

Bank Transaction using Face Recognition

Swarnnalakshmi¹, Ayyanar raja M², Giridharan G³, Navin R⁴

Assistant Professor, Department of Computer Science and Engineering¹

Student, Department of Computer Science and Engineering^{2,3,4}

Dhanalakshmi College of Engineering, Chennai, Tamil Nadu, India

Abstract: *In this project we are going to develop a robust automated web application for transacting money in higher level security purpose with high facial recognition. We must first register our personal information using our faces and pass a liveness detection test. For rapid and accurate results, a Haar cascade-based technique was used. Simple face detection from the input image. The image of the face is then transformed to a grayscale image. The iris, eyebrows, nose, and mouth of candidates are then taken from the intensity valleys of the identified face and stored as datasets, allowing our system to determine who is approved and who is not. While logging in, our faces will be identified, and if we are approved, we will be able to proceed to the authorised page; otherwise, our system will not allow us to log in. For higher security purpose we have used face recognition module. Our face will be identified throughout the transaction, and only the authorised account holder will be able to transact money; others will not be able to transact money.*

Keywords: HAAR Cascade, Web Application, Face Recognition

I. INTRODUCTION

In the banking and financial services industries, this is especially true. Face recognition has been gaining traction over touch and type-based engagements since the dawn of the digital revolution, owing to the ease it provides without jeopardising transaction security. Despite an increase in EMV card usage (Europay, MasterCard, Visa) There has been an increase in financial fraud incidents, which has been attributed to password creation procedures. As a result of the billions of dollars wasted by large banks, there has been a push to move to biometric facial recognition to combat the problem. It means that banking software will rely on facial scans, which will be compared to similar ones submitted into the bank's system by employees to verify the customer's identity. The goal is to verify the identification of the account owner and only allow a transaction to proceed if the identity of the account owner can be positively verified

II. LITERATURE REVIEW

Facial-Recognition Payment: An Example of Chinese Consumers New issues have arisen as a result of the introduction and widespread use of facial-recognition payment technology. Although using a credit card is convenient, it is also easy to misplace one or forget the password. Passwords can be exchanged and cracked because users use simple passwords and reuse them across several accounts and services. QR payment is Smart phones are inextricably linked to them, but they can be lost, transmissions might be unpredictable, and batteries can run out. However, facial-recognition technology, It immediately adds to total efficiency, performance, and accuracy by detecting and describing feature vectors without physical contact. Currently, studies Facial-recognition technology and facial-recognition payment systems are quite popular in terms of technological issues. Many studies have been done on the facial-recognition system's operating principle, its reliability, and its potential development trend. However, research on the characteristics of facial-recognition payment and the factors influencing customer intent to use is rare for non-technical issues, such as from the standpoint of consumers. As a result, the research's purpose has been achieved. is to find out what factors influence people's readiness to utilise facial-recognition payment systems. This study has selected security, The feature variables of the facial-recognition payment system are visibility, expected effort, and social image. Consumers' intent to utilise the system is influenced by the system's safety, security, visibility, and social image, according to the findings of this paper. It can also influence consumers' intent to use by influencing their perception of utility. The amount of effort required has a direct impact on intent to use, but it is also influenced by the mediating element of perceived usefulness.

In this study, the consumer's personality trait of openness moderates the association between security, expected effort, and usage intention.

The usage of cards or internet banking is the most recent trend in financial transactions. A person may have many bank accounts with various banks, making it difficult for him or her to manage transactions, since he or she must either carry multiple cards or utilise a variety of bank websites to complete his or her transactions. This condition necessitates the development of a simple, secure, and high-tech method for completing transactions. We propose Such a system, which leverages slashing technologies such as NFC and multifactor authentication, can be employed on any NFC-enabled smartphone. The multi factor The authentication system uses a 4-digit PIN as the knowledge factor, an NFC-enabled Smartphone as the possession factor instead of cards, and the user's face as the identity factor. The authentication system uses a 4-digit PIN as the knowledge factor, an NFC-enabled Smartphone as the possession factor instead of cards, and the user's face as the identity factor. For the purposes of authentication, the inherence factor is used. The proposed system, which can be implemented as a cross-platform mobile application, allows the user to not only conduct secure transactions, but also to conduct transactions from numerous accounts

Payment cards are progressively would be used in a diverse settings, involving shopping, restaurants, lodges, and online booking of hotels, cinema tickets, aircraft and train tickets, and other. So the problem is that a person must have payment cards with him at all times and keep them secure in order to exploit them. This was also insecure. Biometric face - recognition payments are employed in all types of payments in the current work. As a result, it eliminates the need to learn multiple passwords. Face recognition is a safe, secure, and simple to use payment mechanism. In comparison to other electronic payments, it is more dependable and efficient. Face recognition is used to offer a broad design for an online payment system distance

