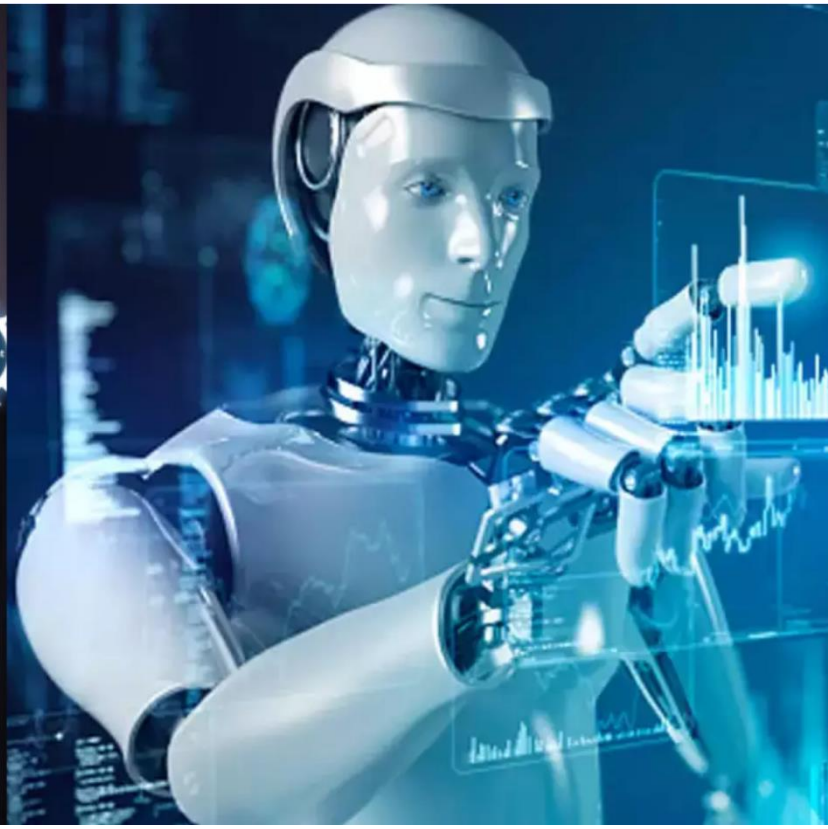
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405310|

Vision – Based Security for the Next-Gen ATM

R.Sathya, M.Mohamed Faisal

Assistant professor, Department of CSE, Sir Issac Newton College of Engineering and Technology, Pappakovil, Nagapattinam, India

Pradeepa P, Petchishri S, Mahalakshmi S, Madhavi M

Department of CSE, Sir Issac Newton College of Engineering and Technology, Pappakovil, Nagapattinam, India

ABSRACT: With the growing demand for enhanced security measures in the banking sector, the utilization of biometric authentication systems has gained prominence. 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 system 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 and automatic teller machines 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.

KEYWORDS: Vision based security, Next-Gen ATM, Facial recognition, Biometric authentication, Surveillance system, ATM fraud detection, Deep learning for security, Real time monitoring.

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. the utmost utilization rate for ALOHA is 36.8%. Therefore, the face recognition a part of this study uses PCA and LDA and therefore the Intelligence RFID access control part uses on binary tree search algorithm. The general design architecture of the system is presented then the precise identity authentication methods. Deep learning attempts to mimic the human brain—albeit far from matching its ability enabling systems to cluster data and make predictions with incredible accuracy. Deep learning is a subset of machine learning, which is essentially a neural network with three or more layers. These neural networks attempt to simulate the behavior of the human brain albeit far from matching its ability—allowing it to "learn" from large amounts of data. While a neural network with a single layer can still make approximate predictions, additional hidden layers can help to optimize and refine for accuracy. Deep learning drives many artificial intelligence (AI) applications and services that improve automation, performing analytical and physical tasks without human intervention. Deep learning technology lies behind everyday products and services (such as digital assistants, voice-enabled TV remotes, and credit card fraud detection) as well as emerging technologies. Enhance ATM authentication by combining physical access cards with biometric facial recognition. Apply Deep Convolutional Neural Networks (DCNN) for accurate facial identification. Strengthen ATM security and minimize unauthorized account access. Introduce real-time face verification links for remote identity confirmation using AI agents.Ensure account access is restricted solely to the legitimate user through unique biometric features. Address rising concerns over ATM fraud with advanced, intelligent security methods.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

