IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

Multimodal Bank Transaction System With Real-Time Secure Clickbait and Biometric ATM User Authentication

A Praveenkumar[1], S Prabu[2], N Pradeep[3] ,G Saravanan[4]
Department of Computer Science and Engineering
Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamil Nadu ,India

Abstract: *ATM or Automated Teller Machines are widely used by people nowadays. Performing cash withdrawal transaction with ATM is increasing day by day. ATM is very important device throughout the world. The existing conventional ATM is vulnerable to crimes because of the rapid technology development. A total of 270,000 reports have been reported regarding debit card fraud and this was the most reported form of identity theft in 2021. A secure and efficient ATM is needed to increase the overall experience, usability, and convenience of the transaction at the ATM. In today's world, the area of computer vision is advancing at a breakneck pace. 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. Specifically, the goal of this project is to give a computer vision method to solve the security risk associated with accessing ATM machines. This project proposes an automatic teller machine security model that uses 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 Clickbait Link will be generated and sent to bank account holder 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. This eliminates the possibility of fraud resulting from ATM card theft and copying. The experimental results on real-time datasets demonstrate the superior performance of the proposed approach over state-of-the-art deep learning techniques in terms of both learning efficiency and matching accuracy. By using this real time dataset, the proposed system achieves the highest accuracy with 97.93%.*

Keywords: Deep Convolutional Neural Network ,Biometric identification techniques, Rapid technology

I. INTRODUCTION

Automated Teller Machines, popularly referred to as ATMs, are one of the most useful advancements in the banking sector. ATMs allow banking customers to avail quick self-serviced transactions, such as cash withdrawal, deposit, and fund transfers.ATMs enable individuals to make banking transactions without the help of an actual teller. Also, customers can avail banking services without having to visit a bank branch. Most ATM transactions can be availed with the use of a debit or credit card. There are some transactions that need no debit or credit card.

Automated Teller Machines have revolutionized the banking sector by providing easy access to customers and loading off the burden from bank officials. Some of the uses of an ATM are-

- The most common uses of an Automated Teller Machine include withdrawing money, checking balance, transferring money, or changing the PIN (Personal Identification Number)
- Newer and advanced ATMs also provide options to open/withdraw a Fixed Deposit (FD), or to apply for a personal loan. You can also book railway tickets, pay the insurance premiums, income tax & utility bills, recharge mobile, and deposit cash. Some of these facilities require you to register at the bank branch
- Customers can now do money transactions at their convenience. ATMs today are installed in public spaces, highways, malls, market places, railway/airport stations, hospitals, etc.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

- Automated Teller Machines provide 24×7 access anywhere
- ATMs help to avoid the hassle of standing in long queues at the bank even for simpler transactions like withdrawing money. It has also helped in reducing the workload of the bank officials.

II. LITERATURE REVIEW

[1] Piyumi Seneviratne; Dilanka Perera; Harinda Samarasekara; Chamath Keppitiyagama; Kenneth Thilakarathna; Kasun De Soyza(2020) In this paper ATM is one of the common information systems in use and often ATM keypad entries include the PIN of an ATM user. The PIN is a piece of confidential customer information which uses for the authentication of a transaction. The banking system operates mainly under the trust assumption that the PIN is secured and kept in private by both the system and the customer to ensure the security requirement of confidentiality. The authordeveloped an experimental design to show that it is possible to infer the PIN using video footage during the situations where both the keypad and fingertips are not visible to the attacker. A lab study was conducted to infer the PIN by human observers. Further, an OpenCV Python program was used to automate the PIN inference.PIN is one factor of the two-factor authentication systemused in ATM transactions. Banks invest heavily to ensure thata PIN is generated inside an HSM and revealed only to thecustomer. This indicates that banks operate under theassumption that the PIN is known only to the customer.However, surveillance cameras installed inside ATM cubiclesto improve physical security open up a side-channel that canpotentially reveal the PIN to third parties.

