IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 13, April 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

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

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

Real Time Secure Click bait and Biometric ATM User Authentication and Multiple Bank Transaction System

C. Saravanan [1], Muhammed Sanhar KT [2], Mirshad KT [3]

Assistant Professor, Department of Computer Engineering, Dhaanish Ahmed Institute of Technology Coimbatore, Tamilnadu India [1]

U.G. Students, Department of Computer Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, Tamilnadu, India [2, 3]

ABSTRACT: ATM or Automated Teller Machines are widely used by people nowadays. Performing cash withdrawal transaction with ATM is increasing day by day. ATMs are a 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 fingerprinting, 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 Convolution Neural Network. If this technology becomes widely used, faces would be protected as well as their accounts. Face Verification Click bait Link will be generated and sent to bank account holders to verify the identity of unauthorized users 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: Text detection, Imprinting, Morphological operations, Connected component labelling.

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.

.

II. RELATED WORK

1. **Impact of Video Surveillance Systems on ATM PIN Security**
   Author:Piyumi Seneviratne; Dilanka Perera; Harinda Samarasekara; Chamath Keppitiyagama; Kenneth Thilakarathna; Kasun De Soyza
   Year: 2020
   Overview
   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

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

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 author developed 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 systemized in ATM transactions. Banks invest heavily to ensure that a PIN is generated inside an HSM and revealed only to the customer. This indicates that banks operate under the assumption that the PIN is known only to the customer. However, surveillance cameras installed inside ATM cubicles to improve physical security open up a side-channel that can potentially reveal the PIN to third parties.

Outcome

Taking security controls for granted can result in additional threats and risks. Guidelines and standards on the placement of surveillance cameras can mitigate this vulnerability to a certain extent.

2. Secure Card-less ATM Transactions

Author:Khushboo Yadav; Suhani Mattas; Lipika Saini; Poonam Jindal

Year: 2020

Overview

In the current system, user needs to visit the nearest ATM, swipe the card in the ATM machine there to with draw money. This physical contact of card and machine makes it easier for the fraudsters to capture the data and misuse it. The proposed solution eliminates this physical contact. The mobile app consists of a special code which flashes on the screen for a period of 1 minute. This code provides strong authentication by dynamically generating a one-time security code . This code can be generated even if there is no network or internet connection. Here the user will first login to the mobile app using the details such as user-id and password. After this the user generates a reference number as per his choice and also specifies the amount to be withdrawn. This reference number would remain valid for a certain period of time and can be used only once. Having generated the reference number, the user visits the nearest ATM and enters the user-id and password along with the code in the app to sign in. If the authorized user is present, he/she would blogged in and would be required to enter the reference number to withdraw the specified amount. If the reference number is correct, the amount is withdrawn else transaction fails. This idea is an amalgamation of current ATM system and online transactions involving OTP. By eliminating the use foot, the problems related to sharing of OTP are successfully overcome. This system provides a three-level security, first when user's
identity is verified while logging in the system, second through user-id, password and the code present in the mobile app – when entered in the ATM machine and last via the reference number.

Outcome

Thus, though the idea aims solving the issue of card cloning but there is a lot that needs to be taken in consideration to make the system work effectively and efficiently.

3. Efficient Cash Withdrawal from ATM Machine Using QRcode Technology

Author: Rahul Patil; Sagar Salunke; Rajesh Lomte; Madhura Kalbhor

Year: 2019

Overview

Nowadays, dependency on banking in the virtual world has been increased to the peak position. To make inconsistent 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 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. Another end, ATM machine will scan the QRcode 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, cave 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 QRcode such as difference in generation time and scanning time is not more than five minutes. ATM will able to detect QRcode from image uniquely, duplicate QRcode will be rejected. System will detect QRcode generated by Get Note (android application)only.

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

Outcome

Reason behind this replacement is the security provided by QR code is of much higher degree. Due to this, there will be no need to hide ATM pin. Customer doesn't have to worry about ATM pin at all because he will not be requiring the ATM PIN during the whole transaction.