Author: Niccolo Mejia, 2019 Conference

Consumer applications such as the ability to unlock one's smartphone with one's face are propelling facial recognition software into the mainstream. Since machine learning became a big topic in the professional world in the early years of the decade, the banking sector has been at the forefront of enterprise adoption of AI; as a result, it's only inevitable that facial recognition technology would start to make its way into banking. There are a few startups delivering facial recognition software to banks that, on the surface, appear to have the C-suite talent that we look for when assessing a company's claims to be employing AI. These businesses provide software with applications regarding the physical security to customer service. to use their faces to persuade withdrawals Facial recognition is one of many ways banks may improve efficiency and accessibility for their customers by lowering the interfacial tension. Some experts believe that this is how banks will prosper in the future, as AI and other innovations enable banks to provide more services with no downtime.

In the financial sector, there is a compelling need to ensure safety. Banking became a lot easier with the arrival of Automatic Teller Machines, however it came with its own set of security issues. The Pos has become insecure as the number of crooks and their actions has increased dramatically. For authenticity verification, ATM systems now just require an access card and a PIN. With the Raspberry Pi controller, an attempt is made to construct a system that integrates biometric identification into the additional authentication process and uses an RFID card to handle many accounts on the same card. Consumers and lending companies alike would benefit from the adoption of such a system, which would protect them against invaders and identity thieves. This study suggests a security system for bank machines. a model that blends an RFID card, a PIN, and biometric facial recognition to the degree of holding the crooks' card Faces, as well as PINs, would be protected if this technology became widely utilized. Although it is clear that manes biometric traits cannot be mimicked, our idea will go a long way toward addressing the problem of account security by allowing only the account owner to access his accounts. The strategy of merging biometric features suits the objective of both identification and authentication.

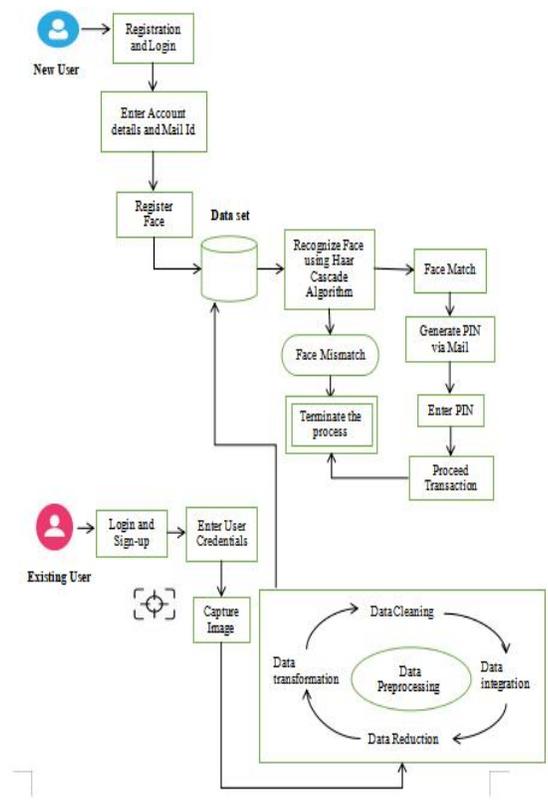
Authors: Dr. SHAIK ADBUL MUZZER, .GOSALA SUBHASIN

More security for web services seems to have been a major priority in current history. As a result, in security systems, secure authentication process is now the most important responsibility. Most systems are currently built on username and password pairs, which solely verify a user's identity at the login phase. During communicate and understand, no

further inspections are made once the user has been identified using a username and password. However, new biometric solutions replace the login details with the user's biometric data. Single shot verification is still inefficient in this manner because the user's identification stays unchanged during the session. As a result, a basic option is to utilise very brief delay for each session and to periodically ask the user to re-enter his credentials.

Face detection utilizing color of skin detection in color photographs is a common and important technique. The tone of a person's face is very important. There are various advantages to using skin colour as a characteristic for tracking a face. Processing colour takes far less time than processing other facial aspects. Each pixel was categorized as skin or non-skin in the skin tone detection phase based on its colour components. The HSV colour model is frequently favoured over the RGB colour model in circumstances where colour description is critical. The colour image is initially segmented into skin and non-skin regions, which is the first stage in face detection. Skin zone and semi region are represented by various ranges of pixels in give some suggestion.

