



High Payload Image Steganography Using DNN Classification and Adaptive Difference Expansion

Shreela Dash¹ · Dayal Kumar Behera² · Subhra Swetanisha³ · Madhabananda Das²

Accepted: 11 March 2024 / Published online: 9 April 2024

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2024

Abstract

The primary intention of this study is to enhance the capacity while ensuring visual integrity and maintaining privacy. A novel information-hiding method based on Adaptive embedding and Machine Learning classifier is proposed. To improve the capacity, the private message is compressed using Adaptive Huffman Encoding. The cover image blocks are classified based on the collected features from each block, determining the ideal Embedding Capacity (EC). The suggested approach has been verified in three distinct categories: the effectiveness of ML classifier, embedding method efficiency, and its robustness. DNN block classifier outperforms the LR and RF classifiers with 99% validation accuracy. The embedding approach with DNN as the block classifier got a PSNR close to 50 at an embedding rate of 1.22 bpp. The robustness of the proposed method is demonstrated with random addition of S&P to the Stego image at 0.5bpp of EC. The proposed scheme sustain S&P noise with accuracy 77% for 50% noise density.

Keywords Data privacy · Deep neural network · Embedding capacity (EC) · PSNR

1 Introduction

The extensive utilisation of the internet, social media, and multimedia has significantly enhanced individuals' daily lives and workplaces, however exposing them more susceptible to emerging risks and security concerns. To improve interpersonal privacy in the area of

✉ Shreela Dash
shreelamamadash@gmail.com

Dayal Kumar Behera
dayalbehera@gmail.com

Subhra Swetanisha
sswetanisha@gmail.com

Madhabananda Das
mndas_prof@kiit.ac.in

¹ Department of CSE, Silicon Institute of Technology, Bhubaneswar, India

² School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar, Odisha, India

³ Department of CSE, Trident Academy of Technology, Bhubaneswar, Odisha, India

information security, the field of cryptography and steganography have gained significant interest in recent times [1–4]. Secret messages are transformed into encrypted files and sent over networks using cryptography. But Secret images are concealed in other multimedia carriers, in steganography. The encrypted representation of images unambiguously reveals the transmission of sensitive data. Conversely, steganography conceals covert images within a regular image, rendering it difficult for an attacker to discern the nature of the concealed data, although being able to view the image [5, 6]. To conceal the secret information, in spatial domain intensity values of cover images are used. The secret images are hidden in the cover image's transforming coefficients in the frequency domain. Different techniques like LSB substitution [7, 8], Modulus function [9–11], Differencing method [12–15], LSB matching [16] and pixel adjustment method [12, 17] are proposed in the literature. Image steganography methods can use evaluation indicators such as security, payload capacity, and visual system perception [18–20]. The level of security in image steganography depends on two key factors: the volume of data to be hidden and the visual characteristics of the carrier image, as well as the extent to which the basic statistical properties change once the message is encoded [21].

In the current research, our objective is to improve the steganography method by considering the maximum embedding capacity with less amount of distortion. For better payload capacity, we are using Adaptive Huffman Coding (AHC) for compressing the secret message before embedding [22]. Most conventional steganography methods dedicate significant effort for selecting the capacity of each pixel to conceal the message. To Determine the capacity of cover image for inserting covert communication is yet a challenging area. The effort is driven by the objective to determine the optimal location for embedding by examining the specific attributes of each block. The notable contributions of this study are stated below.

The proposed work has two objectives:

O1: One goal is to increase the size of payload with reasonable PSNR.

O2: Another objective is to decide the optimal embedding capability of each block in cover image to enhance security and maintain lower level of distortion.

So, the main contributions are:

C1: Before embedding, the confidential information is compressed using the Adaptive Huffman Coding (AHC) approach. The AHC algorithm, which has a high compression code efficiency, is used to reduce the overall length and increase the storage space for the secret message. This paradigm strengthens the EC and increases security when compared to the current research in literature.

C2: The local features are extracted from each block of the cover image. The specific rule is set to decide the target level of block from the value of different features.

C3: Every block in the test image is categorized using different machine learning techniques based on the imputed local attributes that determine embedding capacity. The blocks are categorized into 3 types depending on the target level and each block embeds different amount of secret bit.

C4: The DE method is utilised to embed varying sizes of hidden bits in each block. The effectiveness of the suggested approach is assessed by introducing S&P noise.

Section 2 provides a comprehensive summary of the essential literature review. Section 3 introduces the proposed algorithm and its practical application. The performance evaluation, which demonstrates an enhancement over the existing steganography technique, is shown in Sect. 4. Section 5 contains the conclusion of the work.

2 Literature Survey

Due to the wide range of uses for digital image steganography, there is a growing need for effective algorithms for preserving hidden information. Depending on the application domain, these algorithms can be categorised into two groups: spatial domain approaches and transform domain approaches. The cover image's pixel values are directly manipulated to disguise secret data in the spatial domain [18, 19, 23, 24]. Sagar et al. [20] devised a reversible strategy based on differential evolution (DE) that utilises pixel pair information of changeable differences. This approach aims to reduce the amount of auxiliary information required for embedding into the image while simultaneously increasing the watermark's length. The steganography technique is also utilised in the correlation of social networking behavior. Manju Khari [25] introduced a technique in the spatial domain to protect data in an Internet of Things (IoT) framework. The proposed research in the study is grounded in the spatial domain. So a brief literature review of spatial domain techniques is given in this segment.