4. Design of Embedded Based Dual Identification ATM Card Security System

Author: Priyanka Hemant Kale; K. K. Jajulwar

Year: 2019

Overview

As we know day by day the usage of ATM cards and crimes related to it has been increased in huge amount. The number of causes related to ATM fraud has been registered in the past 3 years from 2016-2018. There are some techniques used by criminals to steal your card information and ATMcard. ATM skimming, Shoulder surfing, Card trapping, Cash trapping are some of the popular techniques for executing suchATM card frauds. Sometimes the intimation from the bank through Short Message Service (SMS) is also blocked by the hackers/fraudsters. If our ATM card information or ATM card itself is stolen and transaction is executed by the fraudster, theATM card owner receives SMS only after completion of the transaction. Hence the transaction can't be retrieved easily. To overcome such crimes the new authentication features of fingerprint and OTP must be added to the ATM. Whenever theATM transaction has been processed the ATM asks to enter PIN. After entering PIN, the OTP is sent to the number to which your bank account is linked and the transaction can be possible. But in this system, only entering PIN is not enough, after entering a PIN the user needs to choose any one option to make the whole transaction successful that option is fingerprint or OTP. If the user chooses the option of OTPgeneration, then an OTP is sent to the user's mobile number to which the bank account is linked this OTP is generated using the GSM module. After entering theOTP, the transaction is executed successfully if the wrong OTP is entered then the process for making transaction is stopped. OTP is safe as per security purpose because OTP is available for a specific duration and for every new transaction a new OTP is generated. If the user chooses another option that is fingerprint, then the user needs to scan their fingerprint on the fingerprint scanner and the user can do future transactions if the fingerprint is not matched with the user's fingerprint than the transaction process is stopped. A person's finger consists of unique pattern which involves more security to the current ATM. Even the Euro pay, MasterCard and Visa (EMV) chip cards which are replaced by magnetic strip ATM cards are not that much secured. EMV-capable chip reader card generates unique code for each transaction. EMV card provides more security to ATM cards but still the cardholder needs to take some precautions as they used to take before.

Outcome

The cardholder will swipe the card and enter the PIN as per the previous ATMs process but only entering the PIN is not enough after entering PIN, they need to select an option of generating OTP or Fingerprint authentication for the successful transaction. This increases the security of the ATMcards and safer transaction.

