IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114167

Face Pin: Face Biometric Authentication system for ATM Using Deep Learning

G. Anusha Bhuvaneshwari[1], Anbumozhi V[2], Deepika R[3], Gokul M[4]

Assistant Professor, Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India[1]

UG Scholar, Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India[2-4]

Abstract: Automated Teller Machines also known as ATM's are widely used nowadays by each and everyone. There is an urgent need for improving security in banking region. Due to tremendous increase in the number of criminals and their activities, the ATM has become insecure. ATM systems today use no more than an access card and PIN for identity verification. The recent progress in biometric identification techniques, including finger printing, retina scanning, and facial recognition has made a great effort to rescue the unsafe situation at the ATM. This project proposes an automatic teller machine security model that would combine a physical access card and electronic facial recognition using Deep Convolutional Neural Network. If this technology becomes widely used, faces would be protected as well as their accounts. Face Verification Link will be generated and sent to user to verify the identity of unauthorized user through some dedicated artificial intelligent agents, for remote certification. However, it obvious that man's biometric features cannot be replicated, this proposal will go a long way to solve the problem of Account safety making it possible for the actual account owner alone have access to his accounts

Keyword: Deep learning, biometric techniques

INTRODUCTION:

Face recognition can be used to secure ATM transaction and is used as a tool for authenticating users to confirm the card owner. Financial fraud is a very important problem for Banks and current secure information in the ATM card magnetic tape are very vulnerable to theft or loss. By using face recognition as a tool for authenticating users in ATMs can be confirmed as the card owner. Face Based ATM login Process the ATMs which are equipped with Face recognition technology can recognize the human face during a transaction. When there are "Shoulder Surfers" who try to peek over the cardholder's shoulder to obtain his PIN when the cardholder enters it, the ATMs will automatically remind the cardholder to be cautious. If the user wears a mask or sunglasses, the ATM will refuse to serve him until the covers are removed.

Touchless - There is no need for remembering your passwords. Only looking at the ATM camera will login the card holder instantly. No physical contact is needed.

Secure - Since your face is your password, there is no need to worry for your password being forgotten or stolen. In addition, the face recognition engine locks access to the account and transaction pages for the card holder as the card holder moves away from the camera of the ATM and another face appears

Face based card holder authentication can be used as primary or as a secondary authentication measure along with ATM PIN. Face based authentication prevents ATM fraud by the use of fake card and stolen PIN or stolen card itself. Face verification is embedded with security features to prevent fraud, including liveness-detection technology that detects and blocks the use of photographs, videos or masks during the verification process.

EXISTING SYSTEM:

Biometrics measure the unique physical or behavioral characteristics of an individual as a means to recognize or authenticate their identity. Common physical biometrics include fingerprints, hand or palm geometry, and retina, iris, or facial characteristics. Biometrics may be used for identity establishment. A new measurement that purports to belong to a particular entity is compared against the data stored in relation to that entity. If the measurements match, the assertion that the person is whom they say they are is regarded as being authenticated. The algorithms were trained and tested using a well-known biometric database which contains samples of face and speech and similarity scores of five face and three speech biometric experts.

Disadvntage:

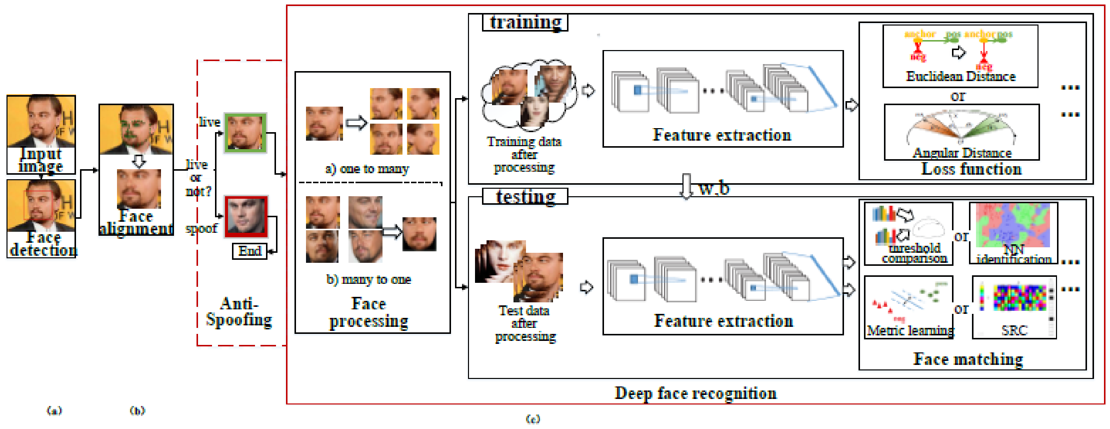
- The accuracy of the system is not 100%.
- Face detection and loading training data processes just a little bit slow.
- It can only detect face from a limited distance.
- It cannot repeat live video to recognize missed faces.
- The instructor and training Set manager still have to do some work manually.
- Unimodal biometric systems have to contend with a variety of problems such as noisy data, intraclass variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates.
- This method is not very secure and prone to increase in criminal activities.
- QRcode scanner is required to detect code
- Should carry the mobile phone with app installed on it

PROPOSED SYSTEM:

This project proposes an automatic teller machine multi modal security model that would combine a physical access card and electronic facial recognition using Deep Convolutional Neural Network.

- **Facial Biometric Authentication System using Deep Learning Techniques**

Deep learning is a subset of machine learning, which, in turn, is a subset of artificial intelligence (AI). When it comes to Face recognition, deep learning enables us to achieve greater accuracy than traditional machine learning methods.



Deep FR system with face detector and alignment. First, a face detector is used to localize faces. Second, the faces are aligned to normalized canonical coordinates. Third, the FR module is implemented. In FR module, face anti-spoofing recognizes Whether the face is live or spoofed; face processing is used to handle variations before training and testing, e.g., poses, ages; Different architectures and loss functions are used to extract discriminative deep feature when training; face matching methods are used to do feature classification after the deep features of testing data are extracted.