[2] Khushboo Yadav; Suhani Mattas; Lipika Saini; Poonam Jindal (2020),In the current system, user needs to visit the nearest ATM,swipe the card in the ATM machine there to withdrawmoney. This physical contact of card and machine makes iteasier for the fraudsters to capture the data and misuse it.The proposed solution eliminates this physical contact. Themobile app consists of a special code which flashes on thescreen for a period of 1 minute. This code provides strongauthentication by dynamically generating a one-time securitycode. This code can be generated even if there is no networkor internet connection. Here the user will first login to themobile app using the details such as user-id and password.After this the user generates a reference number as per hischoice and also specifies the amount to be withdrawn. Thisreference number would remain valid for a certain period oftime and can be used only once. Having generated thereference number, the user visits the nearest ATM and entersthe user-id and password along with the code in the app tosign in. If the authorized user is present, he/she would belogged in and would be required to enter the referencenumber to withdraw the specified amount. If the referencenumber is correct, the amount is withdrawn else transactionfails.This idea is an amalgamation of current ATM system andonline transactions involving OTP. By eliminating the use ofOTP, the problems related to sharing of OTP are successfullyovercome.This system provides a three-level security, first when user's identity is verified while logging in the system, secondthrough user-id, password and the code present in the mobileapp – when entered in the ATM machine and last via the reference number.

[3] Rahul Patil; Sagar Salunke; Rajesh Lomte; Madhura Kalbhor,(2019),In this paper Nowadays, dependency on banking in the virtual world has been increased to the peak position. To make it consistent advanced technologies should be used. As OTP is currently used worldwide for security purposes, it can be overruled by QR code.A QRcode scanner is requiredto detect code and decrypt information in stored in QR code. Scanner need to be installed in the ATM machine to take input credentials from the user. We will provide extra feature to an existing system, so traditional withdrawing option is also there. Onother end, ATM machine will scan the QR code generated by 'GetNote'- android application and decrypt it with the key stored in the database. After decryption ATM will get required credentials such as card number, amount, pin, cvv number on card etc. It will authenticate all the details with the banks database. After successful authentication, cash will be dispensed by the ATM machine. ATM machine will responsible for validating the QR code such as difference ingeneration time and scanning time is not more than five minutes. ATM will able to detect QR code from imageuniquely, duplicate QR code will be rejected. System will detect QR code generated by GetNote (android application)only.

[4] Priyanka Hemant Kale; K. K. Jajulwar (2019),In this paper, As we know day by day the usage of ATM cards and crimes related to it has been increased in huge amount. Then umber of cases related to ATM fraud has been registered in the past 3 years from 2016-2018. There are some techniquesused by criminals to steal your card information and ATMcard. ATM skimming, Shoulder surfing, Card trapping, Cashtrapping are some of the popular techniques for executing suchATM card frauds. Sometimes the intimation from the bankthrough Short Message Service (SMS) is also

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

blocked by thehackers/fraudsters. If our ATM card information or ATM carditself is stolen and transaction is executed by the fraudster, theATM card owner receives SMS only after completion of thetransaction. Hence the transaction can't be retrieved easily. Toovercome such crimes the new authentication features offingerprint and OTP must be added to the ATM. Whenever theATM transaction has been processed the ATM asks to enterPIN. After entering PIN, the OTP is sent to the number towhich your bank account is linked and the transaction can bepossible. But in this system, only entering PIN is not enough,after entering a PIN the user needs to choose any one option tomake the whole transaction successful that option isfingerprint or OTP. If the user chooses the option of OTPgeneration, then an OTP is sent to the user's mobile number towhich the bank account is linked this OTP is generated usingthe GSM module. After entering theOTP, the transaction isexecuted successfully if the wrong OTP is entered then theprocess for making transaction is stopped. OTP is safe as persecurity purpose because OTP is available for a specificduration and for every new transaction a new OTP isgenerated. If the user chooses another option that is fingerprint,then the user needs to scan their fingerprint on the fingerprintscanner and the user can do future transactions if thefingerprint is not matched with the user's fingerprint than thetransaction process is stopped. A person's finger consists of aunique pattern which involves more security to the currentATM. Even the Europay, Mastercard and Visa (EMV) chipcards which are replaced by magnetic strip ATM cards are notthat much secured. EMV-capable chip reader card generates aunique code for each transaction. EMV card provides moresecurity to ATM cards but still the cardholder needs to takesome precautions as they used to take before.