The eminent and easiest approach for obscuring data in images is LSB substitution [26]. Even if it uses the simplest steganography method, the RS analysis may detect it. Before hiding the bits, PVD steganography evaluates the hiding capacity of two pixels in a block by comparing their difference values [27]. However, the methodology is detected by the pixel difference histogram (PDH) test [28]. In their study, Thodi et al. [14] introduced an improved reversible data embedding approach that incorporates a histogram shifting technique. The author introduces two novel reversible watermarking methods: one employing flag bits, and the other utilising a highly compressed overflow map that integrates histogram shifting and difference expansion. The methodology has a maximum embedding capacity of one bpp, which is double that of an embedding strategy based on DE. It is possible to further enhance the embedding capacity of the process, and it is advisable to assess its resilience against statistical attacks.

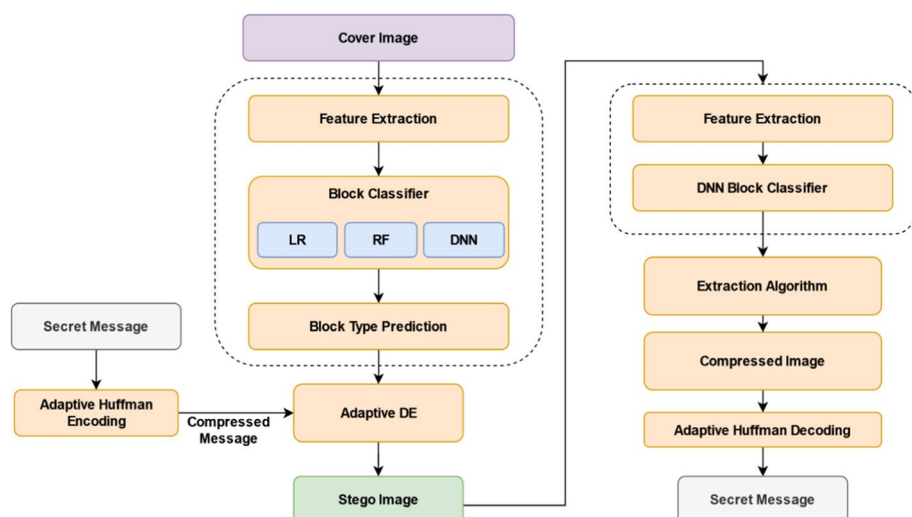
In CDE [21], It is proposed to develop a new lossless centralised difference expansion technique. The embedding approach offers flexibility by allowing different quantities of data to be inserted in each block. Although the stego image has less distortion than earlier attempts, it can yet be enhanced.

Weiqing Wang et al. [29] suggested a right-left shift-based large capacity RDH method. In order to mitigate the distortion caused by the right shift, the peak bins are first pushed towards the right to leave some positions for secret message bits to be embedded. Afterwards, they are shifted towards the left to leave more locations for more data embedding. In order to reduce stego-image distortion, JPEG-LS predictive technique [30] chooses pixels with minimal predicted error values as carriers for secret data bits. The EC value exceeds 1 and the PSNR value approaches 50 in the proposed methodology. The security measures of the method can be strengthened by demonstrating its resistance to various attackers. In [31], a reversible hiding method for greyscale pictures based on the histogram modification is suggested. Throughout the process of embedding, a confidential message is integrated into pixels that have the highest pixel difference within the histogram. However, the method preserves around 30 percent of the entire pixel count of the cover image without making any changes.

In [18] EIRDH author suggested to encrypt the embedded image after hiding the covert message. The empirical findings demonstrate the efficacy of this approach. The payload is nearly same as the traditional DE method i.e. 0.5 bpp. The method provides better security but the payload capacity of the cover image may be increased.

Table 1 Sample rule for defining dataset

Texture	Edge	Mean	Class
L	L	L	00
L	L	M	00
L	M	M	01
M	L	M	01
H	L	L	00
H	M	L	01
H	H	L	10
H	H	H	11

**Fig. 1** Proposed steganography model

3 Proposed Work

A hybrid strategy combining Difference Expansion (DE) and AHC is suggested to accomplish the objective of proposed work. Each cover image's features are extracted prior to embedding. The target level of each block is set using the sample rule mentioned in Table 1. Numerous machine learning classifiers are used to categorise the type of block using these input features. Each type of block embeds different amount of secret message to increase payload with less distortion. The suggested image steganography model is illustrated in Fig. 1.

1. The Adaptive Huffman procedure has been employed for compressing the secret information.
2. The host picture is divided into sub-blocks of size (i, j) , where $(i = j = 3)$.

3. Each block of the host image is used to extract the various local features.
4. The embedding capacity in each block will be determined by the features that were extracted from that block.
5. Each block is classified using a deep neural network utilizing some local features. The secret bits are hidden using an adaptive embedding process based on the capacity of each block.

3.1 Feature Extraction

The suggested technique retrieves three spatial characteristics from every non-overlapping block of dimensions 3×3 in the cover image. The feature values range from 0 to 1.