DOI: 10.17148/IJARCCE.2022.114167

CNN Face Recognition Step

Filters=32: This number indicates how many filters we are using to look at the image pixels during the convolution step. Some filters may catch sharp edges, some filters may catch color variations some filters may catch outlines, etc. In the end, we get important information from the images. In the first layer the number of filters=32 is commonly used, then increasing the power of 2. Like in the next layer it is 64, in the next layer, it is 128 so on and so forth.

kernel size=(5,5): This indicates the size of the sliding window during convolution, in this case study we are using 5X5 pixels sliding window.

strides= (1, 1): How fast or slow should the sliding window move during convolution. We are using the lowest setting of 1X1 pixels. Means slide the convolution window of 5X5 (kernal_size) by 1 pixel in the x-axis and 1 pixel in the y-axis until the whole image is scanned.

input shape= (64,64,3): Images are nothing but matrix of RGB color codes. during our data pre-processing we have compressed the images to 64X64, hence the expected shape is 64X64X3. Means 3 arrays of 64X64, one for RGB colors each.

kernel_initializer='uniform': When the Neurons start their computation, some algorithm has to decide the value for each weight. This parameter specifies that. You can choose different values for it like 'normal' or 'glorot_uniform'.

activation='relu': This specifies the activation function for the calculations inside each neuron. You can choose values like 'relu', 'tanh', 'sigmoid', etc.

optimizer='adam': This parameter helps to find the optimum values of each weight in the neural network. 'adam' is one of the most useful optimizers, another one is 'rmsprop'

batch_size=10: This specifies how many rows will be passed to the Network in one go after which the SSE calculation will begin and the neural network will start adjusting its weights based on the errors. When all the rows are passed in the batches of 10 rows each as specified in this parameter, then we call that 1-epoch. Or one full data cycle. This is also known as mini-batch gradient descent. Hence a proper value must be chosen using hyperparameter tuning.

Epochs=10: The same activity of adjusting weights continues for 10 times, as specified by this parameter.

- **Unknow Face Verification Link Generator** –

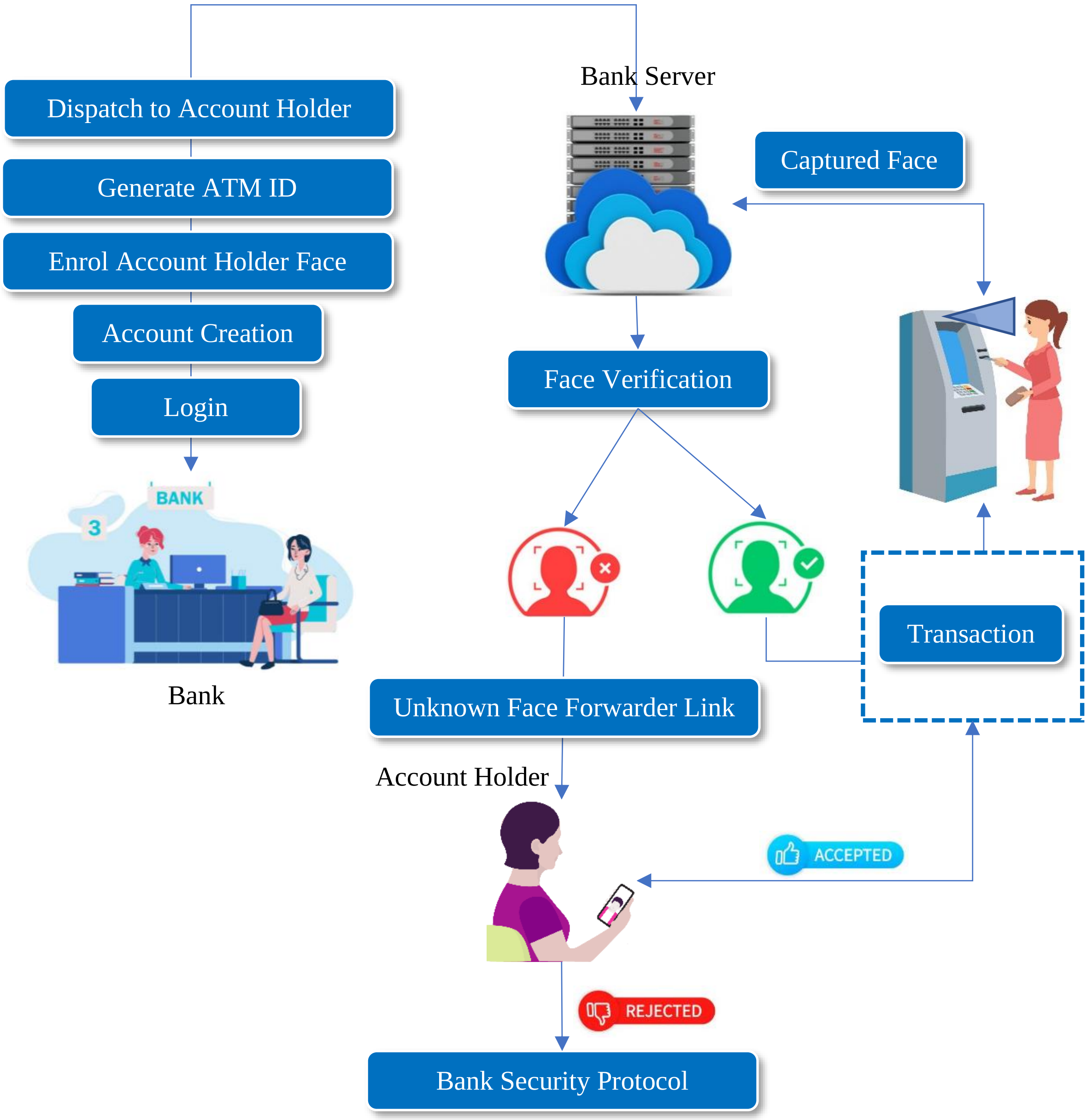
When the stored image and the captured image don't match, it means that he is an unauthorized user. Face Verification Link will be generated and sent to user to verify the identity of unauthorized user through some dedicated artificial intelligent agents, for remote certification, which either authorizes the transaction appropriately or signals a security-violation alert to the banking security system.

