frontiers | Frontiers in Medicine

TYPE Original Research
PUBLISHED 01 September 2025
DOI 10.3389/fmed.2025.1619706

OPEN ACCESS

EDITED BY
Ateeq Ur Rehman,
Gachon University, Republic of Korea

REVIEWED BY
Junaid Zafar,
Government College University, Lahore, Pakistan
Noman Shabbir,
Tallinn University of Technology, Estonia

*CORRESPONDENCE
Doaa Shehab
✉ damenshehab@stu.kau.edu.sa

RECEIVED 28 April 2025
ACCEPTED 31 July 2025
PUBLISHED 01 September 2025

CITATION
Shehab D and Alhaddad M (2025) Image steganalysis using LSTM fused convolutional neural networks for secure telemedicine. *Front. Med.* 12:1619706. doi: 10.3389/fmed.2025.1619706

Image steganalysis using LSTM fused convolutional neural networks for secure telemedicine

Doaa Shehab* and Mohmmed Alhaddad

Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

Deep learning-based image steganalysis has progressed in recent times, with efforts more concerted toward prioritizing detection accuracy over lightweight frameworks. In the context of AI-driven health solutions, ensuring the security and integrity of medical images is imperative. This study introduces a novel approach that leverages the correlation between local image features using a CNN fused Long Short-Term Memory (LSTM) model for enhanced feature extraction. By replacing the fully connected layers of conventional CNN architectures with LSTM, our proposed method prioritizes high-relevance features, making it a viable choice for detecting hidden data within medical and sensitive imaging datasets. The LSTM layers in our hybrid model demonstrate better sensitivity characteristics for ensuring privacy in AI-driven diagnostics and telemedicine. Experiments were conducted on Break Our Steganographic System (BOSS Base 1.01) and Break Our Watermarking System (BOWS) datasets, followed by validation on the ALASKA2 Image Steganalysis dataset. The results confirm that our approach generalizes effectively and would serve as impetus to ensure security and privacy for digital healthcare solutions.

KEYWORDS

steganalysis, steganography, data hiding, healthcare security, LSTM, lightweight

1 Introduction

AI-based digital healthcare solutions require security and data privacy while handling sensitive medical images; therefore, robust techniques are essential to maintain data integrity (1, 2). Particularly, the medical images contain embedded metadata and annotations that may compromise patient privacy (3). Image steganalysis helps in preserving sensitive medical records (4) and by leveraging artificial intelligence (AI) techniques, healthcare professionals can identify potential threats posed by steganographic attacks (5, 6). Beyond privacy concerns, the integrity of medical data is another essential dimension for AI diagnostic systems (7, 8). Malicious actors could use steganography to manipulate images, alter tumor regions, or embed misleading data without detection (1). Advanced steganalysis techniques and emerging telemedicine issues necessitate the integration of robust AI-driven steganalysis tools to improve the security of sensitive health data (2).

Recent image steganalysis techniques exploited the traditional machine learning to extract meaningful features, but human dependencies limited their scope in image steganalysis (9). Low embedding capacity and poor image retrieval rates necessitated the deployment of deep learning assisted steganalysis algorithms. Detailed reviews regarding the recent deep learning strategies and network developments are included elsewhere (10, 11). In this connection, numerous deep learning algorithms were reported for rapid detection of steganographic payloads with reasonable accuracies (12–15). Key modifications include enhancing filters and different activation operators (16), high-order

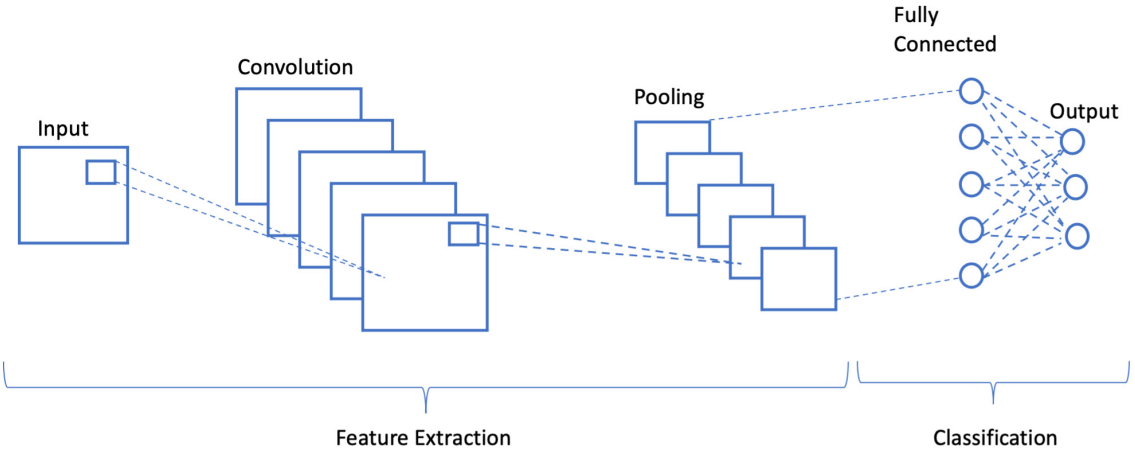

FIGURE 1
Schematic illustration of a generalized convolution neural network.

co-occurrence matrices to capture sensitivity (17, 18), periodic weight capture (19), dimensionality reduction schemes (20), and covariance pooling techniques (16, 21–24).

Moreover, various DL-based models such as Qian et al. (25), Yedroudj et al. (18), Boroumand et al. (19), Deng et al. (16), Zhang et al. (26), Reinel et al. (22), Öztürk Ş and Özkaya (27), and Ozdemir et al. (28) tried to improvise on the stego image feature extraction. In this regard, You et al. (29) exploited EfficientNet, MixNet, and ResNet by removing pooling and stride operations in the first layers. Similarly, (24) applied floating-point quantization to XuNet (24). Recently, LSTM was reported to capture data correlation for image classification tasks (21, 30–32).

In this study, we propose a CNN architecture fused with LSTM by replacing the fully connected layers of the CNN. Our proposed model leverages LSTM to optimize weight matrices and bias vector parameters, ensuring effective training at each time step. In addition, LSTM nodes extract essential contextual features, which is vital for detecting hidden threats within medical images. This research contributes to the field by demonstrating the effectiveness of LSTM fused CNNs in medical image steganalysis by offering a robust security framework to protect sensitive patient data. Furthermore, we compare our proposed architecture with state-of-the-art deep learning models in terms of computational efficiency. By significantly reducing the number of trainable parameters, our model offers a resource efficient and scalable solution for secure medical image transmission and integrity in telemedicine.

The remaining of this work is organized as follows: Explain the Architecture of CNN and LSTM in Section 2. The materials and methods are presented in Section 3. The results discussion is detailed in Section 4. Section 5 concludes the study.

