International Journal of Fuzzy Logic and Intelligent Systems, vol. 6, no. 3, September 2006, pp. 247-254

PC-based Hand-Geometry Verification System

Young-Tak Kim[*], Soo-Jong Kim[*], Chang-Gyu Lee[*], Gwan-Hyung Kim[**],
Sung-In Kang[**], Jae-Hyun Lee[**], Han-Ho Tack[***], Sang-Bae Lee[*]

*** Division of Radio and Information Communication Engineering, National Korea Maritime University.**
**** TongMyong University.**
*****Department of Electronic Engineering, JinJu National University.**

Abstract

Biometrics are getting more and more attention in recent years for security and other concerns. So far, only fingerprint recognition has seen limited success for on-line security check, since other biometrics verification and identification systems require more complicated and expensive acquisition interfaces and recognition processes. Hand-Geometry can be used for biometric verification and identification because of its acquisition convenience and good performance for verification and identification performance. It could also be a good candidate for online checks. Therefore, this paper proposes a Hand-Geometry recognition system based on geometrical features of hand. From anatomical point of view, human hand can be characterized by its length, width, thickness, geometrical composition, shapes of the palm, and shape and geometry of the fingers. This paper proposes thirty relevant features for a Hand-Geometry recognition system. This system presents verification results based on hand measurements of 20 individuals. The verification process has been tested on a size of 320×240 image, and result of the verification process have hit rate of 95% and FAR of 0.020.

Keywords: Biometrics, Hand-Geometry, Identification, verification

2. Introduction

As organizations search for more secure authentication methods for user access, e-commerce, and other security applications, biometrics is gaining increasing attention. Biometrics offer greater security and convenience than traditional methods of personal recognition.

Biometrics is the integral and distinctive parts of human beings. As such, they offer a natural convenience and technical efficiency that other authentication mechanisms which must be mentally remembered or physically produced, do not. For this reason, biometrics can provide identity assurance for countless everyday activities currently protected by traditional means of access control [1, 2]. Thus, biometrics system is gaining more use in admission control systems. They are also widely applied for detection of diligence and laziness in management related systems, criminal investigation, ATM, electronic commerce verification systems, etc.

Reliable identification also makes financial and business dealings safer and more efficient, if only by making the participants more accountable for their actions. When we automate the authentication process, we broaden the range of valuable tasks that computers and other devices can perform for us. These automated authentication processes can bring greater security, efficiency, and convenience to our lives. Automated authentication makes it possible to tailor the way that a device responds to different people and to ensure that it confidently responds to people in a correct manner.

Biometric authentication relies on any automatically measurable physical characteristic or personal trait that is distinctive to an individual. Common biometric verification techniques try to match measurements from an individual's fingerprint, hand geometry, eye, face, signature verification or voice to measurements could have been previously collected from them. There are two general applications for this: identification and verification. The biometric authentication process begins with a biometric sensor of some kind. With identification, the biometric system asks and attempts to answer the question, "Who is X?" In an identification application, the biometric device reads a sample, processes it, and compares it against every record or template in the database. This type of comparison is called a "one-to-many" search (1: N). Depending on how the system is designed, it can make a "best" match, or it can score possible matches, ranking them in order of likelihood. Identification applications are common when the goal is to identify criminals, terrorists, or other anti-social elements. In case of verification, when an individual tries to log in, the sensor collects a biometric reading from them and generates a biometric template from the reading, which becomes the authenticator. The verifier is based on one or more biometric readings previously collected from the same individual. The verification procedure essentially measures how closely the authenticator matches the verifier. If the system decides that the match is "close enough" the system authenticates the respective individual; otherwise authentication is denied. In this paper our

---

Manuscript received Jun. 8, 2006; revised Sep. 13, 2006.

focus is on verification rather than identification. It is desirable that such measurements be non-invasive and simple to perform.

In this paper we focus on the use of shape of the hand as a biometric feature in verification systems. Hand geometry-based verification systems are not new and have been available since the early 1970s. However, there is not much open literature addressing the research issues underlying hand geometry-based identity authentication; much of the literature is in the form of patents [3, 4, 5] or application-oriented description. The recognition of the shape of the hand is based on geometrical structure of the hand. This structure includes width of the fingers at various locations, width of the palm, thickness of the palm, length of the fingers, etc., as shown in Fig. 1. However, unlike palm print verification methods [6], our method does not involve extraction of detailed features of the hand (such as, wrinkles on the skin).

In recent years Jain at el [7, 8, 9] have discussed the merits of hand geometry as a useful biometric. Alexandra at el [10] have proposed a peg-free method. We have extended upon such previous studies by employing state of the art technology, color information in image etc. We have also proposed a set of 30 features that we consider most useful for hand geometry biometric.

