International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

FINGERPRINT AND IRIS BIOMETRIC CONTROLLED SMART BANKING MACHINE EMBEDDED WITH GSM TECHNOLOGY FOR OTP

M.HARINE [1], K.V.PADMAVATHI[2], MR. L.VINOTH KUMAR[3]

[1]26, First cross street, Ragavendra nagar, Ponmeni, Madurai – 625016.
[2]30, Lal Bagadhur Sasthri street, Thirunagar, Madurai – 625006.
[3]Assistant Professor, Dept. of Electrical and Electronics Engineering, Velammal College of Engineering and Technology, Tamil Nadu, India.

Abstract - *Biometrics technology is rapidly progressing and offers attractive opportunities and inventions. In recent years, biometric identification has grown in popularity as a way of private identification in ATM authentication systems. Biometric authentication system is reliable, economical, save time, and has more advantage compare to other like visa cards. The user suspects their password may be stolen or attack by thief then the user changes their password when they expect the password attack by the thief. In order to solve this kind of problem we design biometric authentication system, because biometrics is the science of using human measurements to identify people. Biometric is selective because It has unique characteristics that is no one shares and remain the same over time. In this project, a microcontroller-based prototype of ATM cashbox access system using fingerprint sensor and Iris recognition module is implemented. An Arduino microcontroller developed by Microchip Technology is used in the system. This research, which can increase the speed of money withdrawal almost 3 times fast; could have positive impact on the customer's satisfaction. If proper functioning is ensured by the banks. The necessary software is written in Embedded 'C' and the system is test.*

Key Words: Biometric, Fingerprint, Iris authencation, Card less transactions, GSM technology.

1. INTRODUCTION

Nowadays the interest towards different systems of biometric identification among users of computer systems has grown up. Spheres of use of technologies of identification aren't bounded. Government and personal organizations have an interest in technologies of fingerprint because it allows for increase within the level of protection of secret

and tip. Companies that deal within the sphere of data technologies have an interest in technologies of fingerprints, face, voice, iris recognition so as to see penetration of out of doors people to their net. Payment processing has long been the weakest link within the transaction processing cycle of a typical online business. Despite the advancement in technologies for Ecommerce applications, payment related activities have been the sources of major breach and security concerns. As fraud continues to extend per annum, many financial institutions are trying to find possible solutions to the present problem. Among those new technologies for handling payment processing, biometric payment technology has recently attracted more and more attention as a viable solution to decrease fraud and cheats. The performance of iris recognition systems highly depends on segmentation [1]. In a bid to address issues of safety of customers' funds and avoiding losses through compromise of Personal Identification Numbers (PIN), the apex bank, Central Bank of Nigeria (CBN) is to introduce Biometric authentication of Point of Sale (PoS) and Automated Teller Machines (ATMs) by 2015 [2]. The apex bank had taken an enormous step to realize the arrogance of ATM consumers following the circular enforcing migration from Magstripe sort of open-end credit to chip and Pin (EMV compliance) type of debit card. The main causes of those problems are thanks to the defects in existing security systems. Digital security has acquired special importance thanks to vast amount of digital information and therefore the high value that's frequently been attached thereto. Normally we use passwords for security. Effective user authentication applications are crucial to guard information security. In response to the growing number of threats to data security, a good sort of authentication mechanisms is developed. Here we introduce a new security system which uses finger iris recognition system for authentication in ATM networks.

2. THEORIES PROPOSED

In this proposed model, no ATM card is needed for transaction, so for security purpose, the IRIS is a promising biometric pattern for personal identification in terms of its security and convenience. The iris pattern can only be taken from a live body. Therefore, it is a natural and convincing proof that the subject whose iris is successfully captured is alive. If the person iris and finger print both matches the ATM transaction done successfully if doesn't matches means the atm door automatically closed and emergency message send to police and customer.

2.1 Hardware Requirement

Microcontroller, Alarm, GSM, Serial Communication, Motor, Finger print sensor.

2.2 Software Requirement

MATLAB 13, Arduino IDE, Embedded "C".

3. IMPLEMENTATION ON IRIS RECOGNITION

Iris recognition is done by following modules, 1. Image Acquisition 2. Iris Segmentation 3. Feature Extraction 4. Recognition.

3.1 Image Acquisition

Image acquisition in image processing are often broadly defined because the action of retrieving a picture from some source, usually a hardware-based source, so it are often skilled whatever processes need to occur afterward. Performing image acquisition in image processing is usually the primary step within the workflow sequence because, without a picture, no processing is feasible. The image that's acquired is totally unprocessed and is that the results of whatever hardware was wont to generate it, which may be vital in some fields to have a consistent baseline from which to work. Test iris images are acquired from gallery.

3.2 Iris Segmentation

Next, a segmentation algorithm is employed, which might localize the iris region from an eye fixed image and isolate eyelid, eyelash and reflection areas. Automatic segmentation is achieved using the circular Hough transform for localizing the iris and pupil regions, and the linear Hough transform for localizing occluding eyelids. Thresholding is also employed for isolating eyelashes and reflections. Third, the segmented iris region is normalized to eliminate dimensional inconsistencies between iris regions. This is achieved by the method of implementing a version of Daugman's rubber sheet model, where the iris is modelled as a flexible rubber sheet, which is unwrapped into a rectangular block with constant polar dimensions.

3.3 Iris Segmentation

Third, detection of interest points in iris and find strongest features in iris via Harris Spatio temporal corner detector and SURF feature descriptor. Finally mean feature calculated from HSTCP and SURF.

3.4 Recognition

This is the last stage for iris recognition. In that, machine learning models such as SVM and KNN classifiers are used for iris recognition.

