International Journal of Electrical and Computer Engineering (IJECE)
Vol. 15, No. 6, December 2025, pp. 5594~5603
ISSN: 2088-8708, DOI: 10.11591/ijece.v15i6.pp5594-5603

Intrusion detection based on image transformations and data augmentation

Nada Ali Abood, Asghar A. Asgharian Sardroud
Department of Computer Engineering, Urmia University, Urmia, Iran

Article Info

Article history:

Received Feb 20, 2025
Revised Jul 23, 2025
Accepted Sep 14, 2025

Keywords:

Data augmentation
Deep learning
Dimension reduction
Image transformation
Intrusion detection system

ABSTRACT

The increasing growth of users and communication networks in different platforms has led to the emergence of various types of network attacks. intrusion detection systems (IDS) are one of the important solutions to cope with these problems. An IDS determines whether incoming traffic is intrusive or normal. IDSs often achieve high efficiency with methods based on deep neural networks. However, one of the shortcomings of these methods is the lack of sufficient attention to the spatial features in the data. This research presents an intrusion detection method based on image transformations and data augmentation is presented. In the proposed method, the intrusion detection process is performed by transforming the traffic vector into an image using a convolutional neural network (CNN). Also, we use data augmentation and dimension reduction techniques to increase accuracy and reduce complexity in the proposed method. Simulation results on network security laboratory-knowledge discovery and data mining (NSL-KDD) show that the proposed IDS can classify intrusion traffic with an accuracy of 97.58%.

Corresponding Author:

Asghar A. Asghrian Sardroud
Department Computer Engineering, Urmia University
Urmia, Iran
Email: a.asgharian@urmia.ac.ir

1. INTRODUCTION

In the digital world, various types of computer networks have become vital components of organizations, industries, governments, and individual users [1]. The development of various industries is completely tied to the development of computer networks and requires more attention [2]. In this regard, with the increasing dependence on the internet and network systems, new methods of network security and infrastructure protection have transformed into one of the most important issues in the field of information and communication technology [3]. On the other hand, new threats and numerous attacks emerge in the cyber world every day that can damage the sensitive and vital infrastructure of organizations and cause serious disruptions and irreparable economic losses. Despite the dependence of businesses on digital technology, maintaining the security of computer networks and protecting data against cyber-attacks has become a vital issue [4]. Network security refers to a set of strategies, technologies, and policies used to protect computer networks and confidential data and prevent unauthorized intrusion into the network. Among the network threats are malware and malicious software, phishing attacks, distributed denial of service attacks aimed at disabling online services, and network intrusion by exploiting weaknesses of networks, which can be prevented by using network security [5]. With the advancement of technology, there have been significant changes in the way cyber-attacks are carried out, and unfortunately, the number of people and organizations that are victims of these types of attacks, such as distributed denial of service (DDoS) attacks, malware,

phishing, and other types of attacks, is increasing daily. To increase network security and prevent intrusion and counterattacks, intrusion detection system (IDS) is an efficient and familiar method in the literature. A wide variety of methods have been proposed for IDS, among which machine learning (ML)-based methods are very effective [6]–[8]. However, less research has addressed the attractiveness of working with two-dimensional data and spatial features. Our contribution to this study is to present an Intrusion detection method based on image transformations and data augmentation. In the proposed method, the Intrusion detection process is performed with a convolutional neural network and based on the traffic vector transform to the image. To increase the accuracy, the data augmentation technique is used. Also, to reduce the computational complexity, a dimensionality reduction method is included in the framework of the proposed method. The rest of the paper is as follows: section 2 contains the background of the research. In this section, the main IDS methods are reviewed. In section 3, the proposed Intrusion detection method based on image and data augmentation is presented. In section 4, the dataset is introduced and the simulation results are discussed. Finally, section 5 concludes the paper.

2. BACKGROUND

IDSs can be divided into two categories, traditional intrusion detection methods and new intrusion detection methods. New methods take advantage of machine learning-based methods. These methods are specified in Table 1. As shown in the table, traditional methods usually rely on statistical analysis of traffic vectors.

2.1. Traditional intrusion detection methods

In traditional methods, the feature vector is systematically examined. In these methods, the basic information available in the incoming traffic must be identified and decisions made based on it. signature-based detection [9], rule-based detection [10], statistical methods [11], behavior-based detection [12], flow-based detection [13], hybrid methods, and anomaly-based detection are some of the most important traditional methods [14]. traditional methods are very effective for static and low-dimensional traffic. However, they usually fail against new and dynamic attacks with high dimensions. For example, DDOS attacks are one of the most dangerous attacks carried out on the Internet. The goal of these attacks is not to destroy the desired service but to force the network and server to be unable to provide normal service by targeting network bandwidth or connectivity. These attacks are carried out by sending data packets to the victim, which inundates the victim's network or processing capacity with information packets and prevents users and customers from accessing the service. In general, a DDoS attack on a site occurs when access to a service or network resource is intentionally blocked or reduced because of the malicious activity of another user [14]. Given the nature of these attacks, relying solely on traditional methods cannot be effective.