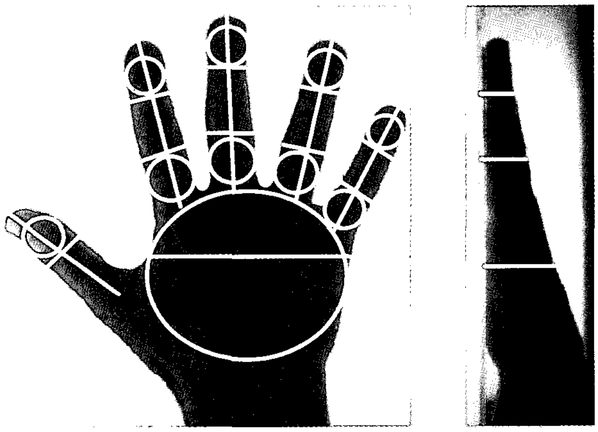


Figure 1. Extraction of geometric feature data from a hand image

Hand geometry is based on the fact that virtually every person's hand is shaped differently than another person's hand and that the shape of a person's hand (after a certain age) does not significantly change its shape. Hand geometry based authentication is limited in scalability but it is an extremely user-friendly biometric. Various methods are used to measure the hand; these methods generally fall into one of two categories - mechanical or image-edge detection. Either method produces estimates of certain key measurements of the hand (length of fingers and thumb, widths, etc.); this data are used to "categorize" a person. To derive such gross characteristics, a relatively inexpensive camera can be employed resulting in a overall low cost of the system. As the computation is also fairly easy, a standalone system is easy to build. As this biometrics is not seen to compromise user privacy, it is quite widely accepted. However, hand geometry based authentication systems are less accurate than fingerprint-based authentication techniques.

In this paper we call shape of the hand the Hand-Geometry and discuss the selection of thirty relevant features for a verification system. We implement a PC-based Hand-Geometry recognition system that extracts and recognizes these feature data in real time.

2. Image Acquisition System

Figure 2 shows the image acquisition system used to acquire a Hand-Geometry image.

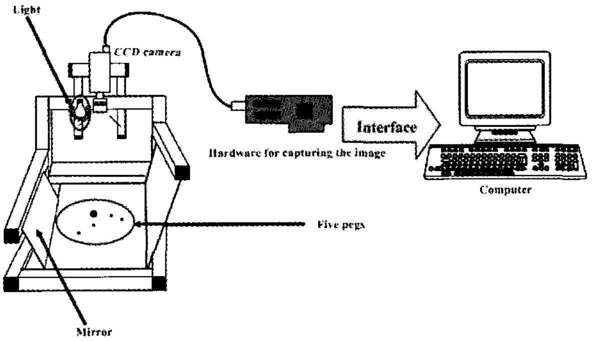


Figure 2. The composition of image acquisition system..

The system consists of a light, a CCD camera, a mirror, a flat surface, five pegs and hardware for capturing the image. The hardware board for capturing the image was specifically designed by us for this system and it was interfaced with the PC. The inclined vertical mirror on the left, provides additional images, from the reflection, a flat surface in the left figure is lined with five pegs for proper alignment of the user's hand.

Figure 3 shows the Hand-Geometry image that is obtained using the Image Acquisition System. Figure 3 shows a live visual feedback of the top-view and the side-view of the hand.

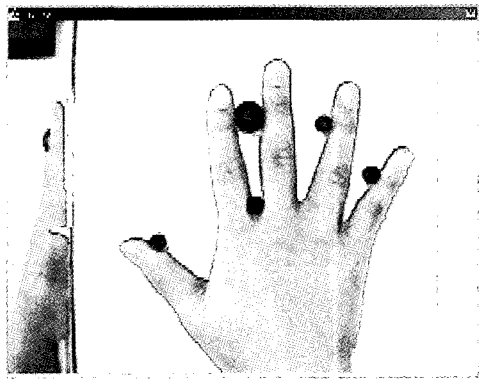


Figure 3. The Hand-Geometry using image acquisition system

The system has following functionality: (i) assist the user in correct positioning of the hand on the surface of the device; (ii) acquires images of the user's hand; (iii) displays images that were captured previously; (iv) extracts features from a given image; (v) registers the user in a database along with the extracted feature vector; (vi) checks whether a given image of the hand matches any of the entries in the database; (vii) updates a particular user's entry in the database by re-computing the feature vector.

As shown in Fig. 3 the color image of the hand is in analog form and an A/D conversion board converts the analog data into a 320×240 pixel color image with 32bits/pixel which is then stored into the computer memory.

