Authentication Using Finger Vein Scanner

Nilesh Phand¹, Sagar Ambale² & Kaustubh Joshi³
Savitribai Phule Pune University, ICEM,
Post Parandwadi, PUNE-410507, India

Abstract: A biometric system is popular as its high security level manage to reduce frauds and unauthorized entry. Vein is one of the recent biometric technology. The vein features are stable and unique for every individual person and duplication of it is impossible. The vein Authentication system authenticates an individual’s identity based on the vein pattern. This technique overcomes the limitations of the Finger print technology. The main aim of this project is reduced the cost of vein scanning device. Vein Authentication System shows the information of authorized person.

Keywords—vein authentication, biometrics, Image pre-prepossessing, NIR, Image Acquisition.

1. Introduction

Authentication is a method of awarding yourself as a user to the system where as Authentication is used to verify you are the requested user. Authentication is in different methods they are shown below [6];
- Something the user has - such as bank cards;
  e.g.: id card.
- Something the user knows - such as password;
  e.g.: xyz@123.
- Something the user is - such as biometrics;
  e.g.: Fingerprint.

Vein Authentication is based on a unique vein network. Vein is defined as the use of biological or physical characteristics to identify a person. Vein patterns are unique to each individual, if there are two matching twins they don’t have same vein pattern. The replacement of vein pattern is unbearable as compared to other biometric technologies. Because veins are located inside the skin of body, so it is difficult to read. Veins authentication doesn’t leave any hint at the authentication process time and so it cannot be copied. Veins pattern comparatively constant through the childhood age to adult age so that re-enrollment of the vein pattern will not be required once it enrolled. On veins pattern, there is no any effect of climate or physical condition like Rushes, cracked, Oily skin and rough skin do not affect the result of authentication.

2. Image Acquisitions

Image acquisition for vein authentication is the process that to capture good images of user. Each person inserts hand into the device containing a near-infrared (NIR) LEDs (wavelengths between 760 to 900 nm), infrared lights and webcam is fitted at the base of device (bottom side). And we use the NIR filter for better Image quality which is put on camera. Hence, the veins that contain a concentration of blood flow appear as dark areas in the image taken by a webcam. Figures 2(a) show structure of acquisition device. And Figure 2(b) shows the Actual capture image of that device. This image is processed by image processing.

Figure 2(a)- vein scanner architecture.
3. Image Processing

3.1 Image Normalization

To achieve high accuracy the original image is normalized into smaller size. E.g. The original image size of 640x480 pixels is reduced to a smaller size, 384x288 pixels.

3.2 ROI Extraction

Edge detection is made to detect the edge points. Image is cropped vertically and horizontally. Below Figure 3 shows Region of Interest Extraction. Figure 3(a) shows actual captured image; Figure 3(b) shows edge detection image and Figure 3(c) shows cropped image.

3.3 Image Enhancement

This step is to highlight the vein pattern and raise the contrast in order to the matching correctness. Contrast limited adaptive histogram equalization (CLAHE) is used to develop the image. By using CLAHE method, vein image is much clear to higher accuracy. Figure 4(a) vein image before and Figure 4(b) after image enhancement [10].

3.4 Image Matching

The real-time image is to match with the database images. Whenever the new image is captured the image will goes in all the test and finally matched with the images in the database also with the threshold and produce a matching score percentage of the new image with the registered image. Only if there is 100% matched the verification will be accepted else the equivalent information will not be displayed.

3.4.1 Algorithm:

Euclidian distance is calculated for both the images – the image to be tested and the image from database. Below formula is used to calculate the Euclidean distance of Images:

$$D (p, q) = [(x-s)^2+(y-t)^2]^{1/2}$$

where, p & q are images.

If the Euclidean distances of both the images match each other, then the user is authenticated otherwise not. If the distances do not match then user is not identified or not-authenticated and he/she is denied access to the system.

Figure 2(b)- Captured image.

Figure 3- ROI Extraction

(a) (b) (c)

Figure 4- (a) Before Enhancement (b) After Enhancement

Figure 3(a) actual captured image; Figure 3(b) edge detection image and Figure 3(c) cropped image.
3.4.2 Modules:
In Vein Authentication System has two stages
- Verification stage
- Registration stage
For both stages includes vein image pre-processing, which includes Image Normalization, ROI, image segmentation, image enhancement then stored in database. The Registration stage is register user info to the system; first it takes the info and vein image from the Image Acquisition device. The verification stages are also get a loginID and vein image from image acquisition device, then match with database images. If Image is match, then shows the user information like Aadhar card.

4. Mathematical Model
Let S be the Whole system which consists:
$$S = \{st, en, IP, OP, DD, NDD, fme, success, failure\}$$
Where,
- \(st\) = Start State System
- \(en\) = End State System
- \(IP\) = Input Analysis
- \(OP\) = Output Analysis
- \(DD\) = Deterministic Data
- \(NDD\) = Non-Deterministic Data

**Input Analysis:**
\(IP \rightarrow \) is the input to the system
\(IP = \{u, dob, g, e, ph, id, n\}\)
Where,
- \(u\) = user name.
- \(dob\) = date of birth.
- \(g\) = gender.
- \(e\) = email
- \(ph\) = phone number.
- \(id\) = LoginID
- \(n\) = Scan images for registration.

**Procedure set:**
\(fme \rightarrow\) procedure applied to the system to process the given input.
\(fme = \{in, re, ie, vl, au\}\)
Where,
- \(in\) = process of image Normalization.
- \(re\) = process of ROI Extraction.
- \(ie\) = process of image Enhancement.
- \(vl\) = process of verifying userID entered input correct or not.
- \(au\) = process of authentication Successfully or not

**Output Analysis:**
\(OP \rightarrow\) is the output of system.
\(OP = \{au\}\)
Where,
- \(au\) = Authorized person or not.

**Success Case:**
\(S \rightarrow\) case of success
\(S = \{accept\}\)
Where,
- accept = only registered user get access to the system.

**Failure Case:**
\(F \rightarrow\) case of failure
\(F = \{ip\}\)
Where,
- \(ip\) = incorrect images captured at time of login.

5. Advantages
I. Internal Nature- Temperature and Humidity have no effect.
II. Non-Traceable- Veins are inside the body, invisible to the eye, and not accessible. Therefore, it is extremely difficult to change.
III. Harmless- Detection method doesn’t have any negative effect.
IV. Secure- Oiliness, roughness of the skin also has no effect on the vein pattern authentication.
V. Small- Image Acquisition devices is small size device.

6. Conclusion
Security is becoming important in all kind of application. This proposed work will to improve the security level. As the vein is use for private authentication in terms of its safety. The vein is inside the body and is mostly unseen to human eyes, so it is difficult to thief. So, this system is might be expectant in improving the security level.

Vein authentication technology has high safety as compared to the other authentication biometric methods. It also can be applied in public to store the criminal records and student or employee records.

REFERENCES


