International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(Research Article)

Check for updates

A hybrid edge-guided Fourier transform image steganography framework with CNN-Based Detection

S. SUREKHA and MERUVU SAI KUMAR *

Department Of Computer Science and Engineering, UCEK(A), JNTU Kakinada, Andhra Pradesh, India-533003.

International Journal of Science and Research Archive, 2026, 20(01), 963–970

Publication history: Received on 20 June 2026; revised on 25 July 2026; accepted on 28 July 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.20.1.1544

Abstract

Image steganography focuses on hiding hidden information in digital images without degrading the quality of images and avoiding any possibility of detecting the hidden message. Traditional edge-based methods adopt predefined algorithms like Sobel and Canny for detecting the regions suitable for embedding, which may not work efficiently if the images have weak and non-clear edges. Besides, traditional spread spectrum techniques require predefined pseudo-noise (PN) sequences as secret keys, which may pose a threat to security and robustness against any geometric transformations. To address these limitations, This paper proposes a secure image steganography framework that integrates Hybrid Edge-Guided Fourier-Domain Steganography Framework with the Convolutional Neural Network (CNN) based learned detector for securing the process of image steganography. A content adaptive attention mechanism will be adopted to detect the best regions of embedding in the spatial domain, whereas PN classes embedding will be done in the Fourier domain. The CNN based encoder-decoder network will be used to hide and recover the data, and a trained CNN classifier will allow a blind detection. Efficiency and security of this approach will be measured by calculating PSNR, SSIM, MSE, BPP and Re using Xu-Net and Ye-Net steganalysis models.

Keyword: Image Steganography; Convolutional Neural Network; Fourier Transform; Pseudo-Noise Sequence; PSNR; SSIM; Content-Adaptive Embedding

1. Introduction

In today's digital age, safe transmission of confidential information and images is one of the foremost criteria for communication systems. In recent times, there have been fast advancements in internet-based applications, cloud storage, multimedia communications, etc., where confidential information is regularly being shared using digital mediums. Thus, there is a need for protection of the information from any type of unauthorized usage, manipulation, and threats that may arise from cyber space. Steganography is a common technique of information hiding technology in which secret information or image is encoded within the cover image. The use of traditional techniques of steganography like Significant Bit (LSB) substitution and fixed spatial domain embedding methods is easy; however, there are certain drawbacks of these techniques such as poor security, visible degradation in image quality, vulnerability to attacks, etc. In order to reduce these imperfections, edge-based techniques were introduced in which secret information is embedded in edges and textures of an image. But the edge-based techniques of steganography use certain fixed algorithms such as Sobel and Canny, that might not work efficiently for images having low contrast edges. Likewise, traditional methods of using pre-defined pseudo-noise (PN) sequences in spread spectrum method could be predictable, which makes the entire system susceptible to any sort of security threats.

To address these limitations, The designed system implements a new scheme of steganography which involves the hybrid combination of the content-adaptive spatial embedding approach with the spread spectrum encoding method in the Fourier transform domain. In addition, this system is based on the pseudo noise code generation system using the

* Corresponding author: S. SUREKHA

PIN code, which makes the process of hidden information encryption safe and personalized since only authorized users have access to decoding of the hidden data. Moreover, the CNN encoder-decoder model is employed by the designed system for intelligent extraction of the features of the images, secret information embedding, and decoding of the encoded secret message. Also, the CNN classifier plays an important role in the receiver side for extracting the hidden information without resorting to the original cover image. With the implementation of deep learning based feature extraction along with the system, the system ensures invisibility, good resistance against compression and noise attack, security, and proper reconstruction of the secret image. The rest of the paper is organized as follows. Section II discusses the literature survey and existing systems while Section III presents the proposed methodology. Experimental results and analysis are presented in Section IV and Section V is the conclusion of the paper.

