International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 25 Issue 5 – APRIL 2018 (SPECIAL ISSUE).

SIXTH SENSE IMAGE PROCESSING ATM USING COLOR RECOGNITION AND GESTURE RECOGNITION

Venmathi.A.R. [#1], S.Jayasakthi[*2],P.Malathi[*3],S.Jasmine[*4]and K.Kalaiselvi[*5]

[#1]*Associate Professor, Department of ECE, Kings Engineering College, Chennai,India*

[*2,3,4,5]UG Student, Department of ECE, KingsEngineering College, Chennai,India

***Abstract*- ATM security has always been one of the most prominent issues concerning the daily users and the frequent ones as well. While commercial banks and postal savings to deposit and draw conveniently and praised by the users but dispute cases and financial crimes about it are increasing day by day. This paper emphasizes on the hypothetical, yet very possible scenario of an individual's ATM machine security with a low but efficient cost hardware system. Our proposed system uses certain factors which would be monitored right from the initial to the end of the respective transaction. The proposed sixth sense ATM which uses no touching of any object but by just using your gesture interface it us do the normal operation of authentication system. Also it uses high alert security for reducing or eliminating ATM thefts.**

***Key Words*- Vibration Sensor, Temperature sensor, Infra red sensor, GSM Technique, Buzzer, Kiel Tool**

I. INTRODUCTION

Secure cash transaction is of serious concern in growing use of cash cards and internet transactions. The main objective of this project is to create a new generation of ATM machine in which transaction can be made without ATM cards and contact on the machine. Because in existing system the user should carry the ATM card without fail and they should touch the screen to operate the machine. Biometrics is biological authentications, based on some physical characteristics of the human body. The list of biometric authentication technologies is still growing. There are two categories of biometric identifiers include physiological and behavioral characteristics. Physiological characteristics are related to the shape of the body, and include but are not limited to: fingerprint, face recognition, DNA, palm print, hand geometry, iris recognition (which has largely replaced retina). Behavioral characteristics are related to the behavior of a person, including but not limited to: typing rhythm, gait, digital signature, some gestures and voice. More traditional means of access control include token-based identification systems, such as driver's license or passport, and knowledge-based identification systems, such as password or Personal Identification Number (PIN) [3]. This paper will introduce the concept of physical browsing and development of a system that will allow users to use their gestures with different colors to securely withdraw cash from ATM machines. The paper presents the new generation of ATM machine for M-Cash withdrawal application, relevant technologies and security issues. By using this system malfunctions can be avoided and the transaction will be much secured. In modern digital world autonomous systems are growing in a rapid way. According to the Indian government instruction in 2020 the plan is to convert every transaction and communications into digital. Therefore social computerization and automation has been increased and ATM (Automated Teller Machine) has been spread out throughout the country to simplify the financial activities. With the help of these activities the manual banking procedures are simplified and credit cards has been installed. Since the financial organizations are increased in proportion the crimes also exponentially increased. The statistics of year 2017 for crimes on ATM are nearing 95%.It is because of the external ATMs and is always exposed to crime. Therefore an efficient solution is needed to solve the problems and GSM is the ultimate target. Mr. Wang et al. Expresses his view providing finger print for more security now a days we are moving towards a new powerful, intelligent, auto rated system, which will give us easy to do the work smoothly, Thus systems are not dependent on human support [1]. Mr. Aru et al. explains Today's ATM systems which is use pin &

access card for identity verification. The recent advance in biometric identification techniques, retina scanning, including fingerprinting, and facial recognition has made a great effort to rescue the unsafe situation at the ATM. This research investigated the development of a scheme that integrates finger gestures without contact into the verification process used in ATMs. The development of such a scheme would help society to protect clients & financial institutions alike from intruders and identity thieves. This paper concentrates on an ATM security system that would combine a security ATM mode and Contactless ATM mode. Nevertheless, it's obvious that, this proposal will go a long way to solve the problem of Account safety making and disease preventing.

