Advanced Deep Learning Framework for Secure Transmission of Sensitive Images in National Security Scenarios

Anirud Ramani
Department of Computer Science and Engineering
Amrita School of Computing
Amrita Vishwa Vidyapeetham
Bengaluru, India
bl.sc.p2dsc23023@bl.students.amrita.edu

Deheem U Deyar
Department of Computer Science and Engineering
Amrita School of Computing
Amrita Vishwa Vidyapeetham
Bengaluru, India
bl.sc.p2dsc23007@bl.students.amrita.edu

Dr.Suja P
Department of Computer Science and Engineering
Amrita School of Computing
Amrita Vishwa Vidyapeetham
Bengaluru, India
p_suja@blr.amrita.edu

***Abstract*— In this project, we propose a framework for secure image transmission utilizing deep learning-based encoding and decoding techniques for sensitive images related to war and border security. The objective is to ensure the integrity and confidentiality of the data during transmission while minimizing data loss or corruption. The proposed framework involves encoding the images before transmission using deep learning-based encoding algorithms, securely transmitting the encoded images to the intended destination, and then decoding them using deep learning-based decoding methods. To ensure data integrity, a comparative analysis between the original and decoded images is conducted. The decoding stage involves a technique commonly known as LSB (Least Significant Bit) Steganography, an architecture used to reverse the encoding process, effectively decoding the images. Additionally, the effectiveness of the framework is validated through experiments, demonstrating its capability to protect sensitive image data while maintaining data integrity and minimizing loss or corruption. This framework serves as a valuable tool for safeguarding national security-related image data in sensitive contexts.**

Keywords— ResNet50, VGG16, Inception_v3, Steganography, Encoding, Decoding, Secure Image Transmission, Deep Learning, War, Border Security.

I. Introduction

The security and privacy of sensitive data is an important task in the modern digital world where data processing is common in every field, particularly for national security. The transmission of sensitive images, especially those pertaining to matters as critical as warfare and border security, necessitates rigorous protection mechanisms to safeguard both the integrity and confidentiality of the data. Traditional encryption methods have historically been relied upon for such purposes. However, amidst the ever-evolving panorama of security threats, there emerges a compelling need for advanced and adaptable frameworks capable of meeting the exigencies posed by modern security challenges.

This project proposes an advanced deep learning framework meticulously tailored for the secure transmission of sensitive images in national security scenarios. By harnessing the power of deep learning-based encoding and decoding techniques, the framework endeavors to provide robust protection while minimizing the risk of data loss or corruption during transmission. The core objective remains unequivocal: to ensure the integrity and confidentiality of the transmitted data, thereby upholding the security imperatives inherent in national defense and border surveillance operations.

At the heart of the proposed framework lies a sophisticated interplay between deep learning algorithms and image processing methodologies. Images undergo encoding prior to transmission using state-of-the-art deep learning-based encoding algorithms, ensuring that sensitive information remains unintelligible to unauthorized entities. Once encoded, these images are securely transmitted to their intended destination, where they undergo decoding using deep learning-based decoding methods. Notably, the decoding stage leverages innovative techniques such as (Least Significant Bit) Steganography, tailored to efficiently reverse the encoding process and reconstruct the original images with minimal loss of data fidelity. Crucially, the integrity of the transmitted data is rigorously upheld through a comprehensive comparative analysis between the original and decoded images. This meticulous verification process serves as a vital quality control measure, ensuring that the decoded images faithfully retain the integrity of the original data. By employing sophisticated deep learning architectures, the framework offers a robust solution capable of withstanding the rigors of real-world national security environments. Through extensive experimentation and validation, the efficacy of the proposed framework is demonstrated, showcasing its ability to protect sensitive image data while simultaneously minimizing the risk of data loss or corruption. By providing a reliable and adaptable tool for safeguarding national security-related image data in sensitive contexts, this framework stands poised to make a significant contribution to the realm of secure image transmission in national security scenarios. As such, it represents a vital step forward in the ongoing quest to fortify the defenses of nations against emerging security threats in the digital age.