2. Related work

Al-Rawashdeh et al. [1] proposed an effective edge based steganography technique, where the information hiding takes place within edges detected using traditional edge detection techniques. They have achieved PSNR values from 42-46 dB and SSIM value around 0.97. This approach has enhanced security by using edges only rather than smooth areas. But the use of fixed edge detection techniques makes it less flexible to images with poor edges. Ray et al. [2] developed a deep learning technique to identify edges within images and use such regions for embedding messages. This method has a PSNR of 38 to 42 dB and an SSIM of around 0.95. An obvious limitation is the high computational burden associated with the process, which makes it time-consuming. Das et al.[3] a multi-image steganographic scheme using deep neural network (DNN) techniques to hide one secret message into multiple images, thus achieving larger embedding capacity at 2–3 BPP. Although PSNR levels between 37 dB and 40 dB have been obtained, handling multiple images greatly raises the system's complexity. Farrag and Alexan [4] proposed a 3D steganography algorithm based on the mesh traversal technique for hiding data inside 3D objects. This technique ensures an error rate of less than 5%, but is only limited to 3D models, and not useful for 2D digital images. Płachta et al. [5] developed a steganalysis model using deep learning techniques and ensemble classifiers to identify any hidden data in images with a detection accuracy of 90–95%. Their research emphasizes that the traditional steganography techniques have become vulnerable to the deep-learning-based detection models. Duan et al. [8] Combined the elliptic curve cryptography (ECC) approach with the deep neural networks (DNNs) to perform encryption and data embedding to reach a PSNR of around 40 dB while offering high security. Nevertheless, combining encryption and DNN makes the process highly complex.

The observations drawn from related works reveal that while edge-based and deep learning-based steganography methods have advanced the field, they each carry trade-offs in computational cost, adaptability, and security. The proposed system addresses these gaps by combining CNN-based adaptive embedding, Fourier-domain spread spectrum encoding, and PIN-based PN sequence generation for superior security, robustness, and accurate secret image recovery.

3. Methodology

The hybrid steganography approach has been divided into three major stages, namely; Input and Preprocessing, Embedding and Transmission and Decoding and Performance Analysis. The details for each stage have been provided below.