2.2. Methods based on machine learning algorithms

Unlike traditional intrusion detection methods, in methods based on machine learning algorithms, a classification problem arises [15]. These methods can be called modern intrusion detection methods. In these methods, there is a training dataset. This dataset is divided into two parts: training and testing. The network is trained based on the training data (traffic labeled as normal traffic or attack) and then decides the nature of the incoming traffic [16]. This decision is made based on the characteristics of the incoming traffic. ML-based IDS methods can be classified into different categories. These methods may use an support vector machine (SVM) [17] or an artificial neural networks (ANN) [18] in the detection process. However, in recent years, methods based on deep networks have been very promising and efficient. Methods based on deep neural networks can also have different subsets. The two important categories of these networks for intrusion detection are vector-based methods and recurrent networks, and image-based methods and convolutional networks. Recurrent networks are themselves a subset of deep networks. In these networks, the input is modeled as a sequence.

In these methods, special attention is paid to the temporal relationship between samples. Recurrent network-based methods are usually known as long short-term memory (LSTM) [19] and gated recurrent units (GRU) [20] networks. The results of previous studies show that LSTM is suitable for modeling a high-accuracy classification model and its performance is superior to traditional machine learning classification methods in binary classes. The LSTM model improves the accuracy of intrusion detection and provides a new research method for intrusion detection. However, in LSTM-based methods, spatial features in the data are not considered. Image-based methods and convolutional networks are also effective methods for intrusion detection that operate based on feature extraction from spatial (image) data [21]. Using the intrusion detection method with convolutional neural network (CNN) has a great advantage that other machine learning methods do not consider. This advantage is that it considers the spatial features in traffic data. However, a data augmentation method must also be used, which has not been considered in previous

methods. Because CNN-based methods require a lot of data [1], [22]. On the other hand, using the data augmentation method may lead to a decrease in speed. For this reason, it is necessary to make the data suitable for network training with a dimensionality reduction mechanism. In this study, these ideas are presented in an intrusion detection framework to overcome the shortcomings of previous methods.

Table 1. General comparison of traditional and new intrusion detection methods

New methods	Traditional methods
Deep neural networks- based detection [6], [15]	Signature-based detection [7], [9]
Recurrent-based detection [16]	Rule-based detection [10]
Image-based detection [21], [23]–[25]	Statistical methods [11]
	Behavior-based detection [12]
	Flow-based detection [13]

3. PROPOSED METHOD

Figure 1 shows the block diagram of the proposed method. The proposed intrusion detection in this research is based on a scheme based on image transformations and data augmentation. Based on this diagram, a CNN network must be trained as a base model at the first step. To train this network, the incoming traffic must be transformed into an image. In this method, the data augmentation technique is used to increase accuracy. Also, to reduce the computational complexity, a dimensionality reduction method (principal component analysis (PCA) method [26]) is included in the framework of the proposed method. After the CNN model is fully trained, it will be used for testing (separating normal and attack traffic).

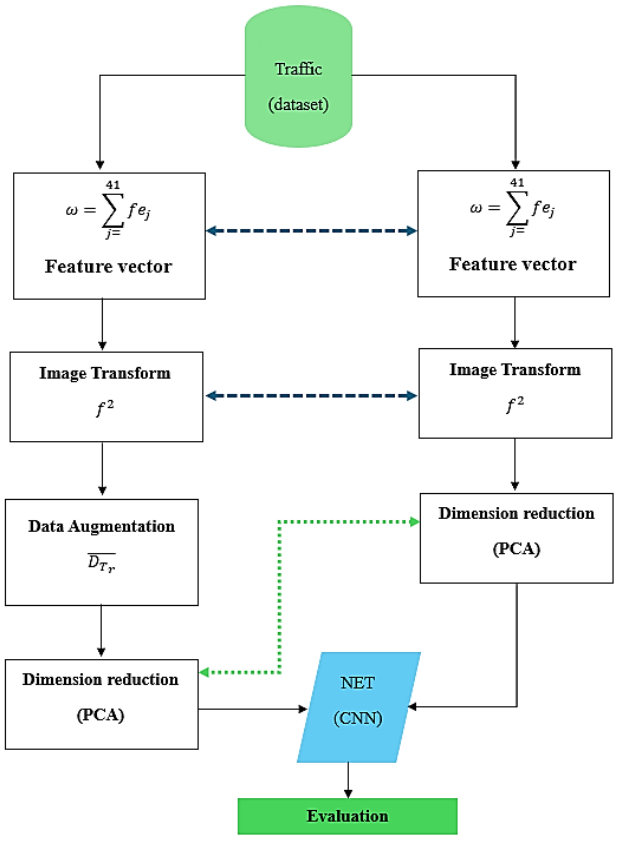

Figure 1. Block diagram of the proposed intrusion detection method

3.1. Feature vector

The input feature vector specifies the traffic characteristics. The number of bytes received and sent, the duration of the activity, the number of login attempts, and even the IP address are all important characteristics of the traffic. For example, a fixed IP is a fixed address that does not change over time. This

type of address is usually used for servers or devices that require fixed access points for remote connections. Hence, it is an important characteristic of incoming traffic. The traffic vector in this study is modeled as ω.

