Journal of Universal Computer Science, vol. 15, no. 5 (2009), 1081-1089
submitted: 1/8/09, accepted: 28/2/09, appeared: 1/3/09 © J.UCS

Vascular Pattern Analysis towards Pervasive Palm Vein Authentication

Debnath Bhattacharyya
(Heritage Institute of Technology, Kolkata, India
debnathb@gmail.com)

Poulami Das
(Heritage Institute of Technology, Kolkata, India
dasp88@gmail.com)

Tai-hoon Kim
(Hannam University, Daejeon, Korea
taihoonn@empal.com)

Samir Kumar Bandyopadhyay
(University of Calcutta, Kolkata, India
skb1@vsnl.com)

Abstract: In this paper we propose an Image Analysis technique for Vascular Pattern of Hand Palm, which in turn leads towards Palm Vein Authentication of an individual. Near-Infrared Image of Palm Vein pattern is taken and passed through three different processes or algorithms to process the Infrared Image in such a way that the future authentication can be done accurately or almost exactly. These three different processes are: a. Vascular Pattern Marker Algorithm (VPMA); b. Vascular Pattern Extractor Algorithm (VPEA); and c. Vascular Pattern Thinning Algorithm (VPTA). The resultant Images will be stored in a Database, as the vascular patterns are unique to each individual, so future authentication can be done by comparing the pattern of veins in the palm of a person being authenticated with a pattern stored in a database.

Keywords: Authentication, Near-Infrared, biometric, Vascular Pattern, multimodal, signature and thinning
Categories: I.4.6, I.4.7, I.4.10, I.5.2, I.5.5

1 Introduction

Biometrics can be defined as the automatic recognition of a person using distinguishing characteristics or traits. Biometrics is used for human recognition which consists of authentication and verification.

Authentication may be defined as “providing the right person with the right privileges the right access at the right time”. In general, there are three approaches to authentication. In order of least secure and least convenient to most secure and most convenient, they are:

- Something we have - card, token, key.
- Something we know - PIN, password.

- Something we are - a biometric.

Any combination of these approaches further heightens security. Requiring all three for an application provides the highest form of security.

In a verification application, the biometric system requires input from the user, at which time the user claims his identity via a password, token, or user name (or any combination of the three). This user input points the system to a template in the database. The system also requires a biometric sample from the user. It then compares the sample to or against the user-defined template. This is called a "one-to-one" search (1:1). The system will either find or fail to find a match between the two.

Automatic identification and authentication systems that make use of biometric data, such as, distinctive anatomical and behavioral characteristics, are becoming ever more widely used for access control, surveillance, computer security, and in law enforcement. Several governments are now using or will soon be using biometric technology. The U.S. INSPASS immigration card and the Hong Kong ID card, for example, both store biometric features for authentication. Measured against alternative approaches, current automatic biometric systems are reliable, efficient, convenient and secure [Zhang, 07].

Biometric recognition or, simply, biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics [2]. By using biometrics, it is possible to confirm or establish an individual's identity based on "who she is", rather than by "what she possesses" (e.g., an ID card) or "what she remembers" (e.g., a password).

What biological measurements qualify to be a biometric? Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- Universality: each person should have the characteristic.
- Distinctiveness: any two persons should be sufficiently different in terms of the characteristic.
- Permanence: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.
- Collectability: the characteristic can be measured quantitatively.

However, 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 practical biometric system should meet the specified recognition accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system [Jain, 04].

There are many different types of Biometrics, these are, IRIS Identification, Retinal Identification, Face Recognition, Speaker/Voice Recognition, Fingerprint, Hand/Finger Geometry, Signature verification, Keystroke Dynamics, and other esoteric biometrics (Odor, Gait, and Ear).

2 Previous Works

Biometrics is not new. Biometrics is used - in Border Security, to avoid Multiple enrollments, to catch Financial fraud, and for User convenience. In general, Biometric features are always varied from person to person. So, Biometrics is more used for human identification.

Following reasons can be considered for the increasing popularity in Biometrics:

- An estimated 10,000 British passports were issued after fraudulent applications in the space of a year. Dhiren Barot, the most senior al-Qaida terrorist ever captured in Britain, had 7 passports in his true identity and 2 further passports in fraudulent identities. 290,000 passports issued by UK were lost/stolen in 2006.
- 40% of user-chosen passwords are readily guessable by programs.
- Personal data is routinely lost & stolen.
- According to The Straits Times, Singapore, March 20, 2007, a complete identity (govt. issued ID, US bank account and new DOB) can be bought for $14.
- Identity thieves steal customer ID & pw to create financial nightmare for customers; 8.9 million ID thefts in U.S. in 2005 resulting in $56.6 billion losses.

