A Technique and Architectural Design for Criminal Detection based on Lombroso Theory Using Deep Learning

Kiran Amjad^{1*}, Prof Dr. Aftab Ahmad Malik²

^{1,2} Department of Software Engineering Lahore Garrison University

¹Kiranamjad012@lgu.edu.pk

Abstract

Crimes and criminal activities are increasing day by day and there are no proper criteria to search, detect, identify, and predict these criminals. Despite various surveillance cameras in different areas still, crimes are at a peak. The police investigation department cannot efficiently detect the criminals in time. However, in many countries for the sake of public and private security, the initiation of security technologies has been employed for criminal identification or recognition with the help of footprint identification, fingerprint identification, facial recognition, or based on other suspicious activity detections through surveillance cameras. However, there are limited automated systems that can identify the criminals precisely and get the accurate or precise similarity between the recorded footage images with the criminals that already are available in the police criminal records. To make the police investigation department more effective, this research work presents the design of an automated criminal detection system for the prediction of criminals. The proposed system can predict criminals or possibilities of being criminal based on Lombroso's Theory of Criminology about born criminals or the persons who look like criminals. A deep learning-based facial recognition approach was used that can detect or predict any person whether he is criminal, or not and that can also give the possibility of being criminal. For training, the ResNet50 model was used, which is based on CNN and SVM Classifiers for feature extracting from the dataset. Two different labeled based datasets were used, having different criminals and noncriminals images in the database. The proposed system could efficiently help the investigating officers in narrowing down the suspects' pool.

Keywords: Lombroso Theory, Criminal Detection, Deep Learning, ResNet50, SVM.

1. INTRODUCTION

In daily life, the crimes are increasing rapidly and threaten the lives of innocent people. Currently, criminals have established different methods to replicate the corporal, biological

and interactive individualities. The efficient investigation can only be done by the timely prediction of suspects and the identification of criminals. With the advancement of technology, criminals have also adopted innovative ways to

escape. New and technologically strengthened methods must be established and assimilated with the outdated approaches or techniques and other camera-based surveillance systems to prevent crimes [1-2]. Many techniques have been developed in various courtiers for the detection of violence and criminal identifications based on fingerprints, DNA, Geofencing, social media data, and some other [3]. Raymond et al [4]

discussed that the police investigation based on DNA analysis could help in the development of partial evidence to support justice. Geofencing is the virtual demarcation of some area around a point of the offense for the detection of criminals and related information.

Win et al [5] discussed the fingerprints based system for the criminal investigation using machine learning algorithms for efficient detection of criminals. Among various methods, facial recognition is one the major and effective technique for the detection of person-related information that can be very useful for criminal detection [3]. Abdullah et al [6] presented the development of a criminal identification system based on facial image recognition from the criminal database. The proposed system can automatically detect the facial image of a criminal from the database with up to 80% efficiency. Elrefaei et al [7] presented a design of the system for real-time detection of criminals using facial image recognition and mobile phone tracking. This type of hybrid criminal identification system could be very useful for law enforcement and investigating agencies. However, few literature reports give an idea or mechanism of detection or prediction to find the possibility of being criminal among many suspects. Many research studies state that findings in the first impression could significantly contribute to the later rounds of investigations. The early intervention based on first impressions could strengthen the

hypothesis and leads towards convincing evidence [8-9].

1.1 Lombroso Philosophy

Italian criminologist Lombroso raised his voice for the detection of criminals based on facial looks. He was a mathematician and began to develop a desire for crime and morals. He settled certain cases based on his research work on criminal activities. He suggested the causes of the crime as it began described in [10]. After Cesare Lombroso (1853-1909) split in the Criminology field, many criminologists commented on and criticized Lombroso and [10-11]. In the late 80s and 90s, many crimes took places such as murder, theft, robbery, assaults, sexual assault and more. Lombroso argued that crime and being a criminal is a characteristic trait of human nature.

Figure 1: Born Criminals based on Lombroso Theory [1]

Historically, crime resolving has been a force for justice and criminal investigations have been the order of the day. However, with the improvement of computer systems, crime detection systems will be more effective in detecting criminals using a different amount of data through a data analyst, using this data can help police investigators and prosecutors to solve and evaluate crime more effectively and accurately [12]. Fraudulent detection is a way of finding out that whenever a person commits a crime he should lie during an investigation.

