Crime Anomaly Detection using CNN and Ensemble Model

Gautam Gupta[1], Prachi Aggarwal[2], Achin Jain[3], Puneet Singh Lamba[4], Arun Kumar Dubey[5], Gopal Chaudhary[6]

[1,2,3,5]Bharati Vidyapeeth's College of Engineering, India
[4,6]VIPS-TC, School of Engineering and Technology, India
Emails: gautamgupta1811@gmail.com; prachiaggarwal476@gmail.com; achin.mails@gmail.com ; singhs.puneet@gmail.com; arudubey@gmail.com; gopal.chaudhary88@gmail.com

***Correspondence:** achin.mails@gmail.com

Abstract

Every single day, thousands of crimes are perpetrated, and hundreds may be probably taking place right now throughout the world. Without a doubt, crime is viewed as a social blight. Nothing can truly stop it, no matter what is done. Surveillance cameras, on the other hand, can dramatically minimize it. Using public surveillance camera systems to prevent, document, and minimize crime can be a cost-effective solution. Installing enough cameras to detect crimes in progress and integrating technology to automate the monitoring of the live stream from these cameras will result in the most effective systems. Because of its self-learning characteristics, the advanced Artificial Intelligence surveillance system is constantly learning and improving. The Deep Learning Algorithms applied in this work processes videos using electronic devices like cameras in real-time termed as image processing, saving both human resources and a great deal of time. The highest accuracy of 86.6% was attained by Ensemble Model, followed by Inception Model with SGD Optimizer, Leaky Relu Activation Function giving an accuracy of 83.43%. Hence, anomalies were detected efficiently using decision making in real-time surveillance scenarios.

Keywords: Anomaly Detection; CNN; Ensemble Model; Deep Learning

1. Introduction

In this technological era, a colossal number of surveillance cameras are installed worldwide to monitor and detect daily anomalies. However, such many electronic devices like cameras generate a tremendous amount of video data. Monitoring of feeds from these surveillance cameras is challenging and adds a massive load on security teams. Therefore, it is necessary to automate the process of anomaly detection in real-time surveillance feeds. Furthermore, detection of an anomaly in surveillance videos is a significant challenge in computer vision. Thus, this problem has attracted many researchers around the world. So far, various video classification techniques have been applied to detect anomalies in real-time surveillance videos [15, 16]. This study aims to compare multiple Convolutional Neural Networks and find out the best parameters for these models.

As the cameras are continuously monitoring the areas, a large amount of data is generated every second. Some of the videos in the dataset were not clear which implied neutrosophic sets and gave the findings which generated partially true and partially false results. Processing such a tremendous amount of video [10] data is challenging and will require more computational resources. Therefore, dimensionality reduction is a must for the detection of an anomaly in real-time surveillance feed [4]. The dataset conditions were modified to work properly and give the proper findings. Deep Convolutional Neural Networks [2] have achieved high success in dimensionality reduction and Image classification. Compared to its predecessors, such as the simple network of fully connected layers, the CNN model can automatically detect important features without much human intervention.

Doi: https://doi.org/10.54216/FPA.110107
Received: December 08, 2022 Accepted: March 28, 2023

For this study, five Convolution Neural Networks viz. InceptionV3, ResNet50, ResNet101, VGG16, VGG19[19] were selected. Top-1 Accuracy for these models on ImageNet ranges from 74% to 79%, while top-5 Accuracy ranges from 91% to 95%. These models have achieved a high accuracy rate in various video classification tasks such as Activity Recognition and Video Summarization, making them apt for frame classification of surveillance videos. Different combinations of optimizer [3] and activation functions along these models have great potential in detecting the anomalies in real-time surveillance videos.

1.1 Optimizers included in the proposed study

- **Adam:** Proposed by Diederik P. Kingma *et al.; in* their paper Adam: A method of stochastic optimization, Adam is an algorithm for first-order gradient-based optimization of stochastic objective functions. It works well on problems with noisy or sparse gradients and non-stationary objectives while consuming less memory. Adam has helped machine learning practitioners to optimize their models better than regular gradient descent significantly. Adam [1] optimizer calculates the individual adaptive learning rate for each parameter from estimates of first and second moments of the gradients.
- **RMSprop:** First proposed by Geoff Hilton, RMSprop is an unpublished optimization algorithm designed for neural networks. It is the default optimizer for models implemented in Keras and TensorFlow. It is a stochastic technique for mini-batch learning. It has proved efficient in dealing with problems of vanishing and exploding gradients. It retains per-parameter learning rates that are adjusted depending on the weighted average of recent gradient magnitudes.
- **SGD:** SGD is an iterative method for optimizing the objective function with suitable differential and sub-differential smoothness properties. Its origin trackback to Robbins-Monro Algorithm. The simplicity of SGD makes it highly efficient for shallow networks. Moreover, as weights get updated after each iteration, SGD converges faster for mini-batch training.
- **Adagrad:** Adaptive Gradient Algorithm is a component adaptive learning rate-based stochastic optimization algorithm. It performs minor updates for frequently occurring features while more significant updates for less frequent features. Though it is computationally [9] expensive, it converges faster compared to standard stochastic gradient descent. In addition, it eliminates the need to update the learning rate manually and is less sensitive to the master step.