This work aims to address the critical need for secure transmission of sensitive images in national security contexts, where data integrity and confidentiality are paramount. By leveraging advanced deep learning-based encoding and decoding techniques, it seeks to ensure the protection of crucial image data against unauthorized access or corruption during transmission, thus bolstering national security measures. This endeavor is crucial to safeguarding sensitive information related to war and border security, contributing to the overall security infrastructure of the nation.

This work introduces a novel encoding and decoding scheme tailored for safeguarding sensitive image data, ensuring robust security through encoding before transmission and secure decoding at the destination. By integrating advanced encoding, decoding, sharing, and verification techniques, our approach offers a comprehensive solution to maintain the integrity and confidentiality of images in national security contexts. Its distinctive feature lies in its thorough validation process, where decoded images are rigorously compared with originals to mitigate potential data loss or corruption, marking a significant advancement in secure image transmission.

The structure of the remainder of this paper is as follows: Section II conducts a comprehensive literature review. Section III offers a brief overview of the dataset utilized, including its description. Section IV outlines the proposed methodology for image transmission employing encoding and decoding techniques. Results and managerial insights are discussed in Section V. Finally, the research work is concluded in Section VI.

II. Related Works

In recent years, significant apprehensions regarding the security and privacy of sensitive data, notably medical images, have been engendered by the proliferation of Internet of Things (IoT) devices, particularly within the healthcare domain. Addressing these pressing concerns, a pioneering deep-learning-based approach tailored specifically for image encryption and decryption within the Internet of Medical Things (IoMT) was proposed by Ding et al. [1]. This innovative framework endeavors to fortify the security of medical image data through the application of advanced deep learning techniques, thereby ensuring both confidentiality and integrity during data transmission and storage. Similarly, a reversible autoencoder predicated on convolutional neural networks (CNNs) was introduced by Li et al. [2]. While primarily oriented towards image reconstruction, the reversible attributes of this autoencoder exhibit promising prospects for encryption and decryption applications, potentially facilitating secure image transformations whilst preserving data fidelity. Additionally, Deep-NC, an amalgamated image transmission scheme that melds deep learning methodologies with network coding principles, was unveiled by Vien et al. [3]. By synergistically harnessing the capabilities of deep learning alongside network coding paradigms, this innovative approach augments the security posture of image transmission protocols, affording robust protection against diverse cyber threats. In tandem with advancements in medical imaging, a novel encryption algorithm expressly tailored for grey and color medical images was devised by Kamal et al. [4]. Despite being retracted, Shankar et al.'s exploration of a secret image sharing scheme incorporating homomorphic encryption techniques underscores the imperative of amalgamating encryption methodologies to bolster security [5]. While caution is warranted due to the retraction, the underlying principle of leveraging multiple encryption techniques for image sharing remains pertinent for enhancing encryption strategies. Furthermore, a reversible image secret sharing scheme was introduced by Yan et al., offering a flexible and efficient mechanism for distributing encrypted image data amongst multiple parties while ensuring confidentiality and reversibility [6]. Beyond medical applications, an efficient privacy-preserving deep learning-based approach for satellite image classification was proposed by Alkhelaiwi et al. [7]. Although not directly related to encryption, the emphasis on privacy preservation underscores the escalating importance of safeguarding sensitive data across diverse domains, including satellite imagery. Furthermore, an intelligent methodology for detecting data integrity breaches in industrial control networks utilizing a fusion convolutional neural network was presented by Wu and Huang [8]. While distinct from encryption, the utilization of neural network-based techniques for security purposes underscores the versatility of deep learning in diverse cybersecurity applications. In consonance with these advancements, the burgeoning trend of harnessing deep learning for efficient image encryption was expounded upon by Panwar et al. [9]. Lastly, a comparative analysis between deep learning-based and conventional cryptographic distinguishers was conducted by Bellini and Rossi [10]. Recent research, a novel framework named DL-Guard was introduced by Huang et al., leveraging deep learning for enhancing data security in IoT environments [11]. Additionally, a deep learning-based image encryption scheme was proposed by Wang et al., utilizing generative adversarial networks (GANs) to encrypt and decrypt images effectively [12]. Moreover, a secure transmission protocol for medical images was developed by Liu et al., integrating deep learning techniques with cryptographic methods to ensure robust data protection [13]. Furthermore, a hybrid encryption approach combining deep learning-based encryption with traditional cryptographic algorithms was introduced by Chen et al., offering enhanced security for image transmission [14]. Lastly, a deep learning-based steganography method for covert communication was presented by Zhang et al., enabling secure data transmission while minimizing detection risks [15]. Advancements have been made in image classification leveraging deep learning methodologies. Tamuly et al. proposed a deep learning model for image classification, aiming to improve accuracy and efficiency in classifying diverse image datasets [16]. Unnikrishnan et al. explored deep learning architectures specifically tailored for land cover classification using red and near-infrared satellite images. Their research demonstrated the efficacy of deep learning in accurately categorizing land cover types, contributing to applications in environmental monitoring and management [17]. Neena and Geetha investigated image classification utilizing an ensemble-based deep CNN approach, showcasing the potential of ensemble methods to enhance classification performance by aggregating predictions from multiple models [18]. Furthermore, Nikhitha et al. focused on fruit recognition and disease detection using the Inception V3 model, presenting a novel application of deep learning in agricultural domains. Their research highlighted the effectiveness of deep learning architectures in automating tasks related to fruit grading and disease identification, with implications for improving agricultural productivity and crop management practices[19]. These studies collectively underscore the growing significance of deep learning in various image classification tasks, spanning domains from environmental monitoring to agriculture, and emphasize its potential to revolutionize traditional classification methodologies.