3.1.1 Extraction of Texture

The LBP, which forecasts the quantity of information in a given block, is used to compute the texture. Less information can be hidden with a smooth texture, while more secret bits will remain hidden with a rough texture. LBP feature extraction technique is used, which is shown in Eq. (1).

$$LBP(X_c - Y_c) = \sum_{i=0}^7 2^i f(C_i - C(X_c, Y_c)) \quad (1)$$

3.1.2 Extraction of Edges

Edge pixel is not as much of vulnerable to the changes caused by embedding. In our proposed work, Sobel filter is used for edge detection [32]. Depending on whether a pixel is an edge or not, each pixel x_i can be either 1 or 0. In order to find the number of edge pixels, the mean value for each block is calculated represented in Eq. (2).

$$E_n = \sum \frac{x_i}{9} \quad 0 \leq i \leq 8 \quad (2)$$

3.1.3 Mean Feature

Darker regions are far more perceptible to the human visual system than are brighter ones. The mean pixel value of each block determines the brightness of each block mentioned in Eq. (3). Less bits can be hidden in darker region than brighter one.

$$B_n = \sum x_i / 9 \quad 0 \leq i \leq 8 \quad (3)$$

3.2 Dataset Preparation

The dataset is prepared by extracting features of 10 random images of size 512×512 . These features are combined to make a dataset. The 3 local features are extracted and the values are normalized. The Otsu thresholding [33] technique is used to generate th_1 and th_2 . Then the 3 ranges are defined for each feature using these threshold values. The ranges are: $0 \leq Low \leq th_1$, $th_1 \leq Medium \leq th_2$ and $th_2 \leq high \leq 1$. For each feature level in the dataset the target class level is set using the rules mentioned in Table 1, where L, M, H represents low, medium and high, respectively.

3.3 Categorization of Block

The proposed solution hides a variable number of secret bits in each given block, and the exact number is dependent on the type of class being used. ML classifier determines the class level of each block.

- The block of pixels is of type I if the output is 00, meaning that each pixel in the block can store one secret bit.
- The block belongs to type II if the output is 01, meaning that each pixel can store two bits.
- A block of type III allows for the embedding of three bits into each pixel if the output is 10.

Block type is classified using three machine learning classifiers: LR (Logistic Regression) [34], RF (Random Forest) [34], and DNN(Deep NN) [35]. Class labels 0, 1, and 2 correspond to Block types 1, 2, and 3, respectively. The feature set is partitioned into train:test sets with ratios 60:40, 70:30 and 80:20. In a 70:30 ratio, Thirty percent of

Table 2 DNN model summary

Layer (type)	Output shape	Param #
BatchNormalization	(None, 3)	12
Layer1 (Dense)	(None, 128)	512
Layer2 (Dense)	(None, 128)	16,512
Layer3 (Dense)	(None, 128)	16,512
Layer4 (Dense)	(None, 128)	16,512
Dropout1 (Dropout)	(None, 128)	0
Layer5 (Dense)	(none, 64)	8256
Layer6 (Dense)	(none, 64)	4160
Layer7 (Dense)	(none, 64)	4160
Layer8 (Dense)	(none, 64)	4160
Dropout2 (Dropout)	(none, 64)	0
Layer9 (Dense)	(none, 32)	2080
Layer10 (Dense)	(none, 32)	1056
Layer11 (Dense)	(none, 32)	1056
Layer12 (Dense)	(none, 32)	1056
Output layer (Dense)	(none, 3)	99

the data are used for validation and seventy percent are used for training. The sklearn library is used to implement the logistic regression and random forest models using default parameters. The architecture of the DNN was created using the Keras sequential model Table 2. The activation function used in the hidden layers is Relu, while in the output layer, it is SoftMax. Six of the 76,143 parameters are non-trainable, while the remaining 76,137 are trainable.

After categorising each block into its own class label, embedding is performed using the algorithm outlined in the following subsection.

3.4 Embedding

In the first phase, the confidential message is compressed. In the subsequent phase, the optimal embedding capacity of each block is predicted using the extracted characteristics from each block. The adaptive algorithm is represented in Table 3.

3.5 Extraction

The process of extracting the confidential information is a reverse procedure of embedding. The extraction method is represented in Table 4.

Table 3 Proposed embedding algorithm

Input: (I: Cover image, H: secret message, block type)

Output: (S: Stego image)

1. Apply Adaptive Huffman Coding to secret messages for generating compressed messages.
2. Apply preprocessing to cover image.
 - Resize I and split I into 3x3 non-overlapping windows.
3. Extract local features and apply ML algorithm to determine class level of each block.
4. Iterate over each block and execute the following actions.
 - $ref = \text{center pixel}$.
 - The difference d_i is calculated as per Eq.(4).

$$d_i = \text{block}(i, j) - ref \quad (4)$$

- The modified difference d_i' is calculated as per the block output in Eqs. (5) - (7).
- If $output=00$

$$d_i' = \begin{cases} d_i + dec(b_i) & d_i \geq 0 \\ d_i - dec(b_i) & d_i < 0 \end{cases} \quad (5)$$

- if $output=01$

$$d_i' = \begin{cases} 2 * d_i + dec(b_{i-1}b_i) & d_i \geq 0 \\ 2 * d_i - dec(b_{i-1}b_i) & d_i < 0 \end{cases} \quad (6)$$

- if $output=10$

$$d_i' = \begin{cases} 3 * d_i + dec(b_{i-2}b_{i-1}b_i) & d_i \geq 0 \\ 3 * d_i - dec(b_{i-2}b_{i-1}b_i) & d_i < 0 \end{cases} \quad (7)$$

5. Each block pixel is revised w.r.t d_i' to produce new pixel.
6. Return stego image S.

Table 4 Proposed extraction algorithm

<i>Input: S = Stego image</i>	
<i>Output: M = Secret message</i>	
1.	Partition <i>S</i> into various blocks of dimension (3 , 3).
2.	To count secret bits, each block 'b' is classified.
3.	For block <i>b</i> calculate difference between each pixel with ref pixel.
4.	Generate the secret bit using Eq. (8).
$s_i = d_i' - d_i \quad (8)$	
5.	Depending on the number of secret bits, s_i is transformed to binary bits to construct message <i>H</i> .
6.	The secret message is generated using the Adaptive Huffman decoding.