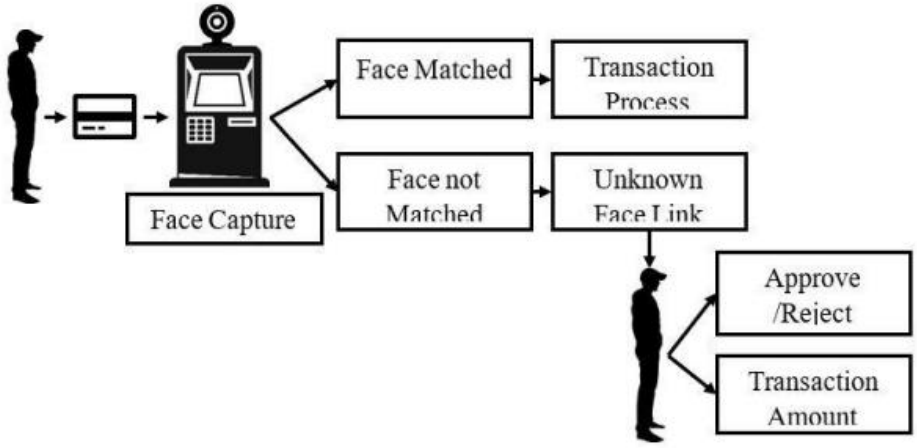
Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405310|

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.



Enhance ATM Security – Develop a biometric-based security system that integrates facial recognition with ATM access to prevent unauthorized transactions.

Implement Deep Learning-Based Face Recognition – Utilize Deep Convolutional Neural Networks (DCNN) to accurately identify and authenticate users at ATMs.

Combine Physical Access Cards with Biometric Authentication – Strengthen security by requiring both a traditional ATM card and facial verification before granting access.

Prevent Unauthorized Access – Detect and prevent fraudulent attempts by verifying user identities through real-time facial recognition.

Enable Remote User Verification – Generate and send a face verification link to the account holder for remote authentication of unauthorized users using AI-driven verification.

Improve Fraud Detection – Use artificial intelligence to analyze suspicious ATM activity and alert authorities in case of unauthorized access attempts.

Reduce ATM PIN Theft – Eliminate the risks associated with stolen or leaked PINs by incorporating biometric authentication.

Ensure Account Safety and Privacy – Leverage unique facial biometric features that cannot be replicated, ensuring only the rightful owner has access to their account.

Enhance User Convenience – Provide a seamless and secure transaction process by eliminating the need to remember or enter a PIN.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405310|

II. RELATED WORK

A.Essaki Muthu; A. Justin Diraviam,…[1] Modern banking relies heavily on Automated Teller Machines (ATMs), although card-based transactions have historically faced security issues. This study proposes Near-Field Communication (NFC) Card Emulation and fingerprint technology as secure alternatives for ATM cash transactions. NFC Card Emulation enables secure data exchanges within a short distance, ideal for handling sensitive information. To augment security during authentication, fingerprint technology is proposed as an additional layer of protection. By employing fingerprint sensors, user identification can be established without reliance on physical cards or NFC tags. This integration ensures a heightened level of security during the authentication process, surpassing the current cardbased approach employed in ATMs. The system eliminates the need for physical cards, enhancing security and mitigating risks such as ATM tampering and magnetic strip damage. A high level of security is guaranteed during ATM transactions as authentication becomes more effective and secure. This novel strategy strengthens ATM security and provides users with a seamless and safe banking experience by incorporating NFC Card Emulation and fingerprint technologies.

