International Journal of Engineering and Techniques - Volume 3 Issue 2, Mar – Apr 2017

RESEARCH ARTICLE OPEN ACCESS

Smart ATM Center With Bring Along Mechanism for Card and Cash Retrieval after Transaction

[1]Swathika. M,[2]Sundari. I,[3]Vanmathi. R,[4]Parthiban.S.

[1,2,3]Final year student,

[4]Assistant professor,

Department of Electronics and Communication Engineering,

V.R.S. College of Engineering and Technology, Arasur.

Abstract:

This paper describes an ATM with a currency dispenser includes a contactless card reader. The contactless card reader can read data from an RFID tag of a customer's ATM card. The contactless card reader, such as an RFID tag reader, can be located so as to provide additional space for another transaction component. The contactless card reader can also be used in conjunction with a magnetic stripe card reader. The ATM includes a housing for the RFID tag reader that is adapted to prevent interception of radio signals. The ATM is able to prevent the missing of the ATM card and dispensed money by the customer inside the ATM centre after the transaction..

Keywords — *IR Sensor. RFID Card Reader. PIC Microcontroller*

I. INTRODUCTION

Banks seek to reduce their infrastructure costs by shifting transactions of their customers to Automatic Teller Machines (ATMs) and Internet websites. Financial users especially prefer ATMs for physical transactions, like cash withdrawal or cash deposit. For these reasons, user experience at the ATM is a very important concern for the banks.

One of the issues that ATMs suffer from is card and/or cash forgetting (CCF), which is a surprisingly common situation. In CCF, the user forgets the card or cash after the transaction, and leaves the system. After a certain waiting period, these items will be swallowed by the ATM, and the user has to go through a tedious and costly process to retrieve the card/cash or have the card reissued. Moreover, the cash is stored in a separate container after CCF, and needs to be manually checked before it is returned to circulation. This means a lot of time and money is being wasted to cope with the consequences of CCF. in the order of tens of thousands, and the extra cost of CCF amounts to several millions of USD per year for a single country [4]. The cost caused by the CCF issues can be reduced by allowing ATMs to re-identify customers which are returning back to the ATM to collect their forgotten item. This requires that the retraction of the items should be delayed, and the next customer is monitored and checked to be a returning customer or not. In this paper we describe how an ATM can adopt this behavior with the help of a camera-based system.

In [5], as soon as a customer inserts the card into the ATM and a session is initiated, the system starts face and body appearance detection using the camera located near the ATM and builds a temporary identity database for the customer. If the customer leaves the ATM without taking his/her card or cash, the ATM waits for the customer to be back, instead of retracting the forgotten item. If the system finds out there is a different customer approaching the ATM, the item is retracted instantly. The main difficulties in our scenario are the uncontrolled and low quality real world images coming from the attached ATM camera (especially the facial images of the returning card holder or another approaching customer).

In the proposed system The IR sensors will sense its surroundings. The motor used at the door will automatically close the door automatically when the customer enters the ATM center. When the customer retrieves the money and the door will open. If the customer forget to take the card or the money the door will remain closed. In some cases such as money transaction failure the ATM centre door will remain closed. In this scenario the customer can press the buzzer, to call the ATM center safety guard, to open the door. At that time the alarm will be switched on and it gives a beep sound, the security guard will arrive and open the door.

The remainder of this paper is organized as follows. Section 2 provides an overview of the related work. Section 3 introduces the overall system design, Section 4 presents the experiments and evaluates the system performance. Finally, Section 5 concludes the paper.

II. SYSTEM DESIGN

To design a highly secured ATM center with the restriction to take along the ATM card and the dispensed money with them after the transaction without forgetting them using RFID door lock and opening system.

Highly sophisticated electronic IR sensors are fixed to the door, cash dispenser and card swiping machine. The IR sensors will sense its surroundings. The motor used at the door will automatically close the door automatically when the customer enters the ATM center. When the customer retrieves the money and the door will open. If the customer forget to take the card or the money the door will remain closed. In some cases such as money transaction failure the ATM centre door will remain closed. In this scenario the customer can press the buzzer, to call the ATM center safety guard, to open the door. At that time the alarm will be switched on and it gives a beep sound, the security guard will arrive and open the door.