In this paper as shown in Fig. 4 the Hand-Geometry verification process involves three steps.

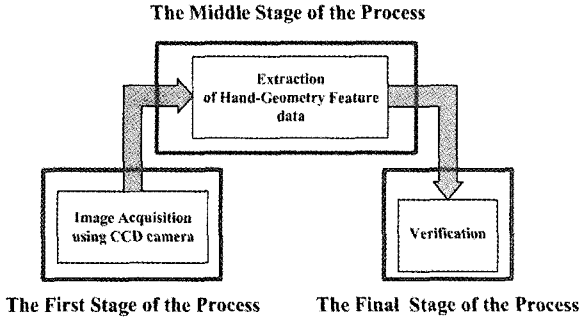


Figure 4. The whole process of Hand-Geometry verification

In the first stage of the process we acquire the Hand-Geometry image using a CCD camera which is part of the image acquisition system. During the middle stage we process the Hand-Geometry image, by extracting feature data of Hand-Geometry after conversion of the color image into a gray image. In the final stage of the process the system identifies the person from the extracted feature data of Hand-Geometry and displays the result by LED and LCD.

3. Extraction of Hand-Geometry Feature Data

The Hand–Geometry–based authentication system relies on geometric invariants of a human hand. Figure 5 shows the 30 axes along which the various features mentioned above have been measured. The five pegs on the image serve as control points and assist in choosing these thirty axes.

Figure 5 shows the thirty features we selected and used in the design of our biometric recognition system. These are length $(L_1 \sim L_5)$, width data $(W_1 \sim W_{15})$ about five fingers, palm's width data (W_{16}), height data of hand $(H_1 \sim H_5)$ and angle data $(A_1 \sim A_4)$ between fingers in the hand geometry.

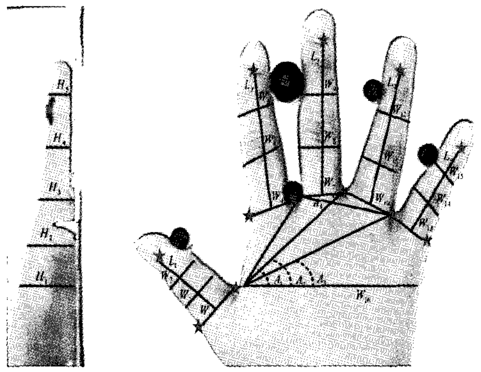
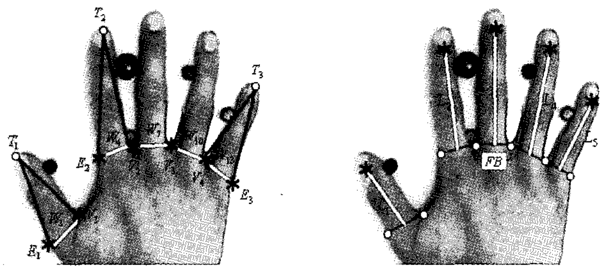


Figure 5. The Hand-Geometry feature data.

As illustrated in Fig. 6 (a), four between-finger valley points are located on the hand boundary. Because the middle finger is the only finger which does not have large spatial variations of its valley points for different placement of the hands, the middle finger baseline is formed by connecting the V_2 and V_3 valley points. The ring finger has two valley points (V_3 and V_4) as well.

It is necessary to establish the correct base line for the length measurements. We use valley points (VP; Valley Point) to accomplish that goal. The VPs are points of valley between a finger and the adjacent finger, as shown Fig. 6. We refer to $W_1, W_4, W_7, W_{10}, W_{13}$ measurements as the finger baseline (FB; Finger Baseline).

Figure 6 (a) shows the position of five FBs. The hand is represented as a vector of the measurements selected above. Since the positions of the five pegs are fixed in the image, no attempt is made to remove these pegs in the acquired images.



(a) The Finger Baseline (b) The Finger Length

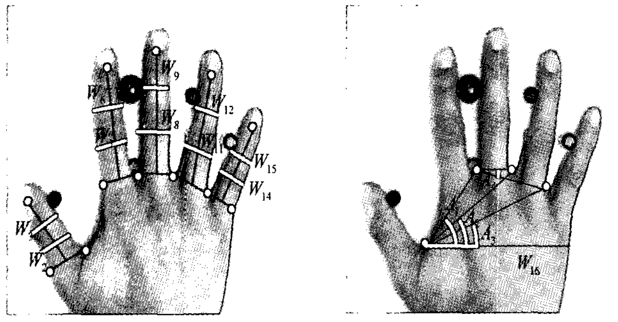
Figure 6. The position of Finger Baseline and Finger Length

The baselines for the thumb, the index finger, and the little finger are formed in the same fashion. We assume that the two end points of each FBs have the same distance from the respective fingertip point. Using one of the respective VPs as one of the end points (V_1, V_2 and V_4), we locate the other end point by searching for the point which has the same distance from the fingertip at another side of the boundary of the finger. The FBs are formed afterwards by connecting pairs of end points.

