JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

REAL TIME SECURE CLICKBAIT AND BIOMETRIC ATM USER AUTHENTICATION AND MULTIPLE BANK TRANSFER SYSTEM

[1]*K.K. Surya*
UG Student,
Dept of CSE,
IFET College of Engineering, Villupuram, India.

[2]*A. Balachandar*
Associate Professor,
Dept of CSE,
IFET College of Engineering, Villupuram, India.

***Abstract*—Automatic Teller Machines, or ATMs, are often utilised by individuals nowadays. The number of people using ATMs to withdraw cash is growing daily. The ATM is a crucial piece of equipment everywhere. The typical ATM that is currently in use is prone to crimes because of the rapid advancement of technology. Debit card fraud has received a total of 270,000 reports, making it the most widely reported identity theft in 2021. To improve the overall transaction experience, usefulness, and convenience at the ATM, a secure and effective ATM is required. Relating to machine vision is developing quickly in the modern world. Recent developments in Authentication via biometrics technologies, like finger printing, a retinal scan, and face identification, it significantly improved the risky ATM situation. The purpose of this project is to provide a computer vision technique that will address the security risk connected to accessing ATM machines. If this system were to be extensively adopted, both the faces and the accounts of the users would be protected. Face Verification, In order to remotely verify an unauthorised user's identity, a dedicated artificial intelligent agent will generate and send a Clickbait URL to the bank account holder. Although it is clear that human biometric characteristics cannot be duplicated. By allowing the legitimate account holder to to his accounts and only his accounts, our solution goes a long way towards addressing the issue with accounts security. This prevents the chance of theft and duplication of ATM cards leading to fraud. The experimental outcomes on real-time datasets show that the suggested strategy outperforms cutting-edge deep learning techniques in terms of learning effectiveness and matching precision. The proposed method achieves the maximum accuracy with 97.93% when using this real-time dataset.**

Keywords*— *Face Detection, Fraud Detection, Machine Learning, Biometric Authentication, Feature Extraction.

I. INTRODUCTION

One of the most helpful developments in the banking industry is the automated teller machine, or ATM. Cash withdrawal, deposit, and fund transfers are just a few of the quick selfservice options that ATMs make available to banking customers. Anyone can do banking transactions via ATMs without a real teller's assistance. Moreover, clients can get financial services without going to a bank location. A debit or credit card can be used for the majority of ATM transactions. Certain transactions can be completed without a debit or credit card. The Bank graph was a device that clients could use to deposit cash and cheques into it. It was developed in 1960 by an American by the name of Luther George Simjian. At a Barclays bank location in Enfield, London, the first ATM was installed in June 1967. Two primary types of automated teller machines (ATMs) exist. One is a straightforward, entry-level device that enables cash withdrawals, balance checks, PIN changes, mini statements, and account modifications. The more sophisticated machines offer features for bill payment, line of credit, and cash or check deposits. There are both on-site and offshore Automatic Teller Machines to make sure that individuals can obtain basic banking services and rapid cash withdrawals even if they are unable to visit a bank office. The existence are scattered, across the nation, the source are situated within the banks. By enabling client access and relieving bank personnel of their duties, ATMs have revolutionised the banking sector. A few applications for an ATM include:

- Cash withdrawals, balance checks, money transfers, and PIN (Personal Identification Number) adjustments.
- The ability to open or withdraw from a Fixed-rate loan or submit an application for a individual loan is available on more contemporary and sophisticated ATMs. Also, you may make cash deposits, recharge mobile devices, pay income tax, utility, and insurance charges. You must register for some of these services at the bank branch. Automated teller machines (ATMs) have proliferated throughout society over the past 20 years, just like the Superman-famous phone booths. Because of how widespread they are, people use these wired currency machines without thinking twice. They don't even consider that something might go wrong. The majority of ATM scams involve the theft of personal identification numbers (PINs) and

debit card data from unsuspecting users of these devices. Many people are unlikely to memorise and recognise a PIN if they are unfamiliar with the concept. The artificial intelligence of things (AIoT) is what is created when you combine AI and IoT. Internet of things devices can be compared to the brain of the system with the neurological system of computers and synthetic intelligence. Facial recognition is a technology for user authentication that can be used to confirm the card owner and protect ATM transactions. Financial fraud is a major issue for banks, and the magnetic tape used in ATM cards contains current security information that is particularly susceptible to loss or theft. ATMs users can be identified being the cardholder by employing face recognition as a technique for authentication.