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 Biometric Recognition. Figure-1 shows the various Biometric systems.

Toshiyuki Tanaka, Naohiko Kubo, 2004, [Tanaka, 04] proposed the certification system that compared vein images for low-cost, high speed and high-precision certification. The equipment for authentication consists of a near infrared light source and a monochrome CCD to produce contrast-enhanced images of the subcutaneous veins. They adopted phase only correlation and template matching as a recognition algorithm. They tested several noise-reduction filters, sharpness filters and histogram manipulations for best effort.

Yuhang Ding, Dayan Zhuang and Kejun Wang, July 2005, have shown [Ding, 05] 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.

Junichi Hashimoto, 2006, has introduced [Hashimoto, 06], 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.

Suleyman Malki, Yu Fuqiang and Lambert Spaanenburg, August 2006, has considered [Malki, 06], an existing feature extraction algorithm, which has been developed for fingerprint recognition, is adapted for vein recognition. The algorithm has been implemented as Cellular Neural Network and realized on a Field-Programmable Gate-Array. The detection quality is comparable to the 99.45% reached earlier by direct image comparison, but suffers from the image resolution sensitivity of the False Feature Elimination.

Shi Zhao, Yiding Wang and Yunhong Wang, proposed [Zhao, 07] 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. The principle of vein imaging is discussed, a new method to acquire vein images, which could enhance the contrast, is proposed, and the algorithm of extracting the vein pattern from low quality images is put forward. They also proposed a novel denoising algorithm.

Finger Print Biometric Sensor Card Palm Print Face Recognition

Figure 1: various Biometric Systems

David Mulyono, Horng Shi Jinn, 2008, has introduced [Mulyono, 08] preliminary process to enhance the image quality worsened by light effect and noise produced by the web camera, then segment the vein pattern by using adaptive threshold method and matched them using improved template matching. The experimental result shows that even the image quality is not good, as long as the veins are clear and also with some appropriate process it still can be used as the means of personal identification.

Kornelije Rabuzin, Miroslav Baca and Mirko Malekovic, October 2007, have shown [Rabuzin, 07] how the concept of complex events presented in the active database theory could be used in order to build a multimodal biometric system. Especially, they explored the paradigm of active rules and complex events, and applied them in order to implement a multimodal biometric system.

3 Our Work

The pattern of blood veins is unique to every individual, even among identical twins. Palms have a broad and complicated vascular pattern and thus contain a wealth of differentiating features for personal identification. Furthermore, it will not vary during the person's lifetime. It is a very secure method of authentication because this blood vein pattern lies under the skin. This makes it almost impossible for others to read or copy.

Benefits of palm vein biometric systems are: a. Difficult to forge; b. Contactless, hygienic and non-invasive; c. Highly accurate; d. Capable of 1:1 and 1:many matching.

The Fujitsu palm vein contactless biometrics system is already used by Bank of Tokyo-Mitsubishi (BTM) in Japan. According to the Fujitsu Whitepaper, June 2005, hemoglobin in the blood is oxygenated in the lungs and carries oxygen to the tissues of the body through the arteries. After it releases its oxygen to the tissues, the deoxidized hemoglobin returns to the heart through the veins. These two types of hemoglobin have different rates of absorbency. Deoxidized hemoglobin absorbs light at a wavelength of about 760 nm in the near-infrared region. When the Palm of the hand is illuminated with near-infrared light, unlike the image seen by the human eye, the deoxidized hemoglobin in the hand veins absorbs this light, thereby reducing the reflection rate and causing the veins to appear as a black pattern (Figure 1). In vein authentication based on this principle, the region used for authentication is photographed with near-infrared light, and the vein pattern is extracted by image processing and registered. The vein pattern of the person being authenticated is then verified against the preregistered pattern.