As seen in Fig. 6 (a), first the three fingertip points (T_1, T_2 and T_3) are identified by image processing. Then three distance measurements, $T_1 - V_1$, $T_2 - V_2$ and $T_3 - V_4$ are obtained and used to locate end points (E_1, E_2 and E_3). There are totally four VPs and three end points which together provide five width measurements.

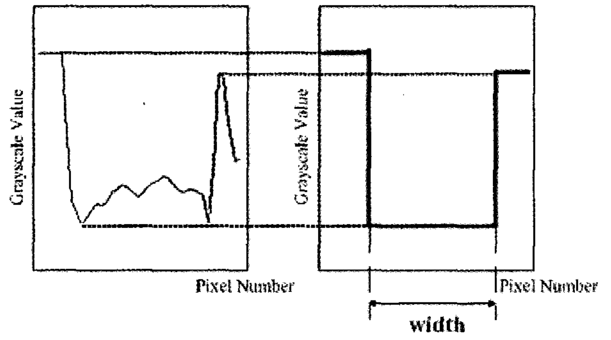
All researchers so far have been using the tip of the nail or the finger as a reference point in extracting the length feature value. For each finger, the fingertip point and the mid-point of its FB (see Fig. 6 (b)) determine the finger length (FL; Finger Length). However, this causes errors in measurement since the nail grows and people get manicures. Based on experimentation we propose the use of the nail bottom (NB; Nail Bottom) as a reference point for the length feature rather than the finger tip. So, the FLs (see Fig. 6 (b)) as L_1, L_2, L_3, L_4 and L_5 are formed by connecting the NB and the mid-point of its FB.

Figure 7 (a) shows the position of ten finger widths (FW; Finger Width). For each finger, the first FW W_i, i=2, 5, 8, 11, 14, is the width at one third of the FL, and the second FW W_j, j=3, 6, 9, 12, 15, is the width at two thirds of the FL.



(a) The Finger Width (b) The Palm Width, Angle

Figure 7. The position of Finger Width and Palm Width, Angle



(a) An observed profile (b) The ideal profile

Figure 8. The projected image along point

In order to offset the effects of background lighting, color of the skin, and noise, the following approach was devised to compute the various feature values. A sequence of pixels along a measurement axis will have an ideal gray scale profile as shown in Fig. 8 (b). The actual gray scale profile tends to be spiky as shown in Fig. 8 (a).

As seen in Fig. 8, for each finger, the FWs are obtained by projecting the grayscale value along a measurement axis (see Fig. 7 (a)).

The palm width (PW; Palm Width) as W_{16}, is obtained in a fashion similar to the FWs (see Fig. 7 (b)). The W_{16} is obtained measuring the width along the horizontal axis starting at point V_1 (see Fig. 6 (a)).

The angle data ($A_1 \sim A_4$) represent the geometry of angles between fingers. The first angle data A_1 is the angle between the PW (W_{16}) and the line formed by V_1 and V_2 (see Fig. 6 (a)), the second angle data A_2 is the angle between W_{16} and $V_1 - V_3$, the third angle data A_3 is the angle between W_{16} and $V_1 - V_4$ and the forth angle data A_4 is the angle between W_7 (see Fig. 6 (a)) and $V_2 - V_4$.

Figure 7 (b) shows the position of PW as W_{16} and angle data ($A_1 \sim A_4$).

Figure 9 shows the position of five height data (HH; Hand Height). The HHs are obtained in the side-view image of the hand. The inclined vertical mirror on the left provides the side-view image, from the reflection.

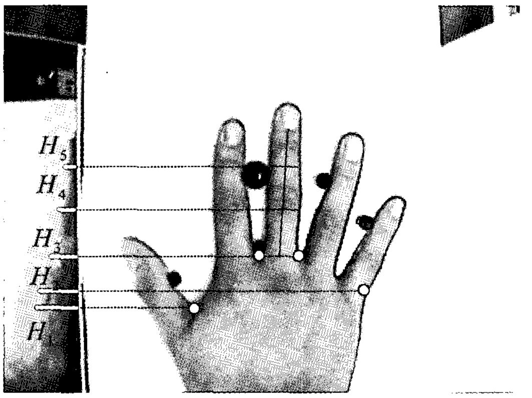


Figure 9. The position of Hand Height

The first HH H_1 is at the extended line of V_1 (see Fig. 6 (a)), the second HH H_2 is at the extended line of E_3 (see Fig. 6 (a)), the third HH H_3 is at the extended line of W_7 (see Fig. 6 (a)), the forth HH H_4 is at the extended line of W_8 (see Fig. 7 (a)), and the fifth HH H_5 is at the extended line of W_9 (see Fig. 7 (a)).