Another parameter that influences the detection competence is the Activation Function, which is used with the CNN model and Optimizer. It defines how different nodes in the Neural Network transform the weighted sum from the input into the output.

1.2 Activation functions included in the study

- **Softmax:** The softmax function as shown in figure 1 helps calculate the probability of a data point belonging to a particular class. Unlike sigmoid, it can be used for multiclass classification. Softmax is the default activation [5] for pre-built DCNN models available in Keras and TensorFlow frameworks.

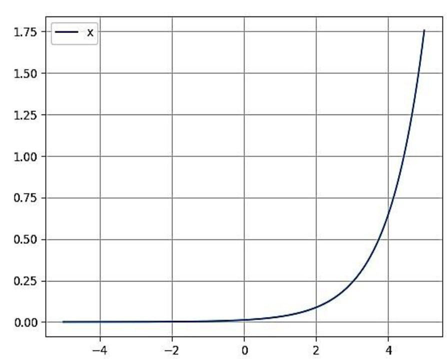

Figure 1: Softmax Activation Function

- **ReLU:** Rectified Linear Unit or ReLU[2] as shown in figure 2 is the most widely used activation function in neural networks. It provides more sensitivity of activation sum input while avoiding linear saturation. It

Doi: https://doi.org/10.54216/FPA.110107
Received: December 08, 2022 Accepted: March 28, 2023

resembles properties of linear function during backpropagation however is non-linear as it returns zero for non-positive values.

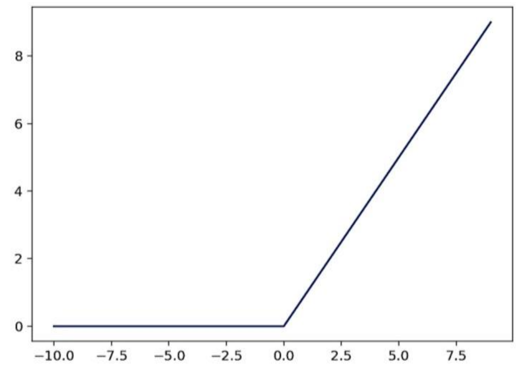

Figure 2: ReLU Activation Function

- **Leaky ReLU:** Rectified Linear Unit as shown in figure 3 may lead to the problem of vanishing gradient for negative inputs. Leaky ReLU[2] solves this problem by introducing a minimal negative component of x. It returns 0.01 times the input value for negative inputs, thus keeping a small gradient value for negative input.

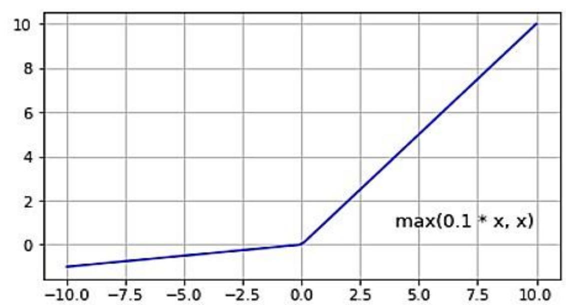

Figure 3: Leakey ReLU Activation Function

All in all, 54 different combinations using the above mentioned CNNS, optimizers and activation functions were trained, analysed, and compared to select the best possible combination for video frame.