Usually, in the image-based biometric systems, a number of pre-processing tasks are required prior to enhance the image quality, such as: contrast, brightness, edge information, noise removal, sharpen image, etc, furthermore, to produce a better quality of image that will be used on the later stage as an input image and assuring that relevant information can be detected [11]. Actually, the better quality of image will gain the better accuracy rate to the biometric system itself. In this paper we propose three required pre-processing tasks which are as follow:

3.1 Vascular Pattern Marker Algorithm

a. Open Near-Infrared Palm Image File in input mode

b. Convert the Loaded Image into PlanarImage

c. Set the Horizontal and Vertical kernels (3 x 3), respectively as follow:

$$\begin{matrix} 1 & 0 & -1 \\ 3 & 0 & -3 \\ 1 & 0 & -1 \end{matrix}_{3 \times 3} \qquad \begin{matrix} 1 & 3 & 1 \\ 0 & 0 & 0 \\ -1 & -3 & -1 \end{matrix}_{3 \times 3}$$

d. Generated PlanarImage in Step-b, is passed through kernels created in Step-c.

e. Modified fine-grained PlanarImage is stored into another Grayscale Image File.

f. Close all Image file(s).

Here we are considering monochrome binary Image, two-pass masking is used, namely, Horizontal and Vertical kernels. The PlanarImage now passed through these masks or kernels. Resultant transformed Image generates the distinct marks of Vascular Pattern; the process is Smoothing the Image.

3.2 Vascular Pattern Extraction Algorithm

```
a.  Open resultant Grayscale Image File from Algorithm 3.1, in input mode
b.  Open Binary Image File in output mode
c.  While not End of File
d.  Loop
e.      Read pixel intensity value
f.      If pixel intensity value lies in between 20 and 130, then
g.          Convert the intensity value to 0 (black)
h.      Else
i.          Convert the intensity value to 255 (white)
j.      End if
k.      Write the intensity value to Binary Image
l.  End Loop
m.  Close all Image Files
```

Thresholding is an image processing technique for converting a grayscale or color image to a binary image based upon a threshold value. If a pixel in the image has an intensity value less than the threshold value, the corresponding pixel in the resultant image is set to black. Otherwise, if the pixel intensity value is greater than or equal to the threshold intensity, the resulting pixel is set to white. Thus, creating a binarized image, or an image with only 2 colors, black (0) and white (255). Image thresholding is very useful for keeping the significant part of an image and getting rid of the unimportant part or noise. This holds true under the assumption that a reasonable threshold value is chosen. In our case the threshold range is taken 20 to 130.

3.3 Vascular Pattern Thinning Algorithm

a. Open the Resultant Binary Image File generated from Algorithm 3.2, in input mode

b. Read each pixel intensity value and stored into corresponding location of a 2 dimensional Matrix

c. Matrix processing as following steps:

```
int rows = Image Width, columns = Image Height;
        for(int i = 0; i < rows; ++i)
        {
                for(int j = 0; j < columns; ++j)
```

```
            {
              if((i==0) || (j==0) || (i==(rows-1)) || (j==(columns-1)))
                        matrix[i][j] = -1;
            }
}
for(int r = 1; r < rows-1; r++)
{
   for(int c = 1; c < columns-1; c++)
   {
     if((matrix[r][c] != -1))
     {
              if (((matrix[r][c+1] != -1) || (matrix[r][c-1] != -1)) &&
                        ((matrix[r+1][c] != -1) || (matrix[r-1][c] != -1)))
              {
                        matrix[r][c] = -1 ;
              }
      }
    }
}
for(int r = 1; r < rows-1; r++)
{
   for(int c = 1; c < columns-1; c++)
   {
     if((matrix[r][c] != -1))
     {
              if(((matrix[r][c-1] == -1)) && ((matrix[r][c+1] == -1)))
              {
                if(((matrix[r-1][c] == -1)) && ((matrix[r+1][c] == -1)))
                {
                        matrix[r][c] = -1;
                }
              }
       }
    }
  }
```

d. Write the 2 Dimensional Matrix into a Binary Image File.
e. Close all Image Files

Generated Binary Image is stored in the Image Database. For each individual one or multiple images are required to be stored. More Images for an individual are desired for perfect Identification of the corresponding individual in future. Thinning is done for capturing the Vascular Pattern of hand Palm of an individual.

4 Result

Due to the unavailability of Hand Palm Image Database, we have considered 8 different individuals Hand Palm Images. One such example is shown in Figure-2 to

Figure-5. The Near-Infrared Image of a Hand Palm is shown in Figure-2, this Image is then processed by Vascular Pattern Marker Algorithm; resultant image is shown in Figure-3. Output of Vascular Pattern Extractor Algorithm is shown in Figure-4, where extracted Vascular Pattern is well marked. Finally, output of thinning Algorithm is shown in Figure-4. This is important for our future work, that is, Authentication Method.

