Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Deep Learning-Based Steganography: A Neural Network Approach for Secure Data Embedding

Omar Farook Mohammad[1], Mohammed Hazim Alkawaz[2], Ammar Mohammedali Fadhil[3]
[1] *Department of Computer Science, College of Education for Pure Science, University of Al-Hamdaniya, Mosul, Iraq*
[2] *Department of Computer Science, College of Education for Pure Science, University of Mosul, Mosul, Iraq*
[3] *Information and Communication Technology, Middle Technical University, Iraq*

ARTICLE INFO

Received: 28 Dec 2024

Revised: 18 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

The urgent need for secure communications in the digital era has led to the development of steganography algorithms. Steganography is a technique for hiding digital data in a media such as an image. Traditional techniques, despite their effectiveness, face some limitations such as imperceptibility, payload capacity, and robustness against attack. The emergence of Artificial Intelligence (AI), especially Deep Learning (DL), has revolutionised the field of data hiding and security. This study reinforced recent developments by highlighting deep learning models by training Convolutional Neural Networks (CNNs) and extracting features such as edges, boundaries, and color contrast between each pixel and its neighbours. When the pixel is selected, it is embedded in the Least Significant Bit (LSB), thus obtaining a high payload capacity of the data, imperceptibility, and a more robust image against attacks. The results obtained proved the worth of the proposed method, as BSNR = 92 dB and MSE = 25 were obtained to produce an image with a higher payload capacity and more security. In the future, the integration of algorithms such as machine learning and deep learning can be utilized to create a hybrid algorithm that is better in terms of statistical attacks.

Keywords: Steganography, Deep learning, Artificial Intelligence, Payload capacity, imperceptibility.

INTRODUCTION

In the era of information and communication technology, protecting sensitive and private data has become of high importance, especially when it is transmitted over computer networks. Traditional encryption methods can ensure the security of data by converting text from readable to unreadable and incomprehensible text [1]. However, they often fail to preserve data, as the intruder, when unable to decode the data, damages or tampers with it, which leads to incorrect information reaching the other party. Steganography deals with the matter by hiding data in other data and making it visible to the public during transmission. Steganography works by embedding data in a media such as an image on the sender's side, then the image is sent to the other side, the recipient, where data ex-traction is done in a reverse process of embedding, thus extracting data in a way that is not noticeable to the public [2]. This process is harmless to the hidden data and therefore imperceptible to unauthorized observers.

Traditional steganography methods that rely on Least Significant Bit (LSB) substitution are considered good but suffer from drawbacks and limitations that make them undesirable in terms of payload capacity and resistance to detection [3]. With the advancement and development of technology and the increasing expertise of intruders, the ease of detecting hidden data has increased, and in addition, traditional methods have also suffered from visual distortion that is reflected in the clarity of the image carrying the data [4]. The goal of the proposed modern methods and the development of steganography is to increase specific criteria such as increasing the capacity of embedding, i.e. the amount of data carried in the image, as well as insensitivity, which is not raising suspicion when transferring the image as it contains secret data or not, and also robustness, which is the ability of the image to withstand attacks [5]. These limitations require finding unconventional solutions due to the accumulated experiences gained by hackers and intruders. From this standpoint, innovative methods must be found that meet these demands and are able to meet the challenges. Deep learning is considered part of artificial intelligence and effective tools in data analysis and

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

processing [6]. The ability of deep learning to analyze patterns and styles makes it one of the most important methods that have recently gained popularity and is suitable for tasks that require high accuracy and undetectable security. Through deep learning techniques, data can be hidden and criteria such as robustness and insensitivity can be enhanced and higher loads of hidden data can be achieved [7].

Deep learning especially that based on convolutional neural networks (CNNs) is a promising solution to solve problems of image processing or data security. Steganography methods can be more sophisticated, robust and secure for data by overcoming the limitations that accompany the selection of the bits that can be included in the confidential data in the image, which is often chosen randomly. In this study, a new approach is proposed based on hiding sensitive data in one of the media represented by the image, and the se-lection of the embedding location is one of the most important steps in deep learning, as it is predicted according to the initial training process on data taken from a standard dataset.