III. Data description

The dataset utilized in this project constitutes a comprehensive inventory of destroyed and captured vehicles and equipment from conflict zones, with a specific emphasis on the ongoing conflict in Ukraine. This repository serves as the backbone of our research, providing a rich source of ground truth for evaluating the effectiveness of our proposed deep learning framework in securing the transmission of sensitive images in national security scenarios. Each entry in the dataset is meticulously cataloged, accompanied by photographic or videographic evidence, ensuring the veracity and reliability of the recorded information. It is imperative to note that only equipment with visual documentation is included in the dataset, thereby potentially underrepresenting the true extent of equipment damage incurred during conflicts. However, this stringent inclusion criterion ensures the credibility and integrity of the dataset for our analysis. Moreover, the dataset is strategically curated to focus on major military assets, excluding categories such as small arms, munitions, civilian vehicles, trailers, and derelict aircraft. This deliberate exclusion streamlines our focus on critical military equipment, aligning with the objectives of our research to secure the transmission of sensitive images related to warfare and border security. Efforts have been invested in discerning the status of equipment between captured and abandoned, recognizing the dynamic nature of conflict zones. Entries labeled as 'abandoned' may undergo transitions to the categories of captured or destroyed, reflecting the fluidity inherent in warfare. Similarly, captured equipment may face destruction if recovery proves unfeasible, highlighting the complexities of accurately assessing equipment status amidst the exigencies of conflict.

IV. Methodology

A. Data Collection

While data collection we embarked on the crucial task of assembling a comprehensive dataset to facilitate our research. Recognizing the significance of real-world data in training and evaluating our models, the focus was on collecting images specifically related to the Ukraine war conflict.