4 Analysis of Results

The suggested methodology is evaluated based on several criteria and the outcomes are compared to those of Thodi et al. [14], Chen et al. [19], Chen and Hong [18], Sagar et al. [20], and Lee et al. [21]. The investigation is conducted using standard images of varying dimensions, specifically (256, 256) and (512, 512) which are widely acknowledged as a standard. Cameraman, Lena, Peppers, Fruit, Zelda, Baboon, Aeroplane, Boat, etc. are among the typical photographs selected for evaluation. This section describes every aspect of the performance analysis and experimental results. The three cases mentioned above are used to test the method’s efficiency.

4.1 Case 1: Evaluation of ML Models

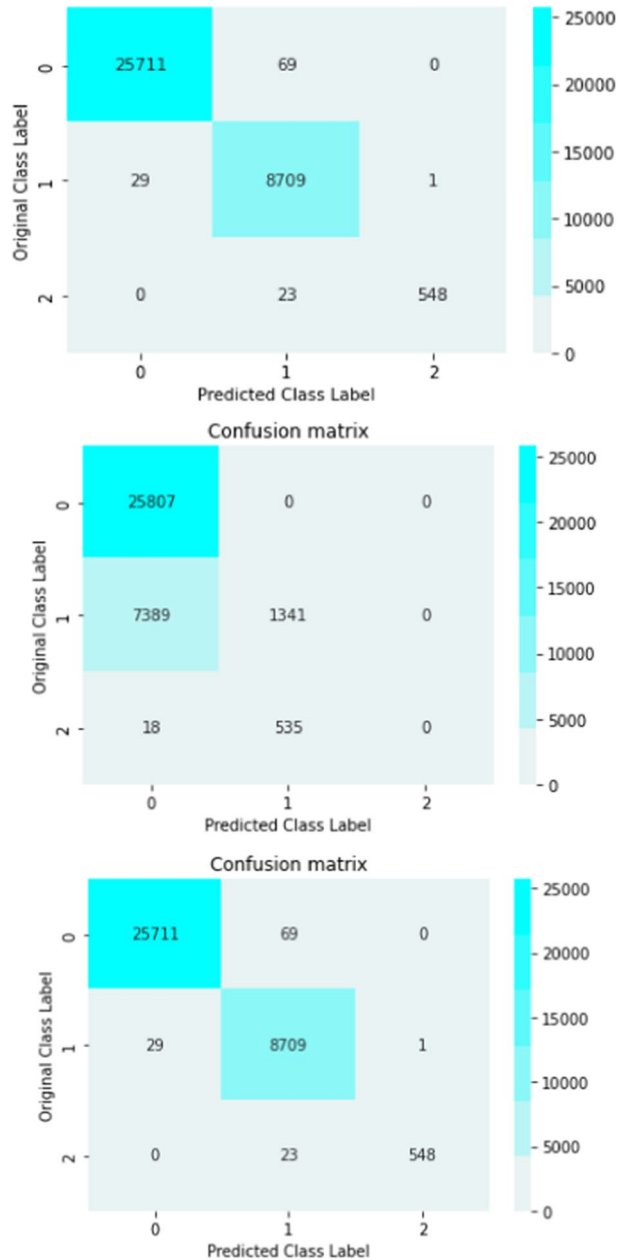
The features are then passed into various machine learning classifiers, which forecast the class labels for every block. Every train-test split ratio’s accuracy evaluation is computed independently. This is done by calculating different accuracy measures like precision, recall, F1-score from the confusion matrix. As the performance behaviour is observed to be same for all the splits, results of 70:30 ratio has been represented. Table 5 shows precision (P), recall (R) and F1 score (F) of different machine learning models for each class. Larger value signifies better result and from the numeric value, DNN signifies best model for all the class labels.

Figure 2, displays the confusion-matrix of all the models.

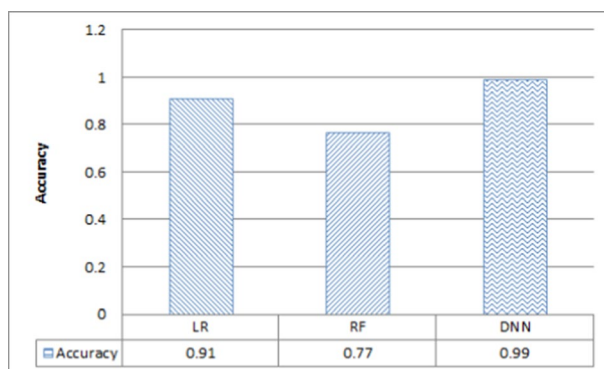
Table 5 Comparative analysis of different ML models

Model	Metrics	Class 0	Class 1	Class 2
LR	P	0.95	0.81	0.67
	R	0.95	0.84	0.39
	F	0.95	0.82	0.49
RF	P	0.78	0.71	0.0
	R	1.00	0.15	0.0
	F	0.87	0.25	0.0
DNN	P	1.00	1.00	0.6
	R	1.00	0.97	0.98
	F	1.00	0.98	0.75

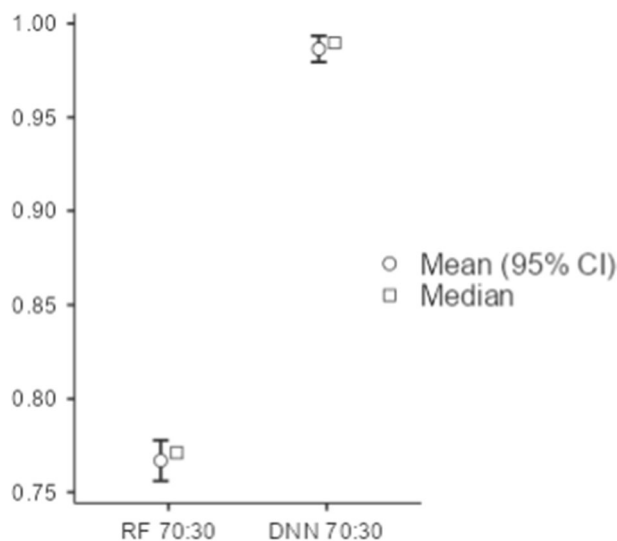
Fig. 2 The confusion matrix **a** LR model, **b** RF model and **c** DNN model