[5] Abhishek Tyagi; Ipsita; Rajbala Simon; Sunil Kumar khatri (2019), In this paper ,Nowadays iris recognition is getting more popular in terms of security. Iris pattern is more stable with ages, uniqueness, acceptability. Because of its high reliability and good rates of recognition, iris recognition is therefore used for highly secure locations. With the arrival of ATM banking has become much easier and it has also become more accessible. The product (ATM) it is manifold due to the highly increasing risk of intelligent criminals. Due to which the banking services are in danger and not secure. This situation is getting progressed as huge progress is made in biometric recognition techniques like fingerprint and iris scanning. Customer's password can be encrypted using selective article points. Therefore, a system is needed which is more secure and provides safe transactions and also help from various frauds.

III. SYSTEM STUDY

Technical Feasibility: The technical feasibility study always focuses on the existing computer hardware, software and personal. This also includes need for more hardware, software or personal and possibility of procuring or installing such facilities. ATM is a system that can work on single stand alone Pentium machine with 128 MB RAM, Hard disk drive size of 80 GB, mouse, monitor and keyboard & it also require internet connection to corresponding computer.

Economical Feasibility: This feasibility is useful to find the system development cost and checks whether it is justifiable. The cost overheads include software and hardware maintenance cost, training costs that includes cost required for manpower, electricity, stationary etc. The proposed system will provide the right type of information at right time, and in the required format. This will save time required for decision-making and routine operations. Considering all these advantages, the cost overheads of the system are negligible. So the system is economically feasible.

Operational Feasibility : It is also known as resource feasibility. The operation users of the system are expected to have minimum knowledge of computer. The developed system is simple to use, so that the user will be ready to operate the system. The proposed system is developed using PYTHON programming language & Mysql database which is platform independent and user friendly. So the system is operationally feasible.

IV. SYSTEM ARCHITECTURE

Existing System

Existing ATM authentication method is the use of password-PINs and OTP.

Presently, ATM systems use no more than an access card which usually has a magnetic stripe (magstripe) and a fixed Personal Identification Number (PIN) for identity verification. Some other cases utilize a chip and a PIN which sometimes has a magstripe in case the chip fails as a backup for identification purposes.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

QR cash withdrawals were enabled so customers could ditch their ATM cards and simply scan a QR-code on ATMs using the QR app to withdraw cash.

A QRcode scanner is required to detect code and decrypt information in stored in QRcode. Scanner need to be installed in the ATM machine to take input credentials from the user. We will provide extra feature to an existing system, so traditional withdrawing option is also there. On other end, ATM machine will scan the QRcode generated by 'GetNote'-android application and decrypt it with the keystored in the database. After decryption ATM will get required credentials such as card number, amount, pin, cvv number on card etc. It will authenticate all the details with the banks database. After successful authentication, cash will be dispensed by the ATM machine.

ATM security system architecture that incorporates both the finger print and GSM technology into the existing PIN-based authentication process.

PIN verification is combined with fingerprint recognition, to identify a customer during ATM transaction. Fingerprint is verified using efficient minutiae feature extraction algorithm. To assure the security while doing transaction through swipe machine, the client will confirm the transaction by an approval message through GSM technology. In both cases, location will be identified through GPS. If any illegitimate person tries to use the card it will automatically be blocked by the system and detail information will be sent to the customer through the message.

The algorithms used in the existing system for biometric authentication are Gaussian Mixture Models (GMMs), Artificial Neural Networks (ANNs), Fuzzy Expert Systems (FESs), and Support Vector Machines (SVMs). LDA, PCA.

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.

Disadvantages

- 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.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

