Lampyrid 2023: Volume 13, 312–315
ISSN: 2041-4900
https://lampyridjournal.com

An Efficient Framework for Fingerprint Based Cash Machine

Mrs. G. S. L. Poornima[1], Y. Sahitya[2], M. Sai Poojitha[3], S. Narayani[4]
[1] Assistant Professor, Department of CSE, Sridevi Women's Engineering College, Hyderabad, Telangana, India.
Email Id: [1]poornima.gsl19@gmail.com
[2,3,4] UG Student, Department of CSE, Sridevi Women's Engineering College, Hyderabad, Telangana, India.
Email Id: [2]sahityareddy117@gmail.com, [3]saipoojitha333@gmail.com,
[4]robinmitti777@gmail.com

ABSTRACT
The project's overarching goal is to provide a more secure system for banking by using fingerprint identification at ATMs and other financial institutions. The project's aim is to use FINGER Fingerprint identification technology to make banks safer and easier for consumers. Identification and verification of the person who owns or runs the business is required for a variety of activities, including withdrawing money from an ATM, managing access to a structure or garage, unlocking a security device, driving a vehicle, etc. Conventional methods of authentication, such as photo IDs and signatures, have their limitations and are not fool proof. Quick and trustworthy systems are necessary for the infrastructure utilised in these places. Automated Teller Machine (ATM) cash withdrawals are becoming less convenient as further identity verification is required. Users lose money at ATMs because of identity theft that occurs with the current system. Fingerprint Based ATM is a desktop application that uses fingerprint scanning as a security feature. Each fingerprint is somewhat different from every other fingerprint, making them useful for identifying individuals. find them without any help. Instead of using your bank card to make a purchase, try this. ATMs that require fingerprints are more secure and safer for users. You can forget about carrying around a debit card inside your wallet, and never having to replace it if you misplace it. Simply use your fingerprint whenever you need to make a monetary exchange. The user must authenticate through his fingerprints and then enter the PIN number before the transaction can be completed. Users may access their money by requesting a withdrawal. A user may transfer funds to another account by simply entering the receiving account number. Users may request a withdrawal by inputting the amount and selecting a withdrawal method. The customer's financial institution account must have enough money in it to make a withdrawal from an ATM. The user has 24/7 access to their account balance information. The latest five transactions made using the system will be displayed for users to peruse.

Keywords- ATM, Fingerprint, Pin code, Sensor

I.INTRODUCTION

User fingerprints may be utilised as biometrics to infer physiological and psychological characteristics. We have access to a wide variety of biometric technologies, including iris readers, face scanners, and fingerprint readers. Our project will include fingerprint biometrics. Users get their fingernails scanned in order to create a database of biometric characteristics. Fingerprints and other patterns exhibit a high degree of uniqueness. Fingerprints always have the same kinds of lines and spaces. Lines are characterised by ridges, and the spaces between them by valleys. Fingerprint biometrics are the best option because to their widespread applicability, low cost, and ease of use. Fingerprints all seem somewhat different because of this variety. Fingerprints are an unusual method of identification.

2. RELATED WORK

A Graphical User Interface-Based Multibiometric Authentication System that Reads Fingerprints and Palm Prints

Challenges addressed by unimodal biometric systems include data noise, intra-class disparities, few degrees of independence, quasi-universality, spoof attacks, and acceptable error rates. Some of these limitations may be ameliorated by using integrative biometric systems, which incorporate information from a number of different sensors. The research shows a multibiometric authentication method that uses a GUI. The proposal includes both a technique for extracting fingerprint features and an algorithm for extracting palm print features. At last, a multibiometric authentication using both methods was executed. The subject's identity may be shown next to the subject's picture once the test shot has been processed. The proposed fingerprints and palm print approach requires less memory and generates results more quickly than competing methods. Results from matching fingerprints and palm prints using the available methods proved the system's dependability across all of the evaluated circumstances.

Financial Infrastructure Security Using Bimodal Biometrics

Challenges addressed by unimodal biometric systems include data noise, intra-class disparities, few degrees of independence, quasi-universality, spoof attacks, and acceptable error rates. Some of these limitations may be ameliorated by using integrative biometric systems, which incorporate information from a number of different sensors. The research shows a multibiometric authentication method that uses a GUI. The proposal includes both a technique for extracting fingerprint features and an algorithm for extracting palm print features. At last, a multibiometric authentication using both methods was executed. The subject's identity may be shown next to the subject's picture once the test shot has been processed. The proposed fingerprints and palm print approach requires less memory and generates results more quickly than competing methods. Results from matching fingerprints and palm prints using the available methods proved the system's dependability across all of the evaluated circumstances.

