Biometric Payment Systems using CNN and Digital Signatures

Mr. Rahul Anjana(Asst.
Professor)School of Computing Science
and Engineering(B.Tech CSE)
Galgotias University, Greater Noida,
Uttar Pradesh, India

Aarush Kumar
School of Computing Science and
Engineering (B.Tech CSE(Hons.))
Galgotias University
Greater Noida, Uttar Pradesh, India
aarushkumar100616@gmail.com

Vani Chug
School of Computing Science and
Engineering (B.Tech CSE)
Galgotias University
Greater Noida, Uttar Pradesh, India
vanichug01@gmail.com

*1.1 **Abstract–***

In this paper we have survey on biometric payment system. Biometric payment system is used for various kinds of payment system instead of the tension of cards to put with them and to memorize theirs difficult passwords and pin numbers. Biometric payment system is much safe and secure and very easy to use and even without using any password or secret codes to remember as compare with previous system like credit card payment system, wireless system and mobile system etc. Biometric payment system is reliable, economical and it has more advantages as compare with others. In daily life the usage of credit cards, check card for shopping, bus card, subway card for traveling, student card for library and department, and many kinds of cards for unlimited purposes and so on. So problem is that a person has to take many cards and has to remember their passwords or secret codes and to keep secure to take with him all time. So the biometric payment system will solve this problem. Greater adoption of biometric payment system will drive down the cost of biometric readers and thus making it more affordable to small business owners. We really need alternate payment systems. This "perpetual toll" to credit card companies has to stop.

1.1.1 Purpose

Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics. The technology is mainly used for identification and access control or for identifying individuals who are under surveillance. The basic premise of biometric authentication is that every person can be accurately identified by intrinsic physical or behavioral traits. The term biometrics is derived from the Greek words bio, meaning life, and metric, meaning to measure. Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics and point-of-sale applications. In addition to security, the driving force behind biometric verification has been convenience, as there are no passwords to remember or security tokens to carry. Some biometric methods, such as measuring a person's gait, can operate with no direct contact with the person being authenticated.

Keywords:Blockchain, Tensorflow, DeepAi, Keras, DNN

LIST OF ABBREVIATIONS

DNN:Deep Neural Networks, DAI: Deep Nets using Artificial Intelligence.

I. I NTRODUCTION

Consumers worldwide support biometrics: Nearly 70% of consumers' worldwide support using biometrics technology, such as fingerprints or voice recognition, administered by a trusted organization (bank, healthcare provider or government organization) as a way to verify an individual's identity, according to new global research from Unisys (www.Unisys.com). In the first worldwide survey of its kind to study consumer security preferences, the Unisys research also found 66% of consumers worldwide favored biometrics as the ideal method to combat fraud and identity theft as compared to other methods such as smart cards and tokens, reports Enterprise Networks and Servers. This finding shows an increase from separate research that Unisys conducted in September 2005, which found 61% of consumers' worldwide favored biometrics as the preferred method to fight fraud and identity theft. [3] In the future, no one will need pockets. That stuff jingling around in there -- keys, credit cards, checkbooks -- will be replaced by something closer to the body. When you need to open a door or make a purchase, chances are you'll do it with a fingerprint, a voice command, or a computer scan of your eyeball. That is, if companies like Pay By Touch have anything to say about it. Pay By Touch, a closely held San Francisco outfit, specializes in biometrics, or the technology of identifying people by unique biologic traits -- not just fingerprints, but also irises, palms, and voices. And increasingly, those traits are being used in place of keys, credit cards, and even computer passwords. Founded in 2002, Pay By Touch has signed up more than 2 million people willing to have their fingerprints used as a surrogate for checks and credit cards at more than 2,000 stores, including several large grocery chains. When making a purchase, a customer presses his pointer finger to a pad and then keys in an identifying number as an added security measure before his purchase is deducted from a checking account or added to a credit-card bill. On Mar. 21, Pay By Touch said its device would be installed in all of Albertson's (ABS) Jewel-Osco stores, a chain of more than 200 outlets that combine supermarkets and pharmacies. It's not just stores that are using biometrics. Elementary schools have installed iris scanners to keep out intruders. Companies increasingly use fingerprint scanners to authenticate computer users. And fingerprint readers have also been installed on locks for house and office doors. [4] That's the philosophy behind Indivos, an Oakland, California, firm that has invented software that uses fingerprint scanners to process electronic payments. "We're putting this in front of the mainstream consumer," said Indivos spokesman Frank Pierce. "You won't need cash or cards to pay for anything. All you need is your finger and you never leave home without it." Many states now fingerprint people that seek driver's licenses or welfare benefits in an effort to detect fraud. Schools fingerprint would-be teachers to weed out pedophiles. In the corporate world, fingerprints are used as biometric keys to access buildings and computer networks. And in Pennsylvania, schools are testing finger scanners that allow students to check out library books and buy food in the cafeteria. [5] Fingerprints are reliable identifiers because, like snowflakes, no two fingerprints are alike, said Gary W. Jones, who worked as an FBI fingerprint specialist for 33 years. [5] For consumers, the biggest draw of finger scan payment is convenience. Pierce offered a scenario where a jogger enters a store after a long run and simply presses her finger against a sensor to purchase a cold drink. And for retailers, fingerprint scanners could reduce costs incurred by bad checks and stolen credit cards, Pierce said. After all, you can't forge a fingerprint. Jones said the only way someone could duplicate one is to make a cast of their finger. In today’s world everybody have number of cards in his pocket or purse for purchasing and selling things, traveling and many facilities for his need. There is problem is that the person have to pick many cards and he has also with secret codes and with other tensions too, so to avoid these kinds of problems the biometric fingerprints payment technique is used for easily to utilized. Fingerprint authentication is still the number one choice of security measure for identity verification in Malaysia and Singapore, according to a Unisys survey. SINGAPORE--Citibank on Wednesday 9th November 2006 launched a new fingerprint authentication payment service that lets its credit card customers pay for goods and services with a touch of the finger. According to Citibank, the biometric payment service will be available from today at nine merchant locations in the island-state, including retail outlets such as music and IT stores, clubs, restaurants and cinemas.

