IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

Brightness Based Password Safeguard System with Face Recognition in ATM

Sowmiya S R[1], Lalitha D[2], Saranya P[3], Abitha A[4]
Professor, Department of Computer Science & Engineering[1]
Students, Department of Computer Science & Engineering[2,3,4]
Dhanalakshmi Srinivasan Engineering College, Perambalur, India
Corresponding author: Lalitha D (lalithacse111@gmail.com)

Abstract: *The importance of security in the authentication process as well as the increase in threat level posed by such malware has attracted many researchers to the field. Many attacks are successful in accessing social network accounts since the current password-based authentication paradigms are not efficient and robust enough as well as vulnerable to automated attacks. The traditional two-factor authentication mechanisms are not applicable to online social networks because physical token or biometric data cannot be easily used to log into users' profiles. The simplest alternative is complementing the single factor (password-based) authentication process with additional identification elements, such as one-time PIN codes, generated by the user's own device (e.g. the smart phone) or received via SMS. Proposed a brightness based authentication mechanism (i.e., Bright Pass) capable of enhancing the security of identity confirmation PIN codes without asking the user to memorize an additional secret value or to solve a complex cognitive task. This method introduces a new input value that is changed at every usage combining a something you know element (i.e., the PIN) with an interface element that cannot be captured by spyware, i.e., a bright or dark circle displayed on the phone screen to tell the user when to digit the correct PIN digit and when to digit a fake one. It prevents the malware from correctly inserting the PIN code, thereby disallowing the possibility to perform critical operations without the user's agreement. Proposed work also focuses on implementing secure face recognition approach for user authentication. This approach will enhance the performance of ATM system.*

Keywords: ATM Interface Creation, User Account Creation, Application Login, PIN verification using Brightness Password, Face Recognition, ATM Application Access

I. INTRODUCTION

Smart- card-centered password authentication is likely one of the most handy and typically used two-factor authentication mechanisms. This technology has been greatly deployed in quite a lot of varieties of authentication applications which incorporate far off host login, on-line banking and entry manipulate of constrained vaults, activation of protection contraptions, and lots of extra. A sensible-card situated password authentication scheme includes a server S and a customer A (with identity IDA). In the beginning, S securely issues a smart-card to A with the wise-card being personalized with admire to IDA and an initial password. This segment is referred to as the registration segment and is applied best as soon as for each customer. In a while, A can access S within the login-and-authentication phase, and this section will also be implemented as commonly as wanted. Nonetheless, in this section, there could have more than a few sorts of passive and active adversaries in the communication channel between A and S. They may be able to eavesdrop messages and even alter, dispose of or insert messages into the channel. The protection intention of the scheme in this segment is to be certain mutual authentication between A and S. In detailed, the purchaser is required to each have the sensible-card and comprehend the password with a purpose to carry out the wise-card-established password authentication effectively with server S. In other words, the scheme must furnish two-factor authentication.

There are any other necessities/residences that are fascinating in observe. For instance, A could want to exchange password occasionally. Conventionally, this requires A to have interaction with S and S has to keep a password database for its purchasers. In this paper, we recommend the thought of letting a change the password at will without

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

interacting with or notifying S (at the same time making certain two-factor authentication), and also casting off any password database on the server side. Beneath are the reasons. Lots of the present methods require the server to keep a database for the passwords or derived values of the passwords of its purchasers. The derived values of the passwords may also be received through using a password-founded KDF (key derivation operate) which takes a password and a known random price called salt and practice a hash operate or a block cipher for a number of iterations. Nevertheless, this procedure not simplest introduces scalability concern to the server but also makes the systems suffer from disastrous loss when the server is compromised and the password database is stolen via adversaries.

Present programs also undergo from other skills security vulnerabilities. One outstanding difficulty is safety towards offline guessing attack (often referred to as offline dictionary assault). The reason of offline guessing attack is to compromise a customer's password through exhaustive search of all possible password values. In a password-established atmosphere, passwords are viewed to be brief and human memorizable, and the corresponding password house is so small that an adversary is in a position to enumerate all possible values within the area within some cheap period of time. For example, most of the ATM deployments use PINs (personal identification numbers) of simplest 4 to 6 digits long, so the password space has no a couple of million possible values. Hence, an additional security requirement for wise-card-established password authentication is security towards offline guessing attack. In particular, compromising a patron's sensible-card must not allow an adversary to launch offline guessing attack in opposition to the patron's password. In observe the adversary may just steal the wise-card and extract the entire information stored in it through reverse engineering. This concept is paying homage to password-founded authentication protocols.

