National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

Credit Card Reader with Face Recognition Based on Webcam and Multimodal Biometrics

Vismaye M, Harshitha Gowda, Keerthishree V, Nidhish VP

ISE, New Horizon College of Engineering, Bangalore, Karnataka, India

ABSTRACT

This paper is focused on proposing a method for transactions on a credit card with face recognition using a web cam. This system initiates transfers based on detection/recognition of the face that is linked with the card. Considering the security issues in detail, when the visa card is used for the transactions, we just scan it which can cause lot of security issues if stolen or misplaced. With face recognition it will become secure and safe, giving a two-step verification. Now considering multimodal biometrics, the paper focuses on face-iris multimodal biometrics. The iris recognition system is composed of segmentation, normalization, feature encoding, and matching. This is to be done to avoid the drawbacks that would occur with only face recognition.

I. INTRODUCTION

In the modern era every individual wants many different modes of payment. Businesses have increased gradually due to enormous payment methods, but how safe can they be? Statistics say that the cybercrimes like Credit card frauds have been increasing gradually over the past few years. It is still the most known cybercrime that is been happening and there is still no measure to control it. The Fundamental issues that every credit card user faces is that they do not have a secure online transaction procedure. The biggest risk that is faced is credit card fraud which can lead to heavy losses. Technology is being used in the wrong way, there are multiple ways where the same technology can be used to reduce the cybercrime(s).

CONCEPTS OF BIO METRICS

Biometrics can be characterized as estimations identified with body and computations identified with human qualities. Biometrics confirmation is utilized for recognizable proof and access control. Biometric identifiers are the unmistakable, quantifiable qualities. Biometric identifiers are frequently arranged as physiological versus social qualities. Physiological qualities are identified with the state of the body. A couple of models are unique mark, palm veins, face acknowledgment, palm print, iris acknowledgment, retina.

FACIAL RECOGNITION

A facial acknowledgment framework is an innovation fit for distinguishing and confirming a person. There are various techniques in which the facial acknowledgment innovation works, however all in all, they work by looking at chosen facial highlights from given picture with faces inside an information base. It is commonly utilized as access control in security frameworks and can be contrasted with different biometrics, for example, unique mark or eye iris acknowledgment frameworks.

IRIS RECOGNITION

The Iris Recognition system being a biometric identification system, uses mathematical patter In the modern era every individual wants many different modes of payment. Businesses have increased gradually due to enormous payment methods, but how safe can they be? Statistics say that the cybercrimes like Credit card frauds have been increasing gradually over the past few years. It is still the most known cybercrime that is been happening and there is still no measure to control it. The Fundamental issues that every credit card user faces is that they do not have a secure online transaction procedure. The biggest risk that is faced is credit card fraud which can lead to heavy losses. Technology is being used in the wrong way, there are multiple ways where the same technology can be used to reduce the cybercrime(s).

CONCEPTS OF BIO METRICS

Biometrics can be characterized as estimations identified with body and computations identified with human qualities. Biometrics confirmation is utilized for recognizable proof and access control.

Biometric identifiers are the unmistakable, quantifiable qualities. Biometric identifiers are frequently arranged as physiological versus social qualities. Physiological qualities are identified with the state of the body. A couple of models are unique mark, palm veins, face acknowledgment, palm print, iris acknowledgment, retina. Facial recognition

A facial acknowledgment framework is an innovation fit for distinguishing and confirming a person. There are various techniques in which the facial acknowledgment innovation works, however all in all, they work by looking at chosen facial highlights from given picture with faces inside an information base. It is commonly utilized as access control in security frameworks and can be contrasted with different biometrics, for example, unique mark or eye iris acknowledgment frameworks.

IRIS RECOGNITION

The Iris Recognition system being a biometric identification system, uses mathematical pattern-recognition techniques to recognize the data.

It uses video camera technology infrared illumination to acquire rich detailed images of the eye.