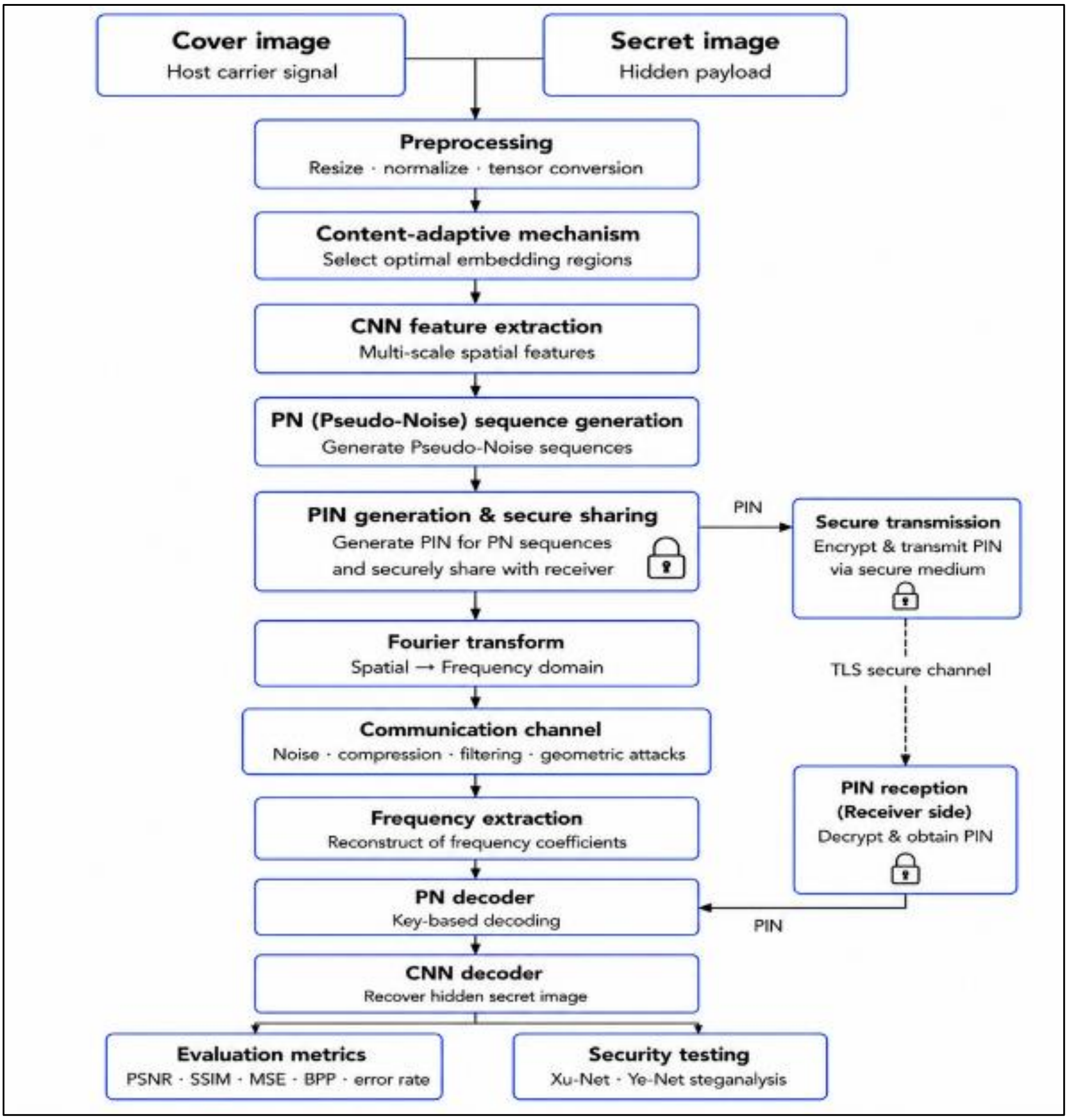


Figure 1 System Architecture

3.1. Phase 1: Image Preprocessing

The proposed system uses two input images – the cover image and secret image. The two inputs go through pre-processing where they are loaded into memory and prepared before any embedding. The process of resizing makes sure that both images are of the same size (256 x 256), and the pixels are normalized to fall between [0-1] range. For numerical stability to compress and enhances using interpolation model.

Creation of the attention map using the gradient edge detection technique marks the content adaptive analysis stage where the textured and high frequency parts of the cover image are selected. After creating the attention map, the next step involves extraction of patterns and features using a Convolutional Neural Network (CNN). This enables automatic selection of textured parts for embedding in order to avoid smooth areas that can be visibly distorted.

3.2. Phase 2: Image Secure Embedding

3.2.1. Algorithm 2.1: Secure Image Steganography Algorithm

INPUT: Cover And Secret Image

OUTPUT: Stego Image

- **Step 1:** Get the user defined PIN and convert it into numerical seed value. Create a unique Pseudo-Noise (PN) sequence using that seed. The created PN sequence becomes a customized Secret Key for that particular session.

- **Step 2:** Use Spread Spectrum technique to multiply the Secret Image with the generated PN Sequence. This will distribute the secret data over multiple frequency components.