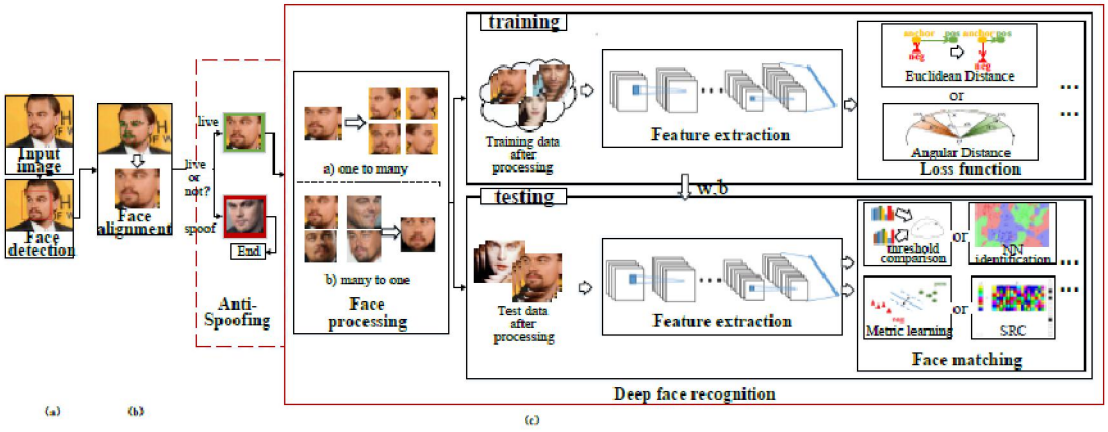


Diagram 1

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.

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.

Unknown 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.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

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

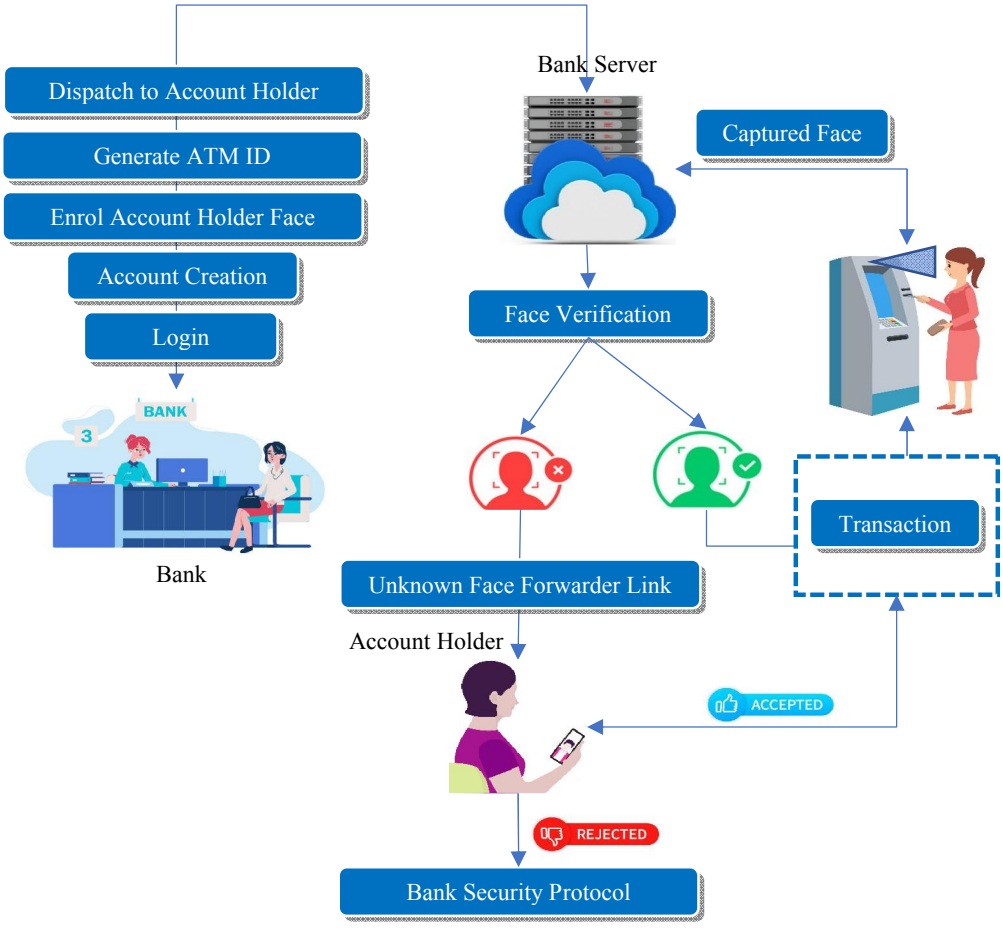


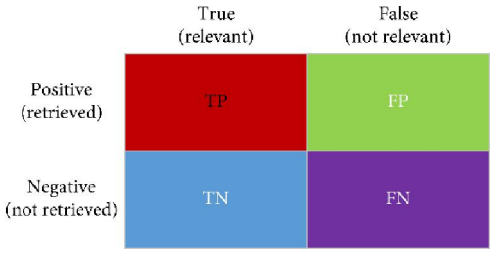
Diagram 2

V. METHODOLOGY

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.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

