Palm Vein Authentication System: A Review

Ishani Sarkar[1], Farkhod Alisherov[2], Tai-hoon Kim[3], and Debnath Bhattacharyya[2]

[1]Computer Science and Engineering Department
Heritage Institute of Technology
Kolkata, India
ishanisarkar12@gmail.com
[2]Hannam University
Daejeon, South Korea
sntdvl@yahoo.com, debnathb@gmail.com
[3]University of Tasmania, Australia
taihoonn@empal.com

Abstract

This paper presents a review on the palm vein authentication device that uses blood vessel patterns as a personal identifying factor. The vein information is hard to duplicate since veins are internal to the human body. The palm vein authentication technology offers a high level of accuracy. Palm vein authentication uses the vascular patterns of an individual's palm as personal identification data. Compared with a finger or the back of a hand, a palm has a broader and more complicated vascular pattern and thus contains a wealth of differentiating features for personal identification. The importance of biometrics in the current field of Security has been depicted in this work. We have also outlined opinions about the utility of biometric authentication systems, comparison between different techniques and their advantages and disadvantages in this paper. Several banks in Japan have used the palm vein authentication technology for customer identification since July 2004. In addition, Fujitsu has integrated the technology into the access control of electronic door lock systems. Fujitsu plans to further expand applications for this technology by downsizing the sensor and improving the verification speed.

Keywords: biometric authentication, Palm vein authentication, Face recognition.

1. Introduction

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are; face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric systems are superior because they provide **a nontransferable means of identifying people** not just cards or badges. The key point about an identification method that is "nontransferable" means it cannot be given or lent to another individual so nobody can get around the system - they personally have to go through the control point.

The fundamentals of biometrics are that they are things about a person:
- measurable - things that can be counted, numbered or otherwise quantified
- physiological characteristics - like height, eye color, fingerprint, DNA etc.
- behavioral characteristics - such as the way a person moves, walks, types

In a practical biometric system (i.e., a system that employs biometrics for personal recognition), there are a number of other issues that should be considered, including:

Performance, which refers to the achievable recognition accuracy and speed, the resources required to achieve the   desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed;

Acceptability, which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives;

Circumvention, which reflects how easily the system can be fooled using fraudulent methods.

A key advantage of biometric authentication is that biometric data is based on physical characteristics that stay constant throughout one's lifetime and are difficult (some more than others) to fake or change. Biometric identification can provide extremely accurate, secured access to information; fingerprints, palm vein and iris scans produce absolutely unique data sets (when done properly). Automated biometric identification can be done rapidly and uniformly, without resorting to documents that may be stolen, lost or altered. It is not easy to determine which method of biometric data gathering and reading does the "best" job of ensuring secure authentication. Each of the different methods has inherent advantages and disadvantages. Some are less invasive than others; some can be done without the knowledge of the subject; others are very difficult to fake [1].

Palm vein authentication has a high level of authentication accuracy due to the uniqueness and complexity of vein patterns of the palm. Because the palm vein patterns are internal to the body, this is a difficult method to forge. Also, the system is contactless and hygienic for use in public areas. It is more powerful than other biometric authentication such as face, iris, and retinal.

Palm vein authentication uses an infrared beam to penetrate the users hand as it is held over the sensor; the veins within the palm of the user are returned as black lines. Palm vein authentication has a high level of authentication accuracy due to the uniqueness and complexity of vein patterns of the palm. Because the palm vein patterns are internal to the body, this is a difficult method to forge. Also, the system is contactless and hygienic for use in public areas.

2. Previous Works

Biometrics authentication is a growing and controversial field in which civil liberties groups express concern over privacy and identity issues. Today, biometric laws and regulations are in process and biometric industry standards are being tested. Automatic recognition based on "who you are" as opposed to "what you know" (PIN) or "what you have" (ID card). Recognition of a person by his body & then linking that body to an externally established identity forms a very powerful tool for identity management Biometric Recognition. Figure 1 shows the different type of biometric authentication.

Canadian airports started using iris scan in 2005 to screen pilots and airport workers. Pilots were initially worried about the possibility that repeated scans would negatively affect their vision but the technology has improved to the point where that is no longer an issue. Canada Customs uses an iris scan system called CANPASS-Air for low-risk travelers at Pearson airport.