WHY IRIS RECOGNITION SYSTEM OVER FACIAL RECOGNITION SYSTEM?

There is no full proof biometrics system but the iris recognition is known to be one of the most secure and renowned for not being faked. There are a few disadvantages to a facial recognition system like, a facial recognition system needs light at all time to authenticate, it needs an accurate reference photograph, one of the major drawbacks was discovered when Apple co. had launched their flagship smart phone the Apple iPhone X. The security access methods to this phone are facial recognition and a pin/password. The drawback is that an identical twin or an identical person that is a person with similar facial features could access the data and the contents in the phone. Even though this is a very rare case such a variable need's to be considered when it relates to the subject of authentication of an individual. The iris individual has a different pattern. There are n- recognition techniques to recognize the data. It uses video camera technology infrared illumination to acquire rich detailed images of the eye.

II. PROPOSED METHOD

The proposed system provides a safe method for credit card transactions which will integrate two step verification system. The basic level of verifications

will be the OTP (one-time password) which will be valid only for a few mints, a second level of verification that can be added is the main subject of this paper that is a verification system using the bio metrics of the user.

One of the existing frameworks looks after the security making sure that there exists a secured payment procedure between the credit card and the holder and subsequently guarantees that card number stays obscure to some other substance. There exists another sort of framework that gives a recommendation, a recognition model to be accessible to catch the conceivable abnormal exchange.

MULTI MODAL BIOMETRICS

Technologists are centred around utilizing biometrics for validation as a safety effort. The expansion of biometrics (three-factor verification) can guarantee and secure the identity of the client. The favorable position for biometrics is that they can only with significant effort be duplicated as they are one of a kind to the client. On the opposite side, this sort of confirmation is less advantageous for shoppers as it for the most part requires a more extended time duty for the checkout cycle as the dealer is requiring an extra factor of verification.

FACIAL RECOGNITION

Advancement application that recognizes 80 nodal centers around the human face and contemplates these concentrations to a painstakingly set aside picture to confirm the character of a specific individual through model ID. Transcendence of modernized cameras on phones, PCs and work zones makes "pay by face" an accessible alternative. May require use of explicit camera foundation on devices; may anticipate that customers should pay additional charges and may raise some security stresses over the limit of facial pictures in information bases. Utilized in US-VISIT (United States Visitor and Immigrant Status Indicator Technology) to check the photographs of new wayfarers attempting to get segment to the United States against those submitted at the hour of visa issuance.

Figure 1: Facial Recognition

IRIS RECOGNITION

Iris Recognition Technology that analyses the subjective case of the iris to see and perceive a person. Image of the iris can be discovered using a standard camera and planning a person's iris with the set aside structure is significantly precise. The iris is difficult to channel from a decent way and can be obscured by eyelashes or eyelids. There can be inconvenience in scrutinizing the iris of people who have cascades or are outwardly debilitated. Iris affirmation is correct currently used for physical access control.

Figure 2 : Iris Recognition

III. METHODOLOGY

BIOMETRIC IRIS RECOGNITION

The process of iris recognition consists of 3 following steps

IMAGE CAPTURE

In this process the image of iris of the person will be captured. It must be ensured that iris is properly focused and image must be captured with clarity.

IRIS LOCATION AND IMAGE OPTIMIZATION

In this progression picture of the iris will be streamlined and iris limits and focal point of the understudy will be distinguished. Consequently, the region of the iris picture will be brake down which will help for include extraction. when the region which is utilized for include extraction is examined improvement of iris locale is finished by eliminating profound shadows and bits which are secured by eyelids. The iris locale which is enhanced will be standardized in a rectangular square and measurements will be fixed which will be contrasted and other filtered pictures of iris. We can't analyze the iris picture that is upgraded with put away iris pictures, the pictures that are put away in the biometric information base are called biometric layouts and this will contain the encoded organized highlights of iris which will be separated from the picture subsequent to applying Daugman's elastic sheet model. Matching and storage of biometric template. The biometric layout is to put away in biometric information base when the enlistment of the individual is done, on the off chance that the examined picture of iris utilized for validation, at that point the biometric format of the checked picture will be coordinated with biometric format which is put away in information base. Biometric face recognition.

