Retinal scan authentication methodology for card payment in retail outlets

Varshni R R[1]
Student,AI&DS Dept.
Panimalar Engineering College, India
varshniramakrishnan19@gmail.com

Archanna T [2]
Student, AI&DS Dept.
Panimalar Engineering College, India
archanna2004@gmail.com

Thrisha K[3]
Student, AI&DS Dept
Panimalar Engg. College
thrishakrish76@gmail.com

.

Dr. P. Kavitha[4]
[4]Associate Professor
Panimalar Engineering College,India

Dr. S.Malathi[5]
[5]HOD,AI&DS Dept.
Panimalar Engineering College,India

ABSTRACT

Counterfeit cards and the theft of credit and debit card information pose the greatest danger to today's modern society. This leads to numerous security concerns. Biometric retina scan authentication mechanism can solve the above mentioned problem considering that a person's retina scan cannot be readily forged and all the information about the person's card remains highly confidential. It also facilitates card payment in merchant establishments. This paper proposes a detailed working of how the retina scan mechanism is used for card payment and the image processing technique is done by using CNN.

Keyword: Counterfeit cards, biometric, Retina scan, Convolutional Neural Network.

I. INTRODUCTION

The proliferation of cashless payments, which has risen in popularity in recent years, intends to drastically alter the country's financial landscape by transitioning from a cash-based to a cashless system using digital technology[1]. For ease and record maintenance, more and more individuals are shifting to digital alternatives. There are numerous alternative options for cashless payments, which comprises UPI applications,QR code scanning, debit or credit cards, and e-wallets.This paper focuses on the threats in card payments which mainly is pin code forgery and theft of card information.

This dilemma can be surmounted by biometric mechanisms. In this contemporary world the population as a whole has begun to switch to biometric authentication methods, which ensures protection, confidentiality, and ease of access. The development of viable, interoperable, and secure components for bolstering biometric authentication and user identification systems has been the target of extensive effort by the biometric industry over the course of the last decade[7].

The most secure biometric authentication technique is retina scan as it is 80 times more reliable than iris recognition and 20,000 times more secure than fingerprints. Retinal scan identification is only one of several friction-reducing strategies banks can deploy with the goal of improving productivity and accessibility for their client base. The biometric retinal-recognition software reduces theft by stopping hackers on the internet from pillaging card details like pin codes or passwords which in turn reduces counterfeit cards[9].

For identification purposes, the fingerprint and iris scan are linked to our Aadhaar card. We'll adopt the same methodology and link the retina scan to the appropriate bank card account. The submitted scans will be verified to the retinal scans taken during payment in merchant establishments to ensure authenticity. This can be achieved by using CNN algorithm[4][3].

II. LITERATURE SURVEY

1. The prospect of payment facilitated with the use of biometrics will soon become an actuality, and certain monetary institutions are currently piloting it in India in some capacity.There are now two primary kinds of biometric authorization systems, behavioral biometrics and non-behavioral

A. K. Visvam Devadoss et al. (eds.), *Proceedings of the 6th International Conference on Intelligent Computing (ICIC-6 2023)*, Advances in Computer Science Research 107,
https://doi.org/10.2991/978-94-6463-250-7_24

biometrics. The non-behavioral biometrics ranges from speech recognition, vein recognition, face recognition, iris and retinal scans, fingerprint recognition. The behavioral biometrics includes signature scan, keystroke, and gait.

2. The study of patterns in human behaviour that are geared towards being used for uniquely identifying and measuring purposes is known as behavioural biometrics. Keystroke dynamics, gait analysis, voice ID, mouse use patterns, signature analysis, and cognitive biometrics are a few instances of behavioral biometric verification strategies. Financial institutions, companies, government institutions, retail point of sale (POS), and an expanding number of other venues use behavioral biometrics for secure authentication.

