Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Smart User Identity Sensing Method for Secure Withdrawal of Money from Atms

Manju Dabas Kadyan
Electronics & Communication Dept. of Engg.,
Rattan Institute of Tech. & Mgmt.,
Palwal, Haryana, India

Jyoti Dabass
Electronics & Communication Dept. of Engg.,
YMCA University of Science & Tech.,
Faridabad, Haryana, India

Abstract—In this paper, we have proposed a new authentication method for verification in withdrawal of money from ATMs. For this, the user's fingerprint will be used instead of entering the traditional 4 digit PIN codes. And the ATMs will be given an unified fingerprint enabled touch panel that combines multiple capacitive TFT based fingerprint sensors. If the user will enter the correctly aligned fingerprint then the withdrawal of money will be done as usual. But if the user is forced by anyone for withdrawal of money then the user can enter wrongly aligned fingerprint followed by the rightly aligned fingerprint. It will allow the withdrawal of money as like as the normal case but along with that it also generate alarm call in the nearest police station without giving any hint at the ATM. Thus giving more security in withdrawal of money.

Keywords- Auto Teller machine, PIN code, TFT, User Identity Sensing, Fingerprint

I. INTRODUCTION

A. ATMs

Auto Teller Machines or automated teller machine or automatic teller machine or cash point or cash machine or automated Banking machine, automatic till machine, or remote service unit is an electronic computerized machine that enables the customers of a Bank to perform financial transactions without the aid of a direct branch interaction or branch representative or teller.

On most modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smart card with a chip that contains a unique card number and some security information such as an expiration date or CVVC (CVV). And before every transactions, there must require an authentication which is mandatorily provided by the customer in form of entering a personal identification number (PIN).

Using an ATM, customers can access their bank deposit or credit accounts in order to make a variety of transactions like easy and quick cash withdrawals, check balances of their account, or credit mobile phones for paying bills or transfer money. ATMs have now become a part of everyone's life. They ease the customer's to do financial operation outside the bank in a variety of places. It is connected to a data system and related equipments and is activated by a bank customer to obtain cash withdrawals and other banking services. It consist of computers with a keypad and screen to perform operations. To access bank accounts, it is provided with a telephone network, a host processor, and a bank computer to verify data. Mostly ATM uses the single entry customer identity verification i.e., pin entry. If somebody gets any customer's pin number and his card details then he can easily access his account and gets the fund by withdrawing money from the ATM[1].

B. ATM CARDs

An ATM card, also known as a bank card, key card or cash card, is any payment card issued by a bank that enables a customer to access an automated teller machine (ATM) in order to perform transactions such as deposits, cash withdrawals, obtaining account information, etc. These card eliminate the need to carry cash or physical checks to make purchases. The first ATM cards were issued in 1967 and 1969 by Barclays Bank in London and Chemical Bank in Long Island, New York respectively. Most ATM cards today are bank cards such as debit or credit cards and they all are ATM-enabled. Also, Interbank networks allow the use of ATM cards at ATM outlet of any Bank other than that Bank that issued the card.

ATM cards allow us to withdraw cash from our checking account through an automated teller machine (ATM). To access our money this way, we will need to use a personal identification number (PIN) that we can establish when we open our account or that the bank will assign this to us. PINs provide an added layer of protection if our card is lost or stolen, so we should choose a PIN that would be difficult for someone else to guess. In order to keep this confidential, we have to memorize this number. But then a question arise, what if someone forces us to withdraw money from ATM? Then nothing can be done at that time, we will be facing two kind of situation, first either we will be fighting with that person and if that person is having some weapon, he must be using them against us or secondly we will be just giving money to him along with our Card and its PIN code. Then it will not remain the most secure way of authentication. So,

there must be some kind of secure authentication method instead of this 4-digit PIN, so that we will not be in any situation mentioned above and we will get immediate help from police if we face this kind of situation.