2 A brief on CNN and LSTM architecture

The encoder in any CNN-based steganography scheme employs binary inputs: one for the cover image and the other for secret image to foster a stego image. It includes pre-processing, feature extraction, and classification stage as illustrated in Figure 1. In the feature extraction phase, convolution is performed multiple times to ameliorate the signal-to-noise ratio of the image and to characterize local features, whereas in classification, the extracted local features are average-pooled and concatenated to yield final feature maps. These feature maps were then classified in terms of class probabilities using SoftMax function.

Though LSTM networks improve the functioning of recurrent neural networks (RNNs) in terms of vanishing gradient, LSTM contains three gates which are an input gate, a forget gate, and an output gate, where x_t, C_t, and C_{t-1} represent the current input, new, and previous cell states, respectively. h_t and h_{t-1} refer to the current and previous outputs, respectively. A non-linear function is used to activate these three gates, which makes LSTM a dynamic model with changing contexts (33). The internal architecture of an LSTM cell is shown in Figure 2.

Within an LSTM cell, forget gate controls the contribution of the previous state C_{t-1} to the current state by using sigmoid function σ and is responsible for LSTM cell memory as given by the expression in Equation 1.

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \tag{1}$$

where f_t is the forget vector, and x_t and h_{t-1} are the current input and previous output. As given in Equation 1, x_t and h_{t-1} are multiplied by the trained weights matrix W_f with offset b_f. Due to sigmoid function, the input vector ranges between 0 and 1, indicating the degree to which values are to be remembered or forgotten. h_{t-1} and x_t are passed via input updated gate to append the relevant information and is governed by Equation 2. Thereafter, new information is obtained as $\widetilde{C}_t$ from Equation 3 after passing h_{t-1} and x_t via tanh function. Finally, the candidate of the cell state C_t for the next time step is generated by combining current moment information $\widetilde{C}_t$ and long-term memory information C_{t-1}

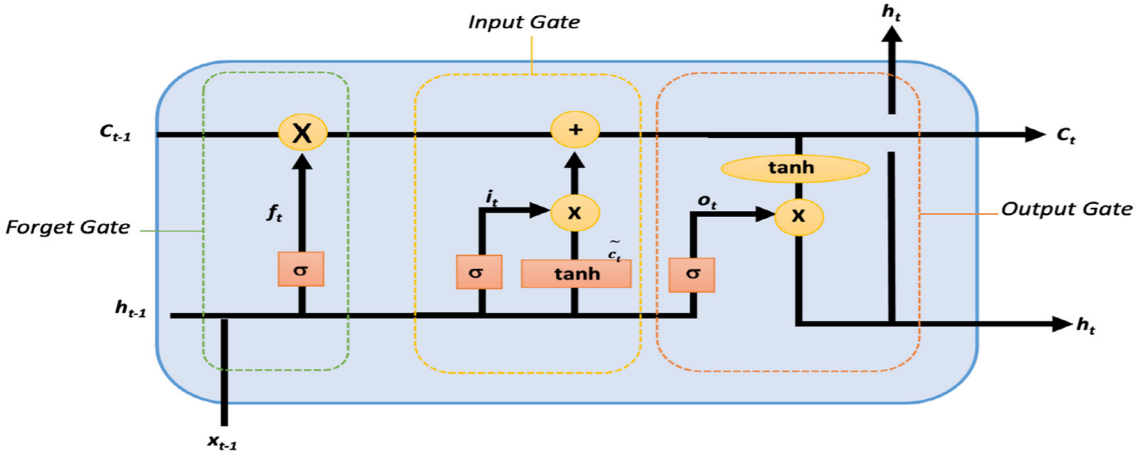

FIGURE 2
Internal architecture of a single LSTM cell.

as shown in Equation 4.

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \quad (2)$$

$$\tilde{C}_t = \tanh(W_i \cdot [h_{t-1}, x_t] + b_i) \quad (3)$$

$$C_t = f_t C_{t-1} + i_t \tilde{C}_t \quad (4)$$

Here, W_i denotes weight matrices that are produced from sigmoid function, and b_i denotes the input gate bias. The output gate controls the require output O_t using the expression in Equations 5, 6.

$$h_t = O_t \tanh(C_t) \quad (5)$$

$$O_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \quad (6)$$

Where W_o and b_o are the weighted matrices of the output gate and LSTM bias, respectively.

3 Materials and methods

With the rapid adoption of remote healthcare services, the risk of cyberattacks and data tampering has increased significantly. The main endeavor of this research is to detect and analyze hidden embeddings in medical images for secure medical data transmission. By continuously analyzing incoming medical images using AI-driven image steganalysis, data security and privacy risks can be minimized. In our proposed architecture, LSTMs were fused within the CNN by replacing the fully connected layers. The idea was to capture and rank the correlation between different stego-noises and to reduce the number of trainable parameters for time efficient classification.

3.1 Pre-processing BOSSBase 1.01 and BOWS 2 databases

For the experiments, Break Our Steganographic System (BOSSBase 1.01) (34) and Break Our Watermarking System (BOWS 2) (35) databases were used. Each database has 10,000 cover images in a Portable Gray Map (PGM) format. The data were prepared by resizing all images to 256 × 256 pixels (36). Then, a corresponding steganographic image for each cover image was generated using with payloads of 0.4 bits per pixel (bpp). In the next stage, the data were partitioned to training, validation, and testing sets. 4,000 images were used pairs for training, 1,000 for validation, and 5,000 for testing purposes. Both datasets were merged to generate a database of 20,000 images in which split 14,000 images were used for training (10,000 BOWS 2 + 4,000 BOSSBase 1.01), 1,000 pairs for validation (BOSSBase 1.01), and 5,000 for testing (BOSSBase 1.01).

3.2 Pre-processing ALASKA2 image steganalysis database

ALASKA2 dataset was chosen due to its massive size and heterogeneous nature for an in-depth validation of our proposed steganalysis algorithm. In this dataset, steganography algorithms transform data with an unknown payload. All the images were resized to 256×256 pixels and compressed with JPEG quality factors of 95, 90, and 75. This database is available on Kaggle platform (37). ALASKA2 database includes 7,500 pairs of images in JPEG format (cover and stego) which were randomly shuffled before partition. We prepared the ALASKA2 database by portioning split 6,000 pairs for training, 1500 pairs for validation, and 7,500 pairs were randomly chosen testing purposes. Furthermore, we prepared another ALASKA2 dataset by using all images via three steganographic algorithms. This database was partitioned in which 9,000 pairs were used for training, 2,250 pairs for validation, and 11,250 pairs for validations.

