Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 6, pp. 2431–2440
DOI : 10.47974/JDMSC-2751

Optimized image steganography using heterogeneous image embedding techniques

Shruti Jairath *
Kunwar Pal †
Department of Computer Science and Engineering
Dr. B R Ambedkar National Institute of Technology
Jalandhar 144011
Punjab
India

Abstract

The need of safe information hiding has been on the rise in the context of the digital communication with the growth of sharing of online data spread exponentially. This paper presents a new method called the optimized Heterogeneous Image Steganography Network (HISN) in which the various attributes of heterogeneous images are used to greatly improve data hiding and security. HISN makes secret images highly invisible and accurate under cover images using convolutional neural networks. HISN, being made of three networks, which are interconnected, the Preparation Network, the Hiding Network and the Reveal Network is highly sensitive to control the optimized embedding processes and the decoding processes. HISN is strong and reliable, with a training accuracy of 92.64% and a testing accuracy of 90.47. The cover images are similar to the original images and the results of the encoder images, the secret images are similar to the original images, so there is an effective data hiding and recovery.

Subject Classification: *Primary 94A08, Secondary 54H30.*

Keywords: *Steganography, HISN, Multimedia, Encoded pictures, Reveal network, Hiding network, Preparation network.*

1. Introduction

The necessity to secure confidential data against unauthorized access by the third parties has increased due to the blistering development of the online data share in the digital world. Some of the fundamental methods in the area of information security are cryptography, watermarking, and steganography [1]. Image steganography generally embeds secret data within digital images by

* *E-mail:* shruti.cs.19@nitj.ac.in (Corresponding Author)
† *E-mail:* kunwarp@nitj.ac.in

preserving the visual fidelity of the cover media [2–4]. Contrastingly, heterogeneously distributed images that consist of images with different format, compression schemes, resolution, textures, and color statistics give intrinsic variability which forms a powerful obstruct to steganalysis models. To an attacker, the variability of images in and of itself might impose generalization in heterogeneous distributions, making the detection more inaccurate with improved security of the secret communication. JPEG uses lossy compression mechanism that changes the frequency coefficients and frequently damages or removes the data embedded in it hence making it hard to hide [5]. PNG is lossless, but has a fairly limited embedding capability and is not as flexible in a variety of applications [6]. BMP images have pixel-level accuracy but have excessive storage and transmission overheads [7]. Robustness can be enhanced through frequency-domain methods, but maintaining invisibility at all formats is a difficulty [8].

Also, a number of steganographic systems that are based on deep learning (DL) are developed on homogeneous data and, therefore, have low generalizability on a wide range of image types like BMP, PNG, and JPEG [9]. These constraints are also revealed by the more developed steganalysis structures, which uses the format-specific, and the dataset-specific artifact to identify the concealed content [10]. Based on these insights, the paper suggests a DL-driven model, the Heterogeneous Image Steganography Network, that is meant to capitalize on the inherent benefits of heterogeneous images to the security of data hiding.

This paper presents HISN as an emerging paradigm that is explicit in exploring image heterogeneity to provide steganographic security, imperceptibility, and resistance to state-of-the-art steganalysis.

2. Related works

In this section, the author will review some of the major advances in the field of image steganography by classifying previous works according to their method.

2.1 *Traditional Embedding-Based Steganography*

Sarkar and Samanta [11] came up with a method that conceals information in portions of the image with high variation (edges) and thus it is more difficult to detect. The small 2x2 blocks of pixels together with a scrambling technique known as the Arnold Map were employed by Pattanayak et al. [14] to make the hidden data less predictable, and thereby enhance the security, yet making it susceptible to noise and image format alterations. As proposed by Shawkat, Tagougui, and Kherallah [16] and Lan, Wang, and Lin [17], the techniques rely on optimization and complex mathematical patterns to conceal greater volumes of data, but they tend to fail when the image is subjected to various alterations Rai et al. [18].