- **Step 3:** Ensure PIN Transmission through Secure TLS

    - **Step 3.1:** Set up a secure connection through Transport Layer Security (TLS) protocol between the sender and receiver. The receiver transmits its Digital Certificate to the sender for authentication.
    - **Step 3.2:** Verify the received Digital Certificate from the sender. Ensure that the digital certificate is valid, trusted, and has not been expired.
    - **Step 3.3:** In case of failure in certificate validation, close the current session. Set up a new secure TLS session and proceed with digital certificate validation.
    - **Step 3.4:** In case of successful certificate validation, go ahead and perform the TLS Handshake. This involves creating a session key to ensure encryption of data transmission.
    - **Step 3.5:** Transmit the PIN by encrypting it with the created session key. The receiver uses the same session key to decrypt the PIN for image extraction process.
- **Step 4:** Perform FFT on the Cover Image to transform it from the spatial domain to the frequency domain and get the frequency coefficients of the Cover Image.
- **Step 5:** Embed the spread spectrum encoded secret data into the selected frequency components of the cover image to get the transformed cover image.
- **Step 6:** Generation and Transmission of the Stego Image
    - **Step6.1**: Perform Inverse Fast Fourier Transform (IFFT) on the modified frequency components. The transformed image will be transformed back into the spatial domain to obtain the Stego Image.
    - **Step 6.2**: Transmit the Stego Image using the regular communication channel. Alongside, the encrypted PIN is transmitted using the TLS communication channel.

3.3. Phase 3: Image Transmission and Decoding

The Generated Stego Image would go through the communication channel where there are chances that this generated image would be subjected to various types of image processing techniques like adding noise to the image, compressing, cropping, and scaling during the transmission. After the receipt of the stego image at the destination side, the Fast Fourier Transform process is applied to this image and thus the image gets converted into the frequency domain. The frequency components with the embedded secret messages would be extracted from the frequency components of the cover image.The authentic receiver utilizes the identical PIN generated by the user during the embedding process. The same PIN is encoded to generate the same numeric value, hence creating the same Pseudo-Noise (PN) sequence required for decoding the hidden data. The resulting image is sent to the CNN decoder, where it undergoes reverse transformation for recovering the secret image. This method will guarantee that only the authenticated receiver, having the correct PIN number, will be able to recover the secret image. It guarantees security and privacy of information, authentication, and robustness against attacks on the communication channel.

3.4. Performance Evaluation and Security Analysis

The performance of the proposed hybrid image steganography scheme is measured based on several image quality, embedding capacity, and recovery accuracy measures. Such measures define the efficiency of secret image embedding, image quality retention, and secret image recovery processes.

- **Peak Signal-to-Noise Ratio (PSNR)**: The PSNR computes the similarity of the original cover image with respect to the stego image. PSNR measures the amount of distortion done during the embedding of data. Higher values of PSNR mean that there is almost no difference between the two images, making the hidden information undetectable by the human eye.

Formula: $$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (1)$$

MAX = Maximum pixel value (255 for 8-bit images), MSE = Mean Squared Error

- **Structural Similarity Index (SSIM)**: The use of SSIM is intended for the purpose of testing the structural similarity between the cover image and the stego image. PSNR, which measures the performance of an image by error, is different from SSIM, which evaluates the quality of an image in terms of its luminance, contrast, and structural similarity.

  Formula:

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

  μ_x, μ_y= Mean intensity values, σ_x^2, σ_y^2= Variance σ_{xy}= Covariance, C_1, C_2= Stability constants

- **Mean Squared Error (MSE):** MSE's worth lies in the mean square of the difference between the pixels of the cover image and the stego image. This will help to find out the distortion that is caused during the embedding process. The smaller the value of the MSE, the lesser will be the distortion..

  Formula: $$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - K(i,j)]^2 \quad (3)$$

  $I(i,j)$= Cover image pixel, $K(i,j)$= Stego image pixel,M, N= Image dimensions

- **Bits Per Pixel (BPP):** BPP refers to the embedding capability of the steganographic technique. This is because the BPP indicates the quantity of data that can be hidden in a single pixel of the cover image. The larger the BPP value, the greater the amount of data that can be embedded.

  Formula:

$$BPP = \frac{\text{Total Hidden Bits}}{\text{Total Number of Pixels}} \quad (4)$$

- **Error Rate (Re):** The Error Rate is the technique used to determine the degree of variation that exists between the secret image that was originally used and the secret image extracted using the extraction technique.