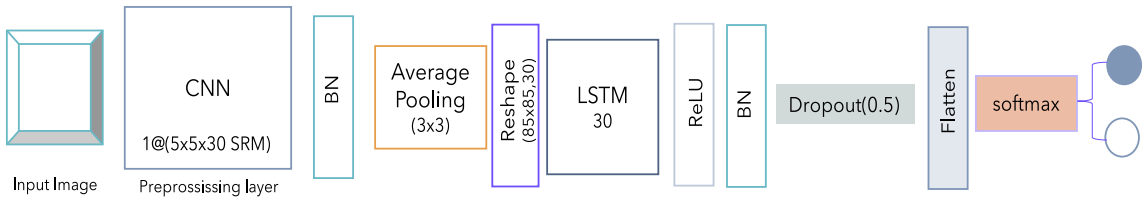

FIGURE 3
Schematic illustration of LSTM for feature representations and classification.

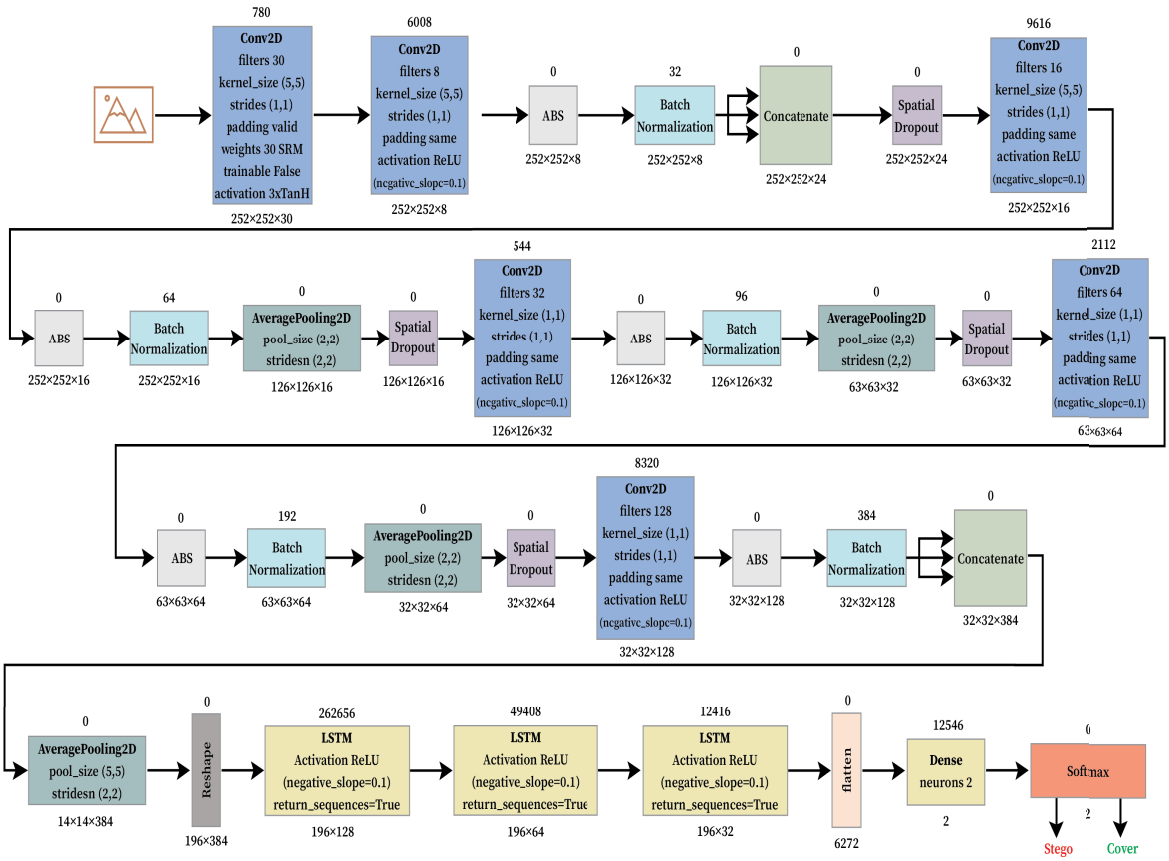

FIGURE 4
Proposed LSTM fused Xu-Net neural network architecture for secured telemedicine.

3.3 Proposed LSTM fused CNN architecture

Initially, we establish the effectiveness of LSTM for steganalysis in securing telemedicine communications and then integrate it into a CNN architecture to enhance both detection accuracy and processing efficiency. Given the critical need for real-time threat detection in remote healthcare, we provide a detailed analysis and comparison with state-of-the-art architectures to assess our model's capability. To simulate real-world security threats in telemedicine, we embedded noise in cover images using five steganographic algorithms. Two of them are spatial steganographic algorithms: S-UNIWARD (38) and WOW (39) with 0.4 bpp payloads. The other three are transform steganographic algorithms: JMiPOD (40), JUNIWARD (38), and UERD (41). Our implementation ensures robust steganalysis for secure medical image transmission.

Our initial approach investigates the applicability of LSTM in image steganalysis and is presented in Figure 3. It starts with an input image, which is first passed through a preprocessing layer using a convolutional neural network (CNN) filter of dimensions ($5 \times 5 \times 30$), indicating the use of 30 SRM (Spatial Rich Model) filters for extracting high-frequency residuals. This is followed by