LITERATURE REVIEW

Steganography techniques are a method of hiding secret data in a specific digital media such as images. Steganography techniques have been used since ancient times when messages were tattooed on the heads of slaves and sent to the last party after the hair grew [8]. After that, secret inks and other primitive methods were used. In the modern and digital era, many traditional techniques have been proposed in research literature. One of the leading methods in this field is the method that depends on replacing the least significant bit (LSB), those bits whose change does not affect the image due to their low importance are chosen sequentially [9]. One of the disadvantages of this method is that it is expected by the hacker and can be easily detected. In another study, it was based on changing the SSB suddenly and randomly adding the embedding to the image pixels. Another study also relied on the embedding by alternating between the first and second bits so that it is not expected by the intruder [10]. Some techniques have eliminated the reliance on the least significant bits in the image and relied on frequencies and transformations such as the discrete cosine transform (DCT) and the discrete wave transform (DWT) and the embedding of the secret data in the frequency domain [11]. These methods mean that the capacity of the addition is low and larger data cannot be loaded into the image. Another technique has been proposed that relies on edge adaptive stealth (EAS) as well as the histogram that embeds data in places where it can be affected but is not noticeable [12]. Another technique has been proposed to embed by choosing the inverted bits in the embedding which may not lead to any perception and is basically difficult to detect. Since the advent of AI techniques, many models have combined AI and Steganography. Tech-niques such as Convolutional Neural Networks have been used in Steganography to add a large amount of data. The algorithms that work on CNN depend on the neural network's adaptation and learning to select the best pixel in the image as well as the best bit of LSB and filtering for embedding [13]. Generative adversarial networks have revolutionized the ca-pacity of data embedded in the image and reduced complex calculations. Effective models have been proposed such as HiDDeN that have made the secret data hiding in an imperceptible way which has become known for its high storage capacity [14]. In a study, pixel identification in the image played a major role by using structures such as U-Net to find the best place to hide the secret data with suitable imperceptibility [15]. Deep learning has been used as a tool to select the best place in the image as well as the best place in the pixel itself [16]. This method has the advantages of speed, accuracy and high storage but suffers from computational complexity at the beginning of training. Despite the advantages of deep learning in stenography, it still suffers from challenges that must be taken into account, such as high computational cost and dependence on training data. Another challenge is the weakness of the method in confronting hostile attacks. Deep learning here is characterized by adaptive efficiency for different types of images and any type of image segmentation. However, the problem that deep learning suffers from in all applications is the long training period, but despite this disadvantage, it is done only once and we do not need to repeat it. The study proposed a deep learning model that aims to address the challenges in this field.

There are many challenges in this field of steganography considered as problem statements, the first of which is the imperceptibility, which is the main goal in the data hiding process [17]. As well as the computational cost that is embedded when using artificial intelligence techniques in steganography. In addition to the limitation of adding with steganography because the addition is on the LSB, where one of the problems it suffers from previously is the storage capacity of the image when adding.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

For this reason, this research paper aims to find a method that takes care of the storage capacity and adds confidential data in an imperceptible way and to a high degree. The objectives can be summarized as follows:

1- To design a data hiding model based on deep learning and the ability to control dynamic weights to find the best storage capacity.

2- To predict the selection of the pixel for embedding in the image to be more appropriate and not affect the imperceptibility.

3- Build a robust system based on embedding sensitive data with lower computational cost and high imperceptibility.

PREPOSED METHODS

In this section we discuss using the steganography method to hide sensitive data, and we choose one of the media which is images as it is the most reliable and flexible. At the sending and receiving end of the data, the embedding process is done, and after sending it, the extraction process is done to separate the secret data from the image and thus we have ensured the secure transmission of sensitive data.

First: Sensitive data that must be hidden is determined.

This data must be in a format of text that can be included and effectively so as not to affect the quality of the transmission medium.

Second: Preparing the carrier media

The choice of the carrier medium is important here to be unobtrusive and to have the ability to transfer data easily. The following must be taken into consideration:

The carrier medium formats as in our study are the image and attention must be paid to the type of image (JPEG or PNG formats are widely used in internet), its size and its ability to be absorbed. The size of the file to be included must be compatible with the size of the carrier file to be absorbed. A high-resolution image is suitable for transferring a large amount of data. The file must be available without repeated compression and repeated editing in order to preserve the data it carries.