2. Background

Biometrics identify people by measuring some aspect of individual anatomy or physiology (such as your hand geometry or fingerprint), some deeply ingrained skill, or other behavioral characteristic (such your handwritten signature), or something that is a of the two (such as your voice).[15] Biometric authentication technologies such as face, finger, hand, iris, and speaker recognition are commercially available today and are already in use.[16] A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the context, a biometric system may operate either in verification mode or identification mode:

Verification mode: In the verification mode, the system validates a person’s identity by comparing the captured biometric data with her own biometric template(s) stored system database. In such a system, an individual who desires to be recognized claims an identity, usually via a PIN Personal Identification Number), a user name, a smart card, etc., and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., “Does this biometric data belong to Bob?”). Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity.

Identification mode: In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual’s identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (e.g., “Whose biometric data is this?”). Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics.

3. Types of Biometrics

There are several human distinguishable traits that fit the definition of biometrics given above. In order to be used for recognizing a person, the human trait needs to be unique and not subject to change. Fingerprints, for example, have been used for over one hundred years and, therefore, are generally well accepted as a recognition technology. Other technologies such as face, hand geometry, speaker and iris recognition are also generally accepted. A biometric that would require giving a blood sample for frequent personal verification would probably not be very well accepted. Performance considerations are important. No biometrics can guarantee one hundred percent accuracy. A brief introduction of the commonly used biometrics is given below:

DNA:

Deoxyribo Nucleic Acid (DNA) is the onedimensional ultimate unique code for one's individuality - except for the fact that identical twins have identical DNA patterns. It is, however, currently used mostly in the context of forensic applications for person recognition. Three issues limit the utility of this biometrics for other applications: (i) Contamination and sensitivity (ii) Automatic real-time recognition issues (iii) Privacy issues Ear: It has been suggested that the shape of the ear and the structure of the cartilaginous tissue of the pinna are distinctive. The ear recognition approaches are based on matching the distance of salient points on the pinna from a landmark location on the ear. The features of an ear are not expected to be very distinctive in establishing the identity of an individual.

Face Recognition:

Different technologies can be used for face recognition. One approach consists on capturing an image of the face using an inexpensive camera (visible spectrum). This method typically models key features from the central portion of a facial image extracting these features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair. Major benefits of facial recognition are that it is nonintrusive, hands-free, provides for continuous authentication and is accepted by most users. Enrollment sample sizes (e.g., 5 face samples) may range from 1 KB-2KB/sample). Smaller template sizes are also used (e.g., less than 100 bytes).