III. SYSTEM ARCHITECTURE



UML is a language for describing, visualising, producing, and documenting software system arte facts. The Object Management Group (OMG) and UML collaborated to establish UML. UML is a general-purpose visual modelling language that may be used to envision, design, and document software systems. Although UML is commonly used to represent software systems, and it is not restricted to this .It can also be used to represent non-software systems, such as process flow in a manufacturing facility. Although UML is not a programming language, it can be used to generate code in a variety of languages using tools based on UML diagrams. Object-oriented analysis and design are inextricably linked to UML. UML became an Object Management Group standard after some standardisation.

IV. SYSTEM IMPLEMENTATION

This paper shows the implementation of

WEB APPLICATION:

- **MODULE 1:** Register
- **MODULE 2:** Login
- **MODULE 3:** Data Preprocessing
- **MODULE 4:** pythonSqlite3Module APIs
- **MODULE 5:** connection.cursor

Register

In this module user have to enter their personal details along with their face. Dataset will be created based on the username.

Login

User have to enter credentials during that period face will be recognized it will allow only authorized user.

Data Preprocessing

In this module the collected dataset from user in the time of registration will be stored in folder and all image are resized to standard and unique size and the image are converted to gray scale image and noise are removed .

PYTHON SQLITE3 MODULE APIS

The following are the most important sqlite3 module algorithms that will allow you to work with SQLite databases from your Programming language. If you get a more generates high, visit the official documentation for the Python sqlite3 module.

`connect.sqlite3 (database [,timeout ,other optional arguments])`This API establishes a connection to a SQLite database. `":memory:"` can be used to open a database connection to a database that is hosted in RAM rather on disc.

If the database is successfully opened, connection object is provided. If several connections visit a database and one of the processes alters it, the SQLite dataset is locked until the transaction is committed. The timeout variable indicates how long the connection should wait for the lock to release prior raising an error. The timeout parameter's possible values is 5.0. (five seconds).This function will start collecting data if the supplied db name does not exist. If you wish to build a database somewhere other than the root folder, you could also specify filename with the appropriate location.

connection.cursor([cursorClass])

This procedure produces a cursor that you'll use throughout your Python database programming. This method is suitable for cursorClass is indeed a single optional parameter. It must have been a custom pointer class that inherits sqlite3 if supplied.

Algorithm Used

Cascade of Haar Here is an example of calculating the Haar value from a rectangular image slice. Pixels with a value of 1 are darker in the haar feature, while pixels with a value of 0 are lighter. Each of these is in charge of identifying a specific feature in the image. Any structure in the image with a quick shift in intensities, such as an edge, a line, or any other structure. The haar feature, for example, can detect a vertical boundary with darker pixels on the right and brighter pixels on the left in the image above. The goal is to calculate the sum of all image pixels in the haar feature's darker area, as well as the sum of all image pixels in the lighter area.

This is only a visual illustration of the haar feature traversal concept. The haar feature would traverse the image pixel by pixel in its actual work. The haar characteristics will also be applied in all feasible sizes. These are divided into three groups based on the attribute that each person is seeking for. The first pair of two rectangular features is in charge of determining whether the edges are horizontal or vertical (as shown above). The second set of three rectangle features is in charge of determining whether a lighter zone is flanked on either side by darker sections or vice versa. The final set of four rectangular characteristics is in charge of determining how pixel intensities fluctuate across diagonals.

System Evaluation

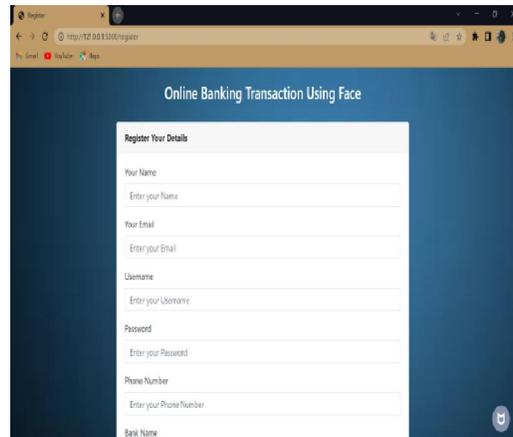
The goal of testing is to find mistakes. Testing is the practise of attempting to find all possible flaws or weaknesses in a work product. It allows you to test the functionality of individual components, sub-assemblies, assemblies, and/or a whole product. It is the process of testing software to ensure that it meets its requirements and meets user expectations, and that it does not fail in an unacceptable way. There are many different types of tests. Each test type is designed to fulfil a distinct testing need.

