SMART ATM SECURITY USING FACE AND IRIS RECOGNITION TECHNOLOGY

Patrick O. Anierobi[1] and Akpu Ifeanyi K[2].
[1,2] Department of Electrical/Electronic Engineering, Federal Polytechnic Oko, Anambra State.
Patrick.anierobi@federalpolyoko.edu.ng and derealcelestino4sure@gmail.com

Abstract:

Today's everyone makes used of ATM system for their easier money transaction, withdrawal, deposit. This system enhances the security of banking sector and protects consumers from fraud. ATM system is mainly used to take money at any time. There is an urgent need to improve the security of the banking sector for money usage. Though using this method there is so issue on withdrawal of money. We know the PIN anybody can use the card. So that's the issue on today's world. We introduce face and iris recognition to scanning both the card pin and the through face of the original card holder using 2D dimension.

Keywords: ATM system, 2D Techniques, Acquisition, and IRIS Recognition.

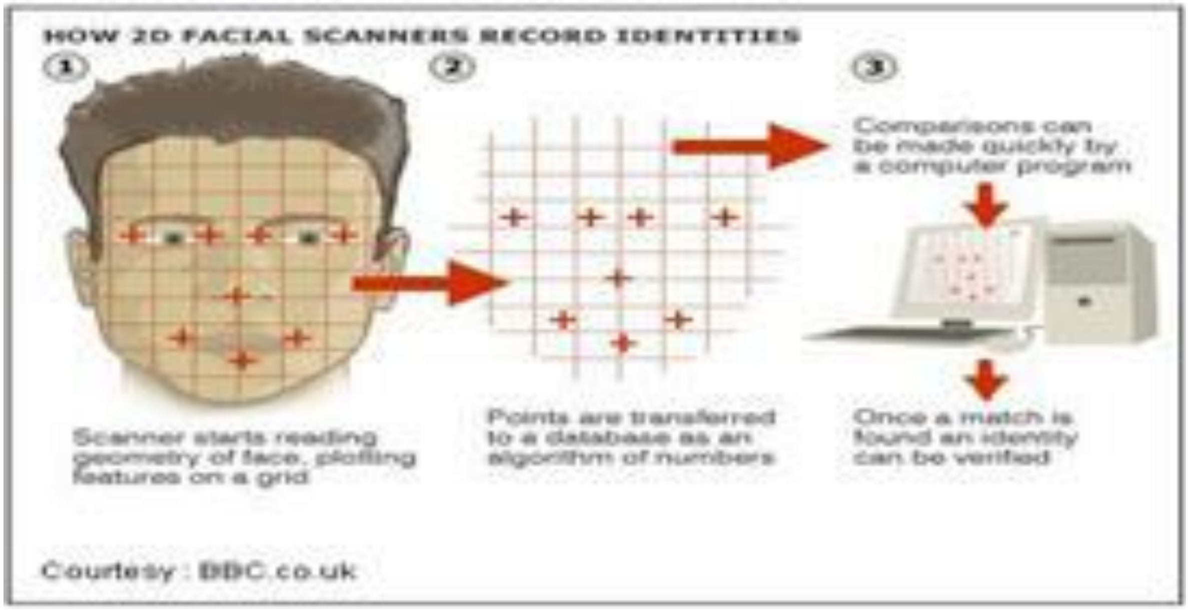
I. INTRODUCTION

Nowadays, banking sector is one of the most important parts of human's daily life. Banking facilities are widely used by people for their economy's activities (Darwin et.al, 2020). In figure 1 below shown an Automated Teller Machine is an electronic telecommunications device that enables the customers of a financial institution to perform financial transactions in bank, particularly cash withdrawal, money transfer, online remittances, and utility bill payments etc. without the need for a human cashier, clerk or bank teller (Sonakshi et.al, 2017).

Figure 1: ATM Machine systems (Arunkumar et.al, 2018).

It is observed that the number of crimes related to ATM is increased hence there is a necessity to provide enhances security to ATM machine. Due to increase in the ATM thefts, which uses a magnetic card and pin number to allow a transaction, are not enough to keep the customer safe from fraud, identity-loss and false transactions. This is where the face Recognition technology comes as a relief to the ailment of the public (Ross and Jain, 2003). This technique used Face and Iris Recognition Technology involves the method of allowing a transaction, only if the identity of the individual is verified and the verification is done by recognizing the iris pattern which include (shape of eyes, nose chin and mouth) of the account holder (Renuka et.al., 2020)

In this paper, iris scans camera is uses ATM to prevent loss due to counterfeit attempts to prevent security such as ATM card theft, PIN theft, customer account information theft and hacking from been have access to the account holder because the faces are seen as 2D dimension the front view of a face and side view of your face as shown in figure 2 below.