  Formula: $$Re = \frac{N_e}{N_t} \quad (5)$$

  N_e= Number of incorrectly recovered pixels/bits, N_t= Total number of pixels/bits

- **Security Testing using Xu-Net and Ye-Net:** Security analysis is performed using Xu-Net and Ye-Net, two CNN-based steganalysis models designed to detect hidden information in images.

Xu-Ne: Xu-Net is a deep convolutional neural network (CNN)-based steganalysis framework specially developed for identifying hidden data inside digital images. The algorithm tries to identify any statistical variations and subtle artifacts introduced to the digital image while the process of embedding data. In our proposed model, Xu-Net is employed in assessing how resistant the generated stego images are from any attacks by the steganalysis approach. When Xu-Net cannot properly recognize the hidden data, it means that the adopted steganographic technique is more secure and imperceptible.

Ye-Net: Ye-Net is a sophisticated CNN-based steganalysis system which has been designed for the purpose of detecting hidden information using the extraction of the highly rich spatial features present in digital images. It uses the concept of deep feature learning to differentiate between the cover images and stego images with a high level of accuracy. In the proposed system, Ye-Net is applied for measuring the robustness of the stego images against the deep learning-based steganalysis attacks. The lesser probability of detection by Ye-Net means that the proposed image steganography system is robust and secure.

4. Results and analysis

The proposed system was evaluated across multiple test images. Figure 2 presents the comprehensive evaluation metrics for each test image. All tested images achieved a BPP of 24.0 and passed the security testing against steganalysis models.

