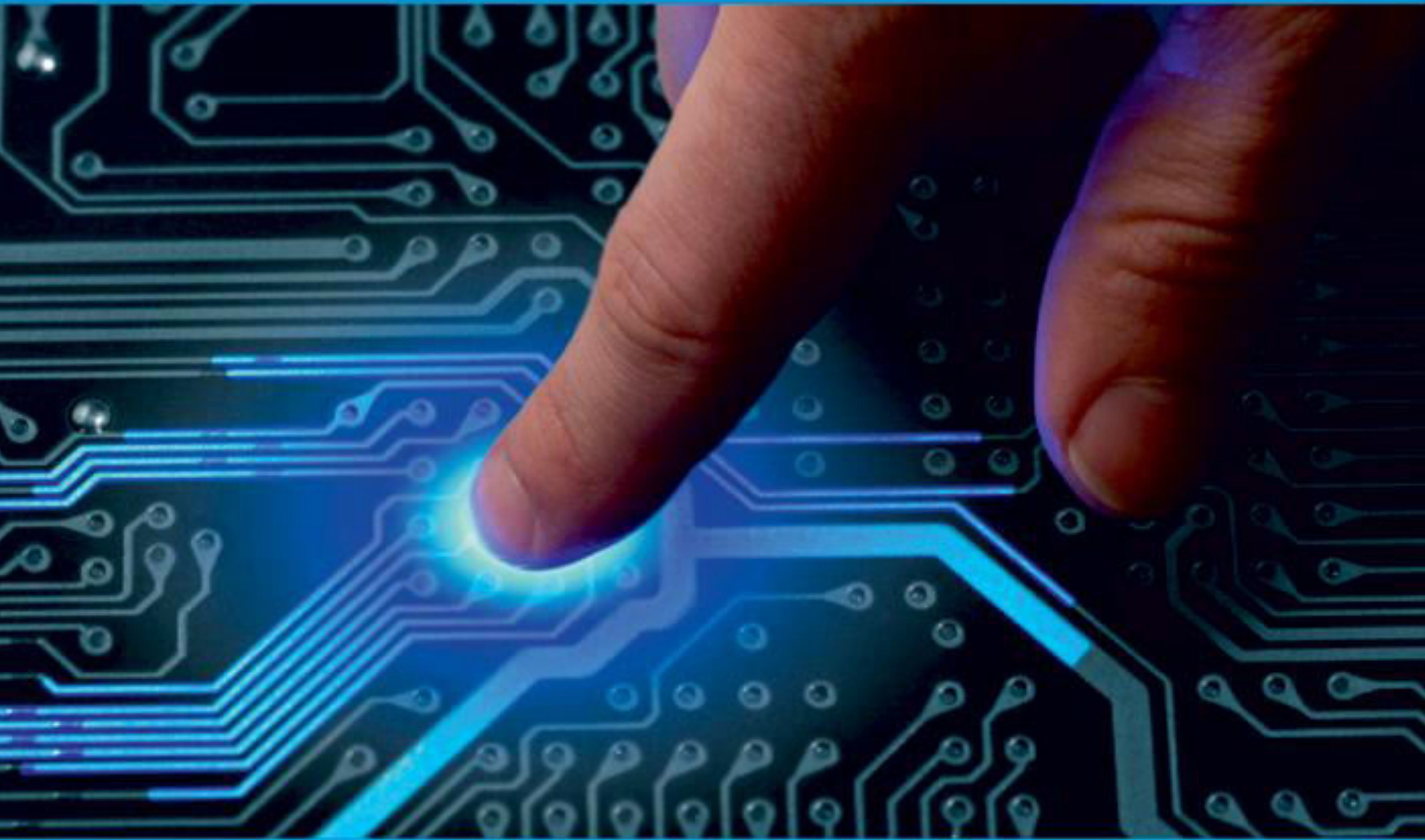
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006236|

ATM Authentication by Face Realization Using Neural Networks

Arvind Sai V S, Ashrath Joji S N, Charan K, Retheesh D

U.G Scholar, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India

U.G Scholar, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India

U.G Scholar, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India

Assistant Professor, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India

ABSTRACT: In the Information age, with enhancements in technology there is always a security threat associated which implies the constant need for security considerations among all the service providers. In this project, we propose a security model that combines physical access card and facial realization using Deep Convolutional Neural Network. So far, ATM's have been using only the physical ATM card & the corresponding PIN for user authentication & verification. It never had a way to recognize whether the user is a legitimate user or an unauthorised user trying to perform fraudulent activities. It is a fact and obvious that one's biometric features cannot be replicated, which proves that the account owner alone has access to the ATM accounts when biometrics play the role of authentication. This could extremely limit the number of criminal cases involving money theft from ATM's. Also, these biometric recognition paves way for cardless ATM transaction with a double layer security.