During the investigation, the heart rate sensor and Tobii glasses were used but in 2018 this method was changed [13].

There are many ways to investigate criminal activities; however, most of the systems cannot predict more accurate results. This research is aimed to target deeper aspects of learning to detect criminals according to the facial feature matching with renowned criminals that could also predict suspicious persons during the investigation process. The present research work is carried out to design a system that can predict or give the first impression about possible suspects or criminals, that can be used to aid the investigation process further. The proposed system can predict criminals or possibilities of being criminal is based on Lombroso's Theory of Criminology. A deep learning-based approach using the ResNet50 model is used for feature extracting of possible suspects.

In section [2] the related work has been discussed where different algorithms and approaches have been discussed for face recognition under different circumstances. Lombroso theory-based working has also been discussed which has given different accuracy factors using various algorithms deep learning models. In section [3] Deep learning-based model has been discussed for criminal's face recognition using the deep learning ResNet50 model for accurate feature extraction. In section [4] model-based Algorithm has been discussed which is going to elaborate the whole working of the Criminal prediction model using deep learning. Different Test datasets have also been given for the prediction of criminals. In the end, in section [5] the conclusion of the whole paper has been mentioned through which the criminal detection system can also be improved in the coming future.

2. RELATEDWORK

Rafter et al. [14] presented that Lombroso's Theory has been proposed for the opening of asylum to treat the criminal-minded persons which are not mentally stable and according to the theory of Cesare Lombroso, these criminals are one of those who have been getting this mental illness from their ancestors through inheritance. Due to this reason, they may behave like criminals [14].

Hashemi et al. [15] has proposed a system that is being dependent on Cesare Lombroso Theory of criminology. It has been proposed in the system that is used for face recognition and criminal detection as well. Face recognition is being used by the same feature extraction technique using the SVM model. The system was based on deep learning-based models with the accuracy at high rank. Mathur et al. [16] presented various surveillance systems to detect suspicious actions that can be monitored by surveillance cameras. It works on different parameters like face detection, hand detection, and to determine the link between the hand and face movements of the same person with different persons. For face detection, various artificially intelligent image extraction techniques and algorithms can be deployed. The Intelligent video-based surveillance system can efficiently help in crime prevention and real-time public security.

Thu et al. [17] discussed the identification of criminals has gone to be a more complicated and time-consuming process that needs a wide network and the access of time as well. Many different algorithms and techniques have been presented which have approximate accuracy in their systems but require more computational time as well as less accurate. Ultimately, an Edge-based Haar face detection and face identifier generation were used that were based on the Local Binary Pattern. In this algorithm,

any smart device will capture the image, after taking the image it will pass through different modes of identification then image generation identifier has applied to the image effect and extract the required facial facts. Finally, the comparison stage generates the results.

Apoorva et al. [18] proposed a new model that deals with image recognition and further share them with others. The main feature of the model was to compare the face with different images and then extract the required part of different images. Then different images would be determined by seeing the emotions on their faces. The model will have the friend list of the users and it matches the image with the friend list to make any similar or known person. The model was based on three layers, face detection with emotions, Face Recognition, and Auto Share Images. The model can detect 15 images at a time and then share the image with different people in a secure manner.

Currently, criminals are going to develop different emerging techniques and methods to imitate the corporal, biological, and communication individualities of legal operators which are known as spoofing assaults. To develop new countermeasures integrated with the traditional biometric systems. De Souza et al. [19] proposed a high accuracy attack detection system with less labeled data. The width-extended CNN model was trained to detect face spoofing.

Cuimei et al. [20] developed an application for automated surveillance where the objects can be recognized using that is being used for the facial detection process. These are the features through which the system is going to be trained, real-time face recognition using an automated surveillance camera. Face detection robustly in real-time environments is the system being used for criminal detection. Haar Cascading Algorithm, Haar-classifier, Open CV platform

are the methods used for face recognition and criminal detections and also for activity detection. The accuracy of a system is very high which is good for the system. The suggested system can effectively distinguish more than one expression which is a positive side of the article. The experimental results are very well satisfied through which the criminals can be detected easily.