3. Analysis of a person's physical traits, such as a face, fingerprint, palm, or iris, is known as physiological biometrics.These characteristics are typically fixed; as you become older, your vein patterns in your palms won't alter. In normal circumstances, your face's overall features and form won't change to an unrecognizably large extent.Then, you may identify, confirm, or validate that individual online using their physical characteristics. Using your face, for instance, to sign in to a financial website. Additional applications for physiological biometrics include facial recognition in surveillance cameras or physical access control.

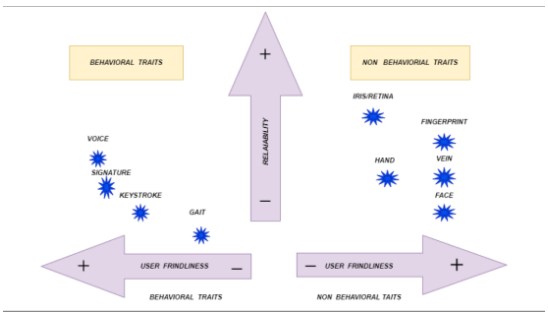

Fig 1. Comparison of behavioral and non-behavioral biometric modalities

4. A device that scans the retina at the back of your eyeball by peering beneath your iris is what is meant by the phrase "retinal scan." The scan provides security similar to a fingerprint, but since each person's retina is unique, it cannot be replicated[2]. The user looks into a small eyepiece for around 30 seconds while the scanner generates a low intensity beam of light to illuminate the back of the eye. The light is safe for the eyes, ophthalmologists and hospitals both use it to scan for diabetes and check for glaucoma, respectively. The scanned image of the retina can be processed using convolutional neural network algorithm [5][6].

5. Retinal scanners can be utilized to enable employees access to workstations or computers in offices with rigorous safety standards. The majority of specialists concur that retinal scanners do not present users with any health problems or other dangers. These devices scan the distinctive patterns of a person's retina to verify that the right people can access the restricted places or information[11].

6. Government offices, particularly the ones with high levels of security, are where retinal scanners are most frequently employed. A retinal scanner can be utilized to unlock a computer or other device, or at any location within an office. Employees must have images of their eyes for identification purposes while setting up retinal scans; while some people find the process painful, there are no known health hazards or problems[8].

7. Another kind of payment that will experience rapid growth in 2023 is contactless commerce. Customers may utilize contactless payment, as the term implies, by simply waving their smartphones across the reader. This sort of waving is much easier and faster than inserting a card.Due to the instantaneous transmission of the encrypted data to the point-of-sale device, contactless payments are also quicker and more secure than PIN technology[10]. A lot of enterprises currently offer methods of contactless payment, like Samsung Pay, Apple Pay, and Google Pay. All a customer needs to do to make payments is download the app, add a card by entering card information, and then wave their phone over any reader.

III. PROPOSED METHODOLOGY

The process starts with scanning each individual's retina and connecting or linking it to their specific bank card account just as how our fingerprints are linked to our Aadhar card. The posterior part of the eye has a thin tissue called the human retina, which is made up of neural cells. Retinal scans are a developing method of verification since each person's retina is distinct and depends on the intricate anatomy of the capillaries that supply it with blood.Even twins who are identical do not have a similar pattern in their retinal blood vessel network since it is not totally genetically determined.

The retina normally does not change from birth until death, despite the possibility of retinal patterns changing in situations of diabetes, glaucoma, or retinal degenerative illnesses.Due to its unique and unchanging nature, the retina appears to be the most precise and reliable biometric, aside from DNA.

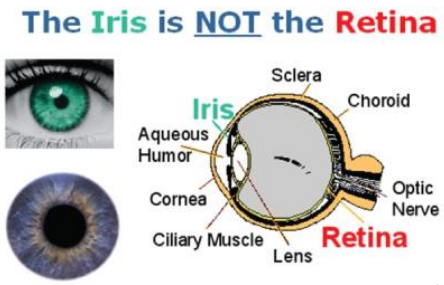

Fig 2. Layer at back of the eyeball

An invisible beam of low-energy infrared light penetrates into the customer's eye as they gaze through the scanner's eyepiece to perform a retinal scan. On the retina, this beam of light follows a predetermined course. The quantity of reflection fluctuates during the course of the scan because retinal blood vessels absorb light much quicker than the surrounding tissue. The variants' pattern has been digitally captured and is kept in a database.