Fingerprints:

Fingerprints are important. By 1998, fingerprint recognition products accounted for 78% of the total sales of biometric technology. These products look at the friction ridges that cover the fingertips and classify patterns of minutiae, such as branches and end points of the ridges. Some also look at the pores in the skin of the ridges. Fingerprint recognition devices for desktop and laptop access are widely available from many different vendors at a low cost. The relatively small size allows the sensor to be integrated in other devices (e.g., mice, keyboards). This biometric technology uses the pattern of friction ridges and valleys on an individual's fingertips. These patterns are considered unique to a specific individual. The same fingers of identical twins will also differ. A user does not need to type passwords - instead, only a touch to a fingerprint device provides almost instant access (typically less than 1 sec.). A typical enrollment identifier may include 2 finger samples (e.g., 1 KB) although smaller finger samples are also used. One of the challenges of fingerprint technology is individuals that have poorly defined (or tenuous) ridges in their fingerprints.

Gait:

Gait is the peculiar way one walks and is a complex spatio-temporal biometric. Gait is not supposed to be very distinctive, but is sufficiently discriminatory to allow verification in some low security applications. Gait is a behavioral biometric and may not remain invariant, especially over a long period of time, due to fluctuations in body weight, major injuries involving joints or brain, or due to inebriety.

Hand and Finger Geometry:

Hand recognition has been available for over twenty years. To achieve personal authentication, a system may measure physical characteristics of the fingers or the hand such as length, width, thickness and surface area of the hand. These methods of personal authentication are well established. Some systems require a very small biometric sample (e.g., 9 bytes). Hand geometry can frequently be found in physical access control for commercial and residential applications, for time and attendance systems, and for general personal authentication applications. In addition, an individual's jewelry (e.g., rings) or limitations in dexterity (e.g., from arthritis), may pose further challenges in extracting the correct hand geometry information.

Iris:

As far as is known, every human iris is measurably unique. It is fairly easy to detect in a video picture, does not wear out, and is isolated from the external environment by the cornea (which in turn has its own cleaning mechanism). The iris pattern contains a large amount of randomness, and appears to have many times the number of degrees of freedom of a fingerprint. It is formed between the third and eighth month of gestation, and (like the fingerprint pattern) is phenotypic in that there appears to be limited genetic influence; the mechanisms that form it appear to be chaotic. So the patterns are different even for identical twins (and for the two eyes of a single individual), and they appear to be stable throughout life.

Retinal Scanning:

This method of personal authentication uses the vascular patterns of the retina of the eye. In healthy individuals, the vascular pattern in the retina does not change over the course of an individual's life. The patterns are scanned using a low-intensity (e.g., near-infrared) light source. It requires the user to look into a device and focus on a given point. The image acquisition involves cooperation of the subject, entails contact with the eyepiece.

Signature Verification:

The way a person signs her name is known to be a characteristic of that individual. Signatures of some people vary substantially: even successive impressions of their signature are significantly different. It is based on measuring dynamic signature features such as speed, pressure and angle used when a person signs a standard, recorded pattern (e.g., autograph). One focus for this technology has been e-business applications.

Voice Recognition:

Voice recognition or speaker recognition is the problem of identifying a speaker from a short utterance. This biometric technology uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (e.g., size and shape of the throat and mouth) and learned behavioral patterns (e.g., voice pitch, speaking style). A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background noise. Speaker recognition is most appropriate in phone-based applications but the voice signal over phone is typically degraded in quality by the microphone and the communication channel.

4. Fingerprint Payment System:

Biometric payment technology allows the consumer to pay with the touch of a finger on a fingerprint scanner linked to a payment file. The fingerprint template is typically linked to a router and transmission media necessary to clear the transaction through an automated clearinghouse. While many biometric payment transaction providers focus on grocery, home improvement and convenience stores, others have indicated interest in quick-serve eateries, car wash locations and select vending operations. Biometric payment providers (e.g., Pay-by-Touch and BioPay) require completion of a pre-enrollment process in which index fingers are scanned and driver's license and banking information is recorded in an account database. This process reportedly takes less than two minutes. In addition to transaction settlement, biometric payment providers may also link captured transactions to loyalty reward programs, gift cards, discount coupons and Web access services.

4.1 Rapid transactions and reduced fees:

Just how fast can biometric payment systems process transactions? Pay-by-Touch and BioPay state transaction times range from 5 to 15 seconds, which they claim is favorable compared to cash, credit card or debit card settlement. While the speed of the transaction may be attractive, decreased transaction fees may be more persuasive as a selling point. Since a biometric payment transaction is treated as an automated clearinghouse debit, fees tend to be significantly lower (estimated at 75 percent) than comparable credit card or signature-debit card transactions.