Advantages

- The advantages can be found as that the face-id is unique for everybody; it cannot be used by anybody other than the user.
- It can be used to reduce fraudulent attempts.
- To prevent theft and other criminal activities.
- Secure facial authentication platform that users can trust
- Provide safe and secure lifestyle infrastructure
- Prevent unauthorized access using Face verification Link.
- Fast and Accurate Prediction

DOI: 10.17148/IJARCCE.2022.114167

ARCHITECTURE DESIGN:



Modules:

This ATM Security Model consists of this module

1. ATM Simulator

2. Face Recognition Module

2.1. Face Enrollment

2.2. Face Authentication

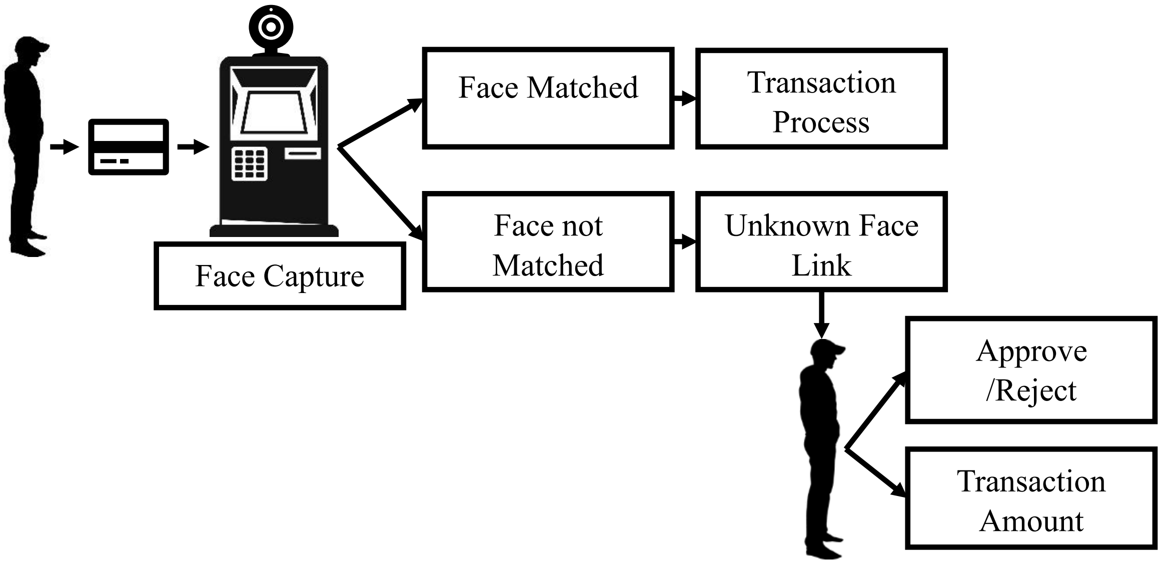
2.3. Unknow Face Forwarder Mechanism.

4. Transaction Model

5. Performance Analysis

DOI: 10.17148/IJARCCE.2022.114167

Block Diagram:



1. ATM Simulator

ATM Simulator is a Next Generation testing application for XFS-based ATMs (also known as Advanced Function or Open-Architecture ATMs). ATM Simulator is a web technology to allow ATM testing with a virtualized version of any ATM.ATM Simulator uses virtualization to provide with realistic ATM simulation, coupled with automation for faster, more efficient testing for face authentication and unknown Face Forwarder Technique.

2. Face Recognition Module

2.1. Face Enrollment

This module begins by registering a few frontal face of Bank Beneficiary templates. These templates then become the reference for evaluating and registering the templates for the other poses: tilting up/down, moving closer/further, and turning left/right.

2.1.1. Face Image Acquisition

Cameras should be deployed in ATM to capture relevant video. Computer and camera are interfaced and here webcam is used.

2.1.1.1. Frame Extraction

Frames are extracted from video input. The video must be divided into sequence of images which are further processed. The speed at which a video must be divided into images depends on the implementation of individuals. From we can say that, mostly 20-30 frames are taken per second which are sent to the next phases.

2.1.2. Pre-processing

Face Image pre-processing are the steps taken to format images before they are used by model training and inference. The steps to be taken are:

- Read image
- RGB to Grey Scale conversion
- Resize image

Original size (360, 480, 3) — (width, height, no. RGB channels)
Resized (220, 220, 3)