II. LITERATURE REVIEW

Both the Android operating system and the PC use this mechanism. The PC terminal can incorporate a voice broadcasting feature that can quickly and efficiently prompt users to take action when "danger" threatens. Facial recognition on Android mobile devices can be utilised for mobile payments, identity security authentication, and other handy operations, considerably increasing the system's use[1].

One of the simplest characteristics that can be used in biometric security systems to identify a user is the human face. Because it doesn't involve any form of physical interaction between the users and the gadget, face recognition technology is quite popular and utilised more frequently. For verification, a camera scans the user's face and compares it to a database. Also, it doesn't need any pricey hardware and is simple to setup. Several security systems, including those for computer user accounts and physical access control, make extensive use of facial recognition technology[2].

The accuracy and effectiveness of identification verification have increased with the advancement of technology for recognizing faces and the widespread usage of RFID technology. The study offers a facial identification system based on FNN, RFID card processing, and face detection based on skin model for an intelligent access control system. This method can be applied to a variety of situations, including access control in uptown and the monitoring of employee records at work. There is a significant practical benefit[3].

This process utilizes image analysis techniques to examine, identify, and recognise facial images in photographs of humans. In public spaces like airlines, campuses, and shopping malls, the technology can be used as a security system. It is capable of detecting and identifying a human face in a variety of circumstances. To recognise human faces, this system uses the "Boosted Cascade of Basic Features method." To identify these faces, "Local Binary Pattern algorithm" is used. The essential component attached to a camera for picture capture is the Raspberry Pi[4].

Electrical bioimpedance (EBI) measurements are used in impedance cardiography (ICG), a noninvasive technique for tracking heart activity. The measuring system described in this work, which implements both a full three-lead ECG recorder and an impedance cardiographer for scientific and educational beneficial projects, is built around two System on Chip (SoC) solutions and a Raspberry PI. The Raspberry PI platform supports worldwide DIY projects and teaching methods[5].

III. EXISTING WORK

Regression issues can be seen in subspace-based face representation. From this vantage point, we first reviewed the bottleneck in face recognition—the issue of recognising faces despite position variations. Next, employing a regressor with a coupled bias-variance tradeoff, we suggest a novel method for cross-pose face recognition.Ridge regression and lasso regression are investigated using the fundamental concept. The
CMU PIE, FERET, and Multi-PIE face databases' experimental results demonstrate that the suggested biasvariance tradeoff can significantly improve generalization ability[6].

Profile photographs taken in unrestricted settings typically have a lot of position variation, which severely hurts frontal face recognition algorithms' effectiveness. The manufactured partial frontal faces are then represented using a sturdy patchbased face representation approach. In the suggested multi-task learning technique, a transformation dictionary is learned for each patch. The features of various poses are transformed into a discriminative subspace via the transformation dictionary. Last but not least, profile matching occurs at the patches level as opposed to the comprehensive level[7].

For effective systems to identify faces, face antispoofing is crucial. A generic antispoofing classifier has already been trained to recognise spoofing attacks on all subjects. The generic classifier, however, is unable to generalise successfully to all subjects due to the individual variances among the subjects. We suggest an individual visual alliance method in this paper. To use a classification that has been specially trained for each subject, it can identify spoofing assaults while ignoring topic influence[8].

Many methods for avoiding identification have been developed as a result of the widespread acceptance and use of biometrics for person authentication. One such method involves surgically changing the look of the face, which presents a problem for face recognition algorithms. The academic society has taken notice of plastic surgery's popularisation and its impact on automated facial recognition. Nonetheless, the nonlinear fluctuations brought about by plastic surgery are still challenging for systems that recognize faces to represent[9].

An illustration of such is the use of RFID. If RFID and IOT (Internet of Things) are used together, it can be fully automated without the need for lectures. For improved speed, we intend to use the Cloud as storage in this case. We can access it at any time and from any location via IOT and the web, giving us maximum standard and mobility[10].