Third: Data Embedding

Embedding is done using Steganography technology which allows the data to be invisible to intruders. In the embedding process, the image is analyzed into its pixel components and then the pixel value is analyzed into binary numbers consisting of 8 bits and the embedding is often done in the Least Significant Bits (LSB) because the embedding in this place has the least effect on the pixel value [29], which leads to an imperceptible change in the image. As shown in Figure 1.

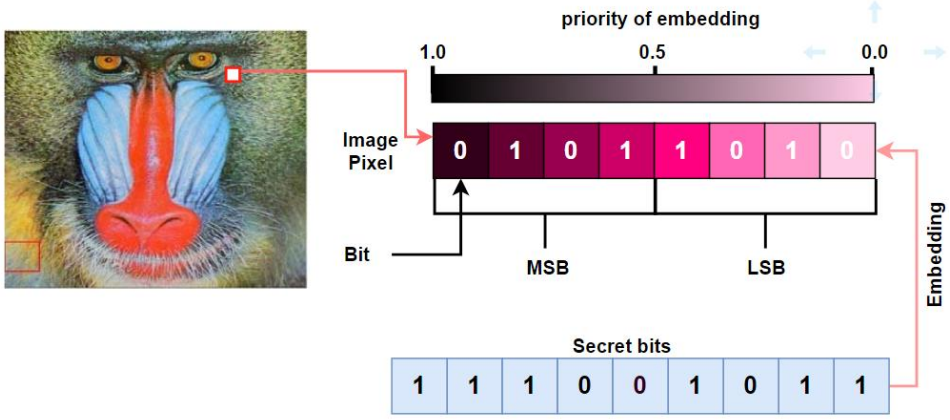

Figure 1: Principles of Embedding in Steganography

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The basic principle of adding deep learning with stenography is the strong ability of deep learning to predict the next pixel for embedding in the image. Hence, we know that deep learning must be adaptive to the nature of the work, and deep learning is designed based on the nature of embedding in stenography. The proposed model includes several steps that can be summarized in the flowchart in Figure 2.