3. LOMBROSOTHEORY-BASED CRIMINAL DETECTION MODEL USING FACE RECOGNITION

For criminal detection face recognition through feature, extraction has become a devastating technique that is going to be applied using an ancient Criminal Theory known as Lombroso Theory of Criminality. Lombroso's theory about the criminals of ancient ages that could be identified through feature extraction. There have been discussed many techniques for criminal detection and multiple applications for criminal identification and recognition and this research work a Lombroso theory-based face recognition model to detect criminals and predict the possibilities of being criminals among many suspects. Automated feature extraction with the help of CNN which eliminates the need for separate feature extraction and a selection step.

The classification of criminals is also termed as grading according to the nature of criminality. Normally, there are four groups namely felonies, infractions, felony-misdemeanors, misdemeanors. These are effective in grading the criminal target and aim. We study bio criminology which is the discipline of criminology regarding the investigation of crimes based on genetic factors and how they are concerned with criminal behavior. The central philosophy is focused mainly on inheritance, therefore, according to Lombroso, the structure of the face and bones reflect criminality exposure which can be compared

with normal humans (having no such signs) to identify criminals through physical defects.

It has been observed that the physical defects on the faces of the criminals are visible particularly those who have been involved in types of criminal Offences child abuse, kidnapping, domestic abuse assault and battery arson, and rape. However, the main offenses are proper crimes, violent crimes, property crime, organized crime, bank frauds consensual or victimless crimes, and nowadays white-collar crimes.

3.1 Face Recognition using Lombroso based Criminal Detection Model

The proposed Face Recognition using the Criminal Detection Model works on the feature extraction technique based on Lombroso Theory. In this model, there are multiple stages and phases

1. Data Training Phase
2. Validation/ Testing Phase

In every phase there are multiple stages which are going to be explained below:

3.2 Data Training Phase:

This is the first phase of the Face Recognition-based Criminal Detection Model which consists of multiple layers like the Data Acquisition Layer, Raw Data, Preprocessing Layer and the last one is Application Training Layer which is further subdivided into multiple layers.

3.3 Data Acquisition Layer:

The Data Acquisition Layer is used for collecting data related to Criminals. In this layer, the data would be collected through the criminal system or any other database of

criminals. In our case, the data would be in the form of classes. The first class would be criminal images and the second ones are citizens or non-criminals. In the Acquisition layer, the data would be made up of classified images

3.4 Data Pre Processing Layer:

When the data are classified into different classes then it will jump into the preprocessing layer. The preprocessing layer is going to handle the values amongst the raw data; after that normalization of the data has been done in the preprocessing layer. The normalization of data means to normalize the data based on the classification of images into different classes. If we talk about normalization this process has visualized the data and arranged the data in a classified manner. It will neglect the unwanted data material and arrange the classified data set for further sending to the next layer. Using this layer the missing values have been eliminated so that the images would be normalized for the further working of layers. In this layer, the classified images will be pre-processed based on features so the classified data has been analyzed for further working.

Batch normalization has been used for the normalization of images or datasets. Batch Normalization is a standardization technique that is used to improve the performance of CNN on image classification. It is used to shortens the effective depth to just tens instead of hundreds or thousands of layers makes deep networks easier to train.

3.5 Application Layer:

After the accomplishment of previous layers, the data will be transferred to other layers that are the application layer. The application layer consists of multiple sub-modules such as:

1. Prediction of Face Recognition layer (Feature Extraction)
2. Performance layer

3.6 Prediction or Face Detection Layer:

The prediction layer is a sub-layer or sub-module of an application layer. The prediction layer is focused on two algorithms first one is Resnet50 and the second one is SVM, which is used to decide whether a person is criminal or not. In the above-detailed model, it is clear that after going through the Resnet50 model prediction layer will generate the results that are based on SVM. The Support Vector Model provides the Computational Results that depend upon the structure of the neural network. The use of SVM at the end of fully connected layers of CNN can improve the classification performance of the overall pipeline. Automated feature extraction with the help of CNN which eliminates the need for separate feature extraction and a selection step. It could also be used at various first level investigation stages as well, in the prediction layer; it can be used to find out whether the person is criminal or not. Whereas the performance layer defines the result and the accuracy of the model. After completion of this layer, it will transfer to the Performance layer [21-22].