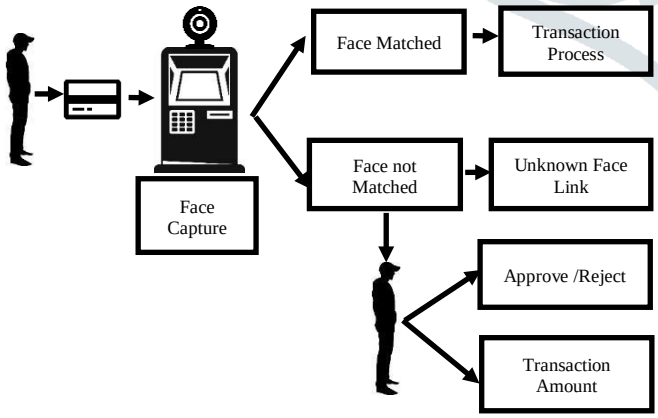
THE TRAINING AND TESTING EXAMPLE OF DATA THAT WILL BE COLLECTED FOR THE ANALYSING PHASE AND TESTING PHASE TO PREDICT THE RESULT

	Train		Test	
Attribute	Pos	Neg	Pos	Neg
Color Photo	8806	29	3772	24
Mouth Slightly Open	674	109	315	57
Round Face	9	588	3	250
Goatee	20	3346	10	1557
Baby	23	9137	15	3913
Bangs	89	5238	44	2080
Bald	114	4413	47	1953
Big Lips	101	751	48	318
Sunglasses	74	8583	50	3631
Partially Visible F.	124	1501	55	601
Mouth Wide Open	107	6593	56	2925
Double Chin	154	172	57	136
Harsh Lighting	113	914	62	487
Outdoor	173	510	63	243
Teeth Not Visible	125	2209	66	1089

IV. PROPOSED WORK

Machine learning, in turn, whereas Artificial intelligence (AI) is a subset of machine learning, which is a subset of robust learning. In-depth learning makes it possible for us to recognise faces more accurately than we could with conventional machine learning techniques. With face detector and alignment, deep FR system. To locate faces, a face detector is utilised first. The faces are secondly positioned according to normalised standardised coordinates. Finally, the FR module is put into practise. Facial examination is employed to control factors prior to training and assessment, including ages and postures, while face antispoofing in the FR module detects if the face is real or false. After extracting discriminative deep features from testing data using various architectures and loss functions, feature classification is performed using face matching techniques.

BLOCK DIAGRAM



If the saved picture and the captured 0069mage don't line up, it's an unauthorised user. To verify the individuality of an unauthorised accountant via those specialised AI investigators for remotely certifying, there will be a Face Verification URL created and to the user; dispatched. This will either properly authorise the transaction or alert the banking vulnerability of a security system.

MODULE

The research suggests a multi-model security framework for ATMs it utilises a Deep Convolutional Neural Network together with a physical access card to integrate computerised facial recognition.

1. Computerised ATM
2. Face recognition
3. Predicting
4. Identified Face Forwarder
5. Financial Model
6. Performance analaysis

1. Computerised ATM

Computerised ATM is a Feature Gen checking instrument for XFS-situated machines. A virtualized replica of any ATM may be used for ATM testing thanks to a web-based programme called ATM Simulator. Furthermore to automating the assessment of the Mysterious Technique for Front Facing and face recognition, ATM Simulator employs virtualization to produce a realistic ATM simulation.

2. Face Recognition

Face Enrollment

The registration of a few frontal face Bank Beneficiary templates kicks off this module. Then, using them as a model, the models for the additional postures — shifting the angle, advancing or receding, making a right or left turn —are reviewed and registered.

Face Image Acquistion

ATMs should have cameras installed to record pertinent footage. Webcam is utilised here as the interface between computer and camera.

Frame extraction

Cameras should be installed in ATMs to capture relevant footage. Here, the interface between the computer and camera is a webcam.

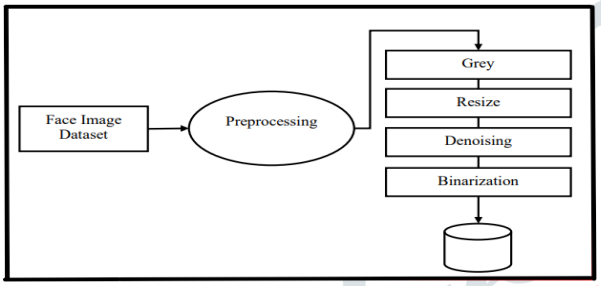
Thresholding

Facial image preparation describes the actions that are photos are formatted before being used by models for inference and training. These steps must be taken:

- Read the image
- Convert RGB to greyscale
- original picture dimensions (360, 480, 3)
- Expanded in size (225, 225, 6)
- Quiet down (Denoise) to remove undesirable noise, we must smooth our image. This is achieved through Gaussian blur.