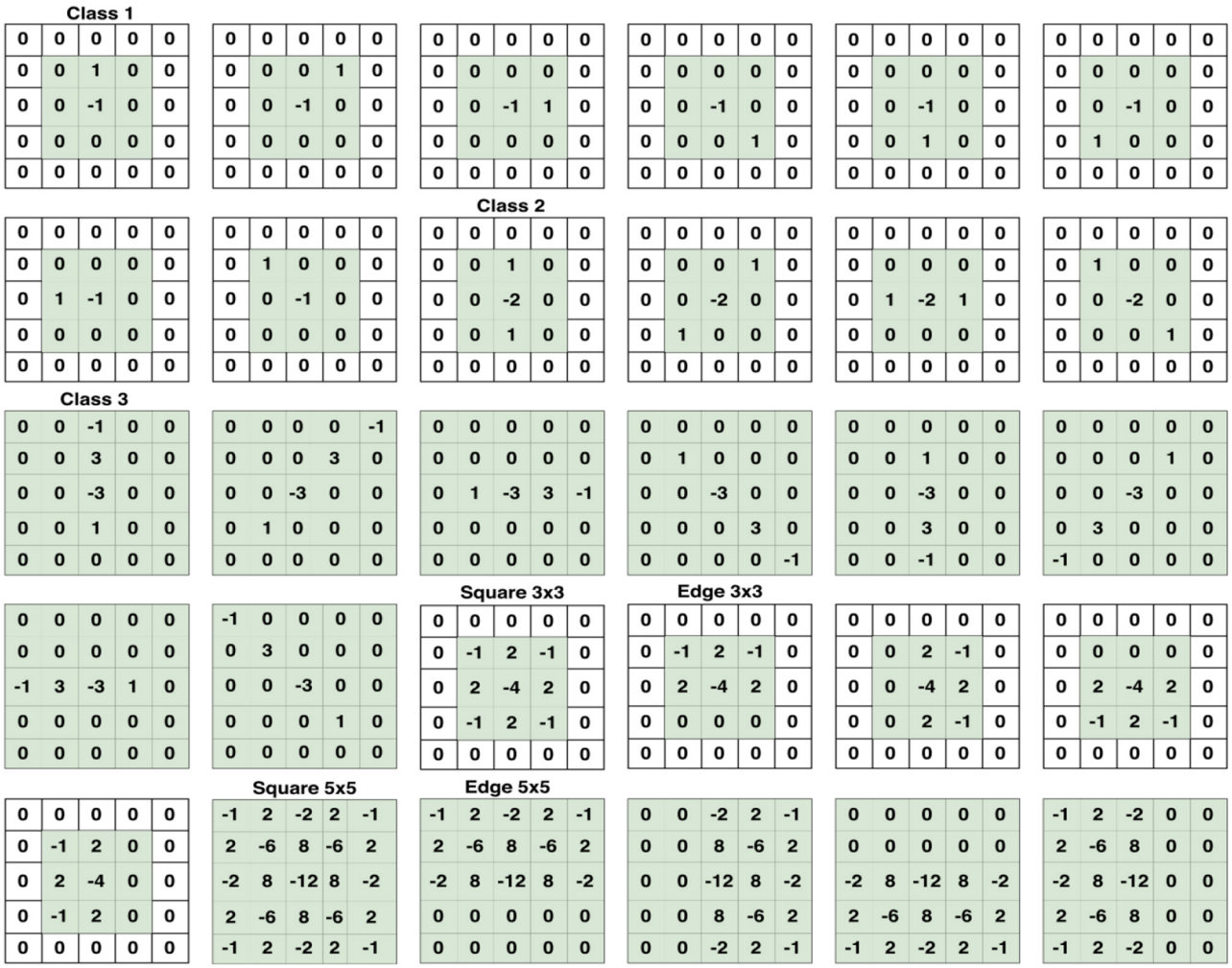

FIGURE 5
Set of 30 SRM Filters per category which are used in the first convolution, or preprocessing stage. Taken from Reinel et al. (22).

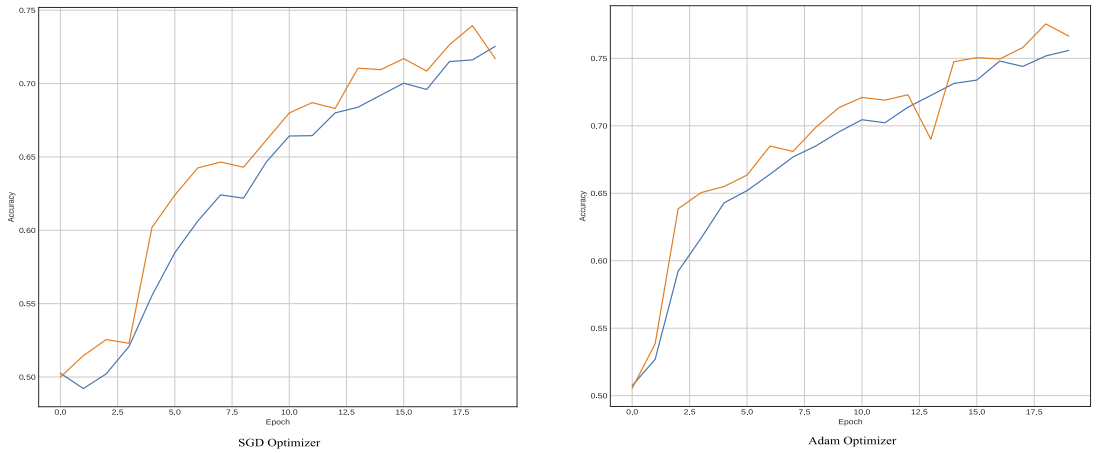

FIGURE 6
Training plots in terms of accuracy for Yedroudj-Net Model using LSTM as a classifier with BOSSBase 1.01 WOW 0.4 bpp.

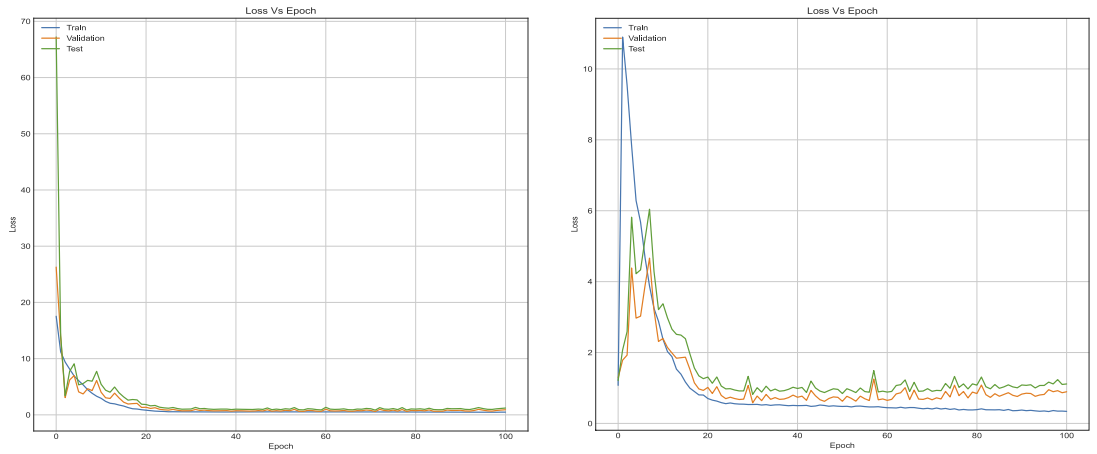

FIGURE 7
Training curves in terms of learning loss for the first method, when using stacked LSTM and FC layers in the classification stage, respectively. With BOSSBase 1.01 S-UNWARD 0.4 bpp.

TABLE 1 Accuracy percentage and number of trainable parameters of the fist method model, when using FC layer and LSTM layer for the S-UNWARD steganographic algorithm with payload 0.4 bpp using BOSSBase 1.01 database.

Scenario	with LSTM	with FC
Training Acc.	75%	**85%**
Validation Acc.	**76%**	75%
Test Acc.	**67%**	**67%**
# Trainable parameters	**433,592**	434,522

The best performances are shown in bold for each scenario.

TABLE 2 Accuracy percentage and loss value of the fist method model, when using FC layer and LSTM layer for ALASKA2 database.