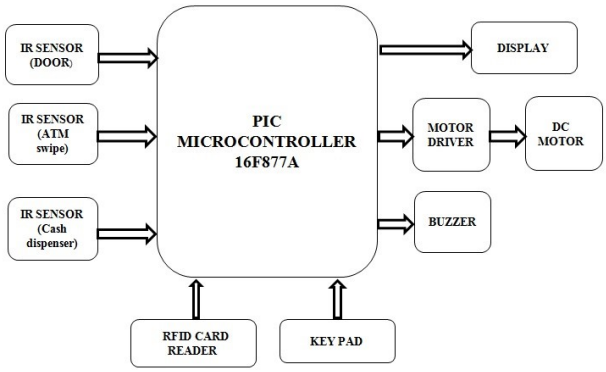


Figure 1. Block diagram of the working system

It consists of three highly sophisticated electronic IR sensors attached to the door, cash dispenser and card for ATM swipe machin. That will sense its surroundings up to 8cm. The RFID card reader is used for automatic identification and data capture. The motor is used for door that will close the door automatically.

III.RELATED WORK

Since our focus is on the application related requirements of the authentication scenario, we do not describe related work in face authentication from video. While the face modality has been studied widely for biometric purposes, it is relatively less considered for ATM-based usage. The main difficulty is that ATMs are typically placed outdoor, and operate under widely changing illumination conditions.

Babaei et al. presented a concept of using face recognition for ATM users together with other biometric features like fingerprint, iris recognition and hand/finger geometry [1]. However, they did not provide any specific method for an actual ATM user scenario. Aru et al. proposed an ATM security model that would combine a physical access card, a PIN, and face recognition to increase the reliability of ATM transactions [2]. Peter et al. presented a face verification based method to improve ATM security [3]. In their proposed system, face verification is performed on the still images of the ATM user, and compared with images of a gallery to make a decision. However, this approach depends on a pre-generated gallery, which typically involves images acquired a long time before the actual use, and under different illumination conditions.

In [4], Derman et al. proposed an approach for actual CCF scenarios for frontal face images captured by an embedded ATM camera. Their work was the first framework to focus on the CCF scenario, but used only a single biometric, namely the face, for authentication. Due to difficult illumination conditions in the field, the facial image by itself produced poor results. In this work, we operate in a similar application scenario, but use profile facial images instead frontal faces, and we also propose fusing face and body appearance verification results. Since our scenario requires the initial acquisition and re-identification to happen within a very short period (within 1 minute at most), the illumination conditions are mostly stable, but not uniform or controlled.

In [5] Guney Kayım, Ekberjan Derman, In their proposed a multimodal authentication system that operates under the constraints imposed by this applications scenario, and implement face recognition and color based body appearance recognition to create a system that improves ATM behavior in case of forgotten card or cash by re-identifying the user from an embedded ATM camera. We focus on the scenario and the platform, and report tests with the proposed system under challenging conditions,obtained from ATMs placed in the field.

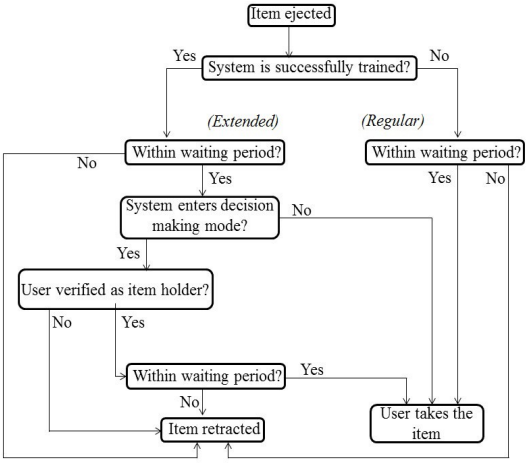


Figure 2. Algorithm for operation of the system

IV.EXPERIMENTS

A. IR SENSORS:

Infrared technology addresses a wide variety of wireless applications. The main areas are sensing and remote controls. In the electromagnetic spectrum, the infrared portion is divided into three regions: near infrared region, mid infrared region and far infrared region.