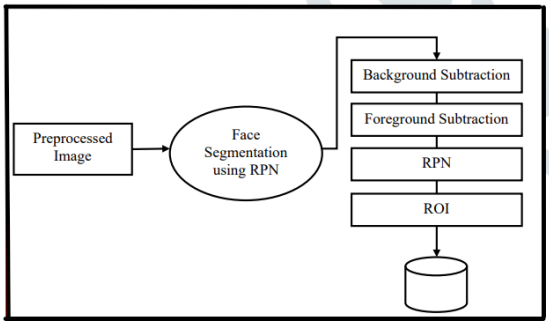
Binarization

An image that is binary, sometimes called image binarization, is created by reducing a grayscale image's 256 grayscales, from many to only two: black and white. This is achieved by taking an image and turning it into a black-and-white image.



Face Detection

As a result, the Region Proposal Network (RPN) throughout this system creates RoIs by dragging convolution layer panels past supports of varying sizes and magnitude relation. Based on an upgraded RPN, a face detection and segmentation algorithm. RoIs are created using RPN, and RoI Align accurately maintains the precise spatial placements. They are accountable for offering a specified bounding boxes collection of different size and percentage this would be useful as a regard when the RPN is initial finding item placements.

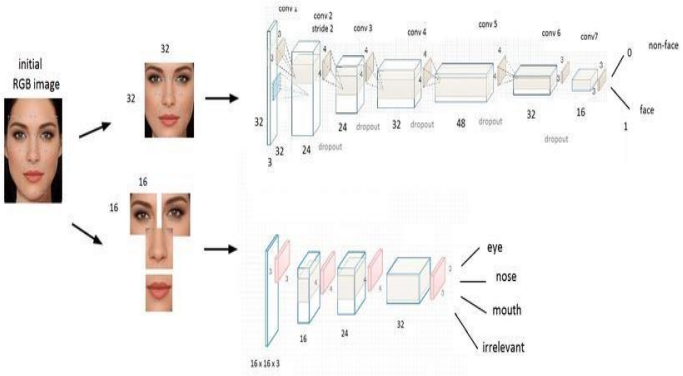


Feature extraction

Following face identification, the feature extraction module uses the face image as input to identify the most important aspects for categorization. The facial elements of each position, such as the lips, nose, and eyes, are automatically extracted their relationship for frontal face templates is utilised to determine the variation's consequences.

Face Categorization

In the course of the application, For the purpose of accurately identifying and ignoring inappropriate face images, DCNN algorithms were developed. It will guarantee accurate enrollment as well as the highest achievement rate.



Face Recognition

The ATM Camera records the face region, which is then forwarded to the module that recognises people. These component locates areas of a picture where people are most likely to be present. The feature extraction module uses the face image as input after face recognition using the Region Proposal Network (RPN) to determine the essential characteristics that is to be categorised. This element generates an extremely tiny feature set that precisely represents the facial image.

3. Predicting

In this prediction, the process of matching is carried out using test live camera-captured classified files and trained classified results. Its variations is computed using the Hamming Distance, and findings are provided along with the prediction accuracy.

4. Identified Face Forwarder

In order to verify an unauthorised user's identity through specialised artificial intelligent agents for virtual authorization, Confirmation of an unidentified picture URL shall be produced and conveyed to owner of the account. These agents will appropriately authorise the transaction, if necessary, or report any security breaches to the banking security system.

5. Financial Model

- Fill in the Withdraw Money box Here, we have to enter the required money and press the enter button.
  To avoid a failed transaction, keep in mind your transaction money does not above your balances.
- Gather the Money
  You must take your money from the machine's lower slot in this section. Before the timer expires, take your money.

6. Performance Analysis

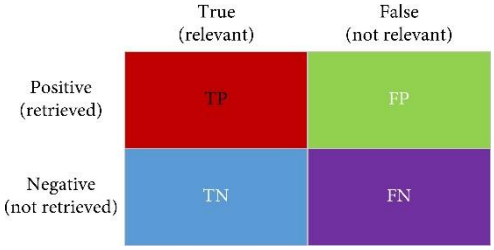
Based on the context of this project, the key points associated with the performance indicators are discussed: True Positive

(TP): The algorithms recognise the Card Holder and there is a Face.