Scenario	with LSTM		with FC	
Database	Acc.	Loss	Acc.	loss
JMiPOD	62%	**.99**	**65%**	1.45
JUNIWARD	60%	**1.00**	**62%**	1.00
UERD	61%	**0.90**	**63%**	0.94
ALASKA2_All	**49%**	**1.00**	46%	1.7

The best performances are shown in bold for each scenario.

batch normalization (BN) to stabilize and accelerate training. Next, average pooling with a 3×3 kernel is applied to reduce spatial dimensions while preserving critical features. This is then reshaped into a sequence format (65×30), which is suitable for temporal modeling via LSTM. After reshaping, the feature map is fed into an LSTM layer with 30 units as illustrated in Figure 3. The output of LSTM is passed through a ReLU activation to introduce non-linearity, followed by another batch normalization to standardize feature distributions. A dropout layer with a rate of 0.5 is included to prevent overfitting by randomly deactivating neurons during the training. The resulting features are flattened into a one-dimensional vector and are further passed through a Softmax classifier. This architecture combines the spatial feature extraction capability of CNNs with the sequential modeling strength of LSTMs, making it particularly robust for detecting subtle patterns in stego and manipulated images.

After the initial proof of concept regarding LSTM architecture for steganalysis, we fused LSTM as a classifier into the CNN architecture by replacing its three fully connected layers which is presented in Figure 4. The model begins with a convolutional preprocessing layer using fixed SRM filters, which are effective in extracting the noise residuals from the images. These initial outputs are passed through several convolutional blocks, each containing Conv2D layers, batch normalization, and spatial dropout. It is further followed by average pooling to reduce spatial dimensions while maintaining the important feature structures. The model uses concatenation operations to merge different channels for a multi-level residual learning. After the hierarchical CNN feature extraction, the architecture transitions into a temporal modeling phase using LSTM layers. Before entering the LSTM block, features are reshaped and passed through an average pooling 2D layer. The sequence of two LSTM layers allows the model to capture long-range dependencies across spatially transformed image features. The final output from the LSTM is flattened and passed into a dense layer with two neurons, corresponding to a binary classification: Stego and Cover. A softmax layer provides probabilistic outputs for the final decision. This hybrid CNN-LSTM design, coupled with residual modeling, makes the architecture well-suited for subtle signal detection tasks.

For this experiment, four famous and recent CNNs for image steganalysis were used, which include Xu-Net (24), Ye-Net (15), Yedroudj-Net (18), and Zhu-Net (26). SRM filters were used to improve the ratio of stego- to image-noise signal. Since the stego signal is always embedded in the high-frequency part of an image, we utilized these filters to initialize the kernels of a convolutional

TABLE 3 Accuracy percentage of the second method models for the S-UNWARD steganographic algorithm with payload 0.4 bpp.

Dataset	BOSSBase 1.01			BOSSBase 1.01+ BOWS		
results	Original	Strategy	With LSTM	Original	Strategy	With LSTM
Xu-Net	73%	78%	76%	–	82%	81%
Ye-Net	68%	81%	80%	–	83%	81%
Yedroudj-Net	77%	79%	79%	–	84%	82%
Zhu-Net	84.5%	78.6%	80.7%	–	86%	81.3%

TABLE 4 Accuracy percentage of the second method models for the WOW steganographic algorithm with payload 0.4 bpp.

Dataset	BOSSBase 1.01			BOSSBase 1.01+ BOWS		
Results	Original	Strategy	With LSTM	Original	Strategy	With LSTM
Xu-Net	79%	82%	81%	–	85%	83%
Ye-Net	75%	84%	83%	–	86%	85%
Yedroudj-Net	84%	85%	83%	–	86%	85%
Zhu-Net	88.1%	82.9%	83.5%	–	75%	83.5%

layer. A bulk of 30 high-pass filters from the SRM are used in the pre-processing block prior to feature extraction phase as indicated in Figure 5.

Experimental implementations used Python 3.8.1 and TensorFlow 2.2.0. In our model using LSTM only, network was trained for 100 epochs using S-UNWARD steganography with payload 0.4 bpp (BOSSBase 1.01 dataset). The LSTM fused CNN implementations presented in Figure 4 used the Google Colaboratory platform on Tesla P100 PCIe (16 GB) having CUDA Version 10.1 with 32 GB RAM to speed up simulations.

4 Results and discussion

4.1 Validation of LSTM classifier on BOSSBase 1.01, BOWS 2, and ALASKA2 dataset

To ensure reliable telemedicine, the LSTM classifier was trained for 100 epochs on the BOSSBase 1.01 and BOWS 2 databases and 50 epochs on the ALASKA2 database. A batch size of 64 images was used, with the Stochastic Gradient Descent (SGD) optimizer set at a momentum of 0.95 and an initial learning rate of 0.005. The training curves, illustrating accuracy and learning loss, are presented in Figure 6. Our model incorporates gating mechanisms to regulate gradients, enabling the architecture to retain critical information necessary for detecting hidden threats in transmitted medical images. This ability to learn and preserve information over extended sequences enhances the reliability of telemedicine via secure data transmission.

Figure 7 reflects the loss function which is binary cross entropy. The results indicate that LSTM model reaches saturation in a time-efficient manner very as the training data hyperparameters were tuned quickly. The gap between validation loss and the training loss using LSTM model is indicative of the fact that LSTM have the ability to adapt to diverse datasets and can generalize to new data. Moreover, the loss value of LSTM model is small and less than that of FC model. The classification accuracy and number of trainable parameters are reported in Table 1 with a fully connected layer and hybrid LSTM for S-UNWARD steganographic algorithm. As presented in Table 1, the fully connected model achieves higher training accuracy (85%) as compared to the LSTM-based model (75%), which suggests that the FC model is better at fitting the training data. However, the similarity in test accuracy between both models indicates that the FC model suffers from overfitting. This is due to specific patterns in the training set that do not generalize well to the unseen data. In contrast, the LSTM model with its inherent regularization via likely promotes better generalization despite its lower training accuracy. This behavior is consistent with the hypothesis that the FC model's capacity to memorize leads to overfitting, while the LSTM model trades some training performance for improved robustness to the unseen data.

Table 2 provides the accuracy and loss results of the CNNs when using either of fully connected (FC) layer or LSTM layer for ALASKA2 databases. Similarly, LSTM classifier outperforms FC on ALASKA2 dataset.