Figure 2: Lombroso Theory-based Criminal Detection Model using Face Recognition

3.7 Prediction Layer based Feature Extraction:

Prediction of expression recognition, we are applying deep learning so for applying deep learning on our classified data we are using two Algorithms Resnet50 and the other one is SVM. Figure 3.2 shows the convolution process using ResNet50 for feature extraction on the prediction layer [21].

Figure 3: Prediction Layer Feature Extraction Model

3.8 ResNEt50 Model:

Resnet50 is a CNN (Convolutional Neural Network) which is a pre-trained model, it is 50 layers deeper than CNN. Resnet50 has been trained in the ImageNet database of using more

than one million images. It has a total of 177 layers and consistent with 50 layers of the residual network. It consists of 5 stages where every stage has a convolution and identity block. Every identity block has furthermore 3 convolution and identity blocks. It is working as a deep residual network and popularly used for image sorting and classification [21].

3.9 Training Data:

First of all, the data would be going to train and that data is in a raw form. Data is going to be normalized and classified first and after that training will take place. Table 1 shows the two classes/ groups of datasets on which the model has been trained.

Table 1. Criminal Detection Parameters

Parameter	Description
Class 1	Criminals
Class 2	Non-Criminals

In Table 1 the parameters or the classification of the model have been used which is classified into two classes first one is Criminal Class and the second one is Citizen Class. On which basis we train the dataset, get the performance, and predict the model results.

3.10 Maintaining Dataset

The dataset is an essential part of the field of presentation and predicting criminals and it offers accurate results using the SVM classifier through ResNet50. The information could be utilized as a benchmark for the execution and forecast of criminal identification. Examination of information can give guidance towards upgrading the exhibition of the frameworks and aiding in distinguishing the assets needed for the dataset preparing and testing

administrations of the criminal discovery model.

Table 2. Dataset Description

Subject area	Criminal detection based on face recognition features extraction through Lombroso Theory using Deep Learning
Nature of data	Images
Development of Data	The data were composed of the internet through FBI recorded criminals images and some other non-criminals images also collected through the internet sources. It is collected using an SVM image Classifier and distributed in different labeled classes.
Data organization	Class labeled form of Raw data(images)
Investigational factors	The training dataset which is up to 2500-3000 images and the testing dataset which is up to 850 images and all the dataset consists of static images. The whole model consists of 50 layers, 1 epoch value in ResNet50 is 0-50 iterations in each layer. 1 epoch against iterations 43 approx. iterations 430.
Features based Experiments	The analysis expects to assemble expectation models. The primary model is utilized to gain from a classified dataset based on images and predict whether the person is criminal or not. The data set that is used in this experimental model holds 2500-28,147 images. An arbitrary dataset of 850 images is used as a testing data set. In the process of training and testing the result is collected based on features extraction like tip nose, sharp jaw dark eyes, etc. based on Lombroso Theory and get the accuracy of 99% through using the ResNet50 model for criminal detection and the SVM model classifier for classifying images based on labeled dataset images.
Data source location	Through the Internet different images from different websites and FBI websites as well.
Data accessibility	Data is available with this research paper.

3.10.1 Criminal Dataset

It contains the criminal's images which we can get through open access from the internet. Here are some of the images from our dataset which contain criminals images based on Lombroso theory's facial features. We collect almost 2000 criminal images through the internet and labeled the data as criminal images. The dataset uses in this section is correlate with the Lombroso theory as it has some sort of features related to Lombroso explained theory of criminality. Lombroso's theory's face features of criminals have to be examined for the construction of a dataset of criminals. Only those images have been chosen for making a dataset of criminals which were following Lombroso Theory based on the following features :

1. The projection of the lower face and jaws (prognathous)
2. Oblique eyelids

3. A nose with a “tip rising like an isolated peak from the swollen nostrils
4. Tattoos on the body
5. A hooked nose

Figure 4: Criminals Dataset

3.10.2 Non-Criminal Dataset

It contains a non-criminals dataset which consists of approx. 2000 non-criminals images. We can openly access these images through the internet, the dataset is classified as non-criminal or citizens.

