BIOMETRIC AUTHENTICATION SYSTEM USING FINGER VEIN

Mr.T.Thirumal Valavan[1], Ms.R.Kalaivani[2]

[1] PG Student, [2]Assistant Professor , Department of Computer Science and Engineering,

PRIST University, Trichy District, India

thirumal_valavans@yahoo.com

ABSTRACT

The research has been done by us long time in the field of finger print recognition. Earlier we used infrared with VGA camera for capturing finger print and there was some questions that were the result good and was it acceptable and secure?. Because of this problem the finger vein recognition came to light. Finger vein authentication is a new biometric method utilizing the vein patterns inside one's fingers for personal identity verification. Vein patterns are different for each finger and for each person. Virtually all biometric methods are implemented using the following 1) sensor, to acquire raw biometric data from an individual; 2)feature extraction, to process the acquired data to develop a feature-set that represents the biometric trait; 3)pattern matching, to compare the extracted feature-set against stored templates residing in a database; and 4) decision-making, whereby a user's claimed identity is authenticated or rejected. This paper discusses the origins, basic working principles, technology features and drawbacks and future development of GSM based sms alert .

1. INTRODUCTION AND HISTORY

HISTORY

Recognition technology was born of Hitachi's advanced research to measure brain-function activity in the field of medical science. In that research, near-infrared light was used to observe the increase in blood flow and was found to be applicable to recognition of the finger vein pattern. As finger vein patterns differ for each finger and for each person, Hitachi thus discovered that finger vein pattern recognition is a viable biometric personal authentication technology for the commercial market.

In the first phase (1997-2000), Hitachi developed its original light transmission technology for finger vein biometric authentication. As opposed to light reflection, whereby a captured image is taken from light reflected off the surface of the skin, light transmission captures a vein pattern image from light that passes through the surface of the skin (see Section 4 for details). In the second phase (2000-2003), the technology was adapted into product form, and the first physical access control system was developed and released in 2002. In 2002 research began on the logical access systems, with commercialization in Japan beginning in 2004.

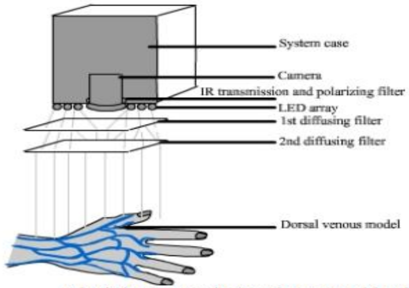
Hitachi developed ATM applications in 2004 and commercialized them in 2005. Finger vein authentication technology has thrived in the Japanese financial sector, with major banks in Japan employing it for ATM end-user verification.

INTRODUCTION

A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from specific physiological or behavioral characteristic that the person possesses [1]. A vein pattern detection has been proved to fully comply with this definition [2,3] and it provides many important biometric features:

- uniqueness and permanence of the pattern
- non-contact detection procedure
- almost impossible to forge or copy.
- The biometric parameter is hidden from general view
- The vein pattern is instigate enough to allow sufficient criteria for positively detecting various subjects even identical.

The vein detection process consists of an easy to implement device that takes a snapshot of the subject's veins under a source of infrared radiation at a specific wavelength. The system is able to detect veins but not arteries due to the specific absorption of infrared radiation in blood vessels. Almost any part of the body could be analyzed in order to extract an image of the vascular pattern but the hand and the fingers are preferred. The reason for this choice is the general availability of the hand. A sketch of an actual vein detection system is shown in figure 1.



A basic hardware vein detection system (sketch)

Fig 1

The infrared radiation is absorbed in a different way in various types of tissue. In order to achieve visual penetration through the respective tissue, lighting should be performed under a very tight optical window namely 740nm up to 760nm (inside the near infrared part of the electromagnetic radiation spectrum). Because of the optical properties of the human tissue, a near-IRvein scanning device cannot penetrate very deep under the skin therefore the device will recognize the superficial veins and rarely the deep veins. Good candidates for the scanning procedure are the dorsal metacarpal veins and the general dorsal venous network. A statistical maximum penetration distance is 3mm and this poses some limitations on the quantity and quality of the extracted vein pattern. Two basic optical coefficients are involved in this absorption process: - absorption coefficient $\propto a$ - scattering coefficient $\propto s$. The absorption coefficient $\propto a$ determines how far light can travel before loosing its intensity while still in its original path, and, the scattering coefficient $\propto s$ determines how far light can travel before losing its original phase and changes direction. Taking these optical properties into account it is obvious that the lighting source should be uniform throughout the region of interest, the degree of illumination should be kept constant for different acquisitions and the contrast of the resulting image should be sharp enough to reduce the need for complex post processing image algorithms.

2. SUMMARY OF AUTHENTICATION PROCESS

The basic principle on which the finger vein authentication system is based is shown in Fig. 2. Near-infrared rays generated from a bank of LEDs (light emitting diodes) penetrate the finger and are absorbed by the haemoglobin in the blood. The areas in which the rays are absorbed (i.e. veins) thus appear as dark areas in an image taken by a CCD camera located on the opposite side of the finger. Image processing can then construct a finger vein pattern from the camera image. This pattern is compressed and digitized so that it can be registered as a template of a person's biometric authentication data. The finger vein pattern and the template are then authenticated by means of a pattern-matching technique. Devices were developed by Hitachi to perform the detection process described above.

