stego image over AWGN constituted wireless channel. The work uses the 802.11a WLAN model [23] and was designed in MATLAB 2021b. The model was designed with 24-bit binary input, BPSK modulation, 48 to 53-bit OFDM including 5 pilots, 16 guard band symbols, and an 80-bit transmission signal. Table 2 shows the parameters related to the OFDM-based WLAN system. The stego image is partitioned in 3-byte blocks and passed to the wireless system. The signal-to-noise ratio (SNR) parameter of the AWGN block in Simulink is varied from 0 to 15dB and PSNR and structural similarity (Ssim) are computed over the complete secret and recovered secret image. Figure 6 depicts the process of transmitting stego bytes over the communication system. The values of xx and yy in Figure 6 are compared to compute the PSNR and Ssim parameters.

Table 2 – Wireless System Model Parameters

<i>Description</i>	Value
<i>Wireless Model</i>	802.11a WLAN
<i>Convolutional Encoder</i>	poly2trellis(7, [171 133])
<i>Code Rate</i>	0.5
<i>Puncture Vector</i>	[1 1 1 1 1 1 1]
<i>Matrix Interleaver</i>	Rows=6, columns=8
<i>Gain</i>	1/sqrt(10)
<i>Pilots (bits)</i>	4
<i>Zero Padding (bits)</i>	11
<i>Cyclic Prefix (bits)</i>	16
<i>Input</i>	24 bits
<i>Input signal power, referenced to 1 ohm (watts) (AWGN)</i>	0.01
<i>Data Rate</i>	6 Mbps

The MATLAB Simulink block schematic diagram for Figure 6 is shown in Figure 7. The embedding and de-embedding processes are developed using MATLAB scripts. After the stego image generation, the 3-byte binary input to the Simulink is obtained in the workspace. The Simulink model is then called the value of xx. The SNR parameter is passed from the workspace and the corresponding bit error rate (BER) is saved to the workspace from the error rate calculation block.