4. Hand-Geometry Verification Algorithm

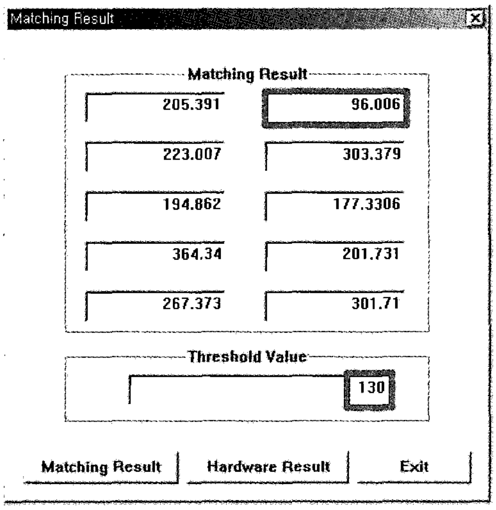
In this subsection we shall discuss the verification process for finding the best match from the enrolled feature data for a newly acquired hand image using an absolute distance metrics.

We refer to the feature data of Hand-Geometry that is enrolled in advance as $F = (f_1, f_2, \cdots, f_{30})$. The feature data of Hand-Geometry for a newly acquired image is referred to as $Y = (y_1, y_2, \cdots, y_{30})$. The absolute distance between two data is calculated corresponding to the following equation:

$$\sum_{i=1}^{30} |y_i - f_i| < \varepsilon_a \qquad (1)$$

The entire process of is as follows (1). The thirty feature data of Hand-Geometry, extracted using the method discussed in section 3 are enrolled in a database along with the user's name in advance. In this study we enrolled thirty feature data of Hand-Geometry for ten users along with each user's name in the database. Then when a user tries to gain access, the same image acquisition system extracts the thirty feature set data from his hand and compares it with the stored data using equation (1). If the result is within the tolerance ε_a, then the user gains access otherwise he/she is denied access.

The Hand-Geometry verification system was trained and tested using a database of 10 users. Ten images of each user's hand were captured. Figure 10 shows the result of an experiment. The accessed user from enrolled users is granted access only if the measured deviation (see equation (1)) within the tolerance ε_a, otherwise he/she is denied access. In Fig. 10 the distance measure (equation (1)) for all 10 stored data are shown. It can be seen that 96 is the closest match. The ε_a value (i.e. threshold in Fig. 10) is 130, hence the access will be granted.



205.391 96.006
223.007 303.379
194.862 177.3306
364.34 201.731
267.373 301.71

130

Figure 10. The matching result

5. Experiments and Results of the PC-based Hand-Geometry Verification System

In this section we describe the PC-based Hand-Geometry recognition system that has been designed to extract the feature data of Hand-Geometry using GA, and discuss experiment and results using that system.

In this section we shall discuss the implementation of the environment for the experiments. Figure 11 shows the experimental setup. The flat surface in the left figure is lined with five pegs for proper alignment of the user's hand. The inclined vertical mirror on the left provides additional images, from the reflection. A single CCD camera can be seen which is meant to capture the image from the top. The camera acquires the direct image as well as the reflection as seen in Fig. 3.

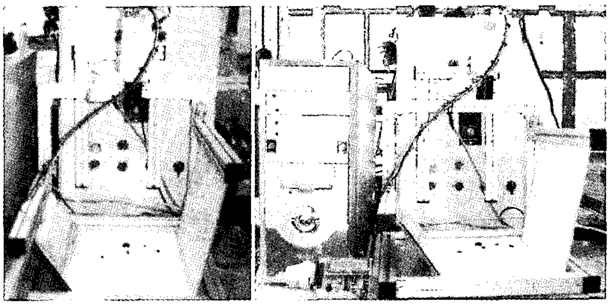


Figure 11. Image acquisition system and the entire Hand-Geometry recognition system

Figure 12 shows the procedure for the acquisition of an image using the appropriate environment for an experiment.