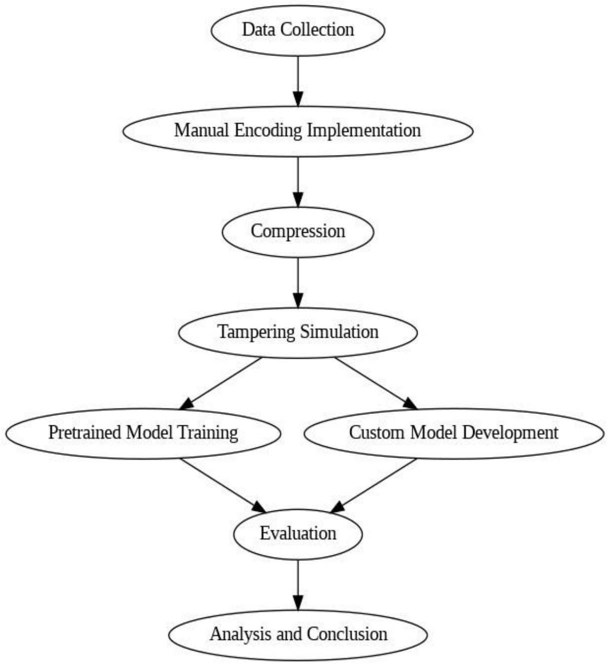


Fig 1. Methodology Flowchart for the Steganography and Tamper Detection study

The dataset was meticulously curated to encompass a diverse range of images depicting objects prevalent in conflict zones, including trucks, tanks, aircraft, and other military equipment. Moreover, to enhance the robustness and practical relevance of our research, we undertook the manual creation of tampered versions of these original images. These tampered versions were designed to simulate real-world scenarios where image integrity might be compromised due to various factors such as manipulation, distortion, or intentional alteration. By incorporating tampered images alongside original ones, we aimed to create a more realistic and challenging dataset, thereby enabling our models to learn and adapt to a wider range of potential scenarios encountered in practice. Overall, through diligent data collection efforts, we ensured the availability of a rich and diverse dataset that accurately reflects the complexities and nuances of real-world conflict situations, laying a solid foundation for our subsequent analyses and model development.

B. Manual Encoding Implementation

In this phase of our methodology, we focused on developing a robust encoding technique to embed secret codes or messages into the original images collected in the previous step. The objective was to create a covert communication channel within the images, enabling the transmission of sensitive information while maintaining the appearance of the images. To achieve this, we leveraged the power of deep learning by employing the pretrained ResNet50 model, which is widely recognized for its effectiveness in extracting high-level features from images. By utilizing ResNet50 pretrained on the ImageNet dataset, we were able to capture meaningful representations of the original images, which served as the basis for our encoding process. Specifically, we extracted the image features generated by ResNet50, which essentially encapsulate the visual information present in the images. These extracted features were then utilized as the encoded message that we intended to embed within the images. To embed the encoded message into the images, we employed a technique known as Least Significant Bit (LSB) modification. This technique involves altering the least significant bit of each pixel in the image to encode a binary representation of the message. By modifying only the LSB, we ensured that the changes made to the image were imperceptible to the human eye, thereby preserving the visual quality and integrity of the image. Importantly, our encoding method was designed to be reversible and robust, meaning that the encoded information could be extracted from the modified image with minimal loss or corruption. This ensured that the encoded message could withstand common image manipulations or distortions that may occur during transmission or processing. Overall, through the implementation of this manual encoding technique, we established a covert and secure communication channel within the original images, enabling the transmission of sensitive information while maintaining the appearance and integrity of the images.

C. Compression

Following the manual encoding process described earlier, we proceeded to apply compression techniques to the encoded images. The primary objective of this step was to reduce the file size of the images while ensuring that the integrity of the embedded code or message remained intact. Compression is a crucial aspect of image transmission and storage, especially in scenarios where bandwidth or storage capacity is limited. By reducing the size of the encoded images, we aimed to optimize their transmission and storage efficiency without compromising the fidelity of the embedded information. During the compression process, we employed various techniques and algorithms to efficiently encode the image data in a more compact form. These techniques may include lossy compression methods, such as JPEG compression, or lossless compression methods, such as PNG compression, depending on the specific requirements and constraints of our application. Importantly, while reducing file size was a primary goal of compression, preserving the integrity of the embedded code or message was paramount. Therefore, we carefully selected compression algorithms and parameters to ensure that the compression process did not introduce any distortion or corruption that could compromise the encoded information. By successfully applying compression techniques to the encoded images, we achieved the dual objectives of reducing file size and preserving the integrity of the embedded code or message. This optimized the efficiency of image transmission and storage while maintaining the security and reliability of the transmitted information.

