International Journal of Research in Engineering, Science and Management
Volume 4, Issue 3, March 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

Facial Recognition Controlled Smart Banking

J. Jayanthan[1*], N. Kaviya Priya[2], S. Praveen Kumar[3], K. Sangeetha[4]
[1,2,3,4]*Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, India*

***Abstract*: Automated Teller Machines are widely used now-a-days by people. But It's hard to carry their ATM card everywhere, people may forget to have their ATM card or forget their PIN number. The ATM card may get damaged and users can have a situation where they can't get access to their money. In our proposal, use of biometrics for authentication instead of PIN and ATM card is encouraged. Here, The Face ID and Fingerprint are preferred to high priority, as the combination of these two biometrics proved to be the best among the identification and verification techniques. The fingerprint of the user is identified and face image is verified, and the appropriate user is given authentication. For the prototype of the system, Raspberry pi microcontroller is used.**

***Keywords*: Biometrics, Facial recognition, Biometric standards, Automatic teller machine technology, Fingerprint, Liquid crystal.**

1. Introduction

Biometrics is a field of technology which performs Recognition, Verification and Identification by behavioural and anatomical characteristics. Biometrics is the best solution as far as security authentication is considered. In proposed system, a combination of bio-metrics is proposed so that the FAR (False acceptance rate) and FRR (False rejection rate) can be reduced.

Recognition used in the description of biometric systems like facial recognition, finger print or iris recognition relating to their fundamental function, "Recognizing" as the biometric input is valid or not. The Recognition confirms the input is valid Fingerprint or Face or Iris. However, the recognition does not include verification.

Verification is the process where the biometric system attempts to confirm an individual's claimed identity by comparing the input to one or more previously enrolled data.

Identification is the process where the biometric system searches a database for a reference finding a match for the enrolled biometric data; a biometric data is collected and compared to all the templates in the database.

In ATM's such a concept could be used to replace the existing system will allow you to access your banking details. Secure authentication is what people need and Biometric is the solution for them, Since the biometrics are one hard thing to hard to replicate.

2. Existing System

Present ATM are good and easy to use for users, and the ATM machines which provide an interactive session while baking in ATM centre. The information displayed on the ATM machine which helps them to interact with the data and information through keypad or touch screen. However, the existing system needs an ATM card which is for the Recognition and Identification process, and It needs a PIN (Personal Identification number), which makes the system, a bit degrading. There can be situations where the user cannot get access to their ATM card, or there may be cases when users forgot their PIN number. In both the cases, the solution to recover from the situation is to apply for a new ATM card. The application of new ATM card, takes minimum of 5 business days to success. Until then, the user lose access to their money or they can go all the way back to Bank to take challan and fill-up to get their money. These all are tedious and time-consuming process. The PIN number which is a four-digit re-changeable number ranges from 0000-9999, which results in 10,000 combinations. Nowadays thermal cameras are easily available in the consumer market. Attackers use this technology to track the finger traces in the keypad finding the possible numbers. In a possible 10000 combinations, if the getting the correct PIN will be almost at 90 percent. Not only the infrared technology, Finger movements can be watched closely, Polythene covers, and much more stealing activities can be done by the attacker. Hence, we have to introduce a system which should be more reliable and hard to replicate the user identity. If that's the question, Biometrics will be the answer. One can question that silicone gel and polythene covers can also be used to steal fingerprint. But, the advancements in sensor field shows a huge development. Capacitive sensors can work only in a material which has the resistivity of skin, and the only material ever found is skin. Also combination of biometrics will hard to break, one cannot replicate every biometric ID.

Fig. 1. Existing system

*Corresponding author: jjayanth003@gmail.com

3. Proposed Plan

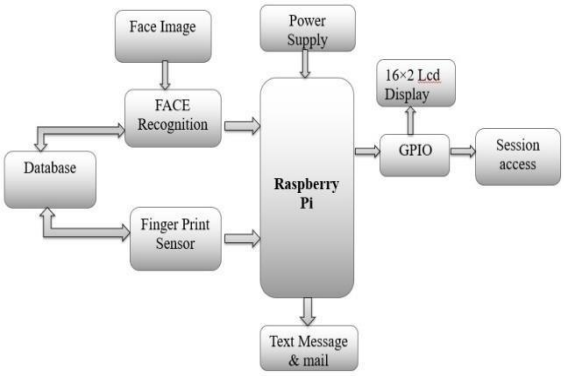

Fig. 2. Block diagram of the proposed plan

In this proposed system we have developed an additional way to access the account through face recognition and finger print. In this system, finger print and face image are used for authentication purpose. face image of person is compared with the database image and then followed by the recognition of fingerprint. When both the recognition schemes match with a same single individual, access for that account will be provided. Here Raspberry Pi microcontroller is used in the controlling part. The fingerprint scanner Id and face Id are searched in a database where the other details of the user account will be stored. The raspberry pi microcontroller performs the search operation in the database and send the necessary information to a display device. Open CV libraries are used for the process of recognition, verification and identification of face images. The fingerprint libraries are used for the above-mentioned process for fingerprints. The program for the process are coded in python.