2. Literature Survey

Anomaly detection based on deep learning is economical, reduces manual labour, increases efficiency and its decision-making capacity is comparatively trustworthy, protecting public safety. This section explores a brief introduction of some of the technologies used in the presented work and some of the currently available systems for detecting anomalies. CNN, or Convolutional Neural Network [11,12, 13], is a subject of deep learning that is primarily used to analyze visual data. It takes the dataset that has previously been provided to it for training purposes, which predicts the probable labels that are assigned later. Due to their excellent representation capabilities and remarkable performance, convolutional neural networks (CNNs) are the most used deep learning model today. CNN's have been used to solve a variety of computer vision and image processing challenges with great success. Three basic CNN models (shallow CNN, moderate CNN, and deep CNN) were put up, in a study, with varied internal depths to test how the depth affected the performance. Three distinct types of traffic datasets were used to test the models. Deeper structures, according to the findings, did not boost performance significantly. Also, CNN models that have been tested outperform VAE models occasionally. The efficiency of the LSTM network [14] in detecting and classifying abnormal events in sensor log files was examined in the study Long short-term memory-based operation log anomaly detection by Vinaykumar and et. al. The results of S-LSTM were compared to those of various network architectures. It was proposed that LSTM models are more resilient to anomaly detection than RNN prediction models based on the results of trials. This research was done on the dataset provided by Cyber Security Data Mining Competition (CDMC2016). In Real-world anomaly detection in surveillance videos research by Sultani W, et al. a MIL-based anomaly detection system was developed and trained on both normal and abnormal occurrences. To forecast anomaly scores, they

Doi: https://doi.org/10.54216/FPA.110107
Received: December 08, 2022 Accepted: March 28, 2023

employed deep anomaly ranking for video-level [17] labelling. In Anomaly locality in video surveillance by Landi et. al. an input tube was used to determine the action representation in the input video [18], and hybrid features, such as inception block and optical flow characteristics, were retrieved and combined using an average pooling layer before being sent into the regression network. By utilizing anomaly information, an anomalous events detection methodology based on learning rank for abnormal event identification was presented, and a MIL scheme based on the graph was constructed in an anomaly-introduced learning method for abnormal event detection.

Table1: Summary of Related Work

S.no	Author	Methodology	Datasets	Accuracy
1.	Kamalakar Vijay Thakarea (2022) [20]	Injecting temporal information in feature extraction	UCF-Crime	84.48
2.	Shuhan Yi (2022) [21]	Batch feature standardization module using a special standardization approach to facilitate the identification of obscure abnormal events	UCF-Crime	84.29
3.	Muhammad Zaigham Zaheer (2021) [22]	Supervised anomaly detection method is trained using only video-level labels	Frame-level AUC UCF-crime	78.27 84.16
4.	Jia-Xing Zhong (2019) [23]	A graph convolutional network was developed to correct noisy labels.	UCF-Crime	82.12
5	Md. Mijanur Rahman (2021) [24]	A fine-tuned ResNet-50 model was made to learn anomalous patterns by exploiting 14 types of anomalous images	14 Anomalous Images	79.69

3. Methodology

3.1 Dataset

This study uses UCF - Crime dataset (table 2) available on Kaggle by Mission-AI. The dataset has 400 anomalous and 150 normal surveillance feeds, making it legit for anomaly detections. The former is divided in the following two sections.

Table 2: UCF-Crime Dataset

Anomaly-Videos-Part 1	Anomaly-Videos-Part 2
1. Abuse 2. Arrest 3. Arson 4. Assault	1. Burglary 2. Explosion 3. Fighting

All the videos included in this research are 30 fps clips. Two text files are provided along with 550 videos which were used to evaluate the accuracy and loss scores [6].

3.2 Dataset Pre-processing

Frames [7] were extracted from each dataset video. The frames were grouped into 16 (as shown in figure 4 and 5) and resized to 1024 X 128 before feeding to the algorithm. Images thus obtained were fed to the neural network for training.

Figure 4: Sample Images with Anomaly

Doi: https://doi.org/10.54216/FPA.110107
Received: December 08, 2022 Accepted: March 28, 2023

Figure 5: Sample Images with No Anomaly

3.3 Model Architecture

Proposed Architecture (figure 6) consists of an Input layer at the top with dimensions 2048 X 256. Succeeding the input layer was a convolution network. Convolution Network [8] assisted in extracting essential features from the frames and reducing the dimensions. Output from Convolution Network was fed to Bi-Directional Long Short-Term Memory Layer, aiding in keeping the memory of previous frames to improve based on previous scenarios. Finally, the tensor obtained was flattened and fed to the Dense layer [20], which classified the combination of frames as anomalous or normal.