Junichi Hashimoto, 2006, has introduced finger vein authentication, a new biometric method utilizing the vein patterns inside one's fingers for personal identification. Vein

patterns are different for each finger and for each person, and as they are hidden underneath the skin's surface, forgery is extremely difficult. These unique aspects of finger vein pattern recognition set it apart from previous forms of biometrics and have led to its adoption by the major Japanese financial institutions as their newest security technology.

Iris scan   Face recognition   Finger print

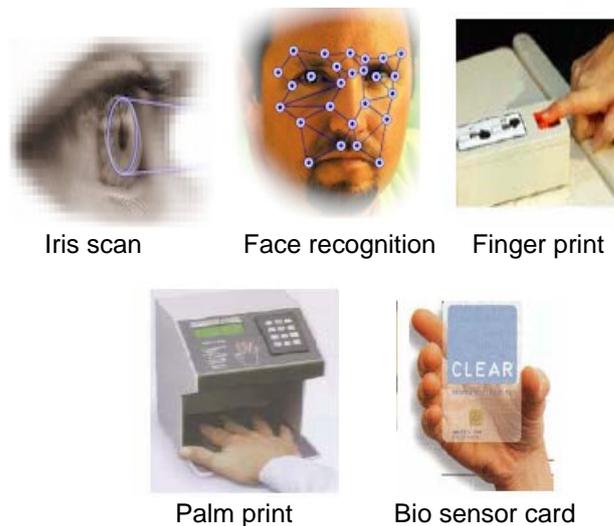Palm print   Bio sensor card

Figure 1. Various Biometric Systems.

Yuhang Ding, Dayan Zhuang and Kejun Wang, July 2005[2], have shown the theoretical foundation and difficulties of hand vein recognition, at first. Then, the threshold segmentation method and thinning method of hand vein image are deeply studied and a new threshold segmentation method and an improved conditional thinning method are proposed. The method of hand vein image feature extraction based on end points and crossing points is studied initially, and the matching method based on distances is used to match vein images.

Shi Zhao, Yiding Wang and Yunhong Wang, proposed [3] a biometric technique using hand-dorsa, extracting vein structures. For conventional algorithm, it is necessary to use high-quality images, which demand high-priced collection devices. The proposed method makes using low-cost devices possible. The results shown that they could extract the vein networks as successfully as using high-quality images

Masaki Watanabe, Toshio Endoh, Morito Shiohara, and Shigeru [4] have shown a biometric authentication using contactless palm vein authentication device that uses blood vessel patterns as a personal identifying factor. Implementation of these contactless identification systems enables applications in public places or in environments where hygiene standards are required, such as in medical applications. In addition, sufficient consideration was given to individuals who are reluctant to come into direct contact with publicly used devices.

3. Review

According to BIOGUARD (innovative biometric solutions) palm vein technology works by identifying the subcutaneous (beneath the skin) vein patterns in an individual's hand. When a user's hand is held over a scanner, a near-infrared light maps the location of the veins. The red blood cells (hemoglobin) present in the veins absorb the rays and show up on the map as black lines, whereas the remaining hand structure shows up as white. This vein pattern is then verified against a preregistered pattern to authenticate the individual. As veins are internal in the body and have a wealth of differentiating features, attempts to forge an identity are extremely difficult, thereby enabling a high level of security. Additionally, the sensor of the palm vein device can only recognize the pattern if the hemoglobin is actively flowing within the individual's veins.