Fig 3. Retina Scanner

A consumer is requested for a retinal scan as they are ready to pay for their purchases in retail outlets. The bank card accounts associated with that specific retinal image will be presented when the customer's retina is scanned, allowing them to choose any one of the accounts for payment.

Fig 4.Scanning of Retina for payment

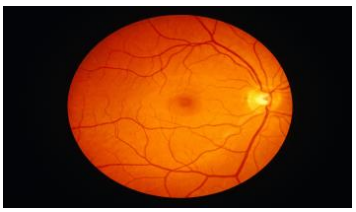

Fig 5. Scanned retinal image

The retinal picture scanned or recorded is compared to the retinal image database. The associated bank accounts for that specific retinal image won't be displayed until it has been validated. The CNN methodology is applied for this retinal image matching.

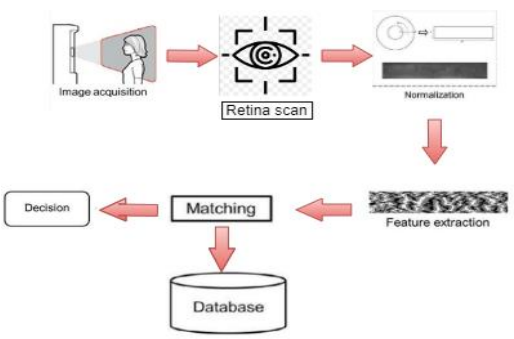

Fig 6. Architectural design for payment using retinal biometric authentication method

CNN:

An Artificial Neural Network (ANN) called a convolutional neural network (CNN) is specifically

created for processing data(pixels) and is employed for image identification .The image's pixels are fed to the neural network's input layer in the process's beginning phase as arrays. Feature Extraction is carried out by the hidden layers using a wide range of computations and operations. The process of feature extraction from an image is carried out by a number of hidden layers, including the convolution, the ReLU, and the pooling layer. There can be multiple convolutional layers and for each layer the pooling process is carried out.

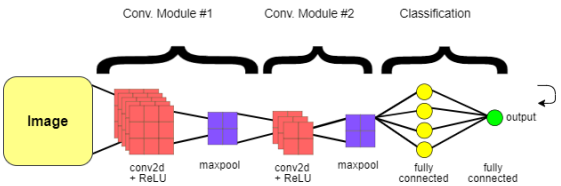

Fig 7. Image matching using CNN

IV. RESULT

In this proposed approach, the accuracy rate of the retinal scan biometric authentication technique is substantially greater than that of the fingerprint and face recognition biometric techniques. In the case of fingerprints,Simply obtaining finger imprints from objects that people touch can be used to create fake fingerprints. So the accuracy of fingerprint scanning is not up to the mark. Images of the authorised person can be exhibited, faked, and even plastic surgery can be performed in extreme cases when it comes to face recognition.Therefore, as compared to retina scan, face recognition is likewise a disadvantage. Due to its unique and unchanging nature, the retina appears to be the most precise and reliable biometric method. In order to prevent fraud, we frequently employ the retinal scan method for card purchases in retail establishments.

