Researchers

P. Ghosh, R. Dutta

Department of Computer Science and Engineering

Department of Electronics and Communication Engineering

Surendra Institute of Engg. & Management, WBUT, Siliguri, India

Email-

papri.mss@gmail.com, ritam_siliguri@yahoo.com

A new approach towards Biometric Authentication System in Palm Vein Domain

Abstract:

Biometric Authentication is a system which deals with the physiological as well as behavioural characteristics of a person. Palm vein structure is unique for every human being even for the twins also. In this paper, firstly we made a comparison study among all different biometric authentication processes that are already been used presently. Secondly, we propose an Image Analysis technique for Vascular Pattern of Hand Palm, which in turn leads towards Palm Vein Authentication of an individual. A 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 more accurately. As an input a near-inferred image of palm vein pattern is taken and it is passed through different processes to implement authentication of an individual. The different processes are (i) Vascular Pattern Pointer Algorithm (VPPA), (ii) Vascular Pattern G-B Conversion Algorithm (VPGBCA) and (iii) Vascular Pattern Thinner Algorithm (VPTA). During first process a near-infrared image is converted into a grayscale image. In the second process the grayscale image is again converted into a binary image. Lastly, the processed binary image is finely thinned to get a proper thinned image. This VPTA process gives an edge to enrich the level of security of perfect biometric authentication to maximum level.

Keywords: Palm Vein, Biometric Authentication, Vascular Pattern, Infrared Image Processing, G-B Image Conversion.

Introduction

Authentication is a process by which a system verifies the identity of a user who wishes to access it. Since Access Control is normally based on the identity of the User who requests access to a resource, authentication is essential to effective security. The process of identifying an individual usually based on a username and password [1]. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual. Authentication may be implemented using Credentials, each of which is composed of a User ID and Password. Moreover, Authentication may be implemented with Smart Cards [2], an Authentication Server or even a Public Key Infrastructure. Users are frequently assigned (with or without their knowledge) Tickets, which are used to track their Authentication state. This helps various systems manage access control without frequently asking for new

VOLUME 1 NUMBER 2 (Mar/Apr 2012)
ISSN: 2277–1891

authentication information. The combination of authentication server and authenticator, which may be separate devices or both reside in the same unit such as an access point or network access server. The authentication server contains a database of user names, passwords and policies and the authenticator physically allows or blocks access. In a verification application, the authentication 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 stored data in the database. The system also requires a sample from the user. It then compares the sample to or against the user-defined data. This is called a "one-to-one" search (1:1). The system will either find or fail to find a match between the two as describes in Figure 1.

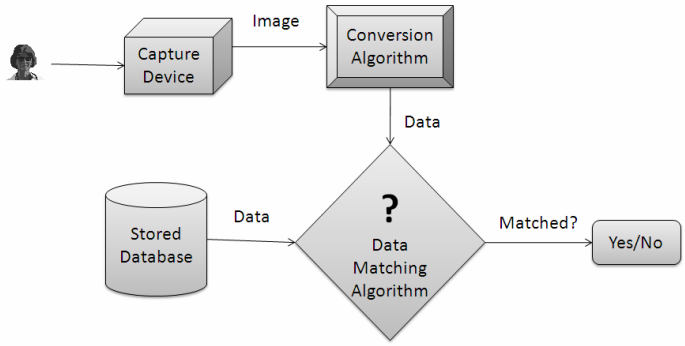

Fig.1 Authentication System Architecture

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:
a. Something we have – card, token, key.
b. Something we know-PIN, P/W.
c. Something we are – a biometric.
In our paper, the section II gives an overview of biometric authentication system. In section III various types of biometric authentication methods are discussed. In section IV a new proposed palm vein authentication process are discussed in details.

Overview of Biometric Authentication System

Biometric recognition or simply biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioural characteristics. 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 Smart Card) or "what she remembers" (e.g., a pin). What biological measurements qualify to be a biometric? Any human physiological and/or behavioural characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

(A) Universality: Each person should have the characteristic.

(B) Distinctiveness: Any two persons should be sufficiently different in terms of the characteristic.

(C) Permanence: The characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.

(D) Collectability: The characteristic can be measured quantitatively.