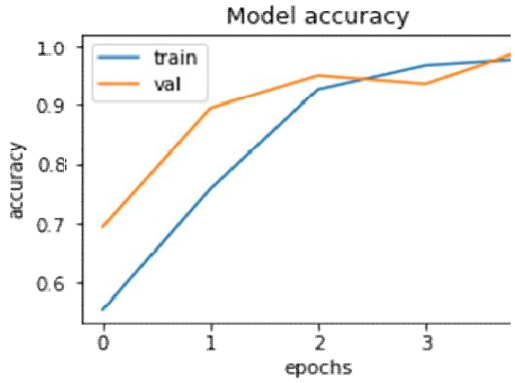


Accuracy

Accuracy is a measure that tells whether a model/algorithm is being trained correctly and how it performs. In the context of this thesis, accuracy tells how well it is performing in detecting Face in ATM Machine. Accuracy is calculated using the following formula.

Accuracy = (T P + T N)/ (T P + T N + F P + F N)

Accuracy: 0.9984025559105432

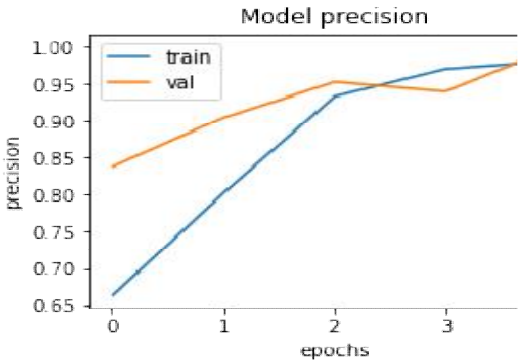


Precision

It denotes the ratio of positively predicted cases that are actually positive. In the context of this thesis, precision measures the fraction of objects that are predicted to be Card Holder and are actually Card Holder Face present in ATM environment. Precision is calculated using the following formula.

Precision = T P/ (T P + F P)

Precision: 0.9990234375



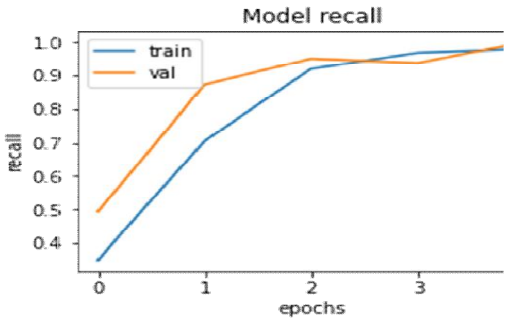
Recall

It is the ratio between actual positive cases that are predicted to be positive. In the context of this thesis, recall measures the fraction of Face that are predicted as Face and identify the card Holder. Recall is calculated using the following formula.

Recall =T P/ (T P + F N)

Recall: 0.9964285714285714

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023



F1 Score

It is also known as balanced F-score or F-measure. F1 score is a measure of accuracy of a model combining precision and recall. In the context of this thesis, a good F1 score shows that there are less false positives and false negatives. This shows that the model is correctly identifying Face in ATM environment.

A model/algorithm is considered perfect if F1 score is 1. It is calculated using the following formula.

F1 = 2 × (Precision × Recall /Precision + Recall)

F1_score: 0.9977122020583142

Training time

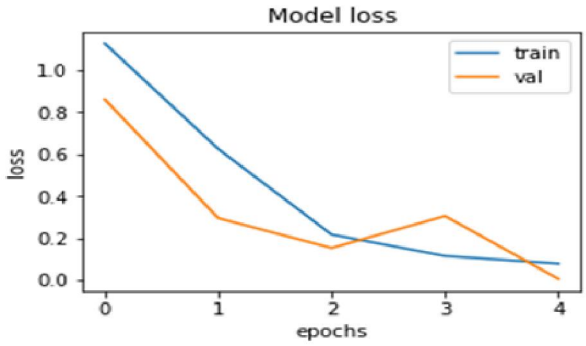
Training time is metric used in this thesis to measure the time taken to train the selected machine learning algorithms on the dataset.