3. IMAGE ACQUISITION

To obtain high quality near-infrared (NIR) images, a special device was developed for acquiring the images of the finger-vein without being affected by ambient temperature. Generally, finger-vein patterns can be imaged based on the principles of light reflection or light transmission [8]. We developed a finger-vein imaging device based on light transmission for more distinct imaging.

Our device mainly includes the following modules: a monochromatic camera of resolution 580 × 600 pixels, daylight cut-off filters (lights with the wavelength less than 800 nm are cut off), transparent acryl (thickness is 10 mm), and the NIR light source. The structure of this device is illustrated in Fig. 3. The transparent acryl serves as the platform for locating the finger and removing uneven illumination. The NIR light irradiates the backside of the finger. In [9], a light-emitting diode (LED) was used as the illumination source for NIR light. With the LED illumination source, however, the shadow of the finger-vein obviously appears in the captured images. To address this problem, an NIR laser diode (LD) was used in our system. Compared with LED, LD has stronger permeability and higher power.

In our device, the wavelength of LD is 808 nm. Fig. 2 shows an example raw finger-vein image captured by using our device.

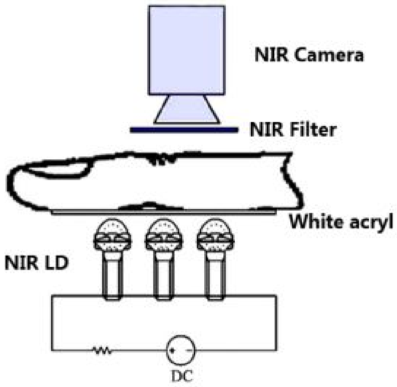
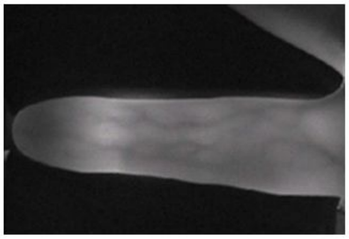


Illustration of the imaging device.

Fig 2



An example raw finger-vein image captured by our device.

4. FINGER VEIN AUTHENTICATION PROCESS

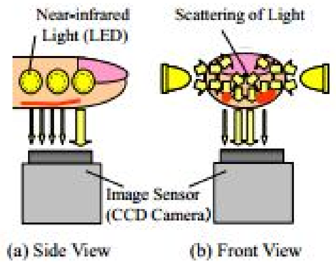
Fig. 5 shows a block diagram of the complete finger vein authentication system. The system consists of an authentication unit and other related devices in addition to the near-infrared light source and the image sensor . The authentication unit includes a CPU core for all sorts of signal processing, video I/O for capturing data from the image sensor, LED power controller, and I/O controller. The authentication outcome flows through the I/O controller. Security applications such as door locking are activated by the signal from the controller.

The system executes four tasks:

(1) Capturing of finger vein pattern image,

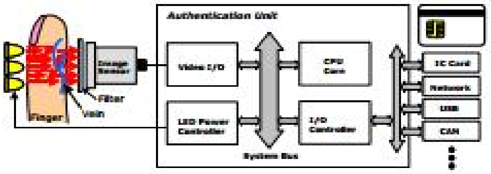
(2) Normalization of the image,
(3) Feature pattern extraction from the image, and
(4) Pattern matching followed by judgment of outcome.

In Task (1), the system takes an image of the finger vein pattern through the image sensor and transfers the image data to the memory of the CPU. At this point, the CPU adjusts the brightness of the light source through the LED power controller to eliminate error caused by individual variations or environmental fluctuations.



Task (2) normalizes the finger vein image to accommodate geometric changes in the positioning or angle of the finger used for authentication. In practical terms, the outline of the finger in the image is detected and then the entire image is rotated so that the slope of the outline remains constant.

In Task (3), the distinctive feature patterns are extracted from the image. This process is essential for reliable authentication so as to control the variation of image data caused by body metabolism or changes in imaging conditions. In particular, uneven brightness due to individual variations in finger size or lighting conditions often appears in the vein pattern image, so the system must extract only the vein patterns from such an otherwise unstable image. (Fig. 3 shows variations in brightness across a single vein in a vein pattern image, where veins clearly appear as dark lines. The shape of the variation forms a 'valley'.)



Block Diagram of Finger Vein Authentication

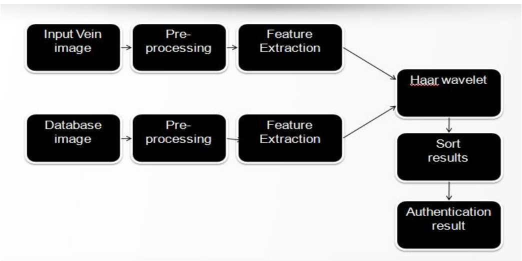
Fig 3

Task (4) calculates the correlation between the extracted feature pattern and the registered pattern in a database – the "matching" process. If the correlation value is higher than a pre-defined threshold value, the vein pattern is authenticated.