I. INTRODUCTION

Automated Teller Machines, popularly referred to as ATMs, are one of the most useful advancements in the banking sector. ATM's 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. 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.

II. LITERATURE SURVEY

CaptureIt! - A Web-based Attendance System Using Face Recognition, 2021 - Shreyas More; Nandita Kadam; SanyamSavla; Sakshi Shelar; Akshit Shah; Swati Mali. This paper describes a system, where the user can record his/her attendance using face recognition, and all the statistics will be inherently calculated by our system for the teachers to analyze in a contactless but efficient manner. Demerit - Manually on the camera and take attendance

Covid-19 Based Automated Screening System, 2021 - HwanjinYong ,Joonwon Lee, and JinSoo Kim. To devise a system for containing the virus to a certain extent wherein a person will be screened at the entry of an organization on the grounds of Mask Detection, Face Recognition and Contactless Temperature Detection. Demerit - Face mask detection only.

SafeCampus: Multimodal-based Campus-wide Pandemic Forecasting, 2021 - Sidi Lu; Baofu Wu; Xiaoda Cong; Yongtao Yao; Weisong Shi. The motivation of this work is to build a multimodal-based COVID-19 pandemic forecasting platform for a large-scale academic institution to minimize the impact of COVID-19 after resuming academic activities. detecting and counting face masks. Demerit - The motivation of this work is to build a multimodal-based COVID-19 pandemic forecasting platform for a large-scale academic institution to minimize the impact of COVID-19 after resuming academic activities. detecting and counting face masks.

Design and Implementation of Entrance Guard System Based on Face Recognition, 2020 - Jianfeng Ye. The method is simple and convenient in design, high in reliability and easy to implement in installation. In the PC, the camera collects image and face recognition, assisted by ultrasonic distance measurement and infrared detection of human body. Face recognition is used to monitor the incoming and outgoing human.

Development of Application and Face Recognition for Smart Home, 2020 - SereeKhunchai; ChaiyaponThongchaisuratkrul. This method includes face recognition system to authenticate each user and alert when the intruder access in the house. It can work well if the user's face is less than a meter from the camera.
An Approach for e-Voting using Face and Fingerprint Verification, 2020 - Shubham Shinde; Manas Shende; Jeet Shah; HarshdeepShelar. e-Voting system that will use fingerprint and face verification along with a combination of firebase-database and server-side file-system at its back-end. It makes the voting process more convenient
Facial Recognition Development to Detect Corporate Employees Stress Level, 2019 - MunifFaisolAbdul Rahman; Vincent; Vito Christian Giovanni. They proposed an idea to recognize motions and emotions on human faces to detect their stress levels. For this, the eigenfaces algorithm is used. Demerit - Monitoring stress level but not the vaccination details.
On Soft-Biometric Information Stored in Biometric Face Embeddings - Philipp Terhörst, Daniel Fährmann, Naser Damer, Arjan Kuijper. The Labeled Faces in the Wild (LFW) [20] and the CelebFaces Attributes (CelebA) [29] datasets provide a large number of attribute annotations and thus, are well suited to perform our predictability-analysis of the face space.
Demerit - Accuracy is low.

III. 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.

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 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 fingerprint 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.

IV. 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.

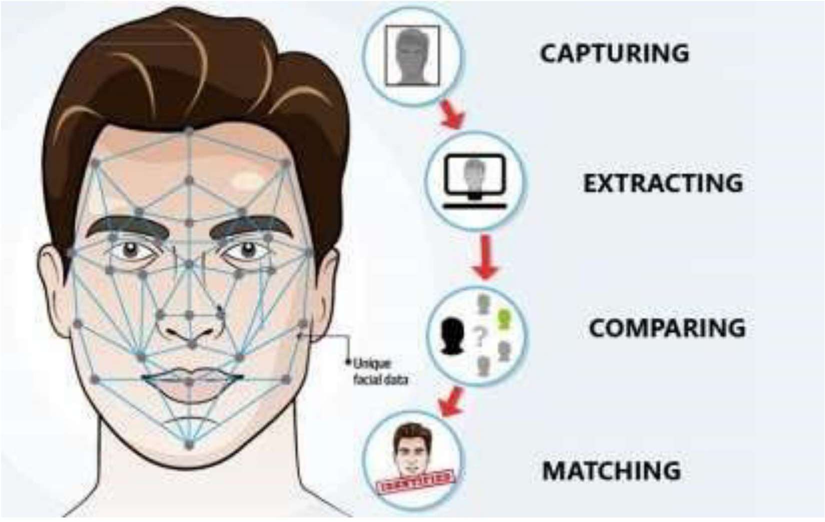


Figure 1 :Facial Biometric Authentication System using Deep Learning Techniques

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 minibatch 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.
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.