Biometric authentication [3] requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during a login). During Enrolment, as shown in the Figure 2, a sample of the biometric trait is captured, processed by a

VOLUME 1 NUMBER 2 (Mar/Apr 2012)
ISSN: 2277–1891

computer and stored for later comparison. Biometric recognition can be used in identification mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match based solely on the biometric. For example, an entire database can be searched to verify a person has not applied for entitlement benefits under two different names. This is sometimes called "one-to-many" matching. A system can also be used in Verification Mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching. 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:

(a) 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.

(b) Acceptability: Which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives.

(c) Circumvention: Which reflects how easily the system can be fooled using fraudulent methods.

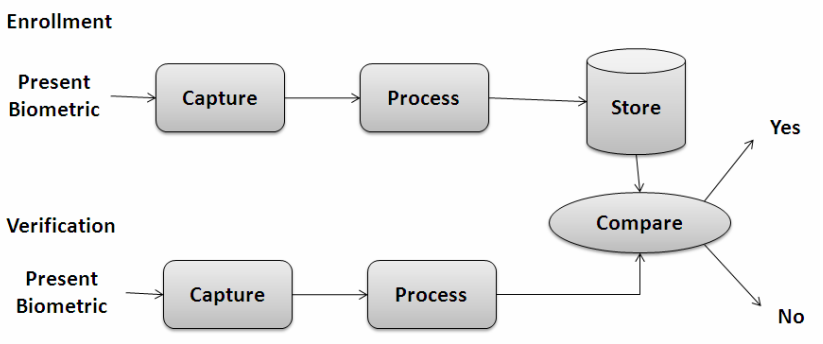

Fig.2 Biometric Authentication System Architecture

Different Types of Biometric Authentication

In today's era the different types of biometric authentication available to us as follows:

(A) Fingerprints Recognition System: Fingerprint verification or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints [4]. Fingerprints are one to many forms of biometrics used to identify individuals and verify their identity.

(B) Face Recognition System: A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database [5].

(C) Iris Recognition System: Iris recognition is an automated method of biometric identification [6] that uses mathematical pattern-recognition techniques on video images of the iris of an individual's eyes, whose complex random patterns are unique and can be seen from some distance [7].

(D)Retinal Scan Recognition System: Retina recognition technology captures and analyses the patterns of blood vessels on the thin nerve on the back of the eyeball that processes light entering through the pupil [8].

VOLUME 1 NUMBER 2 (Mar/Apr 2012)
ISSN: 2277–1891

(E)Voice Recognition System: It combines physiological and behavioural factors to produce speech patterns that can be captured by speech processing technology [9]. Inherent properties of the speaker like fundamental frequency, nasal tone, cadence, inflection, etc. are used for speech authentication [10].

(F) Hand Geometry Recognition System: It is a system which measures either physical characteristics of the fingers or the hands. These include length, width, thickness and surface area of the hand [11]. One interesting characteristic is that some systems require a small biometric sample (a few bytes). Hand geometry has gained acceptance in a range of applications. It can frequently be found in physical access control in commercial and residential applications, in time and attendance systems and in general personal authentication applications [12].

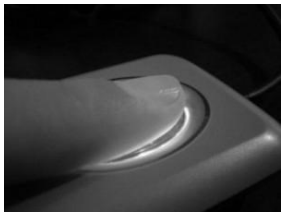

Fig. 3 (a) Fingerprint Recognition System

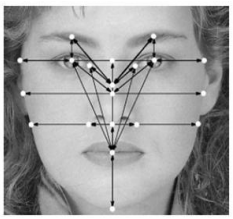

Fig.3 (b) Face Recognition System

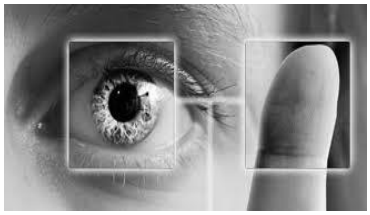

Fig. 3 (c) Iris Recognition System

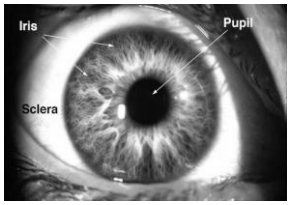

Fig.3 (d) Retinal Recognition System

Fig. 3 (e) Voice Recognition System

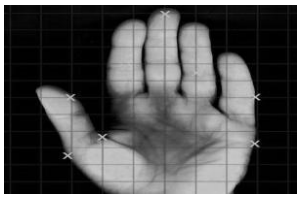

Fig.3 (f) Hand geometry Recognition System

Table 1: Comparing the several biometric types.