3. METHODOLOGY

In order to authenticate a user, fingerprint templates are saved and compared to new fingerprint candidates using matching algorithms. This may be done by directly comparing the original and candidate images or by comparing a subset of characteristics from each. The next thing to do is to apply an automated feature extraction method to the fingerprint picture in order to identify these characteristics. Typically, the coordinates (x, y) and ridge direction () are used to indicate each feature. Algorithms that rely on patterns do so by comparing a candidate fingerprint to a stored template based on the fingerprint's three primary patterns (arch, whorl, and loop). In order to do this, the photos must be oriented consistently. The algorithm does this by locating the exact centre of the fingerprint picture and cantering on it. A visual comparison between the candidate's fingerprint picture and the template is used to establish how close a match there is. After correcting for rotation, translation, and scaling, the matcher subsystem aims to determine the level of similarity between the two feature sets. This degree of resemblance is often quantified with a score. This score is used to determine whether a match will be played or not. The process begins with the choice of a cut-off point. those below the cut-off indicate that the fingerprints do not match; those above it indicate a successful match. The score is usually only a tally of how many minor details match up.

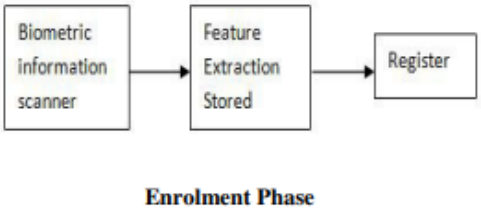

Fig 1-Model diagram

4. RESULT AND DISCUSSION

First, copy the IP address that appears after running the code and paste it into Chrome to access the interface. Otherwise, you won't be able to enter your login information unless you already have an account. Register then Select a fingerprint photo and click the Open button to complete the registration process. If we click the Sign-Up button, we'll be told that the signup is complete and sent to the Login page.

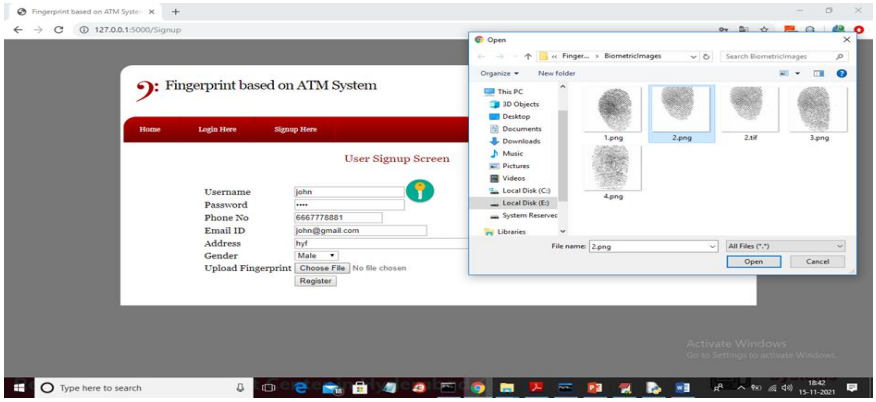

Fig 2-Login page

The following is what happens when I choose the appropriate image file and then click the Login button. When you sign up, you'll be asked to upload an image file; when you log in, you'll be asked to upload the same picture; if they match, only then will you be sent to the transactions page. We'll then be able to do transactions such as withdrawals and deposits. After confirming the successful completion of the transaction, you may check your account balance by selecting View Balance.