2.2 *Deep Learning–Based Steganography*

Sarkar et al. [12] addressed the issue of color fading during hidden-image technologies, particularly in images generated in Internet of Things (IoT) equipment. Kiltz et al. [13] were interested in preserving the quality of the images and also ensuring the possibility of tracing the changes in case they were necessary.

2.3 *Heterogeneous and Multi-Format Steganography*

Giboulot, Pevný, and Ker [8] demonstrated that it is more difficult to use detection tools to detect hidden content when one works with broad types of images. Halboos and Albakry [9] examined systems that adapt to varying image features and found that the more the increased the complexity of things when different image types are involved. A method that was proposed by Taheri and Rahbar [15] conceals the data but not the image itself; it uses fragments of natural images in its place. Shahid and Imtiaz [10] have suggested a cloud-based system, which consists of hidden-image that can be used to store the images securely yet due to the fact that it relies on the particular image formats. Dabas et al. [19] discussed the effect of data fairness in the image processing applications.

Most of the works, however, do not cover more than one area. The problem is that there remains an apparent void in coming up with a single methodology to harness all these strengths particularly one that can be compatible with a broad array of image formats. This is the primary problem that the proposed HISN method should resolve.

3. Proposed Methodology

The methodology presented here has been proposed to solve the problem of securing digital images in case of steganography, namely; Heterogeneous Image Steganography Network (HISN).

It makes use of dissimilar images of different resolutions, color distributions, and texture properties, creating a complex embedding pattern. The HISN technique will be able to support various image formats considering the way each of them manages and compresses data. To stabilize the process in these formats, all the images are decoded and turned into a common form. At that, they are resized and brought to the same scale. The procedure of Figure 1 combines superior preprocessing, embedding schemes, and effective data extraction algorithms of the secure data concealment.

Image-centric process has the data preparation, normalization, analysis of pixels, and training. The tiny-ImageNet data is loaded, normalized, resized and pre-processed to fit deep learning systems.

$$P_{\text{normalized}} = \frac{P_{\text{original}}}{255} \tag{1}$$

Image resizing is crucial in providing uniform input sizes throughout the dataset, which is useful in processing images in batches in neural networks. Mathematically, the resizing transformation of pixel value I (x, y) of the original image to the resized image is as,

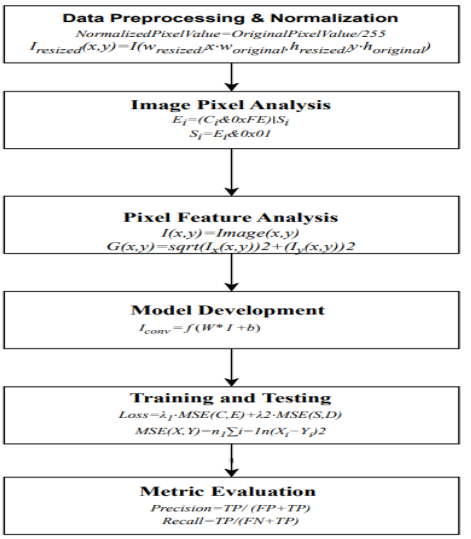

Figure 1
Flow chart for the suggested methodology

$$I_{\text{resized}}(x', y') = I\left(\frac{x \cdot w_{\text{resized}}}{w_{\text{original}}}, \frac{y \cdot h_{\text{resized}}}{h_{\text{original}}}\right) \quad (2)$$

This step subtracts the mean pixel values $\mu_{ImageNet}$ (calculated over the ImageNet dataset) to centre the pixel distribution around zero, as shown in equation (3).

$$I_{\text{preprocessed}}(x, y) = I_{\text{resized}}(x, y) - \mu_{\text{ImageNet}} \quad (3)$$

The JPEG decoding whose mathematical representation is the inverse DCT (IDCT) can be represented as equation 4 below:

$$I_{\text{spatial}}(x, y) = \text{IDCT}\left(\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} C(u, v) \cdot \cos\left[\frac{(2x+1)u\pi}{2N}\right] \cdot \cos\left[\frac{(2y+1)v\pi}{2N}\right]\right) \quad (4)$$

In this case, C(u, v) is the DCT coefficients and NNN is the block size (in JPEG, 8 x 8 is usually used). As an example, the single pixel at location (x, y) in any format is denoted to be,

$$P(x, y) = [R(x, y), G(x, y), B(x, y)] \quad (5)$$

In which R, G, B represent the intensity of the red, green and blue colors, respectively.