4.2 Validation of LSTM fused CNN architecture against BOSSBase 1.01, BOWS 2, and ALASKA2 dataset

In our proposed model for secure telemedicine, the training batch size was set to 64 images for Xu-Net, Ye-Net, and Yedroudj-Net, while Zhu-Net utilized a batch size of 32. These mini-batches optimize computational efficiency, ensuring rapid and scalable analysis of medical images in remote healthcare environments. To enhance model stability and accuracy in detecting hidden threats in transmitted medical data, we trained Xu-Net, Ye-Net, and

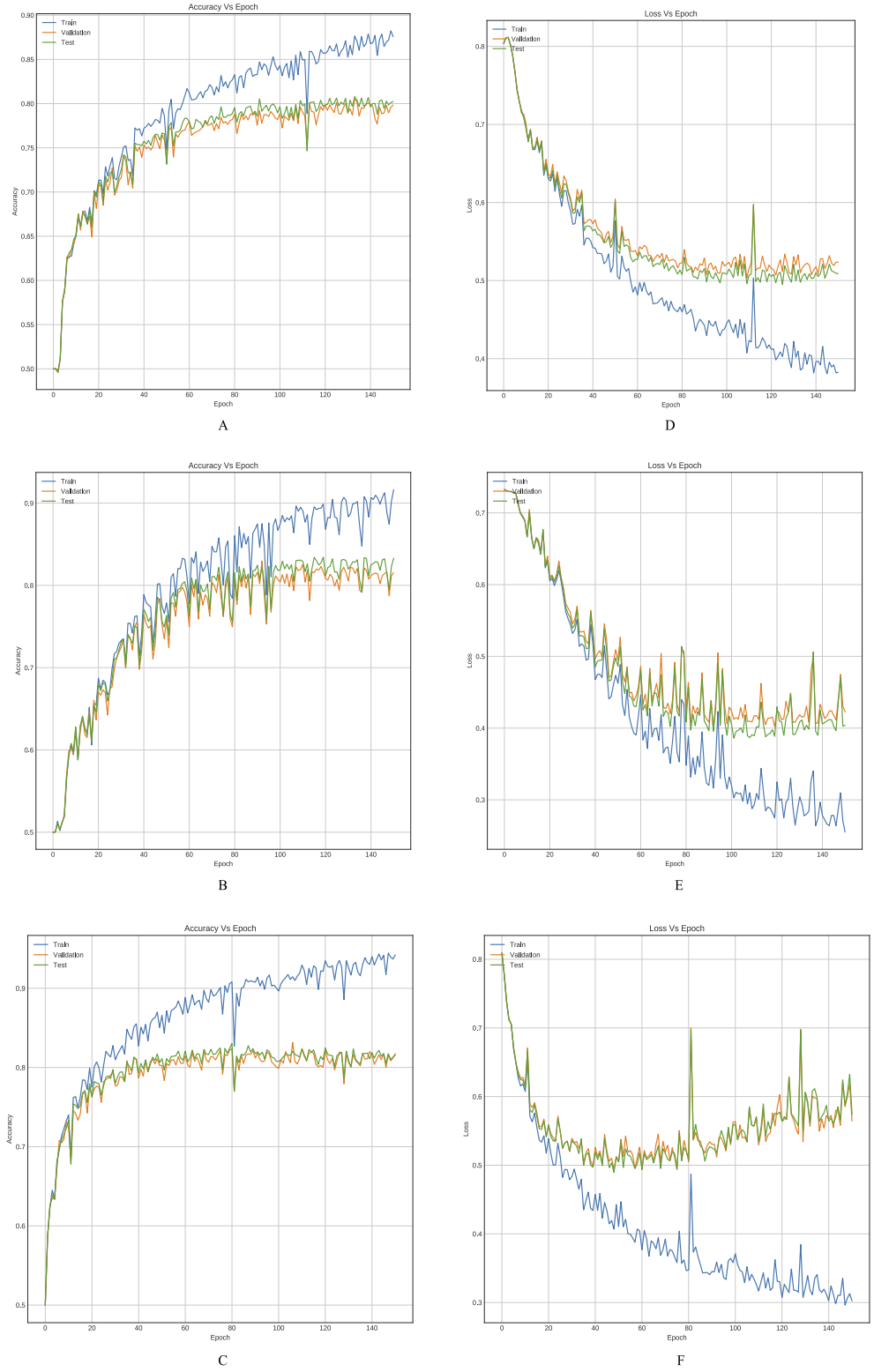

FIGURE 8
Training curves, **(A–C)** reflect the accuracy, and **(D–F)** reflect the learning loss for Xu-Net based on LSTM, Ye-Net based on LSTM, and Yedroudj-Net based on LSTM, respectively, with BOSSBase 1.01 WOW 0.4 bpp.

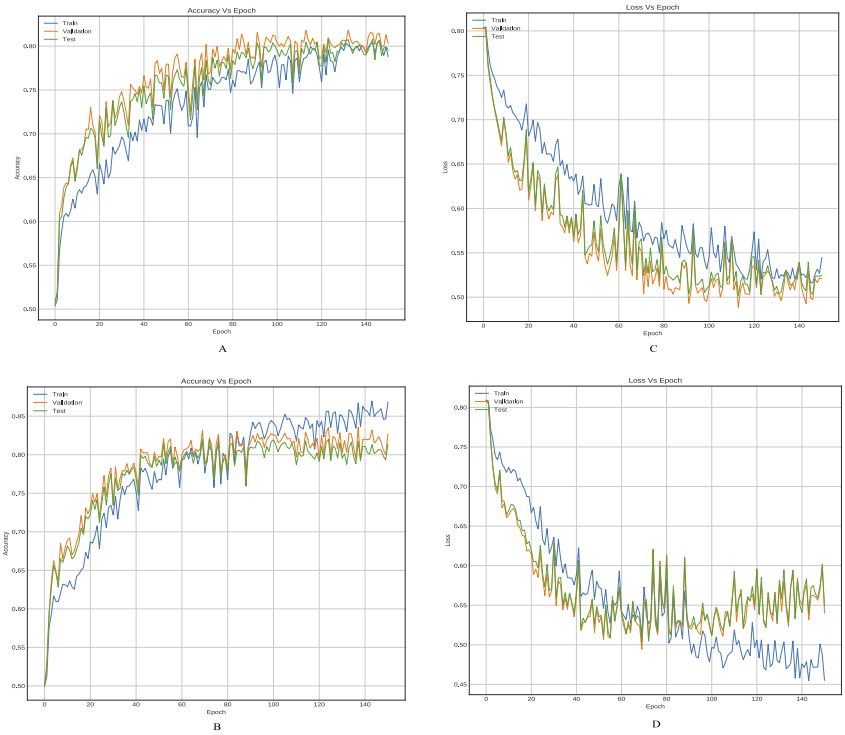

FIGURE 9
Training curves, **(A, B)** reflect the accuracy, and **(C, D)** reflect the learning loss for Xu-Net based on LSTM, and Yedroudj-Net based on LSTM, respectively, with BOSSBase 1.01 + BOWS 2 S-UNWARD 0.4 bpp.