VI. RESULTS

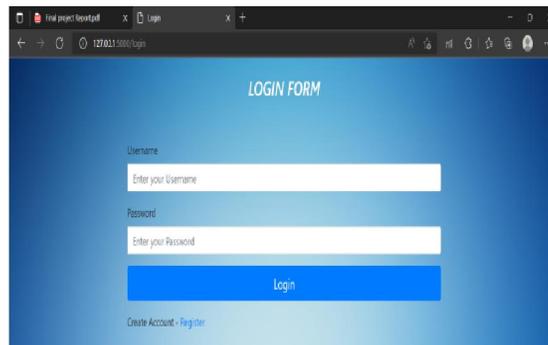
HOME PAGE



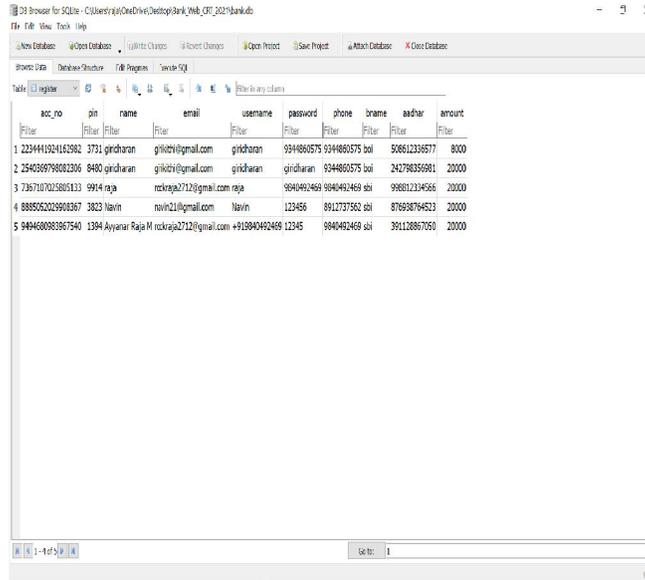
REGISTER PAGE



LOG IN PAGE



REGISTERED USERS RECORD



acc_no	pin	name	email	username	password	phone	brame	aadhar	amount
1 223441324162982	3731	gricharan	gri1ch1@gmail.com	gricharan	994860575	9344860575	bol	508612336577	8000
2 2540589798882306	8480	gricharan	gri1ch1@gmail.com	gricharan	9344860575	bol	24279835981	20000	
3 7367107015805133	9914	raja	rockraja212@gmail.com	raja	9940492469	9840492469	abi	99881234566	20000
4 88855202990367	3823	navin	navin21@gmail.com	Navin	123456	8912737562	abi	876920764512	20000
5 949468983967540	1394	Ayyanar Raja	rockraja212@gmail.com	+919840492469	12345	9840492469	abi	391128867050	20000

OUTPUT SCREEN



TRANSACTION SUCCESS

In this case, if the face detects successfully, it indicates the transaction was a success.else it shows transaction not successful.

VII. CONCLUSION

Realized a reliable, real-time face recognition system on machine learning. Certain progress has been made, and some procedures have been developed, according to the new technological period. of facial recognition have achieved popularity. We are using Haar cascade algorithm for face recognition .Capture module deals with the configuration of video interface and performs the real-time video capture. Each captured frame is analysed by the Face Detection module, which extracts valid faces from each frame. Face Identification deals with face recognition and verification of the detected face. In Future any fraudulent access by the fake user is eliminated with the help of radio frequency identification card

REFERENCES

- [1]. Facial-Recognition Payment: An Example of Chinese Consumers, Wen Kun Zhang ; Min Jung Kang, IEEE Access, Year: 2019

- [2]. Secure multifactor authentication payment system using NFC, AnirudhanAdukkathayar; Gokul S Krishnan ; Rajashree Chinchole, 2015 10th International Conference on Computer Science & Education (ICCSE)
- [3]. Biometric Face Recognition Payment System , Surekha. R. GondkarSaurab. Dr. C. S. Mala International Journal of Engineering Research & Technology NCEES - 2018 Conference Proceedings
- [4]. Facial Recognition in Banking – Current Applications, Niccolo Mejia,2019 Conference Proceedings
- [5]. "Face Detection and Recognition for Bank Transaction ", International Journal of Emerging Technologies and Innovative Research , SudarshanDumbre ,ShamitaKulkarni ,DevashreeDeshpande ,P.V.Mulmule Journal of Emerging Technologies and Innovative Research 2018
- [6]. Continuous User Identity Verification Using Biometric Traits for Secure Internet Services, Dr.SHAIK ADBUL MUZZER, 2GOSALA SUBHASIN
- [7]. Skincolor based Face detection Method, Devendra Singh Raghuvanshi,DheerajAgrawal
- [8]. Face Detection system based on retinal connected neural network (RCNN), Rowley, Baluja and Kanade
- [9]. Combining Skin Color based Classifiers and HAAR Feature using VJ Algorithm, N.Gobinathan, Abinaya and Geetha. P
- [10]. Face Detection and Recognition for Bank Transaction, Sudarshan Dumbre1 , Shamita Kulkarni2 , Devashree Deshpande3 , Prof P.V.Mulmule