Figure 5: Non-Criminal Dataset

3.11 Training Model:

In this training phase, we discuss the number of epoch values of our model. The number of epoch is the number of iterations or the number

of times the whole model has completed its cycle through the data. The more epoch values we are going to run the more will be the model improved. In our Resnet50 model epoch values are 50 means in each epoch 50 iterations will take place and in this way, the whole model will be trained. Figure 6 shows the training process of the dataset.

```
75/75 [=====] - 41s 540ms/step - loss: 0.8084 - accuracy: 0.9971 - val_loss: 0.4937e-04 - val_accuracy: 1.0000
Epoch 23/50
75/75 [=====] - 41s 547ms/step - loss: 0.8116 - accuracy: 0.9966 - val_loss: 0.8028 - val_accuracy: 1.0000
Epoch 24/50
75/75 [=====] - 41s 540ms/step - loss: 0.8061 - accuracy: 0.9992 - val_loss: 5.2938e-04 - val_accuracy: 1.0000
Epoch 25/50
75/75 [=====] - 42s 553ms/step - loss: 0.8068 - accuracy: 0.9997 - val_loss: 9.2803e-04 - val_accuracy: 1.0000
Epoch 26/50
75/75 [=====] - 41s 558ms/step - loss: 0.8094 - accuracy: 0.9966 - val_loss: 4.1423e-04 - val_accuracy: 1.0000
Epoch 27/50
75/75 [=====] - 41s 547ms/step - loss: 0.8111 - accuracy: 0.9958 - val_loss: 0.8298 - val_accuracy: 0.9875
Epoch 28/50
75/75 [=====] - 41s 543ms/step - loss: 0.8093 - accuracy: 0.9975 - val_loss: 0.8016 - val_accuracy: 1.0000
Epoch 29/50
75/75 [=====] - 41s 546ms/step - loss: 0.8180 - accuracy: 0.9882 - val_loss: 0.1591 - val_accuracy: 0.9438
Epoch 30/50
75/75 [=====] - 41s 548ms/step - loss: 0.8048 - accuracy: 0.9700 - val_loss: 0.8351 - val_accuracy: 0.9812
Epoch 31/50
75/75 [=====] - 41s 540ms/step - loss: 0.8138 - accuracy: 0.9945 - val_loss: 0.8014 - val_accuracy: 1.0000
Epoch 32/50
75/75 [=====] - 41s 555ms/step - loss: 0.8125 - accuracy: 0.9949 - val_loss: 0.8034 - val_accuracy: 1.0000
Epoch 33/50
75/75 [=====] - 41s 553ms/step - loss: 0.8057 - accuracy: 0.9983 - val_loss: 0.8038 - val_accuracy: 0.9958
Epoch 34/50
75/75 [=====] - 41s 548ms/step - loss: 0.8073 - accuracy: 1.0000 - val_loss: 0.8400e-04 - val_accuracy: 1.0000
Epoch 35/50
75/75 [=====] - 41s 547ms/step - loss: 0.8161 - accuracy: 0.9941 - val_loss: 0.8013 - val_accuracy: 1.0000
Epoch 36/50
```