4. Software and Hardware Specification

A. Raspberry pi

Fig. 3. Raspberry pi 3

The Raspberry Pi is a series of small single-board computers developed in the United Kingdom by the Raspberry Pi Foundation to promote the teaching of basic computer science in schools and in developing countries. The original model became far more popular than anticipated, selling outside its target market for uses such as robotics. It does not include peripherals (such as keyboards, mice and cases). However, some accessories have been included in several official and unofficial bundles. The Raspberry Pi Foundation recommends the use of Raspbian, a Debian-based Linux operating system. Other third-party operating systems available via the official website include Ubuntu MATE, Windows 10 IoT Core, RISC OS and specialized distributions for the Kody media center and classroom management Many other operating systems can also run on the Raspberry Pi.

B. Web Camera

A web camera is a device which helps to take pictures and video often used for video chatting and video and image capturing for authentication and verification process. In our prototype, the Logitech camera is used for this process. It is one of the cheapest yet a good web camera available in the market. Other cameras can also be used for face capturing. The Logitech camera supports 720p video recording and 5MP image capturing. 5MP image is more than enough for a good Face identification. The camera supports USB 2.0 serial communication, which is widely used. Hence there is no hardship while connecting this camera to the system. The driver software for the camera doesn't have to be separately downloaded. The universal driver available in every operating system will support the Logitech web camera. No additional driver installation is required for using Logitec camera. Additional power supply is required for the camera, as it consumes power from the USB slot itself.

Fig. 4. Webcam

C. Fingerprint Scanner

Fig. 5. Fingerprint scanner

Fingerprint sensor is the major part in the project. As fingerprint plays an important role in Identification, Yet Face recognition is also used to identify an individual. Consider a case involving twins, Face image gets collapsed due to the same face, there fingerprint ID helps to identify the account.

Now-a-days gesture identification are also used to differentiate people with similar faces, Yet Fingerprint is more reliable then gesture identification. It is impossible for two persons to have the same fingerprint since the fingerprints are generated based on different factors. The Victorian scientist Francis Galton published a book on the forensic science of fingerprints and claimed that the chance of two people has same fingerprint is almost impossible, that the probability numbers to 1/64 million. The fingerprint cannot be destroyed until the finger is destroyed. Even a cut or bruise in fingerprint, after healing forms back in same fingerprint as before.

5. Technology

A. Serial Communication Protocol

Serial communication protocol is one of the finest available protocols for digital transmission of data. Here the digital data is transferred serially. As the processors involved in modern age can provide higher MIPS (Million instructions per second), hence the one problem with serial communication is eliminated. Serial communication makes the system compact since it needs a very limited pin from GPIO. IN general, The Serial communication protocol can be seen in a 10-bit arrangement, with starting bit 0 and end bit as 1.

B. Image Processing

Digital image processing is the use of computer algorithms to perform image processing on digital images. As a subcategory or field of digital signal processing, digital image processing has many advantages over analog image processing. It allows a much wider range of algorithms to be applied to the input data and can avoid problems such as the buildup of noise and signal distortion during processing. Since images are defined over two dimensions (perhaps more) digital image processing may be modeled in the form of multidimensional systems.

C. Computer Vision

Computer vision is a sub-field of Digital Image processing, consists of different sets of algorithms to extract input from environment through image processing. In our project, The Face identification used which is also a subset of computer vision. Face identification can be done via many software tools, such as MATLAB, OpenCV etc. Yet OpenCV is the best tool to use, since it is completely an open source tool and provides a lot of readily available modules. The OpenCV modules are used in the project via python libraries, which are available in OpenCV website. The OpenCV is not only available for face recognition, as its name indicates, it is for Computer vision. And it may be one of the strongest building tools for Artificial intelligence

D. Python (programming language)

Python is a high-level programming language for general-purpose programming. The language is highly dynamic as it consists of an interpreter in place of compiler. The design of the language which highly improves the readability and the syntax of control statements which makes the programming and developing easy. That makes python a very powerful language and most commonly used language.

The language as said, it is very dynamic supporting automated memory management which is very helpful in real time object-oriented programs. There are many standard libraries are available for python. The fingerprint libraries and Fingerprint identification and Face identification.

6. Conclusion

The combination of Biometrics will always result in is still growing. The other new Biometric such as Iris pigmentation, and behavioral characteristics of a person, when combined with growing field of artificial intelligence high security. The Face and Fingerprint ID as combined. Now-a-days they are used in military bases and government sectors for secure authentication, and their application, they provide a very advanced authentication technology.

References

[1] J. J. Patoliya, M. M. Desai, "Face Detection based ATM Security System using Embedded Linux Platform ", 2nd International Conference for Convergence in Technology (I2CT), 2017.

[2] M. Karovaliya, S. Karedia, S. Oza, D. R. Kalbande, "Enhanced security for ATM machine with OTP and Facial recognition features", International Conference on Advanced Computing Tech- nologies and Applications (ICACTA), 2015.

[3] Sivakumar T, G. Askok, K. S. Venuprathap, "Design and Implementation of Security Based ATM theft Monitoring system", International Journal of Engineering Inventions, Volume 3, Issue 1, 2013.

[4] C. Bhosale, P. Dere, C. Jadhav, "ATM security using face and fingerprint recognition".

[5] Manoj V, M. Sankar R, Sasipriya S, U. Devi E, Devika T, "Multi Authentication ATM Theft Prevention Using iBeacon", International Research Journal of Engineering and Technology.

[6] L. Wang, H. Ji, Y. Shi, "Face recognition using maximum local fisher discriminant analysis",18th IEEE International Conference on Image Processing, 2011.

[7] K. Shailaja and B. Anuradha, "Effective Face Recognition using Deep Learning based Linear Classification," IEEE International Conference on Computational Intelligence and Computing Research, 2016.