4.2 Fingerprint template:

The first step in fingerprint identification is collecting the fingerprint using a special sensing device. This process is referred to as enrollment. In this step, the fingerprint is acquired for authentication. The captured image (called the fingerprint template) can be stored directly as an image or can be stored as a biometric algorithm. In the case of a biometric algorithm, several data points on the fingerprint template are scientifically measured and stored, thereby leading to discarding of the actual fingerprint. Algorithm software measures 40 or more data points for each fingerprint and may store these measurements as data coordinates or encrypt them into a digital certificate for future authentication. When the mathematical representation of the fingerprint, not the actual fingerprint, is used to prove identity, a higher level of reliability is realized. In addition, some biometric payment systems may require the consumer to also swipe or wave a smart card in addition to scanning a finger to authenticate a transaction. This approach provides another layer of security than exclusively relying on fingerprint matching.

5. Fingerprint Recognition through Circular Sampling:

The use of one's fingerprints as a means of identification has existed long before its common usage today in the field of criminal investigation. Before nineteenth century, fingerprints were primarily used only as a signature for indicating authorship or ownership. Other applications were not acknowledged until about 1860 when William Hershel was regularly imprinting the handprints of those engaged in his contracts. It was not until 1881 when Henry Faulds recognized that fingerprints found at crime scenes may be used to identify the perpetrator. [6] Since 1924, the FBI has accumulated about 30 million sets of fingerprints aking the matching of a single fingerprint with such a collection very difficult. With the advent of advanced computer technology in the past few decades, automated fingerprint identification systems (AFIS) can effectively perform what would otherwise be a laborious and time consuming task.

5.1 Fingerprint Uniqueness:

What actually makes a fingerprint unique depends on one main factor. Fingerprints basically consist of ridges (raised skin) and furrows (lowered skin) that twist to form a distinct pattern. When an inked imprint of a finger is made, the impression created is of the ridges while the furrows are the uninked areas between the ridges. Although the manner in which the ridges flow is distinctive, other characteristics of the fingerprint called 'minutiae' are what is most unique to the individual (See figure 1 for several minutiae representations). These features are particular patterns consisting of terminations or bifurcations of the ridges. Moreover, all fingerprints can be classified into three categories based on their major central pattern. These patterns are the arch, loop, and whorl, which are shown in figure.

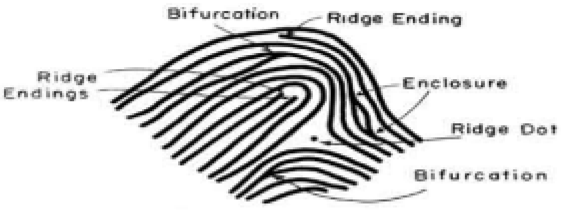
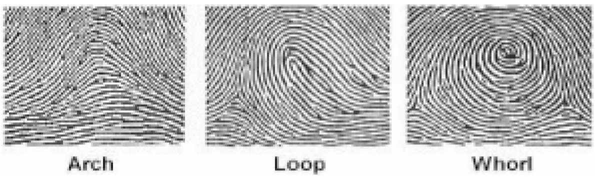


Figure 1. Minutiae examples



An image, such as that of a fingerprint, may be considered as a two-dimensional continuous signal. By this, it can have an infinite number of brightness intensities in an infinitesimal area. In order for an image to be handled by a computer, it must first be digitized. For this study, the image had to be sampled in a different manner. Instead of sampling in the general Cartesian space, the image is sampled through a pattern consisting of concentric circles. It may be considered that this technique is sampling in a polar coordinate space. Under this approach, the sampling resolutions are the distance between the concentric circles and the sampling interval within the circumference of the circles. A high magnitude indicates that at the corresponding shift, the two source signals were more alike than at a shift for a low magnitude. The magnitude is the total area of theproduct of the two signals.

$$g(x) = \int_{-\infty}^{\infty} f_1(\alpha) f_2(\alpha + x) \delta\alpha \qquad (1)$$

In addition, the correlation operation is performed in a circular fashion so that the shifted signal must wrap around the other as shown in fig (3) and Equation: (2).