3.1 *Feature Extraction for Pixel Analysis*

The rationale of using pixel-wise feature extraction in this piece of work is that it is able to preserve the fine details and spatial features of the images and this is necessary to good steganography. Compared to lightweight feature extractors, which focus on computational efficiency, VGG16 offers a richer set

of discriminative representations (features), which makes it easier to embed an image imperceptibly.

The complete steganography model consists of three linked networks: the Preparation Network, the Hiding Network, and the Reveal Network, all having a crucial part in concealing and revealing secret images within other images as shown in Figure 2. This design aims to guarantee the hidden data is highly imperceptible and can be recovered robustly.

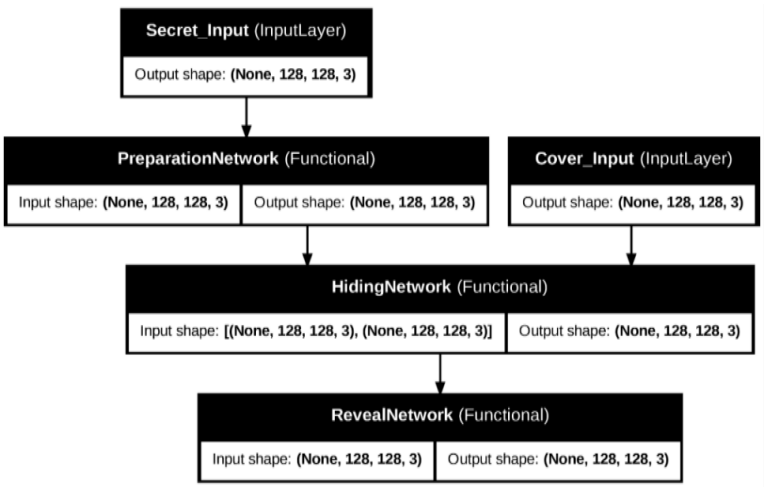

Figure 2
Network architecture for Feature extraction

The first convolutional layer applies a filter F1 of size 3x3 with 50 filters, yielding an intermediate feature map C1 as,

$$C_1 = ReLU\big(Conv2D(I, F_1, padding = 'same')\big) \tag{6}$$

A second convolutional layer, with filter F2 also of size 3x3 and 50 filters, further processes C1 to produce C2 as,

$$C_2 = ReLU\big(Conv2D(I, F_2, padding = 'same')\big) \tag{7}$$

The final convolutional layer in the Preparation Network ensures the output P has the same shape as the input image S with 3 channels as,

$$\mathrm{P} = \mathrm{ReLU}\big(\mathrm{Conv2D}(\mathrm{C}_2, \mathrm{F}_3, \mathrm{padding} = 'same')\big) \tag{8}$$

Overall, the process involves preparation of the secret image, insertion of the secret image into the cover image and subsequently successful removal of the secret image out of the secretly coded cover image.

3.2 *Model Development*

Heterogeneous Image Steganography Network (HISN) is a novel model, which hides and discloses secret images in images using convolutional neural networks. The Table 1 gives the detailed description of the network architecture

displaying the specific layers and configurations used in HISN. The model architecture is given by Figure 3.

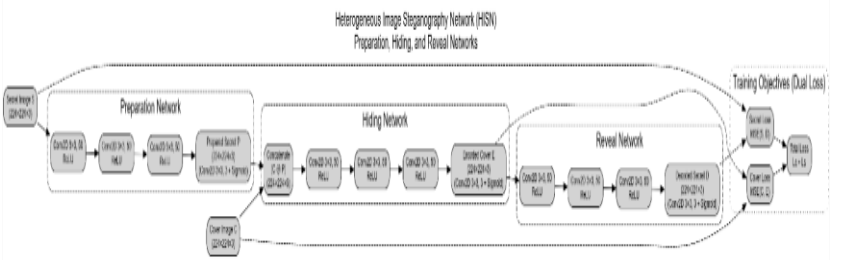

Figure 3
Overall network architecture layer-wise

Mini-ImageNet dataset was chosen to test the suggested HISN framework due to the offered high diversity and difficulty of the presented dataset of natural images with a significant range of variations in texture, color distribution, light, and semantic information.