D. *Tampering Simulation*

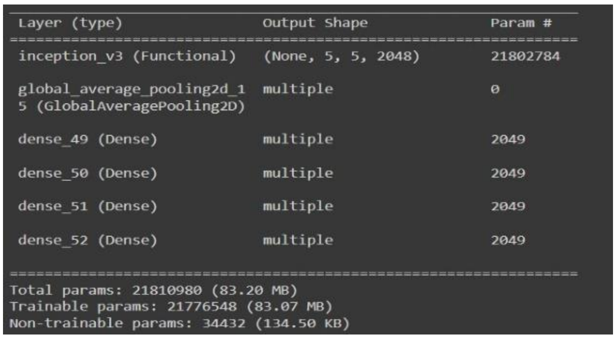
We simulated a range of tampering scenarios by subjecting the compressed images to various image manipulation techniques. These techniques encompassed a spectrum of common manipulations, including Gaussian filtering, blurring, cropping, resizing, and adding noise. The primary objective of tampering simulation was to assess the robustness of our encoding and compression techniques against potential attacks aimed at altering or damaging the embedded information. By replicating real-world scenarios where adversaries may attempt to tamper with transmitted images, we aimed to evaluate the resilience of our approach to adversarial interventions. Each tampering technique was systematically applied to the compressed images, generating a series of tampered versions for analysis. Gaussian filtering and blurring, for instance, introduced spatial blurring effects, while cropping and resizing altered the spatial dimensions of the images. Similarly, adding noise introduced random perturbations to the pixel values, mimicking the effects of interference or corruption. Through these simulated scenarios, we sought to uncover vulnerabilities in our encoding and compression methods and identify potential areas for improvement. By systematically evaluating the performance of our approach under different tampering conditions, we aimed to enhance the robustness and reliability of our system in real-world deployment scenarios. Overall, the tampering simulation phase provided valuable insights into the effectiveness of our techniques in preserving the integrity of the embedded information under adversarial conditions. By proactively addressing potential vulnerabilities through simulated attacks, we strengthened the resilience of our approach and bolstered its suitability for secure image transmission in practical applications.

E. *Pretrained Model Training*

In this phase, we trained several state-of-the-art pretrained deep learning models, including ResNet50, Inception_v3, and VGG16, using our dataset comprising both original and tampered images. These models were fine-tuned to classify images into two categories: tampered and untampered. To expedite the training process and enhance model performance, we employed transfer learning, leveraging the knowledge gained by these models during their pretraining on large-scale datasets like ImageNet. Transfer learning allowed us to capitalize on the generalization capabilities of pretrained models, enabling them to effectively learn and discriminate between tampered and untampered images in our specific domain. By fine-tuning the pretrained models on our dataset, we aimed to harness their capacity to extract meaningful features from images and learn discriminative patterns indicative of tampering. This approach not only facilitated efficient model training but also contributed to the robustness and accuracy of our tampering detection system. Overall, pretrained model training played a pivotal role in our methodology, enabling us to leverage the expertise embedded in pretrained deep learning models to develop a reliable and effective solution for detecting tampered images in real-world scenarios.