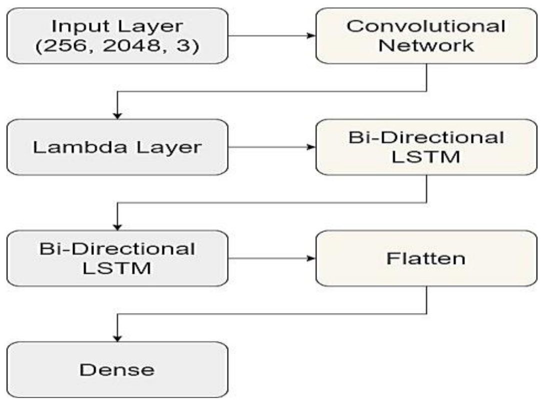

Figure 6: Model Architecture

3.4 Training

In the training phase, images were first loaded into the memory after resizing them to 2048 X 256 to match the dimensions of the input layer. The data was split in ratio 9:1 for training and testing, respectively. Anomalous and Normal classes were assigned a weight of 0.93 and 1.10 to constitute imbalanced frames in the dataset. These frames formed the input to the neural network. Afterward, the model was compiled with different activation functions and optimizers to ascertain the supreme combination for anomaly detection in real-time feeds. Table 3 consists of a summary of hyperparameters of different optimizers.

Table 3: Hyper-parameters of optimizers

Optimizer	Learning Rate
Adagrad	0.000001
Adam	0.01
RMS Prop	0.001
SGD	0.000001

Finally, the model was trained for 20 epochs. After training, the test dataset was input into the model. Different metrics were evaluated from the predictions obtained, and models were compared. The best three models were then selected. These were Ensembled to form a single model. The weights used for ensembling were set as individual accuracy of the model.

3.5 Proposed Ensemble Approach/ Framework

Doi: https://doi.org/10.54216/FPA.110107
Received: December 08, 2022 Accepted: March 28, 2023

In the prediction process, ensemble models are a machine learning strategy that combines several other models. For a particular dataset, a single algorithm may not be able to provide the optimal forecast. Machine learning algorithms have constraints and creating a high accuracy model is difficult. The overall accuracy of the model could be improved if we develop and merge numerous models. The combination can be accomplished by combining the outputs from each model with two goals in mind: lowering model error while retaining generality. Based on accuracies, three best combinations were chosen out of 54 training combinations for the proposed investigation. The above methodology employs the Weighted Average technique for data aggregation. To produce the final observations, weights were applied to individual models. The final findings are shown in the next section, indicating that the ensemble model provided the best accuracy of all the other combinations.

4. Results

In this work, training of 54 variations of Neural Networks by altering CNN models and different parameters like optimizer and activation functions have been performed. The output layer of the model uses a sigmoid function to classify the entire dataset into two categories i.e., anomaly and normal. The anomalies considered for the models are Arrest, Abuse, Arson, Burglary, Fighting, Explosion, and Assault along with a set of normal videos. Accuracy, Loss, Precision, Recall, F1Score, and AUC scores were evaluated for each model. The results obtained are summarized in tables below.

Tables 4-8 gives the count of accuracy score, Loss, F1 score, Precision Score, Recall score and AUC score for Inception Model, ResNet50, ResNet101, VGG16, VGG19 models respectively.

The Inception Model with SGD optimizer and Leaky Relu Activation function gives the highest accuracy of 83.43% as depicted in Table 4.

Doi: https://doi.org/10.54216/FPA.110107
Received: December 08, 2022 Accepted: March 28, 2023

Table 4: Different combination of optimizer and activation function with Inception Model

CNN	Optimizer	Activation	Accuracy	Loss	F1	Precision	Recall	AUC
Inception	Adam	Softmax	0.7442	0.2575	0.731	0.8718	0.7444	0.728
Inception	Adam	Relu	0.7058	0.2941	0.6997	0.7379	0.7058	0.696
Inception	Adam	Leaky Relu	0.7337	0.2662	0.7306	0.753	0.7337	0.727
Inception	SGD	Softmax	0.7123	0.2876	0.7434	0.7583	0.9016	0.726
Inception	SGD	Relu	0.6374	0.3625	0.6364	0.6364	0.6374	0.633
Inception	SGD	Leaky Relu	0.8343	0.1556	0.8438	0.8465	0.8443	0.841
Inception	RMS Prop	Softmax	0.7141	0.2858	0.7134	0.7141	0.7135	0.711
Inception	RMS Prop	Relu	0.6952	0.3047	0.6945	0.6945	0.6952	0.692
Inception	RMS Prop	Leaky Relu	0.6628	0.3371	0.6491	0.7084	0.6628	0.649
Inception	Adagrad	Softmax	0.8125	0.1875	0.8275	0.8372	0.8181	0.812
Inception	Adagrad	Relu	0.7223	0.2776	0.718	0.7493	0.7223	0.714
Inception	Adagrad	Leaky Relu	0.7377	0.2622	0.7377	0.7456	0.7494	0.742

Table 5: Different combination of optimizer and activation function with ResNet50 Model