Prediction Speed

Speed is a metric used in this thesis to measure the time taken for the algorithms to process and detect obstacle.

Loss Function

Loss function, to perform feature matching between the ground truth and the output of segmentation network, optimizing also the network weights on features extracted at multiple resolutions rather than focusing just on the pixel level



VI. FACE RECOGNITION SYSTEM

Working of Facial Recognition

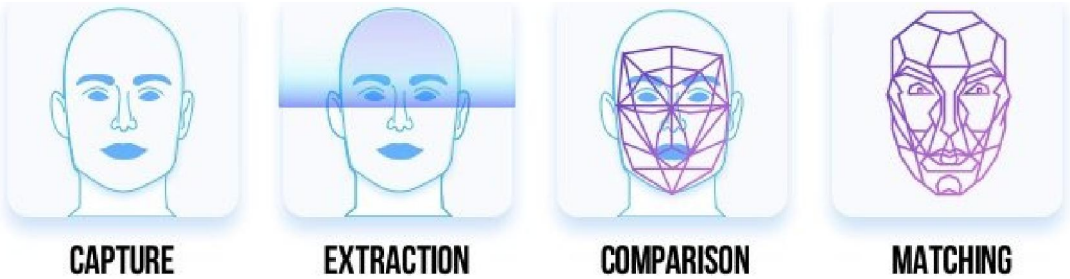


Diagram 3

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

Concept of feature vector: Every Machine Learning algorithm takes a dataset as input and learns from this data. The algorithm goes through the data and identifies patterns in the data. The challenging part is to convert a particular face into numbers – Machine Learning algorithms only understand numbers.

This numerical representation of a "face" (or an element in the training set) is termed as a feature vector. A feature vector comprises of various numbers in a specific order.

You can take various attributes to define a face like:

Height/width of face (cm)

Color of face (R,G,B)

Height/width of parts of face like nose & lips (cm)

We can consider the ratios as feature vector after rescaling

A feature vector can be created by organising these attributes to into a table, say, for a certain set of values of attributes your table may look like this:

Height of face (cm)	Width of face (cm)	Average color of face(R,G,B)	Width of lips (cm)	Height of nose(cm)
23.1	15.8	(255, 224, 189)	5.2	4.4

image now becomes a vector that could be represented as [23.1, 15.8, 255, 224, 189, 5.2, 4.4]. Now can add a number of other features like hair color & spectacles. Keep in mind that a simple model gives the best result. Adding a greater number of features may not give accurate results (See overfitting and underfitting).

[-0.23, -0.54, ..., 0.27]

Machine learning helps you with two main things:

Deriving the feature vector: As it is a difficult process to involve all features by name, we convert it to feature vector. This is then used by the algorithm. A Machine Learning algorithm can intelligently label out many of such features.

Matching algorithms: Once the feature vectors have been obtained, a Machine Learning algorithm needs to match a new image with the set of feature vectors present in the corpus.

Face Recognition Module

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.

Face Image Acquisition

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

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.

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:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

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)
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.

VII. 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

REFERENCES

[1]. J. Liang, H. Zhao, X. Li, and H. Zhao, ``Face recognition system basedon deep residualnetwork," 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 usingautomated face recognition: Based on the PCA & LDA algorithms," inProc. 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 basedon 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]. [4] A. A. Wazwaz, A. O. Herbawi, M. J. Teeti, and S. Y. Hmeed, ``RaspberryPi 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 raspberryPI3 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-poseface 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 withsubject 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 surgicallyaltered face images using multiobjective evolutionary algorithm," IEEETrans. Inf. Forensics Security, vol. 8, no. 1, pp. 89-100, Jan. 2013.

[10]. T. Sharma and S. L. Aarthy, ``An automatic attendance monitoring systemusing RFID and IOT using cloud," in Proc. Online Int. Conf. Green Eng.Technol. (IC-GET), Nov. 2016, pp. 1-4.