*1.1 ATM (Automated Teller Machine***)**

The first ATM machine was installed by Korean exchange bank in 1975. The social network operation of ATM is installed in 1982 by Korea financial telecommunications. In the year 2000 ATM has been increased and in 2015 almost all the National and International banks are linked through network globally. The rapid grow in ATM bring forth the external ATM. In the beginning the protection for ATM machine is controlled with the help of detecting sensors and alarm technique to the control centers. Since it is a human oriented control the safety measures cannot be given properly. Therefore, GSM Technology with addition of some more components above which is to suggest in this study is installed in the ATM.

1.2 *GSM (Global System for Mobile Communication)*

The GSM is one of the leading wireless networks which have low-power, low-cost and convenience to use Global System for Mobile Communications is the most popular standard for mobile telephony systems in the world. GSM is used by over 1.5 billion people across the world more than 212 countries apply the application. It can be adopted through a GSM modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. When a GSM modem is connected to a computer, this allows the computer to use the GSM modem to communicate over the mobile network. While these GSM modems are most frequently used to provide mobile internet connectivity, many of them can also be used for sending and receiving SMS and MMS messages. A GSM modem also can be a dedicated modem device with a serial, USB or Bluetooth connection. In the system we will be using a GSM Modem to send and receive SMS. When the robbery occurs, it will send the message to corresponding banks and near police station (PS) according to the controller response.

II. EXISTING BANKING ATM SYSTEM IN INDIA

Figure1. ATM system in India

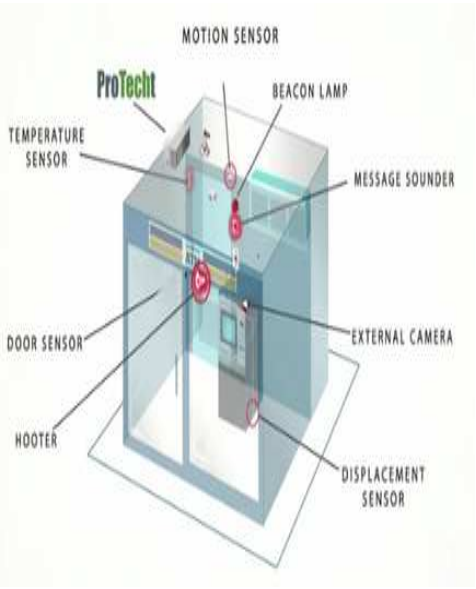
There is no doubt that rapid development of banking technology has changed the way in dealing with banking activities. One of the examples is automatic teller machine (ATM). Using ATM, a customer is able to conduct several banking activities such as cash withdrawal, money transfer, paying phone and electricity bills beyond official hours and physical interaction with bank staff. In short, ATM provides customers a quick and convenient way to access their bank accounts and to conduct financial transactions. Password or personal identification number (PIN) is one of important aspects in ATM security system which is commonly used to secure and protect financial information of customers from unauthorized access.

The system compares the code against a stored list of authorized passwords and users. PIN typically in a form of four digit combination of numbers that entered through ATM panel. If the code is legitimate, the system allows access at the security level approved for the owner of the account. In general, PIN is sufficient to protect against fraud and effectively eliminating most common attempts to gain unauthorized access. The four digits PIN is also easy to memorize and can be typed quickly with few errors and is quite difficult to be cracked if it is managed properly. The most recent cases show that the thefts have used sophisticated cracking programs to steal ATM holders money very easily, some people who live in today's high tech society which are bombarded everyday by so many numbers such as social security number, computer password, credit card number and so on. Sometimes they are confusing, difficult to be recalled immediately which of course can lead to a serious problem. Sometimes it is written down on small piece of paper or on ATM card in order to anticipate such event. The strength of PIN as a security system is weakened since the likelihood of the code leaking to other people increased. PINs are 4-digit numbers in the range 0000-9999 resulting in 10,000 possible numbers, so that an attacker would need to guess an average of 5000 times to get the correct PIN.‖ Biometrics is a rapidly evolving technology that is being widely used in forensics, such as criminal identification and prison security, and that has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. There has been a growing use of Radio Frequency Identification Tags (RFID) in different business environments. A typical example includes supermarkets, airline industry and the majority of supply chains. The main advantage of RFID to businesses is being the effectiveness of identifying System that transmits the identity (in the form of a unique serial number) of an object wirelessly, using radio waves.