CNN	Optimizer	Activation	Accuracy	Loss	F1	Precision	Recall	AUC
ResNet50	Adam	Softmax	0.5973	0.4026	0.5964	0.5961	0.5973	0.593
ResNet50	Adam	Relu	0.6882	0.3117	0.6875	0.6875	0.6882	0.685
ResNet50	Adam	Leaky Relu	0.6306	0.3691	0.6554	0.6511	0.7598	0.64
ResNet50	SGD	Softmax	0.7501	0.2498	0.7504	0.7524	0.7649	0.751
ResNet50	SGD	Relu	0.7237	0.2762	0.7235	0.7235	0.7237	0.722
ResNet50	SGD	Leaky Relu	0.6829	0.317	0.681	0.6823	0.6829	0.677
ResNet50	RMS Prop	Softmax	0.6665	0.3334	0.7154	0.731	0.9067	0.683
ResNet50	RMS Prop	Relu	0.6814	0.3185	0.7059	0.7089	0.8268	0.6916
ResNet50	RMS Prop	Leaky Relu	0.7567	0.2432	0.7694	0.7798	0.8779	0.765
ResNet50	Adagrad	Softmax	0.658	0.3419	0.7206	0.7576	0.9543	0.679
ResNet50	Adagrad	Relu	0.772	0.2279	0.7747	0.7834	0.8479	0.777
ResNet50	Adagrad	Leaky Relu	0.737	0.2629	0.7367	0.7367	0.737	0.735

Table 5 shows that ResNet50 with Adagrad optimizer and Relu activation function gives the highest accuracy of 77.2% with the minimum los of 22.79% for ResNet 50 model.

Table 6: Different combination of optimizer and activation function with ResNet101 Mode

CNN	Optimizer	Activation	Accuracy	Loss	F1	Precision	Recall	AUC
ResNet101	Adam	Softmax	0.6925	0.3074	0.6929	0.6949	0.7039	0.693
ResNet101	Adam	Relu	0.7009	0.299	0.6913	0.7546	0.7009	0.689
ResNet101	Adam	Leaky Relu	0.689	0.3109	0.6873	0.7067	0.689	0.68
ResNet101	SGD	Softmax	0.7966	0.2033	0.7969	0.8009	0.8329	0.799
ResNet101	SGD	Relu	0.6767	0.3232	0.7011	0.7033	0.8201	0.687
ResNet101	SGD	Leaky Relu	0.6852	0.3012	0.7123	0.7266	0.7145	0.672
ResNet101	RMS Prop	Softmax	0.7185	0.2814	0.7188	0.72	0.7208	0.719

Doi: https://doi.org/10.54216/FPA.110107
Received: December 08, 2022 Accepted: March 28, 2023

ResNet101	RMS Prop	Relu	0.7367	0.2632	0.7425	0.7498	0.8211	0.746
ResNet101	RMS Prop	Leaky Relu	0.7641	0.2358	0.7761	0.787	0.8843	0.773
ResNet101	Adagrad	Softmax	0.7702	0.2297	0.7707	0.7794	0.8351	0.775
ResNet101	Adagrad	Relu	0.8142	0.1857	0.8133	0.8273	0.8142	0.81
ResNet101	Adagrad	Leaky Relu	0.7999	0.2	0.7999	0.7998	0.7999	0.799

ResNet 101 with Adagrad optimizer and Relu activation function generates highest accuracy of 81.42% for the ResNet 101 model, as shown in table 6.

Table 7: Different combination of optimizer and activation function with VGG16 Model

CNN	Optimizer	Activation	Accuracy	Loss	F1	Precision	Recall	AUC
VGG16	Adam	Softmax	0.5931	0.4068	0.5721	0.6001	0.5931	0.577
VGG16	Adam	Relu	0.6783	0.3216	0.6593	0.7672	0.6783	0.661
VGG16	Adam	Leaky Relu	0.6952	0.3047	0.6945	0.6945	0.6952	0.692
VGG16	RMS Prop	Softmax	0.6089	0.391	0.583	0.6424	0.6089	0.591
VGG16	RMS Prop	Relu	0.7604	0.2395	0.7608	0.764	0.7882	0.762
VGG16	RMS Prop	Leaky Relu	0.634	0.3659	0.6222	0.6505	0.634	0.621
VGG16	Adagrad	Softmax	0.6526	0.3473	0.6218	0.7669	0.6526	0.632
VGG16	Adagrad	Relu	0.7653	0.2346	0.765	0.765	0.7653	0.763
VGG16	Adagrad	Leaky Relu	0.6633	0.3366	0.6403	0.7543	0.6633	0.645

Table 7 signifies that VGG16 with RMSProp optimizer and Relu activation function generates highest accuracy of 76.04% for the VGG16 model.