Comparison Table of a Biometric Systems			
S.No	**Name of System**	**Pros**	**Cons**
1	Fingerprint Recognition	Cheapest, fastest, most convenient	Forgery can be done
2	Face Recognition	Useful in automation systems	More expensive and complex than other methods
3	Iris Recognition	It is an unique process as it deals with iris	A person who has a color blindness cannot pass through this test
4	Retinal Scan Recognition	The retinal has also unique features but better than iris	Measurement accuracy can be affected by a disease such as cataracts
5	Voice Recognition	Very natural way to interact and No training required for users	More noise in the same place can make more errors
6	Hand Geometry Recognition	Simple, relatively easy to use and inexpensive	It is not unique and cannot be used in identification systems

VOLUME 1 NUMBER 2 (Mar/Apr 2012)
ISSN: 2277–1891

VOLUME 1 NUMBER 2 (Mar/Apr 2012)
ISSN: 2277–1891

Our Work

In Biometric Authentication Methodologies now a day's several Biometric Authentication System is being used for the security measures. In our paper, Palm Vein Authentication Systems is used as it is a much secured method of Authentication because the blood vein pattern lies under the human skin. This is the latest technology used for safety measures as per as Biometric Authentication is concerned. The pattern of blood veins is unique to every individual. Palms have a broad and complicated vascular pattern and thus contain a significant amount of differentiating features for personal biometric identification. In addition with, the latest palm vein technology becomes the most secured one as it will also not vary during the person's lifetime. According to the Fujitsu Whitepaper, June 2005, haemoglobin in the blood is oxygenated in the lungs and carries oxygen to the tissues of the body through the arteries [13]. After it releases its oxygen to the tissues, the deoxidized haemoglobin returns to the heart through the veins. These two types of haemoglobin have different rates of absorbency. Deoxidized haemoglobin 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 haemoglobin in the hand veins absorbs this light, thereby reducing the reflection rate and causing the veins to appear as a black pattern (Fig.6). 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 pre-registered pattern. In this paper we have used 512x512 – M2-PV Reader to capture near-infrared images of palm vein [14]. Here we propose three steps for proper Palm Vein Authentication process. The steps are discussed as follows:

(A) Vascular Pattern Pointer Algorithm (B) Vascular Pattern G-B Conversion Algorithm (C) Vascular Pattern Thinner Algorithm

(A) Vascular Pattern Pointer Algorithm (VPPA):

i. Open an Infrared Palm Image File in input mode.

ii. Convert the Loaded Image into Planar Image.

iii. The operator consists of a pair of 3×3 convolution kernels as shown in Figure 4. One kernel is simply the other rotated by 90°.

-1	0	+1
-2	0	+2
-1	0	+1

Gx

-1	-2	-1
0	0	0
+1	+2	+1

Gy

Fig.4 Masks used by Sobel Operator

iv. Generated Planar Image in Step-ii, is passed through kernels created in Step iii.

v. Modified fine-grained Planar Image is stored into another Greyscale Image.

These kernels are designed to respond maximally to edges running vertically and horizontally relative to the pixel grid, one kernel for each of the two perpendicular orientations. The kernels can be applied separately to

VOLUME 1 NUMBER 2 (Mar/Apr 2012)
ISSN: 2277–1891

the input image, to produce separate measurements of the gradient component in each orientation (call these Gx and Gy). These can then be combined together to find the absolute magnitude of the gradient at each point and the orientation of that gradient. The gradient magnitude is given by:

$$|G| = \sqrt{(Gx2 + Gy2)}$$

Typically, an approximate magnitude is computed using:

$$|G|=|Gx|+|Gy|$$

This is much faster to compute. The angle of orientation of the edge (relative to the pixel grid) giving rise to the spatial gradient is given by:

$$q = \arctan (Gy / Gx)$$

(B) Vascular Pattern GB Conversion Algorithm (VPGBCA):

A digital grayscale image can be represented as a matrix of corresponding pixel values. A pixel is a small block that represents the amount of gray intensity to be displayed for that particular portion of the image. For most integers the pixel integers values range from 0 (Black) to 255 (White) [15]. The 256 possible gray intensity values are shown in Figure 5.