$$\omega = \{fe_j\}, \ i = 1,2,\dots,41 \tag{1}$$

The number of features in the traffic vector is related to the dataset. In this study, 41 features of the traffic are stored in a vector, which is the reason for using the NSL-KDD dataset [27]. We use M to denote the total number of vectors available for training.

$$D_{T_r} = \{\omega_1, \omega_2, \dots, \omega_M\} \tag{2}$$

Also, we use N to denote the number of vectors available for testing. Thus, the total available data is $M + N$.

$$D_{T_s} = \{\omega_{M+1}, \omega_{M+2}, \dots, \omega_{M+N}\} \tag{3}$$

3.2. Image transform

The CNN network works with two-dimensional data for training and feature extraction. Therefore, it is better to transform the traffic vector with a specific mapping to the image. This can be represented as (4).

$$I_{input} = f^2(\omega) \tag{4}$$

There are two general methods for image transformation. The direct copy method and the rotary shift method are shown in Figure 2. The advantage of the direct copy method is to preserve spatial and temporal information. Therefore, if ensemble networks are used in which LSTM or GRU models are present, it is better to use the direct copy method to preserve both spatial and temporal information. However, the rotary shift method is more efficient for IDSs that are only based on images. In this research, the rotary shift method was used.

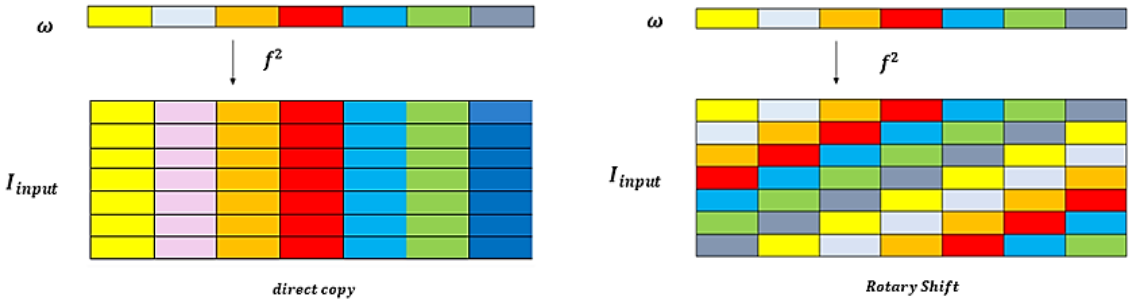

Figure 2. Difference between the direct copy method and the rotary shift method in image transformation

3.3. Data augmentation

Using the intrusion detection method with CNN has a great advantage that other machine learning methods do not pay attention to. This advantage is to pay attention to the spatial features present in the traffic data. However, a data augmentation method must also be used. Because CNN-based methods require a lot of data. On the other hand, using the data augmentation method may lead to a decrease in speed. For this reason, a data augmentation scheme should be used in the proposed method. In the proposed method, each image is transformed into 6 other images according to the following relationship and Figure 3. In this relationship, a_i is the transform coefficient, which is generally equal to one but can have a higher value for some transformations. Dgg_i also indicates the transform type, which is one of the 6 rotation modes.

$$I_{input} \rightarrow [I_{input_0}, I_{input_{\mp 45}}, I_{input_{\mp 90}}, I_{input_{180}}] \tag{5}$$

$$\overline{D_{T_r}} = \cup_{i=1}^{M} \cup_{i=1}^{6} \{a_j Dgg_j \omega_i\} \tag{6}$$