1.1 Biometric Authentication

Biometric authentication includes any type of authentication method that requires a user's biology. While this may seem like new-age technology, you're probably already using it to unlock the screen on your smartphone. Fingerprint scanning is the most well-known form of biometric authentication, but face recognition tools are an increasingly popular choice for developers. Of course, hackers have a *much* more difficult time replicating a users' biological characteristics, but it is important to note that these authentication processes are often less secure than you'd initially assume. Small fingerprint scanners on smartphones only record portions of your fingerprint, for instance. Multiple images of part of a fingerprint are much less secure than a single, clear image. Remember, too, that biometric authentication can't be changed or altered if a user's fingerprints have been compromised. While biometric authentication holds a lot of promise, it's now most useful as an additional login tool to bolster another system.

1.2 Face Recognition:

A face recognition system for an ATM application involves using facial recognition technology to identify and authenticate users attempting to access an ATM. This type of system utilizes machine learning algorithms and computer vision technology to capture an image of a user's face and compare it to a pre-existing database of authorized users. The goal is to prevent unauthorized access to the ATM, enhance security, and simplify the authentication process for users. When a user approaches the ATM, the facial recognition system will capture an image of their face and compare it to the authorized user database. If there is a match, the user will be granted access to the ATM and can proceed with their transaction. If there is no match or the user is not authorized, access will be denied.

The implementation of a face recognition system for an ATM application can improve security and prevent fraudulent activities, such as using stolen cards or PIN numbers. It can also enhance the user experience by eliminating the need for physical cards or PIN numbers, making the process faster and more convenient.

II. RELATED WORK

Dutta, et.al,.[1] proposed the idea of using fingerprints of customers as password included with traditional PIN number. After authorized verification, the customer will be able to proceed for transaction else after three successive wrong attempts, the ATM card will be blocked for 24 hours and a message will be sent to the registered mobile number. The proposal is to use fingerprints in ATMs as passwords involved with the PIN number. Fingerprint recognition will make users relax by preventing unauthorized account access and assuring security. Here, a fingerprint module generates 4-digit code as a message to the customer's assigned mobile number by placing finger on it and on the basis of validation

ISSN 2581-9429 IJARSCT

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

of this code, customers are allowed for further access. A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human hand. A friction ridge is a raised portion of the epidermis on the fingers and toes (digits), the palm of the hand, consisting of one or more connected ridge units of friction ridge skin.

This software is implemented by the steps as follows: first of all. The system is initialized to implement specific task, such as checking ATM system, GSM communication and so on, and then each module reset for ready to run commands. Before using ATM terminal, the mobile number and fingerprint of the customer is required. Automatic Teller Machines is the most used technology in the increasing financial transaction of the current world. There are many possible way to misuse ATM card using PIN. Fingerprint recognition helps to achieve an authentic state of security access through verification and validation. This work identifies a high level model for the modification of existing ATM systems using both security protocols as PIN & Biometric fingerprint strategy and GSM technology..

Sahar, et.al,.[2] implemented Fingershield ATM, ATM Machine that implements biometric identification in the form of fingerprints which is integrated with smart card and database server. Fingerprint technology is powerful identification because of its unique characteristics of each of the minutiae. Fingerprint is a distinct pattern of ridges and valleys on the finger surface of an individual. A ridge is defined to be a single curved segment whereas a valley is the area between two adjacent ridges. Minutiae points are the major features of a fingerprint image and are used in the matching of fingerprints. These minutiae points are used to determine the uniqueness of a fingerprint image. A good quality fingerprint image can have 25 to 80 minutiae depending on the fingerprint scanner resolution and the placement of finger on the sensor.