4. Results and Analysis

This section has done the testing and evaluation of the proposed model on the dataset. The mini-Image dataset that has been introduced by has been used by us in the evaluation of small-scale learning. Nevertheless, it needs fewer infrastructures and resources to execute compared to executing it on the full ImageNet dataset.To achieve reproducibility, the HISN model was trained with a batch size (16) and 25 epochs. An Adam optimizer was used and its starting rate was 0.001, and remained unchanged during the training to achieve consistent convergence. Implementation of the model was done with TensorFlow/Keras with the loss term of Mean Squared Error (MSE) being used to cover and extract secret image in cover images, and the training accuracy of the model showed 92.64%. The computational speed was also efficient in the model where the overall training time was 5.40 seconds and memory consumption was 19.85 GB. The training loss reduced to 0.1191 by the 25 th epoch, which shows that the model is able to learn and to optimize. Such steady

Table 1
Model testing Results

Metric	Value
Average Total Loss (Test 1)	0.0925052097439766
Average Cover Loss (Test 1)	0.042521752566099164
Average Secret Loss (Test 1)	0.0499834568798542
Average Total Loss (Test 2)	0.0952513039112091
Average Cover Loss (Test 2)	0.04438441462814808
Average Secret Loss (Test 2)	0.05086688831448555
Testing Accuracy	0.9047486960887909

reduction in loss signifies better performance in the cover image preservation and secret image reconstruction.

HISN was experimented with test data in two different situations with an average total loss of 0.0925 in the former case and marginally high of 0.0953 in the latter. Accuracy of the HISN model in recreating cover and secret images as well as cover and secret loss values are high. Its testing reliability is approximately 90.47, which means that there is stable hidden image retrieval.

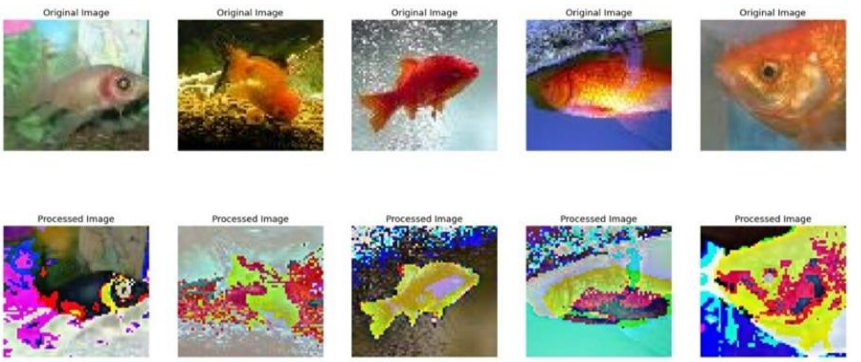

Figure 4
Generated Predictions by the Model

Figure 4 presents the predictions of the HISN, and the images are classified into four parts namely the cover, secret, encoded cover, and decoded secret images. In Secret images in the form of decoded images exhibit certain detail misrepresentation and distortion of colors owing to steganography processes complexity and the limitations of the models.

5. Comparative analysis

This section entails a comparative analysis of the working steganography framework as compared to the current methods in terms of accuracy percentage as the evaluation parameter. This is carried in Figure 5 respectively.