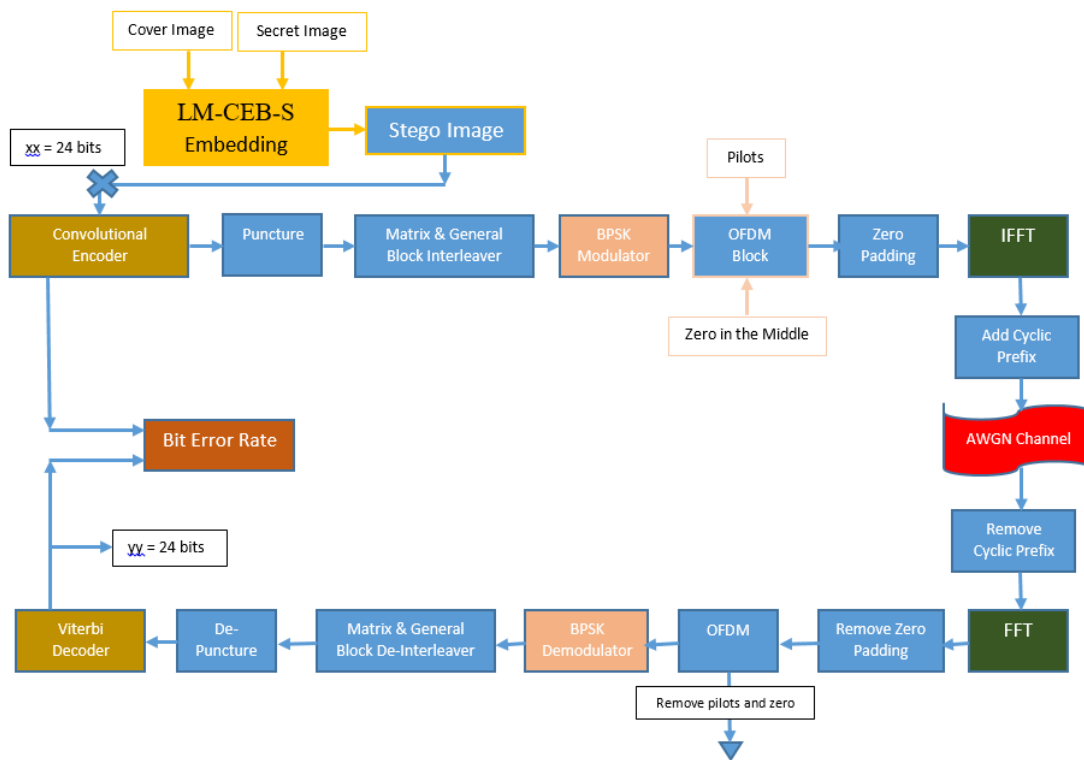


Figure 6 – Transmission of stego image over a wireless system with AWGN attack.

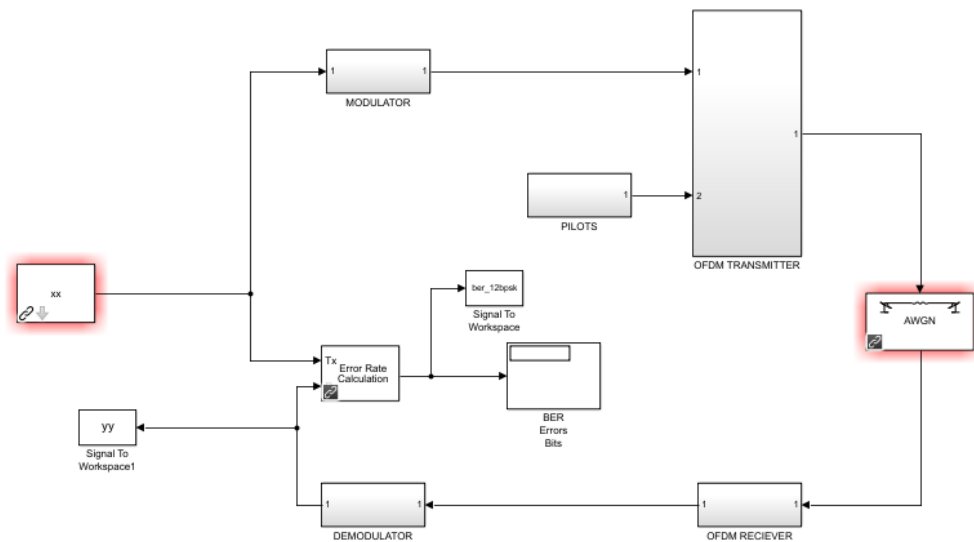


Figure 7 – Actual implementation of Wireless Model in Simulink.

4. Results & Discussion

The proposed LM-CEB-S scheme was tested using different sets of images from various benchmark datasets. The datasets include images from Places365 [24], BDD100k [25], LabelMe [26], and KITTI [27]. We have used the cover image from the Places365 dataset and secret images from all four datasets. Figures 8 and 9 show the results obtained when the stego was passed over the channel. To

reduce the complexity of the time, we have reduced the dimensions of the modulating image and the secret image. A dimension of 150x210 was considered for the carrier image, and the secret image was adjusted to 50x70. The illumination and contents of the host and secret image showed no effect on the PSNR value. In all the cases, the value of PSNR was above 50. The scheme showed better robustness in higher values of C_E . The values of PSNR for different host and secret images are shown in Table 3.