III. METHODOLOGY

1. ATM Simulator

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

2. Face Recognition Module

2.1. Face Enrollment

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

2.1.1. Face Image Acquisition

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

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

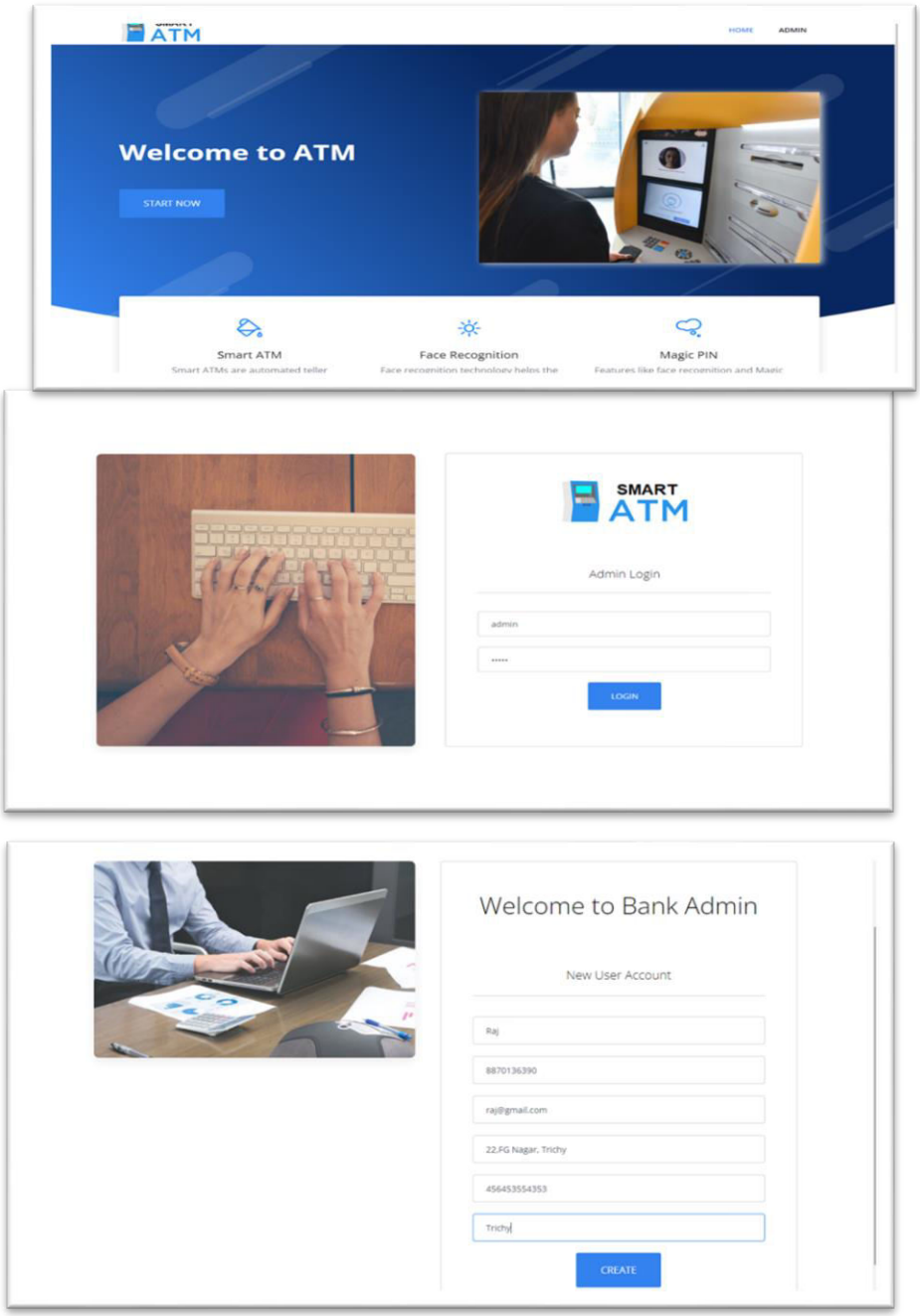
Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

2.1.1.1. Frame Extraction

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

IV. EXPERIMENTAL RESULTS

Figures shows the results of text detection from an image and inpainting by using exemplar based Inpainting algorithm. Figs. 2, 3, 4 (a) shows the original image. (b) is the image obtained by applying first set of criteria. All objects whose area greater than 10000 and filled area greater than 8000 are eliminated and major axis lengths are in between 20 to 3000 are considered to be text. Still, some small non-text objects are detected.