False Positive (FP): Although there isn't a Face, the algorithms identify the person as a Account holder, with their name shown.

False Negative (FN): Despite the existence of a face, the algorithms are unable to identify the cardholder's name and address.

True Negative (TN): Nothing is being detected and there is no Face.

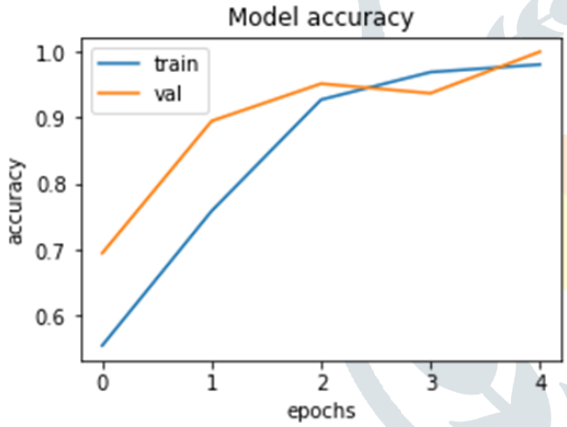


Accuracy

A model's or algorithm's accuracy is a metric that indicates how well it operates and if it was trained appropriately. Accuracy in the context of this thesis refers to how well it works to detect faces in ATMs. The following formula is used to determine accuracy.

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

Reliability: 0.9984025559105432

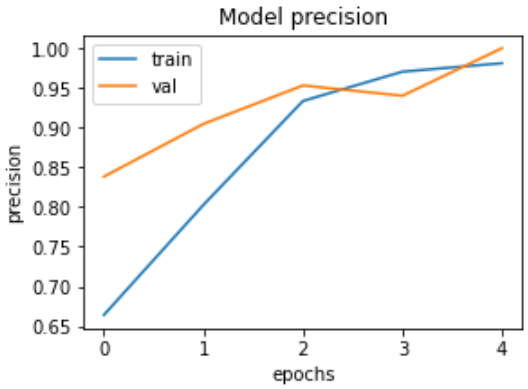


Precision

It represents the percentage of positively projected cases that actually turn out to be positive. Precision, as used in this thesis, refers to the percentage of objects expected to be Card Holders that are actually Card Holder Faces that are present in an ATM environment. The following formula is used to determine precision.

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

Roughness: 0.9990234375

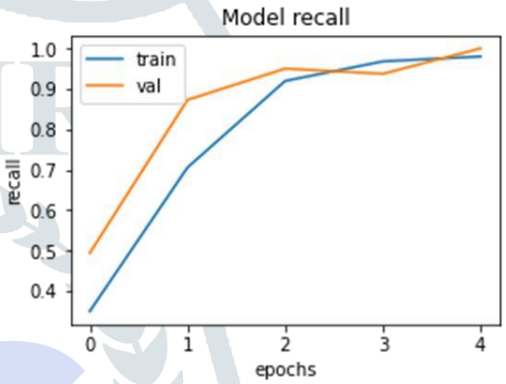


Recollect

The ratio of actual positive cases to those that were expected to be positive is what matters. Recall in this thesis refers to the percentage of predicted Face that correctly identifies the cardholder. The following formula is used to determine recall.

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

Inquiry: 0.9964285714285714



F1 Score

It is sometimes referred to as a balanced F-measure or Fscore. A model's accuracy is evaluated using its F1 score, which combines precision and recall. A high F1 score in the context of this thesis indicates that false positives and false negatives are less common. This demonstrates how well the model recognises faces in an ATM context.

If a model's or algorithm's F1 score is 1, it is deemed perfect. This formula is used to calculate it.