HAAR CASCADE

Haar Cascade, algorithmic guideline is utilized to distinguish objects in an image or video. It's known for distinguishing countenances and parts of pictures. Haar Cascade is superimposing the positive pictures over an assortment of negative pictures. The learning is generally done on a worker and on different stages. Higher outcomes are acquired by exploitation of top quality pictures and expanding the amount of stages that the classifier is prepared. The algorithmic principle has four phases: Haar Feature Choice, making Integral pictures, Adaboost training, Cascading Classifiers. For the most part, 3 kinds of choices are utilized. The 2 rectangular choices are that the differentiation of the pixels at timespans rectangular areas. These locales have same structure and size and are on a level plane or vertically adjacent.3 rectangular alternatives are processed by taking the absolute of 2 external parallelograms at that point are eliminated with the complete in a really focus square shape. Further, inside the four square shapes highlights figures the differentiation between inclining sets of square shapes.

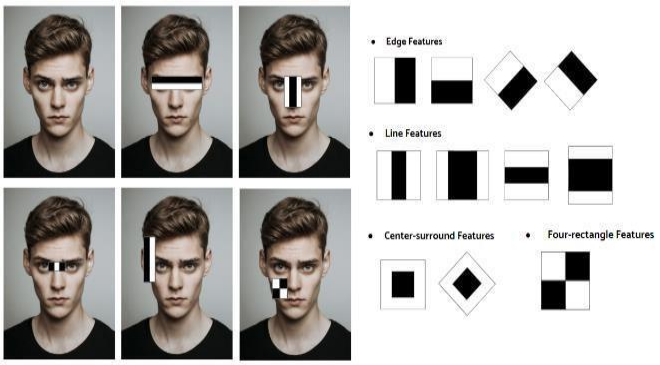

Figure 3: Haar Cascade Algorithm FACE RECOGNITION

Face detection refers to the psychological method by which an individual's face is scanned. Face Detection is the first and essential step for face recognition. It's required for object detection and might be used in several platforms like security, bio-metrics, enforcement, diversion, personal safety, etc. It's also used to observe faces in real time for police investigation. It's widely used in cameras to spot multiple appearances within the frame Example Mobile cameras and DSLR's. Firstly, an image of an individual's face is captured from a photograph or video. After that, identity verification package reads your facial features. Key factors of facial recognition embodies the space between your eyes as well as the distance between forehead and chin. The package identifies facial landmarks, one system identifies sixty-eight of them, which is the key to identify your face. Then your facial signature and a mathematical

formula is compared to an information of far formed faces. And at last a determination is created. Your face print dataset could match with a picture in the database.

GLCM

It stands for Gray-level Co-occurrence matrix. The GLCM perform portray the vibe of an image by calculative anyway for the most part matches of pel with explicit qualities and in an extremely indicated spatial relationship happen in a picturef (Δx , Δy) or (d, ɵ)., making a GLCM. A GLCM may be a matrix wherever the quantity of rows and columns is up to the quantity of grey levels, G, within the image. The framework segments P (I, j | Δx, Δy) is that the recurrence with that 2 pixels, isolated by a pel separation (Δx, Δy), happen at spans a given neighbourhood, one with force 'I' and furthermore the distinctive with power 'j'. The grid parts P (I, j | d, ɵ) contains the subsequent request applied mathematical probability esteems for changes between dim levels 'I' and 'j' at a chose dislodging separation d and at a chose edge (ɵ). Utilizing a sizeable measure of force levels G suggests putting away a lot of transitory data, for example a G × G grid for each blend of (Δx , Δy) or (d, ɵ).