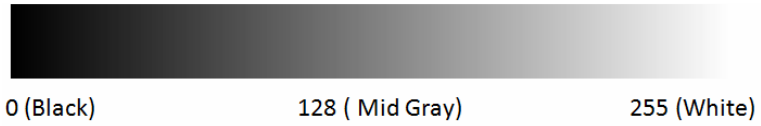

Fig.5 The range of intensity values from 0 (black) to 255 (white)

Using Vascular Pattern Pointer Algorithm, we get a grayscale image. We assume the resultant grayscale image file as gray.jpeg. Using the Vas_Pat_GBC_Algo we convert this gray.jpeg to a binary scale image as bin.jpeg.

```
Vas_Pat_GBC_Algo()
{
File *fg, *fb;
*fg=fopen("gray.jpeg","r"); //open gray image in read mode
*fb=fopen("bin.jpeg","w");//open binary image in write mode
while(!EOF of fg)
{
P←pixel intensity value;
if(p>=20&&p<=130)
p←0; // set to black
else
p←255; //set to white write the p to fb;
}
fclose(fg);
fclose(fb);
}
```


VOLUME 1 NUMBER 2 (Mar/Apr 2012)
ISSN: 2277–1891

(C) Vascular Pattern Thinner Algorithm (VPTA):

The proposed following algorithm is used for converting the 'bin.jpeg' into the 'thin.jpeg'. This 'thin.jpeg' file provides us a thinned vascular pattern which in turn could be very fruitful for enhancing the ultimate accuracy.

```
Vas_Pat_Thin_Algo()
{
File *fb, *ft;
*fb=fopen("bin.jpeg","r");
*ft=fopen("thin.jpeg","w");
int matsrc[100][100], maddest[100][100],r,c,i,j;
matsrc[][]←Pixel Intensity Value of fb;
r← Image Width;
c←Image Height;
while(!EOF of fb)
{
for(i=1;i<r-1;i++)
{
for(j=1;j<c-1;j++)
{
if((matsrc[i][j-1]==0 && matsrc[i][j]==0 &&
matsrc[i][j+1]==0)||(matsrc[i-1][j]==0&&
matsrc[i][j]==0&&matsrc[i+1][j]==0))
{
matdest[i][j]=0; // set to black
}
}
}
for(i=0;i<r;i++)
{
for(j=0;j<c;j++)
{
if((i==0)||(j==0)||(i==(r-1))||(j==(c-1)))
matdest[i][j]=255; //set to white
}
}
}
Ft←matdest[i][j]; //store the final value of maddest[i][j]
into thin.jpeg
fclose(fb);
fclose(ft);
}
```

Result:

In Figure 6 the near-infrared image of vascular pattern of hand palm is shown. Using VPPA algorithm we convert that image into a grayscale image shown in Figure 7. Then using VPGBCA algorithm the grayscale image is again converted into the binary image shown in Figure 8. Finally using VPTA algorithm the binary

image is converted into a thinned binary image (figure 9) which is to be stored in the hand palm image database.

Fig.6 Near-Infrared Image

Fig.7 Gray Scale Image

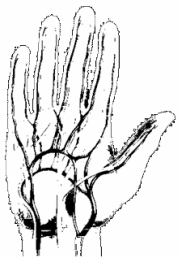

Fig.8 Binary Image

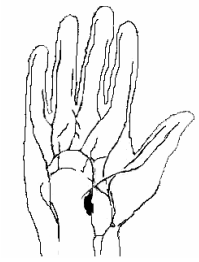

Fig.9 Thinned Binary Image

Conclusion

In this paper three different algorithms for processing palm vein pattern image are proposed. The algorithms have been implemented and also provide satisfactory results. Most importantly as our Vascular Pattern Thinner Algorithm is well programmed, tested & synthesized, therefore this can definitely give an edge towards more secure biometric authentication.

Future Scope

This project can be extended by matching the thinned binary images of vascular pattern of hand palm of an individual with the thinned images that are previously stored vascular pattern of hand palm image database. Moreover, this project can be applicable in different security systems such as physical admission into secured areas, log in control, ID verification in health care services, electronic record management, secure ATM accessibilities in financial services etc.

References

[1] Almuairfi, S.; Veeraraghavan, P.; Chilamkurti, N.; "IPAS: Implicit Password Authentication System" in Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference, DOI: 22-25 March 2011, pp. 430 – 435.