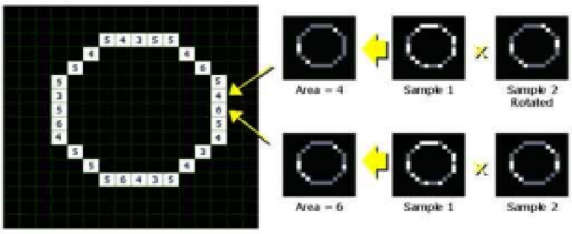


Figure 3. Circular correlation process

$$g_n(i) = \sum_{\alpha=0}^{I_n - i - 1} f_{1n}(\alpha) f_{2n}(\alpha + i) + \sum_{\alpha=I_n - i}^{I_n - 1} f_{1n}(\alpha) f_{2n}(\alpha - I + i) \qquad (2)$$

6. Fingerprint Identification

6.1 Fingerprint Matching :

Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and furrows. The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach. However, it has some of its own shortcomings. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation as shown in fig 4

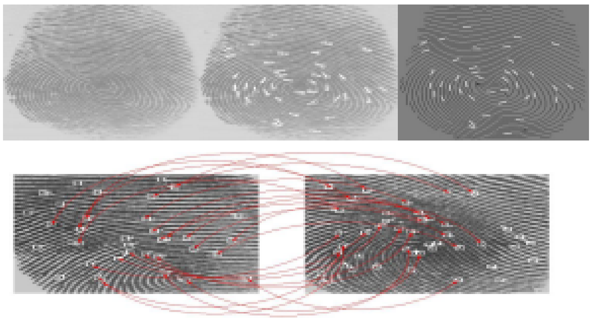


Figure 4. Fingerprint matching

6.2 Fingerprint Classification:

Fingerprint classification is a technique to assign a fingerprint into one of the several prespecified types already established in the literature which can provide an indexing mechanism. Fingerprint classification can be viewed as a coarse level matching of the fingerprints. An input fingerprint is first matched at a coarse level to one of the prespecified types and then, at a finer level, it is compared to the subset of the database containing that type of fingerprints only. Fingerprints are classified into five classes, namely, whorl, right loop, left loop, arch, and tented arch as shown in Figure.5. This information is quantized to generate a Finger Code which is used for classification.

6.3 Fingerprint Image Enhancement:

A critical step in automatic fingerprint matching is to automatically and reliably extract minutiae from the input fingerprint images. However, the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. In order to ensure that the performance of an automatic fingerprint identification/verification system will be robust with respect to the quality of the fingerprint images, it is essential to incorporate a fingerprint enhancement algorithm in the minutiae extraction module

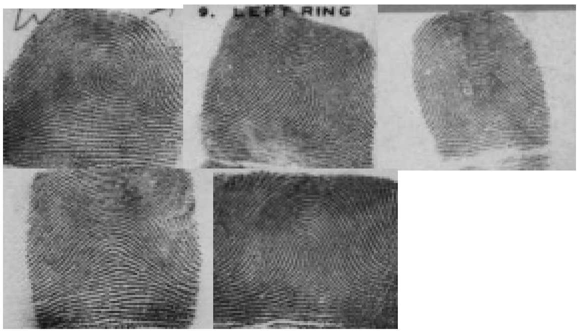


Figure 5. Five classes of fingerprints

7. Some Examples of Fingerprint Payment System

7.1 Pull My Finger... For Payment

A new report says Wal-Mart and Costco are investigating biometric payment systems that scan people's fingers to identify them and call up payment information. The systems are already in use at some supermarket chains, and aim to answer privacy concerns by storing just certain measurements of a person's fingerprint, rather than the entire fingerprint itself The company that makes the equipment pitches benefits to consumers of faster checkout and higher security, but enough questions have been raised about fingerprint scanners -- that the security claims deserve closer scrutiny. The transaction speed is really more of a benefit for retailers; anyway, alongside the lower transaction-processing fees they can pay by getting people to use their checking accounts instead of credit or debit cards. The analyst report says a 20% cut in Wal-Mart's payment-processing costs could translate to a 3-4% increase in earnings per share within three years -- if biometric payment systems can deliver those kinds of results, expect to see them sooner rather than later, privacy concerns or no.