III. SECURITY CONSIDERATION

The Secure M-Application deals with information transfer and financial transactions. Hence, the security elements considered during the design and implementation stage consist of making sure that the RFID and NFC used are in compliance with the ISO 14443 standards. WLAN technologies are equipped with the latest encryption protocol Standard. WEP and WPA address these issues by providing password protection for access control and encryption for privacy. The wireless security protocol 802.11w which is to be introduced in April 2008 has promised to provide facilities that will prevent denial of service attacks and make use of the AES encryption standards. These protocols (WEP and WPA), only deal with access control and privacy issues. That is determining who is allowed to enter your network and hiding information from hackers who may try to intercept information during transmission. However because the Secure M-application is more susceptible to security threats, the design incorporates other security measures such as making use of Biometric data, as a further authentication layer. It can utilize any of the fourteen different types of biometrics that fall within two categories namely: those that measure behavior and those that measure physical traits.

Any of the Biometric information within these types can be used in identifying users, by making use of individual anatomy or physiology, that is either deeply ingrained into the skin, or other behavioral characteristics, or it can be a combination of the two. Hence, the data will be used as a unique personal attribute for security and authentication purposes. Since the focus of this paper is not on analyzing biometrics as a means of authentication, details on the use of biometric can be found in and using biometric data to generated encryption and decryption keys. Both authentication factors are needed to match the stored once before allowing access to transactions else authentication will be automatically denied. This process will be able to reduce the effects of brute force attack, as millions of combinations need to be tried before gaining access and as only 3 tries are allowed this should prevent such attacks from occurring. Also it is important to point out that a single sign-on process will improve the reliability of identity management and access control. Having this application as the security measure, the Secure M-Cash Withdrawal will be able to provide an excellent wireless identity management that will remove the current risk of identity theft and meet the required security standard of implementing the secure M- cash withdrawal and other M-applications



IV. PROPOSED SYSTEM

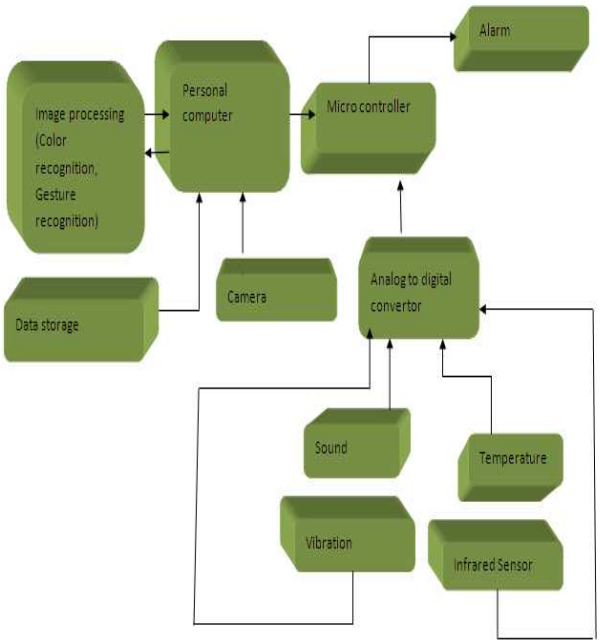


Figure2.1 (a) proposed system machine
Figure2.1 (b) Block Diagram of Contactless ATM mode

The proposed system which uses Mat Lab, KEIL U version 2.0 with Embedded C language uses the useful factors that can eliminate the unwanted spreading diseases because ATM machine serves as best device in transmitting diseases. Also it is visible that the ATM security system has a great flaw nowadays. The existing system has touched based transactions. And the total security is in the hands of security personnel who reside near the ATM machine. With this system tracking of PIN numbers and also the communicable diseases through touch and contacts are high. The securities near the ATM machine are also not the well trained and equipped military persons. Therefore theft and other major issues are the most possible demerits of the existing ATM.

In order to ensure the security of the bank property and to have hurdle free transactions this system proposes a color based non contact or sixth sense technology ATM for transactions. This system is very much useful as well as it improves the security of guarding ATM and the person using the ATM. The system is divided into two modes for the operating system.