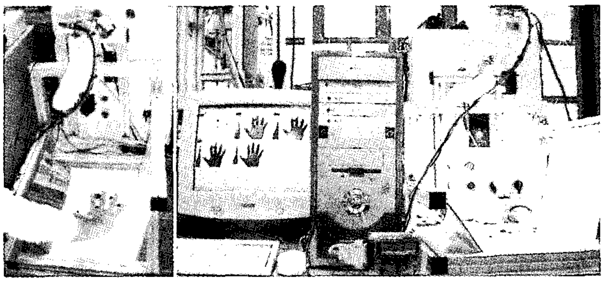


Figure 12. Image acquisition and process monitoring

As shown in Fig. 12 the user is asked to place his right hand on the acquisition surface which has five pegs for consistency in image acquisition. The color image of the hand is in analog form and an A/D conversion board converts the analog data into a 320×240 pixel color image with 32bits/pixel which is then stored into the computer memory. The figure on the left shows the computer monitor which displays the color images that are acquired by the system. We transform the acquired color image into a gray image, and extract the thirty feature data of Hand-Geometry using the method discussed in section 3, and then perform the recognition task using the extracted feature data of Hand-Geometry. Finally the result is displayed as green or red by and LED and a LCD displays the message access granted or denied.

The enrollment phase involves one of the following two tasks: (i) add a new user to the database; (ii) update a current user's feature vector. During the enrollment phase, ten images of the same hand are taken in succession; the user removes his hand completely from the device before every acquisition. These five images are then used to compute the feature vector of the given hand re-computing a feature vector simply involves averaging the individual feature values.

A database was created by obtaining feature data from hand geometry of twenty people. Ten people had painted their nails with blue color and other ten had used red color. Experiments were conducted for performance evaluation by varying the tolerance value, ε_a (see equation (1)). The goal was to determine the impact of tolerance value on performance when the nail color changed to a value other than the one stored in the database. During experiments each person in the database was asked to attempt five times to gain access using the hand recognition system. Hence totally 100 attempts were made. During each attempt the users change of the nail color to various combinations.

There are different methods to rate the accuracy offered by the biometric system like False Rejection Ratio (FRR), false Acceptance rate (FAR). Both methods focus on the system's ability to allow limited entry to authorized users. However, these measures can vary significantly, depending on how you adjust the sensitivity of the mechanism that matches the biometric.

For example, you can require a tighter match between the measurements of hand geometry and the user's template (increase the sensitivity). This will probably decrease the false-acceptance rate, but at the same time can increase the false-rejection rate. In this study we focus on FAR as a performance evaluation measure.

Table 2. The performance about system

Threshold	Hit Rate(%)	FAR
30	24	0
40	47	0.003
50	56	0.006
60	69	0.0073
70	70	0.0078
80	72	0.008
90	84	0.0115
100	91	0.017
110	93	0.0181
120	95	0.020
130	95	0.020
140	95	0.020
150	95	0.020

. Table 1 and Figure 14 show the result of varying ε_a from 30 to 150 in steps of 10. For $\varepsilon_a = 30$, 24 attempts were successful (i.e. Hit rate = 24%) and 76 were unsuccessful. At the same time all 24 persons were correctly identified (i.e. FAR = 0). As threshold increased Hit rate increased till it reached 95% for $\varepsilon_a = 120$. However some of the person's granted accesses were misidentified (i.e. False Acceptance). For $\varepsilon_a = 120$ such misidentification occurred for 2 persons resulting in FAR of 0.02.

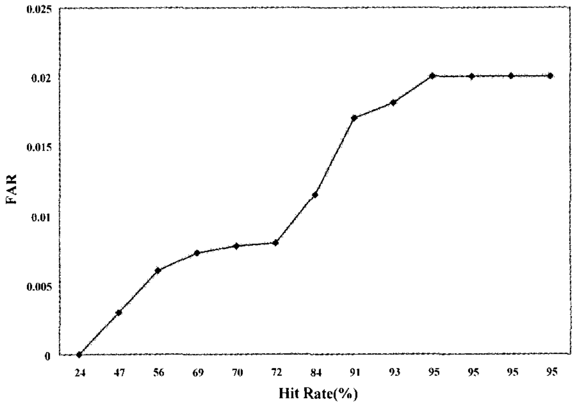
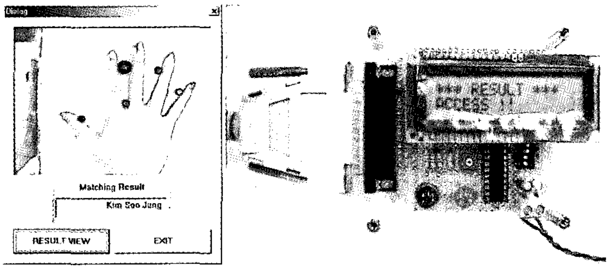