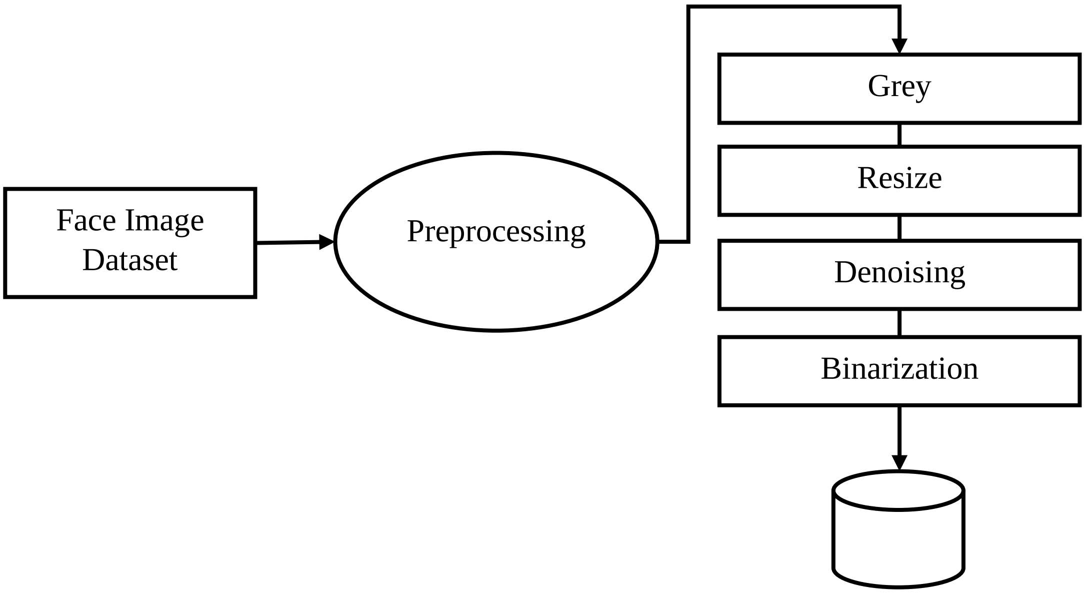
- Remove noise (Denoise)

DOI: 10.17148/IJARCCE.2022.114167

smooth our image to remove unwanted noise. We do this using gaussian blur.

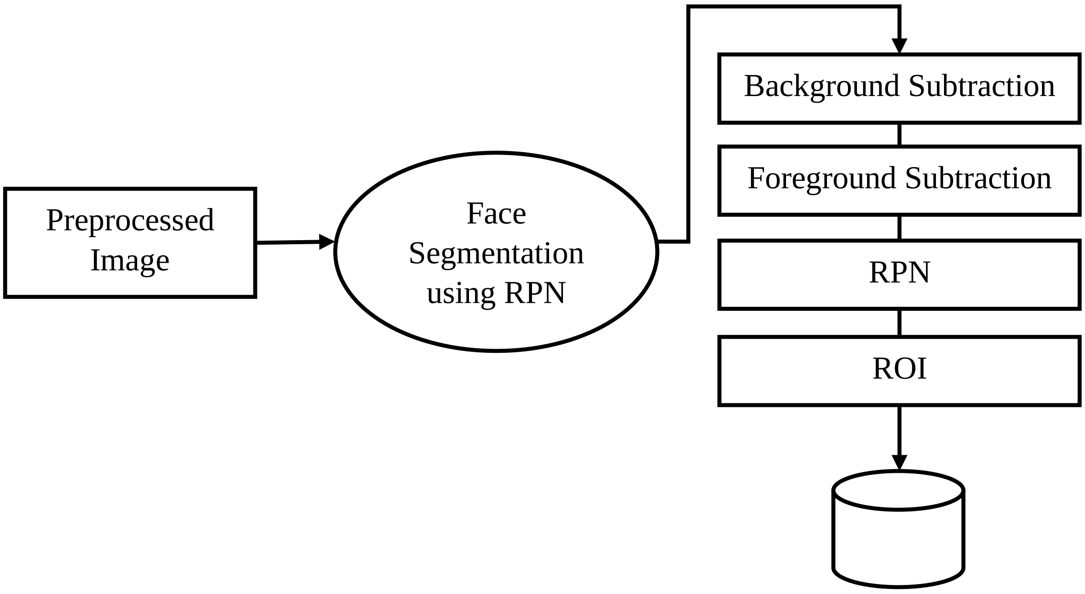
- Binarization

Image binarization is the process of taking a grayscale image and converting it to black-and-white, essentially reducing the information contained within the image from 256 shades of grey to 2: black and white, a binary image.



2.1.3. Face Detection

Therefore, in this module, Region Proposal Network (RPN) generates RoIs by sliding windows on the feature map through anchors with different scales and different aspect ratios. Face detection and segmentation method based on improved RPN. RPN is used to generate RoIs, and RoI Align faithfully preserves the exact spatial locations. These are responsible for providing a predefined set of bounding boxes of different sizes and ratios that are going to be used for reference when first predicting object locations for the RPN.



DOI: 10.17148/IJARCCE.2022.114167

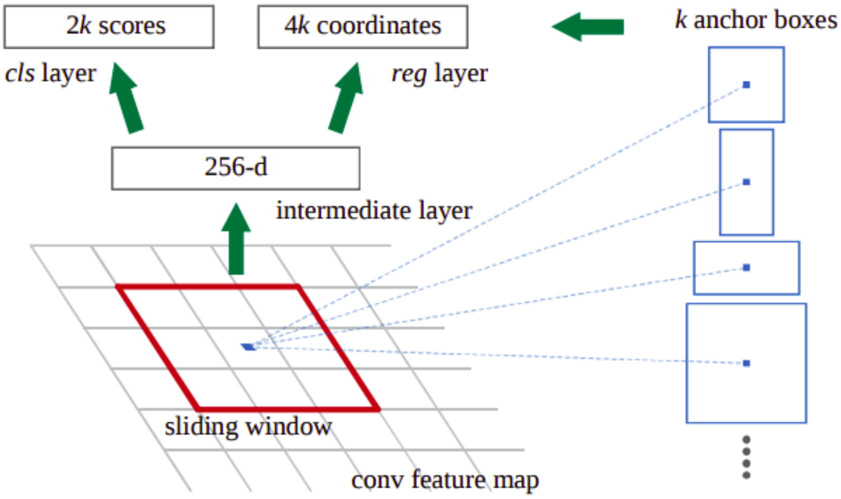
Face Image segmentation using region growing (RG) method

The region growing methodology and recent related work of region growing are described here.

RG is a simple image segmentation method based on the seeds of region. It is also classified as a pixel-based image segmentation method since it involves the selection of initial seed points. This approach to segmentation examines the neighbouring pixels of initial “seed points” and determines whether the pixel neighbours should be added to the region or not based on certain conditions. In a normal region growing technique, the neighbour pixels are examined by using only the “intensity” constraint. A threshold level for intensity value is set and those neighbour pixels that satisfy this threshold is selected for the region growing.