Yedroudj-Net for 150 epochs, while Zhu-Net was trained for 70 epochs. A spatial dropout rate of 0.1 was applied across all layers to prevent overfitting, and batch normalization was configured with a momentum of 0.2, epsilon of 0.001, and renorm momentum of 0.4. The Adam optimizer, with a learning rate of 0.001, beta 1 of 0.9, beta 2 of 0.999, and an epsilon value of $1e-08$, was employed to ensure efficient convergence. To reinforce security in telemedicine image transmission, all layers were regularized for weights and bias, enabling the model to detect anomalies and steganographic threats in real-time. The accuracy results for both the S-UNWARD and WOW steganographic algorithms, which assess the model's ability to identify hidden data in medical images, are presented in Tables 3, 4.

Tables 3, 4 provide an inter-comparison between the accuracy of our proposed LSTM fused CNN architecture with the reported results (36). We achieved a high agreement between strategy and our model in terms of accuracy. The results highlighted in Tables 3, 4 are extracted from Figures 8, 9.

Trainable parameters refer to those parameters which can be learned and updated during the training cycle and has direct relationship with the computation time. Table 5 presents the number of trainable parameters for each model when applying the strategy reported in Tabares-Soto et al. (36) and when we used our proposed hybrid LSTM model.

The results presented in Table 5 confirm that our proposed model significantly decreased the number of trainable parameters as compared to leading available models and hence the computational effort required.

TABLE 5 Number of trainable parameters for state-of-the-arts architectures.

Results	Based on FC		Based on LSTM	
#Trainable parameters	Total	Classification stage	Total	Classification stage
Xu-Net	86,554	59,616	**39,418**	**0**
Ye-Net	**87,562**	22,752	118,570	**0**
Yedroudj-Net	251,110	59,616	**203,974**	**0**
Zhu-Net	275,684	59,616	**265,156**	**0**

The best results are shown in bold for each scenario.

5 Conclusion

Our proposed architecture proves to be highly effective in capturing complex interrelations among different features, making it a viable choice for steganalysis in telemedicine. Experiments conducted on BOSSBase 1.01, BOWS, and ALASKA2 datasets validate that our model demonstrates strong adaptability and generalization capabilities, which are essential for detecting hidden manipulations in telemedicine imaging systems. The achieved validation loss characteristics further reinforce the robustness of our approach in identifying steganographic threats in medical data transmission. A comparative analysis with leading architectures highlights that our model achieves significant dimensionality reduction in terms of training parameters, making it more efficient

without compromising accuracy. This efficiency is critical for real-time telemedicine applications.

However, we acknowledge that the current study does not include validation on real-world clinical datasets or standard medical image formats such as DICOM. Addressing this limitation forms a key part of our future work, where we aim to evaluate the model's performance on actual clinical imaging data to strengthen its practical applicability in telemedicine settings. By continuing to refine and expand our approach, we can contribute to a more secure and reliable telemedicine ecosystem.

Data availability statement

Publicly available datasets were analyzed in this study. The code is available on GitHub: https://github.com/DrDoaaSh/phd-code.git. The data set used to reproduce the results can be downloaded from this link: 10.5281/zenodo.4884116 or from this link https://drive.google.com/drive/folders/18KaJnn432D89WJarNY5NCTAxZB2Z3nw7?usp=drive_link.

Author contributions

DS: Project administration, Data curation, Formal analysis, Methodology, Investigation, Validation, Conceptualization, Writing – original draft. MA: Project administration, Supervision, Conceptualization, Resources, Writing – review & editing.

Funding

The author(s) declare that financial support was received for the research and/or publication of this article. This research was funded by the Cybersecurity Research and Innovation Pioneers Grants Initiative, National Program for Research, Development, and Innovation (RDI) in Cybersecurity, Kingdom of Saudi Arabia, under Grant Number CRPG-25-2030.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Gen AI was used in the creation of this manuscript.

Publisher's note

References

1. Magdy M, Hosny KM, Ghali NI, Ghoniemy S. Security of medical images for telemedicine: a systematic review. *Multimed Tools Appl*. (2022) 81:25101–45. doi: 10.1007/s11042-022-11956-7

2. Hameed MA, Hassaballah M, Bekhet S, Kenk MA, et al. A high quality secure medical image steganography method. In: *2023 3rd International Conference on Computing and Information Technology (ICCIT)*. Tabuk: IEEE (2023). p. 465–70. doi: 10.1109/ICCIT58132.2023.10273950

3. Saidi H, Tibermacine O, Elhadad A. High-capacity data hiding for medical images based on the mask-RCNN model. *Sci Rep*. (2024) 14:7166. doi: 10.1038/s41598-024-55639-9

4. Abdulla AA. Digital image steganography: challenges, investigation, and recommendation for the future direction. *Soft Comput*. (2024) 28:8963–76. doi: 10.1007/s00500-023-09130-8

5. Sirisha BL, Ahamed SF, Aruna V. Patient data hiding and transmitting during COVID-19 for telemedicine application using image steganography. *Curr Med Imaging*. (2024) 20:e15734056276785. doi: 10.2174/0115734056276785240229073917

6. Mansour RF, Girgis MR. Steganography-based transmission of medical images over unsecure network for telemedicine applications. *Comput Mater Contin*. (2021) 68:4069–85. doi: 10.32604/cmc.2021.017064

7. Mansour RF, Abdelrahim EM. An evolutionary computing enriched RS attack resilient medical image steganography model for telemedicine applications. *Multidimens Syst Signal Process*. (2019) 30:791–814. doi: 10.1007/s11045-018-0575-3

8. Le Guern N. Les développements récents de la photographie: de la menace des smartphones au potentiel démesuré de l'IA. *Marché Organ*. (2025) 52:217–47. doi: 10.3917/maorg.pr1.0117

9. Shehab DA, Alhaddad MJ. Comprehensive survey of multimedia steganalysis: techniques, evaluations, and trends in future research. *Symmetry*. (2022) 14:117. doi: 10.3390/sym14010117

10. Himthani V, Dhaka VS, Kaur M, Rani G, Oza M, Lee HN. Comparative performance assessment of deep learning based image steganography techniques. *Sci Rep*. (2022) 12:16895. doi: 10.1038/s41598-022-17362-1

11. Jahromi ZT, Hasheminejad SMH, Shojaedini SV. Deep learning semantic image synthesis: a novel method for unlimited capacity, high noise resistance coverless video steganography. *Multimed Tools Appl*. (2024) 83:17047–65. doi: 10.1007/s11042-023-16278-w

12. Telli M, Othmani M, Ltifi H. A new approach to video steganography models with 3D deep CNN autoencoders. *Multimed Tools Appl*. (2024) 83:51423–39. doi: 10.1007/s11042-023-17358-7

13. Ding K, Hu T, Niu W, Liu X, He J, Yin M, et al. A novel steganography method for character-level text image based on adversarial attacks. *Sensors*. (2022) 22:6497. doi: 10.3390/s22176497

14. Zhuo P, Yan D, Ying K, Wang R, Dong L. Audio steganography cover enhancement via reinforcement learning. *Signal Image Video Process*. (2024) 18:1007–13. doi: 10.1007/s11760-023-02819-1