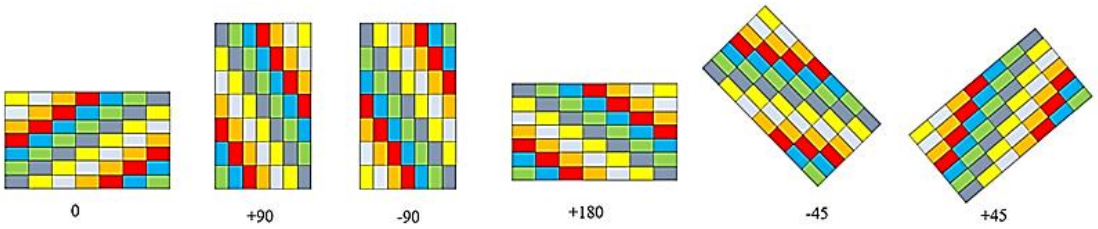

Figure 3. Six images created with the data augmentation technique

3.4. Dimensionality reduction

A dimension reduction algorithm is necessary after the data augmentation technique in the proposed method. This is because the data augmentation algorithm is used in the proposed method. For this reason, it is necessary to reduce the dimensions of the input data to the CNN network. There are various methods for dimensionality reduction. In this research, the fast PCA method is used. This method is a good method for working with traffic images and has low complexity. PCA is a popular data reduction technique in machine learning and a subgroup of unsupervised algorithms. These algorithms are used to identify linear patterns in high-dimensional data [28]. The main goal of PCA is to find a lower dimensional space that preserves the maximum variance in data. This means finding a set of new axes that accommodate the maximum amount of dispersion in the data. These new axes are known as principal components or PCs. By reducing the dimensionality of the data, PCA reduces computational complexity and helps improve the efficiency of machine learning algorithms. It also reduces the noise in the data by focusing on the principal components and helps improve the accuracy of machine learning algorithms. In addition, PCA facilitates the visualization of the data in a lower dimensional space by reducing the dimensionality of the data.

3.5. CNN training and testing

CNN neural network is one of the most important deep neural networks whose architecture follows a similar pattern to the connection of brain neurons to each other and is modeled after the visual cortex section. Small groups of visual neurons are engaged in each part alone and the combination of these neurons and the creation of interconnected networks causes the vision of an area. Figure 4 shows the architecture of the CNN network used. The convolution layer is the backbone of any CNN working model. This layer is the layer where pixel-by-pixel scanning of images takes place and creates a feature map to define future classifications. Pooling is also used as data sampling.

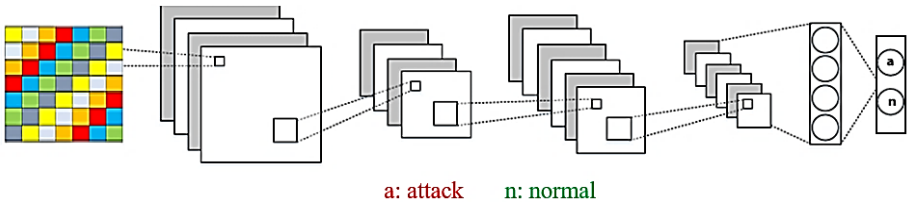

Figure 4. CNN network architecture in intrusion detection

After designing the model, all data must be divided into two training and test sections. The training process uses augmented data. Hence, by substituting the augmented data instead of the training data, we have:

$$D_R = D_{T_S} \cup D_{\overline{T_r}} \tag{7}$$

$$|D_R| = 6M + N \tag{8}$$

In which, the total data is denoted by D_R, the test data by D_{T_S}, and the augmented training data by $D_{\overline{T_r}}$. Finally, the network is trained with default hyperparameters and then it could classify Intrusion and normal traffic. The proposed method of this study only completes the Intrusion detection operation based on images. This is a new idea that has been discussed in a few works. The proposed method should overcome two main problems; the second problem arises due to the solution of the first problem. In fact, the CNN network

requires a large amount of data to work with spatial data. This problem was solved in the proposed method with data augmentation. But this itself increases the complexity of the system, which was included in the framework of the system to solve it by reducing the dimensions. The general scheme of Intrusion detection is both fast and accurate and is based only on images. Algorithm 1 of the proposed method is briefly presented.

Algorithm 1

1. Set the parameters of the neural network and the number of input data samples.
2. Define traffic vectors with 41 features: $\omega = \{fe_j\}$
3. Divide the input data into two parts, training and testing: $D_R = D_{T_s} + D_{T_r}$
4. Transform the vector data into an image using the rotary method: $I_{input} = f^2(\omega)$
5. Multiply the image data by the data augmentation method by 6.

$$I_{input} \rightarrow [I_{input_0}, I_{input_{\mp 45}}, I_{input_{\mp 90}}, I_{input_{180}}]$$

6. Perform dimensionality reduction on the data using the PCA method.

$$\overline{D_{T_r}} = U_{i=1}^{M} U_{i=1}^{6}\{a_j D_{gg_j} \omega_i\}$$

7. Train the CNN network with the following data.
8. Evaluate the proposed method using test data and report the accuracy as output.

$$U_{i=1}^{M} U_{i=1}^{6}\{a_j D_{gg_j} \omega_i\}$$

9. End

4. SIMULATION AND EVALUATION

The simulation of the proposed image-based intrusion detection method has been performed in MATLAB. Also, the NSL-KDD dataset has been selected as the evaluation dataset. The NSL-KDD dataset is a widely used version in evaluating IDS methods. This dataset has 125,973 data for training and 22,544 data for testing. Table 2 shows the distribution of attacks in this dataset. As it is clear, the distribution of data in this dataset is not balanced for traffic classification. However, in this research, our goal is only binary classification of Intrusion. In other words, our goal is to determine the intrusion or normality of incoming traffic. In this respect, this dataset is balanced. The distribution of attacks in the two parts of the train and test is shown in the diagram of Figure 5. As the diagram of Figure 6 shows, DoS attacks have a large share in this dataset. This attack means “denial of service” and is a type of cyber-attack in which the attacker tries to disrupt real users' access to the service by sending a large volume of requests or unusual use of server resources.