In the confusion matrix the row, column represents actual class and predicted class, respectively. In DNN model, the value 25,711 indicates no. of pixel for class-0 classified correctly. Each model has been executed 10 times and the accuracy is recorded. Those values are used for pair-wise t-test to determine the best model. The average test accuracy of several classifiers is displayed in Fig. 3.

Fig. 3 Accuracy of the block classifier

The plot in Fig. 4 reveals that the median increase in DNN model accuracy is near to 0.99, whereas the median increase in RF and LR models are close to 0.77 and 0.92, respectively. Based on these findings, it appears that DNN is more effective than RF and LR. However, we must still assess whether our revelation is statistically significant. By setting null hypothesis H_0 to “there is no difference in accuracy between the two models”, Wilcoxon Rank Test is conducted for paired sample t-test. The test statistic W in the Wilcoxon signed rank test is the sum of the signed ranks which is shown in the Eq. (9).

Fig. 4 Paired sample t-test (RF vs. DNN)**Table 6** Wilcoxon’s paired samples T-test

Model 1	Model 2	Wilcoxon W	P value	Mean difference
RF 70:30	DNN 70:30	0.00	0.002	−0.2172
LR 70:30	DNN 70:30	0.00	0.002	−0.0736
RF 70:30	LR 70:30	0.00	0.002	−0.1464



Fig. 5 Cover and Stego images at 0.5bpp

$$W = \sum_{i=1}^N [sgn(x_{2,i} - x_{1,i}) \cdot R_i] \quad (9)$$

$x_i = (x_{1,i}, x_{2,i})$ signifies the i -th of N measurement pairs, and R_i denotes the pair's rank.

Table 6 represents the test statistic W and P value of paired sample T-test. When the P value is below 0.05, we have sufficient evidence to reject the null hypothesis with a confidence of 95%. As a result, it is inclined to accept the alternative hypothesis that model 2 outperforms model 1.

4.2 Case 2: Evaluation of Embedding Model

PSNR, MSE, EC, SSIM, and other qualitative and quantitative data provided in Eqs. (10)–(13) are used to analyse the embedding algorithm. Higher the ratio of PSNR and lower the value of MSE shows better the quality of the image. Figure 5, displays both the original and stego image. The metric SSIM is employed for evaluation due to the occasional inadequacy of PSNR.

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

$$MSE = \left(\frac{1}{p \times q} \right) \sum_{i=1}^p \sum_{j=1}^q [(F_{ij} - H_{ij})^2] \quad (11)$$

$$EC = \frac{N}{(H \times W)} \quad (12)$$

$$SSIM(C, S) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (13)$$

Figure 6, illustrates PSNR values for test images with varying ECs. The test image of the bird has the greatest EC value of 1.22 bits per pixel (bpp) and PSNR of 47.6. The experiments exhibits that we achieved PSNR of more than 70 in all the test images at EC 0.5 bpp. Figure 7, displays the EC versus PSNR comparison between the suggested approach and the existing models. The graph demonstrates that the proposed model achieves a higher PSNR value while using the same EC.

Figure 7 exhibits that Chen and Hong [18] has lowest EC up to 0.5 in all the test images with PSNR less than 40. Thodi [14], Chang [19] and Sagar [20] methods has EC up to 1 but the proposed method has EC more than 1 in the different Test images.

Table 7 displays the SSIM values of the proposed approach and four other methods, all measured at an embedding rate of 0.5bpp. The proposed method has an SSIM value of roughly 0.96, which is similar to that of previous methods.

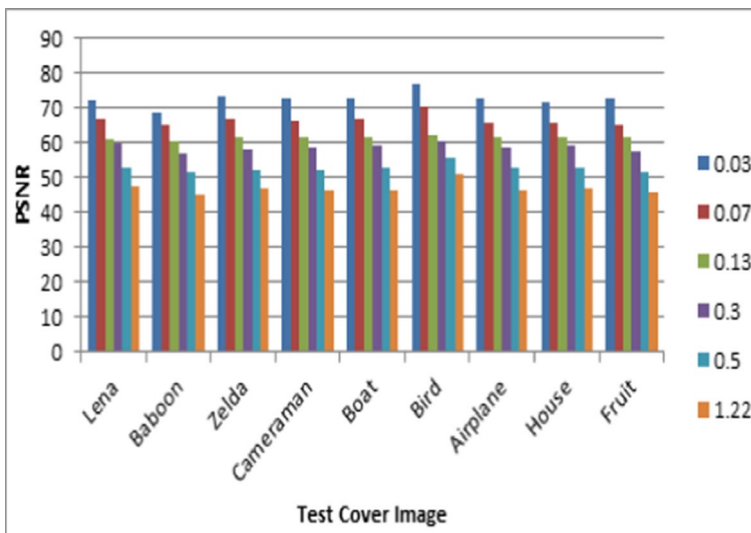
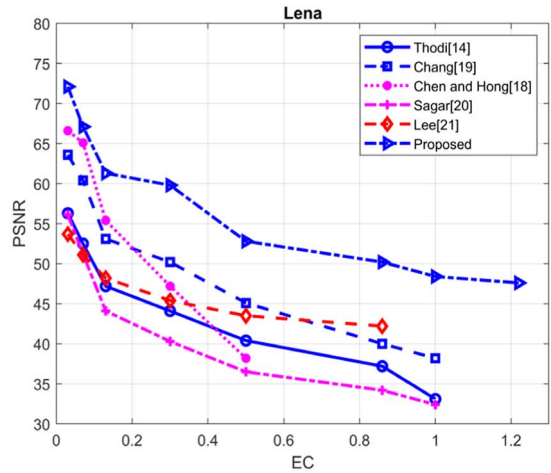
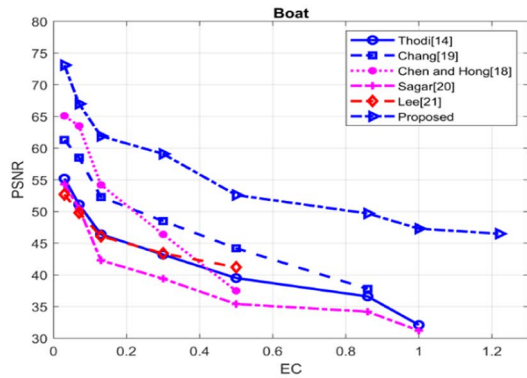