The database server subsystem is comprised of two main processes: fetch data and update data. This function will be used to communicate with the database using an SQL query. Fetch data is a function to fetch the current database record values into the client machine. It has 2 modes: fetch all data field of a record identified by card code; and fetch a name field of a record identified by account number for transfer purposes. Update data is a function to change the values of fields in a record. It have three modes: to change the balance field of a record identified by card code for withdrawal purposes; to change the balance value of a record identified by the account number for transfer purposes; and to change the valid field value of a record for blocking purposes.

Jaiswal, et.al,.[3] presented the idea of using fingerprints of customers as password included with traditional PIN number. After authorized verification, the customer will be able to proceed for transaction else after three successive wrong attempts, the ATM card will be blocked for 24 hours and a message will be sent to the registered mobile number. The proposal is to use fingerprints in ATMs as passwords involved with the PIN number. Fingerprint recognition will make users relax by preventing unauthorized account access and assuring security. Here, a fingerprint module generates 4-digit code as a message to the customer's assigned mobile number by placing finger on it and on the basis of validation of this code, customers are allowed for further access. A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human hand. A friction ridge is a raised portion of the epidermis on the fingers and toes (digits), the palm of the hand, consisting of one or more connected ridge units of friction ridge skin.

This software is implemented by the steps as follows: first of all. The system is initialized to implement specific task, such as checking ATM system, GSM communication and so on, and then each module reset for ready to run commands. Before using ATM terminal, the mobile number and fingerprint of the customer is required. Automatic Teller Machines is the most used technology in the increasing financial transaction of the current world. There are many possible way to misuse ATM card using PIN. Fingerprint recognition helps to achieve an authentic state of security access through verification and validation. This work identifies a high level model for the modification of existing ATM systems using both security protocols as PIN & Biometric fingerprint strategy and GSM technology.

Papadopoulos, et.al,.[4] Propose IllusionPIN (IPIN), a PIN-based authentication method that operates on touch screen devices. IPIN uses the technique of hybrid images to blend two keypads with different digit orderings in such a way, that the user who is close to the device is seeing one keypad to enter her PIN, while the attacker who is looking at the device from a bigger distance is seeing only the other keypad. The user's keypad is shuffled in every authentication attempt since the attacker may memorize the spatial arrangement of the pressed digits. IllusionPIN is a PIN-based authentication scheme for touch screen devices which offers shoulder-surfing resistance. The design of IllusionPIN is

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

based on the simple observation that the user is always viewing the screen of her device from a smaller distance than a shoulder-surfer. Based on this, the core idea of IllusionPIN is to make the keypad on the touch screen to be interpreted with a different digit ordering when the viewing distance is adequately large. This way, when the shoulder surfer is standing far enough, he is viewing the keypad as being different from the one that the user is utilizing for her authentication, and consequently he is unable to extract the user's PIN. Also, the keypad is shuffled in every authentication attempt (or every digit entry) to avoid disclosing the spatial distribution of the pressed digits. We create the keypad of IllusionPIN with the method of hybrid images and we call it a hybrid keypad.

Prabhu, et.al,.[5] proposed IBAUIP model, the Illusion PIN is a PIN based authentication scheme for touch screen devices which offers shoulder-surfing resistance. The design of Illusion PIN is based on the simple observation that the user is always viewing the screen of user device from a smaller distance than a shoulder-surfer. The core idea of Illusion PIN is to make the keypad on the touch screen to be interpreted with a different digit ordering. when the viewing distance is adequately large. This way, when the shoulder surfer is standing far enough, observer is viewing the keypad as being different from the one that the user is utilizing for user authentication, and consequently observer is unable to extract the user's PIN. IPIN uses the technique of hybrid images to blend two keypads with different ordering of digit in such a way, that the user who is near to the device is seeing one keypad to enter user PIN, while the attacker who is looking at the device from a bigger distance is seeing only the other keypad.