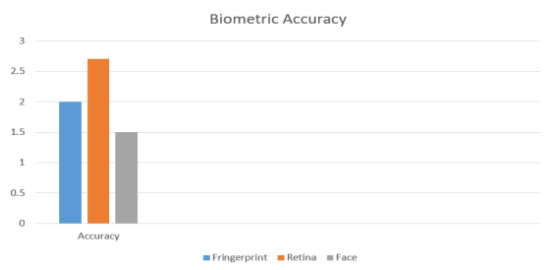

Fig 8. Accuracy rate of Biometric methods

Pin-based card payment methods or tap to pay are the two most common ways to pay in retail establishments. Our approach entails using a retinal scan because every single individual has a distinctive retinal pattern. Compared to other payment methods, the security of this retinal scan biometric payment technique is substantially higher. Retinal scanning is thought and is also observed to increase payment security and eliminate card fraud. The observations among these methods shows that payments using retina scan authentication mechanisms are more secure than the other existing methods. So this ensures that all the card information remains highly confidential and reduces counterfeit cards.

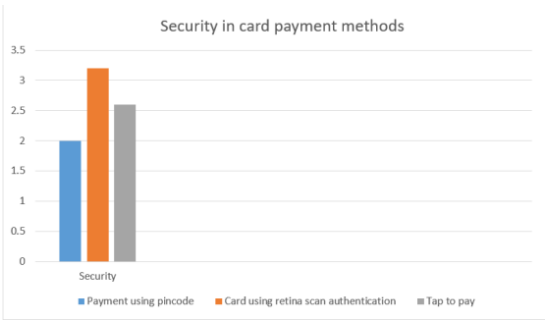

Fig 9. Security in card payment methods

V. CONCLUSION

Since your card information is not falsified and we use a biometric retina scan authentication strategy, this method makes card payments more secure and helps reduce the use of counterfeit cards. This authentication payment technique is more precise and reliable since it utilizes the Convolutional Neural Network algorithm, which is additionally employed to match retinal scan images.

VI. REFERENCES

[1] Yashvi Jain, Vipul Jain, Md. Rizwan Khan “Digital Payments”, published in “National Conference On Information Technology & Security Applications 2021 (NCITSA-2021)”,Volume XV, SPECIAL ISSUE, June 2021,ISSN 0973-2861

[2] Nazariy K. Shaydyuk and Timothy Cleland, MD, MSE,”Biometric Identification Via Retina Scanning With Liveness Detection Using Speckle Contrast Imaging”,Retina Biometrix, LLC, San Antonio, Texas

[3] G. MadhuMithra, G. Sasikala, A.Tharamaraiselvi,”RETINAL IMAGE CLASSIFICATION USING NEURAL NETWORK BASED ON A CNN METHODS”,International Research Journal of Engineering and Technology (IRJET) , Volume: 09 Issue: 07 | July 2022

[4] Srikar Appalaraju,Vineet Chaoji,”Image similarity using Deep CNN and Curriculum Learning “,Amazon Development Centre (India) Pvt. Ltd.

[5] Fahreddin Sadikoglu,Selin Uzelaltinbulat,"Biometric retina identification based on neural network",12th International Conference on Application of Fuzzy Systems and Soft Computing, ICAFS 2016, 29-30 August 2016, Vienna, Austria

[6] Md. Shafiul Azam,Humayan Kabir Rana,"Iris Recognition using Convolutional Neural Network",International Journal of Computer Applications (0975 – 8887) Volume 175– No. 12, August 2020

[7] Kindt, Els. "An Introduction into the Use of Biometric Technology."Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis. Vol. 12. Dordrecht: Springer, 2014. 15-85. Print. Law, Governance and Technology.

[8] Yoichi Seto, Retina Recognition (2009).

[9] Sichmid N. Retina Identification Biometric Systems; 2004.

[10] Ram Kumar Garg,NK Garg,"Developing Secured Biometric Payments Model Using Tokenization",2015 International Conference on Soft Computing Techniques and Implementations- (ICSCTI) Department of ECE, FET, MRIU, Faridabad, India, Oct 8-10, 2015

[11] Akram MU, Tariq A, Khan SA. Retinal recognition:Personal identification using blood vessels. 6th International Conference on Internet Technology and Secured Transactions.

Abu Dhabi: United Arab Emirates; 11-14 December 2011.