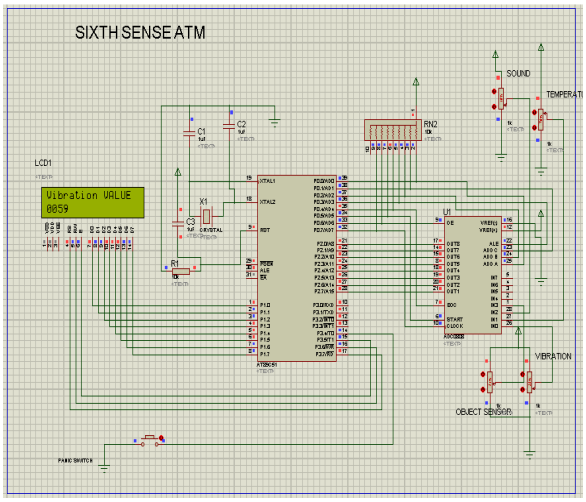
4.1 Contactless ATM mode

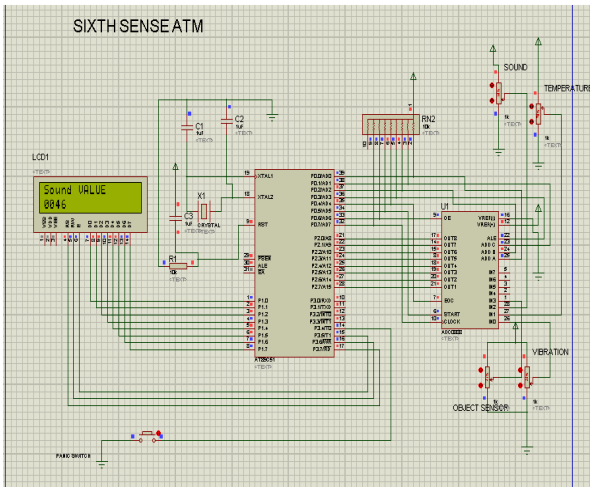
The sixth sense technology uses color bands to do all the transactions which are done by pressing the keys in an ATM machine. A Mat lab interfaced with Webcam is used for serving as contactless mouse for this purpose. This interface does all the transactions which can do using a mouse. This arrangement can solve the problem one identified by touching the ATM machine.

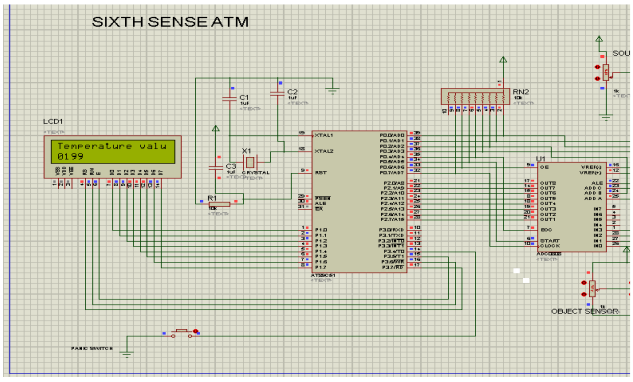
4.2 Security ATM mode

This system elaborates for finding the entry and exit of persons in an ATM counter. The time a person spends in an ATM chamber is noted and if it goes beyond a certain limit an alarm is generated which makes the security personnel to navigate the situation. The model also has a infrared sensor which will start up the main camera and record the face of the cardholder when he starts the transaction. By this process each and every transaction is stored in the data base along with the image of the person who is doing the transaction. The various sensor used in the system ensures the safety of the ATM machine. The temperature sensor connected with the ATM machine registers the temperature. If the temperature increases in the camper of ATM machinery there may be possibilities for unwanted activities like welding and damaging the machine may increase the temperature which can be captured by the temperature sensor. This avoids the ATM machine being cracked by using a heat source. Additionally with this a XYZ accelerometer is connected with the machine to find whether the machine is shaking to fond the possibilities of theft. This also is generating an alarm to save the ATM machine. The sound sensor gives alarm if there is any unwanted sound found in the ATM chamber. This avoids the cases like Bangalore ATM mishap.