The basic concept of an Infrared Sensor which is used as Obstacle detector is to transmit an infrared signal, this infrared signal bounces from the surface of an object and the signal is received at the infrared receiver.

For optical sensing and optical communication, photo optics technologies are used in the near infrared region as the light is less complex than RF when implemented as a source of signal. Optical wireless communication is done with IR data transmission for short range applications.

An infrared sensor emits and/or detects infrared radiation to sense its surroundings.

The working of any Infrared sensor is governed by three laws: Planck's Radiation law, Stephen – Boltzmann law and Wien's Displacement law.

- Near infrared region — 700 nm to 1400 nm — IR sensors, fiber optic.
- Mid infrared region — 1400 nm to 3000 nm — Heat sensing.
- Far infrared region — 3000 nm to 1 mm — Thermal imaging.

Figure 3. IR sensors placements

B. PIC MICROCONTROLLER:

It has high-performance RISC CPU. Only 35 single word instructions. All single cycle instructions except for program branches which are two cycle. Operating speed: DC-20 MHz clock input DC-200 ns and instruction cycle Up to 8 K x 14 words of FLASH Program Memory Up to 368 x 8 bytes of Data Memory (RAM). Up to 256 x 8 bytes of EEPROM data memory Interrupt capability (up to 14 sources). Eight level deep hardware stack.

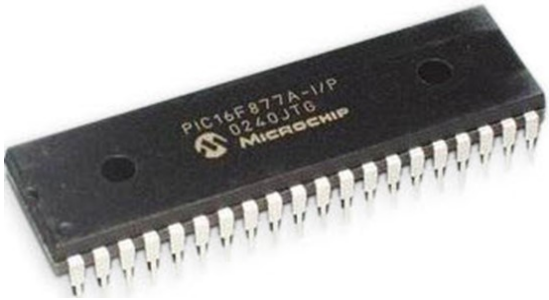


Figure 4. PIC microcontroller

C. RFID CARD READER:

It uses electromagnetic fields to automatically identify and tracks tags attached to objects. The tags contain electronically stored information. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source such as a battery and may operate at hundreds of meters from the RFID reader. Unlike a barcode, the tag need not be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method for automatic identification and data capture.

RFID tags are used in many industries, for example, an RFID tag attached to an automobile during production can be used to track its progress through the assembly line; RFID-tagged pharmaceuticals can be tracked through warehouse; and implanting RFID microchips in livestock and pets allows positive identification of animals.

Since RFID tags can be attached to cash, clothing, and possessions, or implanted in animals and people, the possibility of reading personally-linked information without consent has raised serious privacy concerns.

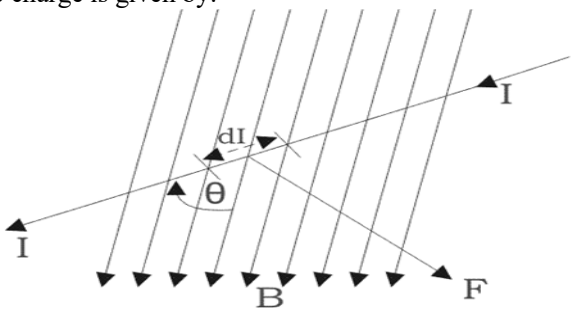
These concerns resulted in standard specifications development addressing privacy and security issues.

Figure 5. RF ID Card reader

D.DC MOTOR:

A DC motor in simple words is a device that converts direct current(electrical energy) into mechanical energy. It's of vital importance for the industry today, and is equally important for engineers to look into the working principle of DC motor in details that has been discussed in this article. In order to understand the operating principle of DC motor we need to first look into its constructional features.