Kalirajan K; Suganya D N,…[2] Automated Teller Machines (ATMs) are often targeted by hackers who use skimmers to obtain customers card information and personal identification numbers (PINs). To address this issue, a novel ATM security system is proposed that generates a temporary password using a vibrator. This temporary password is added to the customer's normal PIN and must be entered every time when the money is withdrawn. By using vibrator to generate the temporary password, it is ensured that it is unique and cannot be easily replicated. Even if a hacker obtains the temporary password along with the customer's normal PIN, they cannot access the cash without rendering the temporary password, which is only valid for a limited time. Moreover, proposed system is designed to detect and alert the owner in the event of theft. If the temporary password is entered incorrectly more than once, the system will activate an alert mechanism and shut down the shutter automatically. This will prevent the thief from accessing the cash, and notify the owner of the attempted theft. To further enhance security, the proposed method incorporates a mechanism to alert the police in case of theft. Once the shutter is shut down, it can only be opened by authorized personnel such as the police, ensuring that the cash is kept safe until the authorities arrive.

S Sridevi; K.M. Monica,…[3] A workflow is proposed for the detection of unauthorized persons in an ATM. Certain assumptions, including the context of identification are made by training their features and storing the datasets. However, not every individual will be a suspect. Suspicious activity on ATMs that are located in remote areas and to reduce the risk of fraudulent transactions. such as using another person's card to withdraw money etc., Various video survey and image processing have been discussed in relation to surveillance methods. It discusses the various processes, preprocessing, classification, feature extraction and the corresponding video processing methods.

Darwin Nesakumar A; Arthi S; Avulu Lahari,…[4] The main objective of this paper is to integrate multiple bank accounts and multiple users accounts into one single smart card using RFID. A Formula based authentication is used for generating OTP using alphabets and operators and substituting the numbers for the alphabets. OTP will be sent to registered phone numbers during registration. To increase security, we have added the biometrics (fingerprint) of the user, which comes in use during each transaction. Thus, the users can register the bank details and now proceed with their transactions without carrying multiple bank ATM cards or memorizing various pin numbers, thereby ensuring security and authenticity through the biometric authentication.

Puspa Setia Pratiwi; Chandra Prasetyo Utomo,…[5] Automated Teller Machines (ATMs) are banking outlets that support customer activities to process regular financial transactions quickly and automatically without the help of tellers. Transaction activities carried out by customers at ATMs are often difficult to predict. Therefore, the banking sector is strongly encouraged to build an intelligent cash management system to provide opportunities for banks to lower operating costs. Customer transaction patterns are needed to make a prediction. This study aims to implement machine learning algorithms to predict transaction values at ATMs with time series algorithms. This study aims to create a machine learning model to determine the predicted value of ATM transactions using four algorithms, Linear Regression, Prophet, ARIMA, and LSTM algorithms. The dataset used is the data set of ATM transactions of XYZ bank. This dataset has around 11.588 rows and ten columns. The results of the calculations with the best evaluation

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405310|

model determined in the LSTM algorithm, which produces the Mean Absolute Error (MAE) value of 20,686.91, the Mean Squared Error (MSE) of 710,590,544.24, and the Coefficient of Determination (R2) 0.72.

III. EXISTING METHODOLOGIES

Existing ATM authentication method is the use of passwordPINs&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.

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 QR code scanner is required to 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. On other end, ATM machine will scan the QR code generated by 'Get Note'- 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 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.

IV. FACE RECOGNITION

Face Enrollment

It is 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.

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 ofindividuals.From we can say that, mostly 20-30 frames are taken per second which are sent to the next phases.

Face Detection

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.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405310|

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 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.

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.