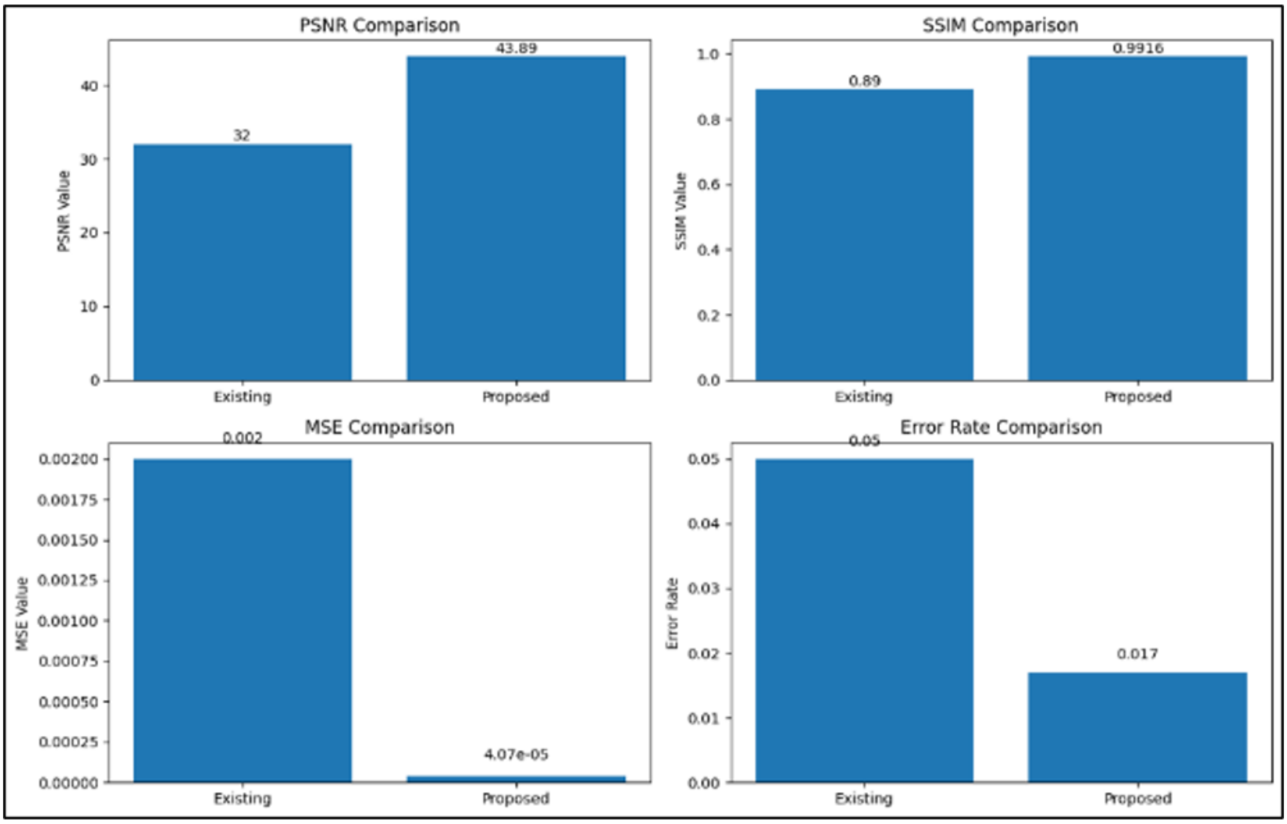


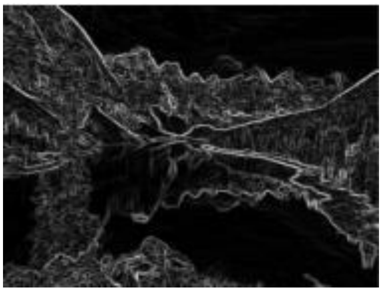
Figure 2 Evaluation Metrics Of Existing vs Proposed System

It is clear from the results that the efficiency is very high for all the tested images. The result of the PSNR values ranging from 43.86-43.97dB and PSNR > 40 dB = Excellent image quality PSNR > 30 dB = Good image quality and Higher PSNR indicates better imperceptibility indicates that the stego images are perceptually identical to the cover images. The SSIM values of 0.9840-0.9917 indicate that there is a complete structural similarity SSIM = 1 then it is a Perfect similarity, SSIM > 0.95 is an Excellent quality preservation Higher SSIM indicates better structural preservation. Furthermore, the low MSE values of 0.00004 indicate that the level of distortion is very low.

The value of error rate 0.014-0.018 indicates that there is very high accuracy in the retrieval of the secret image MSE = 0 have No distortion Lower MSE indicates better image quality. I taken the common secrete image for all this is High PSNR values in all the images used in the testing phase confirm that the Fourier domain embedding process does not focus the distortion on any particular spatial region. Furthermore, using PINs in the PN sequences makes sure that each embedding operation will have its own unique key. High PSNR values in all the images used in the testing phase confirm the success of the Fourier-domain embedding process in distributing the hidden information without focusing the distortion in any specific spatial region. Using PINs in the PN sequences guarantees that each embedding operation will have its own unique key.

Figure 3 Used As Secrete Image For All Given Below Images

Table 2 Represented the various images taken as a cover image and their Evaluation Metrics

NO	Original Image	Content-Adaptive Mechanisms	PSNR	SSIM	MSE	Error Rate
1			43.94	0.983	4.03	0.01770
2			43.96	0.990	4.01	0.01769
3			43.86	0.990	4.11	0.01445
4			43.89	0.99	4.07	0.01700

5. Conclusion

In A Hybrid Edge-Guided Fourier Transform Image Steganography Framework with CNN-Based Detection was introduced for secure image steganography. The proposed model overcomes three major shortcomings of current systems dependence on pre-defined edge detection techniques, susceptibility to deep learning-based steganalysis, and lack of personalization in terms of security keys. Content adaptive feature extraction using CNN and Fourier domain spread spectrum based embedding along with PIN based PN sequence generation ensures both invisibility and security. The performance is quite satisfactory with PSNR of 43.89 dB, SSIM of 0.9916, MSE of 0.0000407, and Error rate of 0.017. All tested images are successfully able to withstand steganalysis detection by the Xu-Net and Ye-Net models, ensuring effectiveness against contemporary steganalysis based on CNNs. The use of PIN based decoding ensures that secret image extraction is possible only by authorized persons having the key.