In many countries, the use of debit cards has become so increased that their usage has overtaken or entirely replaced cheques and, in some cases, cash transactions too. From the mid 2000s, debit cards issued in one country are also allowed to be used in other countries and their usage can also be done for internet and phone purchases.

When the user withdraw money from the ATM using their ATM cards, then payments are immediately transferred from the cardholder's designated bank account. That's why it becomes mandatory that they will not get stolen or misuse by anybody else than the card holder.

C. ATM Safety PIN Software

It is a software application that would allow users of automated teller machines (ATMs) to alert the police of a forced cash withdrawal by entering their personal identification number (PIN) in reverse order[3]. The system was patented by Illinois lawyer Joseph Zingher (U.S. Patent 5,731,575). But this system is not implemented in ATMs till now.

The main motto of this software was that If you should ever be forced by any one (for e.g., robber) to withdraw money from an ATM, then you can notify the nearby police by entering your PIN code in reverse. For example suppose if your PIN is 1234 then you would have to enter 4321 to generate alarm call. The ATM recognizes that your PIN is backwards and different from the PIN of the ATM card you placed in the machine. The ATM machine will still give you the amount of money which you have requested, but unknown to the robber, it also generate alarm call to nearby police station and the police will be immediately dispatched to help you.

If that system was get implemented, then the PINs that are reversible like 5555 or 2112 would be unavailable so that false alarms would not occur and police would not be dispatched to that ATM unnecessarily. Also, the PINs that are semi-reversible like 5255 or 1241, where the first and last digits are the same, would be avoid as well so that accidental alarms would not be triggered by accidently switching the middle numbers.

D. Objective of this Paper

In order to address the above challenges, we propose a novel user identity sensing approach which is highly influenced by the work of Tao Feng, Varun Prakash, and Weidong Shi[9] and added it on the ATM panel. The number system is not used here so instead of the keypad given on the traditional ATM's panel, we will use the identity sensor over there. Thus, the identity of user is then detect from fingerprint's alignment. This approach provides many advantages over the traditional 4 digit PIN Code . Firstly, it provides stronger and more reliable identity detection performance because fingerprint is well established as a reliable and highly accurate data source for identity verification. Secondly, it is safe as no one can get your fingerprint and suppose if one get that he/she can't get your correct alignment of your fingerprint. Thirdly, if you are in danger(e.g., someone is forcing you to withdraw money) then you can send alarm call to police by entering wrongly aligned fingerprint after the correctly aligned fingerprint and that also without letting that person to know.

II. BACKGROUND

A. Touchscreen

From the past few years, Touch screens have been widely used for interacting with portable devices like smart phones, tablets, notebooks, kiosks, gaming gizmos, and many more such devices. Touch screens, used in these consumer portable devices are mainly add on types as the touch screens are separated from the display panel. Due to the high rising demands for these consumer portable devices, the designing and manufacturing of the touch screens used in them, is nowdays become a vast and mature industry which is providing many commercially sensing methods. The most common sensing methods which are widely available and used are: capacitive [6], resistive [5], optical imaging, infrared[7] and acoustic-wave [4] based touch sensing techniques. From these techniques, the capacitive based method is becoming more popular day by day as it has high sensitivity, durability, and ability to detect multi-touches than all other techniques available in use. Also, to many surprise, the typical response time of a capacitive touch panel is 4ms which is better than other touch panels. Because of this, mostly devices now have capacitive touch panel whether it is any new smart phone, tab, notebook or any other smart device.

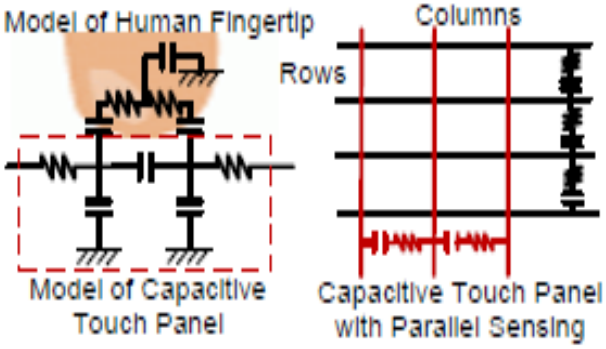

Fig. 1. Left: The equivalent model of the capacitive touch panel and human fingertip. Right: Simple model for the capacitive touch panel with parallel sensing.