RPN

A **Region Proposal Network**, or **RPN**, is a fully convolutional network that simultaneously predicts object bounds and objectless scores at each position. The RPN is trained end-to-end to generate high-quality region proposals. It works on the feature map (output of CNN), and each feature (point) of this map is called Anchor Point. For each anchor point, we place 9 anchor boxes (the combinations of different sizes and ratios) over the image. These anchor boxes are cantered at the point in the image which is corresponding to the anchor point of the feature map.



Training of RPN.

To know that for each location of the feature map we have 9 anchor boxes, so the total number is very big, but not all of them are relevant. If an anchor box having an object or part of the object within it then can refer it as a **foreground**, and if the anchor box doesn’t have an object within it then we can refer it as **background**.

So, for training, assign a label to each anchor box, based on its Intersection over Union (IoU) with given ground truth. We basically assign either of the three (1, -1, 0) labels to each anchor box.

Label = 1 (Foreground): An anchor can have label 1 in following conditions,

If the anchor has the highest IoU with ground truth.

If the IoU with ground truth is greater than 0.7. (IoU >0.7).

Label = -1 (Background): An anchor is assigned with -1 if IoU < 0.3.

Label = 0: If it doesn’t fall under either of the above conditions, these types of anchors don’t contribute to the training, they are ignored.

DOI: 10.17148/IJARCCE.2022.114167

After assigning the labels, it creates the mini-batch of 256 randomly picked anchor boxes, all of these anchor boxes are picked from the same image.

The ratio of the number of positive and negative anchor boxes should be 1:1 in the mini-batch, but if there are less than 128 positive anchor boxes then we pad the mini-batch with negative anchor boxes.

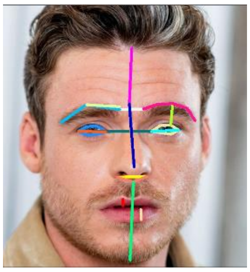
Now the RPN can be trained end-to-end by backpropagation and stochastic gradient descent (SGD).

The processing steps are

- Select the initial seed point
- Append the neighbouring pixels—intensity threshold
- Check threshold of the neighbouring pixel
- Thresholds satisfy-selected for growing the region.
- Process is iterated to end of all regions.

2.1.4. Feature Extraction

After the face detection, face image is given as input to the feature extraction module to find the key features that will be used for classification. With each pose, the facial information including eyes, nose and mouth is automatically extracted and is then used to calculate the effects of the variation using its relation to the frontal face templates.



Face Features

- **Forehead Height:** distance between the top edge of eyebrows and the top edge of forehead.
- **Middle Face Height**: distance between the top edge of eyebrows and nose tip.
- **Lower Face Height**: distance between nose tip and the baseline of chin.
- **Jaw Shape**: A number to differentiate between jaw shapes. this number can be replaced if you use Face Shape Recognition, see (this) notebook.
- **Left Eye Area**
- **Right Eye Area**
- **Eye to Eye Distance**: distance between eyes (closest edges)
- **Eye to Eyebrow Distance**: distance between eye and eyebrow (left or right is determined by whice side of the face is more directed to the -screen-)
- **Eyebrows Distance:** horizontal distance between eyebrows
- **Eyebrow Shape Detector 1:** The angle between 3 points (eyebrow left edge, eyebrow center, eyebrow right edge), to differentiate between (Straight | non-straight) eyebrow shapes
- **Eyebrow Shape Detector 2:** A number to differentiate between (Curved | Angled) eyebrow shapes.
- **Eyebrow Slope**

DOI: 10.17148/IJARCCE.2022.114167

- **Eye Slope Detector 1:** A method to calculate the slope of the eye. it's the slope of the line between eye's center point and eye's edge point. this detector is used to represent 3 types of eye slope (Upward, Downward, Straight).
- **Eye Slope Detector 2:** Another method to calculate the slope of the eye. it's the difference on Y-axis between eye's center point and eye's edge point. this detector isn't a 'mathematical' slope, but a number that can be clustered into 3 types of eye slope (Upward, Downward, Straight).
- **Nose Length**
- **Nose Width:** width of the lower part of the nose
- **Nose Arch:** Angle of the curve of the lower edge of the nose (longer nose = larger curve = smaller angle)
- **Upper Lip Height**
- **Lower Lip Height**

Gray Level Co-occurrence Matrix

GLCM is a second-order statistical texture analysis method. It examines the spatial relationship among pixels and defines how frequently a combination of pixels are present in an image in a given direction Θ and distance d. Each image is quantized into 16 gray levels (0–15) and 4 GLCMs (M) each for Θ = 0, 45, 90, and 135 degrees with d = 1 are obtained. From each GLCM, five features (Eq. 13.30–13.34) are extracted. Thus, there are 20 features for each image. Each feature is normalized to range between 0 to 1 before passing to the classifiers, and each classifier receives the same set of features. The features we extracted can be grouped into three categories. The first category is the first order statistics, which includes maximum intensity, minimum intensity, mean, median, 10th percentile, 90th percentile, standard deviation, variance of intensity value, energy, entropy, and others. These features characterize the Gray level intensity of the tumour region.