Table 8: Different combination of optimizer and activation function with VGG19 Model

CNN	Optimizer	Activation	Accuracy	Loss	F1	Precision	Recall	AUC
VGG19	Adam	Softmax	0.7181	0.2818	0.743	0.7539	0.8815	0.73
VGG19	Adam	Relu	0.7588	0.2411	0.7583	0.7585	0.7588	0.756
VGG19	Adam	Leaky Relu	0.6783	0.3216	0.7219	0.7367	0.9029	0.694
VGG19	RMS Prop	Softmax	0.6289	0.371	0.6268	0.6273	0.6289	0.623
VGG19	RMS Prop	Relu	0.6455	0.3544	0.618	0.7326	0.6455	0.626
VGG19	RMS Prop	Leaky Relu	0.7117	0.2882	0.7004	0.7865	0.7117	0.698
VGG19	Adagrad	Softmax	0.6577	0.3422	0.6554	0.6566	0.6577	0.652
VGG19	Adagrad	Relu	0.7095	0.2904	0.7098	0.711	0.7115	0.71
VGG19	Adagrad	Leaky Relu	0.7176	0.2823	0.7163	0.7173	0.7176	0.713

VGG19 with Adam optimizer and Relu activation function generates highest accuracy of 75.88% for the VGG19 model as shown in table 8. Loss for Incpetion ranges from 0.3625 to 0.1556, while loss for ResNet50 ranges from 0.4026 to 0.2279. Similarly, loss for ResNet 101, VGG16, and VGG19 ranges from 0.3216 to 0.1857, 0.3659 to 0.2395, and 0.3710 to 0.2823, respectively. The loss for ensemble model was least 0.1339. With Inception, Leaky Relu and SGD give the best result with an accuracy of 0.8343 and 0.7567 respectively. Leaky Relu and RMS prop give the best result with ResNet 50. Relu and Adagrad formed the best combination with ResNet 101 with accuracy as high as 0.8142. VGG16 has the best accuracy of 0.7604 with Relu and RMS prop, while VGG19 has the best accuracy of 0.7588 with Relu and Adam. However, ensembling of InceptionV3, ResNet101 and VGG16 resulted increased accuracy of 0.8660.

Doi: https://doi.org/10.54216/FPA.110107
Received: December 08, 2022 Accepted: March 28, 2023

Table 9: Proposed Ensemble Model Empirical findings

CNN	Accuracy	Loss	F1	Precision	Recall	AUC
Ensemble Model	0.8660	0.1339	0.8655	0.8669	0.8660	0.8628

The highest accuracy of 86.60% was attained by Ensemble Model with the minimal loss of 13.39% amongst all other models. The highest accuracy with least loss was given by the proposed Ensemble Model. The graphical representations of the above-mentioned results are shown in the form of comparative graphs for each value. Also, a comparative ROC for varied models is plotted to signify the comparisons among all the applied models. Figure 7 demonstrates the accuracy comparison displaying that the highest accuracy is achieved by the proposed ensemble model, followed by the loss comparison graph in figure 8. Figure 9. represents the F1 Score Comparison, with Ensemble Model having the highest score amongst all other models. Figure 10 and 11 depicts the Precision score and recall score comparisons respectively.