Table 2. Distribution of attacks in the two parts of train and test

Traffick	Train Set (%)	Test Set (%)
Normal	54	52
Dos	40	39
Probe	4	6
R2L	1.5	2
U2R	0.5	1

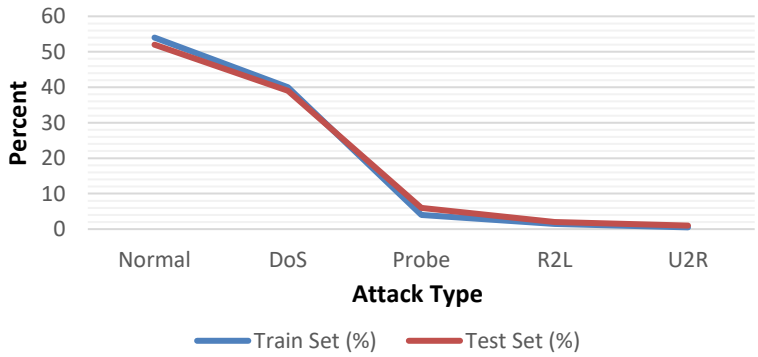

Figure 5. Distribution of attacks in the two train and test sections

In simple terms, in a DOS attack, the attacker sends excessive traffic or requests to the server or network so that the server loses the ability to respond to real users' requests. Therefore, in this case, the number of logins attempts and the number of bytes sent and received will be unusual. For this reason, this attack has taken up a large portion of the data set.

4.1. Results and discussion

Table 3 presents the simulation results for three cases. For this purpose, a comparison of the results between the two parameters accuracy and speed has been made. The first case is IDS without Data augmentation. In this case, the need for CNN network training data has not been increased. The second case is IDS with Data augmentation and without PCA. Also, in the third case, the PCA algorithm is added to reduce dimensions.

Table 3. Comparison of results between two modes of accuracy and speed for three modes

IDS Method	Accuracy (%)	Speed (m) (Training)
IDS without data augmentation	91.25	73
IDS with data augmentation (no PCA)	98.49	214
IDS with data augmentation + PCA	97.58	142

Simulation results show that not using the dimensionality reduction algorithm leads to the complexity of the IDS algorithm. Of course, this complexity is only in the training cycle. However, the data augmentation algorithm in the proposed IDS increases the accuracy because more patterns are learned by the network. The highest accuracy is when the PCA algorithm is removed. The reason is that, in this case, the network learns all the features without reduction, which requires more time and computation. However, a compromise must be made between speed and accuracy. The bar chart in Figure 6 shows the comparison of the results between the two parameters accuracy and speed for three cases.

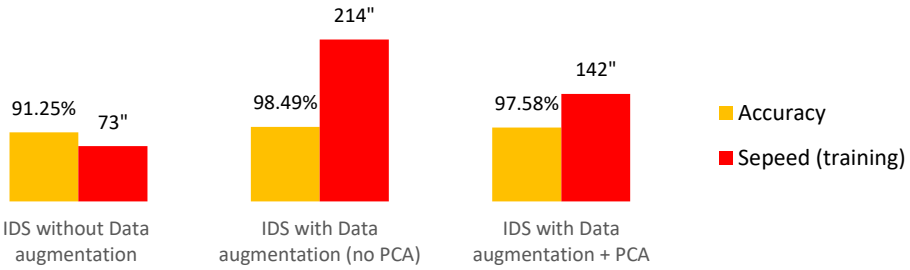

Figure 6. Bar chart comparing the results between the two parameters accuracy and speed for three cases

The comparison of the proposed method with other methods is made in Table 4. The method of Kim *et al.* [22] has obtained good accuracy. However, this method has a delay almost twice that of our method. The reason for this is the large number of layers of the CNN network and its encoding method.