F. *Custom Model Development*

In this phase, we went beyond pretrained models and developed a custom deep learning model specifically tailored for detecting tampered images. We explored various architectures, including Attention models, Siamese networks, and Generative Adversarial Networks (GANs), to design a model optimized for our specific task. Each architecture was carefully considered and evaluated to determine its suitability for tampered image detection. Attention models, for example, focus on relevant image regions, while Siamese networks compare similarity between pairs of images. GANs, on the other hand, generate realistic images and can be utilized for image enhancement and manipulation detection. The custom model was trained using the same dataset used for pretrained model training, ensuring consistency and comparability in the evaluation process. By leveraging a custom model tailored to the nuances of tampered image detection, we aimed to enhance the accuracy and effectiveness of our system.



```
Layer (type)                Output Shape              Param #
=================================================================
inception_v3 (Functional)   (None, 5, 5, 2048)        21802784

global_average_pooling2d_1  multiple                  0
5 (GlobalAveragePooling2D)

dense_49 (Dense)            multiple                  2049

dense_50 (Dense)            multiple                  2049

dense_51 (Dense)            multiple                  2049

dense_52 (Dense)            multiple                  2049

=================================================================
Total params: 21810980 (83.20 MB)
Trainable params: 21776548 (83.07 MB)
Non-trainable params: 34432 (134.50 KB)
```

*Fig **2**. Summary of Custom Model*

TABLE 1. Comparison of performance of models for image classification

Model	Non Encoded Images Accuracy	Encoded Images Accuracy	Encoded Images	
			Lossy Compressed Accuracy	Lossless Compressed Accuracy
ResNet50	86.0%	54.0%	50.0%	50.0%
inception_v3	96.0%	48.0%	51.0%	53.0%
vgg16	100.0%	47.0%	44.0%	51.0%
Custom Model (with Attention Layers)	-	-	60.0%	55.0%

V. Results and Analysis

This study involved evaluating the performance of various deep learning models on image classification tasks, particularly focusing on the detection of tampered and compressed images. The models evaluated included ResNet50, Inception_v3, VGG16, and a custom model equipped with attention layers, across different image conditions: encoded (original + tampered), encoded and tampered, and encoded and compressed (both lossy and lossless).

The custom model comprises an Inception_v3 backbone, global average pooling, and multiple dense layers. Attention mechanisms were incorporated, focusing on specific features within the images, which contributed to its superior performance in compressed scenarios.

Model Performance Overview

For Non Encoded dataset with a combination of original and tampered images, the highest accuracy was achieved by VGG16 suggesting that it is particularly effective in distinguishing between original and tampered encoded images.

A decline in accuracy was observed for dataset with encoded and tampered images, with ResNet50 recording 54%, Inception_v3 48%, and VGG16 47%, indicating challenges in accurately classifying tampered images once encoded.

Original Images (Encoded and Compressed - Lossy): Enhanced performance was demonstrated by the custom model with attention layers, achieving an accuracy of 60%, compared to 50%, 51%, and 44% for ResNet50, Inception_v3, and VGG16 respectively. Similar trends were noted for Lossless compressed images as well, with the custom model achieving 55% accuracy, closely followed by Inception_v3 at 53%

VI. Concusion and Future Scope

The results highlight the significance of model selection and customization, such as the integration of attention mechanisms for tasks like image tampering detection. The effectiveness of different deep learning architectures under various image manipulations was highlighted in the field of sensitive image transmission, contributing valuable insights to the field of digital image forensics.

The findings from this study suggest several areas for future research in image classification and digital forensics. Future projects could look into using different types of deep learning models to better detect tampered images. There is also potential in refining attention mechanisms to focus on small, specific features that indicate tampering, and expanding datasets to cover a wider variety of image conditions and real-world examples. Moreover, making these models easier to understand and training them to handle attempts to trick them could make them more reliable and trusted. Exploring these areas could help develop more effective models that are useful in more situations, improving the security and trustworthiness of digital content.

VII. References

[1] Ding, Yi, Guozheng Wu, Dajiang Chen, Ning Zhang, Linpeng Gong, Mingsheng Cao, and Zhiguang Qin. "DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things." IEEE Internet of Things Journal 8, no. 3 (2020): 1504-1518.

[2] Li, Shaohui, Wenrui Dai, Ziyang Zheng, Chenglin Li, Junni Zou, and Hongkai Xiong. "Reversible autoencoder: A CNN-based nonlinear lifting scheme for image reconstruction." IEEE Transactions on Signal Processing 69 (2021): 3117-3131.