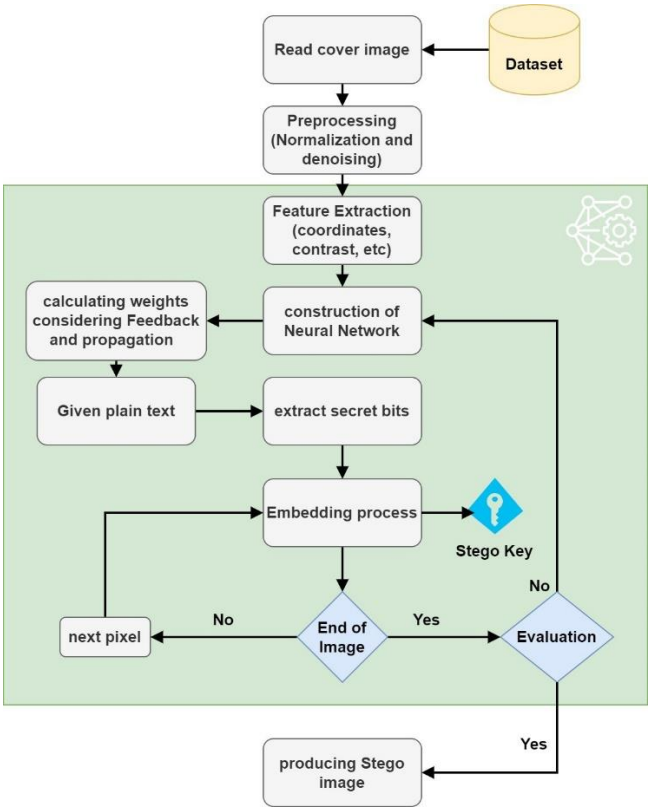

Figure 2: General Framework for Proposed Method

At first, the image is taken from a standard dataset to be trained on, the initial processing process is necessary to prepare the image for the processing stage. The neural network is built on the basis of the input information that comes from the features extracted from the image and thus hidden intermediate layers are established with a variable number of nodes. The data in the input layer passes through the hidden layers and from there to the output layer, which determines which pixels can be added according to the logical sequence of the neural network. The feedback data produced by the hidden layers is dealt with, and then the weights that depend on the feedback are classified. The weights are based on the distance of the data from the output layer and the number of previous and subsequent layers and the vertical distance (number of nodes) and from which path it comes; all these features determine the weight that controls the location of the pixel in the stego image. After selecting the pixel, we take one bit of the text to be included and add it to one of the pixel bits LSB and so on to the rest of the pixels in the image. If the method is not efficient, the structure of the neural network is changed and the process is repeated a large number of times until we reach the form of deep learning that we desire.

There are many variables affecting the deep neural network, sometimes some variables are controlled to have a greater impact on the result. And some variables cannot change along the course of the deep learning process, these variables can change in the case of changing the structure of the neural network. Changing the shape of the deep neural network is the basis for increasing the efficiency of embedding, and this is necessary in to keep the secret message away from intruder, but sometimes it takes a long implementation time.

During the training period, multiple variables control the neural network, and to get a good result, the neural network can predict the result better. Variables such as weight, transaction, recursive number, iteration rate with feedback and acknowledgement are all considered in our study. The creation and updating of hidden layers in the deep neural network depend on the acknowledgment of each layer by feedback to the layer before it, and so on.

Journal of Information Systems Engineering and Management
2025, 10(46s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

RESULTS AND DISCUSSION

The research aims to hide secret data to ensure the safety of the data and prevent this data from being tampered with by unauthorised parties. The sent image contains secret data, and preserving it is important; and the image must be evaluated before sending it. The stego image can be evaluated according to several criteria, and these criteria will be mentioned in detail in this section.

The first criteria considered here is *Peak Signal to Noise Ratio (PSNR)* refers to the quality of image after embedding data in it and can calculated as:

$$PSNR = 10.log_{10}\left(\frac{MAX_1^2}{MSE}\right) \quad (1)$$

Where MSE is Mean Square Error and can find it by:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad (2)$$

Where *MAX* is considered as the maximum pixels value of *m, n* dimensions image and *I* is original image *and K* is noisy image.

PSNR value is negatively affected by MSE. When data is embedded in the image, the image starts to increase its PSNR value. The higher its value, the better, i.e. the image has good quality even with the embedded secret data. Increasing the data loaded in the image leads to gradual image distortion, so traditional methods compete in the amount of data loaded into the image in multiple ways. The percentage of embedding varies from one method to another. The percentage can be measured on a scale of 1/8. The method can be tested in multiple proportions and in other ways, as in Table 1:

Table 1. Imperceptibility of embedding different payload capacities with different techniques

Capacity (Bytes)	Embedding ratio	PSNR (dB)		
		LSB method	LSB with Random distribution	Proposed method DL
17872	6.25%	75	80	92
36345	12.5%	62	72	84
53872	18.75%	59	66	78
73526	25%	52	61	64

The 6.25% ratio means the area of the image that will be exploited by the secret data, which is equal to 16384 bytes, so the PSNR increases as the embedding decreases and vice versa decreases with the increase in the amount of data embedded to the image because it increases the distortion of the image. As for the method followed, it has an effective effect, as the traditional methods that depend on LSB are easy to detect (79 dB) and expected by the PSNR equation. As for the increase in randomness in the distribution, it positively affects the value (90 dB), especially when applying the DL method, as the data is completely hidden. Therefore, the probability of inclusion plays an important role in changing the pixel value. This data was on a single image, so the image also plays an effective role in stating the result. The image with a lot of change in features is better than the image that has the same color change.

In common tests will be on images from a standard dataset and in this case we have three types of embedding on four known standard images from a dataset called SIPI. The results were varied due to the change in the nature of the images.

The original image is exactly the same as the image (stego image) after the embedding, and this is the main purpose of steganography when sending the image via any means of communication, its security cannot be guaranteed, especially in difficult circumstances such as the conditions of the displaced in Iraq, when the addition is made, a

secure communication environment is very necessary. Through the proposed methodology, we can guarantee the required information without any device noticing that the sent image contains data.