Table 4. Comparison of the results for three CNN-based IDS methods

IDS Method	Accuracy (%)	Speed (ms) testing
Jiyeon *et al.* CNN [22]	99	2.23
Elsayed *et al.* CNN [1]	93.86	1.74
IDS with Data augmentation + PCA (ours)	97.58	1.24

Another reason for the good accuracy of the Kim *et al.* [22] method is the two-level image transform and the use of the encoding method. Although this transformation has led to an increase in accuracy, there is a relatively large delay in both the training and testing phases. Figure 7 shows an example of the image transformation in the Kim *et al.* [22] method. On the other hand, our method has higher accuracy than the Elsayed *et al.* CNN [1]. This is due to the use of the data augmentation technique in our method. The results show that data augmentation is a necessity for image-based IDS algorithms.

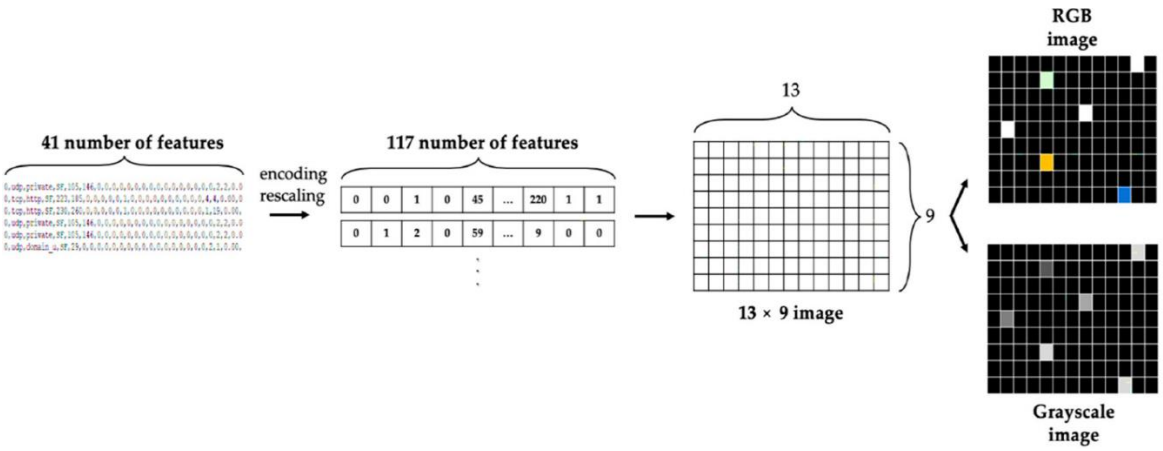

Figure 7. An example of image transform in Kim *et al.* [22] method

The comparison of results between two parameters accuracy and speed for three CNN-based IDS methods is also shown in the graph of Figure 8. The comparison shows that, while our method does not surpass the highest accuracy [22], it achieves a better balance between speed and performance, being significantly faster while maintaining competitive accuracy.

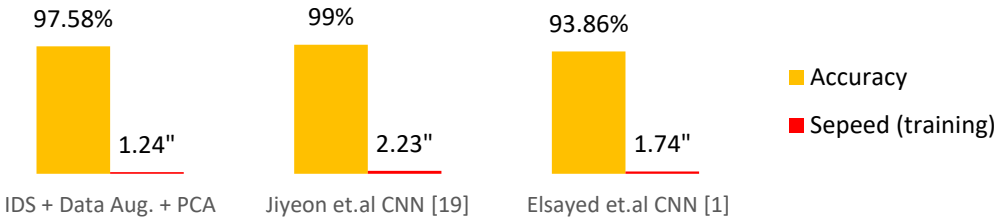

Figure 8. Bar graph comparing results between two parameters accuracy and speed for three CNN-based IDS methods

In Table 5, a comparison is made between the structures used in our method and methods [22] and [1]. This comparison is made in three aspects of data augmentation, dimension reduction and, encoding process. The results show that adding dimension reduction after data augmentation will lead to good accuracy and speed.

Table 5. Comparison between the structures used in our method and other methods

IDS Method	Data augmentation	Dimension reduction	Encoding process
Kim *et al.* CNN [22]	×	×	✓
Elsayed *et al.* CNN [1]	×	×	×
IDS with data augmentation + PCA (ours)	✓	✓	×

One of the most important advantages of the proposed method in our research over methods such as [22] is its ability to handle traffic with long sequences because of our dimension reduction technique. However, increasing the length of the traffic inspection vector in the method [22], may increase the delay exponentially. This issue will be especially noticeable with the growth of new and unknown attacks. There are two ways to solve this problem. The first way is to add an attention mechanism to the neural network which gives low accuracy. The second way is to provide image-based intrusion detection methods because these methods use spatial features. Therefore, our method can be generalized to variety of intrusion detection systems with different vector lengths.