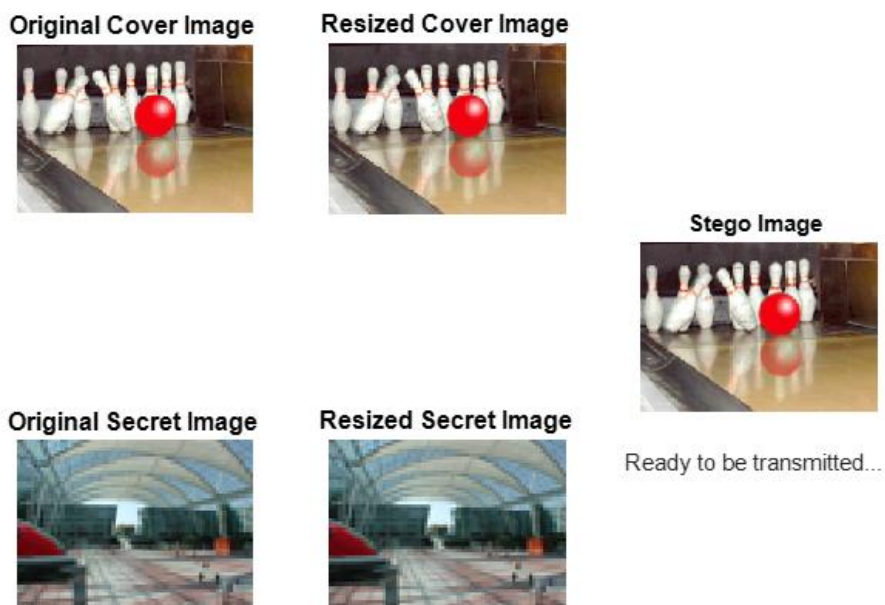


Figure 8 – The carrier image and its resized version. Secret image and its reduced version. Resultant stego image using LM-CEB-S.



Figure 9 – Received Stego image at SNR=12. Extracted secret image without loss.

Table 3 – PSNR values for different host images and secret images.

Cover/SI	KITTI	BDD100K	LabelMe	Places365	Places365
Places365	51.6324	51.6437	51.6348	51.3245	51.6488
Places365	51.6561	51.6803	51.6618	51.6606	51.6309
Places365	51.6314	51.6930	51.6440	51.6802	51.6525
Places365	51.6553	51.6534	51.6554	51.6477	51.6737
Places365	51.6591	51.6669	51.6646	51.6339	51.6702

The influence of SNR values on the stego is shown in Figures 10 to 13. The quality of the recovered image depends on the level of distortion added to the stego image. At lower values of SNR, the distortion is high, which significantly affects the center element; therefore, the received stego image is highly distorted. At higher SNR values, the noise added is low, only the low-illuminated center pixels are affected thereby causing minimum harm. As the SNR value approaches 12, the stego can be recovered without any distortion as seen from Figures 10 to 13 and Figure 9.



Figure 10 - Secret image at SNR=10

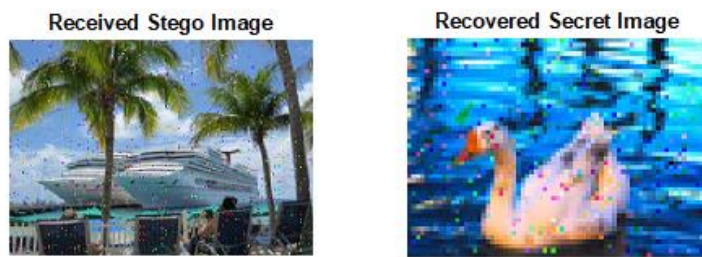


Figure 11 – Secret image at SNR=8

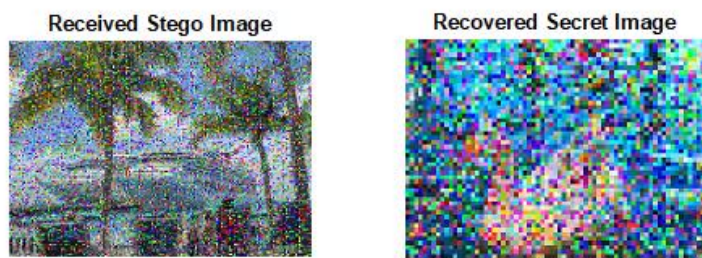


Figure 12 – Secret image at SNR=6

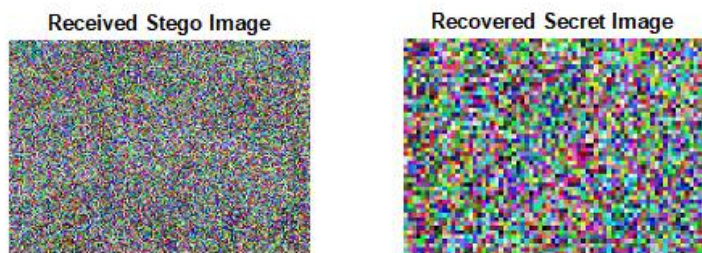


Figure 13 – Secret image at SNR=4

Table 4 lists the values of MSE, PSNR, and Ssim for cover and secret images (considered in Figure 10-13). At 10 dB, the value of MSE=0, PSNR=infinite, and the Ssim=1. The stego image is recovered at the receiver without loss. The performance is not shown for SNR values below 4 dB since the recovered stego image is completely deteriorated.