7.2 Let your fingers do the paying NEW YORK (FORTUNE) -

Buying groceries with the touch of a finger could be closer than you think, if new research touting the benefits of biometric payment for retail giants like Wal-Mart, Target, and Costco is anything to go by. Already in use at supermarket chains like Albertsons (Research) (which yesterday agreed to be sold to a group that includes CVS and Supervalu), Cub Foods (part of Supervalu), and privately held Piggly Wiggly, biometric systems are just one of several emerging payment technologies that retailers are currently experimenting with. Others include self-checkout (widely deployed at Home Depot), contact less cards like J.P Morgan Chase's "blink," and so-called "near field communication," which involves waving your cell phone, say, near a reader. Here's how biometric payment works: To set up an account, customers scan their fingerprint at an instore kiosk, enter their phone number, and then submit checking and credit card account information. To make a purchase, they place their finger on a scanner at the register, enter their phone number, and choose how they want to pay (credit, debit, or checking). The benefits to customers are twofold. First, it offers a speedier checkout—70% faster than traditional forms of payment (unless the reader can't identify your finger, so keep those hands clean.) Second, it enhances security. Of the nearly 10 million cases of identity theft annually, according to a 2003 Federal Trade Commission survey, 13% occurred during a purchase transaction. "Biometric payment systems make conducting transactions safer for consumers," writes Kozloff.

7.3 Cash, Charge or Fingerprint?

Three or four days a week, Darren Hiers gets lunch at a Sterling convenience store near the car dealership where he works. He grabs a chicken sandwich and a soda and heads to the checkout counter, where a little gadget scans his index finger and instantly deducts the money from his checking account, as shown in figure 6. Hier doesn’t have to pull out his wallet to buy lunch -- and if it were up to him, he'd never have to write a check or swipe a credit card again.

7.4 No cash? No card? Just stick in finger TAMPA -

Customers can pay with cash, plastic or their index finger at a new Coast to Coast Family Convenience store here. There are no cards or PIN numbers to remember. Just stick your finger in the scanner and be on your way. “People either love it or think it's a sign of the coming apocalypse,” "Finger scanning is new, so we want to get people used to it by building acceptance at high-frequency, high-traffic retail locations such as gas stations and grocery stores," said Leslie Connelly, spokeswoman for Pay By Touch. "We're also going into places where people who don't have banking relationship cash pay checks." The company is a bit puzzled by customer privacy fears. After all, they say, how can using a unique fingerprint for identification be riskier to theft than a plastic card, key chain token or account number that's tapped into a computer or spoken over the phone? The company pledges not to sell or rent personal information, or access to it. The fingerprint image recorded is not the same as those collected by the federal government or law enforcement. [10] It's similar to the finger-scan technology used at theme park gates. Those systems take measurements of patrons' hands and fingers and link them to a multi-day pass to prevent several people from using one person's pass.

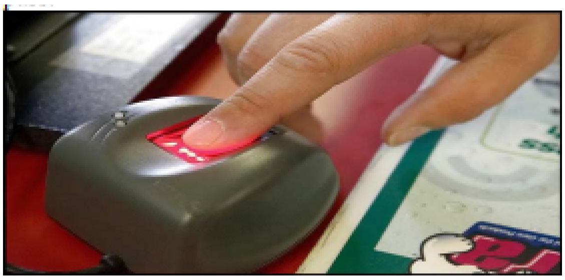


Figure 6. The red light tells the customer, Darren Hiers, that the system is ready to read his fingerprint.

The supermarket is using biometric Epayment software from Indivos Inc. to let customers speed through checkout, using their fingertips for identification. From then on, registered customers will be able to pay for groceries by scanning their fingertips at checkout and entering a personal identification number. If the number and fingerprint match the information in the database, the device will ask customers to choose their form of payment from the credit and debit cards that they previously entered in the database. "It's really about customer convenience and security," says Paul Kapioski, president and owner of that Seattle supermarket. "For one, you won't have to dig your credit cards out of your purse or wallet, and you're assured that no one else is using your cards in our store." Deployment is relatively simple, says Kapioski, who didn't have to replace the existing pointof-sale machines. Readers on the credit-card machines that are located at the checkout counter capture the customers' finger images and send encrypted data to one of Indivos' four data centers. Software matches a fingerprint against the one scanned when the customer enrols in the program. Indivos sends select data from the data center to the point-of-sale terminal. The transaction is routed through conventional financial networks like any other credit-card or debit-card transaction. Using biometric identification to authenticate E-payments is just starting to catch on. Vendors have touted the technology as a method to improve the security surrounding E-payments. Biometric technology makes perfect sense for Epayments, but deployments have been few, says James Van Dyke, research director for research firm Jupiter Media Metrix. "In the long-term, biometric technology can become a big part of E-payments, especially for mobile E-payments," "Using biometric technology with E-payments is perfect because it won't just identify you, but it'll authenticate you, too," Van Dyke says. "It will greatly lower the risk of identity theft."