5. CONCLUSION

Researchers have paid less attention to intrusion detection methods based on image transformations and spatial features. In this research, an intrusion detection method based on image transformations and data augmentation was presented. The proposed method transforms the traffic vector into an image, and after data augmentation and reduction, it uses a CNN Network to detect attacks. The data augmentation technique was used to increase accuracy and the dimension reduction technique was used to reduce complexity within the framework of the proposed method. Simulation results on NSL-KDD showed that the proposed IDS can classify intrusion traffic with an accuracy of 97.58%. One of the ideas recommended for future research is to pay attention to data imbalance. This imbalance in classification and attack-type detection issues can decrease accuracy. Therefore, presenting designs that balance data distribution will be an attractive research area.

FUNDING INFORMATION

The authors declare that no funding was received for this study.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Nada Ali Abbood	✓	✓	✓	✓		✓	✓		✓		✓			
Asghar A. Asgharian Sardroud	✓	✓		✓		✓				✓		✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no conflict of interest.

DATA AVAILABILITY

This study used only publicly available datasets, which can be accessed from standard open repositories. No new data were created or collected.

REFERENCES

[1] M. S. Elsayed, H. Z. Jahromi, M. M. Nazir, and A. D. Jurcut, "The role of CNN for intrusion detection systems: An improved CNN learning approach for SDNs," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 382, Springer International Publishing, 2021, pp. 91–104.

[2] A. M. Awaad, K. M. Ali Alheeti, and A. K. A. H. Najem, "Anomaly-based IDS (intrusion detection system) for cyber-physical systems," *Mesopotamian Journal of Big Data*, vol. 2024, pp. 230–240, Dec. 2024, doi: 10.58496/MJBD/2024/017.

[3] B. I. Farhan and A. D. Jasim, "Survey of intrusion detection using deep learning in the internet of things," *Iraqi Journal for Computer Science and Mathematics*, vol. 3, no. 1, pp. 83–93, Jan. 2022, doi: 10.52866/ijcsm.2022.01.01.009.

[4] O. Iraqi and H. El Bakkali, "Application-level unsupervised outlier-based intrusion detection and prevention," *Security and Communication Networks*, vol. 2019, pp. 1–13, Jul. 2019, doi: 10.1155/2019/8368473.

[5] N. N. Mohd Yusof and N. S. Sulaiman, "Cyber attack detection dataset: A review," *Journal of Physics: Conference Series*, vol. 2319, no. 1, p. 12029, Aug. 2022, doi: 10.1088/1742-6596/2319/1/012029.

[6] R. Chinnasamy, M. Subramanian, S. V. Easwaramoorthy, and J. Cho, "Deep learning-driven methods for network-based intrusion detection systems: A systematic review," *ICT Express*, vol. 11, no. 1, pp. 181–215, 2025, doi: 10.1016/j.icte.2025.01.005.

[7] U. Ahmed *et al.*, "Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering," *Scientific Reports*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-85866-7.

[8] M. Farhan *et al.*, "Network-based intrusion detection using deep learning technique," *Scientific Reports*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-08770-0.

[9] M. Masdari and H. Khezri, "A survey and taxonomy of the fuzzy signature-based intrusion detection systems," *Applied Soft Computing Journal*, vol. 92, p. 106301, Jul. 2020, doi: 10.1016/j.asoc.2020.106301.

[10] C. Turner, R. Jeremiah, D. Richards, and A. Joseph, "A rule status monitoring algorithm for rule-based intrusion detection and