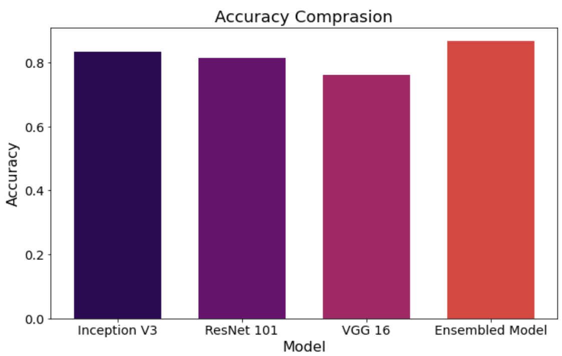

Figure 7: Accuracy Comparison

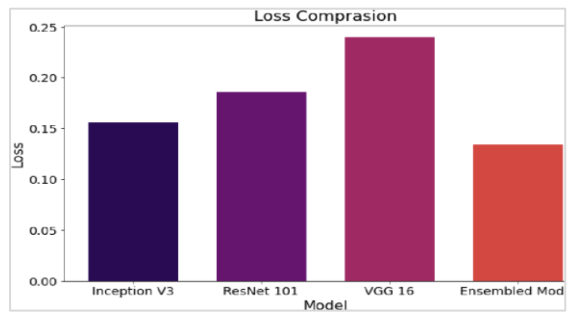

Figure 8: loss comparison

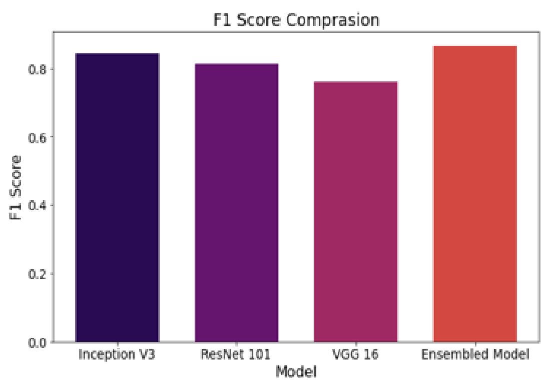

Figure 9: F1 Score Comparison

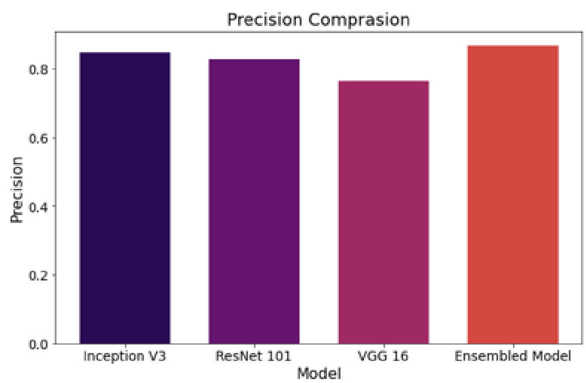

Figure 10: Precision score Comparison

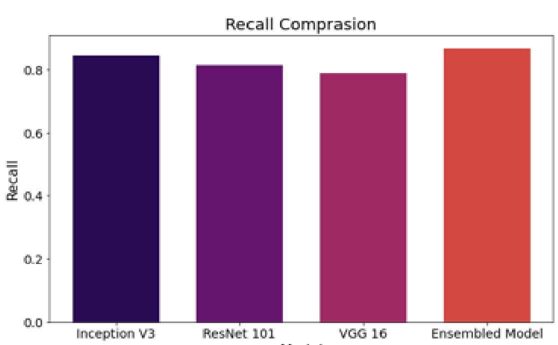

Figure 11: Recall score comparison

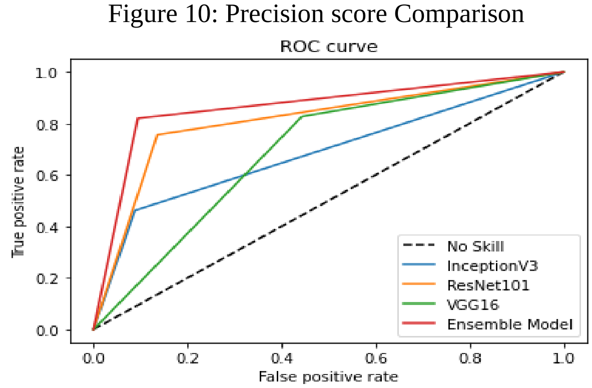

Figure 12: Comparative ROC

Doi: https://doi.org/10.54216/FPA.110107
Received: December 08, 2022 Accepted: March 28, 2023

The graph demonstrated in figure 12, is the pictorial representation of the comparative ROC curve for the pre-eminent combinations and ensemble model.

5. Conclusion

In this paper, various CNN models with different sets of optimizers and activation functions were compared. Although various combinations have a predilection for descrying the anomaly, Ensembling InceptionV3, ResNet101, VGG16 gave the best results. It can be concluded that the Ensemble Model of convolution models combined with the Bi-Directional LSTM layer can significantly detect anomalies in real-time surveillance feeds and diminish the work on security and surveillance teams.

References

[1] Kingma, D. P., & Ba, J. (2014). Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980.

[2] Dubey, A. K., & Jain, V. (2019). Comparative study of convolution neural network's relu and leaky-relu activation functions. In Applications of Computing, Automation and Wireless Systems in Electrical Engineering: Proceedings of MARC 2018 (pp. 873-880). Springer Singapore.

[3] Lydia, A., & Francis, S. (2019). Adagrad—an optimizer for stochastic gradient descent. Int. J. Inf. Comput. Sci, 6(5), 566-568.

[4] Ullah, W., Ullah, A., Hussain, T., Khan, Z. A., & Baik, S. W. (2021). An efficient anomaly recognition framework using an attention residual LSTM in surveillance videos. Sensors, 21(8), 2811.

[5] Sharma, S., Sharma, S., & Athaiya, A. (2017). Activation functions in neural networks. Towards Data Sci, 6(12), 310-316.