Fig. 6 Test image PSNR with different EC

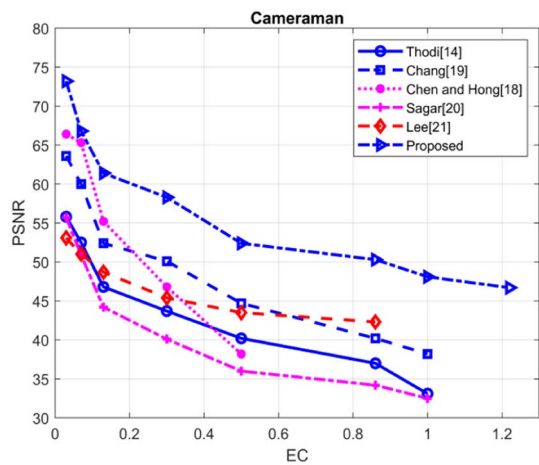
Fig. 7 PSNR versus EC of the test images **a** Lena, **b** Boat and **c** Camera man



(a) Lena



(b) Boat



(c) Camera man

Table 7 SSIM value comparison

Cover image	Chang [19]	Chen and Hong [18]	Sagar [20]	Proposed method
Lena	0.96	0.95	0.97	0.97
Boat	0.95	0.94	0.97	0.98
Baboon	0.96	0.94	0.96	0.96
Zelda	0.96	0.95	0.97	0.97
Cameraman	0.96	0.94	0.97	0.97
House	0.95	0.94	0.95	0.96

Table 8 S&P noise-added steganalysis at EC 0.5

Noise density (%)	TPR	FPR	Precision	Accuracy
10	97.1	2.3	97.3	97.4
20	95.8	4.2	95.2	95.4
30	89.3	10.6	88.6	89.3
40	83.2	16.8	82.1	83.1
50	77.2	22.4	76	77.4
60	70.9	29.4	69.1	70.8
70	64.8	34.8	63.2	64.9
80	60.7	42.1	57.2	59.2
90	53.9	47.3	51.4	53.3
100	51.9	48.5	49.9	51.6

4.3 Case 3: Evaluation of Robustness

By incorporating S&P noise, the embedding algorithm's robustness is confirmed, and the method's accuracy is computed. The salt and pepper noise [28] is utilized by many researchers in for validating the algorithm's robustness. The S&P noise distorts the image quality by applying 255 or 0 in place of the pixel value. With an EC of 0.5 bpp, noise of various densities is applied to the stego image. Once the secret message has been extracted, the effect of adding S&P noise is assessed. Ten distinct 512×512 test images are used in the course of the research. The analysis is conducted in terms of accuracy, precision, true positive rate (TPR), and false positive rate (FPR). It is evident that noise variances have a significant impact on the suggested technique's accuracy and precision. It is evident that the method's accuracy and TPR are still greater than 50 even with a 100% noise addition.

Table 8 displays the measurement outcome for the mean of test pictures at various noise addition degrees. It is evident that noise variances have a significant impact on the suggested technique's accuracy and precision. It is evident that the method's accuracy and TPR are still greater than 50 even with a 100% noise addition.

5 Conclusion

This work suggests a new framework for steganography applications based on, Adaptive Huffman encoding, ML classifiers and Difference Expansion for embedding the secret message. Here, each block's unique characteristics are identified, and the ability of each

block to conceal is assessed through the classification of the local features. Each block contains a compressed private message that is hidden using DE-based steganography. The suggested model outperforms other models that are currently in use when all parameters are taken into account. For embedding capacity 0.5, the average PSNR is higher than 70, indicating less distortion. Following the incorporation of S&P noise, the approach is verified, illustrating improved precision and accuracy. We discovered that the accuracy and precision are higher than 97% with a 10% noise addition. With enhanced PSNR and better EC, the suggested approach offers increased security.

Author Contributions All authors have equal contributions in this work.

Funding No funding is available.

Availability of Data and Materials All the Test images are the common images used for research in image processing and they are publicly available.

Declarations

Conflict of interest Authors Shreela Dash, Dayal Kumar Behera, Subhra Swetanisha and Madhabananda Das declares that they have no conflict of interest.

Ethical Approval It is hereby declared that the manuscript (in part or full) has not yet been submitted nor under consideration anywhere else for possible publication.