7.5 Shell Introduces Pay by Fingerprint CHICAGO --

For the first time, drivers can pay for their gasoline with just the touch of a finger thanks to a new payment method Shell Oil Products US is piloting in Chicagoland starting this week. Shell is the first gasoline retailer in the world to adopt Pay By Touch's convenient and secure biometric payment technology. Shell is piloting Pay By Touch at 10 Chicagoland retail locations. "What's easier than paying at the pump with your finger? Pay By Touch will help Shell customers refill faster and easier, which is why we are so excited to be the first gasoline retailer in the world to offer it to consumers," said Chris Suess, manager of global refueling innovations. "We are always striving to make our customers' experiences more convenient and Pay By Touch is free, fast, secure and easy."

8. Conclusion

Biometrics is a means of verifying personal identity by measuring and analyzing unique physical or behavioral characteristics like fingerprints or voice patterns. The conclusion of this whole paper is that the card-less payment system should be replaced and there must be more easier, reliable, secure, cash free and tension free payment system, i-e biometric payment system in which no body have to take with dozens of cards for shopping, traveling, pass in office, university or bank as door lock. And he must have some secure codes to access as authorization and there is also one another disadvantage is that there may be stolen of cards or it can be losses at any time without any care. So to consider all these kinds of problems and disadvantages of card payment system the fingerprints payment system is suggested to be implemented because it is easier, reliable, feasible, secure and easily authorized to everyone. And there is no any worry that anyone can stolen my finger are can be loosed anywhere so other body can use it. In fingerprint payment system customer has to place his fingers on the finger-scanner and then scanner will recognize the account which belongs to that person and charge the bill. So it is easy for both customer and seller because there is no need to scratch the credit card and then enter code if code is forgot or if some time card cannot read and many more problems can occur in card payment system. And in biometric payment system no need to carry cash with them. Biometric payment system may be like fingerprints, IRIS, face recognition and blood reading or skin reading and it may be installed at any store, university, library, hostel, bank, office, home door lock, internet online shopping and many kinds where card system is installed. So in this paper we explain the biometrics with detailed term, how fingerprint system works, fingerprints' types and fingerprint recognition through circular sampling.

9.References

[1]http://www.zdnetasia.com/news/security/0,39044215,62011592,00.html

[2]http://www.zdnetasia.com/news/security/0,39044215,61965886,00.html

[3] http://fingerprint-it.blogspot.com/

[4] Alex Halperin: "Biometrics: Payments at Your Fingertips", Wednesday, March 29, 2006.

[5] Julia Scheeres: "Will It Be Cash, Check or Finger?"

[6] David H. Chang: "Fingerprint Recognition through Circular Sampling,"

[7]http://www.techdirt.com/articles/20060125/0922251.shtml

[8] Matthew Boyle, Wal-Mart, "Costco weigh merits of allowing customers to pay by scanning fingerprints:"

[9] Ellen McCarthy: "Washington Post Staff Writer".

[10] MARK ALBRIGHT: Times Staff Writer

[11] Should Minneapolis get tougher on panhandlers? http://twincities.bizjournals.com/twincities/stories/2005/05/09/daily57.html

[12] Jennifer Maselli: "Supermarket's biometric system will scan shoppers' fingertips"

[13] Michael L. Kasavana : "Biometric Scanning Offers Vending New Payment Options"

[14] Salil Prabhakar, Anil Jain: "Fingerprint Identification"

[15] Ross Anderson's: "Chapter 13th Biometrics of Security Engineering".

[16] Fernando L. Podio: "Personal Authentication Through Biometric Technologies"

[17] Anil K. Jain, Arun Ross and Salil Prabhakar: "An Introduction to Biometric Recognition" IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[18] Dileep Kumar, Dr.Yeonseung Ryu, Dr.Dongseop Kwon: "A Survey on Biometric Fingerprints: The Cardless Payment System" IEEE ISBAST April, 2008.

[19] L. O'Gorman, "Seven Issues With Human Authentication Technologies", Proc. of Workshop on Automatic Identification Advanced Technologies (AutoID), pp. 185- 186, Tarrytown, New York, March 2002.

[20] http://www.secprodonline.com/articles/52819/