F1 score: 0.9977122020583142

F1 = 2 (Precision Recall /Precision + Recall)

Training Time

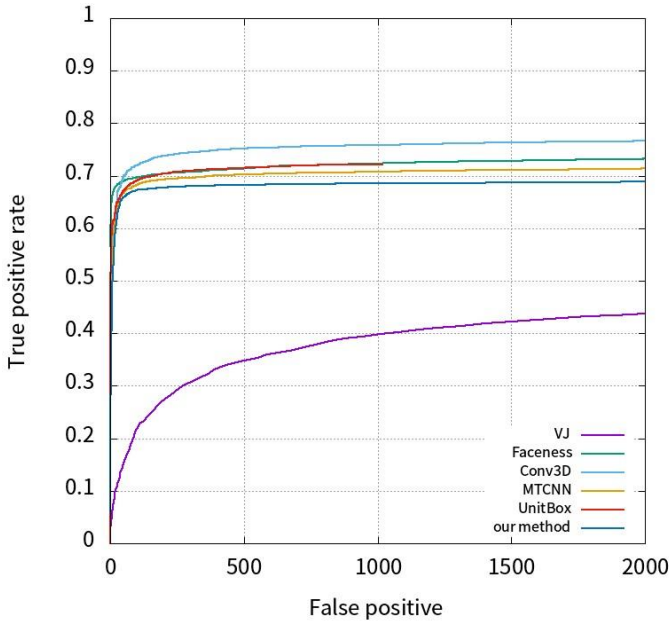
The time it took to train the chosen machine learning algorithms on the dataset is measured in this thesis by the training time metric.

Prediction Speed

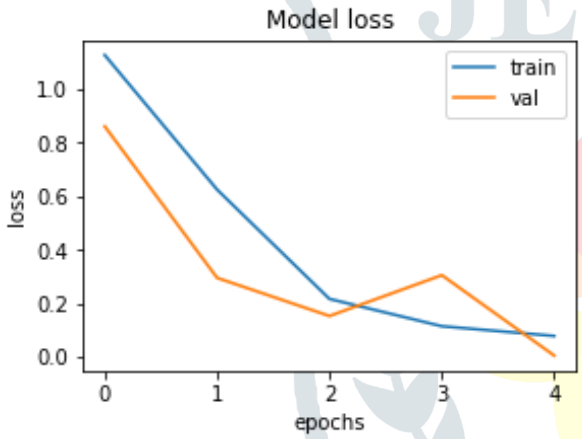
The time it takes for the algorithms to process and recognise obstacles is measured in this thesis using a parameter called speed.

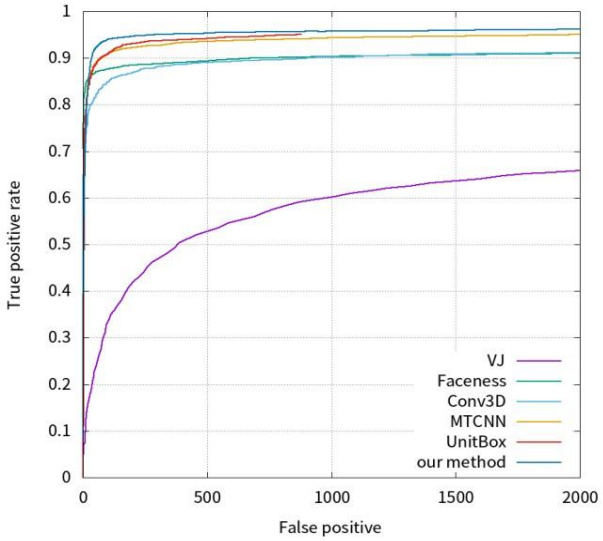
Loss Function

Loss function is used to do feature matching between network's segmentation output and the actual data,



while optimising the network's feature weights retrieved at various resolutions rather than just concentrating on the pixel level.





Divergent ROC Curves

Permanent ROC Curves

V. RESULT AND DISCUSSION

We contrast our method using FDDB's most up-to-date techniques in order to evaluate its performance. Recall rate is used to measure how much of the sample mark's total face is made up of detected faces, while false positive measures how many detected faces contain errors. The Receiver Operating Characteristic (ROC) curve represents these two indicators.