Figure 5 shows that Heterogeneous Image Steganography Network (HISN) has a better performance than its competitors with the highest testing accuracy of 90.47. This is much higher than the performance of the existing models and methods described in the literature. Although SRNet achieved 86.22% and U-Net achieved 87.62%, HISN model shows the significant increase in accuracy. It is observed that the proposed HISN model is more accurate (90.47) by 4.25 of the SRNet model (86.22), 2.54 of the U-Net vs AG-Net models (87.93), 2.85 of the U-Net vs V-Net models (87.62), and 10.80 of the SRNet Proposed model (79.67).

HISN has a high level of imperceptibility (SSIM: 0.987) and good performance with payload rates between 0.4 and 0.5 bpp, giving it a tradeoff between computational cost and security. The conventional approaches such as the U-Net and V-Net have a moderate level of resilience and invisibility but are

not effective in working with a variety of image collections, whereas the methods such as Deng-Net and SRNet are more successful in adversarial training but more computationally expensive.

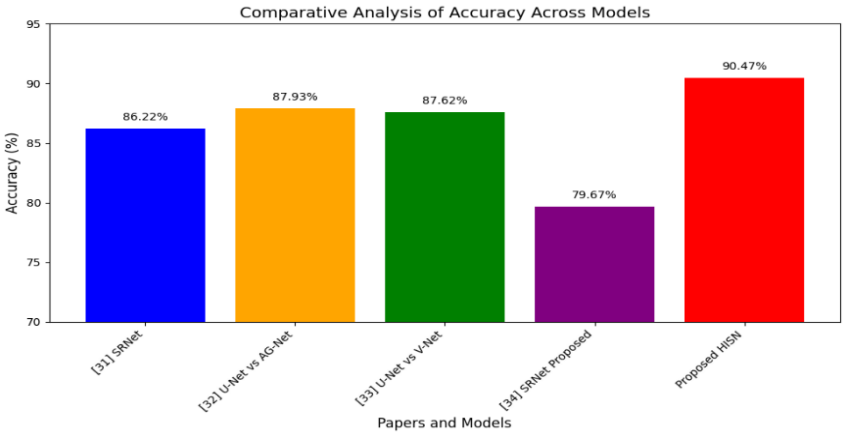

Figure 5

Comparative analysis between our proposed approach and other approaches based on accuracy percentage

6. Conclusion and Future work

The article describes the Heterogeneous Image Steganography Network (HISN) which is a new model designed to conceal and retrieve hidden images within other images. HISN had high accuracy and efficiency having undergone a vigorous training and testing, with a training accuracy of 92.64% and a testing accuracy of 90.47%. HISN is notably useful in real-life cases where streaming media between multi-platforms is involved and sharing of images between applications different in terms of applying compression and formatting criteria are common.

Our work can be expanded in the future to make the proposed steganography structure more robust, secure, and quality. One such field of research is the enhancement of the Mean Squared Error (MSE), so that there is the least amount of distortion between the cover image and the encoded image, and still the integrity of the secret image should not be compromised. Also, more sophisticated metrics and methods, e.g., perceptual quality analysis, adversarial robustness, might be added to make the system more resistant to the contemporary steganalysis attacks.

Competing Interests: Authors declare not conflict of interest

Funding: No funding is applicable

Authors Contributions: - Shruti Jairath wrote the main manuscript, and Kunwar Pal revised the paper. After modification, Shruti Jairath and Kunwar Pal checks the paper. All authors reviewed the manuscript.

References

[1] D. Dhabliya, A. Lavhale, S. Thakur, R. M. Gomathi, A. Kumar, and S. De, "Enhancing cryptographic security through zero-knowledge proofs in theoretical mathematics," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 29, no. 2-B, pp. 913–921 (2026), doi:10.47974/JDMSC-2542.

[2] N. Janu, S. Singhal, and P. Bhardwaj, "Steganography and data encryption in images using contrast stretching and AES encryption," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 6, pp. 2551–2559 (2025), doi: 10.47974/JDMSC-2339.

[3] A. Martín, A. Hernández, M. Alazab, J. Jung, and D. Camacho, "Evolving generative adversarial networks to improve image steganography," *Expert Systems with Applications,* vol. 222, Art. no. 119841 (2023).