Figure 14. The performance for the Hand-Geometry recognition system

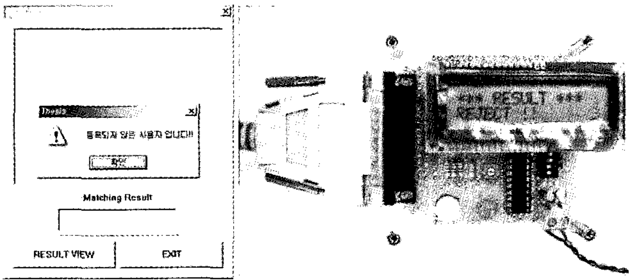
Figure 15 and Figure 16 show the result of access granted or denied for the particular experiments involving a user trying to gain access. Figure 15 shows the displayed result as green by LED and the corresponding message, "access" by LCD. In this case the user was one of the enrolled persons, hence he was granted access.



Kim Soo Jung

Figure 15. The recognition result of enrolled user

Figure 16 shows displayed result as red by LED and the corresponding message "reject" by LCD. In this case the user was an intruder, hence he was denied access.



등록되지 않은 사용자 입니다!!

Figure 16. The recognition result of user not enrolled in the database

6. Conclusions

With the increased concerns in security and other privacy issues, any biometric which proves better in usage towards security applications for the computer visions and the machines gets highly enhanced and widely accepted. At present there is an opportunity for dual or multiple biometrics to be used at the same time. Hand geometry feature that we have proposed in this paper can be an excellent candidate for such systems specifically when face recognition is involved. We have discussed the design of a Hand Geometry verification system for applications involving person authentication and access control. Hand geometry as biometric has several advantages such as ease of data acquisition, simpler feature vectors, smaller databases etc. This makes it easier to manage databases for person authentication and the computations for pattern matching are quite straight forward. In this paper we have presented the results of an actual PC based system which is in operation.

A set of experiments were conducted in order to carry out the performance evaluation of this system. The experiments showed that such a system can be a good tool when the users are expected to cooperate during authentication. If the user does not comply with the requirements of data acquisition phase they are not granted access.

We have proposed a set of 30 feature values that can be useful in acquiring data from a person's hand geometry. We have also employed a novel technique based on Genetic Algorithms for marking the exact location of the Nail Bottom in an acquired image. Exact location of nail bottom is important since if plays an important role in calculating the numeric values of many of the features in our system. We have used colors in the acquired image as an additional dimension in the determination of the location of the Nail Bottom. As a result the accuracy of the system improved considerably due to exact location of the NB.

Hand geometry, as compared to some other means of biometric identification (notably fingerprints), does not produce a large data set. Therefore, given a large number of records, hand geometry may not be able to distinguish one individual from another who has similar hand characteristics. Simply, as the size of the database grow, there must be an increase in the number of distinguishing characteristics of the biometric used in order to place the individual into an increasingly narrow "band" of individuals who share similar biometric characteristics. Reliable personal recognition is critical to many business processes. Since conventional knowledge-and token-based methods rely on surrogate representations of a person's identity to establish personal recognition, any system assuring reliable positive personal recognition must necessarily involve a biometric component. In fact, a sound personal recognition system design must incorporate many biometric and non-biometric components. Biometric-based systems also have limitations with adverse implications for a system's security. For example, the accuracy of current biometric systems is not perfect, and elaborate spoofing attacks can defeat a practical biometric system. Although the evolution of biometric technology will surely overcome some of these limitations, 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 can adversely affect system resources and information assets. A system's security requirements depend on the application's requirements (the threat model) and the cost-benefit analysis. In our opinion, properly implemented biometric systems are effective deterrents to perpetrators.

References

[1] U. Feige, A. Fiat and A. Shamir, "Zero Knowledge Proofs of Identity," Journal of Cryptology, Vol.2, Pages 77-94, 1998

[2] D. Chaum, "Security without identification: Transition systems to make big brother Obsolete," Communications of the ACM, Vol. 28, pages 1935-1044, 1985

[3] R. P. Miller, "Finger dimension comparison identification system," US Patent No.3576538, 1971.

[4] R. H. Ernst, "Hand ID system," US Patent No. 3576537, 1971.

[5] I. H. Jacoby, A. J. Giordano, and W. H. Fioretti, "Personnel Identification Apparatus," US Patent No. 3648240, 1972.

[6] J.R. Young and H.W. Hammon, "Automatic Palmprint Verification Study," Rome Air Development Center, RADC-TR- 81-161 Final Technical Report, June, 1981.