III. EXISTING METHODOLOGIES

Many attacks are successful in accessing social network accounts since the current password-based authentication paradigms are not efficient and robust enough as well as vulnerable to automated attacks. The traditional two-factor authentication mechanisms are not applicable to online social networks because physical token or biometric data cannot be easily (and hence practically) used to log into users' profiles. The simplest alternative is complementing the single factor (password-based) authentication process with additional identification elements, such as one-time PIN codes, generated by the user's own device (e.g. the smartphone) or received via SMS. This can be useful to further confirm the user's identity when signing on from unusual locations or performing specific actions, such as changing or accessing important configuration data within the user's profile. Unfortunately, the mobile devices used for gaining access are often vulnerable to several kind of malware that can be able to retrieve data such as passwords and PIN codes as they are inserted to perform authentication to the target social network applications. Hence, the presence of such malware in mobile platforms can seriously impact the user's privacy and security, reducing the user's trust in performing mobile access to its preferred social network services.

3.1 Pass Window Approach

Pass Window, an authentication method that use PIN digits and a pre-selected image called Pass-icon as the password. The basic idea behind this system is that the Pass-icon is displayed to the user with other randomly selected decoy icons on a graphical grid called Pass-Window. The user has to memorize the pass-location which is the location of pass-icon within the pass-window. Afterward, the virtual keypad in addition to the pass-window without its images appears in the center of the screen. To authenticate, the user has to move the pass-window on the virtual keypad by tilting it (thus using accelerometers) in such a way that the pass-location moves over the PIN. To enter each digit, the user has to cover the rear camera lens with a finger to hide the input. In this way, it prevents shoulder surfing attacks and increases the security against side channel attacks and one time recording attacks. However, this approach is vulnerable to multiple recording attacks and its user study shows that the authentication speed is very low.

IV. SECURE ATM ACCESS USING BRIGHTNESS PASSWORD WITH FACE RECOGNITION APPROACH

Proposed a BrightPass authentication, here screen capture and screen recording techniques do not take the display brightness setting into account. The order of the PIN digits positions is randomly generated by the SE and then secretly shared with the user via an alternating circle's brightness displayed on the mobile device. If the circle's brightness value is high, the user must insert a correct PIN digit. Whenever it looks dark to the user, he is required to enter a misleading lie digit. In this way, only the legitimate user and the SE know the real PIN digits along with its positions in the currently generated sequence. Thereby, even if a mobile malware can steal the PIN by analyzing the differences

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

between inputs recorded through repeated side-channel attacks it will not be able to authenticate in the next operation. This is due to the randomization of PIN digit positions in the sequence generated for each authentication, and to the use of different screen brightness level each time. In our scheme brightness is adopted as a secure channel to secretly tell the user when to input a correct PIN digit and when to input a misleading lie digit. Along with normal PIN verification system, an additional face image verification to ensure tight security. If every entered detail is correct then user continues with face verification process then PIN is verified using Bright Pass system.

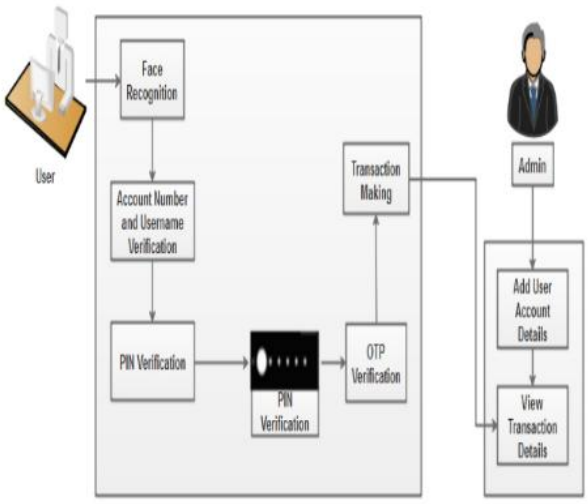


Fig 4.1: Architecture for Proposed Work

V. IMPLEMENTATION

5.1 Framework Creation

Online transaction is thus changing the way people shop and how retailers operate. There is a steep decline in traditional payment methods such as cash and cheque and people are choosing the emerging digital payment technologies as they render convenient and flexible methods for conducting cashless financial transactions. However, this technology and digital convergence has also attracted the threat of cyber-attacks and made banks and financial institutions more vulnerable to fraud. It has led to a new breed of fraud perpetrators that use sophisticated technologies to hack into personal devices and corporate networks. Traditional techniques such as password or tokens are no match to their attacks. To overcome, these attacks, we can design the interface for online transactions in ATM system. In this module, admin and user interface created. Admin can be view the details of users, accounts details and so on. The user can be performing various operations such as net banking, credit card transactions, and debit card transactions and on.