The vein pattern image and the extracted feature pattern represent ultimate personal information. Therefore, strict administration of that information is required when it is stored or transferred. In addition to encryption of the data, tamper resistance is necessary for the device against unauthorized access to the system.

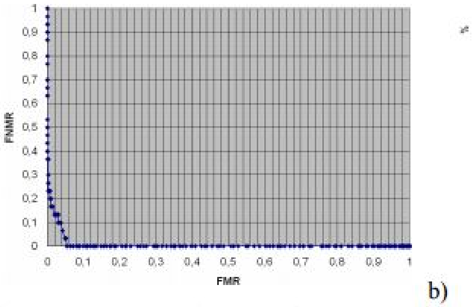
A smart card, which includes high–level tamper resistance, has already been introduced to store the feature pattern. The internal program execution function of the smart card has been used to execute all or a part of the pattern matching process so that no personal information leaks out from the card. The authentication accuracy of the system is less than 0.01% for FRR (False Rejection Rate), and less than 0.0001% for FAR (False Acceptance Rate). These accuracy figures are superior to those of other methods based on fingerprint or iris recognition.

5. COMPARISION OF VEIN IMAGES



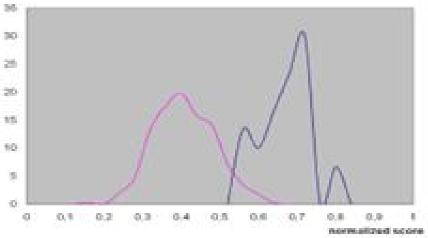
6. EXPERIMENTS

The described prototype was used for the preliminary tests. We had five volunteers at the disposal. The database contains ten different fingers; each was scanned three times. You can see the resulting DET curve in Fig. 4a and the corresponding impostor/genuine curves in Fig. 4b, respectively. As you can see, the results are very promising even in the case of preliminary scans. The minor inaccuracies were caused by an imperfect illumination of the finger top. This problem has already been solved at the present time. We work on a new prototype at the moment which will be suitable for testing of a larger group of volunteers. The range of the tests we are planning to do is in order of hundreds of volunteers



a) b)

Figure 4: a) Finger vein comparison – DET curve;

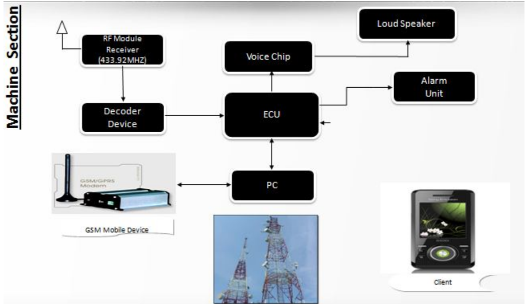


b) Finger vein comparison – genuine and impostor curves.

7. PROPOSED SYSTEM

HIGH ALERT GSM SMS

The Techniques GSM SMS is handled main role in this system of device in which the finger vein is captured and authenticated. This GSM sms alert to the user whose system is accessed by anyone with illegal. This is the technique which is very useful and also it has loud speaker for providing alert signal beep loudly. SMS Alert is new logical techniques for providing high level security for the users and this will be sent to their mobile phones.



8. CONCULSION

We designed, implemented and tested a new method for the finger veins detection and rec-ognition discussed with this paper. The results of our experiments proved that the promised potential of the proposed method is more preferred method . In the future, we are planning to perform much more detailed tests with hun-dreds of volunteers. We proposed a method for sms based alerts and we will apply it to the database of templates in order to improve accuracy of the device.

REFERENCE

[1] Vein pattern recognition. Image enhancement and feature extraction algorithms Septimiu Crisan, Ioan Gavril Tarnovan, Titus Eduard Crisan. Department of Electrical Measurement, Faculty of Electrical engineering, Technical University of Cluj-Napoca, Str.C.Daicoviciu nr.15, 400020 Cluj-Napoca, Romania, E-mail:crisans@mas.utcluj.ro
[2]Finger Vein Authenication : White Papper Hittachi ltd , 2006
[3] A. K. Jain, S. Pankanti, S. Prabhakar, H. Lin, and A. Ross, "Biometrics: a grand challenge", Proceedings of the 17th International Conference on Pattern ecognition (ICPR), vol. 2, pp. 935-942, 2004.
[4] P. Corcoran and A. Cucos, "Techniques for securing multimedia content in consumer electronic appliances using biometric signatures," IEEE Transactions on Consumer Electronics, vol 51, no. 2, pp. 545-551, May 2005.
[5]An Embedded Real-Time Finger-Vein Recognition System for Mobile Devices Zhi Liu and Shangling Song
[6] Feature Extraction from Vein Images using Spatial Information and Chain CodesAnika Pug1, Daniel Hartung2and Christoph Busch1;2anika.pflug@cased.dedaniel.hartung@hig.nochristoph.busch@hig.no