3.1. Palm Vein Authentication Workflow

An individual inserts a smart card into the sensor device and holds her hand over the reader. The vein pattern is instantly captured using a completely safe near-infrared light. The reader converts the image into an encrypted biometric template and compares it against the template on the smart card (1 to 1 matching) or those in the database (1 to N matching).
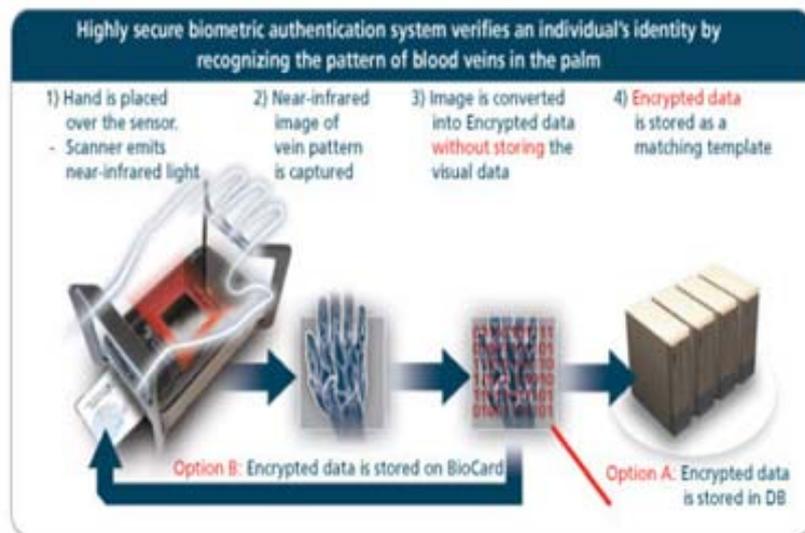

Figure 2. Palm Vein Authentication: How it works.

Using a built-in speaker, the device instructs the user to place his hand over the device and informs the user when the scan is complete. In the example below, the template is stored in a smart card. This enhances security since the template never leaves the card. Alternatively, the reference templates can be stored in a database on a server (1 to N matching).

The first step in all palm vein authentication applications is the enrollment process, which scans the user's palm and records the unique pattern as an encrypted biometric template in the database or on the smart card itself. In banking applications, for

example, once a new customer has been issued a smart card, he/she is asked to visit the bank in order to enroll her vein data.
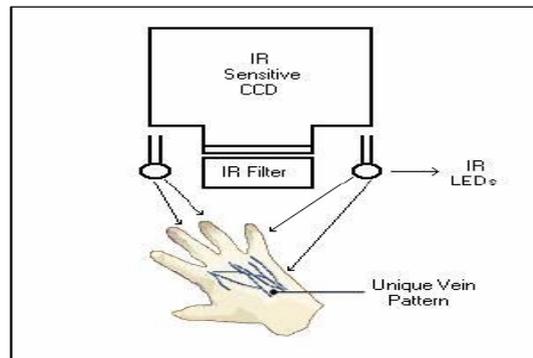

Figure 3. Schematic of the hand vein pattern imaging module.

Whereas Mohamed Shahin, Ahmed Badawi, and Mohamed Kamel proposed [5], biometric authentication using hand vein patterns, they designed a system a near IR cold source to provide back-of-hand illumination. The IR cold source is a solid-state array of 24 LEDs (light emitting diodes). The diodes are mounted in a square shape, 6 LEDs in each side, on a designed and assembled PCB (printed circuit board) and made housing and an attachment for fixing the LEDs around the CCD lens. Our experiments showed that the cold source provides better contrast than the ordinary tungsten filament bulbs. A commercially available, low cost, monochrome CCD fitted with an IR filter is used to image the back of hand. As shown in figure 2 and figure 3 show the system designed in [5], it gives the stages through which the image processed. Figure 4 shows the vein processing stages.
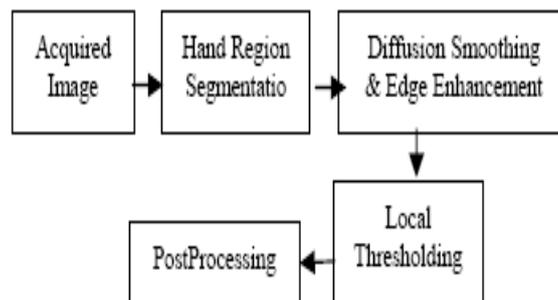

Figure 4. Block diagram of hand veins processing stage.

4. Comparisons

Comparing bioguard and Mohamed Shahin proposal [5], it seems bioguard palm vein technology provide advantages, such as:

Accuracy and Reliability – Uniqueness and complexity of vein patterns, together with advanced authentication algorithms, ensure unsurpassed accuracy. Field test

results show exceptionally low FTE (failure to enroll) rates, recognition attempt duration less than iris recognition, and near-zero false rejection and false acceptance rates.