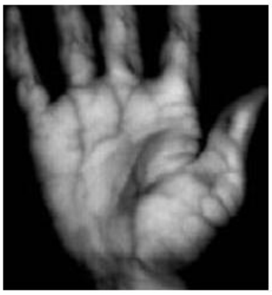

Figure-2: Near-Infrared Image of Hand Palm

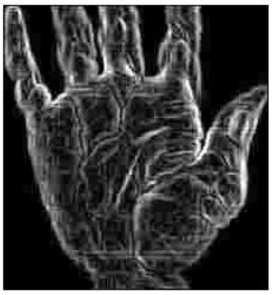

Figure-3: Complex vascular Pattern

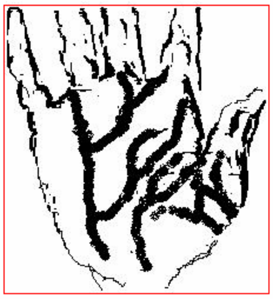

Figure-4: Extracted vascular Pattern

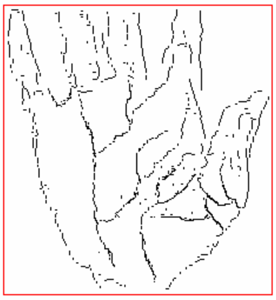

Figure-5: Thinned vascular Pattern

5 Conclusion

We propose three different algorithms for processing Palm Vein Pattern Image of an individual. This processed Image will be used for future authentication. We have already started Statistical Analysis for authentication. Our propose algorithms have been implemented, supplying results in polynomial time. The algorithms are proved to improve the recognition performance with different training samples.

6 Future Work

Applications of palm vein biometrics are: a. Security systems: physical admission into secured areas; b. Log-in control: network or PC access; c. Healthcare: ID verification for medical equipment, electronic record management; d. Banking and financial services: access to ATM, kiosks, vault.

We have already started the work which can be useful for any one above mentioned sectors.

Acknowledgement

We (first and second authors) extend our deep respect and gratitude to our guides Prof. Samir Kumar Bandyopadhyay and Prof. Tai-hoon Kim for their valuable advise and support throughout the development of this work. We are grateful to The Heritage Institute of Technology, the organization we serve in, for its wonderful laboratories where one can culminate oneself. Finally, we thank all our colleagues for their tremendous support and help in creating a very encouraging and creative environment to work in.

We express our whole-hearted thanks and respect to Prof. Tai-hoon Kim, Hannam University, Korea, for his unconditional support to make us carry out this research work.

References

[Ding, 05] 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, pp. 2106-2110.

[Hashimoto, 06] Junichi Hashimoto, “Finger Vein Authentication Technology and its Future”, 2006 Symposium on VLSI Circuits Digest of Technical Papers, 2006, pp. 5-8.

[Jain, 04] Anil K. Jain, Arun Ross and Salil Prabhakar, “An Introduction to Biometric Recognition”, *IEEE* Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004, pp. 4-20.

[Malki, 06] Suleyman Malki, Yu Fuqiang, Lambert Spaanenburg, “Vein Feature Extraction Using DT-CNNs”, 10th International Workshop on Cellular Neural Networks and Their Applications, Istanbul, Turkey, 28-30 August 2006, pp.1-6.

[Mulyono, 08] David Mulyono, Horng Shi Jinn, “A Study of Finger Vein Biometric for Personal Identification”, International Symposium on Biometrics and Security Technologies, 2008, 23-24 April, 2008, Islamabad, pp. 1-8.

[Rabuzin, 07] Kornelije Rabuzin, Miroslav Baca and Mirko Malekovic, “A Multimodal Biometric System Implemented within an Active Database Management System”, Journal of Software, Vol. 2, No. 4, October 2007, pp. 24-31.

[Tanaka, 04] Toshiyuki Tanaka, Naohiko Kubo, “Biometric Authentication by Hand Vein Patterns”, SICE Annual Conference, Sapporo, August 4-6, 2004, pp. 249-253.

[Zhao, 07] 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, pp. 667-671.

[Zhang, 07] David Zhang and Wangmeng Zuo, “Computational Intelligence-Based Biometric Technologies”, *IEEE* Computational Intelligence Magazine, May 2007, pp. 26-36.