Table 4 – Performance parameters for different cover and secret images

SNR-dB	MSE	PSNR	Ssim
12	0	-	1
10	0	-	1
8	372.5	22.42	0.94298
6	5590.1	10.67	0.46739

4	11588.6	7.50	0.06357
---	---------	------	---------

We evaluated the performance of our proposed system for code rates $\frac{1}{2}$ and $\frac{3}{4}$ using the BPSK modulation. It was seen that the BER approaches zero value at 12 dB for $\frac{1}{2}$ and at 15 dB for $\frac{3}{4}$ code rate value. The performance of BER versus SNR is shown in Figure 14 for both the configurations related to code rate. The graph indicates that the BPSK with $\frac{1}{2}$ code rate is superior as compared to BPSK at $\frac{3}{4}$ code rate for the stego image.

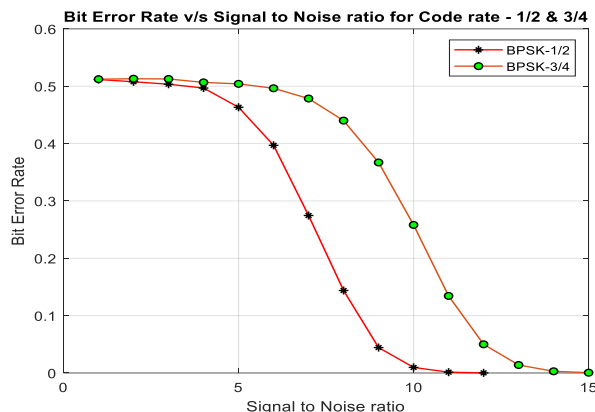


Figure 14 –Performance of LM-CEB-S using BPSK Modulation at Code Rate – $\frac{1}{2}$ and $\frac{3}{4}$.

We compared the performance of our LM-CEB-S scheme with other competing methods relating to MSE, PSNR, and Ssim. Table 5 shows the comparison between all the seven other methods and the LM-CEB-S scheme. The MSE and Ssim are better in the case of the method suggested by Hameed et al. PSNR is better for the technique introduced by Hacimurtazaoglu and Tutuncu. However, there is a trade-off between the former two values and the PSNR. Also, different researchers used different approaches regarding capacity, host and secret images, number and position of bits to be replaced in the host byte, etc. The proposed work maintains a balance between especially the PSNR and Ssim.

Table 5 – Comparison of LM-CEB-S scheme with other competing techniques.

Reference	MSE	PSNR	Ssim
Jebur et al. [28]	3.47	42.75	-
Jebur et al. [28]	27.21	29.28	-
Hameed et al. [29]	0.0149	-	1
Eyssa et al. [30]	-	40.4615	-
Hacimurtazaoglu H. et al. [31]	0.24	54.76	0.998675
Nilizadeh et al. [32]	-	54.00	-
Huang et al. [33]	-	36.60	0.94
Proposed LM-CEB-S Embedding	0.44	51.67	0.99956

5. Conclusion

The work introduced in this article proposes an LSB-embedding scheme that relies on the magnitude of the C_E . The division operation value of C_E determines the starting index of the embedding in the 3×3 neighbourhood of a patch window. The 9:1 embedding scheme produces a stego image with a higher PSNR value and imperceptibility. The stego image can withstand above 10dB of AWGN when transmitted over the communication channel with $\frac{1}{2}$ code rate and 15 dB for $\frac{3}{4}$ code rate using the BPSK modulation. The proposed stego approach showed similar performance for cross-dataset images with higher PSNR and Ssim. The scheme provides a no-key embedding mechanism and higher security.