The future research direction will focus on developing the proposed approach in terms of applications for videos and live multimedia steganography, allowing secure transfer of secret information over live communication channels.

References

[1] R. Al-Rawashdeh, M. M. Rahman, and M. Mahmood niazi, "Robust image steganography approach based on edge detection combined with CNN algorithm," Jul. 2025.

[2] B. Ray, S. Mukhopadhyay, S. Hossain, S. K. Ghosal, and R. Sarkar, "Image steganography using deep learning based edge detection," Multimedia Tools and Applications, vol. 80, no. 24, pp. 33475–33503, Oct. 2021.

[3] A. Das, J. Singh Wahi, M. Anand, and Y. Rana, "Multi-image steganography using deep neural networks," arXiv preprint, arXiv:2101.00350, 2021.

[4] S. Farrag and W. Alexan, "Secure 3D data hiding technique based on a mesh traversal algorithm," Multimedia Tools and Applications, vol. 79, nos. 39–40, pp. 29289–29303, Oct. 2020.

[5] M. Płachta, M.Krzemień, K. Szczypiorski, and A. Janicki, "Detection of image steganography using deep learning and ensemble classifiers," Electronics, vol. 11, no. 10, p. 1565, May 2022.

[6] M. A. Wani and B. Sultan, "Deep learning based image steganography: A review," WIREs Data Mining and Knowledge Discovery, vol. 13, no. 3, p. e1481, May 2023.

[7] J. Zhang, X. He, and Y. Cao, "Errorless robust JPEG steganography using steganographic polar codes," EURASIP Journal on Information Security, vol. 2024, no. 1, p. 22, Jul. 2024.

[8] X. Duan, D. Guo, N. Liu, B. Li, M. Gou, and C. Qin, "A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network," IEEE Access, vol. 8, pp. 25777–25788, 2020.

[9] Y. Moussa and W. Alexan, "Message security through AES and LSB embedding in edge detected pixels of 3D images," in Proc. 2nd Novel Intelligent and Leading Emerging Sciences Conf. (NILES), Oct. 2020, pp. 224–229.

[10] R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, ‘‘Digital image steganography survey and investigation (Goal, assessment, method, development, and dataset),’’ Signal Process., vol. 206, May 2023, Art. no. 108908.

[11] M. H. Kombrink, Z. J. M. H. Geradts, and M. Worring, ‘‘Image steganography approaches and their detection strategies: A survey,’’ ACM Comput. Surveys, vol. 57, no. 2, pp. 1–40, Feb. 2025.

[12] A. Kumar, R. Rani, and S. Singh, ‘‘A survey of recent advances in image steganography,’’ Secur. Privacy, vol. 6, no. 3, p. 281, May 2023.

[13] W. Alexan, E. Mamdouh, A. Aboshousha, Y. S. Alsahafi, M. Gabr, and K. M.Hosny,‘‘Stegocrypt: A robust tri-stage spatial steganography algorithm using TLM encryption and DNA coding for securing digital images,’’ IET Image Process., vol. 18, no. 13, pp. 4189–4206, Nov. 2024.

[14] D. R. I. M. Setiadi and J. Jumanto, ‘‘An enhanced LSB-image steganogra phy using the hybrid Canny–Sobel edge detection,’’ Cybern. Inf. Technol., vol. 18, no. 2, pp. 74–88, Jun. 2018.

[15] I. Kich, E. B. Ameur, and Y. Taouil, ‘‘CNN auto-encoder network using dilated inception for image steganography,’’ Int. J. Fuzzy Log. Intell. Syst., vol. 21, no. 4, pp. 358–368, Dec. 2021.