References

1. Kaur, S., Singh, S., Kaur, M., & Lee, H. N. (2022). A systematic review of computational image steganography approaches. *Archives of Computational Methods in Engineering*, 29(7), 4775–4797. <https://doi.org/10.1007/s11831-022-09749-0>
2. Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2018). An overview of steganography techniques applied to the protection of biometric data. *Multimedia Tools and Applications*, 77(13), 17333–17373. <https://doi.org/10.1007/s11042-017-5308-3>
3. Jung, K. H. (2018). High-capacity reversible data hiding method using block expansion in digital images. *Journal of Real-Time Image Processing*, 14(1), 159–170. <https://doi.org/10.1007/s11554-016-0618-7>
4. Sahu, A. K., & Swain, G. (2016). A review on LSB substitution and PVD based image steganography techniques. *Indonesian Journal of Electrical Engineering and Computer Science*, 2(3), 712–719. <https://doi.org/10.11591/ijeecs.v2.i3.pp712-719>
5. Rajendran, S., & Doraipandian, M. (2017). Chaotic map based random image steganography using LSB technique. *Int. J. Netw. Secur.*, 19(4), 593–598. [https://doi.org/10.6633/IJNS.201707.19\(4\).12](https://doi.org/10.6633/IJNS.201707.19(4).12)
6. Mandal, P. C., Mukherjee, I., Paul, G., & Chatterji, B. N. (2022). Digital image steganography: A literature survey. *Information Sciences (New York)*, 609, 1451–1488. <https://doi.org/10.1016/j.ins.2022.07.120>
7. Sutaone, M. S., & Khandare, M. V. (2008). Image based steganography using LSB insertion. In *IET conference publications* (No. 535 CP, pp. 146–151). <https://doi.org/10.1049/cp:20080166>
8. Rustad, S., Setiadi, D. R. I. M., Syukur, A., & Andono, P. N. (2022). Inverted LSB image steganography using adaptive pattern to improve imperceptibility. *Journal of King Saud University-Computer and Information Sciences*, 34(6), 3559–3568. <https://doi.org/10.1016/j.jksuci.2020.12.017>
9. Sahu, A. K., & Swain, G. (2018). Pixel overlapping image steganography using PVD and modulus function. *3D Research*, 9(3), 1–14. <https://doi.org/10.1007/s13319-018-0188-5>
10. Wang, C. M., Wu, N. I., Tsai, C. S., & Hwang, M. S. (2008). A high quality steganographic method with pixel-value differencing and modulus function. *Journal of Systems and Software*, 81(1), 150–158. <https://doi.org/10.1016/j.jss.2007.01.049>

11. Akhtar, N., Johri, P., & Khan, S. (2013). Enhancing the security and quality of lsb based image steganography. In *Proceedings: 5th international conference on computational intelligence and communication networks, CICN 2013* (No. September 2013, pp. 385–390). <https://doi.org/10.1109/CICN.2013.85>
12. Gulve, A. K., & Joshi, M. S. (2015). A high capacity secured image steganography method with five pixel pair differencing and LSB substitution. *International Journal of Image, Graphics and Signal Processing*, 7(5), 66–74. <https://doi.org/10.5815/ijigsp.2015.05.08>
13. Swain, G. (2019). Very high capacity image steganography technique using quotient value differencing and LSB substitution. *Arabian Journal for Science and Engineering*, 44(4), 2995–3004. <https://doi.org/10.1007/s13369-018-3372-2>
14. Thodi, D. M., & Rodríguez, J. J. (2007). Expansion embedding techniques for reversible watermarking. *IEEE Transactions on Image Processing*, 16(3), 721–730. <https://doi.org/10.1109/TIP.2006.891046>
15. Dash, S., Das, M., & Behera, D. K. (2021). High capacity information hiding using enhanced difference expansion technique. *ICIC Express Letters*, 15(8), 819–827. <https://doi.org/10.24507/icicel.15.08.819>
16. Lerch-Hostalot, D., & Megías, D. (2013). LSB matching steganalysis based on patterns of pixel differences and random embedding. *Computers & Security*, 32, 192–206. <https://doi.org/10.1016/j.cose.2012.11.005>
17. Jung, K. H., et al. (2019). Adaptive pixel value differencing steganography using both vertical and horizontal edges. *Multimedia Tools and Applications*, 7(1), 39–44. <https://doi.org/10.1080/01611194.2014.885817>
18. Shiu, C. W., Chen, Y. C., & Hong, W. (2015). Encrypted image-based reversible data hiding with public key cryptography from difference expansion. *Signal Processing: Image Communication*, 39, 226–233. <https://doi.org/10.1016/j.image.2015.09.014>
19. Chang, C. C., Huang, Y. H., & Lu, T. C. (2017). A difference expansion based reversible information hiding scheme with high stego image visual quality. *Multimedia Tools and Applications*, 76(10), 12659–12681. <https://doi.org/10.1007/s11042-016-3689-3>
20. Gujjunoori, S., & Oruganti, M. (2019). Difference expansion based reversible data embedding and edge detection. *Multimedia Tools and Applications*, 78(18), 25889–25917. <https://doi.org/10.1007/s11042-019-07767-y>
21. Lee, C. C., Wu, H. C., Tsai, C. S., & Chu, Y. P. (2008). Adaptive lossless steganographic scheme with centralized difference expansion. *Pattern Recognition*, 41(6), 2097–2106. <https://doi.org/10.1016/j.patcog.2007.11.018>
22. Savitri, P. A. I., Murdiansyah, D. T., & Astuti, W. (2016). Digital medical image compression algorithm using adaptive Huffman coding and graph based quantization based on IWT-SVD. In *2016 4th international conference on information and communication technology ICoICT 2016* (Vol. 4, No. c). <https://doi.org/10.1109/ICoICT.2016.7571902>
23. Bin Sulong, G., & Wimmer, M. A. (2023). Image hiding by using spatial domain steganography. *Wasit Journal of Computer and Mathematics Science*, 2(1), 39–45. <https://doi.org/10.31185/wjcm.110>
24. Milosav, P., Milosavljević, M., & Banjac, Z. (2023). Steganographic method in selected areas of the stego-carrier in the spatial domain. *Symmetry (Basel)*. <https://doi.org/10.3390/sym15051015>
25. Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2020). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50(1), 73–80. <https://doi.org/10.1109/TSMC.2019.2903785>
26. Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z., & Sajjad, M. (2017). CISSKA-LSB: Color image steganography using stego key-directed adaptive LSB substitution method. *Multimedia Tools and Applications*, 76(6), 8597–8626. <https://doi.org/10.1007/s11042-016-3383-5>
27. Ganguly, N. M., Paul, G., Saha, S. K., & Burman, D. (2020). A PVD based high capacity steganography algorithm with embedding in non-sequential position. *Multimedia Tools and Applications*, 79, 19–20. <https://doi.org/10.1007/s11042-019-08178-9>
28. Sahu, A. K., & Swain, G. (2019). High fidelity based reversible data hiding using modified LSB matching and pixel difference. *Journal of King Saud University-Computer and Information Sciences*. <https://doi.org/10.1016/j.jksuci.2019.07.004>
29. Wang, W., Ye, J., Wang, T., & Wang, W. (2018). A high capacity reversible data hiding scheme based on right-left shift. *Signal Processing*, 150, 102–115. <https://doi.org/10.1016/j.sigpro.2018.04.008>
30. Wu, H. C., Lee, C. C., Tsai, C. S., Chu, Y. P., & Chen, H. R. (2009). A high capacity reversible data hiding scheme with edge prediction and difference expansion. *Journal of Systems and Software*, 82(12), 1966–1973. <https://doi.org/10.1016/j.jss.2009.06.056>
31. Jia, Y., Yin, Z., Zhang, X., & Luo, Y. (2019). Reversible data hiding based on reducing invalid shifting of pixels in histogram shifting. *Signal Processing*, 163, 238–246. <https://doi.org/10.1016/j.sigpro.2019.05.020>