15. Ye J, Ni J, Yi Y. Deep learning hierarchical representations for image steganalysis. *IEEE Trans Inf Forensics Secur*. (2017) 12:2545–57. doi: 10.1109/TIFS.2017.2710946

16. Deng X, Chen B, Luo W, Luo D. Fast and effective global covariance pooling network for image steganalysis. In: *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*. New York, NY: ACM (2019). p. 230–4. doi: 10.1145/3335203.3335739

17. Wu S, Zhong S, Liu Y. Deep residual learning for image steganalysis. *Multimed Tools Appl*. (2018) 77:10437–53. doi: 10.1007/s11042-017-4440-4

18. Yedroudj M, Comby F, Chaumont M. Yedroudj-net: an efficient CNN for spatial steganalysis. In: *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. Calgary, AB: IEEE (2018). p. 2092–6. doi: 10.1109/ICASSP.2018.8461438

19. Boroumand M, Chen M, Fridrich J. Deep residual network for steganalysis of digital images. *IEEE Trans Inf Forensics Secur*. (2018) 14:1181–93. doi: 10.1109/TIFS.2018.2871749

20. Zhang X, Kong X, Wang P, Wang B. Cover-source mismatch in deep spatial steganalysis. In: *International Workshop on Digital Watermarking*. Cham: Springer (2019). p. 71–83. doi: 10.1007/978-3-030-43575-2_6

21. Wang L, Xu X, Gui R, Yang R, Pu F. Learning rotation domain deep mutual information using convolutional LSTM for unsupervised PolSAR image classification. *Remote Sens*. (2020) 12:4075. doi: 10.3390/rs12244075

22. Reinel TS, Brayan AAH, Alejandro BOM, Alejandro MR, Daniel AG, Alejandro AGJ, et al. GBRAS-Net: a convolutional neural network architecture for spatial image steganalysis. *IEEE Access*. (2021) 9:14340–50. doi: 10.1109/ACCESS.2021.3052494

23. Zhu Y, Wang X, Chen HS, Salloum R, Kuo CCJ. Green steganalyzer: a green learning approach to image steganalysis. *APSIPA Trans Signal Inf Process*. (2023) 12:e41. doi: 10.1561/116.00000136

24. Xu G, Wu HZ, Shi YQ. Ensemble of CNNs for steganalysis: an empirical study. In: *Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security*. New York, NY: ACM (2016). p. 103–7. doi: 10.1145/2909827.2930798

25. Qian Y, Dong J, Wang W, Tan T. Deep learning for steganalysis via convolutional neural networks. In: *Media Watermarking, Security, and Forensics 2015, Vol. 9409*. SPIE (2015). p. 171–80. doi: 10.1117/12.2083479

26. Zhang R, Zhu F, Liu J, Liu G. Depth-wise separable convolutions and multi-level pooling for an efficient spatial CNN-based steganalysis. *IEEE Trans Inf Forensics Secur*. (2019) 15:1138–50. doi: 10.1109/TIFS.2019.2936913

27. Öztürk Ş, Özkaya U. Gastrointestinal tract classification using improved LSTM based CNN. *Multimed Tools Appl*. (2020) 79:28825–40. doi: 10.1007/s11042-020-09468-3

28. Ozdemir T, Taher F, Ayinde BO, Zurada JM, Tuzun Ozmen O. Comparison of feedforward perceptron network with LSTM for solar cell radiation prediction. *Appl Sci*. (2022) 12:4463. doi: 10.3390/app12094463

29. You W, Zhang H, Zhao X. A siamese CNN for image steganalysis. *IEEE Trans Inf Forensics Secur*. (2020) 16:291–306. doi: 10.1109/TIFS.2020.3013204

30. Islam MZ, Islam MM, Asraf A. A combined deep CNN-LSTM network for the detection of novel coronavirus (COVID-19) using X-ray images. *Inform Med Unlocked*. (2020) 20:100412. doi: 10.1016/j.imu.2020.100412

31. Wang L, Xu X, Dong H, Gui R, Yang R, Pu F. Exploring convolutional LSTM for PolSAR image classification. In: *IGARSS 2018-2018 IEEE International Geoscience and Remote Sensing Symposium*. Valencia: IEEE (2018). p. 8452–5. doi: 10.1109/IGARSS.2018.8518517

32. Li P, Tang H, Yu J, Song W. LSTM and multiple CNNs based event image classification. *Multimed Tools Appl*. (2021) 80:30743–60. doi: 10.1007/s11042-020-10165-4

33. Zhuang N, Qi GJ, Kieu TD, Hua KA. Differential recurrent neural network and its application for human activity recognition. *arXiv*. (2019) [Preprint] arXiv:1905.04293. doi: 10.48550/arXiv.1905.04293

34. Bas P, Filler T, Pevnỳ T. "Break our steganographic system": the ins and outs of organizing BOSS. In: *International Workshop on Information Hiding*. Cham: Springer (2011). p. 59–70. doi: 10.1007/978-3-642-24178-9_5

35. Piva A, Barni M. The first BOWS contest (break our watermarking system). In: *Security, Steganography, and Watermarking of Multimedia Contents IX, Vol. 6505*. SPIE (2007). p. 425–34. doi: 10.1117/12.704969

36. Tabares-Soto R, Arteaga-Arteaga HB, Mora-Rubio A. Bravo-Ortíz MA, Arias-Garzón D, Grisales JAA, et al. Strategy to improve the accuracy of convolutional neural network architectures applied to digital image steganalysis in the spatial domain. *PeerJ Comput Sci*. (2021) 7:e451. doi: 10.7717/peerj-cs.451

37. Kaggle. *ALASKA2 Image Steganalysis*. (2020). Available online at: https://www.kaggle.com/c/alaska2-image-steganalysis (Accessed February 20, 2023).

38. Holub V, Fridrich J, Denemark T. Universal distortion function for steganography in an arbitrary domain. *EURASIP J Inf Secur*. (2014) 2014:1–13. doi: 10.1186/1687-417X-2014-1

39. Fridrich J, Kodovsky J. Rich models for steganalysis of digital images. *IEEE Trans Inf Forensics Secur*. (2012) 7:868–82. doi: 10.1109/TIFS.2012.2190402

40. Cogranne R, Giboulot Q, Bas P. Steganography by minimizing statistical detectability: The cases of JPEG and color images. In: *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security*. New York, NY: ACM (2020). p. 161–7. doi: 10.1145/3369412.3395075

41. Guo L, Ni J, Su W, Tang C, Shi YQ. Using statistical image model for JPEG steganography: uniform embedding revisited. *IEEE Trans Inf Forensics Secur*. (2015) 10:2669–80. doi: 10.1109/TIFS.2015.2473815