Chi-square is a type of attack on data security transmitted through various media. It detects the probability of data inclusion in the image by checking the data frequencies in the LSB of the image pixels. We notice at the beginning of the image there is a probability of data addition, knowing that it is an original image that cannot include data, because the pixels have similar frequencies in the language at the beginning of the letters, but when completing the rest of the letters represented by the pixel, the probability is completely correct.

The probability of embedding should not exceed 25% of the image, otherwise the addition is exposed and there is data and it is vulnerable to attack. The proposed method has proven its worth through the chi-square attack

With the proposed, the embedding probability looks like the original image, which contributes to the good method. With the simple LSB method probability of embedding is very high and clearly, there is a secret in the image.

CONCLUSION

Integrating AI models with steganography opens up prospects for data security during communications. Deep learning has proven its worth in extracting patterns and processing complex data in the fastest time. The proposed study has enhanced an approach that overcomes some of the limitations in the field of traditional steganography. Convolutional neural networks played an important role in increasing the payload capacity of data on the image and in maintaining the imperceptibility to keep the data safe during transmission and undetectable. This study emphasizes the transformative role of deep learning in the security of transmitted data, in terms of extracting features, the most important of which are edges in the image and color contrast between adjacent pixels. Choosing the appropriate pixels to store sensitive data is one of the most important elements on which steganography is based. The results obtained have proven the worth of the proposed method, as the BSNR=92 dB and the MSE = 25, which are considered good numbers in the context of steganography. In the future, the deep learning method can be combined with machine learning to extract new features that contribute to resisting statistical attacks or Gaussian attacks. Hybrid systems can provide powerful solutions to increase image payload capacity and thus transfer more secret data.

REFRENCES

[1] Chakrabarty, Projjal, Tiyas Sarkar, Manik Rakhra, Kapil Jairath, and Vikrant Sharma. "Enhanced Data Security Framework Using Lightweight Cryptography and Multi-Level Encryption." In 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE), pp. 720-725. IEEE, 2024.
[2] Fadhil, Ammar Mohammedali. "Bit inverting map method for improved steganography scheme." Diss. Universiti Teknologi Malaysia (2016).
[3] Fadhil, Ammar Mohammedali, Hayder Nabeel Jalo, and Omar Farook Mohammad. "Improved Security of a Deep Learning-Based Steganography System with Imperceptibility Preservation." International journal of electrical and computer engineering systems 14, no. 1 (2023): 73-81.
[4] Sanjalawe, Yousef, Salam Al-E'mari, Salam Fraihat, Mosleh Abualhaj, and Emran Alzubi. "A deep learning-driven multi-layered steganographic approach for enhanced data security." Scientific Reports 15, no. 1 (2025): 4761.
[5] Tang, Weixuan, Jiahao Li, Yuan Rao, Zhili Zhou, and Fei Peng. "A trigger-perceivable backdoor attack framework driven by image steganography." Pattern Recognition 161 (2025): 111262.
[6] Abed, Nibras Kadhim, Arfan Shahzad, and Ammar Mohammedali. "An improve service quality of mobile banking using deep learning method for customer satisfaction." In AIP Conference Proceedings, vol. 2746, no. 1. AIP Publishing, 2023.
[7] Aljarf, Ahd, Haneen Zamzami, and Adnan Gutub. "Is blind image steganalysis practical using feature-based classification?." Multimedia Tools and Applications 83, no. 2 (2024): 4579-4612.
[8] Al-Bayati, Amjed Fadhil Hamody, Mesut ÇeviK, and Ammar Mohammedali Fadhil. "An improved steganography system based on contrast variation with fibonacci decomposition to increase imperceptibility." Master's thesis, Altınbaş Üniversitesi/Lisansüstü Eğitim Enstitüsü, 2023.