32. Ravivarma, G., Gavaskar, K., Malathi, D., Asha, K. G., Ashok, B., & Aarthi, S. (2021). Implementation of Sobel operator based image edge detection on FPGA. *Materials Today: Proceedings*, 45, 2401–2407. <https://doi.org/10.1016/j.matpr.2020.10.825>
33. Harb, S. M. E., Isa, N. A. M., & Salamah, S. A. (2015). Improved image magnification algorithm based on Otsu thresholding. *Computers & Electrical Engineering*, 46, 338–355. <https://doi.org/10.1016/j.compeleceng.2015.03.025>
34. Ibrahim, I., & Abdulazeez, A. (2021). The role of machine learning algorithms for diagnosing diseases. *J. Appl. Sci. Technol. Trends*, 2(01), 10–19. <https://doi.org/10.38094/jastt20179>
35. Mohan, E., et al. (2023). Thyroid detection and classification using DNN based on hybrid meta-heuristic and LSTM technique. *IEEE Access*, 11(June), 1–1. <https://doi.org/10.1109/access.2023.3289511>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.



Dr. Shreela Dash is currently working as an Assistant Professor in the Computer Science and Engineering Department, Silicon University, Bhubaneswar. She has more than seventeen years of teaching experience and holds a Ph.D. degree from KIIT DU. Her research interest includes Information Security, Image Processing and Machine Learning. She has more than 14 publications in Scopus/SCI indexed Journals and conferences. In addition, she has four patents. She has guided many M.Tech. and B.Tech Projects.



Dr. Dayal Kumar Behera is currently working as an Assistant Professor (II) in the School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar. He has more than fifteen years of teaching experience and holds a Ph.D. degree from KIIT DU. He obtained a B.E. degree with honours in Information Technology from the National Institute of Science and Technology, Odisha, in 2006 and completed his M.Tech. from the Odisha University of Technology and Research (formerly the College of Engineering and Technology in Bhubaneswar). His research interest includes Recommendation Systems, Computer Vision, Time Series Forecasting, Machine Learning and IoT. He has more than twenty publications in Scopus/SCI indexed Journals and conferences. In addition, he has three patents. He has guided many M.Tech. Projects and two IEDC-funded projects in his area of interest. He is a lifetime member of the ISTE, OITS and IAENG societies.



Dr. Subhra Swetanisha has been working as an Assistant Professor in the department of Computer Science and Engineering at Trident Academy of Technology, Bhubaneswar, Odisha. She has completed her Ph.D. and M.Tech. degree in Computer Science and Engineering from KIIT Deemed to be University, Bhubaneswar. Her research interests include Machine Learning, Data Science, Image Processing and Remote Sensing. She has more than sixteen years of teaching experience and published more than ten Scopus/SCI indexed research articles. She is a life member of the ISTE and IAENG. She can be contacted at email: sswetanisha@gmail.com.



Dr. Madhabananda Das has been working as a Senior Professor in School of Computer Engineering, KIIT Deemed to be University, Bhubaneswar, Odisha. He is having more than 26 years of teaching experience and 13 years of industry experience. His research interests encompass Computational Intelligence, Soft Computing, Artificial Intelligence and Pattern Recognition. He is having a large number of research publications in various international conference proceedings and journals and guided many M.Tech. and Ph.D. Scholars in his areas of interest.