Figure 6: Training Model dataset of feature extraction

3.12 Classification Model:

This is the last layer of the proposed model which is to classify the data and here it is classified into two nodes; which decide whether a person could be a possible criminal suspect or not. This is based on these 2 nodes probability which node has high probability first one is for accuracy and the second one is for miss rate that is discussed in the Resnet50 model. For the classification of the model, we use the SVM model (Support Vector Machine) that classifies images or data into labeled data of two classes. Figure 3.5 shows the process of future extraction on the classification layer. The figure shows the classification layer process.


```

75/75 [=====] - 41s 540ms/step - loss: 0.0185 - accuracy: 0.9983 - val_loss: 0.0027 - val_accuracy: 1.0000
Epoch 37/50
75/75 [=====] - 41s 540ms/step - loss: 0.0058 - accuracy: 0.9987 - val_loss: 6.6931e-04 - val_accuracy: 1.0000
Epoch 38/50
75/75 [=====] - 41s 550ms/step - loss: 0.0022 - accuracy: 0.9996 - val_loss: 0.0227e-04 - val_accuracy: 1.0000
Epoch 39/50
75/75 [=====] - 41s 548ms/step - loss: 0.0008 - accuracy: 0.9996 - val_loss: 4.8555e-04 - val_accuracy: 1.0000
Epoch 40/50
75/75 [=====] - 42s 553ms/step - loss: 0.0059 - accuracy: 0.9979 - val_loss: 8.1138e-04 - val_accuracy: 1.0000
Epoch 41/50
75/75 [=====] - 41s 540ms/step - loss: 0.0048 - accuracy: 0.9983 - val_loss: 8.0756e-04 - val_accuracy: 1.0000
Epoch 42/50
75/75 [=====] - 41s 540ms/step - loss: 0.0058 - accuracy: 0.9979 - val_loss: 4.1914e-04 - val_accuracy: 1.0000
Epoch 43/50
75/75 [=====] - 41s 552ms/step - loss: 0.0036 - accuracy: 0.9992 - val_loss: 3.3679e-04 - val_accuracy: 1.0000
Epoch 44/50
75/75 [=====] - 41s 547ms/step - loss: 0.0054 - accuracy: 0.9979 - val_loss: 3.6071e-04 - val_accuracy: 1.0000
Epoch 45/50
75/75 [=====] - 41s 546ms/step - loss: 0.0035 - accuracy: 0.9983 - val_loss: 2.0147e-04 - val_accuracy: 1.0000
Epoch 46/50
75/75 [=====] - 41s 540ms/step - loss: 0.0015 - accuracy: 0.9996 - val_loss: 1.7373e-04 - val_accuracy: 1.0000
Epoch 47/50
75/75 [=====] - 42s 553ms/step - loss: 0.0015 - accuracy: 1.0000 - val_loss: 2.3991e-04 - val_accuracy: 1.0000
Epoch 48/50
75/75 [=====] - 41s 553ms/step - loss: 0.0041 - accuracy: 0.9987 - val_loss: 1.6875e-04 - val_accuracy: 1.0000
Epoch 49/50
75/75 [=====] - 41s 548ms/step - loss: 0.0021 - accuracy: 0.9992 - val_loss: 0.0011 - val_accuracy: 1.0000
Epoch 50/50
75/75 [=====] - 41s 548ms/step - loss: 0.0039 - accuracy: 0.9996 - val_loss: 2.4095e-04 - val_accuracy: 1.0000

```

Figure 7: Classification layer feature extraction

4. RESULTS AND DISCUSSIONS

In this section, the overall working of the algorithm has been discussed. The proper flow of algorithm discusses the whole model working step by step and after that trained and testing datasets have been declared. The losing graph and accuracy graph has discussed the accuracy of the ResNet50 model through which criminality can be predicted. Different test results have been mentioned which explains the system overall working.

4.1 Working of Algorithm:

The novel idea of computational work is useful when the arrested criminal suspects are in large numbers and then there is a need to start the investigation process first from the most probable suspect and to know how many of them are criminal minded. Police Check Posts can also use the system to randomly access and predict the possible suspects of crimes. The idea uses physical appearances as well as appearances of the state of the human face and body which is according to Lombroso theory. The pseudo-code of the entire system is given below in figure 8:

Figure 8: Pseudo-code of the entire system

Step 1: In the first step, the extract properties will extract all the properties that have to be given for the training model. The extracted properties will be mapped according to the features extractions that have been trained to the given dataset using the ResNet50 model. In the Extraction, Properties will be a collection of properties of facial structure and bone structure as well. The extraction properties will collect the dataset based on features being trained in the proposed system.

Step 2: In this step, the model will check the trained dataset whether the classified image belongs to the criminal or civil side. In the whole process, the trained model ResNet50 will check the images one by one and make multiple iterations to scan the images and to verify that whether the person's image belongs to the criminal's featured dataset or the citizens. The iterations will continue until the verification of dataset images complete.

Step 3: In this step, the dataset will match the images to the ResNet50 based features of criminals that are the face features belongs to Lombroso Theory-based criminals. The parameters of images will check or verify the face features of the trained criminal dataset and extract the facial features to the classified

images. The ResNet50 Model is going to train the images according to the features being trained to the classified dataset of images.