Research Article

[9] Rahman, Shahid, Jamal Uddin, Hameed Hussain, Sabir Shah, Abdu Salam, Farhan Amin, Isabel de la Torre Díez, Debora Libertad Ramírez Vargas, and Julio César Martínez Espinosa. "A novel and efficient digital image steganography technique using least significant bit substitution." Scientific Reports 15, no. 1 (2025): 107.
[10] Zhao, PengBiao, Xiaopei Wang, Qi Zhong, Jingxue Chen, and Zhen Qin. "A Robust Linked List Steganography without Embedding for Digital Images." In International Conference on Frontiers in Cyber Security, pp. 23-35. Singapore: Springer Nature Singapore, 2024.
[11] Deval, Rohit, Nachiket Gupte, Johann Kyle Pinto, Adwaita Raj Modak, Akshat Verma, Anirudh Sharma, and S. P. Raja. "Exploring advanced steganography techniques for secure digital image communication: a comparative analysis and performance evaluation." International Journal of Electronic Security and Digital Forensics 17, no. 1-2 (2025): 233-266.
[12] Taruk, Medi, Hamdani Hamdani, and Salas Sepkardianto. "Steganography Audio Files Using EAS Method and AES CBC Algorithm for Data Security." In 2024 11th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), pp. 336-340. IEEE, 2024.
[13] Angulakshmi, M., and M. Deepa. "Image Stenography Using Deep Learning Techniques." In Enhancing Steganography Through Deep Learning Approaches, pp. 53-74. IGI Global, 2025.
[14] Rahman, Shahid, Jamal Uddin, Hameed Hussain, Sabir Shah, Abdu Salam, Farhan Amin, Isabel de la Torre Díez, Debora Libertad Ramírez Vargas, and Julio César Martínez Espinosa. "A novel and efficient digital image steganography technique using least significant bit substitution." Scientific Reports 15, no. 1 (2025): 107.
[15] Kaneria, Sapna, and Varsha Jotwani. "Comparative performance analysis of deep learning-based image steganography using U-Net, V-Net, And U-Net++ encoders." Image 13 (2024): 20.
[16] Song, Bingbing, Ping Wei, Sixing Wu, Yu Lin, and Wei Zhou. "A survey on Deep-Learning-based image steganography." Expert Systems with Applications (2024): 124390.
[17] Abdulla, Alan Anwer. "Digital image steganography: challenges, investigation, and recommendation for the future direction." Soft Computing 28, no. 15 (2024): 8963-8976.
[18] Abdulla, A. A. (2024). Digital image steganography: challenges, investigation, and recommendation for the future direction. Soft Computing, 28(15), 8963-8976.
[19] Mandal, Pratap Chandra, Imon Mukherjee, Goutam Paul, and B. N. Chatterji. "Digital image steganography: A literature survey." Information sciences 609 (2022): 1451-1488.
[20] Alexan, Wassim, Eyad Mamdouh, Amr Aboshousha, Youssef S. Alsahafi, Mohamed Gabr, and Khalid M. Hosny. "Stegocrypt: A robust tri-stage spatial steganography algorithm using TLM encryption and DNA coding for securing digital images." IET Image Processing 18, no. 13 (2024): 4189-4206.
[21] Abdullah, Noor Gassan, and Shahd Abdulrhman Hasso. "Adaptive Steganography Using Improve Bit-Plane Complexity Segmentation." Al-Rafidain Journal of Computer Sciences and Mathematics 18, no. 1 (2024): 66-73.
[22] Yakut, Selman. "An Efficient Steganography Method Based on Chaotic Functions and XOR Operation for Data Hiding." Bilgisayar Bilimleri ve Teknolojileri Dergisi 5, no. 2 (2024): 58-65.
[23] Mariko, Aikawa, Miyata Sumiko, Hosono Kaito, Miyata Takamichi, and Kinoshita Hirotsugu. "A Consideration of JPEG Resistance Verification of Correlation-based Steganography." Journal of Imaging Science & Technology 68, no. 6 (2024).
[24] Falih, Mohanaed, Ammar Fadhil, Mohammed Shakir, and Baqer Turki Atiyah. "Exploring the potential of deep learning in smart grid: Addressing power load prediction and system fault diagnosis challenges." In AIP Conference Proceedings, vol. 3092, no. 1. AIP Publishing, 2024.
[25] Miah, Abu Saleh Musa, Md Al Mehedi Hasan, Yoichi Tomioka, and Jungpil Shin. "Hand gesture recognition for multi-culture sign language using graph and general deep learning network." IEEE Open Journal of the Computer Society (2024).