HOW 2D FACIAL SCANNERS RECORD IDENTITIES
1
2
3
Comparisons can be made quickly by a computer program
Scanner starts reading geometry of face, plotting features on a grid
Points are transferred to a database as an algorithm of numbers
Once a match is found an identity can be verified

Courtesy : BBC.co.uk

Figure 2: 2Diminsion of digital image is captured for detecting the faces (Bone et al., 2001).

II. RELATED WORKS

According to Guru (2017), developed an ATM security system to monitor all ATM's in the city with a centralized private server. Many types of sensors and switches are used here to capture security related information which is then analyzed and dispatched to the central main server to experiment. Utilizing the data obtained from different ATMs, a statistical vulnerability test is made out through the system and a vulnerability quotient is assigned to all ATM machines. Whereas this method is little complicated and continue monitoring is needed.

According to Sweta et.al, (2016), the proposed system focuses on saving time and solving sensitivity issue of the system. If the user wants to know their balance there is no need to go through the verification system. This model claims that fraudsters will never gain any positivity of the system. Hence, the security will never be compromised.

In paper (Akhilesh et.al 2016), to increase the safety of electronic money transfer via EDC an embedded fingerprint technique with PIN has been introduced. It's a design to secure swipe card transaction by applying bio-metric feature like fingerprint identification with traditional PIN. There are many proposals to raise the safety of the transaction using bio-metric recognition system (Renee and Gomathi (2015). In this given model pin number is completely replaced with bio-metric system such as e-fingerprint, retina and so on. Thus, this serves as an entirely different model from others. The computer operated machine which allows withdrawing the cash from their respective bank account is called as Automated Teller Machine (ATM). During the transaction of money, the card owner has to provide required information for effective transaction which is supported through keypad and card reader. Through the magnetic stripe of the credit or debit card the card reader collects the account related data of the card owner when the person presses the keypad.

Besides, the card owner has their PIN (personal identification number) which is converted into the encrypted form and delivered to the host processor which is responsible for routing the request to the concerned bank. From customer's checking account an electronic fund transfer (EFT) process is taken place to host processor's account based upon cash request. Whenever the host's bank account receives the transferred fund it sends the ATM an approval code to dispense the amount and simultaneously cash is also transferred to the bank account. During swiping the card information is sent to the bank payment system. Each and every data is sent to the payment processor for processing and the data which is processed is further sent to the payment brand and finally it is forwarded to the issuing bank. After verification process an authorized number is generated and routed to the concerned brand to perform payment. As a final process the authorization number is routed to the merchant's payment system from the processor. This is the overall process carried out and after this process the card holder collects his/her receipt. But this has the disadvantage that anyone can enter the ATM center by using any others card and may withdrawal money if they know the PIN of the card.

III. PROPOSED METHODOLOGY

In this proposed system, the valid card holder is allowed and only by the knowledge of account holder others can enter into the ATM by using account holder's ATM card. Once the customer inserts the card inside the ATM machine the card reader collects the information stored in the magnetic strip of the card and then passes into the host for comparing the fingerprint and image of the person which is already updated in form of data. This can be performed with the help of iris camera and finger print module. If everything is matched then ATM machine will allow for transaction. Incase if any unauthorized person inserts ATM card, finger print and image will be verified since it won't match so their image along with an One-Time passwords (OTP) will be sent the randomly generated 6-digit code to the registered mobile number of the corresponding account holders mail, only after entering that OTP in this system it will allow the user to withdrawal the money or else it will stop the process.

IV. IRIS RECOGNITION

Iris recognition is the process of recognizing a person by analyzing the random pattern of iris as show in figure 4 below. The iris is a muscle within the eye that regulates the amount of light entering the eye by controlling the size of pupil .The system is to be composed of a number of sub-systems, which corresponds to every stage of iris recognition technique. The stages involved in iris recognition are as follow: Image Acquisition is the process of acquiring high quality eye image using Cmos camera as shown in figure 3 below. Segmentation is a process of locating the iris region in a digital eye image, Normalization is a process in creation of a dimensionally consistent representation of the iris region. Encoding is the process of generation of the iris code (Sonakshi et.al, 2017). Database Enrollment is the process of storing up of all the iris patterns of the users, Matching is the process of matching the iris of the present user with the database stored. Iris Recognition- It is the last process in the iris biometric technique When the iris of the user is matched with the iris stored in the database, then the system gives a signal in text form saying that iris is been recognized and the user can access further steps and can finally make a transaction.

Figure 3. CMOS Camera (Sonakshi et.al, 2017).