[4] J. Yu, X. Zhang, Y. Xu, and J. Zhang, "Cross: Diffusion model makes controllable, robust and secure image steganography," in *Advances in Neural Information Processing Systems*, vol. 36 (2024).

[5] N. V. Thakur, K. Deshmukh, S. A. Shah, and V. B. Semwal, "A scheme for encrypted image data compression," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-A, pp. 409–420 (2024), doi: 10.47974/JDMSC-1897.

[6] W. Su, J. Ni, and Y. Sun, "StegaStyleGAN: Towards generic and practical generative image steganography," in *Proc. AAAI Conf. Artificial Intelligence,* vol. 38, no. 1, pp. 240–248 (Mar. 2024).

[7] M. Garg, J. S. Ubhi, and A. K. Aggarwal, "Neural style transfer for image steganography and destylization with supervised image-to-image translation," *Multimedia Tools and Applications*, vol. 82, no. 4, pp. 6271–6288 (2023).

[8] Q. Giboulot, T. Pevný, and A. D. Ker, "The non-zero-sum game of steganography in heterogeneous environments," *IEEE Trans. Inf. Forensics Security,* vol. 18, pp. 4436–4448 (2023), doi: 10.1109/TIFS.2023.3295945.

[9] E. H. J. Halboos and A. M. Albakry, "Improve steganography system using agents software based on statistical and classification technique," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 3, pp. 1595–1606 (2023).

[10] A. Shahid and S. Imtiaz, "Designing Secure Architectures for Data Storage in Cloud Environments," *J. Comput. Artif. Intell.,* vol. 1, no. 2 (2023), doi: 10.69591/jcai.1.2.1.

[11] A. Sarkar and S. Samanta, "A radical image steganography method predicated on intensity and edge detection," in *Novel Research and Development Approaches in Heterogeneous Systems and Algorithms*, IGI Global, pp. 173–190 (2023).

[12] M. Sarkar, I. Banerjee, T. K. Ghosh, A. Samanta, and A. Sarkar, "A novel steganography approach using S-CycleGAN with an improvement of loss function," in *Novel Research and Development Approaches in Heterogeneous Systems and Algorithms*, IGI Global, pp. 123–142 (2023).

[13] S. Kiltz, J. Dittmann, F. Loewe, C. Heidecke, M. John, J. Mädel, and F. Preißler, "Forensic image trace map for image-stego-malware analysis: Validation of the effectiveness with structured image sets," in *Proc. ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, pp. 125–130 (Jun. 2024), doi: 10.1145/3658664.3659641.

[14] S. Pattanayak, S. Samanta, D. Dey, A. Sarkar, and S. Bhattacharyya, "An Image Steganography Approach Using Arnold Transformation," in *Advances in Systems Analysis, Software Engineering, and High Performance Computing,* pp. 217–235 (Apr. 2023), doi: 10.4018/978-1-6684-7524-9.ch012.

[15] F. Taheri and K. Rahbar, "Coverless image steganography using content-based image patch retrieval," *The Computer Journal*, vol. 67, no. 9, pp. 2799–2808 (2024).

[16] S. A. Shawkat, N. Tagougui, and M. Kherallah, "Text embedding in image using an optimisation-based key generation method," *International Journal of Intelligent Engineering Informatics,* vol. 11, no. 3, pp. 229–254 (2023).

[17] C. F. Lan, C. M. Wang, and W. Lin, "A novel adaptive image data hiding and encryption scheme using constructive image abstraction," *Applied Sciences*, vol. 13, no. 10, Art. no. 6208 (2023).

[18] S. Rai, A. K. Upadhyay, D. Sharma, D. Raj, A. K. Gupta, and D. Ather, "Quantum Cryptography - a Modern Approach," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 7, pp. 1991–2006 (2023), doi: 10.47974/JDMSC-1839.

[19] V. Dabas, K. Sinha, M. Pasricha, and N. Sharma, "Assessing dataset fairness in image privacy detection," in *Proceedings of the International Conference on Data Analytics & Management*, pp. 239–247 (2024).

Received November, 2025