5.2 User Verification

User has to register the appropriate details in the bank server database for using the online banking template. These details include user name, address, email id, contact number, primary password. These details are stored in the first server database. User should login with the username and PIN. While entering the PIN, the normal keypad will be changed to a Bright pass based keypad. If the details entered matches with the details available, the user will be redirected to the home page. If no match found, the user have to re-enter the details again. After each login, the keypad will be shuffled. This is done to avoid shoulder surfing.

5.3 Face Recognition

The Face Recognition is the study of physical or behavioral characteristics of human being used for the identification of person. These physical characteristics of a person include the various features like fingerprints, face, hand geometry, voice, and iris biometric device. These Face Recognition features can be used to make net-banking systems more secure for authentication purpose in banking based account security systems. Face recognition presents a challenging problem in the field of image analysis and computer vision. The security of information is becoming very significant and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

difficult. In this module, we can implement features based method to detect the facial parts such as nose, lips, eyes, cheeks using iterative closest point algorithm. In this module we use, for performing ICP, a set of features selected based on the tolerance level of spatial deviation.

5.4 Bright Pass System

BrightPass is designed to protect PIN code from automatic action/operation approval by malware. Since this is achieved using the screen brightness as a communication channel that is invisible to the mobile malware, it is obvious that humans can solve this challenge easily. In BrightPass authentication session, where the user inputs the PIN and lie digits according to the circle's brightness. A bright circle tells the user to input a correct PIN digit (highlighted in green) while a dim circle means to enter a misleading lie digit (highlighted in red). Here used the gray color to show the dim circles for presentation purposes, since the screenshot cannot capture the device's brightness.

5.5 ATM Application

In proposed ATM facility, admin would need to register with the institution for the provider, and set up a password and different credentials for user verification. User should complete the verification criteria then access ATM application. In ATM application, user can perform transaction, withdrawal, balance enquiry and mini statement details.

VI. METHODOLOGY

6.1 Face Recognition using Grassmann Learning

The Grassmann Learning Algorithm (GLA) is a machine learning algorithm that is commonly used for face recognition. It operates on the assumption that images of faces lie on a low-dimensional manifold within a high-dimensional space. Here are the general steps involved in using the GLA for face recognition:

- Data Preparation: Collect a dataset of face images that includes multiple images of each person you want to recognize. Each image should be pre-processed to remove noise and standardize the illumination conditions.
- Feature Extraction: Extract features from the pre-processed face images. A popular technique for this is to use Principal Component Analysis (PCA) to reduce the dimensionality of the image data.
- Subspace Learning: Use the GLA to learn the low-dimensional subspace that best represents the face images. The GLA accomplishes this by iteratively refining the subspace until it captures the majority of the variance in the face images.
- Classification: Once the subspace has been learned, you can classify new face images by projecting them onto the subspace and comparing them to the subspace representations of known faces. The closest match in the subspace is the identity of the person in the new image.
- Model Refinement: The performance of the GLA can be improved by iteratively refining the subspace and adjusting the classification threshold until the desired accuracy is achieved.

The GLA is a powerful algorithm for face recognition that learns the underlying low-dimensional structure of face images and uses it to classify new faces. By iteratively refining the subspace and adjusting the classification threshold, the GLA can achieve high levels of accuracy even with noisy or incomplete data.

VII. EXPERIMENTAL RESULTS

Experimental result shows the overall performance of the proposed system. Here Brightness password and Face recognition methods are implemented for ATM application using .NET as front end and SQL as back end software. This will helps to improve user authenticity in ATM application access.