[6] Mohammadi, S., Perina, A., Kiani, H., & Murino, V. (2016). Angry crowds: Detecting violent events in videos. In Computer Vision–ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11–14, 2016, Proceedings, Part VII 14 (pp. 3-18). Springer International Publishing.

[7] Kamijo, S., Matsushita, Y., Ikeuchi, K., & Sakauchi, M. (2000). Traffic monitoring and accident detection at intersections. IEEE transactions on Intelligent transportation systems, 1(2), 108-118.

[8] Andrews, S., Tsochantaridis, I., & Hofmann, T. (2002). Support vector machines for multiple instance learning. Advances in neural information processing systems, 15.

[9] Kooij, J. F., Liem, M. C., Krijnders, J. D., Andringa, T. C., & Gavrila, D. M. (2016). Multi-modal human aggression detection. Computer Vision and Image Understanding, 144, 106-120.

[10] Giannakopoulos, T., Makris, A., Kosmopoulos, D., Perantonis, S., & Theodoridis, S. (2010). Audio-visual fusion for detecting violent scenes in videos. In Artificial Intelligence: Theories, Models and Applications: 6th Hellenic Conference on AI, SETN 2010, Athens, Greece, May 4-7, 2010. Proceedings 6 (pp. 91-100). Springer Berlin Heidelberg.

[11] Kim, J., Nguyen, A. D., & Lee, S. (2018). Deep CNN-based blind image quality predictor. IEEE transactions on neural networks and learning systems, 30(1), 11-24.

Doi: https://doi.org/10.54216/FPA.110107
Received: December 08, 2022 Accepted: March 28, 2023

[12] Kwon, D., Natarajan, K., Suh, S. C., Kim, H., & Kim, J. (2018, July). An empirical study on network anomaly detection using convolutional neural networks. In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS) (pp. 1595-1598). IEEE.

[13] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017, September). Long short-term memory-based operation log anomaly detection. In 2017 International Conference on Advances in Computing, Communications, and Informatics (ICACCI) (pp. 236-242). IEEE.

[14] Pang, S., Ban, T., Kadobayashi, Y., Song, J., Huang, K., Poh, G., ... & Aloul, F. (2020). CDMC'19—The 10th International Cybersecurity Data Mining Competition. In Neural Information Processing: 27th International Conference, ICONIP 2020, Bangkok, Thailand, November 23–27, 2020, Proceedings, Part II 27 (pp. 235-245). Springer International Publishing.

[15] Sultani, W., Chen, C., & Shah, M. (2018). Real-world anomaly detection in surveillance videos. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 6479-6488).

[16] Landi, F., Snoek, C. G., & Cucchiara, R. (2019). Anomaly locality in video surveillance. arXiv preprint arXiv:1901.10364.

[17] He, C., Shao, J., & Sun, J. (2018). An anomaly-introduced learning method for abnormal event detection. Multimedia Tools and Applications, 77, 29573-29588.

[18] Dubey, A. K., & Jain, V. (2020). Automatic facial recognition using VGG16 based transfer learning model. Journal of Information and Optimization Sciences, 41(7), 1589-1596.

[19] Mahadevan, V., Li, W., Bhalodia, V., & Vasconcelos, N. (2010, June). Anomaly detection in crowded scenes. In 2010 IEEE computer society conference on computer vision and pattern recognition (pp. 1975-1981). IEEE.

[20] Thakare, K. V., Sharma, N., Dogra, D. P., Choi, H., & Kim, I. J. (2022). A multi-stream deep neural network with late fuzzy fusion for real-world anomaly detection. Expert Systems with Applications, 201, 117030.

[21] Yi, S., Fan, Z., & Wu, D. (2022). Batch feature standardization network with triplet loss for weakly-supervised video anomaly detection. Image and Vision Computing, 120, 104397.

[22] Zaheer, M. Z., Lee, J. H., Astrid, M., Mahmood, A., & Lee, S. I. (2021). Cleaning label noise with clusters for minimally supervised anomaly detection. arXiv preprint arXiv:2104.14770.

[23] Zhong, J. X., Li, N., Kong, W., Liu, S., Li, T. H., & Li, G. (2019). Graph convolutional label noise cleaner: Train a plug-and-play action classifier for anomaly detection. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 1237-1246).

[24] Rahman, M. M., Afrin, M. S., Atikuzzaman, M., & Rahaman, M. A. (2021, December). Real-Time Anomaly Detection and Classification from Surveillance Cameras Using Deep Neural Network. In 2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI) (pp. 1-6). IEEE.

Doi: https://doi.org/10.54216/FPA.110107
Received: December 08, 2022 Accepted: March 28, 2023