V. SYSTEM MODULES

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

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. 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 securityviolation alert to the banking security system.

4. TRANSACTION MODULE

a. Enter the withdrawal money

In this section, you must 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.

b. 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.

5. PERFORMANCE ANAYSIS

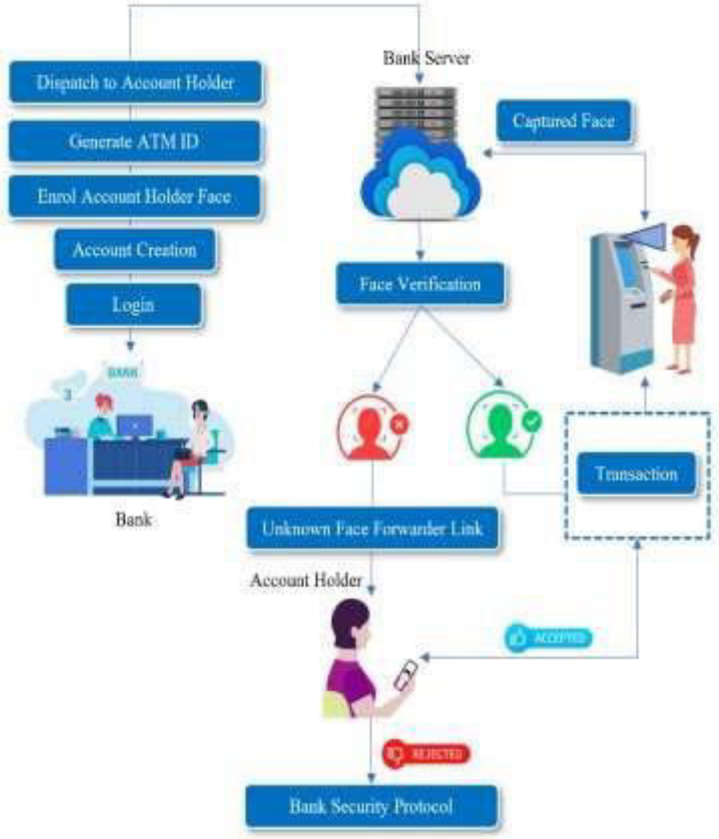
The performance analysis of all experiments was based on the most common evaluation measures used for statistical tests, such as accuracy, precision, recall, and f_measure.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{F\_measure} = \frac{(\text{precision} * \text{recall})}{(\text{precision} + \text{recall})}$$

SYSTEM ARCHITECTURE



VI. CONCLUSION AND FUTURE DIRECTIONS

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.

In the future, the recognition performance should be further boosted by designing novel deep feature representation schemes.

ACKNOWLEDGMENT

The authors would also like to thank the editorial team and all the anonymous reviewers for their valuable suggestions and comments, which helped to improve the quality of the work.

REFERENCES

[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 FNNface recognition,'' in Proc. 2nd Int. Conf. Intell. Syst. Design Eng. Appl., Jan. 2012, pp. 716719, 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 antispoofing 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.

BIOGRAPHY

ARVIND SAI V S is a B.E. final year student in the department of Computer Science and Engineering from Velammal Institute of Technology, Panchetti. His current research focuses on biometrics as means of identifying and authenticating account owners at the Automated Teller Machines

ASHRATH JOJI S N is a B.E. final year student in the department of Computer Science and Engineering from Velammal Institute of Technology, Panchetti. His current research focuses on biometrics as means of identifying and authenticating account owners at the Automated Teller Machines

CHARAN K is a B.E. final year student in the department of Computer Science and Engineering from Velammal Institute of Technology, Panchetti. His current research focuses on biometrics as means of identifying and authenticating account owners at the Automated Teller Machines

Project Coordinator Mr. Retheesh D, M.E Assistant Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

crossref doi

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details

www.ijircce.com