7.1 Framework Creation

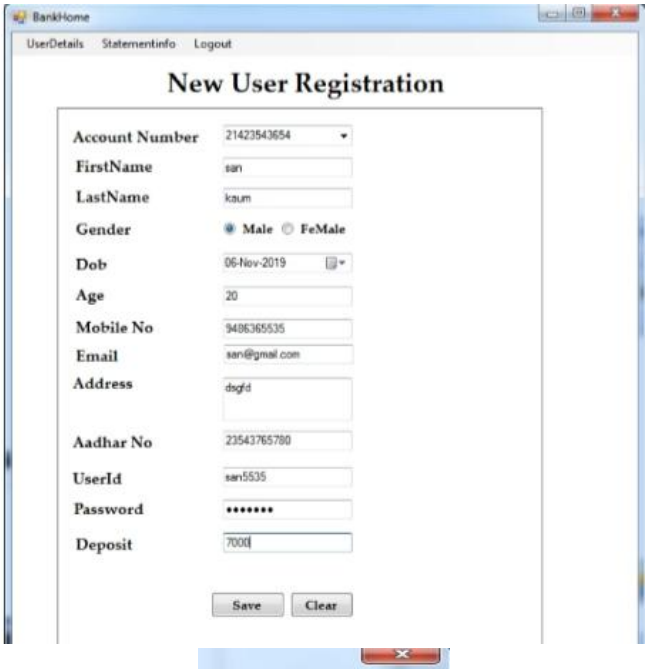
This module explains about framework creation process. Proposed framework has bank login and user login page. Here admin should add account details of user's. Then capture and store the user's face image for real time face recognition process.

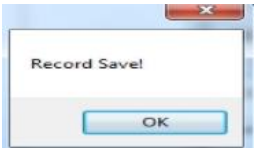
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

Home Page

Bank Login

Add User Account Details





IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

User Face Register

7.2 User Verification

This module explains about the process of user verification.

Here user should verify using their password and face recognition approach. Here user can set their PIN number for further verification process.

User Login home Page

Set PIN Number

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

7.3 Face Recognition

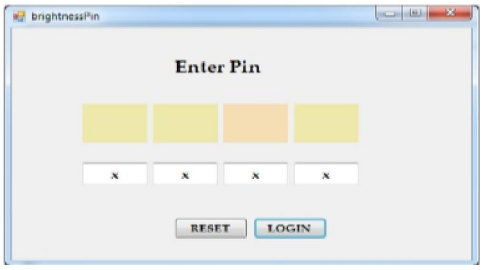
This module explains about the process of user verification using their face image in real time face image capturing process.

Face Capture and Verification

7.4 Bright Pass System

This module explains about the PIN verification using brightness based authentication method. User should enter the correct PIN number in highest brightness value and enter fake one in lowest brightness digit. This will enhance the security in PIN authentication method also avoids the shoulder surfing attack.

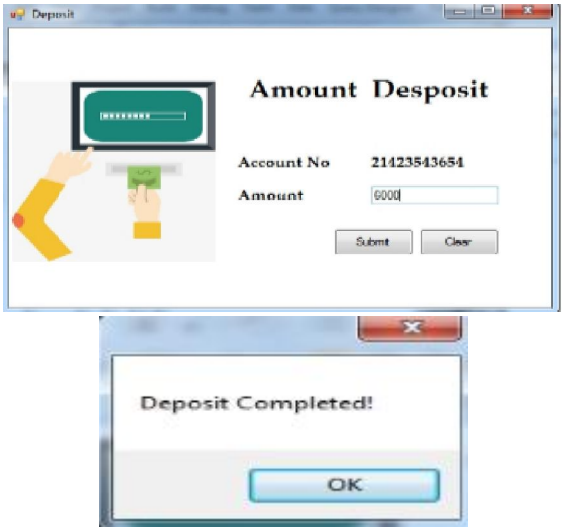
Bright Pass System



7.5 ATM APPLICATION

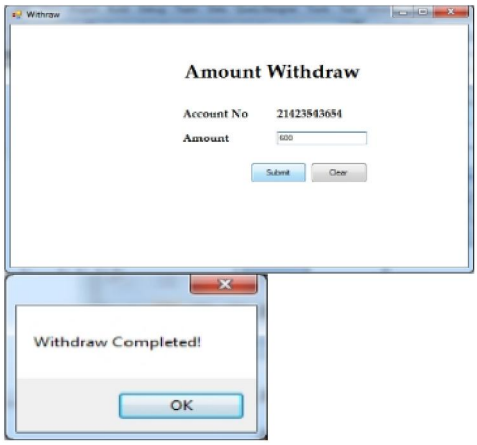
This module explains the process of ATM application access. Here users are allowed to make ATM process such as deposit amount, withdrawal of amount and balance checking.