B. Fingerprint Sensors and Transparent Electronics

It is widely known that the optical type of fingerprint sensor requires a lens system. So we have to look for another alternatives if we takes size into consideration. For this reason we can use TFT (thin film transistor) based fingerprint sensor as they are widely used for creating large size displays. In this technique, the ICs are directly put onto a glass substrate. It is the most cost effective and largely scalable way for creating fingerprint sensors that can cover larger area than the standard CMOS process based approach. In the past, several capacitive fingerprint sensor prototypes and products were developed using poly-Si TFTs [14]. Their Performance characteristics of some fabricated capacitive fingerprint sensing devices are shown in Table I. In the last few years, a revolutionary trend in electronic materials is coming into the existence, which is to implement TFTs using transparent materials and transparent electronic fabrication process. Nowadays, the Transparent electronics has become a rapidly developing technology that employs wide band-gap semiconductors for the realization of invisible circuits [11].

Table I Performance Data Of Some Actual Fingerprint Sensors

Reference	Cell Size	Resolution	Response	Frequency
[22]	42 _m	64 x 256	3ms	4MHz
[19]	81.6 _m	124 x 166	2ms	Not Mentioned
[12]	60 _m	320 x 250	160ms	500kHz
[11]	66 _m	304 x 304	200ms	250kHz
[20]	50 _m	224 x 256	20ms	Not Mentioned

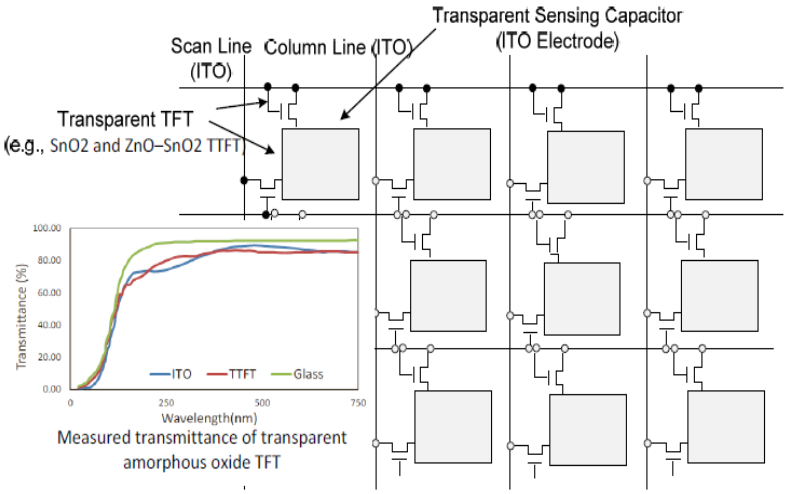

Fig. 2. Equivalent Circuit Model of Transparent TFT Fingerprint Sensing Array (For each sensing cell, all the components can be made from transparent materials, ITOs and transparent thin-film transistors)[10]

It has enabled the electronic manufacturers to design and build a variety of transparent electronic devices such as transparent TFT display (which is already successfully adopted by the consumer market), transparent fingerprint readers, transparent CMOS, or even transparent physical DRAM [12]. The same design and fabrication principle is used to built Transparent fingerprint sensors which is used for the other transparent TFT based electronic devices. Figure 2 shows an abstract circuit model of transparent TFT based fingerprint sensing array. Here all the components are made from transparent materials. At this point one may ask, why transparent fingerprint sensing didn't exist before? For answering this we can say that when compared with the abstract circuit model of multi-touch panel (also made from transparent material, ITO) in Figure 1, one can definately notice that there are two transparent thin film transistors involved in each sensing cell. The discovery of how to fabricate transparent thin film transistor is one of the main key techniques for developing transparent fingerprint sensors.