Unknown Face Forwarder

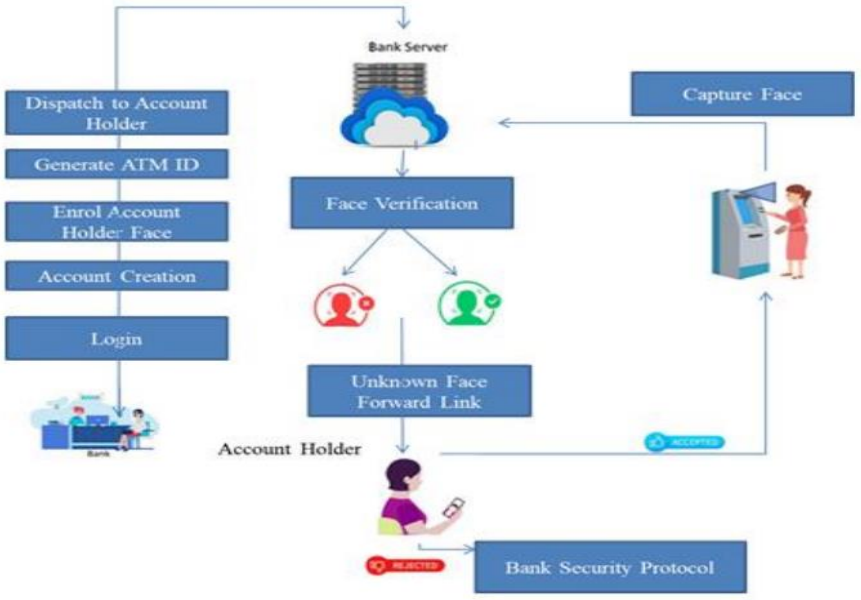
Unknown Face Verification Link will be generated and sent to card holder to verify the identity of unauthorized user through some dedicated artificial intelligent agents, for remote certification, which either authorizes the transaction appropriately or signals a security-violation alert to the banking security system.

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 antispoofing 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.



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405310|

Figure: System Architecture

V. EXPERIMENTAL RESULTS

Dataset and Environment

The system was tested using a combination of publicly available datasets and real-time video feeds:

1.Face Recognition: LFW (Labeled Faces in the Wild), ATM-surveillance dataset (custom).

2.Object/Suspicious Detection: COCO, Open Images Dataset with custom annotations (e.g., weapons, face masks).

Face Recognition Accuracy

Metric	Value (%)
Accuracy	96.5
Precision	97.2
Recall	95.8
F1 Score	96.5
FAR (False Acceptance Rate)	1.1
FRR (False Rejection Rate)	2.3

Suspicious Object Detection

Object/Activity	Precision (%)	Recall (%)	F1 Score (%)
Weapon Detection	94.1	91.6	92.8
Face Mask Detection	97.8	98.4	98.1
Multiple Face Presence	93.6	94.7	94.1

YOLOv7 and EfficientDet were compared; YOLOv7 showed higher real-time performance with mAP of 91.3%.

Real-Time Performance

Component	Average Latency (ms)	FPS
Face Detection & Matching	120 ms	~8 FPS
Object Detection	85 ms	~11 FPS
End-to-End Response Time	250 ms	~4 FPS

VI. CONCLUSION

Face 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.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405310|

REFERENCES

[1] 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.
[2] Li, S. Shan, andW. Gao, ``Coupled bias-variance tradeoff for cross-pose face recognition," IEEE Trans. ImageProcess., vol. 21, no. 1, pp. 305-315, Jan. 2012.
[3] H. S. Bhatt, S. Bharadwaj, R. Singh, and M.Vatsa, ``Recognizing surgically altered face images using multiobjective evolutionary algorithm," IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 89-100, Jan. 2013.
[4] 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.
[5] 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.
[6] 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.
[7] T.R.Lekhaa, “Secured credit card transaction using web cam” International Research Journal of Engineering and Technology, April 2016.
[8] 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.
[9] Wazwaz, A. O. Herbawi, M. J. Teeti, and S. Y. Hmeed, ``Raspberry Pi and computers-based face detectionand recognition system," in Proc. 4th Int. Conf. Comput. Technol. Appl. (ICCTA), May 2018, pp. 171-174.
[10] 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.
[11] A.Kowshika,” Least mobility high power (LMHP) dynamic routing for QoS development in Manet” WirelessPersonal Communications, Springer US, March 2019.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details