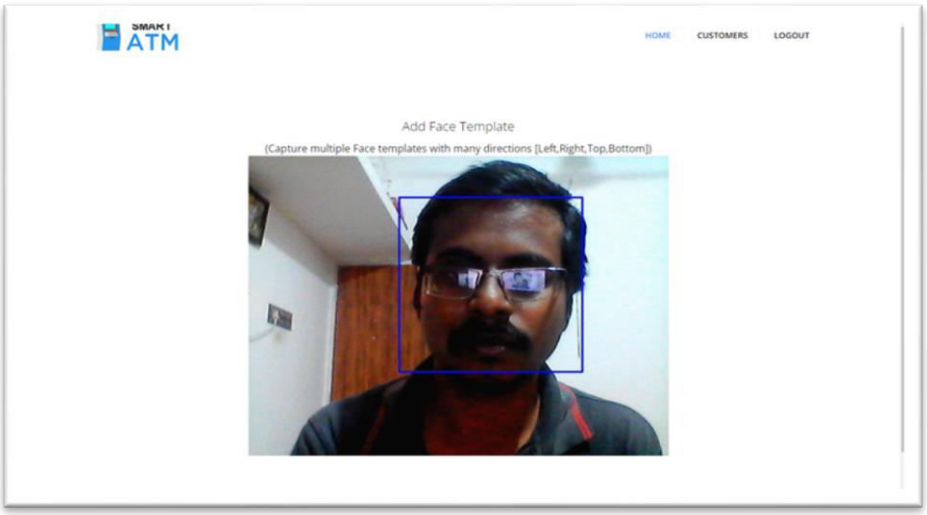


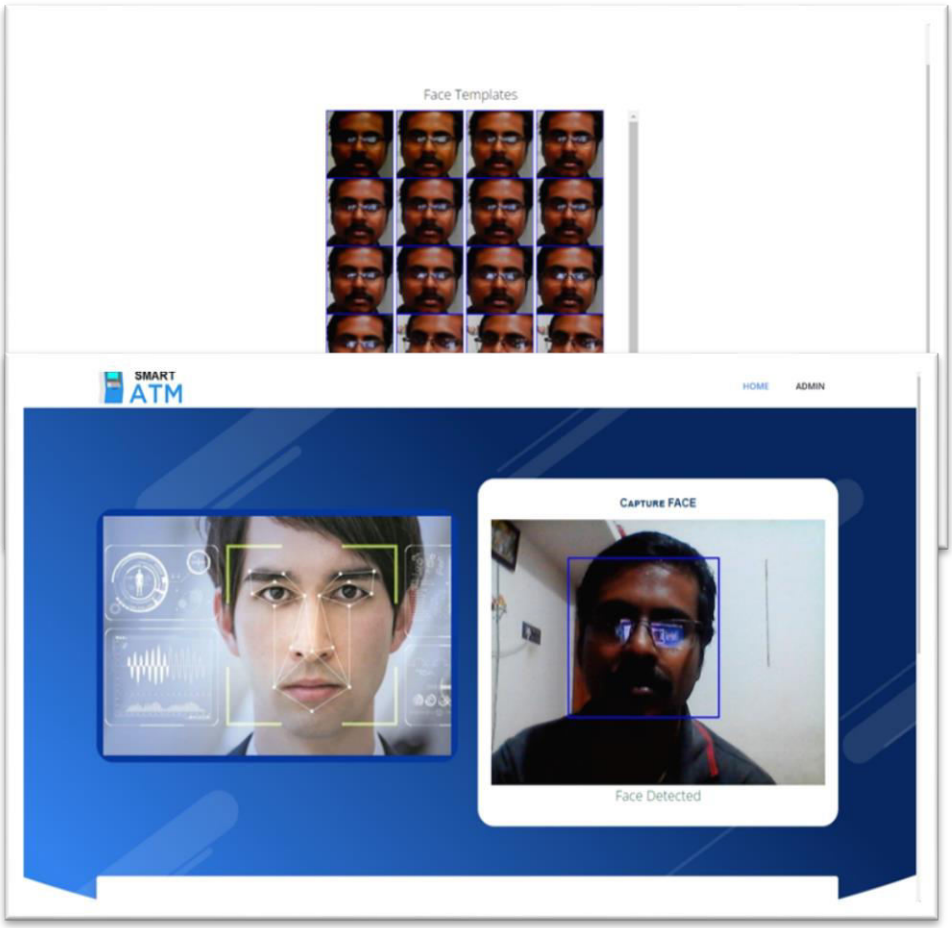
|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India





|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Volume 12, Issue 13, April 2023 ||

International Conference on Recent Development in Engineering and Technology – ICRDET'23

Organized by

Dhaanish Ahmed Institute of Technology, KG chavadi, Coimbatore, India

V. 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 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," 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 based on RFID and FNN-face recognition," in Proc. 2nd Int. Conf. Intell. Syst.Design Eng. Appl., Jan. 2012, pp. 716-719, doi: 10.1109/ISdea.2012.400.
[4] A. A. Wazwaz, A. O. Herbawi, M. J. Teeti, and S. Y. Hmeed, ``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 tradeoffs 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 anti-spoofing 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 surgicallyaltered face images using multiobjective evolutionary algorithm," IEEETrans. Inf. Forensics Security, vol. 8, no. 1, pp. 89-100, Jan. 2013.

INNO SPACE
SJIF Scientific Journal Impact Factor

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

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