Amount Deposit

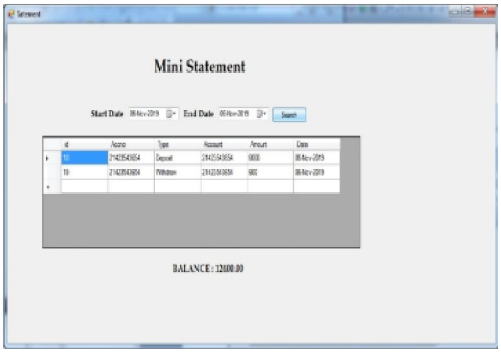


IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

Amount Withdrawal



View Statement



VIII. CONCLUSION

The proposed system explains a hybrid keypad is implemented in a ATM application. The main goal of our work was to design a PIN-based authentication scheme that would be resistant against shoulder surfing attacks. To this end, we created Illusion PIN. The proposed system has quantified the level of resistance against shoulder-surfing by introducing the notion of safety distance. In the context of the visibility algorithm, we had to model at a basic level how the human visual system works. In this process a number of simplifying assumptions that limit the accuracy of our calculations. This means that even if a person perceives the digits on a hybrid keypad to be equally visible to the digits on a digital keypad, the distortion in the hybrid keypad is bigger and the visibility index has a lower value. This is something logical, because when the reference buttons are all same color, a digit that is even slightly visible is considered a big distortion.

REFERENCES

[1]. Dutta, Mithun, Kangkhita Keam Psyche, and Shamima Yasmin. "ATM transaction security using fingerprint recognition." Am J Eng Res (AJER) 6, no. 8 (2017): 2320-0847.

[2]. Sahar, Bayu Aji, Azel Fayyad Rahardian, and Elvayandri Muchtar. "Fingershield ATM–ATM Security System using Fingerprint Authentication." In 2018 International Symposium on Electronics and Smart Devices (ISESD), pp. 1-6. IEEE, 2018.

[3]. Jaiswal, Ashish M., and Mahip Bartere. "Enhancing ATM security using Fingerprint and GSM technology." International Journal of Computer Science and Mobile Computing (IJCSMC) 3, no. 4 (2014): 28-32.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

[4]. Papadopoulos, Athanasios, Toan Nguyen, Emre Durmus, and Nasir Memon. "Illusionpin: Shoulder-surfing resistant authentication using hybrid images." IEEE Transactions on Information Forensics and Security 12, no. 12 (2017): 2875-2889.

[5]. Prabhu, K. D. D. P. "Image based authentication using illusion pin for shoulder surfing attack." Int. J. Pure Appl. Math 119, no. 7 (2018): 835-840.

[6]. Agrawal, Sarita, Manik Lal Das, and Javier Lopez. "Detection of node capture attack in wireless sensor networks." IEEE Systems Journal 13, no. 1 (2018): 238-247.

[7]. Sahar, Bayu Aji, Azel Fayyad Rahardian, and Elvayandri Muchtar. "Fingershield ATM–ATM Security System using Fingerprint Authentication." In 2018 International Symposium on Electronics and Smart Devices (ISESD), pp. 1-6. IEEE, 2018.

[8]. Al Imran, Md, M. F. Mridha, and Md Kamruddin Nur. "OTP Based Cardless Transction using ATM." In 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), pp. 511-516. IEEE, 2019.

[9]. Munadi, Rendy, Arif Indra Irawan, and Yuman Fariz Romiadi. "Security System ATM Machine with One-Time Passcode on M-Banking Application." In 2019 International Conference on Mechatronics, Robotics and Systems Engineering (MoRSE), pp. 92-96. IEEE, 2019.

[10]. Dutta, Mithun, Kangkhita Keam Psyche, and Shamima Yasmin. "ATM transaction security using fingerprint recognition." Am J Eng Res (AJER) 6, no. 8 (2017): 2320-0847.