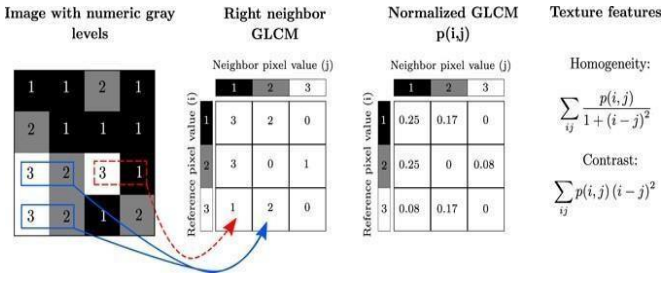

Figure 4 : GLCM Algorithm

HOW DOES IT WORK?

As per the proposed system this is a method in which the user of the credit card has a secure platform for transactions.

The working of the model will be as follows: While a customer registers in the bank for a credit card his/her biometrics (iris and facial features) has to be recorded. This set of database can be accessed only by an authorized electronic card machine with an IR scanner. The process will contain 2 steps of verification where in the first step the credit card holder will receive an otp or enter a pin for the basic level of verification. In the second level of verification the merchant will have to use a camera with IR Scanners to scan the iris and facial features of the individual to authenticate the transaction. In case of online transactions, the user can utilize the camera with an external IR scanner to authenticate his/her transactions.

ALGORITHM

1. Start
2. An individual's personal details must be entered.
3. An individual's face and iris is scanned.
4. After scanning the face for registration, form must be submitted.
5. Payment details must be entered.
6. The features is compared with the database.
7. If the results match, then the transaction becomes successful.
8. Stop

FLOWCHART

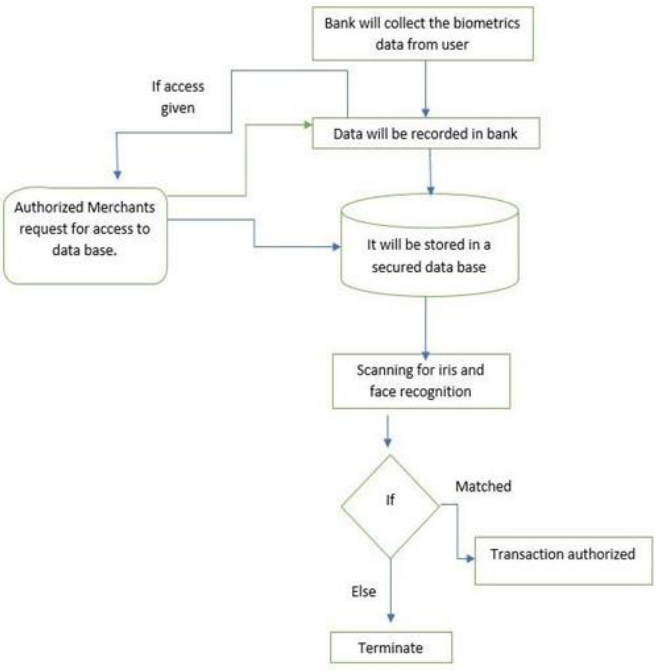

Figure 5 : Flowchart of the execution

III. RESULTS

The user registers in the bank with his biometrics which has to match while transaction is occurring to keep the transaction highly secured.

IV. CONCLUSION

If the above method is followed the user will have a safe and secured platform for transactions. Cyber frauds can be avoided and helps in high security of the credit card transaction system for each individual.

V. REFERENCES

[1]. Recognition https://www.sciencedirect.com/topics/computer-science/iris-recognition

[2]. Biometrics https://www.verifi.com/resources/understanding-biometrics-in-credit-card-security/

[3]. https://fidentity.com/blog/facial-recognition-vs-iris-scanning/

[4]. https://www.researchgate.net/publication/324953705_A_Robust_Multi-Biometric_System_with_Compact_Code_for_Iris_and_Face