III. DESIGN

The block diagram of the proposed high speed TFT fingerprint sensors integrated with a touchscreen is shown in Figure 3. Here, multiple capacitive TFT fingerprint sensors are overlayered on top of a touchscreen. Here, each TFT fingerprint sensor contains capacitive fingerprint sensing cells in form of a matrix. Then, the TFT fingerprint sensors are abstracted from the user with the help of transparent TFTs. The TFT fingerprint sensors are placed to get optimized in such a way that the chances of capturing touches during the user-device interaction is get maximized. After that all the TFT fingerprint sensors are controlled by a controller chip. At the beginning of every process, only the touchscreen remains in fully powered on state and the Fingerprint sensors in idle state by default. When user will place its finger tip

inside the region covered by a fingerprint sensor, then its location will be recorded by the touchscreen controller first and after that the fingerprint sensor controller will be notified. Typically, the touchscreen response time is less than 4ms [7]. Furthermore, for minimizing interferences, different touch technique such as resistive multi touch sensing, acoustic-wave or infrared based touch sensing can be used in Touchscreens. In all cases, each fingerprint sensor and their cell has its unique column and line address. After this, the fingerprint controller will translate the touchscreen location (position in touchscreen X-axis and Yaxis) into a pair that consists of a line and column address. The line address decoder in Figure 3 can then decode the line address and send the decoded output to a parallel-in parallel-out shift register. At a single time, the shift register will enable one row of a capacitive sensing cells. After that, all the sensing cells in the enabled row will be addressed during a clock cycle and disabled when the results of the sensing cells are converted into digital values and fed into the latches situated at the end of each column. For each and every sensor cell, a comparator compares its voltage output with a reference voltage and after doing this, it stores the binary result into the corresponding latch.

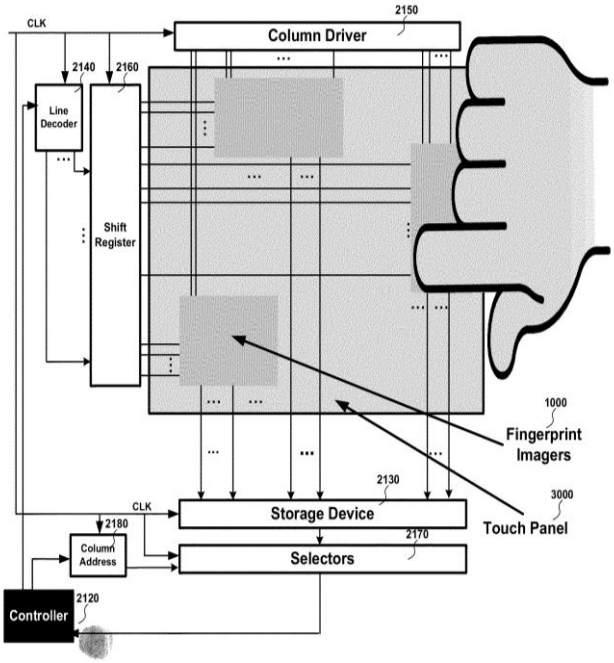

Fig. 3. Touchpanel with Integrated Transparent Capacitive Fingerprint Sensors

This design supports parallel accessing of the sensor cells at an enabled row therefore it will maximize the speed of fingerprint scan. The Pixel results which get stored in the latches are selected and then transmitted to the fingerprint controller. For minimizing the amount of data transferred, the fingerprint controller computes only a selected predefined pair of column addresses. Thus, only results which are stored in the latches within the selected columns are transferred to the fingerprint controller. We can greatly improve fingerprint capture speed using parallel addressing and selected data transfer. The described driving and controlling system is compatible with any TFT based capacitive fingerprint sensor built using transparent components. When the fingerprint data is correctly aligned ,the ATM will allow to withdraw money but if the correctly aligned fingerprint is followed by wrongly aligned fingerprint then it will still allow the user to withdraw money but it also generate alarm call to nearby police station so that police will get immediately dispatched to that ATM's location.