[2] Hung-Min Sun; "An Efficient Remote Use Authentication Scheme Using Smart Cards" in IEEE Transactions on Consumer Electronics, Vol. 46, No. 4, NOVEMBER 2000.

[3] Xiao, Q.; "A biometric authentication approach for high security ad-hoc networks" in Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC, DOI: 10-11 June 2004, pp. 250 – 256.

[4] Jain, A.K.; Lin Hong; Pankanti, S.; Bolle, R.; "An identity-authentication system using fingerprints" in Proceedings of the IEEE Conf., DOI: Sep 1997, Vol. 85, Iss.9 pp.1365 – 1388.

[5] Beumer, G.M.; Tao, Q.; Bazen, A.M.; Veldhuis, R.N.J.; "A landmark paper in face recognition" in Automatic Face and Gesture Recognition, 2006. FGR 2006. 7th International Conference, DOI: 2-6 April 2006, pp.78.

[6] Khin Sint Sint Kyaw; "Iris Recognition System Using Statistical Features For Biometric Identification" In Electronic Computer Technology, 2009 International Conference, DOI: 20-22 Feb. 2009, Pp. 554 – 556.

[7] Yikui Zhai; Junying Gan; Junying Zeng; Ying Xu; "A novel Iris recognition method based on the Contourlet Transform and Biomimetic Pattern Recognition Algorithm" in Signal Processing (ICSP), 2010 IEEE 10th International Conference, DOI: 24-28 Oct. 2010, pp. 1390 – 1393.

[8] Hoshino, K.; Mura, F.; Shimoyama, I.; "A one-chip scanning retina with an integrated micromechanical scanning actuator" in Microelectromechanical Systems, IEEE Journal, DOI: Dec 2001, Vol.10, Iss.4, pp.492 – 497.

[9] Osada, H.; "Evaluation method for a voice recognition system modelled with discrete Markov chain" in Communications, Computers and Signal Processing, 1997. 10 Years PACRIM 1987-1997 - Networking the Pacific Rim. 1997 IEEE Pacific Rim Conference, DOI: 20-22 Aug 1997, vol.2, pp. 600 – 602.

[10] Dutta, R.; Dutta, S.; Mitra, K.; "A VLSI Design Voice Recognition Technology Based Expert Security System Using Xilinx" in proceeding of International Conference on Information Technology, Electronics & Communications, 29-30 Nov. 2011, vol.1, pp.201-205.

[11] Sanchez-Reillo, R. Sanchez-Avila, C. Gonzalez-Marcos, A. "Biometric identification through hand geometry measurements" in Pattern Analysis and Machine Intelligence, IEEE Transactions, DOI: Oct 2000, Vol.22, Iss.10, pp.1168 – 1171.

[12] Kumar, A.; Zhang, D.; "Hand-Geometry Recognition Using Entropy- Based Discretization" in Information Forensics and Security, IEEE Transactions, June 2007, Vol.2, Iss.2, pp.181 – 187.

[13] http://www.prlog.org/10749514-m2sys-fujitsu-partner-to-accelerateworldwide- adoption-of-palm-vein-biometric-authentication-tech.html

[14] http://www.prlog.org/10749514-palm-vein-reader.jpg

[15] http://www.visionsystem.com/technology/machinevision_overview.php

Author Details:

Papri Ghosh

B.Tech. in Information Technology from SIT, Siliguri in 2008 & M. Tech. in Computer Science & Engineering from NITTTR Kolkata in 2010 under West Bengal University of Technology. Presently she is working as Assistant Professor in Surendra Institute of Engineering & management, Siliguri in the Dept. of C.S.E and also holding key positions in the institute. Her current research focuses on ELearning, Expert System, Secured online Biometric Authentication System. She has published several research papers in International & National Journals and Conferences.

Ritam Dutta

B.Tech. in Electrical & Electronics Engineering from SMIT, Sikkim in 2007 & M. Tech. in VLSI Design from SRM University, Chennai in 2009. Presently he is working as Assistant Professor in Surendra Institute of Engineering & Management, Siliguri in the Dept. of E.C.E. His current research focuses on Secured online Biometric Authentication System, VLSI Design, E-Learning. He is having eleven research papers in International & National Conferences and Journals. He is also an associative member of several International Associations such as IAENG, UACEE, IACSIT etc.