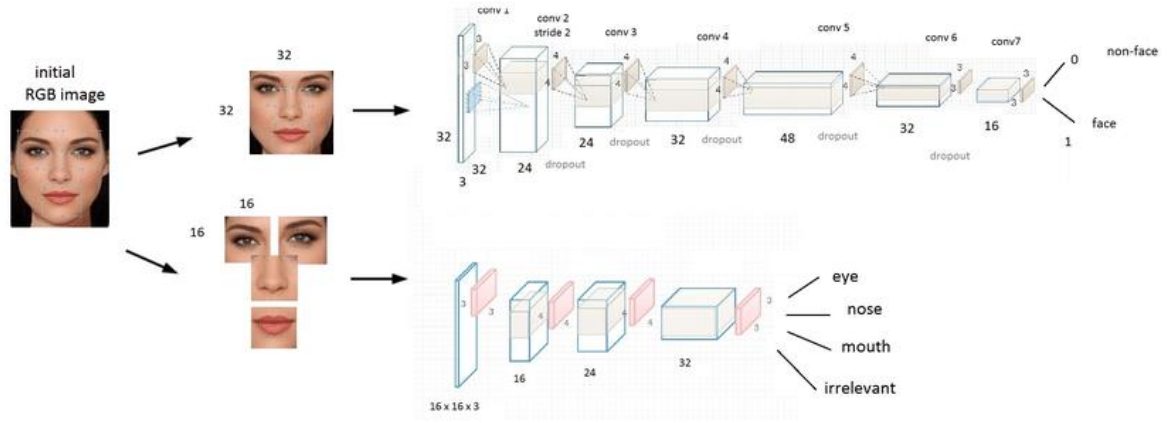


TABLE I. Formulas to calculate Texture Features from GLCM

Sl.No	GLCM Feature	Formula
1.	Contrast	N–1 Σ $P_{i,j}$ $(i — j)^2 i, j = 0$
2.	Correlation	N–1 F(i — μ)(j — μ 1 Σ P I i j) i,j I i, j = 0 I √(σ²)(σ²) I L i j ∠

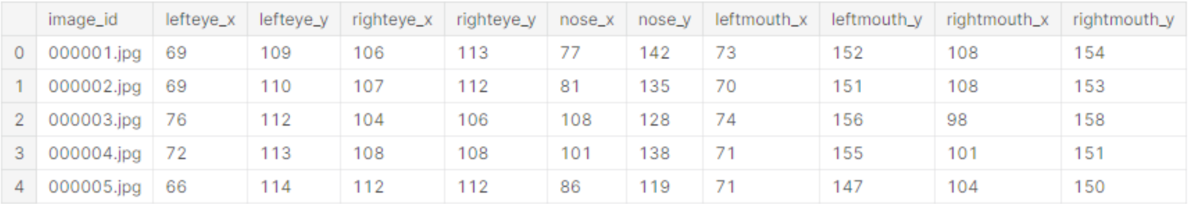
International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114167

3.	Dissimilarity	$\sum_{i,j=0}^{N-1} P_{i,j}\,|i-j|$
4.	Energy	$\sum_{i,j=0}^{N-1} P_{i,j}^2$
5.	Entropy	$\sum_{i,j=0}^{N-1} P_{i,j}\,(-\ln P_{i,j})$
6.	Homogeneity	$\sum_{i,j=0}^{N-1} \frac{P_{i,j}}{1+(i-j)^2}$
7.	Mean	$\mu_i = \sum_{i,j=0}^{N-1} i\,(P_{i,j})\ ,\ \mu_j = \sum_{i,j=0}^{N-1} j\,(P_{i,j})$
8.	Variance	$\sigma_i^2 = \sum_{i,j=0}^{N-1} P_{i,j}\,(i-\mu_i)^2\ ,\ \sigma_j^2 = \sum_{i,j=0}^{N-1} P_{i,j}\,(j-\mu_j)^2$
9.	Standard Deviation	$\sigma_i = \sqrt{\sigma_i^2}\ ,\quad \sigma_j = \sqrt{\sigma_j^2}$

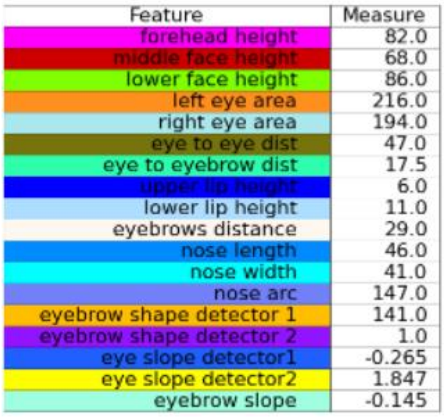
The second category is shape features, which include volume, surface area, surface area to volume ratio, maximum 3D diameter, maximum 2D diameter for axial, coronal and sagittal plane respectively, major axis length, minor axis length and least axis length, sphericity, elongation, and other features. These features characterize the shape of the tumour region. The third category is texture features, which include 22 Gray level co-occurrence matrix (GLCM) features, 16 Gray level run length matrix (GLRLM) features, 16 Gray level size zone matrix (GLSZM) features, five neighbouring Gray tone difference matrix (NGTDM) features and 14 Gray level dependence matrix (GLDM) Features. These features characterize the texture of the tumour region.



	image_id	lefteye_x	lefteye_y	righteye_x	righteye_y	nose_x	nose_y	leftmouth_x	leftmouth_y	rightmouth_x	rightmouth_y
0	000001.jpg	69	109	106	113	77	142	73	152	108	154
1	000002.jpg	69	110	107	112	81	135	70	151	108	153
2	000003.jpg	76	112	104	106	108	128	74	156	98	158
3	000004.jpg	72	113	108	108	101	138	71	155	101	151
4	000005.jpg	66	114	112	112	86	119	71	147	104	150