Security – Vein patterns are internal and unexposed, making them almost impossible to duplicate or forge. Images are converted into encrypted biometric templates at the sensor level, preventing misuse of the actual image.

Contactless – Hygienic, non-invasive, "no touch" technology enables use when hands are dirty, wet or even wearing some types of latex gloves.

Cost-Effective – Attractively priced while saving you the huge potential costs of malpractice litigation, privacy violations, etc. Provides a high level of security at a reasonable cost.

Usability – Compact form factor provides greater flexibility and ease of implementation in a variety of security applications.

Application areas for palm vein technology are it supports variety of banking scenarios:

1. ATMs 2. Walk-in-customers 3. Internal branch security 4. Remote banking.

Whereas the advantages in [5] is that Hand Vein Verification System (HVVS) is accurate in the low to medium security level, these hand vein verification is purely system base, it's puts more effort on the overall performance of a system. These system checks the FAR(%)(false acceptance rate) and the FRR(%)(false rejection rate) with different threshold unit, to get the optimal threshold.

5. Results

As a result of the Fujitsu research using data from 140,000 palms (70,000 individuals), Fujitsu has confirmed that the FAR (false acceptance rate) is 0.00008% and the FRR(false rejection rate) is 0.01%, with the following condition: a person must hold the palm over the sensor for three scans during registration, and then only one final scan is permitted to confirm authentication.

In addition, the following data has been used to confirm the accuracy of this technology: data from 5-year to 85- year old people of various backgrounds based on statistics from the Ministry of Internal Affairs and Communications of Japan's population distribution; data from foreigners in Japan based on the world population distribution announced by the U.N.; data of the daily changes of Fujitsu employees tracked over several years; and data of various human activities such as drinking, bathing, going outside, and waking up.

Palm vein authentication technology offers contactless authentication and provides a hygienic and non invasive solution, thus promoting a high-level of user acceptance. Fujitsu believes that a vein print is extremely difficult to forge and therefore contributes to a high level of security, because the technology measures hemoglobin flow through veins internal to the body. The opportunities to implement palm vein technology span a wide range of applications.

6. Conclusions

Reliable personal recognition is critical to many applications in our day to day life. Biometrics refers to automatic recognition of an individual based on her behavioral

and/or physiological characteristics. It is obvious that any system assuring reliable personal recognition must necessarily involve a biometric component. This is not, however, to state that biometrics alone can deliver reliable personal recognition component.

Biometric-based systems also have some limitations that may have adverse implications for the security of a system. While some of the limitations of biometrics can be overcome with the evolution of biometric technology and a careful system design, it is important to understand that *foolproof* personal recognition systems simply do not exist and perhaps, never will. Security is a risk management strategy that identifies controls, eliminates, or minimizes uncertain events that may adversely affect system resources and information assets. The security level of a system depends on the requirements (threat model) of an application and the cost-benefit analysis.

As biometric technology matures, there will be an increasing interaction among the market, technology, and the applications. This interaction will be influenced by the added value of the technology, user acceptance, and the credibility of the service provider. It is too early to predict where and how biometric technology would evolve and get embedded in which applications. But it is certain that biometric-based recognition will have a profound influence on the way we conduct our daily business.

References

[1] "Palm Vein Authentication Technology" white paper, Bioguard, Innovative Biometric Solutions, March, 2007.

[2] Yuhang Ding, Dayan Zhuang and Kejun Wang, "A Study of Hand Vein Recognition Method", The IEEE International Conference on Mechatronics & Automation Niagara Falls, Canada, July 2005.

[3] Shi Zhao, Yiding Wang and Yunhong Wang, "Extracting Hand Vein Patterns from Low-Quality Images: A New Biometric Technique Using Low-Cost Devices", Fourth International Conference on Image and Graphics, 2007.

[4] Masaki Watanabe, Toshio Endoh,Morito Shiohara, and Shigeru Sasaki," Palm vein authentication technology and its applications", The Biometric Consortium Conference, September 19-21, 2005,USA, pp. 1-2.

[5] Mohamed Shahin, Ahmed Badawi, and Mohamed Kamel, "Biometric Authentication Using Fast Correlation of Near Infrared Hand Vein Patterns", International Journal of Biological and Medical Sciences, vol 2,No.1,winter 2007, pp. 141-148.