The outcome of the identification of ROC curve show that the deep learning-based detection methodology has greatly increased whereas the VJ recall rate of the conventional face recognition method is only 66.8%. With our method, both the continuous ROC curve and the discontinuous ROC curve display cutting-edge performance. The MTCNN cannot compete with the discontinuous ROC curve. At 1900 false positives, they additionally receive the discontinuous ROC curve's greatest rate of genuine positives (96.5%). The inability of our method to accurately identify the side face is yet another possible influencing factor. The indicator AUC is used to demonstrate both the benefits and drawbacks of the procedure because the ROC curve does not make apparent demonstrate which approach is superior. The area percentage in the ROC region, or AUC, has a value between 0 and 1. The performance of the approach will be improved with a higher AUC value. Compared to FDDB, the BROADER FACE collection presents the much more difficult standard on feature selection., should therefore be used for testing. It is quite promising and showing throughout the three areas, our approach continuosly produces good results. For faces with significant occlusion and Angle shift, the dataset for the FDDB's evaluation results are typically consistent with its better robustness.

VI. CONCLUSION

The much-needed and much awaited answer to the issue of unauthorised transactions is provided by biometrics as an approach to using automated teller machines to locate and confirm account owners. The purpose of this study is to put forth a remedy for the dreaded issue of fraudulent transactions, it is only preventable by the card holder being socially there or distantly located at an automated teller machine employing biometric systems and an unidentified face forwarder. As a result, it ends instances of unauthorised transactions at ATM locations without the genuine owner's awareness. The strength of using a biometric feature for identification is increased when a different one is used for authentication. The ATM security architecture accounts for potential data use as a proxy and safety equipment already in place, like Debit and Credit Cards (such as PINs). This contains the user of the current account in real time in visible and convenient money transfers. To further enhance recognition performance, there should be more deep feature representation methods developed.

REFERENCES

[1] Liang, J., Zhao, H., Li, Xingqian & Zhao, H. (2017) Face recognition system based on deep residual network. In: 3rd Workshop on Advanced Research and Technology in Industry (WARTIA 2017). Atlantis Press, pp. 358–362 [DOI: 10.2991/wartia-17.2017.69].

[2] Taleb, Imene, El Amine Ouis, M. & Mammar, M.O. (2014) Access control using automated face recognition: Based on the PCA & LDA algorithms. In: 4th International Symposium ISKO-Maghreb: Concepts and Tools for knowledge Management (ISKO-Maghreb). IEEE Publications, pp. 1–5.

[3] Pan, X. (2012) Research and implementation of access control system based on RFID and FNN-face recognition. In: Second International Conference on Intelligent System Design and Engineering Application. IEEE Publications, pp. 716–719 [DOI: 10.1109/ISdea.2012.400].

[4] Wazwaz, A.A., Herbawi, A.O., Teeti, M.J. & Hmeed, S.Y. (2018) Raspberry Pi and computers-based face detection and recognition system. In: 4th International Conference on Computer and Technology Applications (ICCTA). IEEE Publications, pp. 171–174 [DOI: 10.1109/CATA.2018.8398677].

[5] Hafid, A., Benouar, S., Kedir-Talha, M., Abtahi, F., Attari, M. & Seoane, F. (2018) Full impedance cardiography measurement device using raspberry PI3 and system-onchip biomedical instrumentation solutions. IEEE Journal of Biomedical and Health Informatics, 22, 1883–1894 [DOI: 10.1109/JBHI.2017.2783949] [PubMed: 29990025].

[6] Li, A., Annan, Shan, S. & Gao, W. (2011) Coupled bias–variance tradeoff for cross-pose face recognition. IEEE Transactions on Image Processing, 21, 305–315.

[7] Ding, C., Xu, C. & Tao, D. (2015) Multi-task poseinvariant face recognition. IEEE Transactions on Image Processing, 24, 980–993 [DOI: 10.1109/TIP.2015.2390959] [PubMed: 25594967].

[8] Yang, J., Lei, Z., Yi, D. & Li, S.Z. (2015) Person-specific face antispoofing with subject domain adaptation. IEEE Transactions on Information Forensics and Security, 10, 797–809 [DOI: 10.1109/TIFS.2015.2403306].

[9] Bhatt, H.S., Bharadwaj, S., Singh, R. & Vatsa, M. (2012) Recognizing surgically altered face images using multiobjective evolutionary algorithm. IEEE Transactions on Information Forensics and Security, 8, 89–100 [DOI: 10.1109/TIFS.2012.2223684].

[10] Sharma, T. & Aarthy, S.L. (2016) An automatic attendance monitoring system using RFID and IOT using Cloud. In: online international conference on green engineering and technologies (IC-GET). IEEE Publications, pp. 1–4 [DOI: 10.1109/GET.2016.7916851].