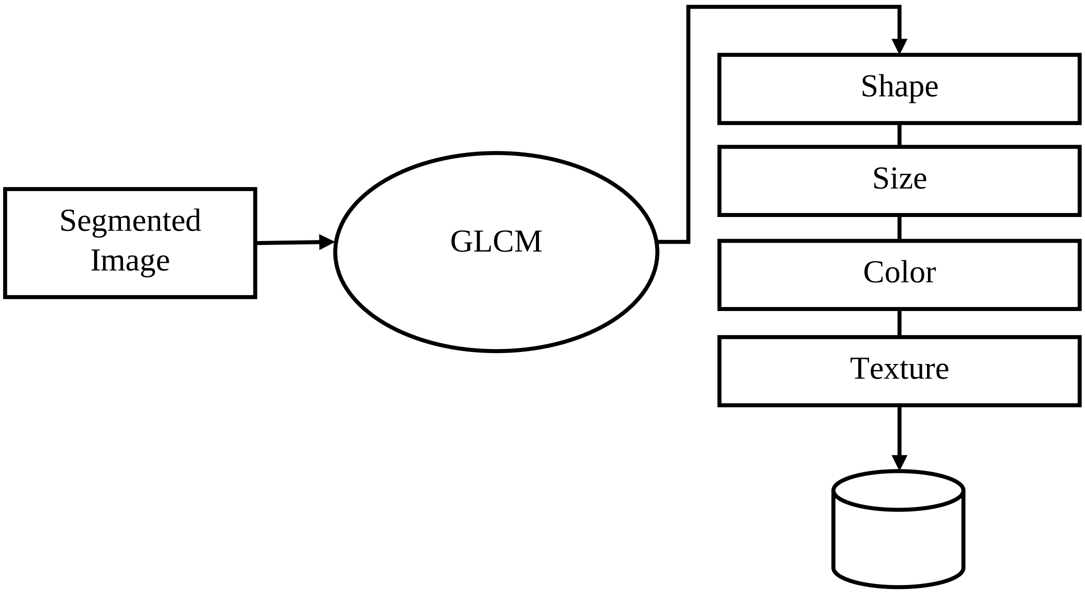
Facial Attribute

DOI: 10.17148/IJARCCE.2022.114167



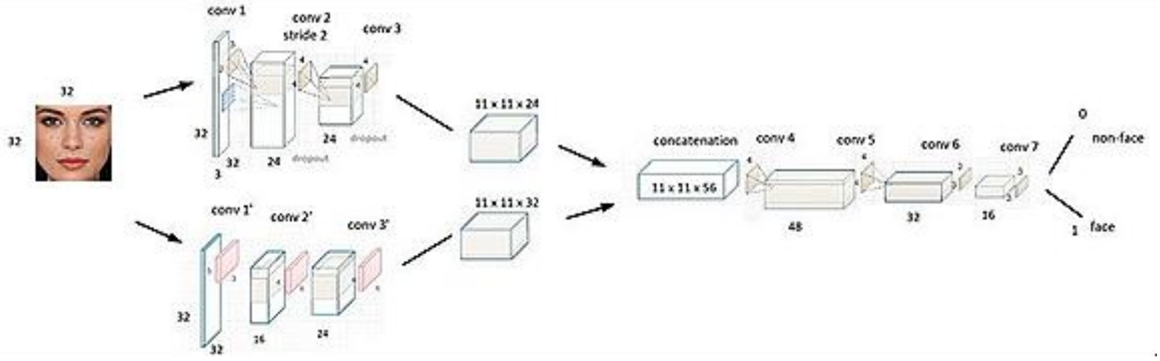
Feature	Measure
forehead height	82.0
middle face height	68.0
lower face height	86.0
left eye area	216.0
right eye area	194.0
eye to eye dist	47.0
eye to eyebrow dist	17.5
upper lip height	6.0
lower lip height	11.0
eyebrows distance	29.0
nose length	46.0
nose width	41.0
nose arc	147.0
eyebrow shape detector 1	141.0
eyebrow shape detector 2	1.0
eye slope detector1	-0.265
eye slope detector2	1.847
eyebrow slope	-0.145

Facial Feature Measurement



2.1.5. Face Classification

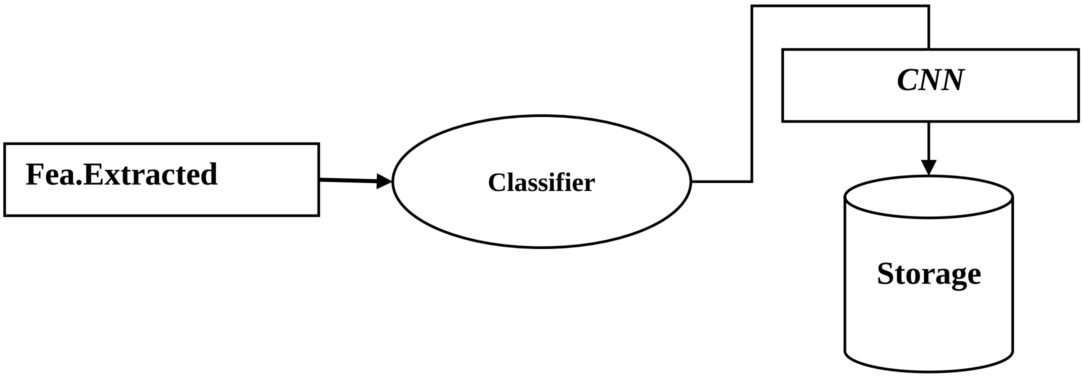
DCNN algorithms were created to automatically detect and reject improper face images during the enrolment process. This will ensure proper enrolment and therefore the best possible performance



The CNN creates feature maps by summing up the convolved grid of a vector-valued input to the kernel with a bank of filters to a given layer. Then a non-linear rectified linear unit (ReLU) is used for computing the activations of the

DOI: 10.17148/IJARCCE.2022.114167

convolved feature maps. The new feature map obtained from the ReLU is normalized using local response normalization (LRN). The output from the normalization is further computed with the use of a spatial pooling strategy (maximum or average pooling). Then, the use of dropout regularization scheme is used to initialize some unused weights to zero and this activity most often takes place within the fully connected layers before the classification layer. Finally, the use of softmax activation function is used for classifying image labels within the fully connected layer.