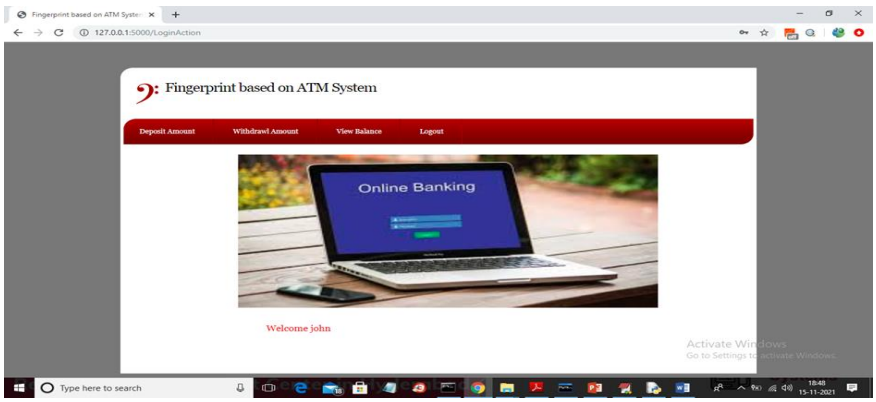

Fig 3-Login successful page

5. CONCLUSION

Autonomous systems are more vital to our contemporary way of life. The fast growth in ATM availability parallels the widespread use of social computing and automated processes. The vast majority of average people often use ATMs. Money transfers, currency exchange, and similar situations are suitable examples. The concept of safety, therefore, is crucial. The security elements were bolstered primarily to ensure the consistency and accuracy of owner identification. Fingerprint technology is the foundation of the whole system, making it more secure, dependable, and user-friendly. To this day, fingerprints remain the most widely accepted biometric for personal identification. Some governments continue to use fingerprinting as a forensic method for identifying residents and criminals at crime scenes. Many thieves illegally alter the ATM machine in order to obtain the consumers' card information. Accounts are at risk of being compromised if the user loses access to their banking information or has their password compromised. Using a payment cardplus a password or PIN to authenticate in a traditional ATM system is not without its flaws. The currently used methods of user authentication, such as passwords with user IDs (identifiers) or ID cards with personal identification numbers (personal identification numbers), have a few drawbacks.

6. REFERENCES

[1] Dr. V. Vijayalakshmi, R.Divya and K. Jaganath, ”Finger and Palm print based Multibiometric Authentication System with GUI Interface” International conference on Communication and Signal Processing, April 3-5, 2013, India, 978-1- 4673-4866-9/13/$31.00 ©2013 IEEE

[2] O.A.Esan and S.M.Ngwira “Bimodal Biometrics for Financial Infrastructure Security” I.O.Osunmakinde School of Computing, College of Science, Engineering and Technology, University of South Africa, UNISA Pretoria, South Africa, 978-1-4799- 0808-0/13/$31.00 ©2013 IEEE.

[3] Rishigesh Murugesh, “Advanced Biometric ATM Machine with AES256 and Steganography”, IEEE Fourth International Conference on Advanced Computing, ICoAC 2012 MIT, Anna University, Chennai. December 13-15, 2012, 978-1- 4673-5584-1/12/$31.00©2012 IEEE.

[4] Rajesh. V and Vishnupriya. S, ”IBIO-A New Approach/or ATM Banking System” 2014 International Conference on Electronics and Communication Systems (ICECS-2014), Feb.13-14, 2014, Coimbatore, INDIA.

[5] G. Renee Jebaline and S. Gomathi , “A Novel Method to Enhance the Security of ATM using Biometrics” , 2015 International Conference on Circuit, Power and Computing Technologies [ICCPCT], 978-1- 4799-7075- 9/15/$31.00 ©2015 IEEE

[6] A.Muthukumar and N.Sivasankari,“A Review on Recent Techniques in Multimodal Biometrics”, 2016 International Conference on Computer Communication and Informatics (ICCCI -2016), Jan. 07 – 09, 2016, Coimbatore, INDIA ,978-1-4673-6680-9/16/$31.00 ©2016 IEEE

[7] Umma Hany and Lutfa Akter,”Speeded-Up Robust Feature Extraction and Matching for Fingerprint Recognition”, 2nd Int'l Conf. on Electrical Engineering and Information & Communication Technology (ICEEICT) 2015.Jahangirnagar University, Dhaka-1342, Bangladesh, 21-23 May 2015, 978-1- 4673-6676- 2115/$31.00 ©20151EEE.

[8] Ms. Archana S. Shinde and Prof. Varsha Bendre, “An Embedded Fingerprint Authentication System”, 2015 International Conference on Computing Communication Control and Automation, 978-1- 4799-6892- 3/15 $31.00 © 2015 IEEE DOI.