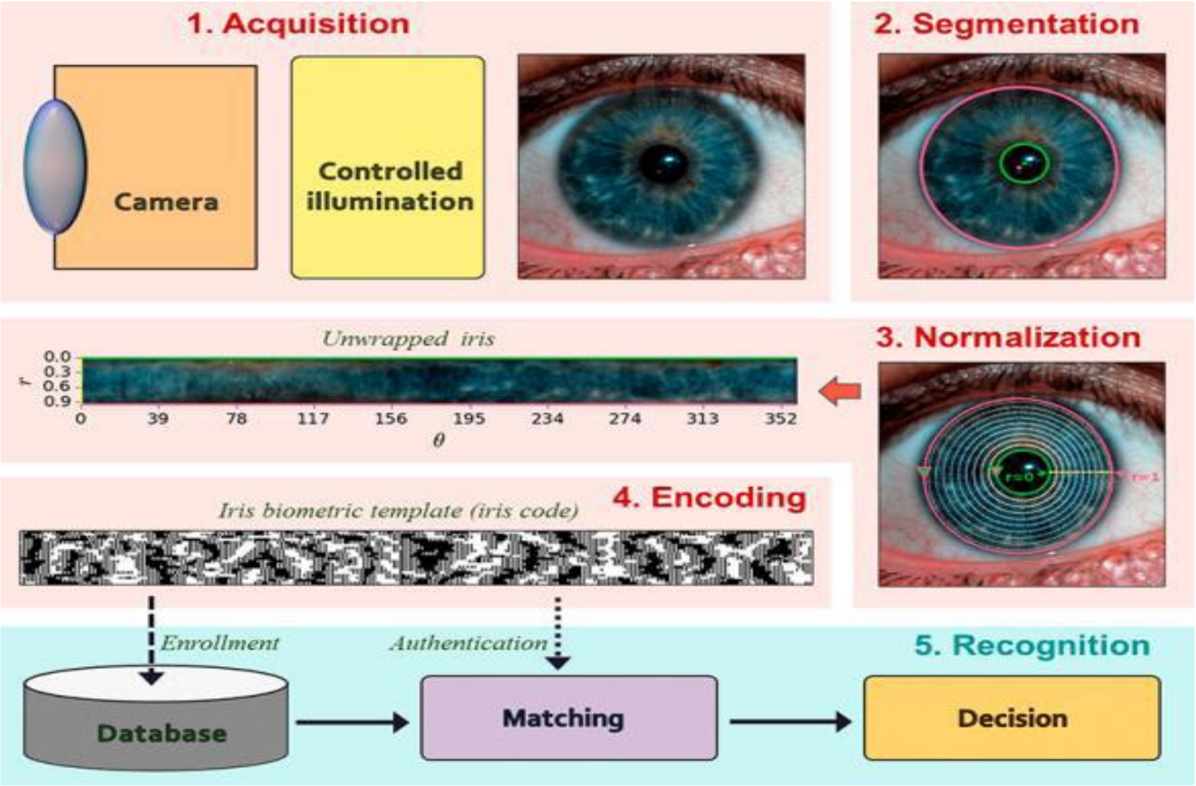


Figure 4. Iris Recognition process (Sonakshi et.al, 2017).

V. CONCLUSION

Face and Iris recognition has proven to be the most secure method of all biometric systems to a point it is widely used in high level security. If this system is used at this level it should show how much technology has changed in order to make this method effective in processes of identification and verification. The biometric ATM system is highly secure as it provides authentication with the information. This system has some disadvantages which can't be a major risk but it has to be considered. Fingerprint won't work when it is wet or wounded.

REFERENCE

Arunkumar V, Vasanth K.V, Naveenly king K, and Aravindan T (2018) "ATM Security Using Face Recognition" India Technical Research Organization Volume-5, pp. 59-62

Darwin N, Suresh T., Nivedha T., Priyadharshini G., and Mugilan P., (2020) "Smart ATM Security Using Face Recognition" European Journal of Molecular & Clinical Medicine Volume 7, pp.1349-1354

Sonakshi B., Vasudha S. and Niteeka K. (2017) "ATM Security using Iris Recognition Technology and RFID" International Journal of Engineering Science and Computing, (IJESC) Volume 7, pp.11486-11488.

Renuka P., Maheshwari R. and Rekha S. (2020) “ATM Security Using Face Recognition” International Journal of Engineering Technology Research & Management Vol.4, pp.1-3

Guru Sarath T., (2017) “Centralized Server Based ATM Security System with Statistical Vulnerability Prediction Capability,” IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), pp.61-66.

Sweta Singh, Akhilesh Singh, and Rakesh Kumar, (2016) “A Constraint based Biometric Scheme on ATM and Swiping Machine,” International Conference on Computational Techniques in Information and Communication Technologies.

Akhilesh Singh, Sweta Singh, and Rakesh Kumar (2016),” Secure Swipe Machine with Help of Biometric Security,” International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp.1056-1061.

Renee Jebaline G., and Gomathi S. (2015), “A Novel Method to Enhance the Security of ATM using Biometrics,” International Conference on Circuit, Power and Computing Technologies [ICCPCT].