The processing steps are summarized in algorithm 1.

Algorithm 1 Pseudocode: Capturing of Fingerprints

```
1:  while true do
2:    Detect Touch Point (x,y);
3:  Transform Touchscreen (x,y) to Fingerprint Sensor Row and
    Column Addresses (r,c)
4:      if Fingertip Location (r,c) Inside the Areas of a Fingerprint
        Sensor then
5:          Drive Fingerprint Sensors and Capture Fingertip Data;
6:          Evaluate Quality of the Captured Data and Apply
             Fingerprint Match;
7:            if Fingerprint Matches with the Owner then
8:              if fingerprint is followed by wrongly aligned fingerprint
                then
 9:             Generate alarm call to the nearest police station
10:             end if
```



```
11:            Continue;
12:            else
13:            Take Pre-defined Response Action;
14:           end if
15:      end if
16: end while
```

IV. CONCLUSION AND FUTURE WORK

This paper explores a novel integrated identity sensing design based on transparent TFT based fingerprint sensors which requires only fingerprint nor any PIN codes by users. Thus, not only giving a secure and reliable method for users identity sensing but also helps in lowering the forced withdrawal of money by robbers. It will makes the ATMs more secure for withdrawal of money. It not only beneficial to the user but also to the banks as loss of money by robberies will also gets lowered. In this paper, we have proposed this idea of user's identity sensing but we are quite hopeful of its feasibility. So, in terms of future work, we are in process of doing more research work in order to transform our proposed work into reality.

REFERENCES

[1] Navneet Sharma and Dr.Vijay Singh Rathore, Analysis of different vulnerabilities in auto teller machine transactions,Journal of Global Research in Computer Science, vol. 3,No. 3, March 2012, pages 38-40.

[2] www.wikipedia.org

[3] ZICUBED ATM SAFETY PIN, ATM Safety PIN aka Reverse PIN Web Site.

[4] R. Adler and P. Desmares. An economical touch panel using saw absorption. Ultrasonics, Ferroelectrics and Frequency Control, IEEE *Transactions on*, 34(2):195 –201, march 1987.

[5] R. Aguilar and G. Meijer. Fast interface electronics for a resistive touchscreen.In *Sensors, 2002. Proceedings of IEEE*, volume 2, pages 1360– 1363 vol.2, 2002.

[6] Atmel. Touchscreen Controllers - Parameters. http://www.atmel.com/

[7] J.-Y. Ruan, P.-P. Chao, and W.-P. Chen. A multi-touch interface circuit for a large-sized capacitive touch panel. In *Sensors, 2010 IEEE*, pages 309 –314, nov. 2010.

[8] S.-J. Kim, J.-M. Song, and J.-S. Lee. Transparent organic thin-film transistors and nonvolatile memory devices fabricated on flexible plasticsubstrates. *J. Mater. Chem.*, 21:14516–14522, 2011.

[9] Tao Feng, Varun Prakash, and Weidong Shi, Touch Panel with Integrated Fingerprint Sensors Based User Identity Management

[10] www.ehow.com

[11] S. Shigematsu, H. Morimura, Y. Tanabe, T. Adachi, and K. Machida.A single-chip fingerprint sensor and identifier. *J. Solid-State Circuits*,34(12):1852–1857, 1999.

[12] W.-S. Cheong, S.-M. Yoon, C.-S. Hwang, and H. Y. Chu. High-mobility transparent sno2 and zno-sno2 thin-film transistors with sio2/al2o3 gate insulators. *Jpn J Appl Phys*, 48(4):04C090– 04C090–4, apr 2009.

[13] T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen. Continuous mobile authentication using touchscreen gestures. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, pages 451–456, 2012.

[14] J. woo Lee, S. Member, D. jin Min, J. Kim, and W. Kim. A 600-dpi capacitive fingerprint sensor chip and image-synthesis technique. *IEEE Journal of Solid-State Circuits*, 34:469–475, 1999.