For clear understanding the principle of DC motor we have to determine the magnitude of the force, by considering the diagram below. We know that when an infinitely small charge dq is made to flow at a velocity 'v' under the influence of an electric field E, and a magnetic field B, then the Lorentz Force dF experienced by the charge is given by:-



$$dF = dq(E + vB)$$

Figure 6. Lorentz Force dF

A.*BUZZER:*

A buzzer or beeper is a signaling device, usually electronic, typically used in automobiles, household appliances such as a microwave oven, or game shows.

V. CONCLUSION

In this work, we proposed a computer vision based ATM user identification framework using face and appearance verification to reduce card and cash retraction. We evaluated the proposed system under various conditions, and with our own database, based on a real scenario. The experimental results reveal that our proposed system is promising for mitigating the card/cash forgetting issue.

Our "Out-of-Session" test condition is the one that is closest to the expected real world application. It is more important in this application to keep a high true positive rate (convenience) as the impostors cannot be expected to mimic the actual users in CCF. Any improvement in the true positive rate directly translates to money saved for the banking institution, and the worst case (zero true positive rate) corresponds to what the current ATM systems have. For future work, we plan to improve the image resolution and quality to decrease the negative effects of motion blur while keeping within the computational limits imposed by the ATM system. Moreover, other challenging cases such as multiple faces appearing in the scene are potential research directions. Fusing information from the ATM camera itself is potentially useful, but in practice, ATM brands have different camera placements.

REFERENCES

[1] H. R. Babaei, O. Molalapata and A. A. Pandor, Face Recognition Application for Automatic Teller Machines (ATM), in ICIKM, 3rd ed. vol.45, pp.211-216, 2012.

[2] Aru, O. Eze and I. Gozie, Facial Verification Technology for Use in ATM Transactions, in American Journal of Engineering Research (AJER), [Online] 2013, pp. 188-193, Available: http://www.ajer.org/papers/v2(5)/Y02501880193.pdf

[3] K. J. Peter, G. Nagarajan, G. G. S. Glory, V. V. S. Devi, S. Arguman and K. S. Kannan, Improving ATM Security via Face Recognition, in ICECT, Kanyakumari, 2011, vol.6, pp.373-376.

[4] E. Derman, Y. K. Gec¸ici and A. A. Salah, Short Term Face Recognition for Automatic Teller Machine (ATM) Users, in ICECCO 2013, Istanbul, Turkey, pp.111-114.

[5] A. Ross and A. Jain, Information Fusion in Biometrics, in Pattern Recognition Letters, vol.24, pp.2115-2125, 2003.

[6] T. Ahonen, B. Hadid and M. Pietikainen, Face Description with Local Binary Patterns: Application to Face Recognition, in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, pp. 2037-2041, Dec. 2006.

[7] T. Ojala, M. Pietikainen and D. Harwood, A Comparative Study of Texture Measures with Classification Based on Featured Distributions, in Pattern Recognition, vol. 29, pp. 51-59, Jan. 1996.

[8] T. Ojala, M. Pietikainen and T. Maenpaa, Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns, in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, pp. 971-987, Aug. 2002.

[9] T. F. Pereira, M. A. Angeloni, F. O. Simoes and J. E. C. Silva, Video-based Face Verification with Local Binary Patterns and SVM Using GMM Supervectors, in ICCSA 2012, Part I, LNCS 7333, pp.240-252.

[10] C. C. Chang and C. J. Lin, LIBSVM: A Library for Support Vector Machines, in ACM Transactions on Intelligent Systems, 2:27:1-27:27, 2011 Available: http://www.csie.ntu.edu.tw/ cjlin/papers/libsvm.pdf

[11] B. Zadrozny and C. Elkan, Transforming Classifier Scores Into Accurate Multiclass Probability Estiamtes, in ACM SIGKDD 2002, pp. 694-699.

[12] G. A. F. Seber and C. J. Wild, Nonlinear Regression, Hoboken, NJ: Wiley-Interscience, 2003.

[13] Guney Kayım, Ekberjan Derman, Albert Ali Salah Short Term Re-Identification of ATM Users via Face and Body Appearance Features.