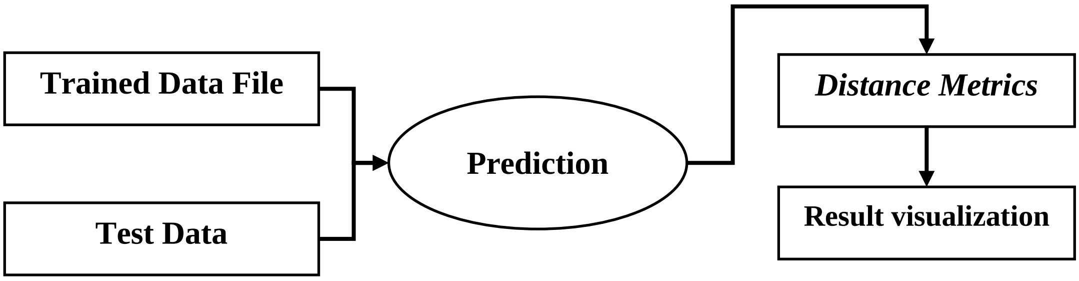


2.2. Face Identification

After capturing the face image from the ATM Camera, the image is given to face detection module. This module detects the image regions which are likely to be human. After the face detection using Region Proposal Network (RPN), face image is given as input to the feature extraction module to find the key features that will be used for classification. The module composes a very short feature vector that is well enough to represent the face image. Here, it is done with DCNN with the help of a pattern classifier, the extracted features of face image are compared with the ones stored in the face database. The face image is then classified as either known or unknown. If the image face is known, corresponding Card Holder is identified and proceed further.

3. Prediction

In this module the matching process is done with trained classified result and test Live Camera Captured Classified file. Hamming Distance is used to calculate the difference according to the result the prediction accuracy will be displayed.



4. Unknow Face Forwarder

Unknown Face Verification Link will be generated and sent to card holder to verify the identity of unauthorized user through some dedicated artificial intelligent agents, for remote certification, which either authorizes the transaction

DOI: 10.17148/IJARCCE.2022.114167

appropriately or signals a security-violation alert to the banking security system.

5. Transaction Module

5.1. Enter the Withdrawal Money

In this section, you have to enter your withdrawal amount and press enter.

But make sure your withdrawal amount does not exceed your balance in the account otherwise transaction will fail.

5.2. Collect the Cash

In this section, you have to collect your money from the lower slot of the machine. Take your money before 30 seconds.

6. Performance Analysis

The important points involved with the performance metrics are discussed based on the context of this project:

True Positive (TP): There is a Face, and the algorithms detect Card Holder.

False Positive (FP): There is no Face, but the algorithms detect as Card Holder and display Card Holder name.

False Negative (FN): There is a Face, but the algorithms do not detect Card Holder and name.

True Negative (TN): There is no Face, and nothing is being detected.

CONCLUSION:

Biometrics as means of identifying and authenticating account owners at the Automated Teller Machines gives the needed and much anticipated solution to the problem of illegal transactions. In this project, we have developed to proffer a solution to the much-dreaded issue of fraudulent transactions through Automated Teller Machine by biometrics and Unknown Face Forwarder that can be made possible only when the account holder is physically or far present. Thus, it eliminates cases of illegal transactions at the ATM points without the knowledge of the authentic owner. Using a biometric feature for identification is strong and it is further fortified when another is used at authentication level. The ATM security design incorporates the possible proxy usage of the existing security tools (such as ATM Card) and information (such as PIN) into the existing ATM security mechanisms. It involves, on real-time basis, the bank account owner in all the available and accessible transactions

REFERENCE:

[1] J. Liang, H. Zhao, X. Li, and H. Zhao, ``Face recognition system based on deep residual network," in Proc. 3rd Workshop Adv. Res. Technol. Ind. (WARTIA), Nov. 2017, p. 5.
[2] I. Taleb, M. E. Amine Ouis, and M. O. Mammar, ``Access control using automated face recognition: Based on the PCA & LDA algorithms," in Proc. 4th Int. Symp. ISKO-Maghreb, Concepts Tools Knowl. Manage. (ISKO-Maghreb), Nov. 2014, pp. 1-5.
[3] X. Pan, ``Research and implementation of access control system based on RFID and FNN-face recognition," in Proc. 2nd Int. Conf. Intell. Syst. Design Eng. Appl., Jan. 2012, pp. 716-719, doi: 10.1109/ISdea.2012.400.
[4] A. A. Wazwaz, A. O. Herbawi, M. J. Teeti, and S. Y. Hmeed, ``Raspberry Pi and computers-based face detection and recognition system," in Proc. 4th Int. Conf. Comput. Technol. Appl. (ICCTA), May 2018, pp. 171-174.
[5] A. Had, S. Benouar, M. Kedir-Talha, F. Abtahi, M. Attari, and F. Seoane, ``Full impedance cardiography measurement device using raspberry PI3 and system-on-chip biomedical instrumentation solutions," IEEE J. Biomed. Health Informat., vol. 22, no. 6, pp. 1883-1894, Nov. 2018.
[6] A. Li, S. Shan, andW. Gao, ``Coupled bias-variance tradeoff for cross-pose face recognition," IEEE Trans. Image Process., vol. 21, no. 1, pp. 305-315, Jan. 2012.
[7] C. Ding, C. Xu, and D. Tao, ``Multi-task pose-invariant face recognition," IEEE Trans. Image Process., vol. 24, no. 3, pp. 980-993, Mar. 2015.
[8] J. Yang, Z. Lei, D. Yi, and S. Li, ``Person-specific face antispoofong with subject domain adaptation," IEEE Trans. Inf. Forensics Security, vol. 10, no. 4, pp. 797-809, Apr. 2015.
[9] H. S. Bhatt, S. Bharadwaj, R. Singh, and M.Vatsa, ``Recognizing surgically altered face images using multi objective evolutionary algorithm," IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 89-100, Jan. 2013.
[10] T. Sharma and S. L. Aarthy, ``An automatic attendance monitoring system using RFID and IOT using cloud," in Proc. Online Int. Conf. Green Eng. Technol. (IC-GET), Nov. 2016, pp. 1-4.