Step 4: In this step, the trained model has matched the images according to the trained ResNet50 features of images. The images are classified into 2 different classes so when the system picks to verify any image, then it will train the dataset according to the features of two labeled classes and get the results. The features that are being extracted from the images are based on the Lombroso Theory of Criminology.

Step 5: This is the last step of the algorithm where the result has been made clear that whether the images belong to the criminal images dataset or the citizen's dataset. After that process results are declared using the ResNet50 model algorithm.

The performance of a model can be calculated and measured using CNN based ResNet50 algorithm to get the best results. For training purposes, the SVM model has been used which contains approx. 2500 images dataset. Using this model, we have achieved a reasonable prediction.

4.2 Test Dataset of Criminals:

The test dataset contains the accuracy of Criminals which describes for these test images, the possibility of being criminal is high. The accuracy is attained through the labeled class dataset of criminals.

Figure 9: Prediction of criminals on test images

4.3 Loosing Function:

Losing is figured on validation and training as well as its interpretation relies on how well the version/model performed in both of these sets. It's the number of mistakes created for each case in training or approval sets. Loss value signifies badly or a version acts after every iteration of testing and training.

Figure 10: Losing Values of Criminal Detection Model

The figure 5.6 shows the losing value of our model it also shows that the loss value is not that high that's why the rate of mistakes in our model is very less. In our model Accuracy values is very high than the losing value.

Figure 11: Accuracy graph of Criminal Detection Model

Figure 5.7 describes the accuracy rate of our criminal detection model that is being implemented on two labeled based classes. And we got the highest accuracy of feature detection. The table shows the feature detection of the model.

Table 3. Accuracy of detection

Accuracy	Miss Rate	Results
0.992	0.001	Positive Result

These results show the positive predicted value which shows the accuracy of the trained model and the miss rate for performance prediction. There can be different classes while we training our model e.g. in this case two classes are used which are criminals and non-criminals or citizens.

5. CONCLUSION

For the experimental results, the ResNet50 model is used by having Keras python based library functions used as a tool for gathering the simulation results and taking the advancement of algorithms as well. The interpretation of results is taken by having 2500 images as an input in the training dataset and 800 used for the testing dataset. The images that are used as

an input in the raw dataset for classification are the static images and having high detection accuracy with a low 2.40 miss rate. Therefore, we establish the superiority of the proposed system being efficient, reliable. However, Characterizing individuals in any way requires care and safety yet anticipating whether an individual is a criminal or not requests significantly more alert and investigation must be viewed with strengthened evidence. Most of the risk of this innovation lies in its limitations. Meanwhile, the misclassifying or wrong prediction of the suspect could have crucial consequences and it can be a more disable job for us as well. Because still there exist the possibility that a suspect may look like a criminal but actually not. Therefore the proposed system could only generate the prediction of the possibility of being criminal; which may be useable as a first impression only for the investigation process. It is also to be suggested that the proposed system may be utilized as a tool to aid a quick start the investigation process but not as a decision system. Furthermore, the prediction efficiency of the system can be improved in future by considering other social attitudes of the suspects and causation theories.

References

- [1] Dawson, M. (Ed.). (2015). New threats and countermeasures in digital crime and cyber terrorism. IGI Global.
- [2] Tilley, N. (2002). Evaluation for Crime Prevention. Crime Prevention Studies, Volume 14. Criminal Justice Press.
- [3] Fatih, T., & Bekir, C. (2015). Police use of technology to fight against crime. European scientific journal, 11(10).