prevention systems," *Procedia Computer Science*, vol. 95, pp. 361–368, 2016, doi: 10.1016/j.procs.2016.09.346.
[11] E. Kabir, J. Hu, H. Wang, and G. Zhuo, "A novel statistical technique for intrusion detection systems," *Future Generation Computer Systems*, vol. 79, pp. 303–318, Feb. 2018, doi: 10.1016/j.future.2017.01.029.
[12] H. Y. Kwon, T. Kim, and M. K. Lee, "Advanced intrusion detection combining signature-based and behavior-based detection methods," *Electronics (Switzerland)*, vol. 11, no. 6, p. 867, Mar. 2022, doi: 10.3390/electronics11060867.
[13] A. Sperotto, G. Schaffrath, R. Sadre, C. Morariu, A. Pras, and B. Stiller, "An overview of IP flow-based intrusion detection," *IEEE Communications Surveys and Tutorials*, vol. 12, no. 3, pp. 343–356, 2010, doi: 10.1109/SURV.2010.032210.00054.
[14] S. Gamage and J. Samarabandu, "Deep learning methods in network intrusion detection: A survey and an objective comparison," *Journal of Network and Computer Applications*, vol. 169, p. 102767, Nov. 2020, doi: 10.1016/j.jnca.2020.102767.
[15] I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Computer Networks*, vol. 188, no. January, p. 107840, 2021, doi: 10.1016/j.comnet.2021.107840.
[16] T. Mehmood and H. B. M. Rais, "Machine learning algorithms in context of intrusion detection," in *2016 3rd International Conference on Computer and Information Sciences, ICCOINS 2016 - Proceedings*, Aug. 2016, pp. 369–373, doi: 10.1109/ICCOINS.2016.7783243.
[17] W. H. Chen, S. H. Hsu, and H. P. Shen, "Application of SVM and ANN for intrusion detection," *Computers and Operations Research*, vol. 32, no. 10, pp. 2617–2634, Oct. 2005, doi: 10.1016/j.cor.2004.03.019.
[18] P. Tao, Z. Sun, and Z. Sun, "An improved intrusion detection algorithm based on GA and SVM," *IEEE Access*, vol. 6, pp. 13624–13631, 2018, doi: 10.1109/ACCESS.2018.2810198.
[19] A. V. Hanafi, A. Ghaffari, H. Rezaei, A. Valipour, and B. arasteh, "Intrusion detection in internet of things using improved binary golden jackal optimization algorithm and LSTM," *Cluster Computing*, vol. 27, no. 3, pp. 2673–2690, Jul. 2024, doi: 10.1007/s10586-023-04102-x.
[20] B. B. Gupta, A. Gaurav, V. Arya, and K. T. Chui, "LSTM-GRU based efficient intrusion detection in 6G-enabled metaverse environments," in *Proceedings - 2024 IEEE 25th International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2024*, Jun. 2024, pp. 118–123, doi: 10.1109/WoWMoM60985.2024.00032.
[21] M. Arsalan, M. Mubeen, M. Bilal, and S. F. Abbasi, "1D-CNN-IDS: 1D CNN-based intrusion detection system for IIoT," in *ICAC 2024 - 29th International Conference on Automation and Computing*, Aug. 2024, pp. 1–4, doi: 10.1109/ICAC61394.2024.10718772.
[22] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, "CNN-based network intrusion detection against denial-of-service attacks," *Electronics (Switzerland)*, vol. 9, no. 6, pp. 1–21, Jun. 2020, doi: 10.3390/electronics9060916.
[23] M. S. Korium, M. Saber, A. M. Ahmed, A. Narayanan, and P. H. J. Nardelli, "Image-based intrusion detection system for GPS spoofing cyberattacks in unmanned aerial vehicles," *Ad Hoc Networks*, vol. 163, 2024, doi: 10.1016/j.adhoc.2024.103597.
[24] P. Horchulhack, E. K. Viegas, A. O. Santin, and J. A. Simioni, "Network-based intrusion detection through image-based CNN and transfer learning," in *20th International Wireless Communications and Mobile Computing Conference, IWCMC 2024*, 2024, pp. 386–391, doi: 10.1109/IWCMC61514.2024.10592364.
[25] Y. Sun and Z. Wang, "Intrusion detection in IoT and wireless networks using image-based neural network classification," *Applied Soft Computing*, vol. 177, 2025, doi: 10.1016/j.asoc.2025.113236.
[26] Y. Xu, H. Wang, K. Zhang, and Y. Han, "Ecological security assessment of urban park landscape using the DPSIR model and EW-PCA method," *Environment, Development and Sustainability*, vol. 26, no. 12, pp. 31301–31321, Jan. 2024, doi: 10.1007/s10668-024-04472-1.
[27] A. D. Vibhute, C. H. Patil, A. V. Mane, and K. V. Kale, "Towards detection of network anomalies using machine learning algorithms on the NSL-KDD benchmark datasets," *Procedia Computer Science*, vol. 233, pp. 960–969, 2024, doi: 10.1016/j.procs.2024.03.285.
[28] F. Nabi and X. Zhou, "Enhancing intrusion detection systems through dimensionality reduction: A comparative study of machine learning techniques for cyber security," *Cyber Security and Applications*, vol. 2, p. 100033, 2024, doi: 10.1016/j.csa.2023.100033.

BIOGRAPHIES OF AUTHORS

Nada Ali Abbood was born in Iraq, Karbala in 1987. She obtained her bachelor's degree in computer science entitled Design and implementation of electronic voting system using private network from the University of Karbala in 2009. She obtained her master's degree in computer from the Modern University for Business and Science in Lebanon in 2020. She is currently working on her Ph.D. thesis in the computer engineering department at Urmia University in Iran. She can be contacted at email: ndydyaaldyn031@gmail.com.

Asghar A. Asgharian Sardroud is an assistant professor in the computer engineering department at Urmia University, Iran. He earned his B.S. degree from Urmia University in 2007, M.S. degree from Sharif University of Technology in 2009, and Ph.D. degree from Amirkabir University of Technology in 2015, all in computer engineering. Since March 2015, he has been a faculty member at Urmia University, and in October 2019, he assumed the role of department head. His current research interests include network security, graph theory, graph algorithms, computer, software-defined networks, and computational geometry. In addition to his academic activities, he also collaborates with industry partners to implement practical solutions for emerging challenges in computer science. He can be contacted at email: a.asgharian@urmia.ac.ir.