3.5 GSM Modem

The GSM (Global System for Mobile) / GPRS (General Packet Radio Service) TTL-Modem is SIM900 Quad-band GSM /GPRS device, which works on frequencies 850 MHZ, 900 MHZ, 1800 MHZ and 1900 MHZ. It is very compact in size and easy to use as connect GSM Modem. The Modem is meant with 3V3 and 5VDC TTL interfacing circuitry, which allows User to directly interface with 5V Microcontrollers (PIC, AVR, Arduino, 8051, etc.) also as 3V3 Microcontrollers (ARM, ARM Cortex XX, etc.). The baud are often configurable from 9600-115200 bps through AT(Attention) commands. This GSM/GPRS TTL Modem has internal TCP/IP stack to enable User to attach with internet through GPRS feature. It is suitable for SMS also as DATA transfer application in mobile to mobile interface.

3.6 Features

The Quad Band GSM/GPRS: 850 / 900 / 1800 / 1900 MHz , inbuilt SIM (Subscriber Identity Module) Card holder , Built in Network Status LED , Inbuilt Powerful TCP/ IP (Transfer Control Protocol / Internet Protocol) stack for internet data transfer through the GPRS (General Packet Radio Service) , Audio Interface Connectors chip (Audio in and Audio out) , Most Status and Controlling pins are available , The Normal Operation Temperature: -20 °C to +55 °C , Input Voltage: 5Vto 12VDC , LDB9 connector (Serial Port) provided for straightforward interfacing.

4. OUTPUT RESULT

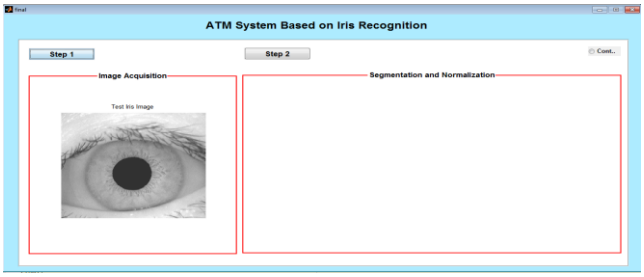

Fig -1: Image Acquisition

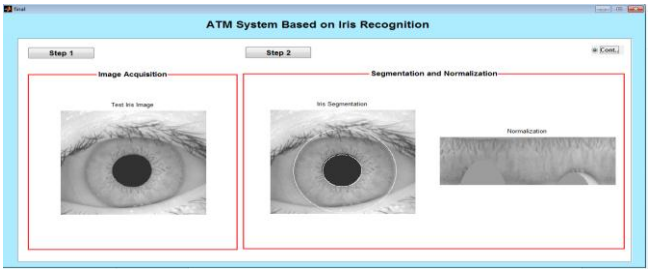

Fig -2: Segmentation and Normalization

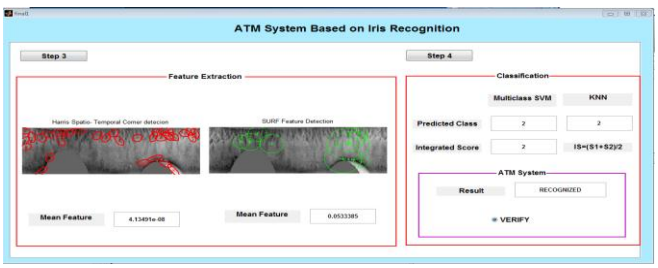

Fig -3: Result

5. CONCLUSION

This project is developed over the basis about more need of safety of ATM banking system. Now-aday's ATM is getting much less secure along emerging methods to hack/crack ATM PIN then ATM card. This type of ATM prototype are often efficiently used with fingerprint recognition. Since, password protection isn't bypassed in our system, the fingerprint recognition done after it yielded fast response and is found to be of ease to be used. Fingerprint images can't be recreated from templates; hence nobody can misuse the system. The security options were increased for the foremost part for the steadiness and dependableness of owner recognition. The whole system was built on the technology of embedded system that creates the system additional safe, reliable and easy to use. The same hardware platform is often used with IRIS scanner to place forward another potential biometric security to the ATMs.

REFERENCES

[1] K. Jain, S. Pankanti, S. Prabhakar, H. Lin, and A. Ross, "Biometrics: a grand challenge", Proceedings of the 17th International Conference on Pattern Recognition (ICPR), vol. 2, pp. 935-942, 2004.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] P. Corcoran and A. Cucos, "Techniques for securing multimedia content in consumer electronic appliances using biometric signatures," IEEE Transactions on Consumer Electronics, vol 51, no. 2, pp. 545- 551, May 2005.

[3] P. J. Phillips, A. Martin C. L. Wilson and M. Przybocki, "An Introduction to Evaluating Biometric Systems," IEEE Computer, Vol.33, No.2, Feb. 2000, pp. 56-63.

[4] S. Pankanti, R. M. Bolle and A. Jain, "Biometrics: The Future of Identification," IEEE Computer, Vol.33, No.2, Feb. 2000, pp. 46-49.

[5] H. Lee, S. Lee, T. Kim, and HyokyungBahn, "Secure user identification for consumer electronics devices," IEEE Transactions on Consumer Electronics, vol.54, no.4, pp.1798- 1802, Nov. 2008.

[6] Wang, J. Li, and G. Memik, "User identification based on finger vein patterns for consumer electronics devices", IEEE Transactions on Consumer Electronics, vol. 56, no. 2, pp. 799- 804, 2010.

[7] Mulyono and S. J. Horng, "A study of finger vein biometric for personal identification", Proceedings of the International Symposium Biometrics and Security Technologies, pp. 134- 141, 2008.

[8] Y. G. Dai and B. N. Huang, "A method for capturing the fingervein image using non uniform intensity infrared light", Image and Signal Processing, vol.4, pp.27-30, 2008.