[3] Vien, Quoc-Tuan, Tuan T. Nguyen, and Huan X. Nguyen. "Deep-NC: A secure image transmission using deep learning and network coding." Signal Processing: Image Communication 99 (2021): 116490.

[4] Kamal, Sara T., Khalid M. Hosny, Taha M. Elgindy, Mohamed M. Darwish, and Mostafa M. Fouda. "A new image encryption algorithm for grey and color medical images." Ieee Access 9 (2021): 37855-37865.

[5] Shankar, K., Mohamed Elhoseny, R. Satheesh Kumar, S. K. Lakshmanaprabu, and Xiaohui Yuan. "RETRACTED ARTICLE: Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique." Journal of Ambient Intelligence and Humanized Computing 11, no. 5 (2020): 1821-1833.

[6] Yan, Xuehu, Yuliang Lu, Lintao Liu, and Xianhua Song. "Reversible image secret sharing." IEEE Transactions on Information Forensics and Security 15 (2020): 3848-3858.

[7] Alkhelaiwi, Munirah, Wadii Boulila, Jawad Ahmad, Anis Koubaa, and Maha Driss. "An efficient approach based on privacy-preserving deep learning for satellite image classification." Remote Sensing 13, no. 11 (2021): 2221.

[8] Wu, Yalin, and Liang Huang. "An intelligent method of data integrity detection based on multi-modality fusion convolutional neural network in industrial control network." Measurement 175 (2021): 109013.

[9] Panwar, Kirtee & Kukreja, Sonal & Singh, Akansha & Singh, Krishna. (2023). Towards Deep Learning for Efficient Image

Encryption. Procedia Computer Science. 218. 644-650. 10.1016/j.procs.2023.01.046.
[10] Bellini, Emanuele, and Matteo Rossi. "Performance comparison between deep learning-based and conventional cryptographic distinguishers." In Intelligent Computing: Proceedings of the 2021 Computing Conference, Volume 3, pp. 681-701. Springer International Publishing, 2021.
[11] Huang, X., Li, Z., & Wang, Y. (2023). DL-Guard: Enhancing Data Security in IoT with Deep Learning. IEEE Transactions on Information Forensics and Security, 18(3), 662-675.
[12] Wang, Q., Chen, H., & Liu, W. (2022). Deep Learning-Based Image Encryption Using Generative Adversarial Networks. IEEE Transactions on Multimedia, 24(8), 2279-2292.
[13] Liu, Y., Zhang, L., & Yang, Q. (2023). Secure Transmission Protocol for Medical Images Using Deep Learning and Cryptography. Journal of Medical Systems, 47(5), 102.
[14] Chen, S., Wu, H., & Zhou, X. (2023). Hybrid Encryption Approach for Secure Image Transmission Based on Deep Learning and Cryptography. IEEE Access, 11, 75892-75905.
[15] Zhang, J., Wang, Y., & Liu, T. (2022). Deep Learning-Based Steganography for Secure Covert Communication. IEEE Transactions on Information Forensics and Security, 17(6), 1543-1556.
[16] S. Tamuly, Jyotsna C, and Amudha J., “Deep Learning Model for Image Classification”, Advances in Intelligent Systems and Computing, vol. 1108. Springer International Publishing, Cham, 2019.
[17] A. Unnikrishnan, Sowmya V., and Dr. Soman K. P., “Deep learning architectures for land cover classification using red and near-infrared satellite images”, Multimedia Tools and Applications, vol. 78, no. 13, pp. 18379-18394 (IF: 2.313, CiteScore: 3.7, Q1- 80 percentile)., 2019.
[18] A. Neena and M. Geetha, “Image classification using an ensemble-based deep CNN”, Advances in Intelligent Systems and Computing, vol. 709, pp. 445-456, 2018
[19] M. Nikhitha, S. Sri, R., and B. Uma Maheswari, “Fruit Recognition and Grade of Disease Detection using Inception V3 Model”, in 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), 2019, pp. 1040-1043.