[7] A.K. Jain, N. Duta, "Deformable matching of hand shapes for verification," Proceedings of IEEE International Conference on Image Processing, October 25-28, Kobe, Japan, 1999

[8] A. Kumar, D.C.M. Wong, H.C. Shen, A.K. Jain, " Personal Verification Using Oalmprint and Hand Geometry Biometric," Proc. Of 4th Int'l Conf. on Audio-and Video-based Biometric Person Authentication (AVBPA), pp. 668-678, Guildford, UK, June 9-11, 2003.

[9] A.K. Jain, A. Ross, and S. Pankanti, "A Prototype Hand Geometry-based Verification System," 2nd International Conference on Audio- and Video-based Biometric Person Authentication, pp. 166-171, Mar, 1999.

[10] Alexandra L.N. Wong and Pengcheng Shi, "Peg-Free Hand Geometry Recognition Using Hierarchical Geometry and Shape Matching," IAPR Workshop on Machine Vision Applications, pp. 281-284, December, 2002.

Young-Tak Kim received the B.Sc degree in Department of Electronic Engineering from Jinju National University in 2001, and M.Sc degree in Department of Radio and Information Communication Engineering from Korea Maritime University in 2003. He is currently pursuing the Ph.D degree in Korea Maritime University, and working as an plural professor at the Mechatronics Engineering Department in Tong-Myong University of Information Technology. His current research interests are Neural Network, Fuzzy Theory, Signal Processing, Pattern Recognition, Machine Vision System and Embedded System.

Phone : +82-51-410-4907
E-mail : yt_kim@bada.hhu.ac.kr

Soo-Jong Kim received the B.Sc and M.Sc degree in Department of Radio and Information Communication Engineering from Korea Maritime University in 2002 and 2004. She is currently working as a professor at the MPS Lecture Team in Tong-Myong University of Information Technology. Her current research interests are Neural Network, Fuzzy Theory, Signal Processing, Pattern Recognition, Machine Vision System and Embedded System.

Phone : +82-51-410-4907

Chang-Gyu Lee received the B.S. degree in Department of Electronic Engineering from the Jinju National University, Jinju, Korea in 2001, the M.S. degree in Division of Radio and Information Communication Engineering from Korea Maritime University, Busan, Korea in 2003. At present, He is researching into control and measurement system of nuclear plant. His research interests include artificial intelligent, fuzzy control theory, microprocessor.

Phone : +82-51-410-4907
E-mail : lck1215@bada.hhu.ac.kr

Gwan-Hyung Kim Ph.D of Electronic Engineering, He is currently working a full-time lecturer Dept. of Computer Engineering in DongMyong University. His research interests include Intelligence Control(Fuzzy, Neural Networks), GA, Signal Processing, Nonlinear System Control, Robotics and so on.

Sung-In Kang received the Ph.D. degrees in electrical communication from Korea Maritime University. He is currently a Full-Time Instructor in Dept. of Computer Engineering, Tongmyong University. His research interests include artificial intelligence, signal processing, and automatic control.

Jae-Hyun Lee received the Ph.D. degrees in electrical communication from Korea Maritime University. He is currently a Full-Time Instructor in the School of Port Logistics, Tongmyong University. His research interests include human interface and artificial intelligent control.

Han-Ho Tack was born july 6. 1959. He received the B.S. degree in Department of Electronic Engineering from Bukyung National University, Busan, Korea, in 1987 He received the M..S. degree in Department of Electronic Engineering from Dong-A University, Busan, Korea, in 1992. He received Ph. D. degree in Department of Electronic & Communication Engineering from the Korea Maritime University, Busan, Korea, in 1998. From 1987 to 1989, he was a Researcher at the Laboratory of Hung Chang Co. Ltd. Since 1991, he has been a faculty member of the Electronic Engineering at the Jinju National University, where he is currently a associate Professor. His research interests are Neural Network, Fuzzy System, Robotics, Factory Automation, Mechanical Vibration, Transfortation, and Multimedia System etc. He is a member of IEEE, KIMISC, KMS, KIEE, and KFIS.

Sang-Bae Lee Ph.D of Electronic Engineering, The Professor of Korea Maritime University, The Director of Fuzzy-Neuro Control Laboratory in Korea Maritime University, The Research Fellow of Intelligent System Research Laboratory(ISRL) in Saskathewan University, Canada, 1993.7-1994.7, A Editor of International Journal of Knowledge-Based Intelligent Electronic Systems, A Editor of International Journal of Control and Intelligent Systems, The interesting parts are Fuzzy Logic, Neural Network, Nonlinear System, Robotics, Welding System and so on.