- [4] Prime, R. J., & Newman, J. (2007). The impact of DNA on policing: Past, present, and future. *POLICE CHIEF*, 74(11), 30.
- [5] Win, K. N., Li, K., Chen, J., Viger, P. F., & Li, K. (2020). Fingerprint classification and identification algorithms for criminal investigation: A survey. *Future Generation Computer Systems*, 110, 758-771.
- [6] Abdullah, N. A., Saidi, M. J., Rahman, N. H. A., Wen, C. C., & Hamid, I. R. A. (2017, October). Face recognition for criminal identification: An implementation of principal component analysis for face recognition. In *AIP Conference Proceedings* (Vol. 1891, No. 1, p. 020002). AIP Publishing LLC.
- [7] Elrefaei, L. A., Alharthi, A., Alamoudi, H., Almutairi, S., & Al-rammah, F. (2017, March). Real-time face detection and tracking on mobile phones for criminal detection. In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)* (pp. 75-80). IEEE.
- [8] Engel, C., Beckenkamp, M., Glöckner, A., Irlenbusch, B., Hennig-Schmidt, H., Kube, S., ... & Towfigh, E. (2014). First impressions are more important than early intervention: Qualifying broken windows theory in the lab. *International Review of Law and Economics*, 37, 126-136.
- [9] Poland, V. L. (2017). *Impression Management and Deception in Witnesses and Suspects*. Southern Connecticut State University.
- [10] Saidi, F., Trabelsi, Z., & Ghazela, H. Ben. (2018). A novel approach for terrorist sub-communities detection based on constrained evidential clustering. *Proceedings - International Conference on Research Challenges in Information Science*, 2018-May, 1-8. <https://doi.org/10.1109/RCIS.2018.8406663>
- [11] Thu, K. M. M., & Thein, N. N. M. (2019). Edge-based Crime Assistance System with Cloud Computing. *2019 International Conference on Advanced Information Technologies, ICAIT 2019*, 43-48. <https://doi.org/10.1109/AITC.2019.8920883>
- [12] Pavithra, R., & Suresh, K. V. (2019). Fingerprint image identification for crime detection. *Proceedings of the 2019 IEEE International Conference on Communication and Signal Processing, ICCSP 2019*, 797-800. <https://doi.org/10.1109/ICCSP.2019.8698014>
- [13] Gangwar, A., Fidalgo, E., Alegre, E., & González-Castro, V. (2017). Pornography and child sexual abuse detection in image and video: A comparative evaluation. *IET Seminar Digest*, 2017(5), 37-42. <https://doi.org/10.1049/ic.2017.0046>
- [14] Rafter, N. (2005). Cesare Lombroso and the origins of criminology: Rethinking criminological tradition. *Publifarum*, (1), 6-6.
- [15] Hashemi, M., & Hall, M. (2020). Criminal tendency detection from facial images and the gender bias effect. *Journal of Big Data*, 7(1), 1-16.
- [16] Mathur, G., & Bunde, M. (2016). *Research on Intelligent Video*

Surveillance techniques for suspicious activity detection critical review. 2016 International Conference on Recent Advances and Innovations in Engineering, ICRAIE 2016, 2016, 1–8. <https://doi.org/10.1109/ICRAIE.2016.7939467>

- [17] Thu, K. M. M., & Thein, N. N. M. (2019, November). Edge based Crime Assistance System with Cloud Computing. In 2019 International Conference on Advanced Information Technologies (ICAIT) (pp. 43-48). IEEE.
- [18] Apoorva, P., Impana, H. C., Siri, S. L., Varshitha, M. R., & Ramesh, B. (2019, March). Automated Criminal Identification by Face Recognition using Open Computer Vision Classifiers. In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC) (pp. 775-778). IEEE.
- [19] de Souza, G. B., da Silva Santos, D. F., Pires, R. G., Papa, J. P., & Marana, A. N. (2018, October). Efficient Width-Extended Convolutional Neural Network for Robust Face Spoofing Detection. In 2018 7th Brazilian Conference on Intelligent Systems (BRACIS) (pp. 230-235). IEEE.
- [20] Cuimei, L., Zhiliang, Q., Nan, J., & Jianhua, W. (2017, October). Human face detection algorithm via Haar cascade classifier combined with three additional classifiers. In 2017 13th IEEE International Conference on Electronic Measurement & Instruments (ICEMI) (pp. 483-487). IEEE.
- [21] Theckedath, D., & Sedamkar, R. R. (2020). Detecting Affect States Using VGG16, ResNet50 and SE-ResNet50 Networks. SN Computer Science, 1(2), 1-7.
- [22] Guo, G., Li, S. Z., & Chan, K. L. (2001). Support vector machines for face recognition. Image and Vision computing, 19(9-10), 631-638.