The proposed scheme uses a round-off operation for logarithmic division operation to find the starting index of LSB embedding. The round-off values cover a range of pixel values in the same range. As a

result, the low-intensity pixel values are finely separated from other clusters. The low distance separation between two clusters can be affected by noise causing false recovery of the initial starting index. On the other hand, higher clusters include a wide range of pixel intensities to result in the same initial starting index.

The future work includes improving the lower range separation distance and increasing clusters in the higher range. The scheme can be evaluated for other modulations such as QAM.

6. References

- [1] S. Dhawan, C. Chakraborty, J. Frnda, R. Gupta, A. K. Rana, and S. K. Pani, "SSII: secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT," *IEEE Access*, vol. 9, pp. 87563-87578, 2021.
- [2] Taha, Mustafa Sabah, et al. "High payload image steganography scheme with minimum distortion based on distinction grade value method." *Multimedia Tools and Applications* (2022): 1-34.
- [3] X. Duan et al., "High-capacity image steganography based on improved FC-DenseNet," *IEEE Access*, vol. 8, pp. 170174-170182, 2020.
- [4] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed, and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," *Journal of Systems Engineering and Electronics*, vol. 29, no. 3, pp. 639-649, 2018.
- [5] Hadad, Abbas Abd-Alhusein, et al. "A Robust Colour Image Watermarking Scheme Based on Discrete Wavelet Transform Domain and Discrete Slantlet Transform Technique." *Journal homepage: <http://iieta.org/journals/isi>* 27.2 (2022): 313-319.
- [6] Y. Ren, T. Liu, L. Zhai, and L. Wang, "Hiding Data in Colors: Secure and Lossless Deep Image Steganography via Conditional Invertible Neural Networks," *arXiv preprint arXiv:2201.07444*, 2022.
- [7] A. Gupta, H. Shukla, and M. Gupta, "A Secure Image Steganography using X86 Assembly LSB," *NEU Journal for Artificial Intelligence and Internet of Things*, vol. 1, no. 1, pp. 38-47, 2022.
- [8] M. A. Hameed, M. Hassaballah, S. Aly, and A. I. Awad, "An adaptive image steganography method based on histogram of oriented gradient and PVD-LSB techniques," *IEEE Access*, vol. 7, pp. 185189-185204, 2019.
- [9] I. Maurya, and S. K. Gupta. "Secure image steganography through pre-processing." In *Soft Computing: Theories and Applications*, pp. 133-145. Springer, Singapore, 2019.
- [10] Xing-Yuan Wang, Xiao-Li-Wang, Lin Teng, Dong-Hua Jiang, and Yongjin Xian, "Lossless embedding: A visually meaningful image encryption algorithm based on hyper chaos and compressive sensing," *Chinese Physics B*, Volume 32, No. 2, 2023, 020503.
- [11] Tutuncu K. and Demirci B., "Adaptive LSB Steganography on Chaos Theory and Random Distortion," *Advances in Electrical and Computer Engineering*, Volume 18, Issue 3, 2018, pp. 15-22.
- [12] Shahid Rahman, Jamal Uddin, Hameed Hussain et al. A Huffman Code LSB based Image Steganography Technique Using Multi-Level Encryption and Achromatic Component of an image, 08 March 2023, PREPRINT (Version 1) available at Research Square [<https://doi.org/10.21203/rs.3.rs-2579014/v1>]
- [13] Rana S. Hameed, Siti S. Mokri, Mustafa S. Taha and Mustafa M. Yaher, "High Capacity Image Steganography System based on Multi-layer Security and LSB Exchanging Method," *International Journal of Advanced Computer Science and Applications(IJACSA)*, 13(8), 2022.
- [14] Sama N. M. Al-Faydi, Shar Khalid Ahmed and Heba N. Y. Al-Talb, "Improved LSB image steganography with high imperceptibility based on cover-stego matching," *IET Image Processing*, volume 17, Issue 7, 29 May 2023, pp. 2072-2082.
- [15] Krystian Grzesiak, Zbigniew Piotrowski and Jan M. Kelner, "A wireless covert channel based on dirty constellation with phase drift," *Electronics*, volume 10, 2021, 647.
- [16] Asmaa A. Eyssa, Fathi E. Abdelsamie and Abdelaziz E. Adelnaiem, "An efficient image steganography approach over wireless communication system," *Wireless Personal Communication*, volume 110, 2020, pp. 321-337.