V. RESULTS AND DISCUSSION







VI. CONCLUSION

Automatic Teller Machines have become a mature technology which provides financial services to an increasing segment of the population in many countries. Biometrics, and in particular fingerprint scanning, continues to gain acceptance as a reliable form of securing access through identification and verification processes. This paper identifies a high level model for the modification of existing ATM systems using both security mode and contactless ATM mode. It also uses face recognition module which is stride in the data base. The prototype of the developed application has been found promising on the account of its sensitivity to the recognition of the temperature, sound, and vibration by using various sensors. This system when fully deployed will definitely reduce the rate of fraudulent activities on the ATM machines such that only the registered owner of a card access to the bank account.

VII REFERENCES

[1] Lauri Pohjanheimo, Heikki Keränen and Heikki Ailisto,—Implementing TouchMe Paradigm with a Mobile Phone , ACM International Conference P, T., Cluitmans, L., Ailisto, H. and Seppä, H. -A user Interaction paradigm for physical browsing and near-object control based on tags: in Proc. Physical Interaction Workshop on Real World User Interfaces, (2003), proceeding Series; Vol. 121.

[2] Keränen, H., Pohjanheimo, L., Ailisto, H. (2005) Tag Manager: a Mobile Phone Platform for Physica
Selection Services in International conference on Pervasive Services (ICPS 2005). Santorini, Greece.
Pp-405-412.

M. Johns and G. Marsden —Mobile Interaction Design|, Wiley and Sons Ltd 2006, pg s178-182.

[3] Openwave Phone Simulator European ATM Security Team, —European ATM SecurityTeam|,Debold, incorporated 2006.

[4] A. Jain, R. Bolle, and S. Pankati, -Biometrics: personal identification in networked society, Kluwer Academic Publishers, 1998.

[5] J. Chirillo and S. Blaul, -Implementing Biometric Security, Wiley & Sons, 2003.

[6] S. Hoque, M.C. Fairhurst, F. Deravi, W.G.J. Howells,-On the Feasibility of Generating Biometric Encryption Keys IEE Electronics Letters, 41(6), 309-311, 2005.

[7] Mr. John Mashurano1, Mr. Wang liqiang2, "ATM Systems Authentication Based On Fingerprint Using ARM Cortex-M3" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 3, March - 2013 ISSN: 2278-0181 1 www.ijert.org IJERTIJERT

[8] Aru, Okereke Eze, Ihekweaba Gozie "Facial Verification Technology for Use In ATM Transactions "American Journal of Engineering Research (AJER)e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-02, Issue-05, pp-188-193 www.ajer.us.

[9] Laudon Kenneth, Traver Carol Guercio, E-Commerce (2005), Second Edition , pp. 237-239, Pearson Education (Singapore), Pvt. Ltd.

[10] Ibidapo, O. Akinyemi, Zaccheous O. Omogbadegun, and Olufemi M. Oyelami, "Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-Banking System" International Journal of Electrical & Computer Sciences IJECS-IJENS Vol:10 No:06

[11] M. Subha and S. Vanithaasri "A study on authenticated admittance of ATM clients using biometrics based cryptosystem" International Journal of Advances in Engineering & Technology, Sept 2012. ©IJAET ISSN: 2231-1963Vol. 4, Issue 2, pp. 456-463.

[12] Lasisi, H.; Ajisafe, A.A., "Development of stripe biometric based fingerprint authentications systems in Automated Teller Machines," Advances in Computational Tools for Engineering Applications (ACTEA), 2012 2nd International Conference on , vol., no., pp.172,175, 12-15 Dec. 2012 doi: 10.1109/ICTEA.2012.6462860.

[13] Patiyoot, D.; Shepherd, S.J., "Security issues for wireless ATM network," Universal Personal Communications, 1998. ICUP'98. IEEE 1998 International Conference on, vol.2, no., 5-9 Oct 1998 doi: 10.1109/ICUPC.1998.733713.

[14] Bharath E, Dhananjaya K M, Anoop C.N, Raghavendra B V "Automated Teller Machine (ATM) Banking a User friendly"ISSN : 2230-9519 (Online) | ISSN : 2231-2463 (Print) IJMBS Vol. 2, Issue 4, Oct - Dec 2012.

[15] Jain, A.K.; Ross, A.; Prabhakar, S., "An introduction to biometric recognition," Circuits and Systems for Video Technology, IEEE Transactions on, Vol. 14, no. 1, pp. 4,20, Jan. 2004 doi:10.1109/TCSVT.2003.818349.