- [17] S. Venkatesh, V. Sivakumar, A. K. Vagheesan, S. Sakthivelan, K. J. Kumar, and K. K. Nagarajan. "GANash -- A GAN approach to steganography." arXiv preprint arXiv:2110.13650, 2021.
- [18] D. Volkhonskiy, B. Borisenko, and E. Burnaev. "Generative adversarial networks for image steganography". Open Review, 2016.
- [19] D. Volkhonskiy, I. Nazarov, and E. Burnaev. "Steganographic generative adversarial networks." In Twelfth International Conference on Machine Vision (ICMV 2019), vol. 11433, pp. 114333M. International Society for Optics and Photonics, 2020.
- [20] H. Shi, X. Zhang, S. Wang, G. Fu, and J. Tang. "Synchronised detection and recovery of steganographic messages with adversarial learning." In International Conference on Computational Science, pages 31–43. Springer, 2019.
- [21] H. Shi, J. Dong, W. Wang, Y. Qian, and Xiaoyu Zhang. "SGAN: secure steganography based on generative adversarial networks." In Pacific Rim Conference on Multimedia, pages 534–544. Springer, 2017.
- [22] A. Quattoni, and A. Torralba, "Recognizing Indoor Scenes," IEEE Conference on Computer Vision and Pattern Recognition, CVPR, 2009.
- [23] T.S. Rappaport, Wireless Communications, Prentice-Hall, 1996.
- [24] Zhou, B.; Lapedriza, A.; Khosla, A.; Oliva, A.; Torralba, A. Places: A 10 million image database for scene recognition. IEEE Trans. Pattern Anal. Mach. Intell. 2017, 40, 1452–1464.
- [25] F. Yu, H. Chen, X. Wang, W. Xian, Y. Chen, F. Liu, V. Madhavan, and T. Darrell (2020) Bdd100k: A diverse driving dataset for heterogeneous multitask learning. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 2636–2645. <https://doi.org/10.48550/arXiv.1805.04687>
- [26] S. Goferman, L. Zelnik-Manor, and A. Tal (2012) Context-aware saliency detection. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 10, pp. 1915–1926. [doi:10.1109/TPAMI.2011.272](https://doi.org/10.1109/TPAMI.2011.272)
- [27] R. McCall et al. (2019) A taxonomy of autonomous vehicle handover situations. Transp. Res. A, Policy Pract., vol. 124, pp. 507–522, Jun. 2019. <https://doi.org/10.1016/j.tra.2018.05.005>
- [28] Sabah A. Jebur, Abbas K. Nawar, Lubna E. Kadhim and Mothefer M. Jahefer, "Hiding Information in Digital Images Using LSB Staganography Technique," iJIM, volume 17, No. 7, 2023.
- [29] Rana S. Hameed, Siti S. Mokri, Mustafa S. Taha and Mustafa M. Yahar, "High Capacity Image Steganography System based on Multi-layer Security and LSB Exchanging Method," International Journal of Advanced Computer Science and Applications(IJACSA), 13(8), 2022.
- [30] Asmaa A. Eyssa, Fathi E. Abdelsamie and Abdelaziz E. Adelnaiem, "An efficient image steganography approach over the wireless communication system," Wireless Personal Communication, volume 110, 2020, pp. 321-337.
- [31] Hacimurtazaoglu M, Tutuncu K. 2022. LSB-based pre-embedding video steganography with rotating & shifting poly-pattern block matrix. PeerJ Comput. Sci. 8:e843.
- [32] Amirfarhad Nilizadeh, Shirin Nilizadeh, Wojciech Mazurczyk, Cliff Zou and Gary T. Leavens, "Adaptive Matrix Pattern Steganography," Journal of Cyber Security and Mobility, Vol. 11(1), pp. 1–28, 2021.
- [33] Huang, C. T.; Shongwe, N.S.; Weng, C.-Y. Enhanced Embedding Capacity for Data Hiding Approach Based on Pixel Value Differencing and Pixel Shifting Technology. Electronics 2023, 12, 1200.